



**PANTEION UNIVERSITY OF SOCIAL AND
POLITICAL STUDIES OF ATHENS**

Department of Public Administration
Master Program in Tax and Auditing

Master Thesis

***Cyber-security and Cyber-preparedness
as a Necessary Part of the Auditing Process***

ANASTASIA KOUKI, B.Sc., MoA,

(A.M. 7117M035)

Supervisor: ***Prof. Ioannis Filos***

(Professor in Accounting and Auditing,
Department of Public Administration, Panteion University)

Athens, May 2019

Triparty Scientific Committee:

Dr. Ioannis Filos, Professor in Accounting and Auditing, Department of Public Administration, Panteion University. (Supervisor)

Dr. Apostolos Apostolou, Emeritus Professor in Accounting, Department of Public Administration, Panteion University.

Dr. Konstantinos Liapis, Associate Professor in Accounting and Business Administration, Department of Economic and Regional Development, Panteion University.

DISCLAIMER

This Master Thesis is the genuine and authentic work of my personal intellectual capacities and knowledge on the examined matter. No part of this Thesis is the work of someone else, natural, and/or legal person. In case it was needed to transfer original passages from a source, such as legal definitions and parts of laws, as well as tables and images, we have proceed to this action with caution and by putting the original passages in brackets and written in italics, and by referring the relevant source.

Copyright @ Anastasia Kouki, 2019

All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, for any trade purpose. It is allowed, though, the printing, storage and distribution of this publication only for non-profit, educative and scientific reasons, if only there will be reference about the origin of the information and the reference to this message.

Questions about the use of this Master Thesis for trade and profit reasons cam be submitted directly only to the writer of the Thesis.

The approval of this Master Thesis from Panteion University of Social and Political Studies does not mean and the approval of writer's opinions.

... To all my
professors,
for making me realize the best capacities of
myself,
and empowered me to pursue my professional and scientific
ambitions.

... To all the great scientists and
philosophers,
that make darkness (even in online worlds) less
powerful.

A C K N O W L E D G M E N T S

This Master Thesis is part of my studies in master level from the Department of Public Administration in Panteion University of Athens, Greece, in specialization of “Tax and Auditing”. Now, that I am reaching the final stage of my studies I would like to express my gratitude to all the wonderful people and scientist, that make this journey possible and so unique for me.

Firstly, I own my deepest gratitude to **Prof. Ioannis Filos**, Associated Professor in Accounting and Auditing, Department of Public Administration, Panteion University, firstly, because he motivated me the most to give the passing exams and to enter in this Master Program, secondly, for his constant guidance concerning not only the thematic of my Master Thesis, but also in its general concretization of ideas, methodology and capacity building. I would like to thank him also for including me in the official extension of the submitting deadline due to a health issue of mine, in which he has shown great empathy. He is not only an inspiring professor, perhaps the ultimate reason why I started be interested in auditing science and profession, but also a trustworthy and eloquent human, something that everyone could noticed during his master lessons “*Methodology of Research*”, “*Auditing and Auditing Standards*”, “*Special Subjects on Accounting and Auditing*” and “*Special Subjects on Contracts and Applied Public Auditing*”.

I would like also to thank **Prof. Apostolos Apostolou**, Emeritus Professor in Accounting and Auditing, Department of Public Administration, Panteion University, not only for the extremely useful knowledge that provide to us during his master lessons on “*Financial Accounting and International Accounting Standards*” and “*Financial Assessment and Business Administration*”, but also for his eternal youthfulness and energy in pursuing his academic aspirations, something that is always great inspiration for me.

It would be a great negligence of mine not to thank the Emeritus Professor in Accounting Business Administration, **Prof. K. Liapis**, the third part of our professor’s triumvirate scientific committee in this Master Program for his positive judgement about my Master Thesis and of course, Emeritus Professor in Accounting and Auditing, **Prof. Anastasios Tsamis**, who gave me mindful incentive as it concerns cybersecurity compliance

issues in corporate governance and in the banking sector, based on the Basel Committee on Banking Supervision Pillar Framework requirements, during his lessons on “*Governance of Corporations and Institutions*” and “*Tax and Corporate Decisions*”.

Last but not least, I must express my gratitude to the only one female professor in this Master Program, **Lecturer Dr. Virginia Theodoropoulou**, a profound law expert in entrepreneurship law and government. She presented us all the fundamental aspects of contracts during the lesson on “*Special Subjects on Contracts and Applied Public Auditing*”.

Moreover, I must truly express my gratitude to **Stamatis Passas**, a guest expert to this Master Program, an expert (in theoretical and practical level) in IT systems, who provided me with useful material and guidance as it concerns aspects of systematic approach upon IT context, that I was not that familiar with.

What is more, I would like to thank for all the knowledge, moral standards and food for thought they provide to us during our one-year lessons all the other visiting professor, experts and guest lecturers: (a) **Prof. George Alifantis**, an amazing aspiring professor on accounting, retired certified accountant-auditor, that despite his senior age, his affection and great morality for accounting science is a true life inspiration; (b) **George Koromilas**, a profound accountant and expert and writer in taxation law, practice and systems, President of the Institute of Economic and Tax Studies for his passion and dedication for high-quality research and professionalism; (c) **BSc, BSc, MSc, MBA, PhD (cand). Varvara Velli**, for introducing us to the theory and practice of creating and assessing data for scientific and academic purposes and quality techniques for writing papers for academic reasons; and (d) **Prof. (BSc, MSc, PhD, Post-Doc) Andreas Georgantopoulos**, not only for his general kindness and amazing scientific capacities, but also for providing me useful food for thought and tools on how to best articulate this Master Thesis. His contribution on

Closing this part of my Master Thesis, I would like to thank all these scientists, experts, auditors, practitioners, academia, theorist, journalist, etc. all around the world for evolving the science, the theory and the practice of cybersecurity and cybersecurity preparedness in order to build long-lasting capacity to the auditing science, methodology and application.

I N D E X		
<i>THEMATIC</i>		<i>PAGE</i>
	ACKNOWLEDGMENTS	4
	INDEX	6
	TABLES	8
	IMAGES	8
	ABBREVIATIONS	9
	ABSTRACT	14
	ΠΕΡΙΛΗΨΗ	16
I	INTRODUCTION	18
	1 Is necessary to integrate cybersecurity and cyber-preparedness in the auditing processes?	18
	2 Introduction to the thematic and sub-thematics of the Thesis	22
	3 Structure of the Thesis	26
II	CHAPTER 1: THE IMPORTANCE OF INCLUSION OF CYBERSECURITY IN AUDITING SERVICE	28
	1 A Historical-Philosophical Perspective	28
	2 The Modern Business Risk Model, Cybersecurity and the Role of Auditing	33
	3 Conclusions	40
III	CHAPTER 2: UNDERSTANDING CYBERSECURITY ENVIRONMENT AND ITS RISKS AND CYBERSECURITY INTERNAL CONTROLS OF THE CLIENT ENTITY	42
	1 Appointment of the IT/Cybersecurity Auditor by the client entity and Cybersecurity Risks Environment	42
	2 Understanding the Correlation between Cybersecurity Dimension and Entities' Internal Controls Systems	47
	3 Presentation of the Most Important Cybersecurity Risks and Entities' Internal Controls	51
	1 Malicious Code and Programs	55
	2 Harmful Malwares	58
	3 Social Engineering and Phishing	59
	4 (Distributed) Denial of Service Attacks	61
	5 Ransomware	62
	6 CEO/CFO scams or Whaling and Identity Thefts	62
	7 Keylogger	64
	8 Financial Information Disclosure and Use of Social Media Vulnerabilities	64
	9 Supply Chain Vulnerabilities	68
	10 Intellectual Property Cyber-thefts and Industrial Cyberespionage	70
	11 Vulnerabilities due to Emerging Technologies	71
	A Blockchain, Smart Contracts and Crypto-assets	72
	B Electronic commerce or e-commerce and e-governance	85
	C Artificial Intelligence	86
	D Internet of Things	88
	E Cloud Services and Software as a Service (SaaS)	88
	12 Outdated Technology Vulnerabilities	89
	13 Conclusions on Cybersecurity Risks and Entities' Internal Controls	90

	4	Understanding an Entity’s Operational Environment and Presentation of the Most Important Cybersecurity Compliance Frameworks		91
		1	National Level	92
			A Great Britain	92
			B United States of America	97
		2	The European Union Auditing-Related Cybersecurity System	153
		3	Conclusions on Cybersecurity Regulatory Compliance Frameworks	165
	5	Understanding the Cybersecurity Risks’ Internal Controls System		167
	6	Conclusions		173
IV	CHAPTER 3: PLANNING AND EXECUTING A CYBERSECURITY AUDITING PROGRAM			175
	1	The Cybersecurity Auditing Program and its Particles		175
	2	Compliance with Cybersecurity Auditing Frameworks		176
		1	The ISO Cybersecurity Auditing Framework	177
			A The ISO Auditing and Auditing Management Standards	177
			B ISO/IEC 27000 Standards Family on Information Security Management Systems and Cybersecurity Auditing	179
		2	ISACA’S Cybersecurity Auditing Framework	188
	3	Planning a Cybersecurity Auditing Program		200
		1	Understanding the areas and the subjects of concern related to cybersecurity and setting of the scope of the Audit Programme	201
		2	Assessing Cybersecurity Risks	201
		3	Developing a detailed cybersecurity audit program	206
	4	Executing a Cybersecurity Auditing Program		216
		1	Performing Audit Tests in Internal Controls Systems	218
		2	Paradigms of Specialized Auditing Tests According to Specific Cybersecurity Risks and Vulnerabilities	221
	5	Conclusions		233
V	CHAPTER 4: ISSUANCE OF CYBERSECURITY AUDITING REPORT			235
VI	CHAPTER 5: FINAL CONCLUSIONS ON HOW CYBERSECURIT HAD TRANSFORMED AUDITING SERVICE			240
VII	BIBLIOGRAPHY			245

T A B L E S

No	Title	Page
1	The Audit Risk Equitation in Modern Business Risk Model	36
2	The Basic Steps of Cybersecurity Audit Process	39
3	The four Tiers of NIST's Cybersecurity Framework Version 1.1	125
4	Analytical Presentation of the Five Core Functions and their Categories of NIST's Cybersecurity Framework Version 1.1	126
5	Short History of COBIT Evolution	189
6	Presentation of ITAF's 2014 Standards and Guidance System	195
7	The five levels of impact analysis of cybersecurity threats	203
8	The Risk Rate Matrix for Cyber-security Threats	205

I M A G E S

No	Title	Page
1	The correlation between Inherent Risk, Residual Risk and Risk Appetite in Risk Based Internal Audits	38
2	Blockchain Technology Applications according to World Economic Forum	83
3	The Three Primary Components of NIST's Cybersecurity Framework Version 1.1	125
4	The Core Elements of NIST's Cybersecurity Framework Version 1.1	125
5	Presentation of COSO's Internal Control—Integrated Framework (2013 edition) and its Components	151
6	COBIT 2019 Design Factors	192
7	Governance System Design Workflow	192
8	The Three Basic Categories of IT/cybersecurity Internal Controls	207
9	The Hierarchy of IT/cybersecurity Internal Controls	207
10	Types of Modified Opinions	237

A B B R E V I A T I O N S	
Abbreviation	Meaning
ABC	Activity Based Costing
AI	Artificial Intelligence
AICPA	American Institute of Certified Public Accountants (USA)
AIFMD	Alternative Investment Fund Managers Directive
AML	Anti-Money Laundering Directive
ASB	AICPA's Auditing Standards Board (USA)
ASC	(FASB's) Accounting Standards Codification
ASEC	AICPA's Assurance Services Executive Committee (USA)
ATMs	Automated Teller Machine
AR	Augmented Reality
ARi	Audit risk
CAEs	Chief Audit Executives
CAQ	Center for Audit Quality (USA)
CATs	FBI's Cyber Action Teams (USA)
CCCA	Comprehensive Crime Control Act (USA)
CCIPS	Computer Crime and Intellectual Property Section (DOJ)
CCTA	UK Government's Central Computer and Telecommunications Agency
CDC	Chamber of Digital Commerce (US)
CDPSE	Certified Data Privacy Solutions Engineer (ISACA)
CEO	Chief Executive Officer
CFAA	Computer Fraud and Abuse Act (USA)
CFO	Chief Finance Officer
CFR	Code of Federal Regulations (USA)
CFTC	Commodity Futures Trading Commission
CGEIT	Certified in the Governance of Enterprise IT (ISACA)
CGMA	AICPA's Chartered Global Management Accountant (USA)
CIO	Chief Information Officer
CIPA	Cybersecurity and Infrastructure Protection Agency (USA)
CIPFA	UK's Chartered Institute of Public Finance and Accountancy
CIRTs	AICPA's Computer Incident Response Teams (USA)
CISA	DHS's Cybersecurity and Infrastructure Security Agency (USA)
CISA	Certified Information Systems Auditor (ISACA)
CISM	Certified Information Security Manager (ISACA)
CIT	EC3 Cyber Intelligence Team (EU)
CITP	AICPA's Certified Information Technology Professional (USA)
CLOUD Act	Clarifying Lawful Overseas Use of Data Act (USA)
CMA	Computer Misuse Act (UK)
CMMI	Capability Maturity Model Integration
COBIT	(ISACA's) Control Objectives for Information and Related Technologies
COIN	Contract INtelligence AI system
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPA	Certified Public Accountant
CR	Control Risk
CRISC	Certified in Risk and Information Systems Control (ISACA)
CRM	Customer Relationship Management
CRMP	AICPA's Cybersecurity Risk Management Program (USA)
CSD	CISA's Cybersecurity Division (USA)

CSET	Cyber Security Evaluation Tool (USA),
CSIRTs	Computer Security Incident Response Teams (USA- AICPA & EU)
CSIS	Center for Strategic International Studies
CSO	Chief Security Officer
CSX-P	CSX Cybersecurity Practitioner (ISACA)
CTO	Chief Technology Officer
CUI	Controlled Unclassified Information (USA)
DAAC	Digital Assets Accounting Coalition
DBMS	Database Management Systems
DCS	Distributed Control Systems
DHS	Department of Homeland Security (USA)
DLT	Distributed Ledger technologies
DOJ	Department of Justice (USA)
(D)DoS	(Distributed) Denial of Service
DPA	Data Protection Act (UK)
DPAs	Data Protection National Supervisor Authority (EU),
DPO	Data Protection Officer (EU)
DR	Detention Risk
DUNS	Data Universal Numbering System
EBA	European Banking Authority
EC3	European Cybercrime Centre (EU-EUROPOL)
ECCG	European Cybersecurity Certification Group (EU)
ECR	Efficient Consumer Response
ECRCC	European Cybersecurity Research and Competence Centre (EU)
ECS	Electronic Communication Service
EDI	Electronic Data Interchange
EDPS	European Data Protection Supervisor
EEA	European Economic Area (EU)
EEC	European Economic Community
EFT	Electronic Fund Transfer
EGIT	Enterprise Governance of Information and Technology (ISACA's)
EIOPA	European Insurance and Occupational Pensions Authority
ENCRYPT Act	Ensuring National Constitutional Rights for Your Private Telecommunications Act (USA)
ENIAC	Electronic Numerical Integrator and Computer
ENISA	European Union Agency for Network and Information Security
EPI	Early Purchasing involvement
ERM	Enterprise Risk Management
ERP	Electronic Resource Planning
ESI	Early Supplier Involvement
ESMA	European Securities and Market Authority
EUROPOL	European Union's Agency for Law Enforcement Cooperation
FAQs	Frequently Asked Questions
FASB	Financial Accounting Standards Board
FBI	Federal Bureau of Investigation (USA)
FCA	Financial Conduct Authority (UK)
FCD	Financial Collateral Directive
FEI	Financial Executives International
FD	(Regulation) Fair Disclosure
FinCEN	Financial Crimes Enforcement Network

FINRA	Financial Industry Regulatory Authority
FISIC	Federal Information Security Incident Center (USA)
FISMA	Federal Information Security Modernization Act (USA)
FOIA	Freedom of Information Act (UK & USA)
FSOC	Financial Stability Oversight Council (USA)
FTC	Federal Trade Commission (USA)
GAO	Comptroller General Office (USA)
GAS	Generalized Audit Software
GAAP	US Generally Accepted Accounting Principles
GAATs	Computer Assisted Audit Techniques
GDPR	General Data Protection Regulation (EU)
GLBA	Gramm-Leach-Bliley Act or Financial Modernization Act (USA)
GSMA	Global System for Mobile Communications Association
GTAG	Global Technology Audit Guide (IIA)
HHS	Department of Health and Human Services (USA)
HIRT	Hunt and Incidence Response Teams
IaaS	Infrastructure as a Service
IAASB	International Auditing and Assurance Standards Board
IAS	International Accounting Standard
IASME	Information Assurance for Small and Medium Enterprises
IC3	FBI's Internet Crime Compliant Center (USA)
ICFRs	internal controls over financial reporting
ICO	Information Commissioner's Office
ICOs	Initial Coin Offerings
ICS	Industrial Control Systems
I(C)T	Information (Communications) Technology(ies)
IESBA	International Ethics Standards Boards for Accountants
IFAC	International Federation of Accountants
IFRS	International Financial Reporting Standards
IIA	Institute of Internal Auditors
IMA	Association of Accountants and Financial Professionals in Business
INTOSAI	International Organization of Supreme Audit Institutions
IOCTA	EC3's Internet Organized Crime Threat Assessment (EU-EUROPOL)
IoT	Internet of Things
IOV	Internet of Value
IP	Intellectual Property
IP Gateway	Infrastructure Protection Gateway (USA)
IPOs	Initial Public Offerings
IR	Inherit Risk
IRS	Internal Revenue Service
IS(s)	Information System(s)
ISA	International Standards on Auditing
ISACA	Information Systems Audit and Control Association
ISD	DHS's Infrastructure Security Division (USA)
ISF	Information Security Forum
ISMS	Information Security Management Systems
ISO/IEC	International Organization for Standardization/ International Electrotechnical Commission
ISQC	International Standard on Quality Control
ISSAI	International Standards of Supreme Audit Institutions (INTOSAI)

ITAF	(ISACA’s) Information Technology Assurance Framework
ITAM	Information Technology and Assurance Management (USA)
ITIL	UK’s Information Technology Infrastructure Library
ITL	NIST’s Information Technology Laboratory (USA)
ITSM	IT Service Management
J-CAT	EC3 Joint Cybercrime Action Taskforce (EU-EUROPOL)
JOBS Act	Jumpstart Our Business Startups Act (USA)
KPMG	Klynveld Peat Marwick Goerdeler (Big 4 Audit Firm)
LANs	Local Access Networks
LIFO	Last-In, First-Out (method of measured)
LLP	Limited Liability Partnership
MEECES	Money, Ego, Entertainment, Cause, Entrance and Status
MFA	multi-factor authentication
MICE	Money, Ideology, Compromise/Coercion, Ego/ Extortion
MiFID	Market in Financial Instruments Directives
MRP(S)	Material Requirement Planning (Systems)
NACD	National Association of Corporate Directors
NATO/OTAN	North Atlantic Treaty Organization/Organisation du Trait� de l’Atlantique Nord
NCAS	National Cyber Awareness System (USA)
NCCIC	National Cybersecurity and Communications Integration Center (USA)
NCFTA	FBI’s National Cyber-Forensics & Training Alliance (USA)
NCIJTF	FBI’s National Cyber Investigative Joint Task Force (USA)
NCSC	National Cyber Security Centre (UK)
NFIB	National Fraud Intelligence Bureau (UK)
NHS	Network(s), Hardware and Software
NICE	National Initiative For Cybersecurity Education (USA)
NIS Directive	Network and Information Security (EU’s Regulations)
NIST	National Institute of Standards and Technology (USA)
NLP	Natural Language Processing
NPPD	CISA’s National Protection and Programs Directorate (USA)
NRMC	National Risk Management Center (USA)
NYSE	New York Stock Exchange (USA)
OGC	UK’s Office of Government Commerce
OLAF	European Anti-Fraud Office (EU)
OMB	Office of Management and Budget (USA)
OS	Operating System
OWASP	Open Web Application Security Project
PCAOB	Public Company Accounting Oversight Board (USA)
PCI DSS	Payment Card Industry Data Security Standard
PCII	CISA’s Protected Critical Infrastructure Information Program (USA)
PCPS	AICPA’s Private Companies Practice Section (USA)
PCS	Process Control Systems
PESTEL-DG	Political, Economic, Social, Technical, Environmental, Legal-Demographic and Geographic (Analysis)
PIEs	Public Interest Entities
POS	Point of Sales systems
PRA	Bank of England’s Prudential Regulatory Authority (UK)
pwc or PWC	PriceWaterCoopers
RATs	FBI’s Recovery Asset Teams (USA)

RCS	Remote Computing Service
RBAC	Role-Based Access Control
RBIA	Risk Based Internal Audits
RFID	Radio-Frequency Identification
RMF	Risk Management Framework (USA)
RnD	Research and Development
RPA	Robotic Process Automation
SaaS	Software as a Service
SAG	PCAOB’s Standing Advisory Group (USA)
SATs	Software Audit Tools
SBA	Small Business Administration (USA)
SBDCs	Small Business Development Centers (USA -SBA)
SC	Scientific Committee
SCA	Stored Communications Act (USA)
SCADA	Supervisory Control and Data Acquisition
SCCG	Stakeholder Cybersecurity Certification Group ()
SCIF	Secure Compartmentalized Information Facilities
SDLC	Software Development Life Cycle
SEC	Securities and Exchange Commission (USA)
SIEM	Security information and event management
SKUs	Storage Keeping Units
SMEs	Small – Medium (Size) Enterprises
SMS	Short Message Service
SOC	Security Operations Center
SOX	Sarbanes-Oxley Act (USA)
SP	NIST’s Special Publication (USA)
SRM	Supplier Relationship Management
STO	Security Token Offering
Swift	Society for Worldwide Interbank Financial Telecommunications
SWOT (Analysis)	Strengths/weaknesses/Opportunities/Threats (Analysis)
TOGAF	The Open Group Architecture Framework
TTPs	Tools, Techniques, and Procedures
UK/GR	United Kingdom/Great Britain
UNCITRAL	United Nations Commission on International Trade Law
USA/HIIA	United States of America/Ηνωμένες Πολιτείες Αμερικής
VAT	Value-Added Tax
VCs	Virtual Currencies
VMI	Vendor Managed Inventory
VoIP	Voice over Internet Protocols
VPN	Virtual Private Networks
VR	Virtual Reality
WEF	World Economic Forum
WISPs	Written Information Security Programs

A B S T R A C T

This Master Thesis aims to provide a deep understanding about the importance and the necessity of cybersecurity and cybersecurity preparedness in auditing processes in modern economic reality. Today entities, no matter if they are public or private or of a mix type, their size (small, medium, large, multinationals, etc.), and in which economic sector they belong to, function in a highly (inter)connected economic environment that demands from them not only to be effectively adapted to current digital applications and demands, but also in order to exist and flourish in long-term, they must shape the new digitalized futures, a reality that is accompanied with a lot of cybersecurity risks and vulnerabilities. Likewise, the auditing sector faces one of its biggest challenge, the cybersecurity dilemma one, which from one side targets to best deal effectively the cybersecurity concerns during auditing tests and controls, and on the other side how to best incorporate digital advancements and their cybersecurity obscurities.

This Master Thesis aims to cover both the above-mentioned aspects of cybersecurity challenge in auditing performances by examining (i) the definitions of cybersecurity and cybersecurity preparedness and their key components (Introduction), (ii) the resonance and its importance of integration of cybersecurity to auditing (Chapter 1), (iii) the importance of understanding the most important types of cybersecurity risks and vulnerabilities in the modern business risk model environment and how entities must respond to these risks by applying the most suitable internal controls, as well as the operational legal environment of the client entity, the obligation of compliance with most important cybersecurity national regulative frameworks (United Kingdom and United States of America) and the European Union's cybersecurity landscape, and the types of controls (preventive, detective, and corrective), that entities apply and auditors must inspect, (Chapter 2), (iv) the major particles of planning and executing a holistic cybersecurity auditing program, and how international standards, like those created by International Standards Organization (ISO) and Information Systems Audit and Control Association (ISACA) provide important guidance in these spheres (Chapter 3), and finally (v) we will examine the process of issuance of the

cybersecurity auditing report (Chapter 4). Our analysis will be based in the provisions of International Auditing Standards (ISA).

In the final chapter (Chapter 5), we will provide our final conclusions about the necessity of inclusion of cybersecurity and cybersecurity preparedness in audit service and how the first had transformed the second.

Key Words: auditing, cybersecurity, cybersecurity preparedness, cybersecurity risks and vulnerabilities, compliance, International Auditing Standards, UK. USA, EU, preventive, detective, and corrective controls, cybersecurity auditing controls, cybersecurity auditing program, ISO, ISACA, cybersecurity auditing report.

Π Ε Ρ Ι Λ Η Ψ Η

Η παρούσα μεταπτυχιακή εργασία στοχεύει στην βαθύτερη κατανόηση της σημαντικότητας και της αναγκαιότητας ενσωμάτωσης της κυβερνοασφάλειας και της κυβερνοετοιμότητας στις ελεγκτικές διαδικασίες και πρακτικές στην σύγχρονη οικονομική πραγματικότητα. Οι σύγχρονες οικονομικές μονάδες, ανεξάρτητα αν ανήκουν στην ιδιωτική ή δημόσια οικονομική σφαίρα ή έχουν μια μεικτή μορφή, ανεξάρτητα το μέγεθός τους (μικρομεσαίες, μεγάλες, πολυεθνικές, κλπ.) και ανεξάρτητα σε ποιόν οικονομικό κλάδο ανήκουν, λειτουργούν σε υπερβολικά (δια)συνδεδεμένα οικονομικά περιβάλλοντα που απαιτούν από αυτές όχι μόνο να προσαρμοστούν αποτελεσματικά στις τρέχουσες ψηφιακές εξελίξεις και απαιτήσεις, αλλά και προκειμένου να εξασφαλίσουν την ανάπτυξη και μακροημέρευσή τους θα πρέπει να δημιουργήσουν τους νέους ψηφιακούς οικονομικούς κυβερνοκόσμους, μια εξέλιξη που συνοδεύεται από μια πλειάδα ρίσκων και ευπαθειών κυβερνοασφάλειας. Κατά συνέπεια, ο ελεγκτικός κλάδος αντιμετωπίζει μια από τις μεγαλύτερες προκλήσεις, αυτή του διλήμματος κυβερνοασφαλείας, γιατί από την μια μεριά θα πρέπει να ανταπεξέλθει αποτελεσματικά στα ζητήματα κυβερνοασφαλείας κατά την διεξαγωγή των ελέγχων, αλλά από την άλλη θα πρέπει να συμπεριλάβει τις ψηφιακές εξελίξεις και τους κινδύνους κυβερνοασφαλείας που αυτές οι ψηφιακές εξελίξεις ενέχουν, στην εκτέλεση των ελεγκτικών εργασιών.

Η παρούσα μεταπτυχιακή εργασία αποσκοπεί να μελετήσει τις διάφορες όψεις της κυβερνοασφαλείας σε σχέση με την ελεγκτική διαδικασία και πιο συγκεκριμένα θα εξεταστούν: (i) ο προσδιορισμός των όρων κυβερνοασφαλείας και κυβερνοετοιμότητας και τα βασικά συστατικά τους στοιχεία (Εισαγωγή), (ii) η λογική αιτιότητα και η σημασία της συμπερίληψης της κυβερνοασφαλείας στην ελεγκτική (Κεφάλαιο 1), (iii) οι πιο σημαντικοί τύποι ρίσκων και ευπαθειών κυβερνοασφαλείας που ενέχει το σύγχρονο μοντέλο επιχειρηματικού κινδύνου σημασία και πως οι οντότητες πρέπει να ανταποκρίνονται σε αυτούς μέσω της αξιολόγησης των εσωτερικών δικλείδων ασφαλείας που σχετίζονται με την κυβερνοασφάλεια, καθώς και η σχέση μεταξύ της συμμόρφωσης με τα πιο σημαντικά

νομικά συστήματα κυβερνοασφάλειας, σε εθνικό επίπεδο (θα εξεταστούν οι περιπτώσεις του Ηνωμένου Βασιλείου και των Ηνωμένων Πολιτειών Αμερικής) και σε επίπεδο Ευρωπαϊκής Ένωσης και της ελεγκτικής, αλλά και τα είδη των δικλίδων ασφαλείας (αποτρεπτικούς, εντοπισμού, και διορθωτικούς) που οι οντότητες χρησιμοποιούν και οι ελεγκτές πρέπει να επιθεωρήσουν (Κεφάλαιο 2), (iv) τα σημαντικότερα στοιχεία των διαδικασιών της διαμόρφωσης και της εκτέλεσης ενός ολιστικού ελεγκτικού προγράμματος κυβερνοασφάλειας με την χρήση διεθνώς αναγνωρισμένων προτύπων, όπως αυτά έχουν διαμορφωθεί από Παγκόσμιο Οργανισμό Προτύπων, και την Ένωση για την Ελεγκτική και τις Δικλίδες Ασφαλείας των Πληροφοριακών Συστημάτων (Κεφάλαιο 3), και (vii) η διαδικασία έκδοσης και δημοσίευσης της ελεγκτικής έκθεσης κυβερνοασφάλειας (Κεφάλαιο 4). Η ανάλυσή μας θα στηριχτεί στις διατάξεις των Διεθνών Ελεγκτικών Προτύπων.

Το τελευταίο κεφάλαιο (Κεφάλαιο 5), περιλαμβάνει τα τελικά συμπεράσματα πάνω στο κεντρικότερο ερώτημα αυτής της ερευνητικής εργασίας, δηλαδή, την αναγκαιότητα της συμπερίληψης της κυβερνοασφάλειας και κυβερνοετοιμοτητας στην ελεγκτική διαδικασία και πρακτική και πως αυτές έχουν μετεξελιχθεί και μεταμορφώσει τον ελεγκτικό τομέα.

Λέξεις Κλειδιά: Ελεγκτική, Κυβερνοασφάλεια, Κυβερνοετοιμότητα, Ρίσκα και Ευπάθειες Κυβερνοασφάλειας, Συμμόρφωση, Διεθνή Ελεγκτικά Πρότυπα, Ηνωμένο Βασίλειο, Ηνωμένες Πολιτείες Αμερικής, Ευρωπαϊκή Ένωση, αποτρεπτικές, εντοπισμού, και διορθωτικές δικλίδες ασφαλείας, διεξαγωγή ελέγχων κυβερνοασφαλείας, διαμόρφωση και εκτέλεση ενός ελεγκτικού πρόγραμμα κυβερνοασφαλείας, Παγκόσμιος Οργανισμός Προτύπων, Ένωση για την Ελεγκτική και τις Δικλίδες Ασφαλείας των Πληροφοριακών Συστημάτων, ελεγκτική έκθεση κυβερνοασφαλείας.

I] I N T R O D U C T I O N

I] 1] Is necessary to integrate cybersecurity and cyber-preparedness in the auditing processes?

Modern economic entities, indifferently if they come from public or private sector, or belong to a mix status, and indifferently of their size (small, medium, large, very large, multinationals) and the sector or sectors they function, face a series of challenges, not only concerning their economic development, but also their security survival, with cybersecurity concerns be amongst the most important of them. It is inevitable for a company, business, organization to exist nowadays seeking for a flourishing future, without taking under serious consideration all the implications upon cybersecurity and cybersecurity preparedness. Under this framework, the role of internal and external auditors is becoming quite pivot for the understanding and immobilizing cybersecurity threats. The auditors, as well as the directors and personnel of the economic entities, must realize that cybersecurity threats and risks co-exist in two parallel roads having an interplay dialogue one another. The first one has to do with the **integrity of the material and tangible equipment** of an economic entity. This includes all the electronic networks, computer equipment, data storage facilities, and the rest of technological equipment controlled by software systems (operations and network security). The last type of equipment brings to light, that a cybersecurity issue (like an attack) can take place, for example, in a car production facility or energy production plant, as long as is controlled automatically with the use of software devices and not manually. Under this spectrum, is more than understandable that almost all equipment of any economic entity in today's informative era can be included in this sphere. The second type has to do with the **integrity of the data and information**, meaning the non-material, non-tangible equipment of an economic entity. Here, we must include all the economic, finance and personal data of a company, like the ones the entities present in their financial statements, data of personnel, clients, customers, the data about equity and assets, programs, software (like ERPs, etc.), privacy and data ethics concerns, etc. We must explain that the data

themselves, as the equipment themselves in the previous type, do not reflect on their own the full spectrum of current and future cybersecurity concerns since their risk neutral, securing their integrity and protection from external and internal cybersecurity attacks and misappropriations is the actual core in every cybersecurity and cybersecurity preparedness system, because is the handling of these data and equipment, that can possess threats and risks.

In order to succeed the full scope of integrity not only of equipment but also of data, economic entities must engage themselves in effective digital transformation and added-value cybersecurity auditing activities, otherwise the risk to get out of the market, can lead to their termination of their function (the major threat in their going concern principle). **Sufficient digital transformation** means that not only the department of I(C)T (it includes all the business and IT networks, devices, machines, facilities, etc., run by people from IT scientific knowledge), but also in managerial level the risk assessment department (it is consisted usually of people from business administration scientific backgrounds and among others perform cybersecurity preparedness assessments of the cybersecurity risks the company faces) of the organization work together in order the individuals, processes and technologies used by the organization to be modernized, updated and in accordance with the legal obligations, the technological needs of the entity and the demands of the market according to the current and future level of technology advancements. Otherwise, as we mentioned before, the organization/entity risks to stay technologically behind, to be surpassed by its competitors better adjusted to current market needs and perhaps to end up apply for bankruptcy. **Effective and added-value cybersecurity auditing** means that companies must have not only sound internal auditing departments, able to spot cybersecurity gaps and threats and to deal with them effectively, cost-productively and time-efficiently, but also must be capable and visionary enough to hire the proper auditing services with strong cybersecurity capacities, and knowledge on how to detect and provide sound recommendations about the successful confrontation of cybersecurity threats within the right time and cost. Economic entities must not be reluctant as it concerns the deployment of the right internal and external auditing services concerning both cybersecurity and cybersecurity preparedness matters. They should not only use them only if they must follow a legal obligation, but also as a precautionary measure.

The needs for fruitful and cost-productive digital transformation and trustworthy cybersecurity auditing choices the last two decades have become a real necessity in all economic entities. The augmented role of technology in modern production systems, the

creation of multibillion multinationals social media giants, like Facebook, Twitter, Instagram, etc., the constantly increased use of social media not only in everyday consumers lifestyle aspects, but also for marketing/advertisement and clientele expansion needs, the amplification of capacities of hackers, the enlarged economic value of modern digital applications, such as e-commerce (most indicative companies are: Amazon, eBay, Wish, etc.), Artificial Intelligence (AI), Virtual Reality (VR), Internet of Things (IoT), Augmented Reality (AR), e-banks, Robotic Process Automation (RPA), etc., the creation and trading of cryptocurrencies and other blockchain technologies, the evolvement of cloud-computing, e-residency schemes¹, constitute that almost all economic entities and states need to have significant cybersecurity capacities and cyberpreparedness skills and personnel.

But what is the cost of not performing effective cybersecurity auditing processes in current economic affairs, local, peripheral, national and international. Even though, it is quite difficult to estimate this cost, is less difficult to estimate the most important cost of cybersecurity in a reverse way: the cost of cybercrime. According to different estimations the cost of cybercrime can be evaluated between \$400 billion worldwide (in 2015 estimations) to \$3 trillion in 2018 with a projection to rise to \$6 trillion by 2021.² According to a joint report published in February 2018, called “*Economic Impact of Cybercrime— No Slowing Down*” from cybersecurity company **McAfee** and international recognized think-tank the **Center for Strategic International Studies** (CSIS), the annual cost of cybercrime in 2017 costed about \$600 billion worldwide, mostly due to the constant growing capacities of hackers, the increase of cybercrime markets, such as the “dark market” and the appearance of cryptocurrencies, especially in trading and transactions. One-fourth of the cybersecurity cost derives from the illegal use of intellectual property rights. Identity theft, business email compromises and online financial manipulation and ransomware attacks are among the worthiest noticed cybersecurity threats, that cost severely in all economic entities. If we take under consideration that the same report indicates that the

¹ Estonia is since 2014 the first country to introduce the e-residency system, which enables individuals and companies to create a full functional 100% online company with access in EU’s Single Market and cross-border capitals and with relatively lower **tax** payments. **Republic of Estonia** (2019), *E-residency: The New Digital Nation*, <https://e-resident.gov.ee> (last retrieved 25/06/2019). Cyber-security concerns had forced the government to freeze the program in 2017, due to fears for digital identification thefts. **Shona Ghost** (6/11/2017), *Estonia has frozen its popular e-residency ID cards because of a massive security flaw*, *Business Insider*, <https://www.insider.com/estonia-freeze-e-residency-id-cards-id-theft-2017-11> (last retrieved 25/06/2019).

² **Steven Wertheim** (June 2019), *Auditing for Cybersecurity Risk*, *CPA Journal: The Voice of the Profession*, June 2019 Issue, by New York State Society of Certified Public Accountants (CPA), <https://www.cpajournal.com/2019/06/19/auditing-for-cybersecurity-risk/> (last retrieved 25/06/2019).

cybercrime cost in 2014 was around \$445 billion worldwide³ is obvious that states, economies, policymakers, academia, business and other institutions cannot turn a blind eye in the constant growing cybersecurity concerns. In parallel time frame (February 2018) the **Council of Economic Advisers of the Executive Office of the President of United States**, best known as the White House, published its report entitled “*The Cost of Malicious Cyber Activity to the U.S. Economy*”, estimating that cyberattacks in 2016 cost in USA economy something between \$57 billion and \$109 billion. This report shed a warning alarm for the "spillover" effect that cybercrime can have to economy and economic entities if critical infrastructures sectors (such as financial sector institutions and power grid and energy sector organizations) experience cyberattacks.⁴ This cost does include not only the reputation loss with all its side-effects (loss of clientele, public confidence, customers' change behavior, competitiveness issues, etc.), but also the so called “clean-up” cost that incorporates (a) a great variety of management efforts and working hours to face the cybersecurity incident and (b) significant spending on turn-over capacities: from money resources lost during a cyber-attack to an entities bank resources, for paying ransom in case of a ransomware attack, for updating old or purchasing new extra cybersecurity protection systems (as networks, hardware, software), for hire better (and usually more expensive) internal or external (third-party) expertise (from Chief Security Officer and other relative technical personnel to external cybersecurity auditing experts) to enhance the level of cybersecurity protection and preparedness (such as the creation and implementation cybersecurity preparedness policies, codes and strategies), to cover compliance fines, fees and penalties from regulatory authorities and other legal expenses in case of being sued by clients, providers, authorities and other stakeholders being negatively impacted by the cybersecurity incident, and many other direct and indirect expenses and costs. Under this spectrum, the importance of an entity to have or/and co-operate with a high quality and adequate quantity cybersecurity auditing expertise is of pivot importance to an entity's surviving and flourishing capacities, since cybersecurity auditors (also well-known I(C)T auditors), internal and external, can track and report cybersecurity vulnerabilities in an entities system and protecting mechanisms, something that will help the entity not only minimize the impact of the two

³ McAfee and Center for Strategic International Studies (CSIS) (February 2018), *Economic Impact of Cybercrime— No Slowing Down*, https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email (last retrieved 25/06/2019).

⁴ Council of Economic Advisers of the Executive Office of the President of United States (February 2018) *The Cost of Malicious Cyber Activity to the U.S. Economy*, <https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf> (last retrieved 25/06/2019).

types of cybersecurity costs (reputation and “clean-up” cost), but also to support the development and long-lastingness of the entity.

I] 2] Introduction to the thematic and sub-thematics of the Thesis

This Master Thesis is based in two fundamental thematic/methodological axons, that runs all over the Chapters: the first one is consisted by the thematic of cybersecurity and its relationship with the auditing and the second one of the cybersecurity preparedness or cyberpreparedness during auditing.

So, what is really cybersecurity or cyber security or cyber-security (in international bibliography the term exists in all three orthographic editions)? Internationally, there seems to be different capacities in the definition of what is considered as cybersecurity. From **Oxford Dictionary** we learn that cybersecurity is “*The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this*”⁵. **Deloitte**, an international audit leader firm and among the so called “Big 4” audit companies in the world enhance the definition further by calling “*Cyber Security as the ability to protect or defend the use of cyberspace from cyberattacks*”⁶. From the above-mentioned terms, we conclude that cybersecurity can be not only an existing situation (*state*) but also a dynamic or future situation (*ability*) for entities and organizations of all kinds. **Kaspersky Lab**, an internationally leading company on cybersecurity software, combines the two concepts by portraying cyber-security as “*the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security*”. So, if we would like to define the basic axons of cyber-security, we could focus on the following domains of an economic entity’s performance:

- Network Security: the practice of immobilizing intruders, attackers and malware from penetrating and destroy the computer network of an establishment by dealing effectively with cyber-attacks and treats against tangible devices and assets, best known as hardware, of the economic entity, such as computers, cables, production machines, etc.,

⁵ **Oxford Dictionaries** (2019), *Definition: Cybersecurity*, <https://en.oxforddictionaries.com/definition/cybersecurity> (last retrieved 25/06/2019).

⁶ **Deloitte** (July 2016), *RBI Guidelines for Cyber Security Framework*, <https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-risk-rbi-guidelines-for-cyber-security-framework-noexp.pdf> (last retrieved 25/06/2019).

Cyber-security and Cyber-preparedness as a Necessary Part of the Auditing Process

- Application Security: how to secure free from attacks and threats software. If there is a compromised application the protected data can be leaked or mistreated, with a wide range of implications for the organization. That is why, is of the utmost importance to design a sound and effective cybersecurity framework in early stages,
- Information Security: ensures the protection of integrity and privacy of information, not only in the phase of storage but also in the phase of process, transition and portability, and
- Operational Security: basic aim of operational security is to provide a holistic view in the processes, decisions and opportunities concerning the proper treatment and protection of what is called as “data assets” (in general we can define them as electronic non-tangible parts of a company that have any economic value⁷). Here, we must include the access permissions and authorizations that the users have in order to access a company’s network and the processes about the ways and the places users can process, share and store the data assets;

Despite the fact that someone can add more domains to the above-mentioned ones, or to even analyze further the ones mentioned here, for the best extension scope of this thesis we decide to focus in the four basic ones, as they were described in an enhancing way previously. The most important conclusion though from their reference is to point out the supreme importance of cybersecurity for every organization’s existence, continuity, and long-lastingness. The second most important perception must be the importance of inclusion of cybersecurity aspects during performing auditing processes. Excluding cybersecurity

⁷ Additional definitions are: 1) “*Data asset* means any software or electronic data that exists in “computer systems” and that is subject to regular back up procedures, including computer programs, applications, account information, customer information, private or personal information, marketing information, financial information and any other information maintained by the “insured organization” in its ordinary course of business.” **LAW INSIDER** (2019), *Definition of Data asset*, <https://www.lawinsider.com/dictionary/data-asset> (last retrieved 25/06/2019). 2) *Information Asset* is an identifiable collection of data stored in any manner and recognized as having value for the purpose of enabling an agency to perform its business functions thereby satisfying a recognized agency requirement. Data or information that is referenced by an agency, but which is not intended to become a source of reference for multiple business functions is not considered to be an information asset of the agency. This is merely information. Information assets are considered to be associated with one of four standard types: transactional; analytical; authored; publication. It should be noted that information content may appear in more than one asset. For example, customer details may exist as a transactional asset, but also be represented in a second analytical asset. In this case there are two assets. It is important to note that an Information Asset may also be considered to be a Public Record if it meets certain criteria. However, not all of an agency’s Information Assets will necessarily be Public Records. Information Assets within the Information Architecture that are technology dependent are implemented in accordance with the Application and Technology Architectures of an agency or the government. Examples included: Record, Document, Electronic message, Row in a database, Table or figure within a document, Whole database table, Collection of data objects about a single logical entity or concept such as ‘customer’, Content identified through a URL or URI and Metadata about other information assets”. **Queensland Government Chief Information Office** (2019), *Information Asset (Definition)*, <https://www.qgcio.qld.gov.au/publications/qgcio-glossary/information-asset-definition> (last retrieved 25/06/2019).

requirements from ordinary auditing performances should be consider from unthinkable to even dangerous to business vitality. Managing (meaning creating, collecting, processing, analyzing storing and transitioning) data is of a great importance to economic functionality in general. That is why, data is considered as the new oil, but we must pay attention to their managing “refineries”, with special focus to the analytical approach of them.⁸

The second axon of our scientific approach in this Master Thesis is the cybersecurity preparedness dimension. We will use the term cyberpreparedness, cybersecurity preparedness and cyber preparedness synonymously. While there is a general consensus of what cybersecurity means in its full content, cyberpreparedness is not that concretized. One of the definition used is the following: “*The process of ensuring that an agency, organization, or jurisdiction has developed, tested, and validated its capability to protect against, prevent, mitigate, respond to, and recover from a significant cyber incident, such as a cyber event with physical consequences to critical infrastructure.*”⁹As it concerns the dimension of cybersecurity preparedness in relation with the auditing we must focus on the following domains:

- Compliance with Laws and Standards: is the active and passive engagement of an economic entity to comply and respect the letter and the spirit of legal norms and standards. Compliance has two basic forms: (a) compliance with legal norms (international, peripheral, national, etc.) is always obligatory, unless the law provides different choice and (b) compliance with standards (international, peripheral, national, etc.) that can be both obligatory and voluntarily, depending the issuer of the standard.
- Cybersecurity Forensic (also known as computer or digital forensics): we can differentiate digital forensics from general cybersecurity efforts on the point of different functionality between them. While, cybersecurity targets to implement and robust an economic entities information security systems and to secure them from cyber-attacks, digital forensics aims at identifying the hack or attack after any event or threat had taken place and to provide solid solutions about the source of the attack and how to recover compromised data and network systems back on right track. Fundamental part of this aspect of cybersecurity preparedness is the ability of the

⁸ **Rajeev Ronanki, Ashish Verma, David Pierce & Mark Shilling** (24 February 2016), *Deloitte Insights: Industrialized analytics: Data is the new oil. Where are the refineries?* <https://www2.deloitte.com/insights/us/en/focus/tech-trends/2016/data-assets-and-analytics.html> (last retrieved 25/06/2019).

⁹ **IGI Global** (2019), *What is Cyber Preparedness*, <https://www.igi-global.com/dictionary/cyber-preparedness/51238> (last retrieved 25/06/2019).

Cyber-security and Cyber-preparedness as a Necessary Part of the Auditing Process

employees involved to be able to detect and analyze extensive series of datasets, something that has created the need for entity to have specialized and certified¹⁰ personnel. In the case of an adverse event, an entity must mobilize/activate its disaster recovery and business continuity plans and actions.

- Disaster Recovery and Business Continuity: disaster recovery, includes the systems, approaches and processes an organization had established in order to effectively face any cybersecurity incident (i.e. cyberattacks, leakages, data embezzlements, etc.) that can harm operative functionality, data integrity and in the end the company's brand name. Target of each disaster recovery policy/framework/plan is within a reasonable time and cost framework to secure restoration of the operation capacities and data integrity in the way they were before the incident. Business continuity refers to the adopted plan, that an organization follows in order to restore capacities while operating without a range of its ordinary resources and powers; and
- The Role of Stakeholders: aims to deal with enhancing personal and professional capacities of all included human resources in order to be able to deal effectively and efficiently with failing cybersecurity procedures and incidents. It contains the training and certification of personnel of all levels to know from basic to very advance cybersecurity requirements, such as deleting viruses and other suspicious emails and do not use of unauthorized USB drives and other portable storage devices, etc.¹¹ Though, we must make a clarification: when we are referring to the right and most resourceful personnel, we are not only referring to the capacities of the staff of the individual or the team that makes the audit trails, but also to the personnel the under examination entity and rest stakeholders having significant impact on cyber-preparedness of the entity, since the minimum of the cybersecurity capacities of an entity is closely related to the cybersecurity capacities of all the people and entities is involved with. For example, if clients' networks (software and hardware) are under a cyber-attack or/and face a lot of cybersecurity vulnerabilities, then the under auditing inspection entity level of cybersecurity resilience can be equally problematic and negatively influenced, despite the fact that the entity's personnel had the best cybersecurity preparedness capacity building.

¹⁰ For example, there is a relevant certification best known as **Cybersecurity Forensic Analyst (CSFA) Certification**, <http://www.cybersecurityforensicanalyst.com/> (last retrieved 25/06/2019).

¹¹ **Kaspersky Lab** (2019), *What is Cyber-Security?*, <https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security> (last retrieved 25/06/2019).

In this Master Thesis we will try to examine thoroughly the connection of the above-mentioned domains of cybersecurity preparedness with the auditing processes and science. The task is not an easy one, but the aim is to perform it with the best diligence we can assure based to the existing scientific and professional available knowledge.

I] 3] Structure of the Thesis

This Master Thesis has a five Chapters structure, while the initial part of this Thesis is the part of *Introduction* which includes the basic axons of the definitions of cybersecurity and cybersecurity preparedness. In *Chapter 1*, we examine the resonance and its importance of integration of cybersecurity to auditing, by analyzing the historical-philosophical perspective of this correlation and the role of cybersecurity auditing in the modern business risk model and how it shapes the cybersecurity auditing process/program. In *Chapter 2*, we look closely to the first two phase of the cybersecurity audit process: the phase of the appointment of the IT/Cybersecurity auditor by the client entity and the phase of understanding the most important types of cybersecurity risks and vulnerabilities in the modern business risk model environment and how entities must respond to these risks by applying the most suitable internal controls, as well as the operational legal environment of the client entity, the obligation of compliance with most important cybersecurity national regulative frameworks (United Kingdom and United States of America) and the European Union's cybersecurity landscape, and the types of controls (preventive, detective, and corrective), that entities apply and auditors must inspect. In Chapter 3, we provide a deeper insight to the third phase of a cybersecurity auditing program, the phase of planning and executing a holistic cybersecurity auditing program and their sub-particles, including important paradigms of specialized auditing tests that can be conducted according to specific cybersecurity risks and vulnerabilities, as well as the role of international standards, like those created by International Standards Organization (ISO) and Information Systems Audit and Control Association (ISACA) in providing important guidance in the best performance of these spheres. In and Chapter 4, we will examine the fourth and last phase of an cybersecurity audit program, the phase of creation and issuance of the cybersecurity auditing report. We must not neglect to mentioned, that our analysis will be based in the provisions of International Auditing Standards (ISA), that set a holistic and comprehensive framework regarding undertaking and conducting an effective, suitable, adequate and meaningful

cybersecurity audit program from scratch, able to spot and mitigate misappropriations in an entity's financial statements reporting system.

The last scientific part of this Thesis, Chapter Five, consisted of the final conclusions, in which we have tried to integrate the concepts of cybersecurity and cybersecurity preparedness and the auditing section and how these spheres influence and transform the modern auditing practice and theory.

What is more, we would like to point out the following aspects: (a) the definition of economic entity. In the text of this Thesis we use this term synonymously with the term organization, institution, business and company in order to describe any business regardless its size, sector of function and sphere of economy, meaning public, private or of mix status and non-for-profit. (b) In order to best describe the arguments presented in this Master Thesis, we will use tables and images.

Last but not least, we would like to indicate the way of citing our bibliography at the end of every page. We will use the following form: **author(s)** (day/month/year), *title*, followed by:

- (a) Publishing company, City of Publishing, Page, for paper books, hard copies, etc.
or
- (b) Website of reference, last day we retrieved the website, for data retrieved from electronic and online bases.

To make the whole process more easy understandable to the readers of this research paper we must add the following explanation: for every book that is in Greek language, we will write inside a parenthesis the titles of the book translated from Greek to English in order the viewer to understand the thematic of this particular resource.

II] CHAPTER 1: THE IMPORTANCE OF INCLUSION OF CYBERSECURITY IN AUDITING SERVICE

II] 1] A Historical-Philosophical Perspective

In order to understand the concept and the importance of inclusion of cybersecurity in auditing processes, we must firstly guide the attention of the reader to what exactly had happened between the “world of business” and consequently the formation of the modern era of auditing and the “cyber-world”, meaning the special way technological advancements had transformed human societies, markets and economies. That is why, we have adopted in our methodological approach a historico-philosophical narrative between the appearance of “cyber-world” and the “modern auditing services world”, as a holistic approach in order to best treat the core thematics of this Master Thesis.

Together with the appearance of the first commercial electronic devices, with computers like ENIAC (Electronic Numerical Integrator and Computer), huge in dimensions but with narrowed processing capacities, destined to execute digitally a series of mathematical problems after the World War II and mostly in the decades of 1950’s and 1960’s, we had also the appearance of initial philosophical and theoretical approaches trying to explain the “cyber” phenomenon and the need and ways to control and monitor it in order to best achieve a harmonic and beneficiary co-existence between humans and machines. In 1948 (republished in 1961), *Norbert Wiener*, a prominent American mathematician, engineer, neuroscientist and philosopher, adopted the word *cybernetics*¹², in order to best describe in a transdisciplinary way the interaction between the way humans, (animals) and

¹² The word cybernetics derives from the Greek word “Κυβερνητική” which means governance/governing. So, cybernetics aims to describe the system that governs, defines and navigate the course of a team or a process.

machines communicate, participate in structures and form systems and institutions. According to Wiener, (a) societies must establish solid mechanisms of communication and control between humans and machines, like those existing during auditing processes and (b) the cybernetics science must study the (inter)connections, the ways of treatment and the controlling of data and information that machines produce, reminding like that a lot the processes used during cybersecurity auditing situations.¹³ Since, auditing deals with the way economic entities collect, process and report their data and the inclusion of computing machines in all the aspects and functions of those entities, vast amounts of data had been created, the expression of **Bateson**¹⁴ dated back in 1972 that data is “*the difference that makes the difference*”, sounds extremely realistic even for moderns auditing configurations. The twentieth century, with the creation of a super flow of data from economic entities across the globe, had constituted data production and integrity an extremely important asset *per se* for entities, investors, regulators and relevant stakeholders. From the data about how to best deal with (mostly tangible) assets of a company we have passed to the reality that data themselves are an important business asset on their own. Dealing effectively, protecting and securing all this data had become a great opportunity but also a significant burden not only for economic entities but also for their auditors (internal and external) to master their performing capacities and talents. These necessities had led to the formation of cybersecurity and cyberpreparedness science and practice and their inclusion on modern auditing science and practice.

Equally important with the cybernetics approach of Wiener in modern cybersecurity auditing, was also, at the same period, the emerging of systematic information and control theories, based on mathematical modeling and statistical (data, metadata) aspects, that helped in the incorporation of mathematical modeling and prediction standards in scientific fields of economy, auditing, etc. **C.E. Shannon**'s work about the best articulation of the idea and impact of “noise” in a system/model in his 1948 “*A Mathematical Theory of Communication*”,¹⁵ can be used to identify the impact of cybersecurity problems (“noise”) in modern economy and state (as type of systems) survival and flourishing, because, after all every auditing report is in its fundamental principle a communication tool to internal and external stakeholders about the creditability, the accuracy and the real vitality of an

¹³ (1) **Norbert Wiener** (1948 & 1961), *Cybernetics or Control and Communication in the Animal and the Machine*, MIT Press, 2nd edition, Cambridge. (2) **Norbert Wiener** (1954), *The Human Use of Human Beings: Cybernetics and Society*, Anchor Publishing, New York.

¹⁴ **Gregory Bateson** (1972), *Steps to an Ecology of Mind*, Paladin Publishing, London.

¹⁵ **C.E. Shannon** (1948), *A Mathematical Theory of Communication*, The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, October, 1948, Reprinted with corrections from Harvard, <http://math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf> (last retrieved 25/06/2019).

economic entity. **R. E. Kalman**, already from 1960 on its historic article “*On the General Theory of Control Systems*”¹⁶, based on both approaches of Norbert Wiener and C.E. Shannon, had predicted the great role and impact (positive and negative) of technological advancements and the insertion of digital computers in controls to economic development of organizations. Kalman, supported the idea that the vast growth of technology will bring a lot of new problems in systems (such as the economic ones), that will challenge the capacities of “*research workers*” to best deal with them. In the category of the “*research workers*” we can include all the professionals and scientist occupying themselves with the developments and improvements of financial reporting, such as auditors and accountant, bookkeepers, economic managers, academia, etc. In order to treat effectively this challenge, Kalman is prompting to the introduction into the whole equation (mathematical-engineerable and methodologic-philosophical) of the concepts of controllability and observability for the best optimization of deterministic control systems, such as those that exist in auditing inspections. Both these concepts, in one way or another have been incorporated in modern auditing performance, and as we will present in this paper, they are of fundamental importance for any trustworthy auditing system upon cybersecurity and cyberpreparedness. Moreover, we can connect Kalman’s insertion of the concept of optimization of regulators based on performance index(es) within a specific time framework, with the importance and the necessity of high-skilled auditors and high-quality, added-value and time-oriented auditing performances, not only upon cybersecurity and cyberpreparedness aspects of the auditing processes, but also in general domains of modern auditing.

Today’s auditors (research scientist and professionals) that target to perform their duties with the most profound ethical and adopted standards, might need useful food for thought not only in the concepts important mathematicians had introduced around the middle of the previous century, but also the concepts introduced by social scientists and philosophers, because in the very end economy and auditing exist for the best protection and thriving of human societies. Later in this Thesis, we will show not only the benefits of auditing cybersecurity and cyberpreparedness in economy, but also in society. For example, in the section analyzing the basic form of cybersecurity dangers [Chapter II] we will present the basic categories of them, such as: malicious behaviours, cybercrime, cyber-attacks and more, including cyberterrorism. Especially the latest can provoke extended and irreversible harm to any economic entity as a way to provoke chaos, and disruption to societies, local,

¹⁶ **R. E. Kalman** (1960), “*On the General Theory of Control Systems*”, on **IFAC Proceedings Volumes, Volume 1, Issue 1**, August 1960, Pages 491-502, Available in the following website: <https://www.sciencedirect.com/science/article/pii/S1474667017700948> (last retrieved 25/06/2019).

national and international. Businesses vital for every economy and state survival, such as critical infrastructure, private and public, nuclear power plants, water facilities, military facilities, banks, public institutions and government bodies (Parliaments, Congresses, Ministries, Agencies, Central Banks, etc.), stock exchanges, etc. can be targets in a cyberattack in order to provoke political and economic disruptions against certain societies (cyberterrorism). So, auditors must have under their radar a sufficient interdisciplinary knowledge about how to best treat cyber dangers. For example, they must take notice of the progress in domains like cyber-psychology, cyber-criminology, computing engineering, data management, cloud computing, applications coding, etc. In reality, is not only about the advancement of cyber technology but as **Paul-Michel Foucault** (1988)¹⁷, one of the most important philosophers, historians of ideas and social theorists, has set the whole problem: the dynamic of modern regulations and controls is based in the interaction of four types of technologies:

- (a) *Technologies of Production*: that allowed us to create, produce, transform, and manipulate objects, such as those auditors must inspect during their controls.
- (b) *Technologies of Symbolic Systems*: that allowed us to use meanings, symbols, and other tools in order to communicate and report, such as those used in order to report financial statements or like the international auditing standards, or like those used in dark web transactions or like those in cyber-criminology to describe certain unlawful cyber-behaviors, or like the cyber-protection and cyber-preparedness schemes and standards government bodies (like US's NIST) or international organizations (like EU) had adopted, and many more.
- (c) *Technologies of Power*: that determine human behavior (in active and passive ways) by subordinating them to specific goals and rules of domination and objectivity, such as all the legal and ethical norms (obligatory and voluntarily) that auditors must comply with when they execute their auditing controls, or like the unformal ones that hackers must follow when they prepare and conduct their attacks inside their secretive communities, etc.

¹⁷ Paul-Michel Foucault system of four types of technologies that exist in the human world and societies had been extracted by the following book (in its Greek Edition – in the parenthesis in italics we provide the translation of the Greek titles of the book): Ángel J. Gordo-López & Ian Parker, Κυβερνοψυχολογία: Μετα-επιστημονικά πλαίσια και σχέδια έρευνας (*Cyberpsychology: Meta-scientific frameworks and patters of research*), in the collective book: **Ángel J. Gordo-López & Ian Parker (editors)** (2008 for Greece-1999 first edition in English for Macmillan Press LTD) *Κυβερνοψυχολογία (Cyberpsychology)*, Published by Εκδόσεις Παπαζήση (Papazisi Publishing Company), Αθήνα (Athens), page 36-37.

(d) *Technologies of Oneself*: that allowed to every human to achieve with their own personal means or with external assistance a variety of interferences upon their body, soul, behavior and way of being with the aim to transform themselves in order to achieve a specific status of happiness, or purity, or wisdom, or perfection, or immortality/recognition. People, as individuals and as members of groups, play the most vital role in cybersecurity schemes, and can be (a) on the side of positive cyber-protection, for example: (i) solid trained internal IT teams can design a cybersecurity system quite sound to external cybersecurity attacks, (ii) visionary managers of all levels, that can understand the importance of cybersecurity, can deploy important resources (human, budgetary, materialistic) in order to create a trustworthy cybersecurity preparedness system, (iii) high-trained auditors can detect and identify cyber related frauds and problems, or (b) they can be on the side of malicious cyber-behavior, for example: (i) an inside of an economic entity member of personnel for many reasons (need for money, revenge, etc.) may choose to harm the IT systems of a company or provoke other cyber-frauds, like providing to rivals protected intellectual property rights resources and (ii) external hackers and other external cyber-fraudsters can design and execute cyberattacks in order to gain recognition in their hacking communities, for example, by stealing and distributing personal data and credit cards data to fraudsters, in order to enter in a specific hacking society. As we are going to examine in the forthcoming sections of this Thesis, malicious cyber-behaviors and cyber-frauds transform the classical “Fraud Triangle” and “Fraud Diamond” with new dimensions concerning cybersecurity aspects of protection, auditing and long-lastingness of an economic entity.

The great (inter)dependence/interaction of the above mentioned technologies and at the same time their inherit vulnerability, together with the constant augmented digitalization of the way economic entities of any kind, form and size, manufacture products, perform services, create and analyze the data related to every stage and process of their function had create significant dangers not only for them and their personnel, but also for the local societies, the nations and the democratic systems inside they exist, promulgating like that the need of a “*Good IT Society*”¹⁸. The holistic approach of the “*Good IT Society*”, can be used as a useful road map for all cybersecurity and cyberpreparedness systems and their relevant auditing performances, because it dialogues upon the moral and functional interaction of four basic cyber-systems (virtual worlds, virtual environments, virtual roles and ubiquitous

¹⁸ **Gunilla Bradley** (2017), *The Good ICT Society: From Theory to Actions*, Routledge Publishing, London and New York.

embedded technologies) that can be hugely related to the four types of technologies by Paul-Michel Foucault that transform societies and the way modern auditing is conducted, so cybersecurity concerns have emerged not only as a necessary but also as a fundamental part of every auditing, internal and external, process.

II] 2] The Modern Business Risk Model, Cybersecurity and the Role of Auditing

This Master Thesis aims to present with solid scientific criteria the importance and the necessity of including cybersecurity concerns in auditing processes and performances. Auditing, as a science and as a profession, goes hand in hand with two important advancement that happened and still happening in the Western (mostly) world after the World War II: (a) *the evolution of traditional business models*, with the creation of multinational conglomerations able to produce and sell products and services in many countries simultaneously and (b) *the constant progress of technology* that enables (a). The need to regulate effectively those technological advanced conglomerations had created not only the need of more complex regulating legal systems, but also the need for more technologically familiarized auditing processes. This need on how to best deal with digital challenges has been integrated in auditing sector in two -sometimes contradictory- ways: (a) *technology as a tool to best performed high efficient auditing services*, (b) *technology as a point of concern, as a risk, as an indicator of danger that must by itself be a part of the auditing controls and inspections processes*.

This dual nature of technology and especially of digital technologies and realities in modern auditing business, both as a tool and as a chimera, had made the need of inclusion of cybersecurity concerns and solutions into auditing processes a pure necessity, especially the last three decades. Approximately at the same timeframe (middle of the decade of 1990's to today) the world had experienced the shifting from the fourth stage of evolvement in auditing methodologies¹⁹, the audit risk model, to what is called as the fifth stage, the

¹⁹ Until so far, the methodologies used during auditing scientific research and professional execution had been categorized in five historical stages: **the first one** (antiquity to first decades of 20th century) based on *catholic inspections* in order to secure free from mistakes, frauds and embezzlements the royal and businessman fortune. The **second one** (first decades of 20th century until the decade of 1970's) we have the *systems-based auditing*, that, since catholic inspections are practically impossible, had introduced the concept of true and correct view of financial statements of economic entities in the meta-industrial economy. The **third one** (decade of 1970's and decade of 1980's) we have more *substantive approaches of defaults*, with the

business risk approach/model, which gives more emphasis in the qualitative aspects of corporate risks and defaults, such as the general environment in which an economic entity functions and the strategic risks and dangers, that can affect her long-lastingness.²⁰

In this complex corporate and economic environment, auditing must not only track and disseminate the above-mentioned risks, but also to neutralize any negative impact in an entities surviving and flourishing instincts, because the inability to understand and counteract to these corporate risks are the biggest danger of auditing. Among the modern qualitative aspects of corporate risks and consequently auditing risks, we must include definitely the cybersecurity one, not only for those service companies that exist almost purely in digital worlds, like social media giants (Facebook, etc.), but also for more traditional manufacturing and retailing economic entities with multinational computerized production and supply chains, a sphere that includes from automakers, food industries, clothing and fashion industries, to all types of retailers -offline and online, and for those that combine both aspects, and other tech-related entity, like creators of hardware (gadgets, devices, cables, electronic systems, chips, networks, etc.) and software (operating systems, applications, search engines, etc.) or both in a mix way. Typically, not even one company can be considered as immune from cybersecurity risks, since all modern entities use and sometimes overuse computers and networks that are connected to any form of net, internal or external, such as internet (worldwide web). And even if an entity does not apply any computational capacity, still the economic society or societies it functions, like public authorities (such as tax authority), suppliers, transportation services, etc., they do operate in computational and online universes. And that is a game-changing risk that cybersecurity incorporates mostly than other corporate risks and defaults: the best applicable cybersecurity level goes hand in hand with the cybersecurity level of an entity's all stakeholder, since a malfunction or an attack in their network, hardware and software systems (best known from the acronym of NHS systems) can also provoke a huge cybersecurity problem in the entity's survival. Let's consider the example of a malware attack in a tax authority or a supplier that results the stealing of millions of sensitive financial data, that can later be used to provoke a major financial fraud to all affected entities. This is the first side and the most evident one of

performing of auditing controls and the formation of true and fair view to be the major auditing goal. The **fourth stage** (decade of 1980's and decade of 1990's) the **audit risk model** is the new model, that targets in the systematic analysis and assessment of risks for important defaults in financial statements and focuses on the civil responsibility of auditors in case of audit scandals and the role of fees due to increased antagonism. Currently, we are experiencing the fifth stage, the business risk approach/model. **Κωνσταντίνος Καραμάνης** (2008 – 1st Greek edition), *Σύγχρονη Ελεγκτική: Θεωρία και Πρακτική Σύμφωνα με τα Διεθνή Ελεγκτικά Πρότυπα* (*Modern Auditing: Theory and Practice according to International Auditing Standards*), Εκδόσεις ΟΠΑ, Αθήνα, Page 54-55.

²⁰ **Κωνσταντίνος Καραμάνης** (2008 – 1st Greek edition), *Ibid*, Page 55.

the cybersecurity, the interconnection, the other side and much more dangerous is the lack of obviousness, since cybersecurity threats and frauds can take place in the background, behind the corporate scenes, even for years, before an entity takes notice (if ever notice them) and attempt to immobilize them. Is not by coincidence that **World Economic Forum (WEF)** in its 2019 *Global Risks Perception Survey* place cyber-attacks, either in the form of data and money theft, either in the form of disruption of infrastructure and operations of organizations, as the fourth and fifth respectively global risk expected to be increased worldwide risks in the next decade. Cybersecurity risks, such as cyber-attacks, data frauds and thefts and breakdowns in critical information infrastructures are also included in WEFs (*Global Risks Report of 2019*) lists of top ten risks in terms of likelihood not only to take place but also due to their turbulent impact.²¹

In order to best understand why is so important to integrate cybersecurity in internal and external auditing inspections and performance, it is of utmost necessity to examine some basic auditing concepts, that comply with International Auditing Standards (ISA) and International Financial Reporting Standards (IFRS), studied though in a cybersecurity perspective. Since the core scope of every auditing process is to provide a *true and fair view* of financial statements of an economic entity and to assure that these financial statements do not contain any material mistreatment and substantial defaults, as **International Standard on Auditing (ISA) 200** on “*Overall objectives of the independent auditor and the conduct of an audit in accordance with international standards on auditing*” states²², the **business risk approach/model**, offers a quantitative model upon how to best calculate the variety of risks and defaults including the cybersecurity one that modern entities of any size and sector are facing in daily scale. All the risks (operational, cash, transactional, cyber, etc.) and their consequences (halt business operations, get out of the market temporarily and permanently, raise business continuity questions according to going concerns principle) the business world faces daily constitute solid trustworthy and realistic financial information an “economic good (with the essence of commodity)” for societies and economies that comes with a significant cost. Cost concerning the gathering, analysis, assessment, production, and distribution of financial information inside and outside the company. Despite the point that this is by all means a significant cost, the information produced can be problematic as it

²¹ **World Economic Forum** (2019), *Global Risks Report of 2019: 14th edition, Pages 5 & 8*, http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf (last retrieved 25/06/2019).

²² **International Federation of Accountants (IFAC)** (2009), *International Standard On Auditing 200 Overall Objectives Of The Independent Auditor And The Conduct Of An Audit In Accordance With International Standards On Auditing (Effective for audits of financial statements for periods beginning on or after December 15, 2009)*, <https://www.ifac.org/system/files/downloads/a008-2010-iaasb-handbook-isa-200.pdf> (last retrieved 25/06/2019).

concerns its quality and quantity.²³ This is the fundamental economic problem auditing, internal and external, is trying to solve, meaning to provide a better assurance about the credibility and integrity of the financial information, including the cybersecurity related is pure of malicious or accidental defaults, mistakes and mistreatments.

As we explain previously, the heart of modern business risk model aims to track through substantive testing significant defaults (irregularities, misconducts and frauds) in the official financial statements of an entity, defaults that they can pass unnoticed from the managing team of an entity, raising the risk of an inappropriate and fraudulent financial reporting or falsified financial statements, a situation that is considered a crime in national legal systems. In order to minimize this catastrophic risk and after a series of very noticeable fraudulent financial reporting and accounting misbehavior cases (such as the scandals of Enron, Worldcom, Maxwell, etc.) the auditing science and practice, internal and external,

Table No 1: The Audit Risk Equitation in Modern Business Risk Model	
$AR_i = IR \times CR \times DR$	
where AR_i	Audit risk
IR	Inherent Risk
CR	Control Risk
DR	Detention Risk
<p>Source: Κωνσταντίνος Καραμάνης (2008–1st Greek edition), <i>Σύγχρονη Ελεγκτική: Θεωρία και Πρακτική Σύμφωνα με τα Διεθνή Ελεγκτικά Πρότυπα (Modern Auditing: Theory and Practice according to International Auditing Standards)</i>, Εκδόσεις ΟΠΑ, Αθήνα, Page 488.</p>	

had emerged with the aim to track any material corporate risk that might lead to fraudulent situations. This process resulted the development of audit risk (AR_i) equitation, which is consisted of three independents to each other, but multiplied all together, factors: the inherit risk (IR), the control risk (CR) ant the detention risk (DR). Table No 1 presents the mathematical expression of this equitation.

But what are exactly the components of this equitation²⁴ and what they represent as it concerns the cybersecurity domain in modern auditing processes?

AR_i - Audit Risk: is the possibility of an entity to create and publish financial statements that they have substantial defaults and frauds, but

the auditor's report fails to include those (individual or accumulated) default(s) in the official auditing opinion. In the context of cybersecurity, the audit risk has to do with the

²³ **Απόστολος Κ. Αποστόλου** (2015), *Ανάλυση Λογιστικών και Χρηματοοικονομικών Καταστάσεων (Analysis of Accounting and Financial Statements)*, Association of Hellenic Academic Libraries, Page 14.

²⁴ The definitions of all types of risk mentioned in this section are being based in the relevant definitions of Prof. Konstantinos Karamanis (**Κωνσταντίνος Καραμάνης**) (2008–1st Greek edition), *Σύγχρονη Ελεγκτική: Θεωρία και Πρακτική Σύμφωνα με τα Διεθνή Ελεγκτικά Πρότυπα (Modern Auditing: Theory and Practice according to International Auditing Standards)*, Εκδόσεις ΟΠΑ, Αθήνα, Pages 488-489.

inability of the cybersecurity auditors (also known as IT auditors), internal and external, to spot any kind of dangers related to NHS systems, a very concrete risk due to the interconnection and the lack of obviousness, the two most distinct characteristics that, as we described previously, incorporates cybersecurity.

IR - Inherent Risk: is the possibility of an entity's financial statements to contain material defaults due to the nature of the entity, its size, the sector, and the economic environment within it operates. It is normal and realistic, especially due to interconnection characteristic of cybersecurity threats, to consider that the more use of NHS systems an entity makes (not matter the ownerships status, meaning if they belong to the entity, or are part of an external, third-party, outsourcing, contractor, service deal) the more the inherent risk is, as we mentioned earlier, even if an entity does not make any kind of use of NHS systems, all the entities that cooperates with will, so the levels of inherent risk due to cybersecurity are still significant.

CR - Control Risk: is the possibility that an entity's system of internal controls neither to track and correct nor to dissuade in time and effectively material defaults in financial statements reporting. At corporate level, control risk is connected with the ability (or the lack of this tremendous important capacity) of the IT department (together not only with top-management and rest of employees, but also with external stakeholders and collaborators) to cuirass NHS systems against malicious cyber threats (such as those we will describe in the next section). At cybersecurity auditing level, control risk is related with the auditors competency to design, apply, asses and disseminate the most applicable, efficient and added-values internal controls that will achieve successfully and vigorously the necessities to spot and deactivate any dangerous and malicious cybersecurity threat. It is critically important for IT departments and IT auditors to understand that the control genre of risk is the result of the combined probability of the interconnection and the lack of obviousness characteristics of cybersecurity. Interconnection is related with the quantity (amount of controls) that must be in an IT/NHS audit trail, while the obviousness obscurity is mostly connected with the quality of the performance of the applied amount and depth of the controls.

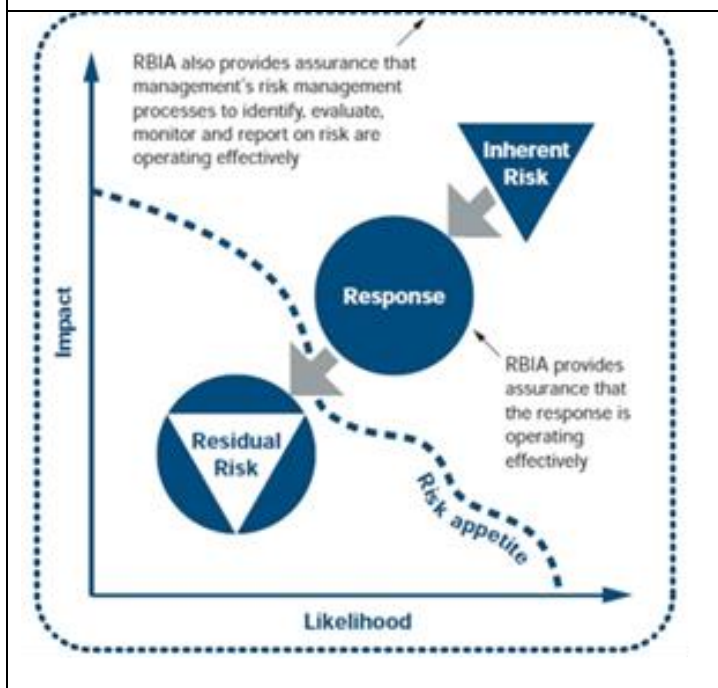
Dr - Detention Risk: is the possibility of auditors' program of internal control and auditing inspections not to detect material (individual or accumulated) default(s) resulting the creation of financial reports with significant mistakes and misappropriations. In cybersecurity domain, this type of risk is apparently connected with the characteristic of lack of obviousness of cyber-threats and their consequent difficulty or inability to be detected and

neutralized in the most affordably way, time, resources and space, before these threats become counter-productive or even “lethal” to both the quality of auditing reporting but also to an entity’s long-lastingness.²⁵

In this framework of risks and due to the nature of cybersecurity (corporate and auditing) threats is important to mention another type of risk, the **residual risk**, which is referred to the potentiality of fraudulent financial reporting despite the application of security controls that function as a protective valve against substantial, strategic, business and entrepreneurial defaults that the nature of the entity possess. In cybersecurity context, residual risk is related also with the risk appetite of the examined entity and can be vary from risk acceptance levels to risk share (usually through external insurance), reduction and

even avoidance behaviors. The more prone or even eager to cyber-risk acceptance an entity is, the more the cyber related residual risk is, and consequently the more the audit risk (and its components), as it was described before, is. This is a widely acknowledge reality during internal and external audit trails. In Image No 1 (in this page) we present the approach of Chartered Institute of Internal Auditors as it concerns the connection between the Risk Based Internal Audits (or RBIA), the Inherent Risk, the Residual Risk and the Risk Appetite of an entity, in order to effectively detect, assess, monitor, disseminate and report the risks of

Image No 1: The correlation between Inherent Risk, Residual Risk and Risk Appetite in Risk Based Internal Audits

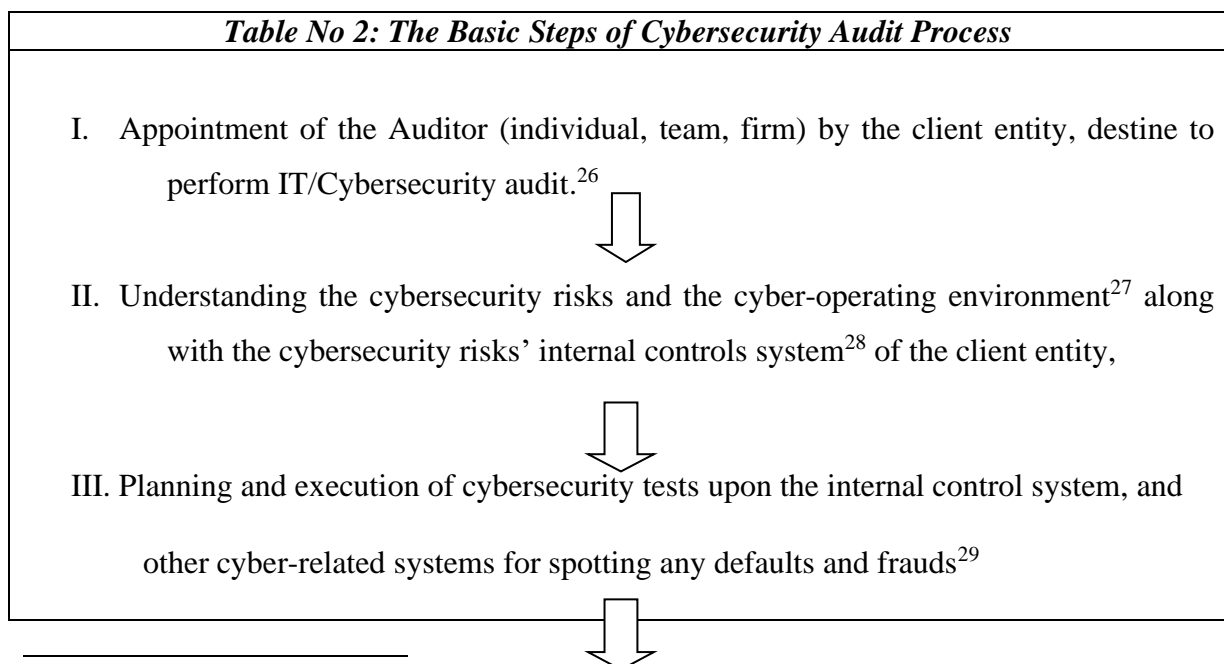


Chartered Institute of Internal Auditors (08/10/2014), *Risk Based Internal Auditing*, <https://global.theiia.org/standards-guidance/topics/Documents/201501GuidetoRBIA.pdf> (last retrieved 25/06/2019).

²⁵ **AICPA**, (29/04/2019), *The audit risk model: your first step in risk assessment*, <https://blog.aicpa.org/2019/04/the-audit-risk-model-your-first-step-in-risk-assessment.html#sthash.0WWnE3fn.dpbs> (last retrieved 25/06/2019). **Chartered Institute of Internal Auditors** (08/10/2014), *Risk Based Internal Auditing*, <https://global.theiia.org/standards-guidance/topics/Documents/201501GuidetoRBIA.pdf> (last retrieved 25/06/2019). **Κωνσταντίνος Καραμάνης** (2008–1st Greek edition), *Σύγχρονη Ελεγκτική: Θεωρία και Πρακτική Σύμφωνα με τα Διεθνή Ελεγκτικά Πρότυπα (Modern Auditing: Theory and Practice according to International Auditing Standards)*, Εκδόσεις ΟΠΑ, Αθήνα.

an entity. This approach can be used also in the case of cybersecurity related risks and threats and moreover in the external cyber-auditing performances.

Taken under serious consideration all the above-mentioned content, is more that clear that the auditing service, as science, art/technique and profession, had to evolve in order to incorporate the cybersecurity dimension. The classic form of audit trail, that is consisted of the following steps: firstly, internal and external auditors must be appointed by the client entity, secondly, the auditing team (again external and internal) must understand the working environment (such as the compliance with legal obligations and norms) of the entity and its risks, following thirdly by the step of plan, creation and execution of the best applicable and appropriate system of controls based on the data from previous step. Last step/phase and the essence of the whole cybersecurity auditing program is the step of assessing the results of in the previous step of applied controls and create the final report based on the finding of this assessment in order to formulate the auditing final opinion that will be publicized according to legal requirements. The Table No 2 shows how traditional audit process is transformed in order to incorporate the cybersecurity dimension.



²⁶ ISA 200 on “Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing”, ISA 210 on “Terms of Audit Engagements” and ISA 220 on “Quality Control for an Audit of Financial Statements”, ISA 230 on “Audit Documentation”, ISA 240 on “The Auditor’s Responsibilities Relating to Fraud in an Audit of Financial Statements”, ISA 260 on “Communication with Those Charged with Governance” and govern the procedure of this appointment.

²⁷ ISA 315 on “Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement”, ISA 250 on “Consideration of Laws and Regulations in an Audit of Financial Statements” provides detail provisions on how to succeed in this step.

²⁸ ISA 220 on “Quality Control for an Audit of Financial Statements”, ISA 265 on “Communicating Deficiencies in Internal Control to Those Charged with Governance and Management” and ISA 330 on “The Auditor’s Responses to Assessed Risks” play a key role on conducting this step.

²⁹ A variety of international auditing standards offers extended provisions on how to conduct this step: ISA 300 on “Planning an Audit of Financial Statements”, ISA 320 on “Materiality in Planning and Performing an

IV. Final Assessment of IT/cyber-risks and Issuance of the Cybersecurity Auditing

Report with Auditor's Opinion upon cyber-security material findings.³⁰

Source: Κωνσταντίνος Καραμάνης (2008–1st Greek edition), *Σύγχρονη Ελεγκτική: Θεωρία και Πρακτική Σύμφωνα με τα Διεθνή Ελεγκτικά Πρότυπα (Modern Auditing: Theory and Practice according to International Auditing Standards)*, Εκδόσεις ΟΠΑ, Αθήνα, Page 485.

II] 3] Conclusions

Cybersecurity, as a way to minimize risk in IT infrastructure and NHS systems on an entity and cybersecurity preparedness, as a form to proactively armor the entity from cyber-related risks and concerns, as we examine previously, not only gives new content to the existing and future working and functioning environment for entities of all kinds, sizes, sectors and genre (public, private, non-profit, mixed), since those environments are expected to be even more computerized and technology driven, but also provide new areas of concern and action to the auditing services that they must adapt to the cybersecurity dimension by adopting a series of cybersecurity controls during auditing performances. Until the final moment of production and publication of the auditing report that will contain the cybersecurity performance of the entity, auditors must not neglect to examine (again if it is necessary) all the cybersecurity related risks and their controls systems and the possible impact that might have not only to the accuracy of the auditing report but also to the longevity, durability, profusion and progress of the examined entity. The abundance of auditing internal controls and their proper execution can bring in light all the apparent and non-so-apparent cybersecurity risks relieving this way their already happening or potential negative effects.

Audit" ISA 500 on "Audit Evidence", ISA 501 on "Audit Evidence-Specific Considerations for Selected Items", ISA 505 on "External Confirmations", ISA 510 on "Initial Audit Engagements-Opening Balances", ISA 520 on "Analytical Procedures", ISA 530 on "Audit Sampling", ISA 540 on "Auditing Accounting Estimates, Including Fair Value Accounting Estimates, and Related Disclosures", ISA 550 on "Related Parties", ISA 560 on "Subsequent Events", ISA 570 on "Going Concern", ISA 580 on "Written Representations", ISA 600 on "Special Considerations-Audits of Group Financial Statements (Including the Work of Component Auditors)" ISA 610 on "Using the Work of Internal Auditors" ISA 620 on "Using the Work of an Auditor's Expert".

³⁰ ISA 700 on "Forming an Opinion and Reporting on Financial Statements," ISA 705 on "Modifications to the Opinion in the Independent Auditor's Report", ISA 706 on "Emphasis of Matter Paragraphs and Other Matter Paragraphs in the Independent Auditor's Report", ISA 720 on "The Auditor's Responsibilities Relating to Other Information in Documents Containing Audited Financial Statements" provides detail provisions on how to succeed in this step.

In the following chapters we will examine more thoroughly all the necessary steps of a cybersecurity audit trail, as those had been developed by theory and practice, that will elaborate us more as it concerns the positive answer of this master thesis, the necessity of inclusion of cybersecurity and cyber-preparedness concerns in auditing performances. Our attempt will start with the examination of most pivot cybersecurity risks and the cybersecurity compliance landscapes that modern entities must adopt in order to be better adapted to cybersecurity and cyber-preparedness norms.

III] CHAPTER 2: UNDERSTANDING CYBERSECURITY ENVIRONMENT AND ITS RISKS AND CYBERSECURITY INTERNAL CONTROLS OF THE CLIENT ENTITY

III] 1. Appointment of the IT/Cybersecurity Auditor by the client entity and Cybersecurity Risks Environment

The first step of any auditing process and consequently of a cybersecurity oriented one, is not in the hands of auditors, but up to the company to make that relevant choice according to its needs, scale, and compliance demands. It is the decision of the entity to apply an audit inspection, for reasons such as to comply with legal obligation, to raise its existing (or potential) audience faith of trust, to enter in the official stock markets, etc.

In this master thesis we are referring to both internal and external auditing services: so as it concerns the internal, the entity's decision is about how to hire (and create a relevant department or perhaps choose an independent external contractor as its internal auditing partner) the needed auditing team. As it concerns the external dimension of auditing, entity's decision is about hiring from the market the firm (or individual) that will act as its independent external auditor. Ideally, the choice of both type of cybersecurity auditors, internal and external, is based on a variety of criteria set by the entity according to its business model, needs and resources and by provisions of relevant laws, such as: auditors capacities to understand the cyber risks the entity faces, their reputation, the efficacy of their control's inspections and the quality of their reports, to be certified, to have a minimum

working experience, to ensure the principle of independence and the principle of no conflict of interest between auditors and the client entity, etc. Due to the fact that it is almost impossible to examine the criteria system of every entity as it concerns the choice of its auditing capacities (individual or teams or external firms), something that exceeds the scope of this research paper, we will consider as granted that the entity will proceed in this step by applying at least the minimum of its criteria mentioned in this paragraph (capacities, reputation, efficiency, certifications, working experience, no conflict of interest, etc.), especially if these criteria are among its legal obligations and part of internationally recognized professionals standards for audit practitioners.

The *International Federation of Accountants* (IFAC) through the *International Auditing and Assurance Standards Board* (IAASB) had issued a number of *International Standards on Auditing (ISA)* that set the criteria and requirements landscape for professionals conducting auditing services to an entity's financial statements, that can have a significant impact in conducting cybersecurity related audit performances. This landscape is governed by several international auditing standards, such as *International Standard on Quality Control (ISQC) 1 on Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance and Related Services Engagements*, *ISA 200 on Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing*, *ISA 210 on Terms of Audit Engagements*, *ISA 220 on Quality Control for an Audit of Financial Statements*, *ISA 230 Audit Documentation*, *ISA 240 on The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements*, to be the most fundamental.

More precisely, *ISA 200 Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing* demands from auditors during their understanding of an entity's functional environment and its risks, planning and executing an audit plan in the entity's internal controls system and preparing for the issue of final audit reporting, to fulfil the following requirements: (a) the ethical requirement when it comes to audit financial statements, like independence and other fundamental ethical principles, such as those set by Part A of *International Ethics Standards Boards for Accountants (IESBA) Code of Ethics for Professional Accountants*: integrity, objectivity, professional competence and due care, confidentiality and professional behavior. (b) professional skepticism and professional judgement, during planning and performing their audits and by taking under consideration all the circumstances that might lead the financial statements to incorporate defaults and materially important mis and takes.

(c) to obtain sufficient appropriate audit evidence about audit risk, that will enable the auditor to decrease audit risk to an acceptable reduced level and to reach to the most appropriate conclusions in order to form a suitable and resourceful audit report; and (d) to perform the auditing duties in compliance with relevant ISAs.³¹ As it concerns the relevance of this standards with cybersecurity, auditors must show the appropriate knowledge, ability to understand cybersecurity threats, to correlate them with overall operational and surviving objectives of an entity and to gather suitable evidence about their impact to the client's entity performances.

ISA 210 Terms of Audit Engagements, that sets a range of terms in order an auditor to accept or continue performing an audit assignment, demands from auditors not only to gain a full access to all information related with the audit by the entity, but also not to accept a limitation on the scope during their audit engagement unless a legal obligations necessitates otherwise.³² So, auditors must ensure not only full access to all the material related to IT functions and cybersecurity threats but also not to accept any restriction on the cybersecurity scope in the overall audit engagement.

ISA 220 Quality Control for an Audit of Financial Statements provides the framework about audit firms (and their personnel) responsibilities on the obligation of developing, preserving, supervising, monitoring and documenting independent quality control systems, policies, procedures, reviews, consultations according to professional standards (such as the previously presented ethical requirements of ISA 200) and regulatory requirements. Supervision clauses permits the identification and addressing of important matters during the audit engagement that can have a significant and modification impact to the planned auditing approach.³³ This standards is highly connected with ***International Standard on Quality Control (ISQC) 1 on Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance and Related Services Engagements***, which aims to ensure the quality requirements of controls performances by

³¹ **IFAC** (2010), *International Standard On Auditing 200 Overall Objectives Of The Independent Auditor And The Conduct Of An Audit In Accordance With International Standards On Auditing*, <https://www.ifac.org/system/files/downloads/a008-2010-iaasb-handbook-isa-200.pdf> (last retrieved 25/06/2019).

³² **IFAC** (2010), *International Standard On Auditing 210 Agreeing The Terms Of Audit Engagements*, <https://www.ifac.org/system/files/downloads/a009-2010-iaasb-handbook-isa-210.pdf> (last retrieved 25/06/2019).

³³ **IFAC** (2010), *International Standard On Auditing 220 Quality Control for an Audit of Financial Statements*, <https://www.ifac.org/system/files/downloads/a010-2010-iaasb-handbook-isa-220.pdf> (last retrieved 25/06/2019).

auditing firms and the planning auditing methodologies.³⁴ Cybersecurity concern can be among these important matters that can alter the designed auditing approach, especially in case there were not in the original plan, but resulted from reality conditions, such a cybersecurity incidence (i.e. a data breach) or the adoption of a relevant legal framework (i.e. EU's General Data Protection Regulation or GDPR).

ISA 230 Audit Documentation demands from auditors to prepare, keep and provide a *sufficient and appropriate record*³⁵ of the basis for the auditor's report and that the evidence planned and performed by auditors complies with ISAs and other legal and regulatory obligations.³⁶ This is very important task as it concerns cybersecurity, because it plays the role of the basis of creating the current terms running audit report, but also can function as a tool to understand, shape and compare future cybersecurity material matters with the records of the previous cybersecurity concerns. For example, if previous audit records and reports had point out the vulnerability of IT network, hardware and software (NHS) systems of a company, auditors that examine the condition of an entity in the current working period must give special attention in case of malicious exploitation of these cybersecurity vulnerabilities that leads to an asset loss or potential loss that must be incorporated to financial statements and to auditing reports: i.e. a malicious breach by a hacking group to intellectual property right records of a pharmaceutical entity had made available to rival companies a very important patent formula.

ISA 240 The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements explicit that misappropriations in financial statements of an entity are the outcome of fraud or error, with the intentionality being the distinguishing factor between the two types of financial reporting misstatements. Frauds that can cause material misstatements are of two types: (a) misstatements that derailing from fraudulent financial reporting and (b) misstatements that derailing from misappropriation of assets, with auditors even if they track a fraud incidence are not legally responsible to determine whether or not a fraud case has actually took place. Auditors primary responsibility is to reasonably assert that overall

³⁴ **IFAC** (2010), *International Standard on Quality Control (ISQC) 1 on Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance and Related Services Engagements*, <https://www.ifac.org/system/files/downloads/a007-2010-iaasb-handbook-isqc-1.pdf> (last retrieved 25/06/2019).

³⁵ According to ISA 230 this record, which can be recorded on paper or electronic form and other media, includes the following examples of documentation: audit programs, analyses, issues memoranda, summaries of significant matters, letters of confirmation and representation, checklists, and correspondence (including e-mail) concerning significant matters

³⁶ **IFAC** (2010), *International Standard On Auditing 230 Audit Documentation*, <https://www.ifac.org/system/files/downloads/a011-2010-iaasb-handbook-isa-230.pdf> (last retrieved 25/06/2019).

financial statements do not contain material misstatement due to a fraud or error by planning and performing a thorough audit, despite the fact that there is always an unavoidable risk of material misappropriation in financial statements. As we will examine in the following section of this Chapter cybersecurity incidents with audit importance can occur both due to fraud and error, as ISA 240 indicates. Moreover, ISA 240 identifies on its Appendix one cybersecurity related cases that can result misstatement in financial statements, categorizing this cases in following categories: (a) risk factors relating to misstatements arising from fraudulent financial reporting: such as (i) high vulnerability due to rapid changes in technology, (ii) new accounting, statutory, or regulatory requirements, (iii) inadequate monitoring of internal controls, including automated controls and controls over interim financial reporting (where external reporting is required), (iv) high turnover rates or employment of accounting, internal audit, or information technology staff that are not effective, (v) accounting and information systems that are not effective, including situations involving significant deficiencies in internal control, (b) risk factors arising from misstatements arising from misappropriation of assets: such as (i) inadequate physical safeguards over cash, investments, inventory, or fixed assets, (ii) inadequate management understanding of information technology, which enables information technology employees to perpetrate a misappropriation, (iii) inadequate access controls over automated records, including controls over and review of computer systems event logs. In Appendix two of ISA 240 includes a set of examples that can be performed in potential audit trials to address cybersecurity related risks of material misstatement due to fraud: (a) visiting locations or performing certain tests on a surprise or unannounced basis, (b) performing computer-assisted techniques, such as data mining to test for anomalies in a population, (c) testing the integrity of computer-produced records and transactions, (d) using computer-assisted audit techniques may be useful in identifying unusual or unexpected revenue relationships or transactions, (e) using computer-assisted audit techniques to further test the compilation of the physical inventory counts – for example, sorting by tag number to test tag controls or by item serial number to test the possibility of item omission or duplication, (f) performing a computerized match of the vendor list with a list of employees to identify matches of addresses or phone numbers, (g) performing a computerized search of payroll records to identify duplicate addresses, employee identification or taxing authority numbers or bank accounts. In Appendix three, ISA 240 presents examples of specific cybersecurity related conditions that can be considered as possible fraud indications: (a) unsupported or unauthorized balances or transactions, (b) evidence of employees' access to systems and records inconsistent with that necessary to perform their authorized duties, (c) missing or

altered documents, (d) unavailability of other than photocopied or electronically transmitted documents when documents in original form are expected to exist, (e) unavailable or missing electronic evidence, inconsistent with the entity's record retention practices or policies, (f) denial of access to records, facilities, certain employees, customers, vendors, or others from whom audit evidence might be sought, (g) unwillingness to facilitate auditor access to key electronic files for testing through the use of computer-assisted audit techniques, (h) denial of access to key IT operations staff and facilities, including security, operations, and systems development personnel. ³⁷

III] 2. Understanding the Correlation between Cybersecurity Dimension and Entities' Internal Controls Systems

Before we present the cybersecurity and cyber-preparedness risks that modern entities face in daily base, it is of the outmost importance to understand how and why cybersecurity risks are related with the internal control system of the client entity. *ISA 315 on Understanding the Entity and its Environment and Assessing the Risks of Material Misstatement* provides a concrete approach in this matter. ³⁸ This standard governs the criteria of recognizing, assessing, and analyzing auditing important risks of material importance, but also the cybersecurity-related risks and the internal controls that entities must apply in order to confront them. The first cybersecurity-related matter is the understanding of technology operated information system(s) or ISs of the entity and the need of auditors to obtain an effective insight about ISs (a) operation and procedural capacities and complexity, (b) the way ISs classify, record, process, amend, transfer and report transactions, accounts, journal entries, unusual events and adjustments, (c) the way ISs perform evaluations, accounts balances, estimations and disclosures upon the particles of (b) and (d) the internal controls related to technology operated and related to ISs. More precisely, according to ISA 315, Information System or Systems can function as components of financial reporting internal controls in the following ways:

³⁷ IFAC (2010), *International Standard On Auditing 240 The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements*, <https://www.ifac.org/system/files/downloads/a012-2010-iaasb-handbook-isa-240.pdf> (last retrieved 25/06/2019).

³⁸ IFAC (2010), *International Standard On Auditing 315 on Understanding the Entity and its Environment and Assessing the Risks of Material Misstatement* <https://www.ifac.org/system/files/downloads/a017-2010-iaasb-handbook-isa-315.pdf> (last retrieved 25/06/2019).

Cyber-security and Cyber-preparedness as a Necessary Part of the Auditing Process

(a) as part of the accounting and financial reporting system, its processes and records ISs can be designed to perform duties like: (i) classifying recording, assessing and reporting transactions, events and general conditions as well as maintaining proper accountability for the related assets, liabilities, and equity, (ii) correcting mistakes in transactions processing, such as automatically suspension of files and procedures for suspended and incorrect elements on a constant time basis, (iii) providing significant information about system overriding or controls bypassing, (iv) allocation of transactions data to central ledger and archiving, (v) providing non-transactional data important to financial reporting such as assets depreciation and amortization information and changes of potential recoverability in accounts receivables, and (vi) delivering important information about obligatory disclosure of financial reporting as it concerns the correct accumulation, recording, assessing, debriefing and reporting in the financial statements.

(b) as part of standard journal entries and journal keeping IS can provide a constant base for (i) recording transactions sales, purchases, cash payments and expenditures in the general book keeping ledger, (ii) recording periodically estimations on accounts, like estimations in uncollectible accounts receivable. Moreover, IS can assist the non-standard journal entries that focus on recording non-recurring, unusual transactions or consolidating adjustments, disposal estimates, such as assets impairment. The application of automated electronic forms in order to sustain the general journal keeping ledger and to arrange financial statements reporting, permits easier data identification through the employment of computer-assisted audit techniques (or GAATs).

(c) as part of the business processes and capacities, like (i) create, purchase, manufacture, sell and deliver an entity's products and services, (ii) safeguards compliance with laws and regulations, and (iii) accommodates data recording, accounting and financial reporting, auditors understanding on how IS assist on transactions recording, assessment and reporting aid them to comprehend the general system of financial reporting in an entity and

(d) ISA 315 recognizes the positive impact of IS and its influence on business processes connected to financial reporting not only for large entities but also for small entities, despite the fact that IS in smaller organizations probably is less advanced but though no less important. Auditors must acquire a sufficient level of understanding on IS accounting processes and computerized sophisticated accounting and book-keeping records even for smaller entities, and the examination on the IS documentation and achieves system can be a part of the auditors standard control assessment.

Cyber-security and Cyber-preparedness as a Necessary Part of the Auditing Process

The second cybersecurity-related matter set by ISA 315 had to do with how technological developments and advancements, such as technology-driven production of goods and services, can impose factors of concern to the industrial operability of an entity.

The third cybersecurity-related matter is related to the impact, positive and negative, of information technology (IT) objectives and strategies of to the overall business risks and to the overall objectives, strategies and policies business success, such as the potential impact to general business realization accomplishments from specific usage of IT when the applied NHS systems are contradictory and improper fitting with the relevant processes. The application of the most suitable IT choices impacts the direction of implemented controls and auditors must measure the effectiveness of controls over general IT systems and applications analogous to their capacity in preserving and ensuring data integrity and process security. General IT controls are referring to policies and procedures related to a variety of applications such as mainframe, miniframe and end-user environments and provide support about the integrity of application controls and the effective operability and on the following: data centers and networks operations, systemic software purchasing, transformation and maintenance, changes in programming, access security and authorization, systemic applications purchasing, establishment and preserving. Paradigms of general IT controls are: (i) program change controls, (ii) controls limiting access to programs or data, (iii) controls over novel editions of packaged software applications, and (iv) controls over access restriction in system software or over monitoring system utilities usage able to alter financial data or records with no obvious audit trail. Application controls are automated (also manual) procedures used in processing of individual applications and function at business process level. They can be preventive or detective in nature, and they are constructed in order to guarantee the integrity of the accounting records and they are related to procedures that initiate, record, process and report transactions or other financial data. Assuring the accuracy, the completeness and the proper authorization of transactions and transactions recording and assessment. Paradigms of automated application controls are: (i) correction controls in entry data, (ii) checks in data arithmetical precision and correction, and (iii) accounts and trial balances keeping and evaluation.

ISA 315 also recognizes that one of the most important matters is the integration of technology advancements and automatizations in internal controls assessment and inspection during audit trails. Auditors can perform their risks assessment either in manual and human labor intense ways or they can incorporate more automated elements and computerized methods. The decision upon which method, manual or automated or blended, auditors will

choose to conduct their internal controls trials impacts the way auditors plan, record, handle, and report transactions in paper or electronic means. Moreover, ISA 315 recognizes the following benefits from the use of IT in internal controls performances: (a) enables the entity to constantly implement preset business rules and directions and to perform complicate calculations and evaluation, since IT can assess significantly large amount of data and information, (b) advances data accessibility, precision and time-suitability, (c) enables further analyzation and examination in the data and information volumes, (d) facilitates further monitoring in the performances of an entity activities, objectives, processes, policies, and operations, (e) decreases the risk controls to be bypassed and sidestepped, (f) increases segregation of duties effectiveness through better implementation of pro-active and protective controls in devices, databases, applications and operating systems and (g) automated elements in internal controls are more reliable and effective than manual elements, since from one side is harder to be circumvented, disregarded and overlooked and on the other side enhance controls better detection and correction of errors and mistakes for excessive volume of data and transactions. The use of technology and automation in internal controls can be accompanied according to ISA 315 from a variety of risks, such as: (a) the first general risk has to do with extended reliability and dependence in IT systems and possible inaccuracy in processing large volumes of accurate data or accurate processing inaccurate data or inaccurate processing inaccurate data, (b) the second general risk has to do with unauthorized or malicious access to data and databases, that might produce general negative outcomes like (i) damage and inappropriate alternations to data, (ii) erroneous keeping record of transactions or (iii) recording unapproved and unauthorized or fictional transactions and more specific risks about datasets access like: (1) misappropriation of segregation of duties by IT employees that exceed the borders of their duties and obtain access more that the permitted one, (2) changes in master files datasets, systems and programs that are not authorized or are mistaken and not correct or are necessary but not performed, (3) unsuitable manual involvement and (4) possible damage and loss in datasets or incapability of proper access to data even thought is expected.

Last but not least, ISA 315 recognizes the following cybersecurity conditions and events that might impose material misstatement risks and auditors must pay significant attention: (a) (frequent) changes in the IT frameworks and environments on an entity, (b) inconsistent matching between the IT strategies and the general business strategies of an entity and (c) induction and establishment of considerable novel IT systems connected to financial reporting processes.

III] 3. Presentation of the Most Important Cybersecurity Risks and Entities' Cybersecurity Internal Controls Response

As we stated previously, the next step in every audit process after the appointment of an auditor (individual or audit firm) by the client entity, is the conduction from the auditor of a thorough and conclusions-productive understanding of the client's entity environment and the risks that might lead to material misstatement according to *ISA 315 on Understanding the Entity and its Environment and Assessing the Risks of Material Misstatement*. In previous section of this Chapter we examined the general approach of ISA 315 on cybersecurity related risks and concerns. Now it is time to concretize on cybersecurity environments and cybersecurity risks that entities must administer in daily base. Since both cybersecurity environment and cybersecurity risks contain a significant amount of information that must be processed by the reader, we decided to split this wide range of knowledge into two sections: in this sub-session of this Chapter we will examine the cyber-related corporate risks an entity faces and what is the most suitable internal controls landscape that entities must apply in order to minimize the impact of this risks and in the next sub-session we will provide a clear view of the cybersecurity compliance environment in which an entity exists, functions, performs its functions, grows and even fails to survive, according to *ISA 250 on Consideration of Laws and Regulations in an Audit of Financial Statements*. We took this decision for two main reasons: the first one is that the extension of cyber-related corporate risks are not that known to the public and the second because knowing the risks is a prerequisite in order to understand the nature of the environment. For example, a lot of compliance norms had been developed in order to deal with particular cybersecurity and cyber-related corporate risks, so we cannot refer to the compliance backgrounds before we had explain the reasons, the risks, that led to their development. That is why, we prefer to first mention the cyber-vulnerabilities, which shape the inherent and residual risk of auditing trail risk and then mention, the related norms and international accounting and auditing standards that are related to each risk.

Mapping cybersecurity dangers and levels of cybersecurity internal control capacities for auditing reasons is a titanic work, providing the fact that new threats or transformed old ones appear multiple times every single day. The problem is so massive that no economic entity can solved it on its own means, posing like that a constant threat to modern economic systems and consequently democratic societies. That is why, more and more states in international, federal, central, peripheral, and local level intervene by adopting relevant

laws, policies and action plans in order to recognize and minimize the proliferation of cybersecurity threats and attacks. According to US *National Institute of Standards and Technology (NIST)*³⁹, combating early detecting cybersecurity threats and other malicious IT behaviors demands a constant and real-time intensive tracking and monitoring of all the electronic devices and resources of an entity. One of the major problems is that not all threats have a malicious context, but some can appear due to normal function and activities of an economic entity, for example, a problem in the digital part of the supply chain system due to problems with the external electricity supplier. Typically, this general security concern is not a malicious one, though it can create many cybersecurity problems: from the destruction of network systems due to different voltage to permanent loss of all data processed during the incident without being properly saved, something that can provoke disturbances, delays, disruption even to put in a temporarily or even permanent halt the whole supply chain system. The same problem can be considered as intentionally malicious, if the shut down in electricity had been provoked intentionally, as part of an attack from a hacker in cooperation with an employee of a company with the aim to cover an electronic industrial espionage attempt, ordered by a rival company⁴⁰. It is more than obvious that auditors (internal and external) must be trained to distinguish analogous cases, in order to report a cybersecurity threat in its proper dimensions, because the magnitude of a situation of that kind can provoke quite big stress not only to the managers and employees of the entity, its shareholders and to the rest of stakeholders (suppliers, clients, local societies, etc.) but also to the reputation of the company, to the price of its share in stock exchanges and to costs from direct or cross-claims from clients (and other stakeholders) due to damages provoked to them directly and indirectly by the cyber-attack.⁴¹ Auditors are in even deeper, more blur and uncharted waters, if the under examination economic entity belongs to the digital ones, companies like social media giants (Facebook, Twitter, LinkedIn, etc.), or integrated digital entities, those that combine multiple digital services from search engines

³⁹ NIST, is the oldest physical science laboratory in USA, created in 1901 and nowadays belongs to U.S. Department of Commerce. It is responsible for the promotion of advanced and innovative and industrial scientific measurements, standards and technologies in order to empower USA's economic competitiveness. **NIST** (14/07/2017), *About NIST*, <https://www.nist.gov/about-nist> (last retrieved 25/06/2019).

⁴⁰ A relevant case of hackers conducting data espionage in cooperation with rival state actors had been revealed recently in Tel Aviv. The extended hacking campaign lasted seven years had as target the acquiring of huge amounts of data from a dozen of global telecommunication companies in more than 30 countries, data concerning individuals working for governments, law-enforcement agencies and decision-making political institutions. **Ari Rabinovitch & Tova Cohen** (25/6/2019), *Hackers steal data from telcos in espionage campaign: cyber firm*, Reuters, <https://www.reuters.com/article/us-cyber-telecoms-cyberreason/hackers-hit-global-telcos-in-espionage-campaign-cyber-research-firm-idUSKCN1TQ0BC> (last retrieved 25/06/2019).

⁴¹ **Waldron Amy & Hallstrom David** (01/09/2013), *A breach of client data: Risks to CPA firms*, Journal of Accountancy, <https://www.journalofaccountancy.com/issues/2013/aug/20138003.html> (last retrieved 25/06/2019).

and email providers to news creators or distributors, like Google, Yahoo, etc. or hardware and software manufacturers, because in these cases companies create new products much quicker than legal systems can regulate themselves and in a much more complex way than auditing science and practice can advance themselves.⁴²

In reality, we can classify cybersecurity threats into two categories: (I) the expected ones, that originate from ordinary activities of an economic entity and derived mostly from inside the entity misbehaviors, such as (a) wrong use and function of networks, hardware, software, rest equipment and data mis-handling, (b) cyber risks in supply chain and other core business parts that had to do with an entities inadequate use, implementation and configuration by employees, (c) misbehavior in the rules of proper function, such as not respecting standards and frameworks of best use of a IT device, and (II) the unexpected ones, mostly referring to both internal and external malicious activities, in order to intentionally harm the economic entity, usually for gaining a benefit (economic, reputational, etc.) and had to do with the exploitation of vulnerabilities on the expected ones by malicious behaviors (internal and third-parties) for purposes other than normal operation and functionality of an entity.⁴³ For example, a hacker can exploit the vulnerabilities in the crypto-asset system of an entity in order to possess illegally these assets for his/hers own benefit. It goes without saying that auditors, during their inspections and creation of their auditing reports, must take under serious consideration both categories of cybersecurity threats since they can be equally catastrophic for a company.

Both expected and unexpected cybersecurity threats, but mostly the unexpected type, are related with the constant rising of what is called cybercrime. This type of cybersecurity alertness includes all the actions that individual actors or group(s) of people can do in order to harm the cyber-systems (of production that use ICT systems and of data creation and reporting) in order to gain financially or in order to produce disruptions or economic harm. Their actions can be registered not only as a violation of internal ethical and good

⁴² This oxymoron situation, meaning regulations being created after a situation and not in advance of the practice, leads pivot companies to self-regulation and self-restriction by forming alliances and other collaborative systems before relevant law be adopted, for example, (a) the **Internet Security Alliance (ISA)**, a pro-market collaborative scheme between banks, auditing companies, multinational companies, etc. established in 2001 aims through leadership, technology, public policy and economics to create a market-base cybersecurity framework and to improve cyber-audits, etc. **ISA** (2019), *Mission and Goals*, <https://isalliance.org/about-isa/mission-and-goals/> (last retrieved 25/06/2019). On the other hand, it seems that companies themselves prefer governments to create the right regulation framework for their industry, such as social media sector, especially when their industry can interact with variable implications to democratic ruling system. **SpaceDaily** (24/06/2019), *Governments must regulate social networks: Facebook's Clegg* http://www.spacedaily.com/reports/Governments_must_regulate_social_networks_Facebooks_Clegg_999.html (last retrieved 25/06/2019).

⁴³ **Κοριαζόγλου Ιωάννης** (2001), *Έλεγχος Συστημάτων Πληροφορικής*, EDP/IT Auditing, Εκδόσεις Anubis, Αθήνα, Page 153.

governance codes, but most of all as a violation against legal norms and obligations and can lead to prosecution and even to punishment in a court and to jail of the cyber-criminal actor. In this category, we can include every action both from inside the company members (executives, employees, etc.) or external actors of a company (hackers, rivals, former employees, partners, etc.) that can manipulate electronic acquired data for personal benefit against the entity's fame, economic resilience, and long-lastingness. Moreover, we can also include, any electronic manipulation concerning the authenticity and creditability of financial statements. In general terms, cyber-attacks can be economically (even politically) driven actions by the so called "black hat hackers" in order to provoke negative impact and disruption in their targets, which can varied from private sector entities to public authorities, non-governmental organizations, etc. In this category, critical infrastructure entities, private and public, such as those managing grids and electricity plants, nuclear power plants, water facilities, military facilities, banks, stock exchanges, telecommunication, and transportation industries, voting systems, etc. must be specially protected and secured from cyber-attacks of any type, due to the fundamental role they play to national economy and security. Successful cybersecurity attacks in this category of entities is a direct offense and even harm to the democratic system of modern states. A lot of cybersecurity protection and compliance standards and frameworks with significant auditing importance, that we will examine in this paper (mostly in the next chapter), were orchestrated in order to protect (not only though) these critical infrastructure systems.

The skyrocketing rising of cybercrime goes hand in hand with the creation of alternative markets, best known as darkmarket, where important data of entities, such as banking data, invoices details, customers data, intellectual property data, etc. are exchanged between cyber-criminals (like cyber-mafia schemes, hackers, crackers, etc.) for profit⁴⁴.⁴⁵ Cyber-spaces and their potential chances of profitability had shape a new incentives paradigm of malicious cyber-behaviors from the traditional malicious motivation acronym of **M.I.C.E.** (Money, Ideology, Compromise/Coercion, Ego/ Extortion), that was being developed by FBI military security counterespionage profiling, to **M.E.E.C.E.S.** (Money, Ego, Entertainment, Cause, Entrance and Status), meaning that nowadays cybercriminals not only aim at obtaining money resources, fame and a better status and respect among their communities, or as challenge of their capacities, but also for reasons of amusement and

⁴⁴ Sometimes, cybercriminals demand through their actions not only profit gains, but also fame among the societies of cybercrime. The bigger the impact of the cyber-attack and the amount of cyber-profit can provoke the bigger the acquired reputation for its creator.

⁴⁵ **Misha Glenny** (2012 for Greek edition, 2011 the original), *DarkMarket: CyberThieves, CyberCops and You*, Papiros Publishing, Athens.

because they can exploit the vulnerabilities, that exist in hardware, software and network of entities in order to enter with success to distinguish cybercriminal societies⁴⁶. Cyber-security incidents and attacks, due to this vulnerabilities, can have an extremely negative impact in auditing performances, due to the fact that the entities that suffered from cyberattacks and their data leaked to darkmarkets, usually prefer not to report these incidents to legal and law enforcement authorities and to their external auditors out of the reputation and business continuity damage, risking like that the quality and truthfulness (*true and fair view* auditing principle) of the auditing reporting.

Another aspect that is quite important when we examine the auditing related cybersecurity vulnerabilities and gaps is the issue of cyber-terrorism, which can provoke a wide range of disruption and destruction in IT systems and capacities in all types and sizes entities, in order to create panic, chaos, public fear and political benefits. Sometimes, malicious cybersecurity threats can combine characteristics: for example, a cyberterrorism group (external cyber-criminal), on its own merit or hired by a rival, can achieve its goal to provoke disruption on a company's production lines or/and cause chaos and public discontent, by executing targeted cyber-attacks to ICT systems of entity, having the aid from an inside the company employee (internal cyber-criminal). Auditors must be in a constant alert while performing their cybersecurity auditing controls in order to spot and report any activity that create suspicion about the integrity of the cyber-systems.

In the following part of this research thesis, we will present the most important cybersecurity threats as it concerns the main cyber-related aspects of an entity: networks, hardware and software (alternatively NHS) not only in a defining way, but also we will present the implications can have to business continuity and what entities (and auditors) must take under consideration when they deal with these types of vulnerabilities.

III] 3. 1 Malicious Code and Programs

This category of malicious code is referring to viruses, worms, Trojan horses and other malicious data files. **Viruses**, is a type of malicious programs designed to be attached to non-harmful program, files, documents, and installed through them in a computer and then to provoke abnormal operation on its functions, harming, corrupting files and programs,

⁴⁶ **Kirwan Grainne and Power Andrew** (2012), *The Psychology of Cyber Crime: Concepts and Principals*, IGI Global, Page 59 and **Radcliff Debrach**, 01/03/2004, *MEECES to pieces*, Network World, <https://www.networkworld.com/article/2330885/meeces-to-pieces.html> (last retrieved 25/06/2019).

spamming email contacts inside the entity and with outside stakeholders, stealing passwords or data, destroying or erasing data, causing permanent damage to hardware, even provoke the full control of an entity's system in favor of an outside the entity player. They can stay in a dormant status, until their creators execute their code and provoke harm, but even in this state they can spread to an entity's software and networks. **Worms** are a type of a virus program with the ability to self-propagate from one device and computer to other with the aim to use the device resources for reasons other than their normal function, something that can halt the responding capacities of a device. **Trojan Horses** are types of computer programs that carry a virus or other malicious and potentially harmful programs, that are attached to malicious usually of a free, open access and legitimate software and perform damaging activities to NHS systems. **Other malicious data files** are non-executable files, like Adobe PDF files, ZIP files, image/picture files, Microsoft Office files, audio and video files, greeting cards, etc. that are used by cybercriminals in order to install malicious codes on NHS systems that will exploit NHS vulnerabilities and weaknesses on the process of opening them. The most frequent ways the above-mentioned malicious codes use to penetrate to an NHS systems are via email, text message attachments, applications, social media, websites, portable and mobile devices, social media scams links, spamming, internet file downloads, scam advertisements, unprotected web surfing, etc. in order to maximize the risk of infection and contagion of NHS systems.

Entities Internal Controls Response: must be in two tiers: first tier is the response in case of a malicious code infecting and compromisingly affecting the NHS systems of an entity and involves three steps: (i) the minimization of the damage and disconnection of NHS systems from online activity in order to spot and "clean-up" them from any malicious code, programs and applications, (ii) the assurance that no other part of NHS systems apart the infected one were not compromised and in case they did, they must be also cleaned-up from any harmful code, (iii) the implementation of a recover, reconstruction and business continuity plan/strategy, that might include reinstalling or installing new safer programs, applications, operational software, etc., (iv) sometimes, there is another step in this tier (though not always obligatory) and that is reporting the incident to authorities. The second tier is more proactive, precautionary and prophylactic, than treating the problem, and has to do with cyber-preparedness of an entity in future malicious code incidents and involve: (i) the use of a reliant, effective and trusted anti-virus, firewall/malicious code blocking and pop-ups advertisements block software for its NHS systems and their regular updating and upgrading, additionally to (ii) the adoption and implementation of a realistic and effective

“anti-virus policy”, which will include (a) cautionary use and obligatory scanning of all emails, data, links, files attachments, websites, web browsers, etc. before opening, saving, sharing and distribution to internal NHS systems⁴⁷, b) adoption of the strategy to frequently change (usually every six month but definitely after a cyber-incident) and trustworthy, strong, difficulty to break, cryptographed if it is possible, passwords, c) limiting the number of installed programs and applications only to the necessary one and permanent uninstalling and removing of the old, unused, problematic and vulnerable programs and applications, since cyber-criminals exploit gaps in unused or outdated programs to provoke harm, d) adoption of a strategy of limited permissions/access accounts, which means that only a limited number of employees are authorized to have access to data and only because their position demands that, in order to avoid sensitive data to be accessed by everyone so the risk to be mal-treated. Any unauthorized, unusual or suspicious activity and access to data and accounts must be handled as a cautionary flag and treated likewise, e) deactivation of all external media automatically running choices (such as AutoRun and AutoPlay features) unless they are firstly properly inspected in order to minimize the risk of co-running behind the scenes malicious code, f) adoption of a non-use blocking strategy of external, public, unauthorized and unscanned WiFi networks by personnel not only for working needs but also for recreational and personal needs, for example during lunch breaks, casual Fridays events, ordering food services, etc., g) application of best cybersecurity practices, h) secure your web browsers from unsafe online surfing, and i) ensuring safe store and back-up capacities for data (in reliable cloud services, in owned by the entity second hard drives or/and in reliable external storing facilities) and especially the most sensitive of them, such as bank details and accounts, invoices, clients transactions, etc. This issue is also related with data protection requirements and with regulatory compliance with relevant legal obligations (something we will see in the next part of this Chapter).⁴⁸

⁴⁷ But also while the internal NHS systems interact and exchange data with external NHS, such as those of clients, providers, auditing services, third-party storing services, public authorities, etc. since an entity’s internal NHS systems can be equally affected if externals stakeholders NHS systems suffer from viruses and other malicious codes.

⁴⁸ **CISA** (11/04/2019 (revised)), Security Tip (ST18-004): Protecting Against Malicious Code, <https://www.us-cert.gov/ncas/tips/ST18-271> (last retrieved 25/06/2019). **CISA** (04/11/2013), *Security Tip (ST13-003) Handling Destructive Malware*, <https://www.us-cert.gov/ncas/tips/ST13-003> (last retrieved 25/06/2019). **McDowell Midi** (for CISA) (11/10/2010), *Security Tip (ST10-001) Recognizing Fake Antiviruses*, <https://www.us-cert.gov/ncas/tips/ST10-001> (last retrieved 25/06/2019). **McDowell Midi** (for CISA) (19/03/2009), *Security Tip (ST05-006) Recovering from Viruses, Worms, and Trojan Horses*, <https://www.us-cert.gov/ncas/tips/ST05-006> (last retrieved 25/06/2019). **Durkota Michael D. and Dormann Will** (2008), *Recovering from a Trojan Horse or Virus*, Carnegie Mellon University, <https://www.us-cert.gov/sites/default/files/publications/trojan-recovery.pdf> (last retrieved 25/06/2019). **CISA** (08/09/2015), *Securing Your Web Browser*, <https://www.us-cert.gov/publications/securing-your-web-browser> (last retrieved 25/06/2019).

III] 3. 2 Harmful Malwares

The word malware(s) derive from the words malicious software and is a type of cyber-threat closely related with the previous one and includes the following variety of cyber-threats:

A] Fake anti-virus online software is a type of malware created in order to obtain data and information illegally from the victims, which the victims believe that they download (usually for free) a legitimate anti-virus software. Since, this harmful software is mimicking standard anti-virus operations, it can even send to the user normal-looking security warning, while at the same time behind the scene is provoking a variety of modifications to NHS systems difficult enough to be tracked, terminated and removed.

Entities Internal Controls Response: certainly a lot of actions described in the previous type of threat can also be used for this cyber-threat, but also top managers must secure that: (i) the personnel must avoid downloading free and third-parties anti-virus(es), using unauthorized search engines, responding to unknown email accounts, surfing in popular social networking pages and sites, responding to online advertisements, subscribing to unrelated with the company services, etc., (ii) no entity's devices of any kind, banking credentials and data should be exploited by the personnel in order to have access to online features, such those described in (i), neither employees must download any unauthorized software using entity's devices, even if employees pay any downloading fees and subscriptions, (iii) the entity's policy of using only authorized software and purchased by the entity must be fully understood and implemented by the employees, (iv) constant monitoring and if it is possible terminate any unauthorized and unusual activity in bank accounts and cards, (v) in case it is obligatory or for extra aid entities can report these type of cyber-incidents to relevant authorities.⁴⁹

B] Rootkits and Botnets: this category of software is not malicious *per se* but it can be used in order to provoke harm to entities, since its main characteristic is that they can be installed and remain hidden without the user to know and sometimes without anti-virus program to be able to track and deactivate them. **Rootkits**, is a type of software that attackers might use in order to monitor their victim's actions, compromise programs and files and take charge of the infected computer, since when they are installed (either as a part of a more complex software systems either by cyber-criminals) can be successfully hidden and stay inactive

⁴⁹ **McDowell Midi** (for CISA) (11/10/2010), *Security Tip (ST10-001) Recognizing Fake Antiviruses*, <https://www.us-cert.gov/ncas/tips/ST10-001> (last retrieved 25/06/2019).

until their creator choose to use them in order to provoke harm. **Botnets or (ro)bot networks**, as an automated computer software (otherwise a robot) enables the control of a computer or a series of computers by using not only one but many other external sources. Usually cyber-criminals use a virus or a trojan horse or any other malicious code (such those described previously) in order to gain access and control to the target computer, even though the compromised computer might appear to function normally. When botnets are not used for normal operating functions, such to monitor employees activities, they can provoke a series of malicious harms that range from inserting to NHS system(s) malicious codes and spams and compromise data to provoking greater harm such as denial-of-service attacks, etc., and despite that harm to stay undetected and even when they are detected it might be extremely difficult to recover.

Entities Internal Controls Response: choices referring to the previous sections, such as (i) use of a reliant and updated anti-virus software and firewall software, (ii) have a strong and difficult to compromise password policy, (iii) always performing the necessary updates and upgrades to software (for example in operating systems) and hardware (for example devices, networks, etc.), (iv) create a strong and sound IT department that follows the best security protocols and practices, is always important to be implemented. Hence, in this list we can also add behaviors like: (v) in case of a relevant incident it might be necessary to erase the compromised file(s) because trusting the pre-attacked file might not be safe, something that augments the importance of having back-up files, especially of the most important data.⁵⁰

III] 3. 3 Social Engineering and Phishing

In a **social engineering attack**, a cyber-criminal take advantage of social communication and other types of human interaction, such as social media, SMS, voice communication, texts, messages, etc. in order to gain access to data and other information of the computers systems of an entity with the aim to compromise data and to provoke harm. The attacker may use respectable credentials by impersonating someone respected with the scope to acquire important information. If the amount of information is not enough or not of the desired quality and quantity, the attacker can continue to contact to other employees of the same entity and even use the information acquired from previous social engineering attempts.

⁵⁰ **McDowell Midi** (24/09/2011), *Understanding Hidden Threats: Rootkits and Botnets*, <https://www.us-cert.gov/ncas/tips/ST06-001> (last retrieved 25/06/2019).

In **phishing attacks**, which is a form of social engineering, hackers can send malicious emails, links, websites, and attachments to an entities communication gateways in order to present themselves as legitimate and trustworthy social interaction channels, such a financial or credit card entity or a charity, and by this way to gain access to an entity's email correspondence and pursue access to sensitive companies information (patents, design patterns, etc.) or to obtain bank passwords and other financial documents in order (a) to ask for money for not reveling the sensitive information to rivals or/and b) to gain as much is possible from entering to bank accounts. The passwords gained by cyber-criminals can be used to provoke internal problems to the entity's NHS systems, for example to shut down electricity systems, networks and other hardware and software of a company. Sometimes attackers use special situations, such as natural disasters, economic and financial hardships, tax reporting occasions, official election events, epidemics, and health concerns, etc., in order to convince employees to start interacting with them and to exchange information. If a fraudster uses a voice type of communication to obtain confidential information, such as telephone, Voice over Internet Protocols (VoIP), etc., we call the attack "*vishing*", but if the fraudster uses SMS, or text messages the attack is characterized as "*smishing*", next to used of email which is the original meaning of "*phishing*". Banking sector frauds conducted in this kind of ways (phishing/vishing/smishing) are extremely serious for both financial institutions and their clients. This malicious behavior manipulations use legitimate actions, such as sending a humoristic email, an advertisement, or a discount offer, or other non-suspicious ways to stimulate employees to open them, or respond to them, etc. Even if these emails are discharged into spam, they still can provoke damage to an entity.

Entities Internal Controls Response: entities must have a clear policy (mostly by applying the right software and by promoting the right mentality to its employees) about (a) which type of emails should enter in an entity's communication gateways, (b) the way they should be deleted in order not to activate their negative results, (c) not to reveal information about the entity, its networks, its financial position, personal information of employees, etc., (d) how to change passwords in a more reliable way, especially if these passwords had been revealed in a phishing attack. Additionally, to have a high level of anti-virus and firewall protection and to increase their anti-phishing capacities of email providers and web browsers, entities must perform phishing simulations that can adhere the anti-phishing resilience and capacities of an entity's not only as it concerns internal critical players, like

top executives and staff, but also external players, like clients, providers, banking providers, etc.⁵¹

III] 3. 4 (Distributed) Denial of Service Attacks

A Denial of Service (or DoS) attack takes place when targeted computers, devices, email accounts and providers, networks, information systems, online accounts (like those of a bank or a payments organization), websites, online service providers cannot proceed their normal operations due to fact that a cyber-actor had orchestrated a vast traffic on those systems provoking either inability of them to respond normally or their (usually) temporary crash out from the ordinary functionality blocking like that the normal access to important services from legitimate users and an entity's employees. DoS attacks can provoke significant costs in entities: from reputation loss to money and worktime resources spending in order to restore to normal services and NHS systems affected by the DoS. When the attack is happening due to the organized action of a series of devices or/and botnets (like those described previously in III] 3. 2 B section) or any other series of maliciously controlled online devices organized in that way to provoke large scale traffic attacks then we are talking about Distributed Denial of Service or DDoS.

Entities Internal Controls Response: since hackers can sell or rent their capacities to provoke DDoS to any person or organization willing to harm an entity, especially now that more and more computerized applications (such as Artificial Intelligence (AI), Internet of Things (IoT) applications, etc.) govern the everyday reality of any entity's operations, it is more necessary than before entities to increase their shield systems against (D)DoS, even though complete immunity is non-achievable. Using the services of a (D)DoS protection and clean up service (can be an external provider or an inside the entity team or both) that detects, redirects and decreases any external abnormal traffic to an entities network is the primary tool for an entity to face this kind of challenge. Additionally, having a clear and effective (D)DoS crisis recovery plan that will contain alternative and emergency communication networks to the main one are another useful tool, that modern entities must have, next to the standards ones that takes place for every vulnerability mentioned in this section, meaning the installation of effective updated and upgraded anti-virus, firewall

⁵¹ **US Federal Trade Commission** (2019), *Phishing*, <https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/phishing> (last retrieved 25/06/2019). **Luxembourg Bankers Association** (ABBL) (2019), *Phishing/Smishing/Vishing*, <https://www.abbl.lu/topic/phishing-smishing-vishing/> (last retrieved 25/06/2019).

protection systems and the constant evaluation of security configurations and settings to all NHSs from the IT department.⁵²

III] 3. 5 Ransomware

In this way hackers install successfully a malicious software on an entity's systems with the aim to disrupt normal function or provoke other problems to an organizations operability and continuity capacities, in order the entities to be forced to pay significant amounts (ransom) of money (or crypto-assets) for the deactivation or removal of the malicious "ransomware" software. In case of the ransom is not paid (but even if it does) hackers usually destroy data and other capacities of a company as a revenge against the entity's decision not to succumb to their blackmail, or just to cover their trails.

Entities Internal Controls Response: first line of defense is the application. Updating and upgrading of the NHS systems to secure networks and software from being compromised and to minimize their vulnerability to this type of cyber-attacks must be a priority in all organizations. Moreover, organizations must (a) constantly train their personnel against ransomware attacks, (b) create a relevant ransomware attack and recovery plan, (c) apply strong configuration and control of access to important accounts, even for the privileged individuals, such as top managers, (d) deactivation of macro-scripts for the office files that are transferred via corporate emails, (e) performing back-up and back-up verification and security in regular basis, (f) application of software restriction policies and any other relevant restrictive controls to minimize the possibility of a ransomware attack due to overuse of popular internet websites, or downloaded/uploaded compressed/decompressed files and programs, and (g) cooperate with law enforcement authorities (police, government agencies, etc.) to deal these situations.⁵³

III] 3. 6 CEO/CFO scams or Whaling and Identity Thefts

Hackers usually impersonate themselves through emails or other means of digital communication pretended to be the CEO or CFOs or other top executive individuals asking

⁵² **CISA** (04/11/2009), *Security Tip (ST04-015): Understanding Denial-of-Service Attacks*, <https://www.us-cert.gov/ncas/tips/ST04-015> (last retrieved 25/06/2019).

⁵³ **US Federal Trade Commission** (2019), *Ransomware*, <https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/ransomware> (last retrieved 25/06/2019). **FBI** (2019), *Cyber Crime*, <https://www.fbi.gov/investigate/cyber> (last retrieved 25/06/2019).

from employees to make or divert (usually immediately) payments to bank accounts usually not related to official entities accounts, accounts that are controlled by hackers. The employees conduct the payments and transfer the money out of the need to comply with their superiors demands, despite the fact that these income capacities end up to cyber-fraudsters. In general terms, identity thefts take place when a malicious person obtain, use and even sell and trade other people or entities information, such as phone numbers, addresses, credit card numbers, accounts data, clients' information and any other potential profitable information about an entity's databases and NHS systems. Since identity theft is considered mostly as a type of opportunistic crime, meaning that a person or an entity can be a victim because their data is easily accessible and available by cyber-criminals, reasons like (a) easy accessible, poorly protected and/or compromised database, (b) the type of the company and the demographic of its clients, for example a bank's database with account details of its customers is high valuable in darkmarkets. Identity theft is a crime and in some countries, there is relevant legislation that leads to severe types of punishment, while at the same time is recognized as a type of illegitimate behavior that involves also other types of illegal action, such as used as a mean to cover identification fraud, computer fraud, mail fraud, credit card fraud, wire fraud, financial fraud, etc.⁵⁴

Entities Internal Controls Response: they must create, endorse and implement a clear policy for all involved in payments employees, so before they make any payment, must perform first a due diligence and inspection of the legitimacy and authentication of the digital communication they receive in order to avoid transfer capital of their company to hackers. Moreover, entities must decide to make transactions and business only with high reputable stakeholders and avoid those that they receive a lot of relevant attacks in the past. Implementing strong password policies and other security features (like anti-virus protection, firewalls, effective privacy policies, strategy of minimum public disclosure of information, etc.) is also extremely important.⁵⁵

⁵⁴ These types of frauds usually are considered as crimes and are accompanied by heavy penalties, even prison time. For example, in United States of America, the Identity Theft and Assumption Deterrence Act constitutes identity theft not only a violation of federal law but also can signify heavy fines, and even up to 15 years imprisonment. **United States Department of Justice** (07/05/2017), *Identity Theft*, <https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud> (last retrieved 25/06/2019).

⁵⁵ **CISA** (21/11/2018) (revised), *Security Tip (ST05-019): Preventing and Responding to Identity Theft*, <https://www.us-cert.gov/ncas/tips/ST05-019> (last retrieved 25/06/2019). **United States Department of Justice** (07/05/2017), *Identity Theft*, <https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud> (last retrieved 25/06/2019). **Luxembourg Bankers Association (ABBL)** (2019), *CEO Fraud*, <https://www.abbl.lu/topic/ceo-fraud/> (last retrieved 25/06/2019).

III] 3. 7 Keylogger

Despite the fact that is one of the oldest types of malicious cyber issues is not well-known as a threat, usually because a keylogger service can be used for normal function reasons within an institution, such as monitoring the activity of the staff, testing NHS capacities, fixing problems remotely, assisting security and anti-virus attempts, observing user experience, enhancing legal and intelligence authorities surveillance, etc. In reality, a keylogger is a monitoring software that tracks, monitors and keeps records of the (physical) keystrokes that a person had performed on a keyboard and then send this information to a third-party, which can be from a law enforcement officer to an IT expert inside an entity to even a cyber-criminal. The later can exploit these sensitive personal, functional, financial, banking, clientele and other type of data of an entity or its staff in order to sell them to rivals, to darkmarket, etc., or to blackmail the company, something like a “data kidnapping”, in order to ask for ransoms.

Entities Internal Controls Response: in order entities to secure themselves from malicious keyloggers threats must adopt early on a anti malicious keylogger policy that will include, (a) the application of keylogger identification techniques in allocation and monitoring of resources, procedures, and information, (b) the use of anti-keylogger, relevant anti-virus and cyber-protection software, (c) the deactivation of self-running files in internal network from external devices, like non-authorizes USBs and other portable devices not connected to the entity, (d) to change passwords regularly and have a policy of strong passwords (difficult to be obtained passwords) and a strategy of two-factor authentication and other means of protection like the use of virtual onscreen keyboards that are harder to be keylogged.⁵⁶

III] 3. 8 Financial Information Disclosure and Use of Social Media Vulnerabilities

In a highly connected world in digital and operational terms, entities of any kind and size, tend to use media, not only the traditional media channels (newspapers, magazines, etc.) but also the recent social media (Facebook, Twitter , LinkedIn, etc.), in order to publicize important press releases, earnings, designed and future plans and other catching

⁵⁶ McAfee (23/07/2013), *What is a Keylogger?*, <https://www.mcafee.com/blogs/consumer/family-safety/what-is-a-keylogger> (last retrieved 25/06/2019). Swinhoe Dan (11/12/2018), *What is a keylogger? How attackers can monitor everything you type*, CSO, <https://www.csoonline.com/article/3326304/what-is-a-keylogger-how-attackers-can-monitor-everything-you-type.html> (last retrieved 25/06/2019).

the audience attendance news about their operations in an attempt to increase customers base and their loyalty, to attract new customers, to obtain more shareholders and raise the price of their stock, to forge new business collaborations, to diversify marketing and communication channels and to monetize these open-access communication networks. After all presentation, publication of material information and public disclosure of financial information in the appropriate way, especially for enlisted to stock exchanges entities, is a legal obligation according to a series of International Accounting Standard (IAS) and International Financial Reporting Standard (IFRS) and their amendments. More precisely *IAS 1 on Presentation of Financial Statements*, *IAS 10 on Events after the Reporting Period*, *IAS 24 on Related Party Disclosures*, *IAS 27 on Separate Financial Statements*, *IAS 29 on Financial Reporting in Hyperinflationary Economies*, *IAS 32 on Financial Instruments: Presentation*, *IAS 34 on Interim Financial Reporting*, *IFRS 1 on First-time Adoption of International Financial Reporting Standards*, *IFRS 3 on Business Combinations*, *IFRS 7 on Financial Instruments: Disclosures*, *IFRS 8 Operating Segments* and *IFRS 12 on Disclosure of Interests in Other Entities*. Moreover, disclosing information in social media platforms can be a low-cost choice but a quite powerful tool for managing reputation and brand performance of an entity, though no risk free at all, on the contrary it can function as an activator and/or accelerator factor for cyber-related risks.⁵⁷ Associate Professor of Information Systems at Columbus State University in Georgia, USA and a highly recognized expert in this field, *Tommie Singleton*⁵⁸, recognizes the inherent risk of using social media and media in general are similar as those of other IT systems, focusing mostly on potential problems having to do with their effectiveness, their efficiency, their ability to function as an opportunity and their added-value instruments or even can be considered as being a wasting of an entity's money, time and effort. He explains also that these means of publication carry two unique characteristic risks: a) the public image or reputation risk, due to negative comments and feedback in social media outlets, that can hurt the fame of an entity⁵⁹ and b) the operational effectiveness⁵⁹ risk, that auditors must correlate with the

⁵⁷ An executives opinion survey (192 individuals from USA) in 2012 conducted by Deloitte & Touche LLP and Forbes Insights, identify the use social media as the fourth largest risk over the next three years, able to trigger financial related risks and costs, even regulatory authorities (SEC) violations and penalties. **Deloitte & Touche LLP and Forbes Insights** (2012), *Aftershock Adjusting to the new world of risk management*, https://deloitte.wsj.com/cfo/files/2012/10/Aftershock_Adjusting-to-the-new-world-of-risk-management.pdf (last retrieved 25/06/2019).

⁵⁸ **Prof. Singleton Tommie** (2012), *What Every IT Auditor Should Know About Auditing Social Media*, *ISACA Journal*, Volume 5: 2012, Page 12-13, http://www.isacajournal-digital.org/isacajournal/2012vol5?article_id=1077872&pg=NaN#pgNaN (last retrieved 25/06/2019).

⁵⁹ In a recent study on Standard and Poor's 1500 firms index (covers almost 90% of US stock market capitalization) about strategic dissemination of financial information (quarterly earnings announcements) to social media like Twitter, the researchers found that when the news and earnings are bad and plunging, firms are less likely to disseminate that information to the public. The publication displays also in a cross-sectoral

business model and goals of an entity's management team from using this communication tools. These two types of risks can take the form of: 1) loss in productivity and mistakes from distracted employees overusing social media during working hours, 2) negative comments and posting, 3) inefficient control of the posts content and posts with offending content for some cultures, 4) increased potentiality of breaches, able to harm not only the reputation of an entity but also its confidentiality level, 5) increased potentiality of a back-fire incident or even a revenge event, 6) increased potentiality of being victim of a hacking incident, malware attack, identity theft, social engineering, loss of sensitive or strategic type of data and information not only of the entity's but also of its customers and other related organizations, 7) increased probability to be presented as a brand with unstable and inconsistent behavior, 8) misuse of network and communication networks, 9) possible compliance violation of corporate laws, regulations and legal obligations, internal policies, ethical codes and best practices strategies, mostly concern data privacy, data security requirements and financial disclosure requirements,⁶⁰ 10) increased risk of financial damage

analyses that corporations “with lower level of investor sophistication” and those that have a large scale of attractiveness in social media audience tend to use more social media for strategic financial information disseminations. Another characteristic spotted by this research has to do with the detectability of strategic financial dissemination in social media, which is increased in “high litigation risk firms, but not in low litigation risk firms”. Another finding of the research had to do with the audience performance and engagement and what potential dangers this engagement can bring, since tweeting or retweeting negative news by followers of a firm can provoke extra production in news and articles from traditional media, a back-fire danger by dissemination reporting in Twitter. **Jung Michael. J., Naughton James P. Tahoun Ahmed & Wang Clare** (2018), *Do Firms Strategically Disseminate? Evidence from Corporate Use of Social Media*, The Accounting Review (2018) by American Accounting Association,, Volume 93, Issue 4, Pages 225–252, <https://meridian.allenpress.com/accounting-review/article-abstract/93/4/225/53582/Do-Firms-Strategically-Disseminate-Evidence-from?redirectedFrom=fulltext> (last retrieved 25/06/2019).

⁶⁰ Sometimes financial dissemination and disclosure, especially of publicly traded companies, a domain of financial reporting that is strictly regulated, can trigger authorities' reaction in case of possible or actual financial information disclosure misconduct. For example, in April 2013 US SEC released a report to clarify on how entities can use social media (such as Facebook and Twitter) in order to announce important information that complies with Regulation Fair Disclosure (or Regulation FD) requirements, that demand from companies to disclose significant information in a broad access, non-exclusive and non-selective manner to relevantly notified public and investors. The release came to enrich the 2008's SEC guidance about the prerequisite using websites as effective channels of financial disclosure and dissemination information to investors as long as they informed and notify in advance those investors that they post to social media with this intention, and since these posts *constitute selective disclosures* must be accompanied by a *careful Regulation FD analysis*. The reaction of SEC was the outcome of an inquiry conducted by SEC's Division of Enforcement against a post on Facebook's personal account by Netflix CEO Reed Hastings, updating users about his firm monthly online viewing had surpassed for the first time one billion streaming hours, helping like that the Netflix's stock price to increase from \$70.45 when the Facebook post is made to reach \$81.72 by the end of the next trading day. Even though SEC did not start an enforcement action of supposed wrongdoing and regulations violation against Hastings or/and Netflix, since the company did not report this material to investors through official channels, like a press release or Form 8-k reporting and since neither Hastings nor Netflix had used Hastings' personal Facebook page as a public disclosure information medium before or had inform the investors that they will use it, recognizing the gap of regulatory application of Regulation FD in the case of social media outlets, the SEC released the relevant report of investigation in accordance to Section 21(a) of the Securities Exchange Act of 1934, making clear that personal social media of an enlisted company employees are not among the normal disclosure channels of corporate information so the public must be notified in advance about their use since the lack of that notification might not be qualified as an approved medium of an entity's material information publication and disclosure according to securities regulations. **SEC**

due to negative impact of a post in stocks price and strategic plans and performance, 11) damage on the personal reputation of an employee or a manager, 12) physical safety risks by releasing travelling data, etc.⁶¹ 13) third-party risks, such as probable identity theft, copyright and trademark complications due to outsourcing marketing, advertising, media and social media performance, 14) poor governance performance, due to low-quality coordination, insufficient understanding of the opportunities and dangers of using social media channels, lack of a visionary attitude about the transformative impact of social media, low maturity business model that consumes ineffectively social media and money resources⁶² and 15) for enlisted companies and any other relevantly obliged entity there is always the danger to pay significant fines and penalties for violating regulation on recognized ways to publicly disclosure material and financial information, are among the basic reputation and operational effectiveness risks. An example that incorporates a variety of the above-mentioned risk list (numbers 2-5, 7-11 & 13 and is connected to reference 43), is the 2018 settlement case for securities fraud charge and lack of proper disclosure controls and procedures on CEO's Musk using his personal Tweet account in order to announce material financial information by SEC on Tesla and Tesla's CEO and Chairman Elon Musk, that not only forced Musk to resigned as the company's Chairman (Musk cannot be elected as the firm's Chairman before a three years period pass) and to be succeeded by an independent Chairman but also obliged Musk and Tesla to pay a \$20 million penalty each, with the allocation of these penalties money resources to harmed investors by Elon Musk Tweeting (August 07, 2018) of taking Tesla private at \$420 per share. Among other requirements of this settlement are not only the appointment of two new independent directors in the Board of Directors of Tesla, but also the obligation of Tesla to establish a new instrument, a Committee of Independent Directors, as well as the adoption of additional controls and measures to supervise the legitimacy and the impact of statements and communication releases of former CEO Musk.⁶³

Entities Internal Controls Response: the managing team of an entity must understand fully the cyber-dangers the entity faces by being active to media and more precisely to social

Release 2013-51 (02/04/2013), *SEC Says Social Media OK for Company Announcements if Investors Are Alerted*, <https://www.sec.gov/news/press-release/2013-2013-51.htm> (last retrieved 25/06/2019).

⁶¹ **Gargano Antonello** (30/09/2011), *Managing Privacy Risk in a Social Media-Driven Society*, Protiviti, Page 19-20, http://www.aiea.it/sites/default/files/attivita/sds/roma_30_settembre_2011_gargano.pdf (last retrieved 25/06/2019).

⁶² **Deloitte** (2013), *The digital grapevine: Social media and the role of Internal Audit*, <https://www2.deloitte.com/global/en/pages/risk/articles/social-media-internal-audit.html> (last retrieved 25/06/2019).

⁶³ **SEC Release 2018-226** (29/09/2018), *Elon Musk Settles SEC Fraud Charges; Tesla Charged With and Resolves Securities Law Charge*, <https://www.sec.gov/news/press-release/2018-226> (last retrieved 25/06/2019).

media and promote this message to its personnel and other related stakeholders. Especially, as it concerns the publication of the entity's financial data the managing team must take all the appropriate measures to intensify the compliance with all the relevant regulations, regulations that concern the data privacy and security, such as the ***Gramm-Leach-Bliley Act*** (GLB Act or GLBA of 1999, also known as the Financial Modernization Act), a United States of America federal legislation that demands from financial institutions to explain on how they secure, protect and share with the public their clients' private and sensitive data. Additionally, the United States Federal Trade Commission (US FTC) had developed the so called ***Privacy Rule*** (or Privacy of Consumer Financial Information Rule) in accordance to GLBA's Safeguards Rule that offers a variety of means for best protection of customers data, among which, is the obligation of the adoption of a written information security plan about the best protection of customers' data. Violations of the GLBA are accompanied with significant fines.⁶⁴ Relevant requirements are set by other authorities and regulations, such as (a) the USA ***Financial Industry Regulatory Authority*** (FINRA) that demands from entities offering financial services to keep and publicize in an approved way records, such as disclosures in social media outlets, and is also extended to communications over social channels and (b) the ***Payment Card Industry Data Security Standard*** (PCI DSS) that demands from entities to demonstrate that cardholders' data are not publicly available in unsecured mediums of communication, such as social media platforms.⁶⁵

Next to the reasonably understanding and comply with regulations actions, entities must ensure that they have the acquired level of protection against publication vulnerabilities by adopting the most efficient and best-applicable tools: such as 1) to obtain all the necessary certifications, and 2) to adopt a system of controls as it concerns (a) data privacy, privacy assessment and security, with emphasis to most sensitive information, (b) a cost-effective incidence response plan in case of an emergency situation, (c) a trustworthy vendor and client communication management channel, and (d) increased physical security policies regarding not only equipment but also people, etc.⁶⁶

III] 3. 9 Supply Chain Vulnerabilities

⁶⁴ **Federal Trade Commission** (April 2006), *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying> (last retrieved 25/06/2019).

⁶⁵ **Deloitte** (2013), *Ibid*.

⁶⁶ **Gargano Antonello** (30/09/2011), *Ibid*, Page 23.

Securing supply chain systems had experience their importance inside the modern economic and globalized world skyrocketing the last 30 years, despite the fact that as a corporate activity is as old as corporates themselves. Nowadays, supply chain system can be considered as the core of any modern economic entity since coordinates everything from: (a) production capacities and supply of primary, secondary and semi-processes materials, (b) handling fix and tangible assets like equipment and materials of manufacturing, operation, building, maintenance and repair and their depreciation and impairment in value, (c) use, accounting, reporting and amortization of intangible assets, like patents, trademarks, copyrights and intellectual property rights, (d) packaging material and services, (e) services, like logistics, consulting, security, call centers, customs duties, currency fees, taxes, leasing, borrowing/loans, state grants, third party-services and outsourcing, cleaning services, legal services, accreditation services, insurance services, auditing services, contractors services (incoming and outcoming), joint ventures, energy and telecommunication services, etc., (f) sales, customers and returning (g) providers and suppliers, (h) storage and warehouse needs, (i) pricing and transportation of goods and services. In a nutshell, supply chain management is pivot for all the processes of strategic goals of planning, design of goods, production, total quality management, logistics, invoice, contracts, and sales, marketing, and shipment activities of an entity, connected with a number of obligations deriving from International Accounting Standard (IAS) and International Financial Reporting Standard (IFRS).⁶⁷

Entities Internal Controls Response: the great abundance, variety, complexity and significance of data produced by all these activities demand high-performance and sophistication supply chain management systems, such as ERP (Electronic Resource Planning), EDI (Electronic Data Interchange), EFT (Electronic Fund Transfer), MRP or MRPS (Material Requirement Planning Systems), CRM (Customer Relationship Management), SRM (Supplier Relationship Management), RFID (Radio-Frequency Identification), Barcoding, ABC (Activity Based Costing), ECR (Efficient Consumer Response), POS (Point of Sales systems), VMI (Vendor Managed Inventory), EPI (Early Purchasing Involvement), ESI (Early Supplier Involvement), DUNS (Data Universal Numbering System), SKUs (Storage Keeping Units), and other systems, that are susceptible

⁶⁷ Among the most related to supply chain performances IAS and IFRS are: IAS 2 on Inventories, IAS 8 on Accounting Policies, Changes in Accounting Estimates and Errors, IAS 11 on Construction Contracts, IAS 12 Income Taxes, IAS 16 on Property, Plant and Equipment, IAS 17 on Leases, IAS 18 on Revenue, IAS 20 on Accounting for Government Grants and Disclosure of Government Assistance, IAS 21 on The Effects of Changes in Foreign Exchange Rates, IAS 23 on Borrowing Costs, IAS 28 on Investments in Associates and Joint Ventures, IAS 36 on Impairment of Assets, IAS 38 on Intangible Assets, IAS 40 on Investment Property, IAS 41 on Agriculture, IFRS 2 on Share-based Payment, IFRS 3 on Business Combinations, IFRS 4 on Insurance Contracts, IFRS 5 on Non-current Assets Held for Sale and Discontinued Operations, IFRS 6 on Exploration for and Evaluation of Mineral Resources, IFRS 13 on Fair Value Measurement, IFRS 15 on Revenue from Contracts with Customers, IFRS 16 on Leases, and IFRS 17 on Insurance Contracts.

to cyber related dangers, attacks and misconducts, like those we describe above.⁶⁸ Entities can minimize those cyber risks and other supply chain security risks by adopting and applying widely accepted and respected relevant standards, such as the implementation *ISO 28000:2007 on Specification for security management systems for the supply chain*.⁶⁹

III] 3. 10 Intellectual Property Cyber-thefts and Industrial Cyberespionage

This kind of risk is very closely related with the risk of supply chain vulnerabilities (as we described it previously) because intellectual property (IP) attacks and trade secret breaches through cyber channels can spot, target and exploit vulnerabilities in manufacturing and supply chain vulnerabilities, even though in order to achieve in succeeding a cyberespionage attack will use one or more malicious codes and behaviors dangers, from the ones we described earlier, as a vehicle of achieving their desired cyber-penetration. Intellectual property assets include trademarks, patents, copyrights, and other intangible assets, that are susceptible to IAS 38 set of criteria about the ways an entity must recognize, measure, sell, transfer, license and disclosure them.⁷⁰ Intellectual property or industrial or trade secrets cyber-espionage targets especially the manufacturing, entertainment, education, healthcare, information, professional/technical, finance, retail and public sectors, since these sectors are the most advanced in producing and patterning intellectual properties,⁷¹ and have the most *industrial control systems* (ICSs). ICSs contain a series of audit related control systems, such as the Process Control Systems (PCS), the Distributed Control Systems (DCS), and Supervisory Control and Data Acquisition (SCADA), the performance of which enables auditors during their internal control inspections.⁷²

Entities Internal Controls Response: due to the significance of intellectual property rights as an entity's more data nature assets, is important for companies to take early measures to tackle this potential danger, securing like that that they will not lose their reputation,

⁶⁸ Λάιος Λάμπρος (2001), *Διοίκηση Εφοδιασμού (Supply Chain Management)*, Εκδόσεις HUMANTEC, Πειραιάς, multiple pages.

⁶⁹ ISO, *ISO 28000:2007 on Specification for security management systems for the supply chain*, <https://www.iso.org/standard/44641.html> (last retrieved 25/06/2019).

⁷⁰ IFRS Foundation (2019), *IAS 38 Intangible Assets*, <https://www.ifrs.org/issued-standards/list-of-standards/ias-38-intangible-assets/> (last retrieved 25/06/2019).

⁷¹ Verizon (2019), *2019 Data Breach Investigations Report*, <https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf> (last retrieved 25/06/2019).

⁷² KPMG (2016), *Securing Industrial Control Systems*, <https://assets.kpmg/content/dam/kpmg/ca/pdf/2016/11/ca-kpmg-cyber-securing-industrial-control-systems.pdf> (last retrieved 25/06/2019).

profitability, the advantage of being the first to introduce a new product to the market, their negotiating position and capacity and even losing entire parts of market and lines of production in favor of their rivals and attackers. So, for their best protection, entities must develop and store all the related to IP data in copper shielded, blocking radio waves, cameras, online activities and unauthorized devices and related individuals to use Secure Compartmentalized Information Facilities (SCIF) or best known as safe rooms in order to develop the IP assets. The same solution is used by governments for best protection of national and defense secrets, but it can be also used in order to protect corporate IP assets and other types of sensitive data. Additionally, entities can use a certified with high reputation third-party service for storing its IP data next to its own relevant capacities. In any case, entities must apply a strict confidentiality and non-disclosure policy not only with its external development and storage of IP processes and data providers, but also with its internal relevant employees (such as Research and Development -R&D- employees, copyright experts and lawyers, marketing creators), in order to minimize the possibility of its IP secrets to be exposed. Moreover, entities might choose to be insured against cyber-espionage threats. Last but not least, in order to prevent any attack on its NHS systems for cyber-espionage aims, entities must secure the least from any malicious threat, such as those described earlier in this sub-Chapter.⁷³

III] 3. 11 Vulnerabilities due to Emerging Technologies:

Emerging technologies offer new and innovative solution for entities, though due to their digital nature can be a great source of many and complex cyber-vulnerabilities not only during an entity's operation activities, but also during auditors' performance. Despite the fact that, these technologies were designed with the aim to minimize fraudulent incidents in entities, to assist auditors during their internal controls' inspections and aid auditing committees and Board of Directors during their work, they can provoke quite a lot cybersecurity problems on their own, that is why, it is of the outmost importance an entity to be adequately prepared.⁷⁴ The use of these emerging technologies, and to the point that in

⁷³ **Gelinne John, Fancher J. Donald and Mossburg Emily** (25/07/2016), *The hidden costs of an IP breach: Cyber theft and the loss of intellectual property*, Deloitte Review Issue 19, <https://www2.deloitte.com/us/en/insights/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html> (last retrieved 25/06/2019). **KPMG** (2016), *Securing Industrial Control Systems*, <https://assets.kpmg/content/dam/kpmg/ca/pdf/2016/11/ca-kpmg-cyber-securing-industrial-control-systems.pdf> (last retrieved 25/06/2019).

⁷⁴ **Centre for Audit Quality** (December 2018), *Emerging Technologies An Oversight Tool For Audit Committees*, CAQ, https://www.thecaq.org/wp-content/uploads/2019/03/caq_emerging_technologies_oversight_tool_2018-12.pdf (last retrieved 25/06/2019).

their functionality process is based usually in external providers, constitutes auditors' job and controls planning processes more difficult and complicated, that is why, they must be in constant alert for any gap in ordinary business performances. We must clarify that as other types of examined here vulnerabilities, such as information disclosure through web channels, supply chain and intellectual property owning and production are not pure cybersecurity dangers *per se*, though they can become if cybercriminals perform malicious attacks, using one or more of methods we had already described previously. Moreover, innovative technologies, such as those we are about to examine here (Internet of Things, Artificial Intelligence and Robotic Process Automatization, Blockchain and Smart Contracts) are not only areas where auditors must intensify their controls processes, but also useful tools to conduct their auditing performances, able to transform the auditing profession.⁷⁵

III] 3. 11. A) Blockchain, Smart Contracts and Crypto-assets

Despite being in existence for more than a decade⁷⁶, the world became more familiar with blockchain technology and perhaps its more risky edition, crypto-assets and cryptocurrencies like bitcoin crypto-currency, from 2017 and after, due to the skyrocketing of the price of bitcoin and the frauds accompanied this event. Nowadays there are dozens of hundreds crypto-currencies available and even companies endorsed their own, despite the fact that numerous scams, frauds, thefts, hacking attacks even kidnappings⁷⁷ are being correlated with this art of blockchain application. Unlike any centralized traditional banking system and making business and trade system that are based on public's trust that clients data, records and money resources are well-kept, protected and maintained by the centralized ledgers, like central banks, federal bank, banks, business entities with private and secure databases, blockchain is a type of Distributed Ledger Technology (or DLT), a

⁷⁵ **Raphael Jon** (01/04/2017), *Rethinking the audit: Innovation is transforming how audits are conducted—and even what it means to be an auditor*, Journal of Accountancy, <https://www.journalofaccountancy.com/issues/2017/apr/rethinking-the-audit.html> (last retrieved 25/06/2019). **Boillet Jeanne** (28/09/2018), *How can you build trust when emerging technologies bring new risks?*, https://www.ey.com/en_us/digital/how-can-you-build-trust-when-emerging-technologies-bring-new-risks (last retrieved 25/06/2019).

⁷⁶ The theoretic base of blockchain crypto—currency application is originated in a white paper published in October/November 2008, after the 2008 global financial crisis and believe to existed financial institutions crisis, by “Satoshi Nakamoto” (a pseudonym for a person or a group of persons) on how a peer-to-peer digital cash payment method could be used soon to substitute official centralized financial organizations and banking system with the issuance of a non-supported by central governments and states currencies. The implementation of this idea started early next year with the creation of code and issuance of the now famous Bitcoin.

⁷⁷ **BBC** (29/12/2017), *Exmo Bitcoin exchange manager freed by kidnappers*, <https://www.bbc.com/news/business-42518235> (last retrieved 25/06/2019). **Kaspersky** (2019), *4 Common Cryptocurrency Scams and How to Avoid Them*, <https://www.kaspersky.com/resource-center/definitions/cryptocurrency-scams> (last retrieved 25/06/2019).

decentralized and not central bank supported technology, of which the auditability of the ledger is open, shared and viewed by all the users involved, something that brings pros and cons to the whole idea. In the next paragraphs we will present basic concepts concerning blockchain and crypto-assets technology, their applications, their connection with regulatory compliance obligations and their correlation to the auditing profession and practice.⁷⁸

Some of the benefits and drawbacks by using a blockchain technology in financial sector are: (a) banks (commercial and even central) now have a rival electronic payments and money storing system that will force them, comparing to the actions that led to 2008 financial crisis, to be less reckless and risky with their clients and taxpayers money. (b) since the system is not centralized, no bail-out government resources will be expected to be

⁷⁸ Unless is stated otherwise, the information for building this section of the Thesis is taken from the following sources: **Investopedia** (2019), *Blockchain explained*, <https://www.investopedia.com/terms/b/blockchain.asp> (last retrieved 25/06/2019). **US Federal Trade Commission** (October 2018), *Consumers Information: What to know about Cryptocurrency*, <https://www.consumer.ftc.gov/articles/what-know-about-cryptocurrency>, (last retrieved 25/06/2019). **Deloitte**, *What is a Blockchain?*, <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-what-is-blockchain-2016.pdf>, (last retrieved 25/06/2019). **PWC** (2017), *Blockchain: a catalyst for new approaches in insurance*, <https://www.pwc.com/gx/en/insurance/assets/blockchain-a-catalyst.pdf> (last retrieved 25/06/2019). **Yaga Dylan, Mell Peter, Roby Nik & Scarfone Karen** (October 2018), *NISTIR 8202: Blockchain Technology Overview*, NIST, <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf> (last retrieved 25/06/2019). **Iansiti Marco and Lakhani Karim R.** (2017), *The Truth About Blockchain*, Harvard Business Review: January-February 2017 Issue, <https://hbr.org/2017/01/the-truth-about-blockchain> (last retrieved 25/06/2019). **Maguire Eamon, Nagaraj Kiran, Wyner Sam and Goens LaDarius** (2017), *Securing the Chain*, KPMG International, <https://advisory.kpmg.us/content/dam/advisory/training/pdf/securing-the-chain.pdf> (last retrieved 25/06/2019). **Murray Joe** (June 2019), *ICYMI : The Coming World of Blockchain: A Primer for Accountants and Auditors*, CPA Journal, Issue June 2018, <https://www.cpajournal.com/2019/06/20/icymi-the-coming-world-of-blockchain/> (last retrieved 25/06/2019). **Appelbaum Deniz and Smith Sean Stein**(2018) *ICYMI: Blockchain Basics and Hands-on Guidance: Taking the Next Step toward Implementation and Adoption*, CPA Journal, Issue June 2018, <https://www.cpajournal.com/2019/06/27/icymi-blockchain-basics-and-hands-on-guidance/> (last retrieved 25/06/2019). **Loop Paula** (13/09/2018), *Blockchain: What Boards Need to Know*, National Association of Corporate Directors (NACD), <https://blog.nacdonline.org/posts/blockchain-boards-need-to-know> (last retrieved 25/06/2019). **Ernst & Young LLP** (2018), *Cryptocurrencies and cryptoassets: Managing the new asset class*, [https://www.ey.com/Publication/vwLUAssets/ey-cryptocurrencies-and-cryptoassets-managing-the-new-asset-class/\\$File/ey-cryptocurrencies-and-cryptoassets-managing-the-new-asset-class.pdf](https://www.ey.com/Publication/vwLUAssets/ey-cryptocurrencies-and-cryptoassets-managing-the-new-asset-class/$File/ey-cryptocurrencies-and-cryptoassets-managing-the-new-asset-class.pdf) (last retrieved 25/06/2019). **Wollmert Peter** (10/04/2019), *How to prepare for the digital transformation of reporting*, EY, https://www.ey.com/en_gl/assurance/are-you-prepared-for-the-digital-transformation-of-reporting (last retrieved 25/06/2019). **US SEC** (2019), *Spotlight on Initial Coin Offerings (ICOs)*, <https://www.sec.gov/ICO> (last retrieved 25/06/2019). **US SEC** (25/07/2017), *Securities Exchange Act Of 1934, Release No. 81207, Report of Investigation: Pursuant to Section 21(a) of the Securities Exchange Act Of 1934: The DAO*, <https://www.sec.gov/litigation/investreport/34-81207.pdf> (last retrieved 25/06/2019). **US SEC: Divisions of Enforcement and Trading and Markets** (07/03/2018), *Statement on Potentially Unlawful Online Platforms for Trading Digital Assets*, <https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading> (last retrieved 25/06/2019). **Sterley André** (2019), *Cryptoassets: Accounting for an Emerging Asset Class*, CPA Journal, Issue June 2019, <https://www.cpajournal.com/2019/06/21/cryptoassets-accounting-for-an-emerging-asset-class/> (last retrieved 25/06/2019). **US IRS** (2019), *Virtual Currencies*, <https://www.irs.gov/businesses/small-businesses-self-employed/virtual-currencies> (last retrieved 25/06/2019). **Houben Robby and Snyers Alexander** (June 2018), *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion*, EU European Parliament, <https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf> (last retrieved 25/06/2019). **European Securities and Market Authority –ESMA** (09/01/2019), *ESMA50-157-1391: Advice on Initial Coin Offerings and Crypto-Assets*, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf (last retrieved 25/06/2019).

used in case of a crisis· (c) *proof of work*, one of two major operational blockchain protocols to enhance reliability and trust to the blockchain (used by Bitcoin, Ethereum and other crypto-currencies), offers protection to the system in the following way: transactions confirmation and building new blocks demand from miners and blockchain users to prove they had solve the difficult mathematical and computational problems. The first person that solves the mathematical problem (an equation) is rewarded with the native currency, can also put the blocks in the right sequence and by that confirms the transaction(s) and so on, according to the workload of blockchain, the volume and amount of transactions, the amount of miners mining at the same time, etc. These efforts demand great computational capacity and electric power, include fees analogous to the demand and volume of mining and transactions and can be a time and energy consuming activity, plus they are not immune to hacking attacks and malicious behaving· (d) *proof of stake*, is the other major operational protocol, and allows to the blockchain system to randomly select a miner or miners to create the next sequence block (that is actually the process of “mining”) and add more native tokens (type of security keys) by expected them to provide a “stake”, a portion, of their own native gained cryptocurrencies to the blockchain system. Despite being less decentralized, proof of stake systems enhance network stability and are more environmental friendly and computational power and energy overuse restricted, they are accused of having what is called as the “*rich getting richer*” approach, since the more the coins a person stacks, the higher are the odds in favor of him/her to mine the next block of the chain. This reality prevents other miners with low coin capacity to mine new blocks, but at the same time protect the whole blockchain network from malicious behaviors, since any malicious action of a miner towards the system will result his/hers losing the coin tokens that he/she owns.

For the best protection of blockchain networks and system from cybersecurity threats and attacks, blockchains apply their own protective mechanisms: (a) each transaction that is part of any blockchain system is firstly *cryptographed* (hence the expression “crypto”-assets and “crypto”-currencies) in a complex predetermined in length thread of numbers and letters. This cryptographed string functions as a transactions identifier and is generated by the blockchain users in the form of public and private keys· (b) *private keys* function as a form of electronic signatures for the digital identification and verification of each blockchain individual user and are unique for each user, while *public keys* (also known as digital “wallets” or crypto-wallets) derives from personalized private keys and are the ones to be disclosed to the public before any transaction in order the transaction to be completed, but there is no access to a public key without knowing the private key first· (c) *masternodes*

(node is another name for individual user), is the governing heart of a crypto-asset network and keeps the system in actual time frame, keeps full record of blockchain transactions and activities, and ensures that they are constantly running and are being properly updated. It is quite difficult to obtain a masternode (status), because not only demands more native coins staking and important storage capacities, but also because it incorporates an upper managing authority and governing power, though for that rewards (such as receiving regular payments in native coins) are significantly higher and more often. Masternodes, provide higher level of stability and protection to the blockchain networks by its ability to track efforts of crypto-assets price manipulation by big wallet and coins owners-individuals that dump immense amounts of coins in an given moment in order to control their market price. (d) *trace transactions ability*, is referring to the characteristic of the blockchain technology to track any transaction made to the network, since once a transaction is confirmed, it is grouped in the form of block together with other transactions, creating a chain of blocks that are validated by distributed ledgers according to each blockchain agreed and used proof protocols. Every validated and approved block offers a link to the previous block, which incorporates a link for the previous block and so on in a repeated link process, where all the blocks of the blockchain are connected with links to each other. Since all blocks are anchored to each other, the related users can trace transaction and find any misconduct to the blockchain, through the initial creation process, enhancing like that the intactness, accuracy and cybersecurity integrity of blockchain technology from falsifications. (e) *validated blockchains cannot be destroyed*, unless the majority (at least 51%) of users agree to make necessary changes and adjustments. Achieving this majority can be quite difficult adhering like this to the protective and cyber-safeguarding mechanism of the blockchain technology. (f) *smart contracts*, in general terms a smart contract is an agreement, a deal, between two individuals that is presented in the form of a computer program (code), that permits under specific circumstances the automated relocation of values and data to a database for storage and do not allow any change in the data provided⁷⁹. (g) *blockchain refresh process*, allows to the data of block to be refreshed automatically and regularly many times within a day, so validation of confirmation and accuracy of transactions remain intact and functional and no conflicts emerge. After every refresh all blocks that did not receive the minimum amount of confirmations in this multiple third-party validation process fall off the blockchain, creating what is called as extinct blocks. The rival between two miners on who is going to place first

⁷⁹ Ethereum is a global, community-based, open source, public, blockchain distributed computing platform and operating system, that can be used to verify smart contract accuracy and functionality. **Ethereum** (2019), *What is Ethereum?*, <https://ethereum.org/what-is-ethereum/> (last retrieved 25/06/2019).

his/hers block in the blockchain also leads to the creation of extinct blocks, in this first to place block contest the block of the miner who was second in this rivalry is also an extinct block. In the very end, only confirmed and validated blocks after a refresh are connected with the main blockchain and can be used further, blocking like that any virtual fraud and double use and spending attempts, (h) *tokens and Initial Coin Offerings (ICOs)*, the ICOs function similarly to stocks' Initial Public Offerings (IPOs) but instead of the investor to receive stocks from the Stock Exchange, receives tokens (another name of coins), which permit access to the product or service of the traded blockchain application ICO.

The applications of blockchain, as all the other emerging technologies examined here, can be multiple covering almost any sector of modern economic life. Due their internal quality characteristics blockchain applications can be quite useful achieving the following functions: (a) *enhance inside and cross-border payments and transactions*: people will no longer need to pay high commissions and fees and wait for a lot of days in order to see their fund transactions to be completed successfully according to the legal requirements by Society for Worldwide Interbank Financial Telecommunications (Swift) or national, since with blockchain application, like Internet of Value (IOV), even large amount of money can be transferred within seconds with only a small amount of fees (usually about a cent or less).⁸⁰ This is a much more time and resources saving mechanism comparing to traditional money transferring methods, while banks must check their own actual liquidity and foreign currency capacities before they make any money allocation to the correspondent bank, a situation accompanied with high fees and capital requirements. (b) *enables thorough accounting and auditing*: blockchain technology permits a time and resources saving inspection of financial accounts, invoices, records, payments, transactions and balances, since physical examination can be replaced by a more effective, easier-examined, validated, difficult to be manipulated and change transactional history within the blockchain system. Blockchain technology enables the so called "*smart audits*", used by audit firms in order to enhance audit tests efficiency and resources focusing on client's entity records and financial statements since all entries, transactions and changes in accounts payable and receivable are kept secure in blockchain records of distributed ledgers. (c) *promotes efficient logistics*, because blockchain enables and improves better communication between the partners of supply chains like carriers, traders, production companies, better tracking of shipping and

⁸⁰ Ripple, an advanced blockchain crypto-asset that permits to its clients to instantly and cheaply allocate money all around the globe. Many bank conglomerations, like Santander Banco, payment providers, like Moneygram, American Express, Western Union, and digital asset exchanges even corporations use Ripple for making their transactions. **Ripple** (2019), *Instantly Move Money to All Corners of the World*, <https://ripple.com> (last retrieved 25/06/2019).

merchandising on and off-shore, more transparency and documentation in supply chain record keeping· (d) *assists in real-time data acquisition, verification and allocation*, which helps accountants and auditors to perform time precise analytical tests and examinations during financial statements inspections and to minimize the verification time and resource consumption during these inspections· (e) *ameliorates different levels of access*, since blockchain permits differentiated access permissions can assure the addition of new or/and different users without compromising data protection level by exposing material data to unauthorized users and (f) *secures accurate corporate and governmental record keeping*, blockchain networks can store, verify, and maintain relatively safe large amounts of important data, no matter if they are corporate data or central governments and authorities data, like tax data, persons identification data, voters registration data, property ownership data, etc., a capacity of blockchain that helps reducing time leverage of a completed transaction (like transferring property rights) additional to reducing identity thefts danger.

Another element of blockchain and more specifically of crypto-currencies and other crypto-assets is the point that these intangible values can be accepted by existed or future (national mostly) law as assets, so the issue of compliance with legal requirements and the proper recognition of them in financial statements appears and demands further attention from the side of entities and corporations. The evolving of crypto-assets landscape had created different types crypto-currencies and the determination of their nature, meaning if they are intangible forms of assets, securities, or cash in financial statements, is quite difficult. Until, so far their major types are: (a) *security or asset-backed tokens or securitized tokens or investment type crypto-currencies*, that can be used in a way similar to stocks, derivatives, equities and bonds, and other conventional types of securities, can be issues by an entity through a similar to ICOs process called Security Token Offering (STO) and must comply with national (for example US's federal) laws governing securities· (b) *utility tokens*, a type of digital coupon, that permits either discounted fees either access to a blockchain application or a service, and unlike security tokens they are not usually considered as investments, so there is no obligation to must comply with national security (federal) laws, and (c) *payment-type crypto-currencies*, like Bitcoin, do not have any tangible value apart from providing to their holder the expectation of the potentiality to serve as a means of exchange or as a means of payment in order to acquire goods or services.

Countries have developed different approaches towards all these types of crypto—assets in the form of tokens (coins), but the general approach must be based on the

characteristics of each token and its ICO.⁸¹ In *United States*, Securities and Exchange Commission (SEC) guidance determines when a token transaction is an investment transaction or not using the (established from 1946 from the 1946 case *SEC v. W.J. Howey Co.*, 328 U.S. 293, based on Securities Act (1933 and amendments) and Securities Exchange Act (1934 and amendments)) so called *Howey Test*, which determines that if a money investment conducted in a common enterprise with the expectation of profiting from the solely efforts of the promoter or third party, then this investment is a security, that must be reported, disclosed and governed according to relevant laws, otherwise there can be a rule violation, something that can include criminal penalties.⁸² Moreover, the USA tax authority, IRS, had issued a relevant guidance with which virtual currencies, like Bitcoin, will be taxed regularly as a form of property⁸³, investment, and payment method for goods and services, so they incorporate tax liability in case of improper tax disclosure. The whole regulation process of crypto-assets can include also the involvement and action from other related authorities in USA, such as the U.S. Commodity Futures Trading Commission (CFTC), the Financial Crimes Enforcement Network (FinCEN), and the Financial Industry Regulatory Authority (FINRA).

In *European Union's* level also there are some attempts to regulate virtual currencies, so obligations, guidance and/or advice produced by different EU institutions, raise awareness about issues like: (a) anonymity, (b) money laundering, (c) tax evasion and (d) financing terrorism and market stability. More precisely, the fifth *Anti-Money Laundering Directive* (AMLD5-EU Directive 2018/843 of 30/05/2018)⁸⁴ defines in Article 1 *virtual currencies* “as a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established

⁸¹ The case by case decision approach is the one that United Kingdom's (UK) responsible authority, Financial Conduct Authority (or FCA) had adopted. **Financial Conduct Authority** (27/02/2019), *Initial Coin Offerings*, <https://www.fca.org.uk/news/statements/initial-coin-offerings> (last retrieved 25/06/2019).

⁸² SEC had also issued numerous subpoenas and requests for additional information for companies and advisers related to crypto-currencies. **Eaglesham Jean and Vigna Paul** (28/02/2018), *Cryptocurrency Firms Targeted in SEC Probe: Regulator issues subpoenas to parties engaged in booming market for initial coin offerings*, Wall Street Journal, <https://www.wsj.com/articles/sec-launches-cryptocurrency-probe-1519856266> (last retrieved 25/06/2019).

⁸³ Other countries recognize crypto-currencies and more specifically Bitcoin, either as private money (“units of accounts”), in the case of Germany, either as a commodity for tax purposes, in the case of Canada's Revenue Agency. **Mandjee Tara** (2015), *Bitcoin, its Legal Classification and its Regulatory Framework*, Journal of Business & Securities Law, Volume 15, Issue 2, Page 165, Published by Digital Commons at Michigan State University College of Law, 2016, <https://digitalcommons.law.msu.edu/jbsl/vol15/iss2/4/> (last retrieved 25/06/2019).

⁸⁴ **Official Journal of the European Union** (19/06/201), *Directive (EU) 2018/843 of the European Parliament and of The Council Of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance)*, L 156/43, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN> (last retrieved 25/06/2019).

currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically” and custodian wallet provider, such as crypto-currencies platforms, “as an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies”. In Article 47 the Directive determines that “Member States shall ensure that providers of exchange services between virtual currencies and fiat currencies, and custodian wallet providers, are registered, that currency exchange and cheque cashing offices, and trust or company service providers are licensed or registered, and that providers of gambling services are regulated.” Moreover, Article 57a requires from all persons that work or have worked or acting on behalf of competent authorities supervising credit and financial institutions that must comply with this Directive as well as auditors and other experts to cooperate and exchange information with Member States according to the provisions and requirements of professional secrecy. This is not the first attempt of EU to clear out the connectivity of EU regulations to ICOs and crypto-assets (crypto-currencies): *European Commission’s 2018 FinTech Action Plan*⁸⁵ had the same objective. The **European Securities and Markets Authority** (ESMA) had identified from late 2017 that the issue of ICOs and crypto-assets demands deeper evaluation from its Standing Committee on Financial Innovation, due to their novelty, rapid development, the high price volatility of the related markets, the demanding attention business model, possible speculation concerns and lack of relevant regulatory framework in national and European level. ESMA had issued two relevant Statements: in November 2017 a *Statement on Initial Coin Offerings* (ICOs) and in February 2018 a *joint-Warning on Virtual Currencies* (VCs) in cooperation with European Banking Authority (EBA) and European Insurance and Occupational Pensions Authority (EIOPA) driving attention to the speculation matter, to lack of knowledge and worry from the investors about the high risks ICOs and VC impose and to need for compliance with EU regulations for the active in these domains firms. According to ESMA’s early January 2019 *Advice on Initial Coin Offerings and Crypto-Assets*⁸⁶ a closer examination of crypto-assets as transferable securities or other types of MiFID (Market in Financial Instruments Directives framework) financial instruments, connected with a number of EU’s financial laws such as the *Prospectus*

⁸⁵ **European Commission** (2018), *COM 109/2 Communication From The Commission To The European Parliament, The Council, The European Central Bank, The European Economic And Social Committee And The Committee Of The Regions: FinTech Action plan: For a more competitive and innovative European financial sector*, https://ec.europa.eu/info/sites/info/files/180308-action-plan-fintech_en.pdf (last retrieved 25/06/2019).

⁸⁶ **European Securities and Market Authority –ESMA** (09/01/2019), *ESMA50-157-1391: Advice on Initial Coin Offerings and Crypto-Assets*, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf (last retrieved 25/06/2019).

Directive, the Transparency Directive, MiFID II, the Market Abuse Directive, the Short Selling Regulation, the Central Securities Depositories Regulation and the Settlement Finality Directive, the Financial Collateral Directive (FCD), the Alternative Investment Fund Managers Directive (AIFMD), the Electronic Money Directive and the Payment Services Directive, the Electronic Identification and Trust Services for Electronic Transactions in the Internal Market Regulation, must be conducted in order to ensure a technology neutral approach in the matter and the harmonized applicability of the same standards in all cases, since different requirements and confronting approaches from the above-mentioned legal document enhance even more to (a) the obscurity, suitability and definition issues, (b) the demand for accurate, transparent and time-related record (book)keeping, disclosure and reporting, (c) the market manipulation, abuse and poorly regulation danger, (d) the reduction of potential systemic risks and other risks (like insolvency, collateralization, settlements, transferability, ownership, custodian banking/safekeeping, operations maintenance, cyber-attacks, money laundering, etc.) related with the existence and trading of such values, and (e) the regulatory and enforcement gaps created upon these significantly important financial and economic thematic.

This entire regulatory (national/federal and European) framework creates a very important question about crypto-assets: How entities must report them in accounting and auditing terms according to relevant standards, such as ***US Generally Accepted Accounting Principles (US GAAP)*** and/or ***International Financial Reporting Standards (IFRS)***?, Are these standards sufficient and applicable enough? What are the purposes of their creation and how do they fit in an entity's business model? In general terms, virtual currencies are recognized as: (a) *assets*, fitting the definition criteria of assets of both US GAAP and IFRS recognized assets as items that their cost or value can be estimated in reliable ways, and are obtained and controlled by an entity resources as an outcome of past actions with the aim of future economic benefits deriving from their position in favor of the entity. So, entities must assess whether the virtual currencies they hold meet these criteria in order to recognize them as assets. (b) *cash or cash equivalents*, after being recognized as assets they must be classified in the right category of assets, with cash or cash equivalent be among the possible categories. Though in order to be categorized as such must be central bank and government supported and generally accepted as a mean of payments and exchange, so as their volatility not to provoke to holders great distress and uncertainty, something that in current terms crypto-currencies do not fulfill as a criteria. (c) *inventory*, both IFRS and US GAAP recognizes as inventories assets any asset that is either held for sale as finished goods during

the ordinary function (course) of a business, either as goods soon to be finished but still in process to be produced in order to be sold and either as raw materials and supplies that will be used during production or will be rendered of a service. IFRS recognize as inventories intangible assets that are produced in order to be resold, like software (while GAAP show differences in this matter) and also both recognize properties purchased or developed in order to be resold in the ordinary course of business. Criteria, like being mined or purchased in order to be resold and their intangibility (for IFRS but not for US GAAP) can be in favor of crypto-currencies, however due to the fact that their trading volumes and penetration in transactions capacities are not so widely spread, do not adequately qualify them to be considered as succeeding the clause of being “*held in the ordinary course of business*”. In case though they are being classified as inventories, they must be measured at the lower of cost and net realizable value, according to both IFRS and US GAAP (US GAAP demands inventories that are estimated according to Last-In, First-Out -LIFO- method or retail methods to be measured at the lower cost and market, but crypto-currencies do not fit in this criteria, so we choose the common criteria of measurement). Irrelevantly to the used method of measurement, due to the volatility of that market, probably the related information about crypto-currencies in financial statements will not elaborate usefully their readers. Purchasing and selling crypto-currency transactions by commodity brokers and dealers that measure these currencies at fair value and the cost of selling are much less and able to recognize profit or loss from these transactions as part of the ordinary course of their business might provide more reliable financial information.

(d) *intangible assets*, both IFRS and US GAAP recognize this type of assets as an identifiable (meaning being separable, transferable, rentable, exchangeable either individually or together with a related contract, asset or liability, or arising from contractual or other legal rights regardless if these rights are transferable), non-monetary (or financial for US GAAP) asset, not having a physical substance. Only, IFRS though determines that it must be controlled by the entity and to be expected to provide future economic benefits to the entity (as the asset supposed to do). To the fact that crypto-currencies are entirely digital in nature covers the non-physical substance clause. Their almost unlimited and unexpired nature that constitutes them capable to be exchanged either cash, either goods, or services, constitutes crypto-assets under US GAAP to be initially recognized at cost and be prone to annual impairment, especially in case their value decline below cost. Under IFRS intangible assets are recognized either at cost either at “fair value” revaluation having accumulated any impairment losses at the date of being revaluated (in an active market of sufficient transactions of assets and liabilities in volume and frequency that provides data about the prices of them on an ongoing basis) and

(e) *financial instruments*, which are monetary contractual assets (or contractual rights about the delivery or receiving cash other financial instruments or an individual's ownership evidence of an entity) that can be traded, or packed with other capital in order to be traded together, measured at fair value and recorded of changes in profit or loss also in fair value. This category can be perceived as the natural identification belonging category of crypto-currencies, but since they do not generally provide to their holder the contractual right of purchasing and selling cash or other financial instruments, is unlikely to be considered as financial instruments. Some crypto-currency futures though provide contractual rights of purchasing and selling crypto-currencies in the future and can be reconciled with cash, allowing them to be perceived as derivatives and subsequently can be considered as financial instruments. US GAAP can allow under specific circumstances the hold of crypto-currencies as a form of investment under the capacity of an "investment company status", that demands this type of investment to be recognized at fair value, initially and subsequently.⁸⁷

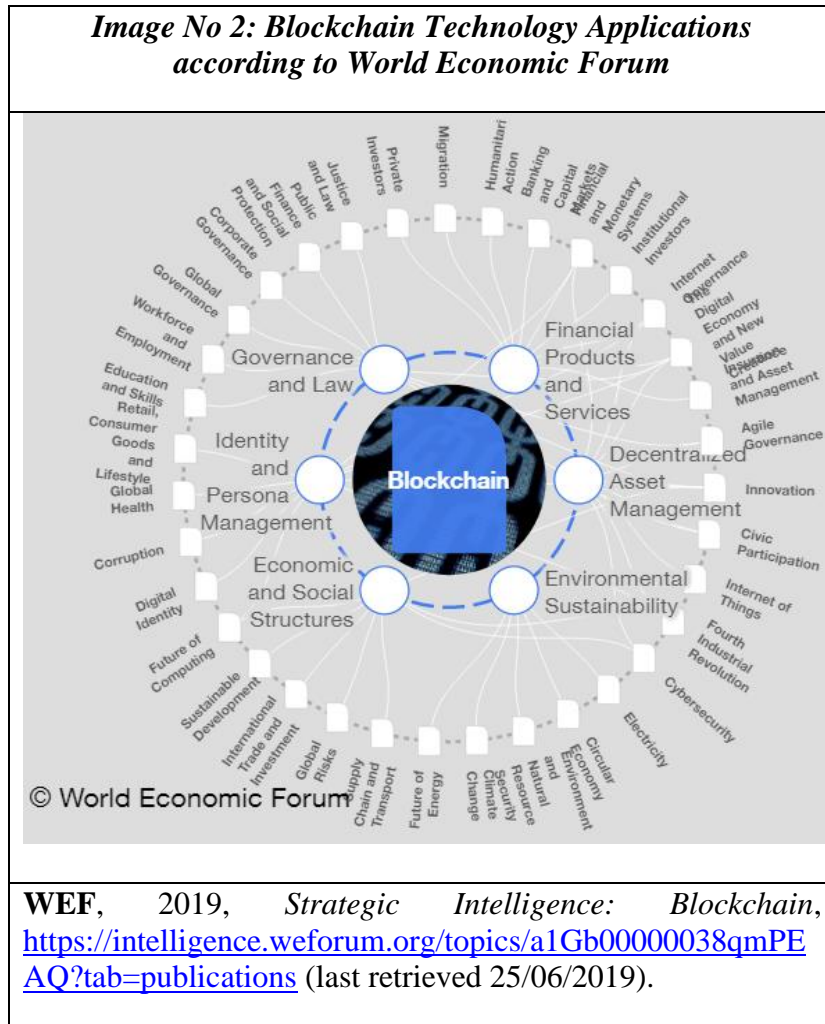
Taking under consideration the whole philosophy and nature of blockchain and its more forward application like crypto-currencies we can understand their impact and applicability in modern business model and environment. It is not by coincidence that World Economic Forum had recognized more than 30 economic and social sectors, where blockchain technology applications can advance, even thrive: from energy and utilities sector, supply chain, retail and transportation to finance, banking, investing, institutional, insurance even climate change and civic participation as the Image No 2 below demonstrates.

Especially as it concerns the accounting and auditing sector, blockchain can bring numerous benefits, among the ones mentioned previously: (a) *time-effective accounts due diligence*: data in blockchain can be verified and approved much faster and accurate both from entity's managers and other counterparts (like third-party suppliers, internal auditors,

⁸⁷ Private initiatives and interest groups have an analogous approach in this matter, but the controversy remains. For example, the *Chamber of Digital Commerce* (CDC), an USA advocacy pro-blockchain trade group that represents blockchain industry and its Digital Assets Accounting Coalition (DAAC), attempt to clarify the situation about accounting and regulating digital currency issues, like adequate recognition, measurement, bookkeeping and disclosure and develop relevant accounting and reporting standards for digital assets, in accordance with existed accounting standards like GAAP. Moreover, they try to collaborate with authorities and institution that set relevant standard, such as the Financial Accounting Standards Board (FASB) and the American Institute of CPAs. According to CDC, digital currencies can be treated withing the following FASB's Accounting Standards Codification (ASC): ASC 305 on Cash and Cash Equivalents, or ASC 825 on Financial Instruments, or ASC 350 on Intangible Assets – Goodwill and Other, or ASC 330 on Inventory. **Prestigiacomio Lorenzo** (October 2017), *What Is The "GAAP" In Regard To Digital Currency?*, Mazars-USA, <https://mazarsusa.com/ledger/what-is-the-gaap-in-regard-to-digital-currency/> (last retrieved 25/06/2019).

Cyber-security and Cyber-preparedness as a Necessary Part of the Auditing Process

external auditors, responsible authorities, etc.) in real time· (b) *easier reporting process*, internal and external auditing reporting is now much easier to be conducted (in monthly, quarter, semester and annual basis), since automatic results in actual streamline audit tests can be verified and soon after any transaction is being completed, making periodic closing and its reporting an easier task· (c) *increased accuracy in revenue recognition and less*



correcting errors, smart contracts and blockchain aid at making revenue resources more apparent and errors more noticeable and prone to correction· (d) *in real time automatic identification and classification of net assets*, that reduces time-effort and resources allocation for communication, classification, recognition, analysis, interpretation and reporting of net assets· (e) *effective and reliable evidence and data automatic collection*,

sampling, confirmation and updating in real time, between auditors, internal and external, the client entity, entity’s external providers as it concerns major accounts, like payments, receivables, payables, loans/leasing, inventory, assets, account balances, etc· (f) *efficient recalculation and reperformance of auditing tests*, in case is needed, which raise the level of accounts accuracy verification to its maximum. In general times, blockchain technology can revolutionized the accounting and auditing profession by offering continuous, rapid and technology reliant and almost 100% validated auditing and evaluation capacities to the professionals and aids in the minimization of errors, misconducts, defaults and external cyber-threats. That is why, auditors, internal and external, must cooperate closely with the entity’s board of managers, not only because they are responsible about any decision

concerning the use of blockchain or not, but also because lack of proper knowledge or misconception about the benefits, costs and risks of blockchain technology, as any other technology, emerged and older one, can have a significant impact on the truthfulness of financial statements, thus and to the processes auditors must conduct on them.

Despite the fact that blockchain technology had been developed with the security concern as priority, though as every technological tool is accompanied by its own inherent risks. Is not only that its encryption capacities can be hacked and receive malicious attacks, but also its immutability perception, meaning the safe storage of data on public ledger deposits without the risk to be compromised, can be both tempered, corrupted and manipulated. Additional to market and financial implications and threats, like (a) investors protection due to price volatility, bubble risks, secondary trading, conflicts of interest, frauds, etc., (b) market integrity and efficiency, financial crime, terrorist funding, tax evasion, money laundering and speculation concerns, (c) financial stability and markets decentralization, (d) lack of harmonized relevant standards, due to the economic nature of this technology, the major pure cybersecurity risk from blockchain are of two types: (i) the first type if referring to the risks derailing from the technological nature of blockchain and crypto-assets, such as (1) *private/encrypted and public key theft*, since hackers can steal the encryption keys in order to succeed achieving fraudulent and illegal transactions, withdrawals and embezzlements, (2) *anonymity concerns*, especially in case of a public blockchain and ledger, that can make identification attempts extremely difficult, (3) *cybercriminals consensus to perform malicious attacks*, that will benefit only the cybercriminals interests, Crypto-assets mining attacks orchestrated by hackers in order to illegally obtain cryptocurrency and other funds from blockchain systems is a paradigm of that category. Financial crime increase due to crypto-currencies mining and illegal selling of an entity's cryptoasset demands more focus by boards and auditors, (4) *physical security blockchain risks*, concerning undistracted electricity and air-cooling supply, physical protection of hardware, etc., (5) *secure data management, assessment and storage* of blockchain applications. (ii) The second type refers to standard cybersecurity and management demands and practice risks, such as (1) *vulnerabilities due to false and insufficient development, usage, maintenance poor performance* of blockchain NHS systems, (2) *access concerns by unauthorized people* to sensitive blockchain data, like encrypted keys and software, (c3) *identity and privacy issues and misconducts of personalized data*, that can lead to identity and personalization thefts, as we described them

in vulnerability No 6, (4) *business continuity and disaster recovery* concerns in case of enlarged scale attack(s).

III] 3. 11. B) Electronic commerce or e-commerce and e-governance

The abundance in technological advancements together with multi-national manufacturing and retailing demands and the demand of state operations modernization had help in the emerge of both the electronic or online transactions or e-commerce and the e-governance. Moreover, the appearance of e-banks, mobile and web payments and banking, web information of the citizens according to relevant constitutional principles gave to all types and sizes of entities and institutions (private and public) new universes of functionality, since nowadays entities can exist in selling all types of goods (from material products and services to intellectual property goods, like films, video games, etc.), survive even thrive through only web worlds, such as Amazon, Netflix, social media like Facebook, Twitter, etc. This evolvement in doing business had enlarge the necessity to implement strict laws concerning That is why, the new realities of e-signatures, e-contracts and consumers protection right in e-commerce transactions of this trade area had created the prerequisite of its strict regulation not only with national laws but also with international multilateral agreement, such as the *United Nations Convention on the Use of Electronic Communications in International Contracts of 2005*, the *United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce* (of 1996) and the *UNCITRAL's Model Law on Electronic Signature* (of 2001), *United Nations Guidelines on Consumer Protection* (of 2001) for best articulation of cross-borders electronic payments and transactions. European Union also had adopted already from 1999 relevant laws (*Directive 1999/93/EC on a Community Framework for Electronic Signatures*, which created the legal framework on how to perform e-signatures and certify services within and across European Union territory and 2014 *Regulation on Electronic Identification and Trust Services for Electronic Transactions*).⁸⁸

⁸⁸ **United Nations Conference on Trade and Development: Trade and Development Board Investment, Enterprise and Development Commission** (2015), *Cyberlaws and regulations for enhancing e-commerce: Case studies and lessons learned*, UNCTAD, https://unctad.org/meetings/en/SessionalDocuments/ciem5d2_en.pdf (last retrieved 25/06/2019).

III] 3. 11. C) Artificial Intelligence

Artificial intelligence (or AI) is the process when technology (like a computer or a computer-controlled robot and machines in general) controlled by another technology, like a computer, to be able to learn and perform tasks in the intellectual ways humans do, such as reasoning, ability to learn through experience, to memorize, to determine meaning and significance and to make generalizations. In order to achieve a reliable level of artificial intelligence we need the cooperation of other emerging technologies, like (a) **machine learning**, which is the method that trains a computer, robot and any other capable device, to learn from input information without having to be programmed for every single circumstance and situation, (b) **natural language processing** (or NLP), which as a part of artificial intelligence aids computers to better comprehend, analyze, process, interpret, interact and manipulate natural (human) language in order to transform human linguistics into computational linguistics and (c) **robotic process automatization** (or RPA), is the process and the software in which robots and the machines learn to automatically work and execute artificial intelligence applications.⁸⁹ AI and its components had helped in the technological evolvement of modern business for at least 20 years, that drive entities from all sectors and sizes even to create their own AI-systems.⁹⁰ AI cost-effectiveness, added-value and transformative nature and its ability to be connected with other technological advancements, like 3D/4D printing, IoT, blockchain technology, quantum computing, and many other, constituted AI a unique tool for every business, organization, institution and authority of private and public sector, like industrial/manufacturing, automotive, engineering, finance, banking and auditing, retailing and distribution, electricity and grids, educational and remote working, healthcare and medicine, assist money anti-laundering attempts, to many other. Unfortunately, the same benefits of AI that entities use, like speed, problem solving, ability to process effectively and target-oriented huge data flows, enhance distance monitoring, human-to-computer and computer-to computer interaction, minimize

⁸⁹ **Encyclopedia Britannica** (2019), *Artificial intelligence*, <https://www.britannica.com/technology/artificial-intelligence/Reasoning> (last retrieved 25/06/2019). **Dickey Gabe, Blanke Sandra and Seaton Lloyd** (June 2019), *Machine Learning in Auditing: Current and Future Applications*, <https://www.cpajournal.com/2019/06/19/machine-learning-in-auditing/> (last retrieved 25/06/2019). **Vasarhelyi Miklos A. and Rozario Andrea M. (June 2018)**, *How Robotic Process Automation Is Transforming Accounting and Auditing*, CPA Journal, <https://www.cpajournal.com/2018/07/02/how-robotic-process-automation-is-transforming-accounting-and-auditing/> (last retrieved 25/06/2019).

⁹⁰ For example, JP Morgan's had created an AI software system that uses machine learning in order to check the legitimacy, litigation and reliance of financial deal contacts, saving 360,000 of lawyers working hours, called COntract INtelligence AI system (or COIN). **Son Hugh** (28/02/2017), *JPMorgan software does in seconds what took lawyers 360,000 hours*, <https://www.independent.co.uk/news/business/news/jp-morgan-software-lawyers-coin-contract-intelligence-parsing-financial-deals-seconds-legal-working-a7603256.html> (last retrieved 25/06/2019).

resources allocation and use, minimize human fatigue, automatization of the work load, duties and performances, monitor activities and transactions, etc., the same benefits can be used by hackers and cybercriminals in order to provoke major cybersecurity attacks to an entity's NHS systems. What is amazing in the particular case of AI and its applications is their dual (self-contradictory) applicability, meaning they can simultaneously be used as the first line of attack in order to provoke malicious attacks and behaviors by cyber-criminals, but at the same time they can function as the first line of defense from entities and auditors in order to spot and neutralize these attacks. As much as a tool for managers and auditors, AI and its applications can be not only an aid regarding the discovering, decreasing, monitoring and mitigation risks, but also an inherent risk that these technological choices possess on their own, apart from being a weapon of penetration and disruption to the hands of cybercriminals and hackers. Risks, like (a) increased bias due to algorithmic pre-existing or intentional bias targeting programming, (b) overrating and over-appreciation of the capacities of AI systems and applications, especially if the original training data are of poor quality, inadequate and erroneous, (c) misleading outcomes and poor performances due to misappropriations and problematic programming, (d) legal compliance and normative misconduct, especially as it concerns data acquisition, analyzation and protection regulations, and (e) reputation and hacking incidence disclosure risks from bad performing AI applications for the entities developing and using these AI applications, must be under the constant risk assessment and mitigation eye of an effective managing team and the auditors (internal and external).⁹¹

⁹¹ **Boillet Jeanne** (01/04/2018), *Why AI is both a risk and a way to manage risk*, https://www.ey.com/en_us/assurance/why-ai-is-both-a-risk-and-a-way-to-manage-risk (last retrieved 25/06/2019). Prof. **Klous Sander** (08/06/2018), *In AI we trust?: Assurance is more important than ever in the age of machines*, KPMG, <https://home.kpmg/xx/en/home/insights/2019/04/in-ai-we-trust.html> (last retrieved 25/06/2019). **Kokina Julia and Davenport Thomas H.** (2017), *The Emergence of Artificial Intelligence: How Automation Is Changing Auditing*, American Accounting Association: Journal of Emerging Technologies in Accounting, Volume 14, Issue 1, available at <https://meridian.allenpress.com/jeta/article-abstract/14/1/115/116001/The-Emergence-of-Artificial-Intelligence-How?redirectedFrom=fulltext> (last retrieved 25/06/2019). **Brennan Bill, Baccala Mike, and Flynn Mike** (02/02/2017), *Artificial Intelligence Comes to Financial Statement Audits*, CFO online, <https://www.cfo.com/auditing/2017/02/artificial-intelligence-audits/> (last retrieved 25/06/2019). **Issa Hussein, Sun Ting, and Vasarhelyi Miklos** (2016), *Research Ideas for Artificial Intelligence in Auditing, The Formalization of Audit and Workforce Supplementation*, American Accounting Association: Journal of Emerging Technologies in Accounting, Volume 13, Issue 2, available at <https://meridian.allenpress.com/jeta/article/13/2/1/115980/Research-Ideas-for-Artificial-Intelligence-in> (last retrieved 25/06/2019).

III] 3. 11. D) Internet of Things (or IoT)

The technology of IoT is referring to embedded software that permits interaction, processing and sharing of information between internet connected networks and devices with or without human involvement. IoT has, due to devices like wearables, tablets, smartphones, activity trackers, smart home, smart cities and smart grids, appliances, geospatial, environmental sensors and distance monitoring technologies, a great variance of application in modern business worlds: in industrial and manufacturing procedures, in healthcare, medical and insurance sector, in agricultural sector, in automobile sector with autonomous and self-driven cars, in electricity production, grid/utilities and energy sector, etc. We can distinguish the risks derailing from this method in three major categories: (a) *business risks*: like data and users' privacy, compliance with relevant regulations, costs for adopting the technology, interruption of an entity's cycle of service and business due to an attack or malfunction in IoT systems, etc., (b) *operational risks*: like poor performance due to lack of adequate preparation by the personnel, functionality problems due to access to IoT systems by unauthorized or unverified individual(s), etc. and (c) *technical risks*, that had to do mostly with the IoT devices and their vulnerabilities (due to bad usage, or how easy is to be hacked, or to be targets of an DDoS attack, or to be destroyed due to an energy shortage or a hacking attack to energy and cooling systems, etc.), lack or improper updating, mismanagement, certain lifespan and effectiveness, low level of physical security, lack of sufficient level of security and interface between connected devices and software like cloud, mobile, network, web/online, etc.⁹²

III] 3. 11. E) Cloud Services and Software as a Service (SaaS)

Many times, in this paper we set as a trustworthy solution the outsourcing of an entity's data to external storage service providers. Cloud, data centers solutions services and other Infrastructure as a Service (IaaS) solutions, and software (such as antivirus and firewalls) solutions in the form of external service had gain quite popularity among the modern economic world for a variety of reasons: (a) external providers' advantage and

⁹² **Cooke Ian and Raghu R. V.** (01/09/2018), *IS Audit Basics: Auditing the IoT*, ISACA Journal, Issue 2018: Volume 5, <https://www.isaca.org/resources/isaca-journal/issues/2018/volume-5/is-audit-basics-auditing-the-iot> (last retrieved 25/06/2019). **Protiviti** (2016), *The Internet of Things: What is It and What Should Internal Audit Care?*, https://www.protiviti.com/sites/default/files/united_states/insights/internal-audit-and-the-internet-of-things-whitepaper-protiviti.pdf (last retrieved 25/06/2019). **Salman Syed** (29/10/2015), *Auditing the Internet of Things: The rise of Internet-connected devices and systems bring both new opportunities and risk for modern organizations*, Institute of Internal Auditors, <https://iaonline.theiia.org/2015/auditing-the-internet-of-things> (last retrieved 25/06/2019).

deeper knowledge, experience and effectiveness on the theme, (b) cheaper solution that create an inside department and hire the needed personnel, (c) share of risks, since the belonging of the risk is distributed to more players than the single one entity, (d) ability to hire more than one storing solutions, something that decrease the potentiality of total loss of all data in case of a single storage solution policy, etc. Despite these positive aspects, there is always the drawback of transferring a great deal of performing technologies and controls in sensitive data to an another outside entity, so any cyber-breach and misconduct in this entity's NHS systems is exposing their clients data too. In general terms, that is the biggest danger concerning every third-party IT outsourcing activity. That is why, is of the outmost importance the decision-making process of an entity to use external parties IT capacities must governs not only by the level of the expense but also of their expertise and their commitment to follow the standards and frameworks exist for this sectors. Most advanced related standards in this domain are, ISACA (Information Systems Audit and Control Association)'s *Information Technology Assurance Framework (or ITAF)* and more precisely 3630.3 IT Service Delivery and 3630.5 Outsourced and Third-party IT Activities, *ISACA's COBIT* (Control Objectives for Information and Related Technologies), *ISACA's IT Audit and Assurance Guidelines* (formerly IS Audit Guidelines) and *ISO's 27000 Family of Standards*, that we are going to examine in the next section of this Master Thesis. Some of them can be applied also for internal data storage solutions and consequently for the internal IT data storage auditing trails.⁹³

III] 3. 12 Outdated Technology Vulnerabilities

Apart the above-mentioned major categories of more advanced and highly sophisticated technologies, cyber-risks that entities face, and auditors must take under serious consideration, can occur due to outdated technological choices and realities of an entity. This kind of cybersecurity dangers can occur when the NHS systems of an entity are relatively old and ineffective due to entity's reluctance, lack of knowledge of the danger outdated technologies may impose to an entity survival and lack of the acquired resources to make the needed shift to more advanced technological capacities. If these outdated NHS systems are exposed to the malicious behavior and coding of cyber-criminals, then significant damage can be provoked to an entity valuable assets: from loss in sensitive and

⁹³ Singleton Tommie W (01/05/2010), *IT Audits of Cloud and SaaS*, ISACA Journal, <https://www.isaca.org/resources/isaca-journal/past-issues/2010/it-audits-of-cloud-and-saas> (last retrieved 25/06/2019).

material information and loss of patents formulas or intellectual property rights content to permanent destruction of NHS systems functionality.

Entities Internal Controls Response: entities must not be afraid to skip modern, updated and more protective technologies and applications. Doing so, means: (a) better involvement of Board of Directors and other top executives in planning and installing the new technologies where they are needed, (b) sufficient training and capacity building of the personnel to treat effectively new technologies, (c) if skipping to new technologies if not possible, due to cost considerations usually and to staffs reluctance and lack of proper knowledge, at least proper maintenance activities to be conducted regularly to the old ones, that are in use, (d) the company to acquire and insurance, that will protect the entity for cyber-attacks. Usually the cost of insurance in this case is quite high, but not that high that the change-over situation.

III] 3. 13 Conclusions on Cybersecurity Risks and Entities' Internal Controls

In this part of this Chapter we focus our attention on the examination of the most crucial, demanding further action and destructive cybersecurity risks that entities, institutions and organizations face in daily scale and auditors must administrate during their controls' performances. These risks can be categorized in two types: (a) the first type is synonymous to malicious behavior *per se* (inside an entity and outside entity), and we can identify them as authentic cybersecurity risks, and the target from their conduction is to provoke negative impacts to an entity's well-being and long-lastingness: malicious code and programs, harmful malwares, social engineering and phishing, denial of service attacks, ransomware, CEO/CFO scams or whaling and identity thefts, intellectual property cyber-thefts and industrial cyberespionage and (b) the other type includes cybersecurity related vulnerabilities that are not cyber-dangerous *per se*, but in the hands of malicious and unauthorized individuals, not well-trained or malicious employees and stakeholders and of course rivals can be equally catastrophic as the malicious *per se*: keylogger, financial information disclosure and use of social media vulnerabilities, supply chain vulnerabilities, vulnerabilities due to emerging technologies, like blockchain, smart contracts, crypto-assets, electronic commerce or e-commerce, e-governance, artificial intelligence, internet of things, cloud services, software as a service and outdated technology vulnerabilities. Due to the complexity of this cybersecurity risks and vulnerabilities, audit profession is becoming extremely demanding, difficult, dense and multi-factorized, especially in a working reality

where one hundred percent immunity from cybersecurity threats is neither in current terms nor in future ones possible. Moreover, the dual nature of these threats, meaning that is not only entities that can be victims of them, but also auditors themselves can experience cyber-related dangers, for example a hacking breach in an auditing firm can expose to malicious actors sensitive data and the secrets of their clients, constitute cybersecurity knowledge and receiving the right protective measures from auditors a real necessity. This fact signifies that the development and adoption of proper cybersecurity preparedness legal frameworks, standards, best practices, etc., is a pure necessity in order to provide a cybersecurity shield of protection to modern business, including auditing firms. Auditors, internal and external, must not only obtain a deep knowledge of these protective mechanisms, but also correlate them in the most effective way with the above-mentioned both types of cybersecurity threats in order first to plan, construct, execute and disseminate a functional audit controls trail and second to propose the most adequate, applicable and reliable solutions to their client entity. The next part of this Chapter focuses exactly in the examination of the most important regulatory frameworks and standards related to cybersecurity and cyber-preparedness, that had been developed until so far by states (we will examine the case of United Kingdom and United States of America) and the European Union.

III] 4. Understanding an Entity's Operational Environment and Presentation of the Most Important Cybersecurity Compliance Frameworks (National and European)

Understanding an entity's operational environment is a key component according to *ISA 315 on Understanding the Entity and its Environment and Assessing the Risks of Material Misstatement*. This operational environment is shaped by the measurement of elements, like (a) the *type of the entity*, meaning private, public, mix type, non-governmental and charitable, (b) the *size of the entity*, that can be extend from small and medium size entities (or SME), to large conglomerations that can be enlisted to stock markets and multi-nationals that compliance with specific national and international financial reporting regulations is mandatory, (c) *the industry or sector* or multi-sectors they function, based upon the goods and services or their combination they produce and (d) the *obligation of*

applying internal controls and producing specific financial information in the form of appropriate and with no mistakes financial statements according to specific laws and regulations. Auditors must have a concrete understanding and evaluation of these elements and especially of the legal and regulatory compliance requirement due to the fact that non-compliance may result not only regulatory penalties but also to cost the survival and failure of the examined client entity. *ISA 250 on Consideration of Laws and Regulations in an Audit of Financial Statements* provides specific guidance on how auditors must proceed in the examination of an entity's regulatory framework and the importance of taking under consideration legal and regulatory concerns during their audit trail in financial statements.⁹⁴ In this section of this Chapter, we will examine the cybersecurity regulatory environment, firstly in national level with the examination of the cases of United Kingdom and United States of America and secondly in European Union's (EU) level, since EU regulations have a significant impact in international regulatory systems concerning data security and entities cybersecurity operations and performances.

III] 4. 1. National Level

III] 4. 1. A) Great Britain

United Kingdom's national cybersecurity related legal framework is almost thirty years old, since the *Computer Misuse Act (CMA)* was adopted in 1990. CMA (and its amendments) aims to protect stored by organizations and entities personal data from misuse due to unauthorized access and modifications, by imposing penalties that range from heavy fines to even imprisonment for failing to comply with CMA entities. CMA recognizes the following computer misuse offences: (a) *unauthorized access to computer material*: like hacking and any other without permission enter in computer systems case, (b) *unauthorized access to computer materials with intent to commit or facilitate commission of further offences*: that refers to any malicious activity gained by unauthorized access, such as the attempt to enter in a computer system with the aim to steal data, plant a virus or destroy NHS systems, (c) *unauthorized acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.*: which include malicious behaviors like unauthorized

⁹⁴ **IFAC** (2010), *International Standard On Auditing 250 on Consideration of Laws and Regulations in an Audit of Financial Statements*, <https://www.ifac.org/system/files/downloads/a013-2010-iaasb-handbook-isa-250.pdf> (last retrieved 25/06/2019).

data modifications or (permanent) data loss and delete, cases of electronic vandalism with the introduction of malwares, spywares and other malicious software as those we examined in the previous section of this Chapter, data thefts, etc., (d) *unauthorized acts causing, or creating risk of serious damage*, when damage must be of “material kind” and affect human welfare⁹⁵, environment, economy, and national security and (e) *making, supplying or obtaining articles and anything that can be used in the above mentioned computer misuse offence cases*.⁹⁶ Data integrity and protection for personal and customers use, gathered, and used by organizations and government institutions are regulated by **Data Protection Act (DPA) 1998**. The most recent amendment in this Act took place in 2018 under the influence of EU’s General Data Protection Regulation requirements.⁹⁷ The **Information Commissioner’s Office** is the country’s independent authority with its mandate to be: (a) to defend public interest information related rights, (b) to protect data privacy for citizens and individuals, (c) to promote more openness by public institutions, and (d) to realize the provisions of Data Protection Act 2018 (DPA) and Freedom of Information Act 2000 (FOIA).⁹⁸

Sector provisions with auditing compliance importance about cybersecurity concerns identification and data protection and privacy protection of telecommunication sector, contain **The Telecommunications (Data Protection and Privacy) Regulations 1999** (and its amendments)⁹⁹ as well as **The Privacy and Electronic Communications (EC Directive) Regulations 2003**, created in order to comply with EU relevant laws initiated with Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.¹⁰⁰ Furthermore, additional sectoral guidance concerning specific economic aspects that can be related to cybersecurity threats and must be taken into account by auditors during compliance performance audit trail offers the **Financial Conduct Authority (FCA)**

⁹⁵ A definition that covers damages that range from a human loss to human illness or injury, to disruption of human made infrastructure, such as the system of communication, transportation, health related services and service providing like supply of money, food, water energy and fuels. (Article 3ZA of CMA).

⁹⁶ **UK Legislation National Archives**, *UK Public General Acts: Computer Misuse Act 1990*, <https://www.legislation.gov.uk/ukpga/1990/18/contents> (last retrieved 25/06/2019).

⁹⁷ **GOV.UK** (2019), Data Protection, <https://www.gov.uk/data-protection> (last retrieved 25/06/2019). **UK Legislation National Archives**, *UK Public General Acts: Data Protection Act (DPA) 1998*, <http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted> (last retrieved 25/06/2019).

⁹⁸ **Information Commissioner’s Office** (2019), *Who we are?*, <https://ico.org.uk/about-the-ico/who-we-are/> (last retrieved 25/06/2019).

⁹⁹ **UK Legislation National Archives**, *UK Public General Acts: The Telecommunications (Data Protection and Privacy) Regulations 1999*, <http://www.legislation.gov.uk/uksi/1999/2093/contents/made> (last retrieved 25/06/2019).

¹⁰⁰ **UK Legislation National Archives**, *UK Public General Acts: The Privacy and Electronic Communications (EC Directive) Regulations 2003*, <http://www.legislation.gov.uk/uksi/2003/2426/contents/made> (last retrieved 25/06/2019).

Handbook for the regulation, supervision and standards implementation of financial entities and financial markets,¹⁰¹ and the **Bank of England's Prudential Regulatory Authority (PRA) Rulebook** for the regulation and supervision of capital firms (such as banks, building societies, and investment firms), solvency firms (such as insurance firms) etc.¹⁰²

Further cybersecurity concerns had been administered by national legislation in compliance with EU related legislative framework in order to facilitate among other the cybersecurity harmonized operability of European Economic Area, like the General Data Protection Regulation (also known by the acronym GDPR), as we examine previously, and the Network and Information Security Regulations 2018 (also known by the acronym NIS Regulations), that we are going to analyze further in other section of this Chapter. The process of (potential) exiting of UK from EU creates significant legislative and practical issues, as it concerns the existence and functionality of EU cybersecurity laws in UK's territory.

Since June 2014, the country's **National Cyber Security Centre** (NCSC - a government body) had developed together with the Information Assurance for Small and Medium Enterprises (IASME) consortium and the Information Security Forum (ISF) the **Cyber Essentials Scheme** in order to help organizations of any size, any sector and any type to protect themselves against the most common cyber threats and internet-based vulnerabilities that can occur in the online sphere and IT infrastructure. The Scheme is a national-wide cyber-security market-based standard that sets a framework about the right implementation of controls of technical type¹⁰³ and is non-obligatory for organizations, though is mandatory (from 1st of October 2014) for organizations with bidding contracts with Central Government that incorporate certain types of sensitive and personal data handling and so have to be certified withing the Cyber Essentials Scheme. There are two levels of certifications within the Scheme: (a) the Cyber Essentials: is a verified self-assessment tool that provides protection against the most basic cyber-threats (the cost is a fix amount £300 plus VAT) and (b) the Cyber Essentials Plus: that incorporates the approach of the Cyber Essentials but includes also the conduction of a hands-on technical verification.

¹⁰¹ FCA (2019), *FCA Handbook*, <https://www.handbook.fca.org.uk/handbook> (last retrieved 25/06/2019).

¹⁰² Bank of England's Prudential Regulatory Authority (2019), *Rulebook*, <http://www.prarulebook.co.uk> (last retrieved 25/06/2019).

¹⁰³ Such as a) the use of firewalls, anti-virus, anti-malware, whitelisting, sandboxing (a security software management policy that aims to prevent malicious malware attacks by restricting unauthorized access to critical applications, resources and programs) and other software in order to best secure an organization's online gateways, devices and networks, b) the application of the most effective and suitable cyber-security structures for hardware and software, c) the use of an adequate access control system such as the role-based access control (RBAC), which enables better level of security and control by restricting access to an organization's network according to the role and security allowance of the individuals and users of those networks and d) regular conduction of control checks and needed upgrades in hardware and software in order to be updated against the recent more advanced widespread cyber-threats.

The cost depends according to the size and the complexity of technologies and networks of the organization. Both levels of certification have a duration of twelve months period, after which an organization must get a new one. This certified cybersecurity badge system apart the obvious market benefits that bring to the organizations that obtain it, such as the offer of a fair view of an organization and the reassurance of its customers and other stakeholders about the level of cybersecurity within the organization, something that can attract new customers and contracts, especially if the organization works with UK's Government¹⁰⁴, can function also as a very good tool during cyber-preparedness auditing controls and inspections in at least three ways: the first one is, that the certification itself can function as a type of evidence among those collected during cyber-related auditing performance checks. the second one is, that for cases that its acquisition is obligatory (legal obligation) and there is no any evidence that the organization had acquired it or is the process to do so, then auditors must raise a red flag that must be incorporated in auditing reports as it concerns the lack of legally obliged document and the third one, has to do with the cases of failing to obtain the certificate. In the event of an organizations failure to receive the certification, the Certification Body (the recognized authority that accredit other organizations with the Cyber Essentials badge) provides a feedback about the cyber domains that must be improved within the organization in order to be better eligible to gain a Cyber Essentials certification. This can function for (internal and external) auditors as an identification of problematic areas as it concerns cyber-security within an organization, that auditors must give special attention during their auditing controls and their reporting.

Auditors must also take under serious consideration during their reporting any incident reported to the **Action Fraud** reporting line of the **National Fraud & Cyber Crime Reporting Centre** in which organizations (like large corporations, financial institutions, charities even individuals) can report any cyber-attack to their hardware and software and cyber-crimes, such as hacking incidents, account compromise occurrences and internet extortion cases. Action Fraud reports the incidents to **National Fraud Intelligence Bureau** (NFIB) for additional analysis and assessment. The NFIB can redirect the entities to relevant

¹⁰⁴ The information about the Cyber Essentials Scheme are collected from the following sources: 1) **GOV.UK**, 16/01/2018, *Guidance - Cyber Essentials Scheme: overview*, <https://www.gov.uk/government/publications/cyber-essentials-scheme-overview> (last retrieved 25/06/2019). 2) **National Cyber Security Centre**, 2019, *About Cyber Essentials*, <https://www.ncsc.gov.uk/cyberessentials/overview> (last retrieved 25/06/2019). 3) **Cyber Essentials**, 2019, *Cyber Essentials*, <https://www.cyberessentials.ncsc.gov.uk> (last retrieved 25/06/2019).

police authorities for further action and investigation.¹⁰⁵ So, auditors must have under their radar the fate of those reports, especially if law enforcement authorities are involved, due to the fact that perhaps they must incorporate in their cyber-auditing reports the expense, the vulnerability and the fame costs they might have on organizations.

Last but not least, we must mention that the country had developed a very useful best practices framework, entitled *Information Technology Infrastructure Library* (or ITIL), that provides a set of detailed procedures, practices, tasks, checklists, etc., concerning IT Service Management (ITSM) planning, implementation and evaluation with fulfilling business objectives and needs to be the primary goal of ITIL. ITIL had been established by UK Government's Central Computer and Telecommunications Agency (CCTA) in the 1980s as a set of recommendations intended to systematize IT management practices throughout government functions. After the merging (April 2001) of CCTA into the UK's Office of Government Commerce (OGC), an office of the UK's Treasury and the integration of OGC into the Cabinet Office (in 2011), OGC is no longer the owner of ITIL. AXELOS, a joint venture between the Cabinet Office and Capita, a former division of the non-profit organization CIPFA (Chartered Institute of Public Finance and Accountancy), but from 1991 an listed to London's Stock Exchange company, provides to organizations licenses to use the ITIL framework, relevant accreditations to examination institutes, and updates the ITIL, that is from February 2019 in its fourth edition. Nowadays, millions of IT and digital services professionals use ITIL and core businesses are build based on ITIL, since ITIL offers a professionally recognized certification system and guidance for applying an inclusive, cost-effective, real-world and verified IT service management framework, that empowers entity's management risk capacities, accelerates business change, ensures information security, provides proper evaluation and reporting, and promulgates digital transformation and development.¹⁰⁶

¹⁰⁵ **Action Fraud** (2019), *What is Action Fraud?*, <https://www.actionfraud.police.uk/what-is-action-fraud> (last retrieved 25/06/2019). **Action Fraud** (2019), *Who reports fraud to us*, <https://www.actionfraud.police.uk/who-reports-fraud-to-us> (last retrieved 25/06/2019).

¹⁰⁶ **Axelos** (2019), *What is ITIL?*, <https://www.axelos.com/best-practice-solutions/itil/what-is-itil> (last retrieved 25/06/2019). **White Sarah K. and Greiner Lynn** (18/01/2019), *What is ITIL? Your guide to the IT Infrastructure Library*, CIO, <https://www.cio.com/article/2439501/infrastructure-it-infrastructure-library-itil-definition-and-solutions.html> (last retrieved 25/06/2019).

IV] 4. 1. B) UNITED STATES OF AMERICA

United States of America are considered the role model for many technological advancements, so cybersecurity could not escape from that pattern of recognition. In the following pages we will present the institutional and legal framework as it concerns the regulation of auditing related cybersecurity concerns. In the previous section of this Chapter we mentioned the impact of ***Gramm-Leach-Bliley Act*** (GLB Act or GLBA or Financial Modernization Act), on demanding from financial institutions to provide an explanation on how they protect and share with the public their clients private and sensitive data. GLB Act establishes: (a) an information security framework concerning the protection of clients' information, (b) a security policy strategy, that aims to address important issues, such as access controls, exchange controls, encryption application considerations and monitoring and incident response matters. The applied security policy must be constantly evaluated as it concerns its ability to spot, identify and deal with internal and external business threats and especially those threats related to proper handling of customers' data. That is why, a Risk Assessment Information Security and Configuration Management program must be set in place by management, that among the above-mentioned functions, must perform adequate access control, real-time and auditing monitoring. GLB Act demands also from covered by this law entities to have adequate systems of data and security breaches reporting and security applications, devices and networks auditing capacities. In the following pages we will examine the additional to GLBA relevant to cybersecurity legal documents and institutions that the country had established and have a significant impact in auditing services.

Following the financial fraud scandals on Enron, WorldCom, and Tyco , Senator Paul Sarbanes and Representative Michael Oxley drafted, proposed and passed the ***Sarbanes-Oxley Act (also best known as SOX) of 2002***¹⁰⁷ in order to protect shareholders and the public from financial and accounting frauds, financial statements errors and fraudulent behaviors and practices by publicly-traded (listed) entities, registered public accounting firms and any other securities related entity¹⁰⁸, supervised by Securities and

¹⁰⁷ Also known as the "Public Company Accounting Reform and Investor Protection Act" and the "Corporate and Auditing Accountability and Responsibility Act".

¹⁰⁸ More precisely, SOX applicability is extended to certain foreign firms, such as "*Any foreign public accounting firm that prepares or furnishes an audit report with respect to any issuer, broker, or dealer, shall be subject to this Act and the rules of the Board and the Commission issued under this Act, in the same manner and to the same extent as a public accounting firm that is organized and operates under the laws of the United States or any State*". **Congress** (2002), *Public Law No: 107-204 (07/30/2002)- 107th Congress (2001-2002)*:

Exchange Commission (SEC). Among the aims of SOX is to strengthen corporate governance, to enhance proper accountability according to relevant standards and minimize gaps and loopholes in accounting principles and practices, to promote an auditing mentality with internal controls application and to establish auditing committees in the covered by SOX entities, to empower whistle-blower principles, to reinforce compliance monitoring, and to increase the entities' transparency, reporting and disclosure accuracy and performance by imposing severe penalties for both corporates and executives. SOX also established the Public Company Accounting Oversight Board (PCAOB) as the auditing profession supervising body. SOX text does not provide any direct norm as it concerns cybersecurity and cybersecurity internal controls, so in general terms we can find relevant provisions in the following sections:

(a) *Section 302 - Corporate Responsibility For Financial Reports*: which sets the general corporate responsibility for providing accurate and correct financial statements and the responsibility of principal executive officer or officers and the principal financial officer or officers, or any other person that perform similar functions, to have established, maintain and evaluate a system of internal controls that permits to management, the auditing committee and auditors to have a fair representation on entities financial capacities in order to avoid frauds and misstatements in entity's financial reports. The financial statement signing officers, such as those mentioned previously and mainly referring to CEOs and CFOs, must disclose and reveal to auditing committee and auditors any deficiency or weakness on the designed and implemented internal controls and any fraud irrelevant if it is of material kind or not that involves the management or any other member of personnel, since those can have a severe impact in internal controls functionality and proper recording, assessing and reporting capacities resulting to poor-quality or fraudulent statements of financial data. Moreover, it obliges the management signing officers to disclose in their reports any significant change in internal controls landscape that can have an important impact in the proper functionality of internal controls, additionally to include any corrective activity with the aim to control and minimize these significant deficiencies and material weaknesses. Section 302 allows to consider that among these internal controls can be also all these mechanisms and procedures that protect an entity from cybersecurity threats, such as data breaches and losses, unauthorized access and transaction happening due to malicious malwares and human behaviors, due to external actors like hackers or internal personnel's fraudulent or erratic performance, etc., and

(b) *Section 404 - Management Assessment of Internal Controls*: which indicates the responsibility of management not only to establish and maintain an adequate level of effective internal controls and procedures, but also to assess these internal controls with the aim to produce an internal controls report, that will be reviewed by an external third party auditing firm. the results of this assessments will for quality financial reporting. In cybersecurity context, Section 404, obliges entities not only to have cybersecurity related internal controls, such as those concerning data handling and privacy, NHS security, authorized physical and logical access, etc., but also to assess these internal controls and disclosure them to external auditors for their auditing evaluation.¹⁰⁹

The modern advancements in evaluating enterprise risk management (ERM)¹¹⁰ that include the cybersecurity dimension and the wide number and range of cybersecurity threats, such as the cyber-attacks and cybersecurity related vulnerabilities we described in previous section of this Chapter, constitute the enrichment of SOX compliance framework in order to best deal with cybersecurity concerns and risks a pure necessity. That is why, in 2016 a proposed Bill called *Cybersecurity Systems and Risks Reporting Act* was introduced with the aim to amend SOX in order to extend its application to cybersecurity systems and cybersecurity systems officers that under the proposed Act must comply with the same obligations SOX had created for corporate responsibility as it concerns creating financial reports and for management as it concerns assessment of internal controls structures and procedures for financial reporting for all these entities and companies publicly traded and are oversighted by SEC. The Bill introduces the definition of three very important cybersecurity definitions: (a) the definition of cybersecurity system, as a “*set of activities or state, involving people, processes, data or technology, whereby the protection of an information system of the issuer is secured from, or defended against, damage, unauthorized use or modification, misdirection, disruption or exploitation*”, (b) the definition of cybersecurity risk, as a “*means a significant vulnerability to, or a significant deficiency in, the security and defense activities of a cybersecurity system.*”, and (c) the definition of information system, as “*a set of activities, involving people, processes, data, or technology, which enable the issuer to obtain, generate, use, and communicate transactions and information to maintain accountability and measure and review the issuer’s performance or progress towards achievement of objectives*”. Moreover, the Bill amends SOX by adding (a) to Section 302 after the word “reports” the expression “and information systems”, (b) to

¹⁰⁹ Congress (2002), *Public Law No: 107-204 (07/30/2002)- 107th Congress (2001-2002): Sarbanes-Oxley Act Of 2002*, <https://www.congress.gov/bill/107th-congress/house-bill/3763/text> (last retrieved 25/06/2019).

¹¹⁰ Like the COSO-ERM, that we examined in page

Section 404 after the word “controls” the expression “and information systems”, and (c) to Section 407 after the word “expert” the expression “and cybersecurity systems experts”, which constitutes the use of qualified and experienced cybersecurity experts equal to the financial experts. In general terms, the Bill dynamically inserts the cybersecurity dimension in SOX requirements, and guidelines an entity’s Chief Security Officer (CSO) or/and Chief Technology Officer (CTO) to establish, assess and report an effective system of cybersecurity internal controls in IT and NHS systems, that must be included in the entity’s financial statements reporting. If the bill had passed it would have given the green light to SEC to establish rules and norms about the definition of cybersecurity experts and issue requirements about the entity (issuer of securities) to disclosure if the entity’s audit committee has at least one member identified as a cybersecurity expert and if not to provide the reasons why it does not have. Moreover, SEC has the right to review the entity’s (issuer) information systems and cybersecurity systems reports and statements. During arranging these reviews SEC must take under consideration entity’s cybersecurity risks disclosures.¹¹¹

Apart SOX and its amendments, there is a number of more specialized and sectoral legal documents (both Bill and Acts) in USA that can affect the entities regulatory compliance obligation and must be taken into account from auditors during their audit trails according to ISA 250. The most relevant are the following:

➤ ***Federal Information Security Modernization Act of 2014, also known as FISMA 2014 or FISMA Reform***: amends FISMA 2002 and its creation had been considered as necessary after a series of attacks to Governments information systems and agencies, so the need of updating the Federal governments cybersecurity capacities and policies had become a demanding further action issue. FISMA 2014 aims in the providing of a comprehensive and effective framework for (a) enhancing effectiveness and functionality of information security controls and government management to federal agencies and assets computing and information resources environment for better administrating information security risks and increasing national security capacities and (b) developing and overseeing the application of standards, tools, policies, guidelines, principles, processes, etc., concerning the creation, operability, and implementation of information security systems and commercially created information security products. Moreover, the Act: (i) codifies the ***Department of Homeland Security’s (DHS)*** role and authority in overseeing the implementation of obligatory information security policies for Federal Executive Branch agencies information systems, by providing among others technical support (on the agencies request) and most suitable

¹¹¹ **Congress** (26/04/2016), *Text: H.R.5069 — 114th Congress (2015-2016): Cybersecurity Systems and Risks Reporting Act*, <https://www.congress.gov/bill/114th-congress/house-bill/5069/text> (last retrieved 25/06/2019).

technologies utilization, enhances DHS role in supervising the compliance requirement of the overseen agencies with those policies, and establishes by law the *Federal Information Security Incident Center (FISIC)* within DHS¹¹². (ii) obliges Federal Executive Branch agencies to report major information security incidents, additionally to report data breaches to Congress, OMB, DHS, and the Comptroller General Office (GAO) when they occur and in annual basis, with reports must contain information about: (1) the threats, threat actors, vulnerabilities, and their impacts; (2) the risk assessments of systems that receive the threat before the incident and their situation and compliance identification during the major incident; (3) the activities concerning discovering, replying and remedying the incident; (4) the total number of incidents; and (5) providing a picture about the number of individuals affected by the incident, the types of data and information stolen and exposed, including personally identifiable information. (iii) revises and illuminates the Office of Management and Budget's (OMB) oversight mandate over federal agencies information security practices, especially as it concerns the notification of individuals in case of data breaches in federal agencies and promulgates the revision and simplification OMB A-130 incident reporting system, in order to eradicate unproductive and wasteful reporting, while enriching reporting conditions for major information security incidents. Section 3555 of FISMA 2014, demands from each Federal Agency to conduct an annual independent evaluation on the effectiveness and robustness its information security program, policies and practices by testing and assessing their security capacities of that agency to determine the effectiveness of such program and practices. This evaluation will be performed either from Inspector General of each Agency (appointed under the Inspector General Act of 1978) or by an independent external auditor, established by the Inspector General of the agency and for the Agencies that do not have an Inspector General they must use the services of an independent external auditor that will perform this annual evaluation.¹¹³

➤ ***Computer Fraud and Abuse Act of 1986 (or CFAA 1986)***: amended the existing national computer fraud law (known as 18 U.S.C. § 1030), which was incorporated in Comprehensive Crime Control Act of 1984 (known as CCCA of 1984 and provides an extension of the United States Secret Service's jurisdiction over credit card frauds and computer frauds) and criminalized additional to 18 U.S.C. § 1030 computer-

¹¹² United States Computer Emergency Readiness Team (or US-CERT) act as the country's FISIC US-CERT by analyzing and decreasing cyber-threats and cybersecurity related vulnerabilities, publishing data on cyber threat warning and notifications, and coordinating incident response actions. **US-CERT**, *United States Computer Emergency Readiness Team*, https://www.us-cert.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf (last retrieved 25/06/2019).

¹¹³ **Congress** (24/06/2014), *Text: S.2521 — 113th Congress (2013-2014), Public Law No: 113-283 (12/18/2014): Federal Information Security Modernization Act of 2014*, <https://www.congress.gov/bill/113th-congress/senate-bill/2521> (last retrieved 25/06/2019).

related actions, such as the distribution of malicious code, denial of service attacks, passwords trafficking, etc. CFAA and its amendments¹¹⁴ aims: (a) to prohibit unauthorized access or exceeding authorized access to computers, (b) to ensure that computer-related crimes and incidents receive proper and sufficient punishment, (c) to extend the concept of tort law, which allows to the claimant person who suffer a loss or being harmed such as emotional issues, financial losses, injuries even invasion of his/hers privacy to ask for a private civil remedy from the person that is considered liable for committing the tortious action. In reality, CFAA recognizes the following computer fraud and abuse activities and treats them with the mentioned below penalties:

- *accessing a computer for committing espionage* according to Espionage Act of 1917 with the aim to willfully disclosing or attempting to disclose, or willfully failing to return, classified information concerning national defense, foreign relations or atomic energy, that can be used to injure the national defense and security of the United States, or can be used in favor of a foreign nation to take an advantage over USA national defense secrets of a foreign nation [18 U.S.C. 1030(a)(1)], which results not more than ten years (and not more than twenty years for repeat offenders) and/or a fine analogous to the severity;
- *computer trespassing* resulting in exposure and obtaining certain governmental, credit, financial, commercial and consumers records and information [18 U.S.C. 1030(a)(2)], which results for simple violations not more than one year and/or a fine, for violations regarding illegal gains or involving damage of more than \$5,000 of value, not more than five years and/or a fine analogous to the severity, but as for repeat offenders, not

¹¹⁴ The law had been amended 1089, 1994, 1996 with National Information Infrastructure Protection Act of 1996, 2001, 2002 and 2008 with Identity Theft Enforcement and Restitution Act of 2008 which amends the federal criminal code in order to: (1) authorize criminal restitution orders in identity theft cases to compensate victims for the time spent to remediate the intended or actual harm incurred; (2) expand identity theft and aggravated identity theft crimes to include offenses against organizations (currently, only natural persons are protected); (3) include conspiracy to commit a felony within the definition of "felony violation" for purposes of aggravated identity theft crimes; (4) include making, uttering, or possessing counterfeited securities, mail theft, and tax fraud as predicate offenses for aggravated identity theft; (5) enable prosecution of computer fraud offenses for conduct not involving an interstate or foreign communication; (6) eliminate the requirement that damage to a victim's computer aggregate at least \$5,000 before a prosecution can be brought for unauthorized access to a computer; (7) make it a felony, during any one-year period, to damage 10 or more protected computers used by or for the federal government or a financial institution; (8) expand the definition of "cyber-extortion" to include a demand for money in relation to damage to a protected computer, where such damage was caused to facilitate the extortion; (9) prohibit conspiracies to commit computer fraud; (10) expand interstate and foreign jurisdiction for prosecution of computer fraud offenses; and (11) impose criminal and civil forfeitures of property used to commit computer fraud offenses. Directs the U.S. Sentencing Commission to review its guidelines and policy statements for the sentencing of persons convicted of identity theft, computer fraud, illegal wiretapping, and unlawful access to stored information to reflect increased penalties for such offenses. **Congress** (14/05/2008), *H.R.6060 — 110th Congress (2007-2008): Identity Theft Enforcement and Restitution Act of 2008*, <https://www.congress.gov/bill/110th-congress/house-bill/6060> (last retrieved 25/06/2019).

Cyber-security and Cyber-preparedness as a Necessary Part of the Auditing Process

more than ten years and/or a fine analogous to the severity, additional to civil liabilities, such as compensatory damages and injunctive relief or other equitable relief;

- *intentional, unauthorized access to any non-public computer of an USA Agency and trespassing in the governmental cyberspace used exclusively by or for the federal government [18 U.S.C. 1030(a)(3)], which results prison time not more than one year and not more than ten years for repeat offenders) and/or a fine, which range from \$100,000 for misdemeanors to \$250,000 for felonies or twice the amount of the loss or gain associated the violation according to 18 U.S.C. 3571, additional to other punishments like forfeiture, restitution, money laundering, civil liability found in other legal documents;*
- *unauthorized access or exceeding authorized access to a government computer, a bank or other's financial institution computer, or a computer used in, or affecting, interstate or foreign commerce with the aim to commit fraud and obtain anything of value and worth (no more than \$5,000 in any one-year period) [18 U.S.C. 1030(a)(4)], which results prison time not more than five years and not more than ten years for subsequent offenses and/or a fine analogous to the severity under Title 18 U.S.C. 1030(c)(4) additional to civil liabilities recompensating, such as compensatory damages and injunctive relief or other equitable relief. Moreover, this violation can be connected with a serious of other federal laws about financial and computational fraud and crimes, that have an extensive auditing interest, such as: 18 U.S.C. 1343 for wire fraud; 18 U.S.C. 2314 for interstate transportation of stolen property; 18 U.S.C. 659 for theft from interstate carriers; 18 U.S.C. 1832 for economic espionage; 18 U.S.C. 1832 for theft of trade secrets; 18 U.S.C. 1029 for fraud involving credit cards and access devices; 18 U.S.C. 641 for theft of federal property; 18 U.S.C. 1001 for false statements on a matter within the jurisdiction of a federal agency or department; 18 U.S.C. 1014 for false statements on federally insured loan and credit applications; 18 U.S.C. 1010, 1012 for false statements concerning various from US Department of Housing and Urban Development (HUD) transactions; 18 U.S.C. 287 for false claims against the United States; 18 U.S.C. 1344 for bank fraud; 18 U.S.C. 657 for theft or embezzlement by officer or employee of lending, credit and insurance institutions; 18 U.S.C. 1005 for false entries bank officers or employees; 18 U.S.C. 1006 for false entries by officers or employees of federal credit institutions; 18 U.S.C. 1007 for false statements to influence the Federal Deposit Insurance Corporation; 18 U.S.C. 2319 for copyright infringement); 18 U.S.C. 1956 and 1957 for money laundering; 18 U.S.C. 1962 for racketeering and other fraudulent business deals.*

- *intentional (without authorization) and recklessly damaging or provoking loss, or intentional transmitting a program, information, code or command of a government computer, a bank or other's financial institution computer, or a computer used in, or affecting, interstate or foreign commerce [18 U.S.C. 1030(a)(5)], which results (a) for first-time offenders, that did not provoke serious damage prison time of not more than one year, (b) for repeat offenders, that provoke serious damage recklessly or intentionally are being punished more harshly than category (a) offenders, (c) for an offender with a prior conviction, that causes not severe damage, there is prison time punishment for more than 10 years, but for intentionally or recklessly causing not severe damage offenders with a prior conviction there is prison time punishment for not more than 20 years, (d) for an offender that causes intentionally severe damage through a knowing transmission to a protected computer, there is prison time punishment for not more than 10 years, there is prison time punishment but not more than 20 years for repeat offenders, (e) offenders that cause recklessly serious damage due to unauthorized access or attempted (unauthorized) access, might serve prison time punishment that will not exceed five years and not more than 20 years for a second or subsequent offense, (f) offenders that knowingly or recklessly provoked or attempted to cause severe physical injury or a human loss by knowingly performing an intentional damaging transmission to a protected computer might serve prison time punishment for not more than 20 years (g) more severe punishments apart the (f) can be provoked in the following damage cases: (1) financial loss that exceeds \$5,000 over a year's time; (2) services actual or potential modification, or impairment; (3) physical injury provoking; (4) public health or safety threatening; (5) impact and negative influence on a computer belonging to justice, national defense, or national security entity and agency; and (6) impact and negative influence to 10 or more protected computers over a year's time. Moreover, this violation can be connected with a serious of other federal laws about financial and computational fraud and crimes, such provoking damage or destruction to federal property, or to financial institutions property or to interstate or foreign commerce property, that have an extensive auditing interest, such as: 18 U.S.C. 844(f) for destruction of federal property by arson or explosion; 18 U.S.C. 1853 for destruction of timber of U.S. lands; 18 U.S.C. 2071 for destruction of government records; 18 U.S.C. 1361 for destruction of federal property; 18 U.S.C. 1362 for destruction of federal communications property; 18 U.S.C. 32 for destruction of aircraft or aircraft facilities; 18 U.S.C. 33 for destruction of motor vehicles or their facilities; 18 U.S.C. 2280 for*

destruction of maritime navigational facilities; 18 U.S.C. 1992 for causing a train wreck; 18 U.S.C. 1367 for damaging an energy facility.

- *knowingly trafficking of a government computer passwords or similar information, or when the trafficking affects interstate or foreign commerce* [18 U.S.C. 1030(a)(6)], which results not more than one year in prison and not more than ten years for repeat offenders and/or a fine analogous to the severity and civilly liabilities in favor of the victims. Moreover, this violation can be connected with a serious of other federal laws about financial and computational fraud and crimes, that have an extensive auditing interest, such as: prohibition against trafficking in access devices (credit card fraud) under 18 U.S.C. 1029(a)(2); the wire fraud provisions of 18 U.S.C. 1343; a criminal breach of racketeer influenced and corrupt organizations or RICO (18 U.S.C. 1962); and money laundering prosecution (18 U.S.C. 1956, 1957); and
- *threatening to provoke damage (such as the loss of one or more people and aggregating loss of at least \$5,000 in value during any one-year period or provoke physical injury to any person; or threaten public health or safety) or to transmit and communicate obtain information or to damage data confidentiality, integrity and availability (such as actual or potential modification and impairment modifies of medical records, examinations, diagnosis, treatment, or care of one or more individuals) - without authorization or exceeding authorization to a protected government computer, a bank and other financial institutions computer, or a computer used in, or affecting, interstate or foreign commerce with the intention to extort or to enable the extortion of individuals, firms, educational institutions, financial institutions, associations, governmental body, or any other legal entity for money obtaining or other valuables obtaining* [18 U.S.C. 1030(a)(7)], which results not more than five years and not more than 10 years for repeated offenses) and/or a fine analogous to the severity of the action, additional to civilly liabilities in favor of the victims. Moreover, this violation can be connected with a serious of other federal laws about financial and computational fraud and crimes, that have an extensive auditing interest, such as: 18 U.S.C. 1951 for extortion that affects commerce; 18 U.S.C. 875 for threats transmitted in interstate commerce; 18 U.S.C. 876 for mailing threatening communications; 18 U.S.C. 877 for mailing threatening communications form a foreign country; and 18 U.S.C. 880 for receipt of the proceeds of extortion.¹¹⁵

¹¹⁵ **Doyle Charles** (15/10/2014), *Congress Research Service: Cybercrime: A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Laws*, <https://fas.org/sgp/crs/misc/RS20830.pdf> (last retrieved 25/06/2019). **Congress** (03/10/1986), *TEXT H.R.4718 — 99th Congress (1985-1986): H.R.4718 - Computer Fraud and Abuse Act of 1986*, <https://www.congress.gov/bill/99th-congress/house-bill/4718> (last retrieved 25/06/2019).

- ***Freedom of Information Act (FOIA) of 1967 and FOIA Improvement Act of 2016:*** FOIA and its amendments (a) provides the right to the public to request access in federal agencies' records and (b) demands from federal agencies not only to fulfil the request and provide access to the requested data, unless the request is one of nine exemptions, such as personal privacy, national security, and law enforcement, but also requires from federal agencies to disclose proactively online specific types of information, such as frequently requested records.¹¹⁶
- ***Privacy Act of 1974:*** this law (a) amends FOIA, (b) establishes a *Code of Fair Information Practice* concerning the collection, maintenance, use, and dissemination of an individual's personally identifiable information that are kept and stored to systems of records by the federal agencies, (c) demands from the agencies to provide to the public a notification about their personal records by communicate relevant data to the Federal Register, (d) forbids any agency to disclose any record contained in a system of records by any means of communication to any person, or to another agency, without the written consent of the subject individual, unless the disclosure belongs to one of twelve statutory exceptions, such as for statistical purposes by the Census Bureau and the Bureau of Labor Statistics, for law enforcement purposes, or congressional investigations etc., (e) obliges from each federal agency to have an administrative and physical security system with the scope to prevent the release of personal records without authorization and to have a Data Integrity Board, that will inform in annual base with a report the OMB and the public about any violations, (f) allows individuals to seek access, modify, correct and review their records, together with the ability to be informed which of their records have been disclosed and (g) establishes *Privacy Protection Commission*, as an independent agency, that investigates and reports violations of this Act to specified sources; reviews agencies' reports upon proposals on information systems or data banks or significant expansions of such systems in order to define their impact on the privacy and other rights of individuals; and (3) creates and submits key findings and recommendations as it concerns further legislative and administrative proposals to enrich and meet the scope of the Privacy Act.¹¹⁷ SEC had to amend its system of records for enforcement files according to Privacy Act of 1974 (SEC-42) that clarifies SEC's ordinary process as it concerns (a) the disclosure of the collection of amounts ordered to be paid in civil and administrative proceedings, (b) the incorporation of

¹¹⁶ **Congress** (30/06/2016), *TEXT S.337 — 114th Congress (2015-2016): Public Law No: 114-185 (06/30/2016), FOIA Improvement Act of 2016*, <https://www.congress.gov/bill/114th-congress/senate-bill/337/text> (last retrieved 25/06/2019). **FOIA.GOV** (2019), *Freedom of Information Act Statute*, <https://www.foia.gov/foia-statute.html> (last retrieved 25/06/2019).

¹¹⁷ **Congress** (30/06/2016), *TEXT: H.R.16373 — 93rd Congress (1973-1974): Privacy Act*, <https://www.congress.gov/bill/93rd-congress/house-bill/16373> (last retrieved 25/06/2019).

statements concerning disclosure to consumer credit reporting agencies, (c) the updating of statutory and regulatory references in certain routine uses, (d) the updating in the way SEC addresses the system administrators, and (e) the identification of exemptions from disclosure under the Privacy Act system of records claims.¹¹⁸

➤ ***Promoting Good Cyber Hygiene Act of 2015:*** requires from the NIST to develop for the federal government, the private sector, and for any individual or organization a list of non-obligatory voluntary best practices that will promote effective and strong cyber hygiene to shield information systems or devices against cybersecurity threats, such as unauthorized access, modification of data or programming code running on such systems or devices, and unauthorized denials of service. Moreover, the Department of Homeland Security, together with NIST and the Federal Trade Commission (FTC) have to (a) evaluate cybersecurity threats relating to mobile devices and what could be their effect on the level of cybersecurity protection on federal government's information systems and networks, and (b) propose recommendations for best dealing with this threats.¹¹⁹

➤ ***Cybersecurity Responsibility and Accountability Act of 2016:*** this Bill demands from National Institute of Standards and Technology (NIST) to provide a wider cybersecurity framework for its computer standards as it concerns agency information systems and to create for the Office of Management and Budget (OMB) a process on how agencies can apply, implement, independently evaluate and report NIST's information security standards, procedures and practices. Moreover, NIST must (a) provide additional development to Agencies heads about information security training and certification, (b) deal further information security challenges and knowledge gaps concerning Agencies, (c) evaluate information security constitutional obligations, and (d) establish national security systems standards. Agencies must (a) establish Chief information security officers based on professional responsibilities created by to be developed by the OMB and NIST, (b) create obligatory information security training and certification to safeguard that each agency's head have a solid understanding federal cybersecurity policies and frameworks concerning proper cybersecurity functioning and protection of every Agency's systems, cyber-threats, attack and data breaches, and that official communication must be conducted in proper way and not through private email servers or private messaging systems, (c) certify that the each Agency comply properly with information security standards and in case they do not they must provide the reasoning why, (d) plan in annual base the implementation of information

¹¹⁸ SEC (18/07/2002), Release No. PA-32 ; File No. S7-27-02: Privacy Act of 1974, Amended System of Records for Enforcement Files, <https://www.sec.gov/rules/other/pa-32.htm> (last retrieved 25/06/2019).

¹¹⁹ Congress (01/10/2015), Text: H.R.3664 - Promoting Good Cyber Hygiene Act of 2015, <https://www.congress.gov/bill/114th-congress/house-bill/3664> (last retrieved 25/06/2019).

security recommendations of the Government Accountability Office (GAO) and inspectors general relevant recommendations and in case of an implementation failure the reasoning must be reported to OMB for approval and (e) provide proper reporting upon any OMB-defined as a major cybersecurity incident, that involves classified information exposure to the OMB, the Department of Homeland Security, NIST, Congress, and the GAO, otherwise the Agencies' head will be considered as accountable.¹²⁰

➤ ***Small Business Cyber Security Improvements Act of 2016***: this Bill attempted to amend the Small Business Act and among others attempted to authorize the *Small Business Administration* (SBA) in order not only to provide grants to small business development centers (SBDCs) but also SBA in cooperation with Department of Homeland Security (DHS) must develop the Small Business Development Center Cyber Strategy after the Government Accountability Office (GAO) submitted its report about the needed resources of federal agencies to support cybersecurity in small businesses. This Small Business Development Center Cyber Strategy must be submitted to the Congress, and must incorporate: (a) plans and proposals on how SBDCs can introduce cybersecurity programs that will assist small business, (b) aid, support and guidance on how small business can improve their cyber security infrastructure capacities, threat understanding and responsiveness, develop the proper training programs for employees, including providing knowledge from Information Sharing and Analysis Centers and external cybersecurity experts and (c) an investigation on SBDCs ability to influence other federal Agencies programs and establish develop cooperation's that will advance cybersecurity services to small businesses.¹²¹

➤ ***National Cybersecurity Preparedness Consortium Act of 2016***: the goal of this bill is to authorize the Department of Homeland Security (DHS) (a) to join efforts with a consortium, including the National Cybersecurity Preparedness Consortium, in order to address cybersecurity risks and incidents, such as cybersecurity threats or terrorists attacks, (b) to provide proper education, training and technical assistance not only to state but also to local first line responders and officials, in order to be able to face this incidents, (c) to conduct cross-sector cybersecurity training and simulation exercises, that will include state and local governments, critical infrastructure owners and operators, private industry entities, (d) to assist states and communities to develop their cybersecurity information sharing

¹²⁰ **Congress** (21/09/2016), *TEXT H.R.6066 — 114th Congress (2015-2016): H.R.6066 - Cybersecurity Responsibility and Accountability Act of 2016*, <https://www.congress.gov/bill/114th-congress/house-bill/6066> (last retrieved 25/06/2019).

¹²¹ **Congress** (06/06/2016), *TEXT S.3024 — 114th Congress (2015-2016): Small Business Cyber Security Improvements Act of 2016*, <https://www.congress.gov/bill/114th-congress/senate-bill/3024> (last retrieved 25/06/2019).

programs, and (e) to support the inclusion of cybersecurity risk and incident prevention and response activities into existing state and local emergency plans and operation continuity plans.¹²²

➤ ***Ensuring National Constitutional Rights for Your Private Telecommunications Act of 2016 or ENCRYPT Act of 2016:*** this document forbids any state of the Union from demanding from a manufacturer, developer, seller, or provider of any technology product or service (such as computer(s), electronic device(s), online service(s) and any other publicly and commercially available good) to proceed to the alteration of the security operations and requirements in their product(s) or service(s) in order to permit to a government agency to perform a physical search or users' surveillance, or to use their product(s) or service(s) with the aim to decrypt encrypted data. Moreover, it forbids a state from prohibiting the manufacture, sale or lease, or provision any technology product or service, that uses of encryption technology or any other relevant cybersecurity protective mechanism and function.¹²³

➤ ***Data Breach Insurance Act of 2016:*** provides an amendment to the Internal Revenue Code (IRC) with the scope to allow a business tax credit, applicable for a five years period and equal to 15% of the annual insurance premiums paid or incurred due to ordinary taxpayer's trade or business, for entities purchasing a qualified data breach insurance. The definition of qualified data breach insurance covers expenses or losses in connection with the theft, loss, disclosure, inaccessibility, or manipulation of data that is provided by a legal insurance entity. Taxpayers must obtain an insurance that complies with: (a) the Framework for Improving Critical Infrastructure Cybersecurity published by the National Institute of Standards and Technology (NIST), or (B) any comparable standard established by the Internal Revenue Service (IRS).¹²⁴

➤ ***Cybersecurity and Infrastructure Protection Agency Act of 2016:*** amends the Homeland Security Act of 2002 and constitutes as the nation's Cybersecurity and Infrastructure Protection Agency (CIPA), the Department of Homeland Security's (DHS's) National Protection and Programs Directorate, that will be controlled by an appointed by the President with the Senate's consent Director of National Cybersecurity, with the aim (a) to direct national efforts that will protect and strengthen the security and resilience of U.S.

¹²² **Congress** (15/03/2016), *Text: H.R.4743 — 114th Congress (2015-2016): National Cybersecurity Preparedness Consortium Act of 2016*, <https://www.congress.gov/bill/114th-congress/house-bill/4743> (last retrieved 25/06/2019).

¹²³ **Congress** (10/02/2016), *Text: H.R.4528 — 114th Congress (2015-2016): ENCRYPT Act of 2016*, <https://www.congress.gov/bill/114th-congress/house-bill/4528> (last retrieved 25/06/2019).

¹²⁴ **Congress** (14/09/2016), *Text: H.R.6032 — 114th Congress (2015-2016): Data Breach Insurance Act*, <https://www.congress.gov/bill/114th-congress/house-bill/6032> (last retrieved 25/06/2019).

cyber and critical infrastructure systems, (b) will develop and update every two years not only a national risk assessment as it concerns cybersecurity and critical infrastructure risks in collaboration with other DHS departments and federal entities, but also an integrated assessment that will compare risks and incidents to their impacts and effects. Four departments of DHS (1) the Cybersecurity Division, (2) the Infrastructure Protection Division, (3) the Emergency Communications Division, and (4) the Federal Protective Service will be the institutional particles that will compose CIPA. Additionally, to these departments another one the Office of Biometric Identity Management will be established within DHS in order to provide relevant standards and services for DHS, federal, state, local, territorial, and tribal agencies, foreign governments, and the private sector.¹²⁵

➤ ***To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes Act*** best known as ***Cybersecurity Act of 2015***: this legal document creates a voluntary framework between federal government and agencies, state governments and private entities on sharing information about cybersecurity threats and incidents by dealing simultaneously with a series of cybersecurity affairs and more precisely: (a) Act's Title I entitled "Cybersecurity Information Sharing" consisting the *Cybersecurity Information Sharing Act of 2015* establishes the major cybersecurity information sharing framework as a real-time voluntary process upon cyber threat indicators and defensive measures among non-federal entities, such as State, tribal, or local governments and federal entities, providing at the same time liability protections and an antitrust exemption, such as the clause for protecting public entities "no cause of action shall lie or be maintained in any court against any private entity" for the monitoring, sharing, or receipt of cyber threat indicators or defensive measures in accordance with the Act. This part of the Act demands from all parties involved before the share the needed information to Federal or non-Federal entities, to remove any "personal information of a specific individual or information that identifies a specific individual" that has no direct relationship with the cybersecurity threat: (b) Title II of the Act entitled Federal Cybersecurity Enhancement consisting the *Federal Cybersecurity Enhancement Act of 2015*: not only amends Homeland Security Act of 2002, d Security Act of 2002 in order DHS together with the Office of Management and Budget (OMB), to implement an intrusion assessment plan with the aim to identify and eradicate intruders in federal agency information systems, but also establishes a *National Cybersecurity and*

¹²⁵ **Congress** (07/06/2016), *Text: H.R.5390 — 114th Congress (2015-2016): Cybersecurity and Infrastructure Protection Agency Act of 2016*, <https://www.congress.gov/bill/114th-congress/house-bill/5390> (last retrieved 25/06/2019).

Communications Integration Center (NCCIC) within DHS, as the federal entity responsible for the implementation and sharing of information mentioned in previous Title, Title I, with the duty to coordinate the sharing cyber threat indicators, defensive measures, and other information related to cybersecurity risks and incidents with Federal and non-Federal entities, and conduct relevant collaborations with international partners in order to promote and strengthen cybersecurity and resilience in global level. (c) Title III entitled Federal Cybersecurity Workforce Assessment constituting *Federal Cybersecurity Workforce Assessment Act of 2015* requires from the federal agencies to assess the cybersecurity capacities of all their personnel and to enrich these capacities among other by establishing corresponding employment code that the National Institute of Standards and Technology (NIST) will develop in its must include in the National Initiative for Cybersecurity Education's National Cybersecurity Workforce Framework and (d) the last Title IV entitled Other Cyber Matters is home to specific provisions, such as (i) the obligation of DHS to report to Congress on threats relating to the security of the mobile devices of the federal government, including its plan for accelerated adoption of secure mobile device technology, (ii) the provision for Department of State to develop a comprehensive strategy relating to U.S. international cyberspace policy that will support relevant activities from the President's International Strategy for Cyberspace and the need to establish norms, descriptions and guidelines in collaboration with foreign governments (such as China, Russia, Brazil, and India) upon responsible international behavior in cyberspace; and cyberspace threats to U.S. national security not only from foreign countries, state-sponsored actors, but also from private actors to federal and private sector infrastructure, U.S. intellectual property, and U.S. citizens; with the participation of the State Department's Office of the Coordinator for Cyber Issues, (iii) the provision for cyber protection and cyber-preparedness of national health sector with the Department of Health and Human Services (HHS) obligation to report to Congress regarding these issues and how the health care industry is properly prepared for cybersecurity threats and the obligation of HHS to collaborate with DHS, health care industry stakeholders, NIST, and other entities to establish a single, voluntary, national, health-specific cybersecurity framework with a common set of standards and security practices as a resource for cost-effectively reducing cybersecurity risks for health care organizations. Moreover, this Title amends the federal criminal code to extend extraterritorially the application of penalties for fraud offenses involving an access device, such as any card, code, electronic serial number, telecommunications service, or other means of account access that can be used to initiate a transfer of funds or to obtain money, goods, or services, issued, owned, managed, or controlled by a financial institution, account

issuer, credit card system member, or other entity organized under the laws of the United States or any U.S. state or territory.¹²⁶

➤ ***Secure Data Act of 2018:*** this law forbids (a) a federal agency from demanding from a manufacturer, developer, or seller of any computer hardware, software, or electronic device that is commercially available to the general public to proceed to the alteration of the security operations and requirements in their product(s) or service(s) in order to permit to a government agency to perform a physical search or users' surveillance; and (b) a court from issuing an order to force any such manufacturer, developer, or seller to proceed to the alteration of the security operations and requirements in their product(s) or service(s) in order to permit to a government agency to perform a physical search or users' surveillance. Moreover, the Bill provides an exemption from that type of prohibitions: the case of requests or court orders that allows such authorization under the Communications Assistance for Law Enforcement Act.¹²⁷

➤ ***Clarifying Lawful Overseas Use of Data Act or the CLOUD Act of 2018:*** this Bill that was signed into law on March 2018 amends the federal criminal code and to the Stored Communications Act (SCA) of 1986¹²⁸ and Electronic Communications Privacy Act of 1986. CLOUD Act clarifies that an electronic communication service (ECS) or a remote computing service (RCS) provider must comply with existing requirements and must allow that federal law enforcement requests via subpoena or a warrant or in response to an order from a foreign government with which the United States has an executive agreement on data access, to have access to information about preservation, back-up, and disclosure of the contents of an electronic communication or non-content records or information stored relating to a customer or subscriber, irrespectively if the communication or record system is in US soil or outside. In case the customer or subscriber is not a U.S. citizen or national, lawful permanent resident, corporation, or other unincorporated entity; or the customer or subscriber does not reside in the United States; and the required disclosure creates a material risk that the provider violates the laws of a foreign government with which the United States has in effect an executive agreement on data access, then the ECS or RCS provider have the right to challenge the domestic warrant that demands disclosure of the contents of an electronic communication. Moreover, CLOUD Act provides a framework on how United

¹²⁶ **Congress** (27/10/2015), *Text: S.754 — 114th Congress (2015-2016): To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes*, <https://www.congress.gov/bill/114th-congress/senate-bill/754> (last retrieved 25/06/2019).

¹²⁷ **Congress** (14/09/2016), *Text: H.R.5823 — 115th Congress (2017-2018): Secure Data Act of 2018*, <https://www.congress.gov/bill/115th-congress/house-bill/5823> (last retrieved 25/06/2019).

¹²⁸ Law Enforcement Access to Data Stored Abroad Act or LEADS Act of 2015 and the International Communications Privacy Act or ICPA Act of 2017 failed to amend the SCA, since they did not manage to pass other than being introduced to the Senate.

States can forge executive agreements with foreign governments about data access issues. But in order any executive agreement to be valid, it fulfil concrete provisions, such as (a) the foreign government provides a strong procedural privacy protection and (b) the adopted procedures offers the minimum level of data access. After all, the Act does not prohibit from a foreign authority to obtaining assistance in case of a criminal investigation or prosecution.¹²⁹

➤ ***Internet of Things Cybersecurity Improvement Act of 2019 or IoT Cybersecurity Improvement Act of 2019***: this Bill demands from the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) to carry out specialized action with the aim to intensify cybersecurity for Internet of Things (IoT) devices, due to the fact that IoT importance derives as the extension of Internet connectivity into physical devices and everyday objects. Until, September 30, 2019, NIST must complete its efforts concerning actions for administering IoT cybersecurity risks, such as potential cybersecurity concerns of IoT devices. Moreover, March 31, 2020, is the milestone for NIST to establish recommendations and standards about the proper use and management of IoT devices operated and belonged by the government, as well as creating a minimum of information security requirements for managing IoT cybersecurity risks. Additionally, the OMB must publish a set of guidelines for each agency coherent with NIST's recommendations. Last but not least, NIST and the OMB must issue guidelines on policies and procedures for the proper reporting, organizing, disclosing, and obtaining information concerning security vulnerability of IoT device used by the government and how to best deal with such security vulnerability.¹³⁰

As we examine previously from all these legal documents federal agencies and governmental bodies must establish and acquire cybersecurity and cyber-preparedness norms, specialized divisions, and Center's. For example, ***Department of Justice*** (DOJ), which is the governmental body accountable for federal computer crime laws enforcement and leads to prosecution all the relevant cases, had established the ***Computer Crime and Intellectual Property Section*** (CCIPS). CCIPS is the body responsible not only to implement DOJ's national strategies related to fight against computer and intellectual property crimes nationally and worldwide and to investigate and prosecute related crimes by collaborating closely other government agencies, the private sector, academic institutions,

¹²⁹ **Congress** (26/02/2018), *Text: H.R.4943 — 115th Congress (2017-2018): Clarifying Lawful Overseas Use of Data Act or the CLOUD Act*, <https://www.congress.gov/bill/115th-congress/house-bill/4943/text> (last retrieved 25/06/2019).

¹³⁰ **Congress** (11/03/2019), *Text: S.734 — 116th Congress (2019-2020): Internet of Things Cybersecurity Improvement Act of 2019*, <https://www.congress.gov/bill/116th-congress/senate-bill/734> (last retrieved 25/06/2019).

and foreign counterparts. CCIPS's attorneys and experienced personnel aim to ameliorate not only domestic but also international efforts to efficiently pursue network infrastructure, legal, technological, and operational criminals. Due to the fact that Intellectual Property (IP) productions enhance the most to the national economic development, protection of copyright, trademark, trade-secret and other IP productions from cyber-thefts, constitutes the high significance of CCIPS more obvious, that is why its attorneys must (a) conduct complex investigations, and (b) resolute important and unique legal and investigative cases based on difficulties derive from emerging computer and telecommunications technologies and their threats. Moreover, CCIPS investigates litigate cases and provides litigation support to other prosecutors, provides training to federal, state, and local law enforcement personnel, comments relevant legislations and last but not least initiates and contributes to relevant international attempts that aim to offer solutions and to combat computer and intellectual property crime worldwide.¹³¹ From December 2014, withing CCIPS the Criminal Division had created the *Cybersecurity Unit*, that functions as the central leading hub providing expertise and legal guidance concerning criminal electronic surveillance and computer fraud and abuse situations, additionally to develop cybersecurity legislation, to safeguard public's privacy protection, to ensure nationwide protection of computers networks, to strengthen capacities of law enforcement authorities to prosecute cybersecurity perpetrators, to protect individuals from being victims of cyber-attacks and to collaborate with private sector for development and promotion of proper legal cybersecurity practices and behaviors. Cybersecurity Unit, also, creates guidelines and white papers upon significant cybersecurity matters, such as (a) cybersecurity incident preparation, response and reporting, (b) security of IoT devices, (c) implementation of Cybersecurity Information Sharing Act and collaboration between DHS and DOJ upon the matter, (d) technical guidance on facing cyber threats, like ransomware, (e) implementation of anti-trust policy concerning information sharing in cooperation with Securities and Exchange Commission (SEC), etc.¹³² The proper sharing of cybersecurity information with the public in order to enhance national antitrust policy has been a subject for action between DOJ and Federal Trade Commission with the issuance in 2014 of a common antitrust policy statement that encourages private entities to share legitimate cyber threat information, and especially technical cyber threat information, such as threat signatures, indicators, and alerts, with the public including their competitors without raising antitrust issues, since these type of information sharing and

¹³¹ US Department of Justice (2019), *Computer Crime and Intellectual Property Section (CCIPS)*, <https://www.justice.gov/criminal-ccips> (last retrieved 25/06/2019).

¹³² US Department of Justice (2019), *Cybersecurity Unit*, <https://www.justice.gov/criminal-ccips/cybersecurity-unit> (last retrieved 25/06/2019).

disclosures can enrich and improve not only current or future stock prices, production and business plans, but also the security, availability, integrity and efficiency of the nation's markets and information systems.¹³³

Department of Justice is not the only law enforcing and investigating cyber-crimes and cyber incidents reporting authority in the country. ***Federal Bureau of Investigation***, best known as FBI, through its Cyber Division (established in 2006 in FBI headquarters), sometimes in collaboration with other bodies, like DOJ and DHS, provides not only guidance for civilians and entities and investigates cybersecurity crimes, such as computer intrusions, theft of intellectual property and personal information, business email compromise, child pornography and exploitation, and online fraud, but also provides support and protection to those had received a cybersecurity attack by reporting the cyber incident to FBI's and receiving relevant expertise from ***FBI's Internet Crime Compliant Center (IC3)***. The reporting of cyber incident to FBI is accompanied with a series of benefits: (a) the Bureau's *Computer Crimes Task Forces* and experts in federal, state and local level will identify and block the malicious cyber activities such as information sharing and data loss, since the FBI's specialists collaborate closely with an entity's cybersecurity and technical teams with the aim to identify, understand and stop the negative effects of an cyber incident, (b) with its *Cyber Assistant Legal Attachés* and all over the globe, the Bureau offers support together with its international law enforcement associates for locating stolen data or recognizing the criminals, (c) from February 2018 the *Recovery Asset Teams (RATs)* of IC3 function as a communication channel between financial institutions and infected entities assisting them in the recovering and obtaining back their funds and assets transferred to domestic accounts due to fraudulent behaviors. Only in the first year (2018) of their function, RATs had managed to recover 75% of fraudulently transferred funds, (d) in cooperation with DOJ proceed with accusations and other law enforcing and detection acts to arrest cybercriminal and minimize their capacities, and (e) provoke disruptions and confiscate cyber-actors technical capacities and infrastructure and at the same time can track electronic evidence of the fraudulent and malicious acts. That is why, DOJ and FBI promotes cooperation and forging of a good relationship between companies and entities with one of 56 *Local FBI Field Offices* around the nation before a cybersecurity incident takes place, since this proactive relationship not only provides to the economic entities with a devoted FBI point of contact in case of an incident occurs, but also enables the entities to

¹³³ **Federal Trade Commission** (10/04/2014), *Department Of Justice And Federal Trade Commission: Antitrust Policy Statement On Sharing Of Cybersecurity Information*, <https://www.ftc.gov/public-statements/2014/04/departement-justice-federal-trade-commission-antitrust-policy-statement> (last retrieved 25/06/2019).

be supported by FBI's cyber mitigation and resolving incidents capacities and resources. FBI's *Cyber Action Teams* (CATs) are located in Local FBI Field Offices nationwide and can be deployed all around the world within 48 hours providing investigative assistant, critical inquiries support, forensic investigations, malware analysis and rapidly move case forwards in cases of an intrusion in an entity's computer networks, trade secrets, customers' personal information, and other critical data by identifying what is called as the cyber-criminals and hackers personal signature, consisted of TTPs—tools, techniques, and procedures. With its *National Cyber-Forensics & Training Alliance* (NCFTA), established in 1997 in Pittsburgh, the Bureau provides a globally recognized model based on the collaboration between law enforcement authorities, private industry, and academia¹³⁴ that develops and shares resources, strategic information, and threat intelligence capacities regarding the identification and halting of emerging cyber threats and mitigating the already known ones irrelevant if they take place nationwide or internationally, such as spam attacks, botnets, stock manipulation schemes, intellectual property theft, pharmaceutical fraud, telecommunications scams, and other financial fraud schemes that cost in annual base billions of dollars in losses for companies and consumers. Last but not least, FBI participates in *National Cyber Investigative Joint Task Force* (NCIJTF), established in 2008, which is a multi-agency cyber center consisted of over 20 partnering agencies from across law enforcement, the intelligence community, and the Department of Defense, with representatives located in and working to succeed in the cybersecurity attempts of their organization from a wide range of governmental objectives. NCIJTF (a) coordinates participating organization cybersecurity actions, (b) integrates, and shares relevant to cyber threat investigations information, (c) provides intelligence analysis for local decision-makers, (d) enhances the national in place efforts against cyber threats, (e) coordinates joint efforts between internal forces, international and private sector's forces, aiming to identify, track, and defeat actual terrorists, spies, and against national systems' criminals and other perpetrators.¹³⁵

¹³⁴ Significant particles of this collaboration are: The FBI Cyber Division's Cyber Initiative and Resource Fusion Unit (CIRFU) hundreds of private sector NCFTA members, NCFTA intelligence analysts, Carnegie Mellon University's Computer Emergency Response Team (CERT), and the FBI's IC3.

¹³⁵ **US Federal Bureau of Investigation** (2019), *Cyber Crime*, <https://www.fbi.gov/investigate/cyber> (last retrieved 25/06/2019). **US Federal Bureau of Investigation** (2019), *National Cyber Investigative Joint Task Force*, <https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force> (last retrieved 25/06/2019). **US Federal Bureau of Investigation and IC3**, *Internet Crime Report 2018*, https://pdf.ic3.gov/2018_IC3Report.pdf (last retrieved 25/06/2019). **US Federal Bureau of Investigation** (26/10/2016), *National Cyber Security Awareness Month: FBI Deploys Cyber Experts to Work Directly with Foreign Partners*, <https://www.fbi.gov/news/stories/fbi-deploys-cyber-experts-to-work-directly-with-foreign-partners> (last retrieved 25/06/2019).

Cyber-security and Cyber-preparedness as a Necessary Part of the Auditing Process

In the following pages, we will examine the influence and the actions of major US's institutions that provide guidance, supervision or even litigation in cybersecurity accounting and auditing matters. First station in this process will be the Securities and Exchange Commission (SEC).

Securities and Exchange Commission (SEC) have been established by Securities Exchange Act of 1934 after the big economic recession of 1929, in order to enhance investor confidence to USA capital markets and public-traded companies and to deliver proper regulating rules through disclosing reliable information to shareholders, investors and the general public. SEC oversees securities exchanges, securities brokers and dealers, investment advisors, rating agencies, mutual funds and other related entities, advocating reliable disclosure of significant market-related information, providing fair trading, and safeguarding the capital markets against frauds bringing numerous civil enforcement actions against individuals and entities in case they violate securities laws, such as insider trading situations, accounting fraud, providing false or misleading financial statements and disclosures for issued securities and the entities that bring the securities to markets. In a nutshell, SEC is the primary regulator and supervisor of the U.S. securities markets, and collaborates with institutions, like Congress, federal departments and agencies, stock exchanges (New York Stock Exchange or NYSE, and The Nasdaq Stock Market), Financial Industry Regulatory Authority (FINRA), and numerous private sector entities in order to protect the country's capital markets, according to the laws that govern the securities markets: the Securities Act of 1933, Securities Exchange Act of 1934, the Trust Indenture Act of 1939, that applies to debt securities such as bonds, debentures, and notes that are offered for public sale, the Investment Company Act of 1940, the Investment Advisers Act of 1940, the Sarbanes-Oxley Act of 2002, as we describe them previously, the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 and the Jumpstart Our Business Startups (JOBS) Act. Moreover, SEC's Chairman of the SEC represents the institution in the Financial Stability Oversight Council (FSOC).

As it concerns the accounting and auditing sector, SEC (a) issues, interprets and enforces federal securities laws, and amends existing rules, (b) supervises securities firms, brokers, investment advisers, and ratings agencies and their information disclosures against frauds, (c) oversees private regulatory organizations in the securities, accounting, and auditing firms and entities by monitoring (i) the activities of the accounting and audit professionals and firms and more precisely of the Financial Accounting Standards Board (FASB), in order to create the generally accepted accounting principles (best known as GAAPs), (ii) the application by U.S. entities registered to implement the International

Financial Reporting Standards (IFRS) created by the International Accounting Standards Board, and (d) manages and organizes U.S. securities laws with federal, state, and foreign authorities.¹³⁶

As it concerns the cybersecurity dimension regarding accounting and auditing obligations, SEC most recent action was issuing in February 21, 2018 a new interpretive guidance upon proper cybersecurity disclosures for public traded companies and entities, that supplements the previous one that had been issued in October 2011. The new interpretive guidance provides a lot of clarification as it concerns accurate cybersecurity disclosures. First of all, recognizes the possible costs that a company might suffer from a successful cyber-attacks or experience other cybersecurity incidents: (a) remediation costs: like costs for liabilities for stolen assets or information, repairs of system damage, and incentives to customers or business partners in an effort to maintain relationships after an attack; (b) increased cybersecurity protection costs: such as costs for making organizational changes, deploying additional personnel and protective technologies, training employees, and engaging third party experts and consultants; (c) costs from loss of revenues resulting from the unauthorized use of proprietary information or the failure to retain or attract customers following an attack; (d) litigation and legal risks costs, including regulatory actions by state and federal governmental authorities and non-U.S. authorities; (e) increased insurance premiums; (f) reputational damage which results adversely affects to customers' or investors' confidence; and (g) competitiveness loss, stock price, and long-term shareholder value damages.

The guidance contains specific requirements as it concerns the CF Disclosure filing, comparing to SEC's Division of Corporation Finance previous guidance of October 2011, that did not provide specific disclosure obligations relating to cybersecurity risks and incidents, other than companies may be oblige to disclose cybersecurity risks and incidents. The 2018 Guidance not only addresses the importance of acquiring, maintaining and enriching comprehensive cybersecurity policies and procedures, that establishes the proper controls, which ensure accurate, not misleading, and timely sound disclosures of material cybersecurity events in accordance with federal securities law and standards (such as Securities Act of 1933 and the Securities Exchange Act of 1934, Regulation S-K and Regulation S-K16, Regulation S-X, Form 10-K for annual reports, Form 10-Q for quarterly reports, Form 20-F for private issuers periodic reports disclosures, Form 8-K27 or Form 6-K for specific incidents management's discussion and analysis of financial condition and

¹³⁶ US Securities and Exchange Commission (10/06/2013), *What We Do*, <https://www.sec.gov/Article/whatwedo.html> (last retrieved 25/06/2019).

Cyber-security and Cyber-preparedness as a Necessary Part of the Auditing Process

results of operations or MD&A), but also extends the application of insider trading prohibitions in the cybersecurity context, where an entity's directors, officers, and other corporate insiders must apply general antifraud provisions regarding federal securities laws and must abstain from making selective disclosures of material nonpublic information about cybersecurity risks or incidents.

As it concerns the proper cybersecurity disclosure issue, the 2018 Guidance explains that companies must not proceed to detailed disclosures (such as technical information about their cybersecurity systems, the related networks and devices, or potential system vulnerabilities in extreme details) that might compromise its cybersecurity efforts and can assist penetrators to commit their actions, but they are expected to disclose cybersecurity risks and incidents that have a material significance are to investors, and must include related financial, legal, or reputational consequences. Moreover, companies must recognize properly the incidents, that took place after the initial disclosure, to cooperate with law enforcement and investigation authorities and not to avoid disclosure these incidents, but on the contrary entities have the duty to correct and update prior untrue or mistaken disclosures into tailored made reports to any particular cybersecurity risks and incidents and avoid generic cybersecurity-related disclosure. Among the evaluating cybersecurity risk factors that entities can disclosure are: (a) the occurrence of prior cybersecurity incidents, including their severity and frequency, (b) the probability of the occurrence and potential magnitude of cybersecurity incidents, (c) the adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs, including, if appropriate, discussing the limits of the company's ability to prevent or mitigate certain cybersecurity risks, (d) the aspects of the company's business and operations that give rise to material cybersecurity risks and the potential costs and consequences of such risks, including industry-specific risks and third party supplier and service provider risks, (e) the costs associated with maintaining cybersecurity protections, including, if applicable, insurance coverage relating to cybersecurity incidents or payments to service providers, (f) the potentiality for reputational harm, (g) existing or pending laws and regulations that may affect the requirements to which companies are subject relating to cybersecurity and the associated costs to companies, and (h) litigation, regulatory investigation, and remediation costs associated with cybersecurity incidents. The new Guideline takes under serious consideration the role and the responsibility of Board of Directors and its oversight on the cybersecurity related issues, its engagement to a company's cybersecurity risk management, that must be present in the disclosures. As it concerns the disclosure of controls and procedures regarding cybersecurity risk management policies and procedures, those key elements of the entity's general risk

Cyber-security and Cyber-preparedness as a Necessary Part of the Auditing Process

management and mitigation approach, such as compliance with the federal securities laws, must be thorough, sufficient, effective, assessed regularly and involve the appropriate personnel, such as senior management and the Audit Committee, before they are incorporated to cybersecurity disclosure. One of the aims of cybersecurity controls and procedures is to prohibit directors, officers, other corporate insiders from trading based on material non-public information about cybersecurity risks and incidents. Additionally, companies in order to comply with Exchange Act Rules 13a-15 and 15d-15, must secure that their disclosure controls and procedures are not only effective but also constructed in such way so the information they must be disclosed in the entity's reports is (a) "*recorded, processed, summarized and reported, within the time periods specified in the Commission's rules and forms,*" and (b) "*accumulated and communicated to the company's management ... as appropriate to allow timely decisions regarding required disclosure.*" Controls and procedures, also, must allow to the companies not only to identify cybersecurity risks and incidents, assess and analyze their impact on a company's business, but also to evaluate their significance, and facilitate open communications between technical experts and disclosure advisors for creating timely disclosures regarding such risks and incidents. What is more, Exchange Act Rules 13a-14 and 15d-1455 for the formation of proper certifications by an entity's principal executive officer and principal financial officer regarding the construction and effectiveness of disclosure controls and procedures must be fulfilled, while Item 307 of Regulation S-K and Item 15(a) of Exchange Act Form 20-F demands from entities to disclose conclusions on the effectiveness of disclosure controls and procedures. These certifications and disclosures must give special attention not only to controls and procedures' adequacy and capability to efficiently identify cybersecurity risks and incidents, but also to assess and analyze their impact, especially if these cybersecurity risks or incidents can influence negatively the capability of an entity to record, process, summarize, and report information necessary for filling the disclosures. The entity's management team must search and take under serious account, if there are any deficiencies and malfunctions in disclosure controls and procedures that constitute them unproductive and inefficient.

As it concerns the prohibition of insider trading based to cybersecurity insider knowledge, the 2018 Guidance reminds that directors, officers, and other corporate insiders should always try to comply with related laws which expands the insider trading information also in knowledge about cybersecurity risks and incidents, including vulnerabilities and breaches, since according to Rule 10b5-1(a) of the Exchange Act it is illegal to trade a security "*on the basis of material nonpublic information about that security or issuer, in breach of a duty of trust or confidence that is owed directly, indirectly, or derivatively, to the*

issuer of that security or the shareholders of that issuer, or to any other person who is the source of the material nonpublic information”, which now expands to non-public material about a company’s cybersecurity risks and incidents. This action constitutes a legal violation of antifraud provisions for directors, officers, and other corporate insiders if they proceed in trading their company’s securities in breach of their duty of trust or confidence while they are in possession of that material non-public information. Apart from Securities Exchange Act anti-fraud provisions and other federal securities laws, companies and more precisely their directors, officers, and other corporate insiders must never forget that there is a series of insider trading related rules that they must comply, such as those imposed by many exchanges (for example, NYSE Listed Company Manual Section 303A, NASDAQ Listing Rule 5610, and Section 406(c) of the Sarbanes-Oxley Act of 2002), that usually demand from public traded companies to adopt codes of conduct and policies with the aim to comply with applicable laws, rules, and regulations, and which include the prohibiting of insider trading based on material non-public information related to cybersecurity risks and incidents. Federal antifraud provisions do not only promulgate full and fair disclosure, but also forbid insider trading able to harm both individual investors and the solid foundations of securities markets by damaging investor confidence in the integrity of those markets. Applying the proper restrictions on securities’ insider trading must be among the entities considerations not only when they investigate and assess significant cybersecurity incidents, but also when they address underlying facts, consequences, and materiality issues of these incidents. Proper proactive and preventive actions, such as insider trading policies and procedures, that aim to protect the entity, investors, and markets against directors, officers, and other corporate insiders trading of material non-public information on a cybersecurity incident must be applied before and during the period following an incident and prior to the final dissemination of disclosure process.

Last but not least, SEC’s 2018 guideline correlated the obligation of disclosure on cybersecurity issues with Regulation FD and Selective Disclosure Companies, since under Regulation FD, *“when an issuer, or person acting on its behalf, discloses material nonpublic information to certain enumerated persons it must make public disclosure of that information.”* SEC reminds not only that it had adopted Regulation FD, but also insider trading is both unethical and illegal, and must be faced firmly. As it concerns selective disclosure of material nonpublic information related to cybersecurity, entities must guarantee that they comply with Regulation FD, so companies and all the persons acting on companies’ behalf should abstain from selectively disclosing material, non-public information regarding cybersecurity risks and incidents to Regulation FD relevant

individuals before proceed to the same information disclosure to the public. SEC expects from companies to establish the proper policies and procedures that not only safeguard non-selective disclosures of material non-public information related to cybersecurity risks and incidents, but also comply with Regulation FD obligation for simultaneous (for intentional disclosure as defined in the rule) or promptly (for non-intentional disclosure) public disclosures.¹³⁷

Following the February's 2018 Cybersecurity Disclosure issued Guidance, SEC, under the reality of many cyber-attacks and data breaches in public traded entities, had issued in April, 2018, its first ever action against an entity for a cybersecurity disclosure violation, the Accounting and Auditing Enforcement Release No. 3937 against Yahoo! Inc. and its successor, Altaba for misleading investors by failing to properly disclose its late 2014 data breach, which was considered back then as the world's largest data breach and had affected more than 500 million of Yahoo!'s user accounts, forcing Altaba, to pay a \$35 million penalty. The Securities and Exchange Commission recognized that the examined entity had conducted possible violations against Section 8A of the Securities Act of 1933 (the "Securities Act") and Section 21C of the Securities Exchange Act of 1934. The SEC identified that despite the fact that Yahoo! information security team tracked the breach data, which contained data like usernames, email addresses, phone numbers, birth dates, encrypted passwords, security questions and answers of the users' accounts, and had notified relevantly the entity's leading management team and legal department, though failed to properly examine the breach and disclose it with its investors, auditors and outside lawyers for more than two years, until the company was being bought off by Verizon Communications, Inc. The later used the breach in order to lower the acquisition price by 7.25 percent. For SEC, Yahoo! not only failed over a period for two-year period to develop the proper disclosures about the breach and its possible impact to business continuity capacities and legal consequences in its timely relevant quarterly and annual reports, but also when Yahoo! reported the occurrence of the breach, tried to undermine the situation by presenting a softer edition of the constituted risk and its potential negative influence. SEC in its settlement release also noticed that Yahoo! did not succeed in designing, implementing and maintaining the appropriate, suitable and more effective disclosure controls and procedures that would had guaranteed the timely evaluation and intensification of cyber-

¹³⁷ SEC (21/02/2018), Release Nos. 33-10459; 34-82746: *Securities and Exchange Commission 17 CFR Parts 229 and 249 on Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, <https://www.sec.gov/rules/interp/2018/33-10459.pdf> (last retrieved 25/06/2019).

incidents.¹³⁸ The Yahoo! data breach case was not the only SEC's first action against a public traded company on the grounds of cybersecurity concerns, that SEC supervises, but also the first derivative lawsuit¹³⁹ filed by shareholders in Delaware and California Courts against the entity's former top management team and Board of Directors, including former CEO Marissa Mayer, resulted to a settlement of \$29 million as fiduciary duties concerning the non-proper handling of its users' data during a series of cyberattacks taking place from 2013 until 2016, affecting more than three billion Yahoo! users. The relevant decision of Santa Clara's, California Superior Court, is historically and judiciary important because it is the first time that shareholders have been granted monetary damages after winning a derivative lawsuit regarding a cybersecurity issue, a data breach, since all the breach-related derivative lawsuits, despite being only a few, had been discharged by the courts or settled without any damages payment to the shareholders.¹⁴⁰

Yahoo!'s data breach case was not the only one that SEC had searched. In October, 2018, SEC issued an investigative report with the aim to bring more light to a concrete type of cyber-empowered fraud, the identity theft fraud where criminals impersonate an entity's executives, managements and vendors through spoofed email addresses and domains to manipulate members of the personnel in order to proceed to unauthorized payments. According to SEC nine public companies fell victims to these malicious practice, losing almost \$100 million over the period of weeks or months with the majority of the money resources never to be recovered and in some cases the frauds were being discovered only due to the probes of law enforcement authorities or external parties acts. The identity theft fraud took place in two ways: (a) the first one and less sophisticated concerned cyber-criminals pretend to be member of the executives management sending emails to mid-level finance personnel but with the authority to conduct fund transfers between accounts, demanding urgent payments to be executed to alleged foreign bank accounts in order to compensate well-known and established law firms for facilitating pressing merging

¹³⁸ SEC (24/04/2018), *Accounting and Auditing Enforcement Release No. 3937: Order Instituting Cease-And-desist Proceedings Pursuant To Section 8A Of The Securities Act Of 1933 And Section 21C Of The Securities Exchange Act Of 1934, Making Findings, And Imposing A Cease-And-Desist Order*, <https://www.sec.gov/litigation/admin/2018/33-10485.pdf> (last retrieved 25/06/2019).

¹³⁹ A derivative lawsuit as a legal mechanism provides the right to shareholders, as the owners of a company, to file a claim on the company's behalf and proceed to justice the entity's directors and management in order to be considered as accountable for their actions. Any payment provided by the lawsuit is not distributed among individual shareholders but goes in the corporation, due to the fact that the examined violation harmed only the company. ¹³⁹ Newman Craig A. (23/01/2019), *Lessons for Corporate Boardrooms From Yahoo's Cybersecurity Settlement*, <https://www.nytimes.com/2019/01/23/business/dealbook/yahoo-cyber-security-settlement.html> (last retrieved 25/06/2019).

¹⁴⁰ Newman Craig A. (23/01/2019), *Lessons for Corporate Boardrooms From Yahoo's Cybersecurity Settlement*, <https://www.nytimes.com/2019/01/23/business/dealbook/yahoo-cyber-security-settlement.html> (last retrieved 25/06/2019).



processes. Instead of the funds being transferred to law firms to support legal activities, the funds were transferred to be possessed by the cybercriminals accounts, who among others had asked from employees not to reveal the payments and keep them as a secret, and (b) the second way and more sophisticated, had to do with the hacking of the actual email accounts of the entities' foreign vendors by cybercriminals asking again from deceived employees into revealing to them the authentic purchase order and invoice sensitive data, and then hackers misled employees to replace the vendors' original payment information by giving them controlled by hackers bank accounts credentials. Despite the fact that SEC did not initiate any enforcement actions against the affected entities, the authority used this situation in order to issue a report that highlights the obligatory responsibility of public companies to develop, implement and maintain adequate systems of internal accounting controls, which must deliver judicious assurance about the existence of a mechanism of proper general or more specified authorization that grants access to only the right individuals, especially when it concerns handling of the company's assets and during the execution of its transactions. Moreover, SEC, point out that it was mostly companies' employees lack of adequate awareness, knowledge, understanding and failing to identify multiple red flags signaling possible cyber malicious fraudulent behaviors on companies' internal controls systems, that allowed hackers to penetrate and succeed in their goals. That is why, SEC had advised public companies to be further ready, conscious and aware of cyber threats when they design and maintain their internal accounting controls, so these controls to be adequate and effective.¹⁴¹

Many times, in this Master Thesis we had referred to *National Institute of Standards and Technology* (or NIST), the responsible body for setting standards nationwide, that had gain global respect and significance. NIST obligation to develop, establish and update nation's cybersecurity standards is based initially in February 2013 the Executive Order 13636 aims to improving Critical Infrastructure Cybersecurity, in December 2014 - Cybersecurity Enhancement Act of 2014 (P.L. 113-274) and in May 2017 Executive Order 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. Consequently, NIST issued its first edition of Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 in February 2014 and updated it by publishing *Cybersecurity Framework Version for Improving Critical Infrastructure Cybersecurity 1.1* in April 2018. The major differences between Version 1.0 and Version

¹⁴¹ SEC (16/10/2018), Release No. 84429: Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements, <https://www.sec.gov/litigation/investreport/34-84429.pdf> (last retrieved 25/06/2019).

1.1 are the following: (a) Version 1.1 has greater applicability, since it can be applied to all system lifecycle phases, (b) provides better guidance as it concerns supply chains' cybersecurity management, (c) includes new guidelines for effective self-assessment, (d) offers advice for more improved accounts regarding authorization, authentication and identity proofing, (e) contains guidance on emerging vulnerability information sharing, known as coordinated vulnerability disclosure and (f) encompasses better administratively handled updates as it concerns informative references¹⁴².

The Cybersecurity Framework in consisted of three major components: the *Tiers*, the Profile and the Core as the Image No 3 and 4 indicate respectively. Tiers, that is four in number, have a hierarchical order from the weakest to the strongest and aim to identify the level of cybersecurity protection and mitigation of cybersecurity risk factors in a company, an entity of any kind. Table No 3 presents the four tiers.

Image No 3: The Three Primary Components of Cybersecurity Framework Version 1.1	Table No 3: The four Tiers of Cybersecurity Framework Version 1.1		
	Tier 1: Partial	Refers to limited cybersecurity risk awareness Need for ad hoc risk management Deployment of low external participation and support especially concerning supply chain risks management and monitoring	
	Tier 2: Risk Informed	Initial increased level of awareness, but still no implemented related program Application of some risk management practices Informal external aid participation	
	Tier 3: Repeatable	Implementation of an entity-wide program Risk management formulation Receives official external party support, especially concerning supply chain risks management and monitoring	
	Tier 4 : Adaptive	Application of adaptive risk management practices A risk information and mitigation program is part of general entity's culture Actively shares data with employees and external stakeholders and partners, specialized supply chain risks management and monitoring actions	
	Image No 4: The Core Elements of Cybersecurity Framework Version 1.1		
			
NIST (2019), <i>Framework Documents</i> , https://www.nist.gov/cyberframework/framework (last retrieved 25/06/2019).			

¹⁴² Informative References provides clarification about the relationship between Framework Functions, Categories, and Subcategories and specific sections of other standards, guidelines, and best practices common among Framework stakeholders.

The *Profile* is produced with the evaluation on which Tier strategy the entity belongs to. Based on the Tiers analysis the Framework provides the current profile of the entity about its present state of cybersecurity risk appetite, risk tolerance and mitigation capacities and resources according to the organization structure, mission, targets and needs. Moreover, it provides the necessary information about the desired level of protection, about the target state of cybersecurity preparedness and cyber-safeguarding according again to the organization’s requirements, risk appetite and resources. After having the cybersecurity profiling of the entity the formulation of the proper and most applicable adaptive to this profile strategy must be implied based on the elements of *Core*, which is consisted of five *Functions*, which as the Image No 4 presents, that aim to identify, protect, detect, respond and recover, any cyber-related risk and vulnerability within an organization. These five Functions are consisted of 23 *Categories* and the Categories of 108 *Subcategories*, which are related to specific NIST and other institutions’ relevant Standards. Employee awareness and education programs and workshops and the obtaining of proper certifications results in the realization of the most functioning adaptive strategy based on Cybersecurity Framework Version 1.1. In Table No 4 we aim to present and provide a solid identification about the five functions and their 23 Categories.¹⁴³

<i>Table No 4: Analytical Presentation of the Five Core Functions and their Categories of Cybersecurity Framework Version 1.1</i>			
<i>Function Unique Identifier</i>	<i>Function</i>	<i>Category Unique Identifier</i>	<i>Category</i>
ID	IDENTIFY Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework.	ID.AM	ASSET MANAGEMENT The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy
		ID.BE	BUSINESS ENVIRONMENT The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
		ID.GV	GOVERNANCE The policies, procedures, and processes to manage and monitor the organization’s

¹⁴³ NIST (16/04/2018), *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.0416.2018.pdf> (last retrieved 25/06/2019).

	Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs		regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk
		ID.RA	RISK ASSESSMENT The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
		ID.RM	RISK MANAGEMENT STRATEGY The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
		ID.SC	SUPPLY CHAIN RISK MANAGEMENT The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.
PR	PROTECT Develop and implement appropriate safeguards to ensure delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event	PR.AC	IDENTITY MANAGEMENT AND ACCESS CONTROL Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
		PR.AT	AWARENESS AND TRAINING The organization’s personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity related duties and responsibilities consistent with related policies, procedures, and agreements.
		PR.DS	DATA SECURITY Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.
		PR.IP	INFORMATION PROTECTION PROCESSES AND PROCEDURES Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
		PR.MA	MAINTENANCE Maintenance and repairs of industrial control and information system components are performed consistent with policies and

			procedures.
		PR.PT	PROTECTIVE TECHNOLOGY Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
DE	DETECT Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events.	DE.AE	ANOMALIES AND EVENTS Anomalous activity is detected, and the potential impact of events is understood
		DE.CM	SECURITY CONTINUOUS MONITORING The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
		DE.DP	DETECTION PROCESSES Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.
RS	RESPOND Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident	RS.RP	RESPONSE PLANNING Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents
		RS.CO	COMMUNICATIONS Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).
		RS.CO	ANALYSIS Analysis is conducted to ensure effective response and support recovery activities.
		RS.MI	MITIGATION Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident
		RS.IM	IMPROVEMENTS Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
RC	RECOVER Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function	RC.RP	RECOVERY PLANNING Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.
		RC.IM	IMPROVEMENTS Recovery planning and processes are improved by incorporating lessons learned into future activities.
		RC.CO	COMMUNICATIONS Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of

	supports timely recovery to normal operations to reduce the impact from a cybersecurity incident		attacking systems, victims, other CSIRTs, and vendors)
<p>Source: NIST (16/04/2018), <i>Framework for Improving Critical Infrastructure Cybersecurity Version 1.1</i>, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (last retrieved 25/06/2019).</p>			

We must clarify that NIST’s Framework in both of its editions is a voluntary computer and information technology related guidance framework that offers to federal agencies and private sector’s entities, based on previous well established standards, guidelines, and practices¹⁴⁴, advice to organizations on how to deal, manage and minimize better and more effectively the impact and negative influence of cybersecurity risks and incidents, as well as to help organizations communicate and disclose with internal and external stakeholders, like internal and external auditors, all the necessary information and actions concerning the cybersecurity risks landscape. That is why, when is implemented by an entity must be customized according to the structure, threats, capacities and needs of every entity, and must take under serious account the entity’s communications channels, level of cybersecurity risks awareness, IT infrastructure, future business expanding and planning, operating facilities and units, senior executives style of governance and risk appetite. The Framework has a specialized applicability to critical infrastructure¹⁴⁵ entities,

¹⁴⁴ NIST’s Cybersecurity Framework can be applied together and in dialogue with a number of other cybersecurity standards, such as (a) National Initiative For Cybersecurity Education (NICE) Cybersecurity Workforce Framework, which aims to empower workforces cybersecurity skills and capacities and provides a detailed set of cybersecurity related work roles, tasks, and knowledge, skills, and abilities (KSAs) for mitigating cybersecurity risks, performing those actions, the connection with is recognized by NIST Special Publication 800-181, (b) DHS’s 2014 Critical Infrastructure Cyber Community (C3) Voluntary Program, a voluntary program to promote use of the NIST Framework and help critical infrastructure organizations improve their cybersecurity, (c) DHS’s Cyber Resilience Review (CRR), (d) NIST’s Cyber-Physical Systems (CPS) Framework, that aims to assist manufacturers create new CPS in order to enhance cybersecurity of smart systems that amplify the interconnection between physical and computational landscapes, (e) NISTIR 8228, Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, (f) Baldrige Cybersecurity Excellence Builder, and (g) U.S. Office of the Director of National Intelligence (ODNI). **Newhouse William, Keith Stephanie, Scribner Benjamin, Witte Greg** (08/2017), *NIST Special Publication 800-181: National Initiative For Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf> (last retrieved 25/06/2019). **NIST** (2019), *Questions and Answers*, <https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics#federal>, (last retrieved 25/06/2019).

¹⁴⁵ Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience (also known as PPD 21) of 2013 defines critical infrastructure as the “Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters”.

Cyber-security and Cyber-preparedness as a Necessary Part of the Auditing Process

such as infrastructure utilities, that provide energy and water, but also entities from sectors like transportation, financial services, communications, healthcare and public health administration, food and agriculture industries, chemical and other related facilities, dams, key manufacturers, emergency services and several others representatives across all industries spectrum.

The Framework can be deployed not only from large organizations, but also from smaller even the smallest. After all with its *Small Business Cybersecurity Corner*, together with Federal Trade Commission, the Small Business Administration, the National Initiative For Cybersecurity Education (NICE), National Cyber Security Alliance, the Department of Homeland Security, the CISA, supports small business efforts to combat cybersecurity risks and vulnerabilities. Moreover, with the issuance of its publication *NISTIR 7621 Rev. 1-Small Business Information Security: The Fundamentals* of November 2016, provides valuable guidance for small business among key cybersecurity concerns, with great auditing interest, such as access control, awareness and training; configuration management, contingency planning, identification and authentication, media protection, personnel security, physical and environmental protection, planning, system and communications protection, system and information integrity, and system and services acquisition that follow the five Core functions identify, protect, detect, respond and recover approach.¹⁴⁶

The Framework is especially applicable to U.S. federal agencies information system and infrastructures, since according to *Presidential Executive Order 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* of May 11, 2017, all federal agencies had maximum 90 days after the issued day of this Executive Order to provide a risk management report to the Secretary of Homeland Security and to the Director of the Office of Management and Budget (OMB), which will present the Agencies' action plan on the implementation of NIST's Cybersecurity Framework.¹⁴⁷ Furthermore, the Framework assist agencies on best integration of Agencies' existing risk management and compliance efforts and effective communication channels, not only regarding personnel preparedness but also for top executives and leadership adequate preparedness. The value of

The White House: Office of the Press Secretary (12/02/2013), Presidential Policy Directive - Critical Infrastructure Security and Resilience, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil> (last retrieved 25/06/2019).

¹⁴⁶ **NIST** (11/2016), *NISTIR 7621 Rev. 1-Small Business Information Security: The Fundamentals*, <https://csrc.nist.gov/publications/detail/nistir/7621/rev-1/final> (last retrieved 25/06/2019).

¹⁴⁷ **The White House** (11/05/2017), *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/> (last retrieved 25/06/2019).

the Framework in adequate management of federal information and information systems according to the **Risk Management Framework (RMF)**, in compliance with ***Federal Information Security Management Act of 2002 and its amendments (FISMA)***, provided by *NIST Special Publication 800-37 Revision 2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, offers comprehensive knowledge and guidance on (a) integration of privacy risk management processes, system life cycle security engineering processes, and supply chain risk management processes to general cybersecurity efforts, (b) complementary use of the Framework with RMF with the aim to effectively manage security and privacy risks in an entity's operations and assets, as well as individuals, other organizations, and the Nation, (c) offering a set of organization-wide RMF tasks, destined to prepare information system owners about the proper conduction of system-level risk management activities, with the aim to augment the effectiveness, efficacy, and cost-effectiveness of the established RMF, in order to fulfil an entity's missions and functions, and to ameliorate the communications lines about risk mitigation between senior leaders, managers, and operational personnel.¹⁴⁸ The methodology on effective implementation and assessment of the needed security and privacy controls in Federal Information and Organizations is based in the following NIST's documents: (a) *NIST Special Publication (SP) 800-53A revision 4- Assessing Security and Privacy Controls in Federal Information Systems and Organizations Building Effective Assessment Plans of 2014*, that provides research, guidelines, and outreach efforts upon the proper set of procedures that must be conducted during security controls and privacy controls assessments for enhancing deployed information system security, according to the technical findings, physical standards, guidelines and research of NIST's Information Technology Laboratory (ITL),¹⁴⁹ (b) *NIST Special Publication (SP) 800-39 Managing Information Security Risk: Organization, Mission, and Information System View of 2011*, provides structured, but flexible guidance for a cohesive, entity-wide program on applying, managing, assessing, and monitoring information security risk related not only to the protection of an entity's mission, functions, image, reputation assets, but also to the protection of individuals, other organizations, and the Nation due to operating and using of federal information systems, in compliance with other legislation, directives, policies, programmatic initiatives, or mission/business requirements and in complementary use with

¹⁴⁸ NIST (12/2018), *NIST Special Publication 800-37 Revision 2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf> (last retrieved 25/06/2019).

¹⁴⁹ NIST (12/2014), *NIST Special Publication 800-53A revision 4- Assessing Security and Privacy Controls in Federal Information Systems and Organizations Building Effective Assessment Plans*, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf> (last retrieved 25/06/2019).

an entity's comprehensive Enterprise Risk Management (ERM) program. SP 800-39 offers a description about the risk management process that must be deployed to federal organizations, but also to private sector entity's in optional and voluntary terms. This process is composed of (i) four distinct steps: Frame, Assess, Respond, and Monitor, (ii) three distinct organizational Tiers: Organizational, Mission/Business, and System level, and (iii) risk management roles and responsibilities within those Tiers, in order to succeed even in the high-level risk management cases. Within the SP 800-39 process, the Cybersecurity Framework can function as a tool of better provides communication and organization, with Framework's Profiles to serve as channels to express risk nature, obtain risk assessment information, investigate gaps, and structure a remedy response¹⁵⁰ and (e) *NIST Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations of 2016, amended in 2018*, aims to protect the absolutely important for federal agencies Controlled Unclassified Information (CUI) present in non-federal systems and organizations, which can have a significant impact in the ability of the federal government to successfully perform, the assigned missions and business operations deployed to them by law.¹⁵¹ *NIST Special Publication (SP) 800-171A on Assessing Security Requirement for Controlled Unclassified Information*, guides federal and non-federal organizations with the proper, flexible and prone to an entity's needs customization assessment tools, procedures, and a methodology for the effective assessment of the CUI security requirements, such as self-assessments; independent, and third-party assessments; or government-sponsored.¹⁵²

The *American Institute of Certified Public Accountants (CPAs)*, also known as AICPA, is the professional accountants association in the USA, established in 1887, responsible to establish the ethical standards for the accounting profession and also to create the applied in U.S. auditing standards, with members coming from a wide variety of entities: from private companies and nonprofit organizations to federal, state and local governments, as well as practitioners in a variety of industries, such as business and manufacturing, public practice, government, education, consulting, auditing, etc. As the largest members accounting association in the world, with more than 431,000 members in 130 countries and

¹⁵⁰ **NIST & Joint Task Force Transformation Initiative** (03/2011), *NIST Special Publication 800-39 Managing Information Security Risk: Organization, Mission, and Information System View*, <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf> (last retrieved 25/06/2019).

¹⁵¹ **Ross Ron, Dempsey Kelley, Viscuso Patrick, Riddle Mark, Guissanie Gary** (20/02/2018), *NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, <https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final> (last retrieved 25/06/2019).

¹⁵² **Ross Ron, Dempsey Kelley & Pillitteri Victoria** (June 2018), *NIST Special Publication 800-171A on Assessing Security Requirement for Controlled Unclassified Information* <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171a.pdf> (last retrieved 25/06/2019).

territories, AICPA develops and provides the Uniform CPA Examination system, additionally to offering specialty credentials for CPAs concerning personal financial planning, forensic accounting, business evaluation, information management and technology assurance.¹⁵³

As it concerns the cybersecurity domain, in 2017, AICPA presented its *Cybersecurity Risk Management Reporting Framework*, developed by AICPA's Assurance Services Executive Committee's (ASEC), Cybersecurity Working Group and the AICPA's Auditing Standards Board (ASB) following relevant requests from corporate leaderships. AICPA's Framework is a voluntary, market-based solution that aims to augment public trust in entities disclosures regarding the adequacy and effectiveness of their cybersecurity risk management programs, using the same language for cybersecurity risk management reporting —as US GAAP or IFRS apply for financial reporting. This robust reporting framework and its related criteria can be used not only from the management of an entity, but also from CPAs, since it can be applied in order to perform an examination-level attestation engagement, also known as a *System and Organization Controls (SOC) for Cybersecurity examination* that will address the needs in a wide spectrum of current and potential report users looking for reliable and valuable information on an entity's cybersecurity actions and preparedness. AICPA had developed three different types of System and Organization Controls or SOC, SOC 1®, SOC 2® and SOC 3®, based on AICPA, Professional Standard- SSAE No. 18, Attestation Standards: Clarification and Recodification, for CPAs and auditors, engaged to evaluate and report of entities controls. A SOC 1® engagement examines the influence set by the entity controls to the issued by entity financial statements, by describing the entity's service organization's services and system management as it concerns the designed suitable appropriateness and effective operability of the controls to succeed in established by management control targets. The report by the service auditor provides a fair professional opinion upon the suitability and functional capacities of these controls according to the results of the service auditor's tests. A SOC 2® engagement examines the influence of set by the entity controls to security, availability, processing integrity confidentiality, or privacy requirements that an entity must fulfil, by describing the entity's service organization services and system management as it concerns the designed suitable appropriateness and effective operability of the controls to succeed in providing reasonable assurance that the service organization's obligations and system requirements must fulfilled, according to the applicable trust services criteria. Again, the report by the service auditor provides a fair professional opinion upon the suitability and

¹⁵³ AICPA (2019), *About the AICPA*, <https://www.aicpa.org/about.html>

functional capacities of these controls according to the results of the service auditor's tests. A SOC 3® report is just like a SOC 2®, meaning both are based to Trust Services Criteria, with the difference that SOC 3® report can be freely distributed and disclosed to the public, while SOC 1® and SOC 2® reports are disclosed only to the entity's management, that proceed to the relevant engagement.¹⁵⁴

But what is exactly AICPA's approach on SOC for Cybersecurity examination and reporting? AICPA's Framework for reporting on an entity's cybersecurity risk management program demands from management to formulate concrete information about the entity's cybersecurity risk management program and from the CPA to examine and report on that information according to AICPA's attestation standards. The subsequent cybersecurity report must provide information about three key areas: (a) *Management's description*: which contains the leadership's view on the entity's cybersecurity risk management program (this is known as the "Description") and provides data about (i) the entity's way to identify its most sensitive information, (ii) the ways deployed by entity to manage cybersecurity risks and threats, and (iii) the main security policies and processes the entity applies to defend the entity's data assets against those threats. The Management's description offers a detailed background the report users, such as external auditors, investors, stakeholder, authorities, need to comprehend the presented by management assumptions, and by the CPA's opinion, about the effectiveness and functionality of the cybersecurity controls among the entity's cybersecurity risk management program. (b) *Management's assertion*: that delivers management's statement about the effectiveness of the "Description", the description's criteria and implemented controls of the entity's cybersecurity risk management program on achieving the entity's cybersecurity goals based on the applied control criteria. AICPA develops control criteria since 1997 that evaluate and report controls over the security, availability, processing integrity, confidentiality, and now also processing integrity privacy over information and systems, by presenting a revised edition of its *Trust Services Criteria for Security, Availability, and Confidentiality* (known as trust services criteria) in 2017 entitled *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy*, that can be used by CPAs, that provide advisory or attestation services with the aim not only to appraise the applied by an entity cyber risk management program controls cyber risk management program, or for relevant SOC 2® and SOC 3® audit services reporting engagements, but also to assist the management due to its flexibility in examining the effective and suitable appropriateness in

¹⁵⁴ AICPA (2019), *SOC for Service Organizations: Information for CPAs*, <https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/cpas.html> (last retrieved 25/06/2019).

construction and operability of their controls. However, management can use other criteria, such as those provided by the NIST Critical Infrastructure Cybersecurity Framework and ISO 27001/27002, as long as they are appropriate and comply with the AICPA's attestation standards. (c) *Practitioner's opinion*: the final element of the Framework is referring to the CPA's opinion about the correctness and adequacy of the description and about the effectiveness of controls of the entity's cybersecurity risk management program. Summarizing, the Framework consisted of three types of supportive resources for proper cybersecurity risk management reporting: (i) the description criteria, used by management to present the entity's cybersecurity risk management program in a reliable way and can be used by CPAs report on management's description and (ii) the control criteria, used by CPAs that offer advisory or attestation services to estimate and report on the effectiveness of the client's program controls and (iii) the Attestation Guide called *Reporting on an Entity's Cybersecurity Risk Management Program and Controls*, that provide guidance on how to assist CPAs in proper examination and reporting on an entity's cybersecurity risk management program.¹⁵⁵

AICPA offers, also, to its members *Private Companies Practice Section (PCPS) Exploring Cybersecurity Toolkit*, that provides to firms and entities important practical tools, such as learning resources, staff training tools, beneficial tools that address an entity's client's needs for high-quality cybersecurity services, concerning (a) understanding, recognizing and analyzing cybersecurity concepts and recognizing and analyzing cybersecurity issues and threats, (b) implementing cybersecurity considerations by safeguarding sensitive information and constructing a solid cybersecurity practice and (c) reporting cybersecurity controls and issues. More precisely, as it concerns (a) understanding cybersecurity, the Toolkit offers (i) *AICPA's Introduction to Cybersecurity Guide*, that gives a general indication of cybersecurity, the reasons why CPA firms and their clients are at risk, offers best practices that firms must apply, clarifies cyber insurance aspects and can be used as a starting point for assisting a CPA firm's clients cybersecurity considerations, (ii) the *Cybersecurity Learning Matrix*, that provides advice about the great variety of existed cybersecurity frameworks, crucial regulations influencing modern cybersecurity compliance, reference resources, recognized by the practice and sector, useful sources concerning security intelligence and leadership capacities, (iii) the *Service Opportunity*

¹⁵⁵AICPA (26/04/2017), *AICPA Unveils Cybersecurity Risk Management Reporting Framework*, <https://www.aicpa.org/press/pressreleases/2017/aicpa-unveils-cybersecurity-risk-management-reporting-framework.html> (last retrieved 25/06/2019). AICPA (2018), *Cybersecurity risk management reporting fact sheet*, <https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/cybersecurity-fact-sheet.pdf> (last retrieved 25/06/2019).

Grid, a spreadsheet that offers plenty cybersecurity related service opportunities, guides professionals to cybersecurity advisory services, and connects the data provided by users with possible proper engagement choices, (iv) the *Cybersecurity PowerPoint – Internal*, that provides a template to CPA firms in order to educate and train their staff on cybersecurity basics and on how they must approach their clients' cybersecurity issues and (iv) the *Client Cybersecurity FAQs*, a documents that provides answers to the most important and demanding cybersecurity questions that a clients can set for its CPA firm, next to encompass useful information about how to brand a CPS firm and keep the firm's clients updated. (b) As in concerns implementing cybersecurity considerations, the Toolkit offers (i) the *Cybersecurity Service Implementation Checklist*, this step-by-step guidance checklist provides assistance in the implementation and application of cybersecurity service offerings by CPA firm, (ii) the *Client Assessment Template Formulas*, that offers a variety of cybersecurity service prospects that CPA firms can offer to their client's about how to enhance and administer better their current status of cybersecurity protection, and (iii) the *Cybersecurity Services Introduction Letter*, this letter template offers not only a customizable template on how CPA firms can best initiate a fruitful discussion with their clients regarding their cybersecurity concerns that are significant for them, but also on how the CPA firms can introduce to their clients any novel cybersecurity service choices and offerings. (c) As it concerns reporting the Toolkit offers the *System and Organization Controls for Cybersecurity: Engagement Overview*, this new edition of SOC, provides to CPA firms further assistance as it concerns how entities must best report and communicate their cybersecurity policies.¹⁵⁶

What is more, AICPA offers a specialized tool for *Chartered Global Management Accountant (CGMA)*, the *CGMA Cybersecurity Risk Management Tool*, that assist not only the engaged entities but also their vendors, suppliers and other related stakeholders and providers, to manage, treat and monitor the risks that cybersecurity threats encompass and how to best react and deal with potential cybersecurity breaches. The tool provides the following:

(a) deep understanding on most crucial cybersecurity risks, like malwares, ransomware, botnets malvertising, phishing, application attacks, etc., and the costs provoked by these risks, such as loss of business production or revenue, harm on reputation and brand name and value, loss of customers, legal consequences, including fines, lawsuits,

¹⁵⁶ AICPA (2019), *Exploring Cybersecurity*, <https://www.aicpa.org/interestareas/privatecompanies/practicesection/qualityservicesdelivery/exploring-cybersecurity.html> (last retrieved 25/06/2019).

settlements costs and negative impacts for sensitive sectors like health care records exposed after breaches,

(b) promotes a protective system, based on the above-mentioned Cybersecurity Risk Management Reporting Framework, consisted of the established by management cybersecurity objectives that deal with cybersecurity risks and threats, that must fulfil the description criteria of availability, confidentiality, data integrity and processing integrity, cybersecurity risks and threats and is consisted of three types of controls: (i) protective controls, for proper identification, authentication, authorization & verification and secrets protection for stored and for in transit sensitive data; (ii) detective controls, for proper event monitoring, intrusion detection and prevention systems, threat monitoring and users' reporting; (iii) responsive controls, through Computer Incident Response Teams (CIRTs- also known as Computer Security Incident Response Teams -CSIRTS) these controls aims to reduce losses, to support investigations when it is necessary form law enforcement and forensic authorities, to provide decision-making assistance during an incident happening and actions planning, and to enable crisis communications and disclosure with customers, law enforcement bodies, media, general public, etc.,

(c) provides specific applied cybersecurity options, such as: (i) centralized management, for desktops, laptops, mobile devices, network configuration, network firewalls, application and antivirus and endpoint products; (ii) centralized monitoring consisted of event logging and aggregation actions, security information and event management (SIEM) monitoring systems, (iii) modern Security Operations Center (SOC) functions, such as incident response team, threat intelligence team, hunt team and insider threat team, (iv) forensic analysis for tracking and examining the traces of a breach and in is consisted of three primary components: the first is system-level analysis that inspects system components for any configuration changes and established fake accounts created that enable without proper authorization services, the second is storage analysis in databases and cloud environments for deleted and overwritten files, and the third is network analysis, which collects and analyses data concerning network traffic and content, (v) malware analysis, for spotting any unauthorized software installation, by applying reverse engineering and decompilation and disassembly techniques; (vi) penetration testing, in order to shandle weak points and vulnerabilities in software systems before opponents discover them and take advantage of them, and is conducted through network discovery, vulnerabilities probing and exploiting; (vii) software security, which is the creation of resilient and robust to attacks software by applying the three major software security tiers: Tier 1, enables successful blocking of attacks, Tier 2, assists alert security (SIEM) preparedness about attacks by

providing critical information, and Tier 3, enables evasive actions, like the protection of sensitive data (i.e., credit-card information, and accounts' locking capacities). Software security is realized through design review, that inspects design or architectural weaknesses (like customer records, intellectual property, payment data, etc., code review and security testing).¹⁵⁷

AICPA provides the following a number of important cybersecurity certifications for CPA:

- (a) **Cybersecurity Practical Applications Certificate**, that enhance the ability of its holder to apply effectively a trustworthy cybersecurity risk management program, enrich its sound cyber hygiene implementation skills for both organizational and personal levels. The Certificate demonstrates the ability of proper determination on the most suitable way to prevent and respond to frequent cybersecurity threats, of useful identification of tools and processes for good cyber hygiene, of recognition of cybersecurity best practices and of additive identification of crucial components of an effective cybersecurity risk management program (CRMP). AICPA provides a relevant training course that through case studies and actual real-life conditions assist the learners in their cyber-loss mitigation and cyberattacks prevention competences and their proper respond skills to occurring attacks.¹⁵⁸
- (b) **Cybersecurity Fundamentals for Finance and Accounting Professionals Certificate**, this Certificate enhances confidence for proper cybersecurity strategic decision-making to non-IT professional, since it is specially designed for finance and accounting professionals in public accounting, business and industry to grasp capacity skill in order to protect CPA firms and their clients from cyber threats. The holders of this Certificate are able to communicate knowledgeably about cybersecurity risks to internal teams and external clients, to conduct sensible strategic decisions regarding cybersecurity investments, and to have a better clarification and a deeper comprehension on AICPA's cybersecurity risk management reporting framework.¹⁵⁹
- (c) **Cybersecurity Advisory Services Certificate**, this Certificate is specially designed for CPAs in public accounting that provides trusted advisory services in order to assist the entities to track cybersecurity weaknesses, to recognize potential risks and to be able

¹⁵⁷ AICPA (May 2017), *CGMA Cybersecurity Risk Management Tool*, <https://www.cgma.org/content/dam/cgma/resources/tools/downloadabledocuments/cgma-cybersecurity-tool.pdf> (last retrieved 25/06/2019).

¹⁵⁸ AICPA (2019), *About the Cybersecurity Practical Applications Certificate Program*, <https://certificates.aicpastore.com/certificates/cybersecurity-practical-applications> (last retrieved 25/06/2019).

¹⁵⁹ AICPA (2019), *About the Cybersecurity Fundamentals for Finance and Accounting Professionals Certificate Program*, <https://certificates.aicpastore.com/certificates/cybersecurity-fundamentals-finance-accounting-professionals> (last retrieved 25/06/2019).

to present sound advice regarding an entity's information and NHS systems. The holders of this Certificate will enhance their skills upon: the nature and kinds of potentially offered cybersecurity advisory services, the major components and aspects for each one of those advisory service, and the essential capacities that a cybersecurity advisor must possess to best perform the advisory services.¹⁶⁰

- (d) **SOC for Cybersecurity Certificate**, is specially designed for CPAs in public accounting since it provides the basis for better attestations engagement performance regarding the evaluation and reporting of an entity's cybersecurity risk management program, according to AICPA's cybersecurity risk management reporting framework.¹⁶¹
- (e) Among AICPA's specialty credentials but with cybersecurity interest is the **Certification on Information Technology Professional (CITP)** that collaborates the finance accounting aspect with technology, demonstrating its holders particular skills, expertise and experience to understand, to evaluate the impact and to proper report in business areas, like (a) information security and cyber risks, (b) business intelligence, data management and analytics and (C) IT governance, risks and controls.¹⁶²

AICPA with its ***Cybersecurity Resource Center*** aims to assist CPA firms companies, organization and businesses, to identify and protect themselves from cybersecurity threats, attacks and risks, by providing resources on risk assessment and adopting proactive actions to defend their data and information systems. Moreover, AICPA provides assistance and cybersecurity resources to CPAs firms offering advisory or assurance services. More precisely, as it concerns CPAs firms offering cybersecurity and information technology protection advisory to their clients aiming to identify and deal with potential internal cybersecurity risks by offering proactive steps to protect valuable client and customer data. Information, AICPA provides to these CPAs with an IT skillset, who often hold the Certified Information Technology Professional (CITP) credential, and are prone to advise clients on cybersecurity assurance issues the following resources:

- ***Information Technology and Assurance Management***: through its Information Technology and Assurance Management (IMTA) Section and its IMTA Cybersecurity Task Force, that create useful cybersecurity advisory resources (such as the

¹⁶⁰ AICPA (2019), *About the Cybersecurity Advisory Services Certificate Program*, <https://certificates.aicpastore.com/certificates/cybersecurity-advisory-services> (last retrieved 25/06/2019).

¹⁶¹ AICPA (2019), *About the SOC for Cybersecurity Certificate Program*, <https://certificates.aicpastore.com/certificates/soc-for-cybersecurity> (last retrieved 25/06/2019).

¹⁶² AICPA (2019), *Credentials: CITP Overview*, <https://www.aicpa.org/membership/join/credentials.html?tab-1=4> (last retrieved 25/06/2019).

Top Cybercrimes whitepaper), AICPA supports CPA, like CITPs and other IT professionals, in their cybersecurity advisory pathway to their clients.

- *Private Companies Practice Section (PCPS) Exploring Cybersecurity Toolkit* as we described it in previous pages.
- *Cybersecurity Risk Management Reporting Framework*, the Framework had been analyzed in previous pages.
- *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy*, as we presented them in previous pages, and
- *Cybersecurity Advisory Services Certificate*, as we also presented it in previous page.¹⁶³

As it concerns CPAs firms offering cybersecurity and information technology protection assurance services and is based on System and Organization Controls (SOC) for Cybersecurity examination guidance, AICPA provides the following resources:

- *System and Organization Controls (SOC) for Cybersecurity examination* landscape as we described it previously,
- *AICPA Guide on Reporting on an Entity's Cybersecurity Risk Management Program and Controls*, as we presented it previously,
- *SOC for Cybersecurity Certificate*, as we presented it previously,
- *Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program (description criteria)*, as we presented them in previous pages,
- *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy (control criteria)*, as we presented them in previous pages,
- *SSAE No. 18, Attestation Standards: Clarification and Recodification* (which includes AT-C section 105, Concepts Common to All Attestation Engagements, and AT-C section 205, Examination Engagements), mentioned previously while presenting AICPA three different types of System and Organization Controls or SOC, SOC 1®, SOC 2® and SOC 3®. This Standards is used by CPAs that evaluate and report on an entity's cybersecurity risk management program according to the attestation examination described in the above-mentioned Guide on Reporting on an Entity's Cybersecurity Risk Management Program and Controls,
- *SOC for Cybersecurity Brochure*, a useful tool on how CPAs should co-brand and present their SOC for cybersecurity services, and

¹⁶³ AICPA (2019), *Cybersecurity Resources for CPAs Providing Advisory Services*, <https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/cybersecurity-resources-for-cpas-providing-advisory-services.html> (last retrieved 25/06/2019).

- *Non-attest Services FAQ Document*, created by AICPA Professional Ethics Division, that provides answers to frequently asked questions (FAQs) regarding the issue of independence for non-attest cybersecurity services.¹⁶⁴

Sarbanes-Oxley Act of 2002 act is the legal basis for the creation of **Public Company Accounting Oversight Board or PCAOB**, the USA's institution destined to oversee register public accounting firms that perform audits of public companies with the aim to safeguard the need and interests of investors and public for informative, accurate, and independent audit reports. From 2010, through an amendment to SOX Act the **Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010**, PCAOB's mandate includes also the overseeing of brokers and dealers registered with the Securities and Exchange Commission audits. PCAOB's primary duty is to oversee the right financial reporting of 7,659 public companies (\$43.2 trillion in global market capitalization), of approximately 410 registered firms perform audits and of more than 3,350 SEC-registered broker-dealers, in 2018. The other three duties of PCAOB are (a) the creation, development and adoption of relevant attestation, quality control, ethics, and independence standards, (b) the inspection of registered audits firms and their quality control systems and (c) the investigation and potential disciplinary action against registered public accounting firms and their associated employees for violating relevant laws, rules, or professional standards. PCAOB is governed by a five members Board, the chairman of which is appointed for five years by the SEC, following the consultation with the Board of Governors of the Federal Reserve System and the Secretary of the Treasury. SEC's role in PCAOB is crucial since is the overseeing authority over the PCAOB activities, and among other approves PCAOB's Board rules, standards, and its budget. In PCAOB are registers approximately 1,900 public accounting firms located in 85 countries around the world, with about 600 of those registered firms is responsible for auditing more than 12,000 issuers entities that must issue financial statements and disclose them in SEC. PCAOB performs research upon economic matters and risks analysis and promotes domestic and international cooperation with other stakeholders and regulators in order to enhance auditors' capacities.¹⁶⁵ PCAOB had recognized the influence of technology and technology issues in proper financial and auditing reporting and with the inclusion of technology based tools, such as data analytics in planning, executing, performing and reporting audits, is assessing the need for including relevant considerations in its guidance, standards and regulatory activities. Despite the fact

¹⁶⁴ AICPA (2019), *SOC for Cybersecurity: Information for CPAs*, <https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/cybersecurityforcpas.html> (last retrieved 25/06/2019).

¹⁶⁵ PCAOB (2018), *Strategic Plan 2018-2022*, <https://pcaobus.org/About/Administration/Documents/Strategic%20Plans/PCAOB-2018-2022-Strategic-Plan.pdf> (last retrieved 25/06/2019).

that, PCAOB recognizes that PCAOB professional standards and PCAOB quality control standards are not preventing but neither clearly encourage firms to use technology-based tools, there is a significant need for better understanding of how technology-based tools, such as data analytics, can assist auditors not only to identify the risks related with the use of technology, such as cybersecurity concerns, but also to properly assess these risks resulting in the production of possible material misstatement in an entity's financial statements and default audit engagements and performances.¹⁶⁶

The establishment of the *Data and Technology Task Force*, which member coming from academia, CFA Institute, and the most important audit firms worldwide, such as Baker Tilly Virchow Krause, LLP, PricewaterhouseCoopers LLP, Ernst & Young LLP, Brown Brothers Harriman & Co., Deloitte & Touche LLP, Grant Thornton LLP and SEC's observing members AICPA, provides further comprehensions to PCAOB staff, concerning the use of technology-based tools, such as data analytics and other emerging technologies, by auditors and other people preparing audits.¹⁶⁷

Moreover, *June's 2018 PCAOB's Standing Advisory Group (or SAG) panel meeting*, was dedicated to the discussion of cybersecurity issues and their potential impact and their implications in proper financial reporting and auditing, due to the fact that cybersecurity issues remain a matter of increasing apprehension for public companies, investors, audit committees, regulators, auditors, and other related professionals. The panel's briefing publication not only mentioned recent cybersecurity incidents and data breaches and their impact as well as indicated recent governmental and audit sectoral guidance, such as those we described previously by SEC, NIST, AICPA, assuring PCAOB's capacity in monitoring cybersecurity developments and considerations concerning auditors' responsibilities and performances during an audit of the financial statements and the internal controls over financial reporting (known also as ICFRs), including the auditors' reaction and response to a cyber incident. Moreover, the panel took under consideration that PCAOB Inspections staff continues not only to review but also to develop further insight about the way firms evaluate the cybersecurity related risks of material misstatement and any possible impact of them to the related ICFRs and financial statements, due to the fact that ***PCAOB Audit Standard 2110 on Identifying and Assessing Risks of Material Misstatement*** demand from an auditor to obtain a reliable view and understanding of the entity's information system related to

¹⁶⁶ PCAOB (2019), *Changes in Use of Data and Technology in the Conduct of Audits*, <https://pcaobus.org/Standards/research-standard-setting-projects/Pages/data-technology.aspx> (last retrieved 25/06/2019).

¹⁶⁷ PCAOB (2019), *Data and Technology Task Force*, <https://pcaobus.org/Standards/research-standard-setting-projects/Pages/Data-Technology-Task-Force.aspx> (last retrieved 25/06/2019).

financial reporting, such as information technology (IT) systems and applications and how IT can affect the trustworthy creation of financial statements. The Panel, also, referred to a *2016 Inspection Staff Brief* on cybersecurity incidents according to which even though the cybersecurity incidents were not strictly associated to the risks of material misstatement in an entity's financial statements, and disclosures, neither resulted in an identification of material weaknesses in the entity's ICFR, the risks endure and perhaps in the near future cyber-attacks may impose a greater impact for an issuer's financial statement reporting process, an emerging risk that according to Inspections staff interpretation demands continuing focus.¹⁶⁸

The next year's *November 2017 Staff Inspection Brief* contained more information gathered from 2016 inspection cycle concerning not only inspections staff commitment to review and gather information regarding firms' attitudes towards information technology risks in audits, but also inspections staff focusing in acquiring a deeper understanding of use of data analytics from auditors during audits, since the used by audit entities software audit tools (SATs) characterized by either increased differentiation, either extended customization, either development from scratch. SATs, due to their performance effectiveness and efficiency, are employed either to perform substantive audit procedures, either for conducting risk assessments, such as (a) testing manual journal entries for potential fraud identification, (b) supporting auditor's evaluation on the appropriate sample size for testing an amount of high-risking transactions, as well as other complete populations of transactions important for accounting and financial reporting, (c) supplementing auditor's examination on investment securities pricing, (d) monitoring procedures and firm quality controls concerning the creation and application of SATs in audit practice, (e) improving internal training and/or audit firm's aid resources on using certain audit tools, and (f) evaluating the efficacy of segregation of duties in the examined entity. PCAOB's inspections team acknowledged that (a) an important number of audits trails in 2016 contained the use of at least one SAT, (b) despite the abundant investment from some companies in novel and more sophisticated SATs, containing even the use of artificial intelligence, audit firms did not include these tools in their audit examinations, (c) audit companies must continuously examine not only the effective operability of SATs in auditing providing trustworthy assurance systems of quality control, but also their proper application by audit teams, as well as to resourcefully assist auditors in their obligation to comply with relevant applied auditing standards, and (d) that the inspections staff must not stop to

¹⁶⁸ PCAOB (5-6/06/2018), *Standing Advisory Group Meeting: Panel Discussion*, <https://pcaobus.org/News/Events/Documents/Cybersecurity%20Briefing%20Paper.pdf> (last retrieved 25/06/2019). PCAOB (April 2016), *Staff Inspection Brief: Vol. 2016/1*, <https://pcaobus.org/Inspections/Documents/Inspection-Brief-2016-1-Auditors-Issuers.pdf> (last retrieved 25/06/2019).

develop and conduct practices, that appraise and comprehend the implemented by firms' the proper assurance controls, and SATs empirically involvement data investigation, assist in achieving audit objectives. Moreover, the Brief contains a section referring to cybersecurity, since some high profile and impactful data breaches had brought the attention of regulatory authorities into modern cybersecurity risks. The Brief not only repeated June 2018 SAG's panel meeting commitment to review and better understand audit firms cybersecurity risks and their potential impact to relevant ICFR in producing material misstatements in financial statements, but also referred to main conclusion of Inspections staff Brief of 2016, as we presented in previous page, meaning that cybersecurity incidents had not provoked material misstatement until so far, but the risk is considered high in future. That is why, the Brief considers as important for auditors to have a good understanding about the potential results of material misstatement to the financial statements and to cybersecurity risks, and make the necessary modifications to their approaches about audit planning, in order to include from now on tests in IT general controls. Moreover, for any cybersecurity incident takes place during the audit performance period, auditors must examine possible effects and implications of this incident not only in the creation of financial statements and disclosures, but also on ICFRs. That is why, inspections staff intends to keep being updated and to proper process knowledge in these spheres.¹⁶⁹

The potential increased use of emerging technological opportunities and capacities in auditing performances and the recognition of disruptive role of technological innovations not only in the size and nature of acquiring data by auditors, but also in the development of their opinion, constitutes the enhancement of technological strong skills in auditors a pure necessity according to *PCAOB's Strategic Plan for 2018-2022*. The use of technological advancements, such as data analytics, for improving audit quality and decrease audit performing deficiencies, but also their potential cybersecurity chimeric and malicious effect are present in the three out of five major goals and their sub-objectives set by this Strategic Plan: Goal One, Drive improvement in the quality of audit services through a combination of prevention, detection, deterrence, and remediation, Goal Two, Anticipate and respond to the changing environment, including emerging technologies and related risks and opportunities, and Goal Four, Pursue operational excellence through efficient and effective use of our resources, information, and technology.¹⁷⁰

¹⁶⁹ **PCAOB** (November 2017), *Staff Inspection Brief: Vol. 2017/4*, <https://pcaobus.org/Inspections/Documents/inspection-brief-2017-4-issuer-results.pdf> (last retrieved 25/06/2019).

¹⁷⁰ **PCAOB** (2018), *Strategic Plan 2018-2022*, <https://pcaobus.org/About/Administration/Documents/Strategic%20Plans/PCAOB-2018-2022-Strategic-Plan.pdf> (last retrieved 25/06/2019).

US Cybersecurity and Infrastructure Security Agency (best known as CISA), that belongs *Department of Homeland Security* (DHS), was established in November 2018 by **Cybersecurity and Infrastructure Security Agency Act of 2018** with main responsibility to provide to critical infrastructure systems of USA proper protection against physical, digital, man-made, technological, and natural threats, a task achieved by succeeding effective and productive cooperation and coordination between a great number of governments institutions and private entities. The protection of critical infrastructures in the country derives from **Critical Infrastructure Information Act of 2002** and its *Protected Critical Infrastructure Information (PCII) Program* together with 6 Code of Federal Regulations (CFR) part 29, *Procedures for Handling Critical Infrastructure Information*. Final Rule (published in the Federal Register on September 1, 2006) had established a harmonized process about receiving, validating, processing, storing and marking voluntarily reports from private sector (operators and owners) upon protection of infrastructure information that must be submitted to the DHS with the information shared with interested government bodies without compromising the integrity of the contained sensitive data due to exposure.¹⁷¹ The country had prior to the creation of CISA another institutional body to supervise the implementation of Critical Infrastructure Information Act of 2002 the National Protection and Programs Directorate (NPPD), the predecessor of CISA.

More precisely, CISA offers protection from a variety of cyber threats through its Cybersecurity Division (CSD). CISA's CSD primary responsibilities are: (a) the direction of endeavors for the protection of the so called federal ".gov" domain of civilian government networks, and (b) the cooperation with the private sector entities, the ".com" domain, with the aim to intensify the security of critical networks.¹⁷² Moreover, CISA offers:

(a) *comprehensive cyber protection*, through its **National Cybersecurity and Communications Integration Center (NCCIC)**, CISA provides 24/7 constant support and guidance not only to governmental authorities (federal , state, local, tribal and territorial) but also to private entities and to international partners as it concerns cybersecurity knowledge, awareness, incident response and cyber defense capacities. Through cybersecurity protection tools, like (i) the *Suspicious Activity Reporting Tool* of DHS that allows critical infrastructure partners to report to government any suspicious, and irregular event and activity through a harmonized process that permits reliant data sharing and efficient

¹⁷¹ **CISA** (06/07/2009), *Protected Critical Infrastructure Information (PCII) Program*, <https://www.cisa.gov/pcii-program> (last retrieved 25/06/2019).

¹⁷² **CISA** (23/07/2007), *Cybersecurity Division Mission And Vision*, <https://www.cisa.gov/cybersecurity-division> (last retrieved 25/06/2019).

response¹⁷³, (ii) the *National Cyber Awareness System (NCAS)*, which offers through its subscription service important resources and information about cyber threat and advices, and (iii) the *Hunt and Incidence Response Teams (HIRT)*¹⁷⁴, that provide free on-site incident response diagnostics, cyber incident identification, assistantship, assessment, reporting and follow-up, CISA defends the essential networks of federal and private significance.

(b) *infrastructure resilience and risk assessment*, through its ***National Risk Management Center***¹⁷⁵, CISA enhance national and private infrastructure security and resilience by coordinating public-private partnerships, by providing education and training and by offering technical aid and assessment to federal and private owners and operators

(c) *emergency communications security and providing*, through education, training, coordination, tools, and advice CISA improves safety of key communications in the full governmental extend and help collaborators and stakeholders to achieve an effective level of capacity in their emergency communication protection. Moreover, together with stakeholders all over the nation, supports and conducts nationwide involvement to raise the capabilities of emergency response providers and related governmental officers in durable communication even in cases of destructive events, such as national disasters, or provoked by humans disasters, like terrorists attacks.¹⁷⁶

(d) establishing *Infrastructure Protection Gateway* (or IP Gateway) together with DHS through its Infrastructure Security Division (ISD) that aims in the coordination of efforts between governmental institutions (federal, state, local, tribal, territorial), private sector and other stakeholders in national level to safeguard country's critical infrastructure from all natural and human provoked threats by administrating risks and boosting resilience through assessing opportunity costs and adjustment expenses. IP Gateway not only permits better informed and proper cost evaluation and decisions, but also functions as the single channel for DHS partners to access into a wide variety of cohesive infrastructure protection

¹⁷³ **CISA** (07/12/2012 original edition, 06/03/2019 revised), *Suspicious Activity Reporting Tool*, <https://www.cisa.gov/suspicious-activity-reporting-tool> (last retrieved 25/06/2019).

¹⁷⁴ Based on the ***DHS Cyber Hunt and Incident Response Teams Act of 2019***. **Congress** (31/01/2019), Text: S.315 — 116th Congress (2019-2020): DHS Cyber Hunt and Incident Response Teams Act of 2019, <https://www.congress.gov/bill/116th-congress/senate-bill/315/text> (last retrieved 25/06/2019).

¹⁷⁵ CISA's National Risk Management Center offers a comprehensive total-risks analysis together with stakeholders from private and public spheres through the Identify, Analyze, Prioritize and Manage approach in order to spot and deal with material and impactful risks and hazards USA critical infrastructure can face for critical infrastructure nationwide. **CISA** (2019), *What Does CISA Do?*, <https://www.cisa.gov> (last retrieved 25/06/2019).

¹⁷⁶ **CISA** (2019), *What Does CISA Do?*, <https://www.cisa.gov> (last retrieved 25/06/2019).

Cyber-security and Cyber-preparedness as a Necessary Part of the Auditing Process

tools and useful data that permits faster vulnerabilities and risk identification and assessment, incident response and preparedness homeland security associates.¹⁷⁷

(e) *providing systematic methodical, and constant evaluation of an entity's security status*, through its *Cyber Security Evaluation Tool (CSET®)*, a desktop software instrument that provides guidance to asset owners and operators through a step-by-step procedure, which appraise industrial control system (ICS) and information technology (IT) network security practices of the entity. Moreover, the users can assess their own cybersecurity position by using many well-established federal and sectoral standards and recommendations.¹⁷⁸ CISA additionally *offers proactive support for Industrial Control Systems (ICS)*, which are all the mechanism, NHS systems and controls that used by entities in order to conduct and automate industrial processes and operations.¹⁷⁹

Among the organizations that provide guidance in cybersecurity auditing affairs in United States of America, and influence the audit practice and profession in national and international level, is the based in Washington DC, *Center for Audit Quality* or CAQ, founded in 2007, as an independent, non-profit, non-governmental, non-partisan, public policy organization, affiliated with AICPA, devoted: (a) to augment investors' and public's confidence and trust in international capital markets, (b) to promote high quality auditing capacities by public company auditors, (c) to organize and cooperate with other stakeholders in order to improve the dialogue of crucial auditing matters, that demand further action and involvement, and (d) to support policies and standards regarding the encouragement of public company auditors' impartiality, effectiveness, and readiness to constantly changing market reality conditions.¹⁸⁰ CAQ's publications and tools offer important guidance to auditors as it concerns the skillset empowerment of the audit professionals. Those publications worth mentioning are:

- *CAQ Member Alert No 2014-3 of March 21, 2014 entitled Cybersecurity and the External Audit*: provides useful information about latest developments regarding cybersecurity auditing, such as: (a) how cybersecurity transforms the corporate technology related risks, since is not anymore only an "IT" matter, but an issue that attracts the interest and actions from regulatory institutions, like Congress and SEC, (b)

¹⁷⁷ CISA, (06/05/2014 original, 06/03/2019 revised), *Infrastructure Protection Gateway*, <https://www.cisa.gov/ip-gateway> (last retrieved 25/06/2019).

¹⁷⁸ CISA (2019), *Downloading and Installing CSET*, <https://www.us-cert.gov/ics/Downloading-and-Installing-CSET> (last retrieved 25/06/2019).

¹⁷⁹ CISA (2019), *Industrial Control Systems*, <https://www.us-cert.gov/ics> (last retrieved 25/06/2019).

¹⁸⁰ CAQ (2019), *Our Mission: Serving Investors, Public Company Auditors & the Markets*, <https://www.theacaq.org/about-us/> (last retrieved 25/06/2019).

the responsibilities of the independent external auditor concerning cybersecurity aspects related to issuance of the financial statements and internal controls over financial reporting (ICFRs) auditing processes, especially if those responsibilities derive from regulatory and relevant standards obligations. Therefore, external auditors during their financial statement audit and ICFR audit trails in IT system and databases (such as operating systems and Enterprise Resource Planning (ERP) systems) must give special attention, perform tests and evaluate properly the following: (i) unauthorized access indicators for material misstatement to an entity's financial statements, (ii) accounting methods for cybersecurity-related losses and their impact on the creation of financial statements and disclosures, such as fixed assets and contingent liabilities or claims, (iii) accounting methods of the impact of certain transactions or cybersecurity events and incidents, and the associated costs of these incidents, (iv) as it concerns ICFR, the auditors responsibility extends to the assessment of cybersecurity-related controls, concerning appropriate recording and disclosing of the required information in the financial statements, (v) external auditors must develop customized audit programs and be in a dialogue with an entity's leadership team and Audit Committee (in order to comply with PCAOB Auditing Standard No.16), and (vi) the procedures that auditors must perform concerning financial statement disclosures and Form 10-K filing, since in current terms cybersecurity risks must be disclosed in several sections of Form 10-K (such in, risk factors, MD&A, legal proceedings, business description, and financial statements section) concerning the full spectrum of financial statements or information that must be registered in Form 10-K but outside the financial statements, in accordance with *PCAOB's AU Section 550, Other Information in Documents Containing Financial Statements*.¹⁸¹

- *CPA's Role in Addressing Cybersecurity Risk: How the Auditing Profession Promotes Cybersecurity Resilience of May 2017*: this paper investigates from one side the growing role of auditing profession in addressing the various cybersecurity challenges, threats and impacts for the sake of corporate and capital markets integrity and the demanding need of stakeholders for accurate corporate information in the constant changing technological landscape and from the other side how AICPA's new

¹⁸¹ CAQ (21/03/2014), *CAQ Member Alert No 2014-3: Cybersecurity and the External Audit*, https://www.thecaq.org/wp-content/uploads/2019/03/caqalert_2014_03.pdf (last retrieved 25/06/2019).

cybersecurity reporting framework, as we described it earlier can assist in these efforts.

182

- *Cybersecurity Risk Management Oversight: A Tool for Board Members of April 2018:* provides suggestions on crucial questions that board members must have under consideration when they examine the risks, the responsibilities, and tasks with both management and CPA firms. The tool offers important assembled recommendations from resources deriving from the CAQ, the American Institute of CPAs, the National Association of Corporate Directors (NACD), and others institutions and groups, and suggests questions that are grouped in the key sections: (i) understanding how auditors consider cybersecurity risk regarding financial statements and, if applicable, ICFR and other disclosures, (ii) understanding the role of management and responsibilities of the financial statement auditor related to cybersecurity disclosures, (iii) understanding management's approach regarding cybersecurity risk management and (iv) understanding how CPA firms can assist Boards of Directors in their oversight of cybersecurity risk management.¹⁸³
- *Emerging Technologies: An Oversight Tool for Audit Committees of December 2018:* following the Committee of Sponsoring Organizations of the Treadway Commission's (or COSO) framework of five key components Internal Control—Integrated Framework (of May 2013): (i) Control Environment (ii) Risk Assessment (iii) Control Activities (iv) Information and Communication and (v) Monitoring Activities, CAQ's publication offers an analogous five sections/components framework and key questions that audit committees must take under consideration and request from management and auditors in order to get a solid understanding and insight over entities proper financial reporting concerning emerging technologies, like those examined previously. Moreover, this publication emphasizes the growing role of two emerging technologies, artificial intelligence, and robotic process automatization, and how currently these technologies had been incorporated to modern financial reporting landscapes.¹⁸⁴
- *Emerging Technologies, Risk, and the Auditor's Focus: A Resource for Auditors, Audit Committees, and Management of May 2019:* this publication can be considered as the

¹⁸² CAQ (May 2017), *CPA's Role in Addressing Cybersecurity Risk: How the Auditing Profession Promotes Cybersecurity Resilience*, https://www.thecaq.org/wp-content/uploads/2019/03/caq_cpa_role_in_addressing_cybersecurity_risk_2017-05.pdf (last retrieved 25/06/2019).

¹⁸³ CAQ (April 2018), *Cybersecurity Risk Management Oversight: A Tool for Board Members*, https://www.thecaq.org/wp-content/uploads/2019/03/caq_cybersecurity_risk_management_oversight_tool_2018-04.pdf (last retrieved 25/06/2019).

¹⁸⁴ CAQ (December 2018), *Emerging Technologies: An Oversight Tool for Audit Committees*, https://www.thecaq.org/wp-content/uploads/2019/03/caq_emerging_technologies_oversight_tool_2018-12.pdf (last retrieved 25/06/2019).

enriching continuance of the previous publication, since this time the emphasis is given to the auditing implications in financial reporting processes including not only the emerging technology of artificial intelligence, but also of the Internet of Things, and smart contracts. The publication explores the significant advantages and the risks from using these technologies by auditors, audit committees, and management in order to perform their tasks diligently and effectively. Moreover, highlights key areas of auditing emphasis that must be in the spotlight when auditors perform their impact analysis of these emerging technology on core business functions, internal controls over financial reporting (ICFRs), and audit committee supervision actions.¹⁸⁵

Before we proceed to the examination of the cybersecurity regulating framework withing European Union, that create important compliance requirements with auditing interest, and since we mentioned it, we would like to provide some further explanation about the ***COSO's Internal Control Integrated Framework***. COSO is a joint initiative from the following five organizations of private sector: (a) the American Accounting Association, (b) AICPA, (c) Financial Executives International (FEI), (d) the Association of Accountants and Financial Professionals in Business (IMA), and (e) the Institute of Internal Auditors (IIA). COSO aims to provide leading advice and guidance through the development of holistic frameworks and guidelines in areas, such as: internal control, enterprise risk management, fraud prevention in order to enhance business capacities performances and fraud reduction.

Within this scope, COSO published it first edition of Internal Control—Integrated Framework in 1992 and it was soon recognized globally as a leading framework concerning proper constructing, implementation, execution, and effectiveness evaluation of internal control systems in business. This original edition was enriched during time and in May 2013 COSO published the current edition and most advanced version of the framework. COSO's 2013 Internal Control—Integrated Framework is consisted, as the Image No 5 indicates, of five key components: (i) Control Environment (ii) Risk Assessment (iii) Control Activities (iv) Information and Communication and (v) Monitoring Activities and can be used not only from inside an entity players, like (a) the Board of Directors and its sub-committees, and especially the Audit Committee, (b) senior managers, (c) other levels of management and personnel, and of course (d) internal auditors, but also from external players, such as (a) the entity's independent/external auditors, in order to assess the effectiveness of the customer's internal control system toward sound and proper financial reporting, (b) other relevant

¹⁸⁵ ¹⁸⁵ CAQ (May 2019), *Emerging Technologies, Risk, and the Auditor's Focus: A Resource for Auditors, Audit Committees, and Management*, https://www.thecaq.org/wp-content/uploads/2019/05/caq_emerging_technologies_risk_auditors_focus_2019-05.pdf (last retrieved 25/06/2019).

professional organizations that provide related guidance, and (c) educators and academia individuals. First of all, the framework provides a definition of what is “internal control”, as a process, effected by an entity’s board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operation, reporting and compliance. Before we analyze the five components of the

Image No 5: Presentation of COSO’s Internal Control—Integrated Framework (2013 edition) and its Components

Source: COSO (May 2013), *Internal Control—Integrated Framework: Executive Summary*, <https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf> (last retrieved 25/06/2019).

Framework, we will make a small dive in the three objectives set by the definition of

internal control and more precisely:

- (a) *operating objectives*, aims to evaluate the effectiveness and efficiency of an entity’s operations, such as operational and financial achievements and assets protection from losses and frauds, (b) *reporting objectives*, aims to obtain a good understanding about internal and external financial and non-financial reporting performances, in which we can integrate transparency, consistency, timelessness, and other standing that the entity on its own, or regulating authorities or relevant standards had set, and (c) *compliance objective*, aims to provide assurance that the entity complies properly with the set laws, norms and other type of regulations, such as those

we mentioned in the previous Chapter.

The five components of COSO’s of Internal Control—Integrated Framework are:

- (a) *Control Environment*: is the necessary and deep impactive to the overall internal control system set by applied standards, procedures, policies and structures that function as the foundation for the creation of an entity’s internal control system, as these system developed by the aims and scope of Board of Directors and Senior Management and is enforced by all levels of management across the entity. This

Cyber-security and Cyber-preparedness as a Necessary Part of the Auditing Process

environment is consisted of: (i) the integrity and ethical values and codes of the entity, (ii) the factors that allows to the Board of Directors to perform its leadership duties, (iii) the authority and responsibilities duties allocation and structure in organizational level, (iv) the actions the entity applies in order to attract, hire, empower and keep the best and more competent professionals, and (v) how the entity holds its staff accountable for high quality performances and the rewarding system on achieving these performances.

- (b) Risk Assessment: in order to track and deal with all the types of external and internal threats and their possibility to occur resulting a negative impact to an entity's capacity to achieve its objectives. Risk assessment is a dynamic and repeated process that aims not only to identify but also to assess these risks and in related to the risk appetite and tolerance behavior of the entity, but also with its risk management attitude towards risks. That is why, management must had already as a precondition o proper established in a clear and suitable way, the entity's operations, reporting and compliance objectives. Management must not be afraid to proceed with the necessary changes and their possible impact in order not to constitute the internal control system ineffective.
- (c) Control Activities: are consisted of the actions, preventive or detective, manual or automated, such as policies, procedures, authorizations, verifications, reconciliations and reviews, that the management applies in all levels, at various business processing stages and according to the technologies used in order to assure risks' mitigation and to achieve entity's objectives. Segregation of duties is the typical process for proper establishment of control activities, but wherever is not practical, alternative control activities must be selected and implemented by management.
- (d) Information and Communication Activities: information is a necessity for proper conduction of internal control duties and fulfilling entity's objectives, that is why, management must assure that the information used from internal and external sources is accurate, and appropriate enough to assist proper functionality of sub-components of the internal control. Communication is a constant, repeated process regarding the proper offering, distributing, and obtaining the required information. Through internal communication the need for entity-wide sharing and follow-up of information is covered, and also provides to the personnel in a clear way the targeted by management message concerning the severity of control responsibilities. External communication is a two-way channel: from one side it facilitates inbound communication of appropriate

external information, and from the other side, it directs information to external stakeholders (such as external auditors) according to the entity's needs and objectives.

- (e) *Monitoring Activities*: is referring to the needed evaluations, ongoing, separate, combined, that entity's must perform in order to assure that every one of the five components of internal control is in place, active and properly working. Ongoing evaluations, are established in core business processes at all levels with the aim to offer timely information, while separated evaluations, are implemented periodically and obey to a variety of aims, and sometimes are influenced by the risks assessments results and effectiveness of ongoing evaluations, as well as other contemplations set by the management. Here, the role of criteria set by regulating authorities, relevant standards, management and the Board of Directors play a key role in evaluating the findings and results of those evaluations, and any deficiency observed by them must be communicated to the management and the Board of Directors.¹⁸⁶

III] 4. 2. The European Union Auditing-Related Cybersecurity System

European Union (EU) as the successor of European Economic Community (EEC-founded in 1958) is an economic and political union consisted of twenty-eight member-states of the European continent, of which nineteen have the same currency, called euro. For the best facilitation of achieving a trustworthy, stable and flourishing internal market, EU institutions, raise awareness and create obligatory regulations for important economic and corporate issues, as we examined in the part of blockchain and crypto-assets regulatory framework, concerning: (a) corporate and banking functioning and transparency, (b) protection and circulation of the common currency, euro, (c) securities, investments and financial markets regulation, (d) money laundering, (e) tax evasion, (f) market stability and market abuse matters, etc. Mostly, throughout the following EU regulations: the *Anti-Money Laundering Directive* (AMLD5-EU Directive 2018/843 of 30/05/2018), the *Market in Financial Instruments Directives* (MiFID I & II), the *Prospectus Directive*, the *Transparency Directive*, the *Market Abuse Directive*, the *Short Selling Regulation*, the *Central Securities Depositories Regulation and the Settlement Finality Directive*, the *Financial Collateral Directive* (FCD), the *Alternative Investment Fund Managers Directive* (AIFMD), the *Electronic Money Directive*, the *Electronic Commerce Directive*, the

¹⁸⁶ COSO (May 2013), *Internal Control—Integrated Framework: Executive Summary*, <https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf> (last retrieved 25/06/2019).

Payment Services Directive, the *Electronic Identification and Trust Services for Electronic Transactions in the Internal Market Regulation*, and other, and through the institutions of the European Securities and Markets Authority (ESMA) and the European Banking Authority (EBA), secures the proper and without frauds corporate functioning and internal market stability. This regulatory framework is quite demanding and complex, but has significant auditing interest, since it is obligatory for entities established in EU territory (is the territory of the twenty-eight member- states, possible twenty-seven from 2020 if Brexit, the exodus of Great Britain from EU, will take place) and for all the others not established in EU but working and have clients within EU. So, in case of violations or non-proper execution of this framework, since EU basic laws such as the founding Treaties, Regulations, Directives, Decisions, are not only obligatory norms but also prevail in comparison with member-states national law, issues of compliance and perhaps heavy fees and penalties from EU related institutions emerge and must be identified and reported analogously from entities in their financial statements and their auditors reporting.

The European Union, recognizes two types of auditing standards: (A) the first set is concerning the regulation of internal market and proper financial reporting, corporate and public interest entities (PIEs) operation, and the performance of entities-wise auditing standards, such as those examined in this paper. EU recognized already from May 2006 with the *Audit Directive 2006/43/EU*, that all statutory audits performed in European Union will be conducted based on International Standards of Auditing (ISA) of International Federation of Accountants (IFAC), as we examined them in multiple parts of this Master Thesis. In current affairs the audit practice in European Union is regulated by two EU laws: (i) *Audit Directive 2014/56/EU*, that amends the previous Directive 2006/43/EU, and provides the comprehensive framework concerning statutory audits, fortifies public oversight and supervision of the audit profession and enhances collaboration among relevant authorities in EU,¹⁸⁷ and (ii) *Audit Regulation 537/2014 on specific requirements regarding statutory audit of public-interest entities*, that sets specific requirements for conducting statutory audits of public interest entities (PIEs), such as listed companies, banks and insurance undertakings.¹⁸⁸ In general terms, these two very important documents for audit profession

¹⁸⁷ **Official Journal of the European Union** (27/05/2014), *Directive (EU) Directive 2014/56/EU of the European Parliament and of the Council of 16 April 2014 amending Directive 2006/43/EC on statutory audits of annual accounts and consolidated accounts (Text with EEA relevance)*, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0056> (last retrieved 25/06/2019).

¹⁸⁸ **Official Journal of the European Union** (27/05/2014), *Regulation (EU) No 537/2014 of the European Parliament and of the Council of 16 April 2014 on specific requirements regarding statutory audit of public-interest entities and repealing Commission Decision 2005/909/EC Text with EEA relevance*, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0537> (last retrieved 25/06/2019).

and practice establish the framework of how statutory audits of PIEs within EU must be conducted, a framework that includes specific demands, such as (i) regular rotation of the auditing company from the client PIE, (ii) the fees for the provision of statutory audits to PIEs must not be contingent and conditional fees, (iii) prohibition of the provision of non-audit services, during carrying out statutory audit services, (iv) proper preparation of the statutory audit and assessment of threats and auditors independence, (v) proper dealing with irregularities, such as frauds, (vi) performing engagement quality control review, (vii) the accurate application of International Auditing Standards (ISA), (viii) the proper construction and delivering of the audit report, (ix) the provision of submitting any additional report to the audit committee (x) the duty to submit the audit report to supervising of PIEs authorities, (xi) the communication of annual transparency report for statutory auditor or an audit firm that carries out statutory audits of PIEs, (xii) the obligation of statutory auditor(s) or audit firm(s) to provide to competent authorities information about revenues generated from audited public-interest entities, (xiii) the obligation of statutory auditor or an audit firm to keep records of the documents and information related with audit trails, (xiv) the applied conditions regarding proper appointing, duration, dismissal and resignation of audit engagements, (xv) the obligation to hand-over the audit file in case of a replacement, (xvi) the promotion of requirements of independence, professional secrecy, confidentiality, protection of personal data for statutory auditor(s) or audit firm(s) and competent authorities responsible to supervise statutory auditor(s) or audit firm(s). It is easy to end up to the conclusion that this framework not only encourages, diversity, transparency and high quality performances in audit markets and services but also strengthens investors' and public trust upon PIEs and financial information and reporting originated from them, a development that progresses proper conditions for cross-border investment and economic development within the EU.¹⁸⁹ And (B) the second set of auditing standards is concerning the applied by European Court of Auditors relevant standards, which based its decisions not only on IFAC's standards but also of International Organization of Supreme Audit Institutions' (INTOSAI) *International Standards of Supreme Audit Institutions* (ISSAI), a benchmark framework of external audit standards for auditing public entities, that is not a material of

¹⁸⁹ **European Commission** (2019), *Auditing of companies' financial statements: The EU provides regulations on statutory auditing to improve the integrity of financial statements*, https://ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/auditing-companies-financial-statements_en (last retrieved 25/06/2019).

analysis in this research paper, since they apply to relevant institutions and not to corporate and other public interest entities, that we examine here.¹⁹⁰

Within this general auditing background in EU, cybersecurity gains its important role relatively late. Despite the fact, that the first related to cybersecurity agenda, obligatory norm, the Directive 95/46/EC has been adopted from 1995, regarding the regulation of privacy affairs and proper handling of personal data within EU, the creation of a comprehensive, solid and dynamic framework upon cybersecurity is the result of current labors in EU, and most prominently with the adoption of the *NIS Directive* of 2016, the *European Commission's Cybersecurity Package* and the *Cybersecurity Act* of 2017, which combined intend to empower EU resilience and proper response to cybersecurity matters, such as cyber-attacks, by solidifying the *European Union Agency for Network and Information Security* (or ENISA) cybersecurity capacities, by establish an EU-wide cybersecurity certification framework, by providing a Blueprint on proper responding to large-scale cybersecurity incidents and crises, by establishing the *European Cybersecurity Research and Competence Centre* and by enhancing related international cooperations with institutions like NATO, that will protect the single market and more prominently the EU's Digital Single Market from malicious and catastrophic cybersecurity behaviors and frauds. In the following pages, we will present the major legal framework and institutional bodies that promotes these pure cybersecurity and cyber-preparedness objectives and have an auditing interest:

- *Directive 2016/1148/EU (06/07/2016) on the Security of Network and Information Systems* or *NIS Directive*, that member-states incorporated into their national legal systems in 09/05/2018. NIS Directive identifies that some categories of operators of essential services, such as (i) operators from electricity, oil and gas sub-sectors of the energy sector, (ii) operators from air, rail, road and water sub-sectors of the transportation sector, (iii) banking services operators, (iv) financial markets infrastructures operators, (v) health sector and health care sector operators, (vi) drinking water supply and distribution operators and (vii) digital infrastructure operators, had to comply with until 09/11/2018. The NIS Directive targets to harmonize the legal instruments for high level security of network and information systems, and for better enhancement of the overall capacities of cybersecurity across EU by safeguarding: (a) the adoption by all member-states of a national strategy concerning the security of network and information systems, (b) the establishment of the Cooperation Group, that

¹⁹⁰ **European Court of Auditors** (2019), *Audit Methodology*, <https://www.eca.europa.eu/en/Pages/AuditMethodology.aspx> (last retrieved 25/06/2019).

not only assists and promotes the cooperation and exchange of relevant information, but also enriches trust and confidence between member-states, (c) the creation of a **Computer Security Incident Response Teams Network** (or CSIRT network), that will help in the realization of (b) additionally to promulgate relevant effective operational collaboration, (d) the establishment of a security and notification obligation landscape for operators of essential services and for digital service providers, such as online marketplace providers, online search engine providers and cloud computing service providers, (e) the obligation of member-states to establish proper and national competent authorities, single points of contact and CSIRTs with duties relevant to protection and enhancement of security of network and information systems, (f) the encouragement of development and usage by member-states of non-discriminatory and technological impartial European and international accepted related standards and specifications, in collaboration with ENISA, (g) the voluntary notification to national competent authorities by entities that are not identified as operators of essential services and digital service providers, any incident that might impose a business continuity problem to the service provider, and (h) the establishment by member-states effective, proportional and discouraging rules concerning penalties on offences and infringements related to the NIS Directive.¹⁹¹

- **Regulation 2019/881/EU (17/04/2019) on European Union's Agency for Network and Information Security (ENISA) and on EU Cybersecurity Certification Framework, best known as Cybersecurity Act:** that enters into force in 28 June 2019 and will be fully applicable from 28 June 2021. This Regulation aims to empower and strengthen the capacities of European Union's Agency for Network and Information Security (ENISA), that is based in Greece, and its mandate is designed to expire in June 2020. Until now, ENISA's role is more to provide expertise and advice rather than dealing and leading cybersecurity operations across EU. However, ENISA under the NIS Directive must provide secretariat operations to NIS Directive CSIRTs. The Regulation 2019/881/EU provides the basis (a) into how ENISA will be the EU's Cybersecurity Agency with a permanent mandate, superior operational capacities, concrete governing structure, (b) be able to support member-states during their attempt towards NIS Directive implementation, (c) will administrate the established by the

¹⁹¹ **Official Journal of the European Union** (19/07/2016), *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (last retrieved 25/06/2019).

Regulation's Information and Communication Technologies (ICT) cybersecurity certification framework and (d) will assist EU attempts to combat fraud, corruption and unlawful activities in cooperation with European Anti-Fraud Office (OLAF) and Court of Auditors. The second objective of the Cybersecurity Act is to establish a comprehensive, common, EU cybersecurity certification framework, consisted of relevant set of rules, technical requirements, standards and procedures, that provides customized and risk-assessing EU certification schemes concerning ICT digital products, services and processes, aiming like that not only to harmonize the highly differentiate cybersecurity certification schemes¹⁹², but also to increase public trust, awareness and security for digital goods (products, services and processes) that are necessary for achieving a flourishing Digital Single Market within EU. Each European scheme upon a specific ICT-based product or service should provide information about: (a) the sorts of products and services covered by it, (b) the cybersecurity requirements must fulfil, such as compliance with specific standards or technical specifications, (c) the type of evaluation, like self-assessment processes or third party evaluation, and (d) the projected level of cybersecurity risk assurance it will provide and associated with in terms of using the products, services and processes and in terms of the potential impact of an cybersecurity incident, that can be categorized from basic/initial level, to medium/substantial and/or high, in order after an agreement at EU level for the evaluation of its to be certified as complying with the framework. This means that, the applicable levels of assurance for evaluating cybersecurity certifications are three: (a) the *basic level*, that includes evaluating activities that contain at least an evaluation, a review of the technical documentation of the examined scheme, such as a conduction of a self-assessment, (b) the *substantial level*, that includes evaluating activities that contain at least “*a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities*”, and (c) the *high level*, that includes evaluating activities that contain at least “*a review to demonstrate the absence of publicly known vulnerabilities; testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities at the state of the art; and an assessment of their resistance to skilled attackers using penetration testing*”. So, if a service provides a high level of assurance, that was certified to it by successfully passing the most demanding and high aspirations

¹⁹² Paradigms of such schemes are UK's Cyber Essentials scheme, the Dutch scheme for BSPA (Baseline Security Product Assessment), France's CSPN (Certification S curitaire de Premier Niveau) and ISO 27001

cybersecurity tests, then this service is accompanied with a certification recognized in pan-EU level (meaning from all EU member-states) and empower its holder entity to trade across EU borders and aid its customers to better comprehend the security characteristics of the examined product or service. For the best establishment and application of this framework, all member-states relevant authorities must participate in the *European Cybersecurity Certification Group (ECCG)*, next to the *Stakeholder Cybersecurity Certification Group (SCCG)*, which will provide advice to the European Commission and ENISA regarding key matter of cybersecurity certification, and assistance to the European Commission regarding the preparation of the EU relevant systematic work programme, and the *National Liaison Officers Network*, composed of representatives of all Member States, the National Liaison Officers. The use of the certification schemes might be on a voluntary basis for entities in the initial level, but creating and promoting a high level of cybersecurity standard certification scheme might translated into a strong competitive advantage for entities providing their clients a good level of cybersecurity protection and assurance products and services are at a certain level of cybersecurity. This behavior will thus promote "*a cybersecurity by design*" level of protection and assurance within EU Digital Single Market. This development will benefit (a) citizens and end-users, such as operators of essential services cybersecurity capacities and decision-making processes, (b) vendors and providers of ICT products and services, and customer entities, such as SMEs, existing or new entities, that now must follow a single certification process, that will award them European certificate valid and usable to all Member States and saving like that important money resources, than obtaining a certificate in all the EU countries, and (c) governments, since now will be better informed to make proper decision and better equipped to handle institutional requirements concerning key ICT security certification priority areas. As we stated previously, in its initial phase the Certification will be voluntary, but the European Commission must periodically assess the certified schemes' efficiency and application and to judge if the certification must be constituted as mandatory. The first assessment of that kind must be conducted by 31 December 2023, and subsequent assessments will be conducted every two years after the first one, with schemes influencing operators of essential services, as those we described in NIS Directive, to have priority during assessments. The EU Cybersecurity Act allows to individuals and entities to lodge a complaint against the issuer of any European cybersecurity certificate, as well as the right to receive an effective judicial remedy, concerning decisions made in conformity with assessment bodies or the related national

cyber security certification authority. The Act also indicates a system of “*effective, proportionate and dissuasive*” penalties for relevant infringements and offences.¹⁹³

- ***Directive 2019/713/EU (17/04/2019) on the combatting of fraud and counterfeiting of non-cash means of payment***, that regulates the sector of non-cash payments instruments, such as payment cards (credit and debit), credit transfers, direct debits, e-money, virtual currencies, mobile money, vouchers, coupons, fidelity cards, etc., which can be subject to a great variety of frauds, such as phishing, skimming or obtaining information in order to steal credit card credentials and sold them on the dark-markets, or counterfeiting or stealing cards used to pay in stores (with points of sales -POS- devices or withdraw cash at ATMs or by hacking an entities information systems to proceed with fraudulent payments, and other illegal transactions. The Directive updates the relevant EU’s criminal law and strengthens security of EU’s Digital Single Market Strategy, by enriching the member-states capacities to indict and punish non-cash payment fraud by: (a) enhancing law enforcement authorities ability to spot, tackle and identify crimes connected with information systems frauds and payment transactions, including virtual currencies transactions, (b) provides a landscape of harmonized norms upon penalties by setting a minimum level for the highest set my member-states penalties, that varies from two to five years in prison. According to this directive, related crimes are any offense of possessing, selling, procuring for use, importing or distributing a stolen or unlawfully seized counterfeited or falsified payment instrument, (c) provides further clarification on the matter on member-states jurisdiction, since member-states have the right to pursue offence, that has been committed using an information system located within the territory of any member-state, even if the offender is located outside of it or even if the offender is located within the territory of the member-state but the information system that has been compromised is located outside of it. Moreover, member-states are entitled to exercise their jurisdiction right even in cases the offence provokes damage in their territory, such as theft identity harm, (d) safeguards the right of cybercrime victims to access information about available assistance and support and ameliorates conditions and incentives for victims and private entities to report the received crimes, (e) promotes measures to facilitate better criminal

¹⁹³ **Official Journal of the European Union** (07/06/2019), *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)*, <https://eur-lex.europa.eu/eli/reg/2019/881/oj>
European Commission (17/09/2017), *State of the Union 2017: The Commission scales up its response to cyber-attacks*, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_3194 (last retrieved 25/06/2019).

justice cooperation across EU and (f) facilitates the providing of trustworthy statistical data concerning frauds and counterfeiting attempts of non-cash means of payment. Member-states must take all the necessary actions, such as the adoption of relevant laws, regulations, and administrative norms, until 31 May 2021 in order to incorporate the Directive into their legal systems and comply with Directive's requirements.¹⁹⁴

- ***Regulation 2016/679/EU (27/04/2016) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, best known as General Data Protection Regulation or GDPR***: that not only replaces Directive 95/46/EC but also (a) offers a more comprehensive and strong than Directive 95/46/EC level of individual's data protection and privacy within the EU and the and the European Economic Area (EEA), (b) deals with the issue of transferring personal data outside the EU and EEA, since it provides to individuals the control over their personal data, and (c) harmonizes relevant obligatory requirements that entities must follow. GDPR, that have become actual enforceable on 25 May 2018, indicates that an individual's (called as 'data subject') personal data¹⁹⁵ must be handled according to the following principles: (a) *the principle of lawfulness, fairness and transparency* when they are processed, (b) *the principle of purpose limitation*, since their collection must be according to specified, explicit and legitimate purposes with no exceeding the mandate of their collection, unless the collection aims to fulfill purposes regarding public interest, scientific or historical research purposes or statistical purposes, (c) *the data minimization principle*, that narrows the process to only what is adequate, relevant, limited, and necessary, (d) *the accuracy principle*, that demands only accurate and only necessary data to be updated, otherwise all the personal data that are inaccurate must be erased or rectified without delay, (e) *the storage limitation principle*, that demands data that permits identification of data subjects to be stored no longer than is necessary in order to fulfil their processing purposes, (f) *the integrity and confidentiality principle*, that demands personal data to be properly secured and protected against unauthorized or unlawful processing, against accidental loss, destruction or damage, by applying the proper technical or

¹⁹⁴ **Official Journal of the European Union** (10/05/2019), *Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.123.01.0018.01.ENG (last retrieved 25/06/2019).

¹⁹⁵ Article 4 of GDPR recognizes as 'personal data' "*any information relating to an identified or identifiable , directly or indirectly, natural person, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

organizational actions, and (g) the *accountability principle* for the data controller of personal data, that must prove that complies with the above principles. **Data controllers**¹⁹⁶ and/or **data processors**¹⁹⁷ of personal data, are professionals that entities have, with duties to (a) implement the most appropriate technical and organizational measures, such as pseudonymization or full anonymization in order to fulfill the above mentioned data protection principles, (b) proper handle, safeguard and protection of personal data by designing and applying the most suitable information systems that enhance data privacy and protection from being in a wrong way available to the public and (c) when they must clearly disclose any collected dataset, they must declare the lawful basis and purpose for the data processing, additionally to provide information about the retaining duration and the possibility of sharing these datasets with any third parties or outside of the EEA. That is why, personal data must only be processed under one of six lawful bases: consent, contract, public task and interest, vital interest, legal obligation, legitimate interest or legal requirement. As it concerns the case of consent, that should be in specific, freely-given, plainly-phrased, and explicit affirmed given by the data subject, the data subject has the right to revoke the consent permission at any time desires. GDPR provides to the data subjects the following rights: (i) *the right to be informed*, (ii) *the right to access*, (iii) *the right to rectification*, (iv) *the right to erasure*, (v) *the right to restrict processing*, (vi) *the right to data portability*, (vii) *the right to object*, and (viii) *rights concerning automated decision-making and profiling*. One of the innovations of the new Regulation is the obligation of every public authority and business entity that among their core activities is included the systematic and continued collection and processing of personal data to deploy a **Data Protection Officer** (or DPO), a consultancy professional responsible for ensuring and managing the entity's attempt to best comply with GDPR. In case of a data breach, the entity must report the incident to the **Data Protection National Supervisor Authority** (or DPAs), that each member-state must have or establish, within seventy-two hours of the adverse effect of the data breach event. The **European Data Protection Supervisor** is EU's independent data protection authority responsible to monitor, assure and advice EU institutions and bodies concerning the processing protection by them of individuals' personal data. GDPR provides also a series of remedies, liabilities and penalties for violations of the

¹⁹⁶ Article 4 of GDPR recognizes as "controller", "a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."

¹⁹⁷ Article 4 of GDPR recognizes as "processor", "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."

Regulation that vary from just a writing warning for the first non-intentional non-compliance and the conduction of regular data protection audits in periodic basis to hefty fines for corporate entities, that can reach even the maximum of €20 million or up to 4% of the annual worldwide turnover of the preceding financial year, with the obligation to be chosen the penalty that is the greater among these two choices. The Regulation is not applicable to data collection and processing cases that are related to (a) lawful intervention, national security, military, police, and judicial affairs, (b) the data of deceased persons, that are covered by national legislation norms, (c) data collected and processed based on a dedicated law regulating the employer-employee relationships, and (d) personal data processed by individuals for purely personal or household activities and situations. However, GDPR is also applicable to the following cases: (a) for any data controller and processor resided outside of the EEA, but with operations of offering of goods or services, even if a payment transaction is not required, to data subjects within the EEA, (b) in cases of monitoring the behavior of data subjects inside the EEA, even if processing does not take place. Non-EU entities, that must comply with GDPR are obliged to designate a person or a company as their "**EU Representative**" within the EU, to operate as the entity's contact point of compliance with GDPR, otherwise risks to receive a penalty of up to €10 million or up to 2% of the annual worldwide turnover of the preceding financial year, again in this case the greater of the two amount will be selected. Last but not least, GDPR prohibits to entities to transfer EU's data subjects personal data to countries outside of the EEA (the so called third countries), with the exception of applying the proper safeguarding measures, and in case of the third country's data protection regulatory norms are formally accepted as adequate by the European Commission.¹⁹⁸

- **EUROPOL and European Cybercrime Centre at Europol (EC3):** EUROPOL additionally to all other related crimes with European importance investigates and deals with a series of cyber-related crimes and situations, such as data protection and transparency issues, intellectual property thefts and cyber-related frauds. With the establishment of its European Cybercrime Centre (EC3) in 2013 EUROPOL provides not only high quality law enforcement response against cybercrime within the EU, but also protects European citizens, business entities and governments from high-profile

¹⁹⁸ **Official Journal of the European Union** (04/05/2016), *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*, <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (last retrieved 25/06/2019).

online crime, by proceeding to hundreds of arrests, and thorough analysis of hundreds of thousands of files upon malicious cyber-behaviors annually. Through its annual publication of the *Internet Organized Crime Threat Assessment (IOCTA)*, EC3 provides strategic analysis into emerging cybercrime threats and developments, as well as the response of EC3 to these threats based on its three-core methodological approach to combat cybercrime: (a) the *forensics approach*, through its two forensics teams, the digital forensics team and the document forensics team, offers operational assistance, examination and development in different aspect of cybercrimes, (b) the *strategy approach*, through its two strategy teams, the one related to prevention and stakeholder management, and among others develop relevant partnerships and alliances, standardizes cybercrime training and coordinates prevention and awareness procedures and the other team is related to strategy and development by providing strategic analysis, internet governance and articulation of policy and legislative procedures and norms, and (c) the *operations approach*, with which EC3 develops operational capacities against (i) cyber-related dependent crimes, (ii) online child sexual exploitation crimes, and (iii) fraud crimes associated with payments and transactions. EC3 as the EU/EUROPOL's central hub provides criminal information and intelligence against cybersecurity crimes in EU level, in Member-states level and in private sector's entities level, as well as protecting vulnerable individuals from cyber-crimes, (a) through its *Cyber Intelligence Team (CIT)*, gathers and assess significant cybercrime-related of related data from public, private and open sources in order to identify emerging cyber-threats and cybercrime patterns of action and (b) by functioning as the *Joint Cybercrime Action Taskforce (J-CAT)*, deals with the most demanding and significant international cybercrime cases that impact not only EU member-states and their citizens.¹⁹⁹

All the above-mentioned legal documents and the institutional bodies and authorities created by EU with the aim to regulate the cybersecurity sphere within EU. Auditors, during their audit trails must inspect whether or not their client entities comply firmly and boldly with these obligatory norms, especially with those accompanied by serious and hefty fines, like GDPR and NIS Directive. The potentiality of a fine or the necessity of an entity to acquire a cybersecurity certification scheme and its failure to do so must be recorded and reported in auditors' final opinion and published report. Before we close this part of relevant to cybersecurity laws in European continent we must mentioned also the existence

¹⁹⁹ **EUROPOL** (2019), *EUROPEAN CYBERCRIME CENTRE - EC3: Combating crime in a digital age*, <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3> (last retrieved 25/06/2019).

Cyber-security and Cyber-preparedness as a Necessary Part of the Auditing Process

of *Council of Europe's Convention on Cybercrime of 2001* (entered into force in 01/07/2004) – best known as the *Budapest Cybercrime Convention*. This Convention is not a EU's legal document, but except for Ireland and Sweden, all the other EU Member-States participate in it. The Convention is the first international treaty that regulates the cyber-crime incidents committed via the Internet and other computer networks, such as copyright infringements, computer-related frauds, child pornography situations and network security violations. The Convention offers a series of powers and procedures in case of cybercrimes tracked and handling, with computer networks investigation and interception to be among the proposed instruments. Through this instruments and processes, the Convention aims (a) to establish a common criminal policy, (b) to promote the adoption of proper and efficient legislation frameworks, and (c) to encourage further international co-operation, among its signatories.²⁰⁰ For those nations that choose to incorporate the Convention to their national legal order or plan to do so, and are plenty not only from European continent, but also from Asiatic (i.e. Israel. Japan), American (i.e. USA, Canada), African, and Oceania (i.e. Australia) continents, this legal document is or will be part of their national legal framework, which means that compliance with the Convention will be obligatory for individuals and entities. So, auditors, must assure, among others, the compliance with this Convention also.

III] 4. 3. Conclusions on Cybersecurity Regulatory Compliance Frameworks

Modern obligatory regulatory compliance frameworks are characterized by heavy complexity, multiple levels of requirements, multiple texts regulating or co-regulating an industry, and are accompanied with the acquisition of cybersecurity certification accreditation demands and sometimes with hefty fines and penalties (such in the case on GDPR and NIS Directive). They cover almost all industries in the full range of economic sphere, and mostly for publicly traded listed entities, that are the ones obliged to have internal audit departments, Audit Committees as part of their Board of Directors and external auditors. This development constitutes not only the compliance obligation from the side of entities an exceedingly difficult and complex job, but also from the side of audit professionals and audit firms an equally demanding job.

²⁰⁰ **Council of Europe** (2019), *Details of Treaty No.185: Convention on Cybercrime of 2001*, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185> (last retrieved 25/06/2019).

Cyber-security and Cyber-preparedness as a Necessary Part of the Auditing Process

Entities attempt to deal with their cybersecurity compliance obligations and requirements, by adopting, as we are going to examine in the next section of this Chapter, the proper system of cybersecurity-related internal controls. Moreover, next to create and adopt cybersecurity protection and preparedness plans, codes, roles, and responsibilities, they also establish proper entity-wide cybersecurity management teams and/or professionals, apart those appointed by legal obligations, such as the data controllers and/or processors, the Data Protection Officer (DPOs), etc. Some examples of non-obligatory officers that entities adopt in order to treat with important cyber-security matters are: (a) *Chief Compliance Officer*, which is responsible to develop the proper policies, training and enforcing processes in order to assure compliance with the above-mentioned regulatory frameworks, (b) *Chief Risk Officer* and/or *Chief Cyber-Risk Officer*, the first one administrates with all the issues related to all the risks, including the cybersecurity ones, that an entity faces, while the second focus his/hers attention to only cybersecurity risks, by providing proper function of cybersecurity risks detection, identification, monitoring, prevention, assessment, investigation, mitigation, as well as training and communication activities, (c) *Chief Legal Officer*, that provides awareness, identification, compliance, litigation, examination and relevant policies creation concerning the obligatory legal and regulatory norms, that an entity must respect and implement, and (d) *Chief Privacy and Data Protection Officer*, in case is a different person from GDPR's data controllers and/or processors and Data Protection Officer roles. A Chief Privacy Officer must (i) have a deep knowledge and understanding of privacy laws and frameworks, that the entity must obey, (ii) create and enforce the proper policies, (iii) conducts adequate training and communication activities within the entity and (iv) performs all the relevant privacy and data protection audits.

On the other side, auditors, internal and external, during their examination upon the achieved compliance by client entity, must construct their audit trail in a very effective and multi-layer way, as we are going to examine in the next Chapter, a task quite difficult and complex. Assistance in this task can play the specially designed and accredit standards and schemes that organizations like International Standards Organization (ISO) and Information Systems Audit and Control Association (ISACA) had developed, and we will be examined them in the following Chapter.

III] 5. Understanding the Cybersecurity Risks' Internal Controls System

Cybersecurity internal controls are mechanisms (like process, plans, rules, etc.), that have been developed by the entity in NHS systems, IT applications and all the other relevant to cybersecurity concerns systems and materials, in order to assure that the business objectives set by the management of an entity can be achieved and any cybersecurity-related irregularities an anomalies or unexpected events can be spotted, neutralized and corrected before they produce their negative effects. A primary set of internal controls responses to entities behavior analogous to the cybersecurity risks and vulnerabilities they face we mentioned in the relevant sub-section of this Chapter. Internal controls are classified in three categories: 1) preventive, 2) detective and 3) corrective. Below we will present the three categories, providing further clarification about their characteristics and indicative paradigms about the most important cybersecurity internal controls according to each category:

1] PREVENTIVE CONTROLS: are those implemented in order: (a) to control the proper functionality and entrance/access to NHS and IT systems, (b) to predict concrete but potential issues and provide the necessary adjustment and correction in order the issues not to occur and (c) to enhance the cybersecurity preparedness status and level of protection of an entity. Paradigms are:

- Application of systems controlling physical access to NHS systems.
- Application of systems controlling logical access to NHS systems, such as strong password policy.
- Adoption of the best authentication and conduction procedures of transactions, such as obligatory second confirmation from authenticated person or robots on important transactions, usage of multi-factor authentication (MFA).
- Use fire protection materials in buildings, such as fire-proof building materials, install sprinklers, conduct fire drill training and practices, and prohibit smoking inside the building (or allowed smoking only to strictly controlled areas).
- Regular maintenance of devices, routers, servers, systems, and cybersecurity related infrastructure, like data storage devices. Purchasing only accredit and high-standard compatible devices and material.

Cyber-security and Cyber-preparedness as a Necessary Part of the Auditing Process

- Creation and regular check of the legal and technical compliance requirements lists, especially as it concerns data privacy and data protection concerns (i.e. GDPR compliance).
- In the potential case of a significant physical issue (i.e. a terrorist attack, or a tsunami or an earthquake, natural disasters, etc.) adoption of escape maps and automatic storage of present and sensitive data must be present.
- Usage of the best applicable backup and data internal storage mechanism, and/or usage of external third-party data centers.
- Adoption and regular up-dating and upgrading of cybersecurity policies, codes, strategies, and software, like anti-virus and firewall software.
- Usage of encrypted protocols and virtual networks, such as Virtual Private Networks (VPNs) to protect sensitive data and communications.
- Hire people with the right cybersecurity certification and competence, like holders of ISACA's accreditation schemes.
- Better filtering not only to regular communication ways (called lateral communication between colleagues, managers, and employees or between workstations) but also with external channels of communication in order to avoid creation of institutions and backdoors.
- Adoption of the most suitable and applicable disaster and recovery plan.²⁰¹ This type of plan prepares the entity (management and personnel) in case of an emergency.
- Adoption of the most suitable and applicable business continuity plan, which aims to maintain core business functions and operations in case of a major disruption, like a natural disaster, a power loss, a terrorist attack, an extended fire in NHS systems, a collapse of the authentication access (physical and logical) systems or a severe data breach.
- Adoption of a policy that segments and segregates networks, applications, operations, and functions.

²⁰¹ In United States, for example, in general terms laws do not acquire from firms and entities to create a disaster and business continuity plan with the exemption of CPA firms that are subject to SEC rules. **Konrad Martin** (2018), *Embracing Compliance for the Sake of Cybersecurity: Looking Beyond Legal Requirements to Find Best Practices*, CPA Journal, <https://www.cpajournal.com/2018/07/06/embracing-compliance-for-the-sake-of-cybersecurity/> (last retrieved 25/06/2019).

- Establish a third-party management program to protect the entity from cybersecurity vulnerabilities due to cooperation with external vendors, such as cloud providers, which includes (a) identification and classification all external vendors analogous to their significance, potential impact and resources allocation, (b) evaluation of the applied cybersecurity protection level and security processes of external vendors, (b) constant compliance monitoring and accountability of contracts and transactions with third-party suppliers.

2] DETECTIVE CONTROLS: are those that (a) detect and locate cybersecurity vulnerabilities and problems (b) report the incident of the problem. Paradigms are:

- Install surveillance cameras.
- Regular training of personnel and external stakeholders to detect cybersecurity irregularities and issues.
- Detect any fire incident by install fire alarms and smoke detection sensors.
- Hiring the most adequate and certified internal team or hiring an external vendor to create, apply and monitor detection mechanisms to NHS systems and create reports about the results of these processes.
- Usage of non-authorized and malicious access detection system.
- Periodical inspections to NHS systems and use data analysis from firewalls and anti-viruses to detect any cybersecurity related damage.
- Application of intrusion detection system.
- In case of a data breach, the proper detection system must be implemented and report the incident inside the entity and to infected external stakeholders (such as suppliers, data center providers, etc.) and must not neglect to report the incident to the right authorities, especially if that is a legal obligation.

3] CORRECTIVE CONTROLS: are those implemented in order to (a) minimize the impact of the cyber-threats and malicious incidents (b) repair the occurred problems that were tracked by detective controls, (c) resolve mistake produced by failures in NHS systems and (d) modify properly the IT systems aiming to minimize the appearance of future problems and vulnerabilities. Paradigms are:

- Activate disaster and recovery plan rules, which include proper contact and information with essential staff and communication with affected external stakeholders, NHS vendors

Cyber-security and Cyber-preparedness as a Necessary Part of the Auditing Process

(like external data centers providers), secure communication systems and channels for the team that conducts the recovery plan, reassurance of protection level of back-up storage systems, NHS and conduction of integrity evaluation and analysis of the present situation and correlation with the prepared recovery scenarios, etc.

- Activate business continuity plan or strategy.
- Enhance relevant authorities' corrective role, such as permit to police and other applying laws authorities to track cyber-criminals or ransomware attackers and to return the stolen data or money back to the entity.
- Usage of back-up systems as it concerns data, buildings/infrastructure, human resources and financial resources.
- In case of a fire: (a) use functional fire extinguishers and (b) activate the process of obtain fire insurance compensation.
- Activate the entity's cybersecurity incidence response strategy or plan in case of a large-scale attack or breach.
- Activate cybersecurity related insurances.²⁰²

Sometimes, there are types of control mechanism that an entity can apply, usually in compliance with laws, that can integrate all the three quality aspects (preventive, detective, and corrective) of internal controls. For example, in United States of America, the Massachusetts' Data Security Regulation and the Gramm-Leach-Bliley Act Safeguards Rule, require the production of Written Information Security Programs (or WISPs) as an integral part of an effective compliance framework. WISPs identify and assist in the implementation of the proper actions (such as use of encryption for emails and data storage drivers, adequate training of personnel) that must be conducted in case of a data breach, which enhance the personal data protection and confidentiality in a compatible with standards way, assist in further assurance and integrity of data against of potential threats, and increase the protection level against unauthorized access to data or the utilization of them in a manner that can impose a cyber-risk, like identity theft or fraud in a substantial way. Next to these preventive qualities there are also the detective one, since a WISP recognize a cybersecurity

²⁰² Νεγκάκης Χρήστος Ι. Και Ταχυνάκης Παναγιώτης Δ. (2017), *Ελεγκτική- Εσωτερικός Έλεγχος: Θεωρία και Εφαρμογές (Auditing – Internal Auditing: Theory and Applications)*, Εκδόσεις Αειφόρος Λογιστική Μονοπρόσωπη ΙΚΕ, Θεσσαλονίκη, Pages 630-631.

breaches when those take place, and corrective by taking the necessary actions to correct the impact of a breach.²⁰³

Auditors, internal and external, during their audit inspections must not only acquire a deep understanding about an entity's cybersecurity internal control system but also effectively assess them with the most suitable and quality results productive methods, in order to secure that financial statements do not contain any default due to material mistakes in cybersecurity related internal controls and systems. In the next Chapter we will provide more details about the assessment processes during the phase of planning and execution of a holistic and effective cybersecurity auditing program. In the following lines we will try focus our attention to the difficulties an auditor, internal and external, can face in his/hers/theirs communication with the management of the entity in order to acquire the necessary information and data about the cybersecurity related system of internal controls of the entity. ***ISA 260 Communication with Those Charged with Governance*** administrates the process of an effective, constructive and respecting auditors' independence and objectivity two-ways communication between those responsible for the governance (and the management) of the entity and the auditor or auditing team, upon matters like the entity risks and its functional environment, internal controls system, audit evidence resources, information about special transactions and events. Auditors can inform those responsible for the governance/management about the planned scope and timing of the audit and about significant difficulties confronted during the audit, in which they can include the auditors approach on significant cybersecurity related risks and low-quality functionality of relevant internal controls, can result to material misstatement due to cybersecurity related frauds (such as malicious attacks) and errors (such as malfunctions to the supply chain computer systems) or any attempt from the management to impose restrictions upon the examination of these auditing focus areas.²⁰⁴

Moreover, ***ISA 265 on Communicating Deficiencies in Internal Control to Those Charged with Governance and Management govern the procedure of this appointment*** administrates the issues related to the proper communication of deficiencies in internal controls to the entity's responsible governance and management teams with cybersecurity type of deficiencies to be also included in the communication and disclosure process.

²⁰³ **Konrad Martin** (2018), *Embracing Compliance for the Sake of Cybersecurity: Looking Beyond Legal Requirements to Find Best Practices*, CPA Journal, <https://www.cpajournal.com/2018/07/06/embracing-compliance-for-the-sake-of-cybersecurity/> (last retrieved 25/06/2019).

²⁰⁴ **IFAC** (2010), *International Standard On Auditing 260 Communication with Those Charged with Governance*, <https://www.ifac.org/system/files/downloads/a014-2010-iaasb-handbook-isa-260.pdf> (last retrieved 25/06/2019).

According to ISA 265 there are two types of deficiencies: (a) deficiency in internal control, which take place in the following two situations: (i) when the design, implementation and operation of a control does not allow the prevention, or detection and correction of misstatements and other defaults in the financial statements on a timely basis; or (ii) when a necessary control aim to prevent, or detect and correct, misstatements and other defaults in the financial statements on a timely basis is not in place and is absent and (b) significant deficiency in internal control, which refers to a deficiency or a combination of deficiencies in internal control systems that according to the auditor's professional capacities and judgment, has critical and sufficient significance and must be brought to the attention of those charged with governance and management.²⁰⁵ Preventive, detective and corrective internal controls related to cybersecurity and cyber-preparedness and the protection of NHS systems and IT applications from errors and/or malicious actions, such those we examine previously can be easily categorized in one of the above mentioned two types of deficiencies. For example, the lack of proper authentication and authorizations systems for physical and logical access, or insufficient mechanisms about data and privacy protection, or lack of adequate compliance with cybersecurity laws and norms, or improper detection of misstatement that were not detected by relevant IT controls, can be for a small in size and not computerized entity a simple deficiency of the first type, if the impact to normal functions is not that crucial, but to a full automatized and computerized entity can belong to the second type of significant deficiencies with crucial negative impact to operational capacities of the examined entity.

After having a thorough understanding of the client entity's internal controls system related to cybersecurity risks and concerns, auditors must plan and execute a holistic and effective auditing program according to *ISA 330 on The Auditor's Responses to Assessed Risks* that is consisted of performing tests in these controls or other substantive processes in periodical basis, which is normally at interim period and at the examined period end. In general terms, there is an analogy between to the gravity and extension of risk of material misstatements and defaults in financial statements and the extension and amount of audit processes and tests, that must be performed. Those aspects of cybersecurity auditing will be examined in the next Chapter.

²⁰⁵ **IFAC** (2010), *International Standard On Auditing ISA 265 on Communicating Deficiencies in Internal Control to Those Charged with Governance and Management govern the procedure of this appointment*, <https://www.ifac.org/system/files/downloads/a015-2010-iaasb-handbook-isa-265.pdf> (last retrieved 25/06/2019).

III] 6. Conclusions

As hard as it is to provide a general conclusion for a Chapter that exceeds one hundred dense pages, in this sub-section we will attempt exactly that hefty work. We started this Chapter by presenting the necessary aspects concerning the proper appointment of the IT/Cybersecurity auditor by the client entity and the need for auditors to understand the cybersecurity risks landscape, that entities must deal with. We continued this Chapter emphasizing the importance from the side of auditors, internal and mostly external, regarding the accurate and productive understanding of the correlation between cybersecurity dimension and cybersecurity threats and internal controls systems, that entities must and indeed do apply. The next step in our research pathway was the closer examination of the most crucial cybersecurity threats, vulnerabilities, and conditions and how the entities can defend themselves, by adopting the most suitable actions and decisions. In the following sub-section, we referred to the most important regulatory and institutional norms, that exist in United Kingdom, United States of America and of course the European Union, regarding the requirement of regulatory compliance during cybersecurity auditing performances and concerns mostly privacy and data protection issues, networks and infrastructure protection and security matters, freedom of information, cybersecurity certification schemes, proper cyber-protection of securities markets and economic growth, etc. These norms offer some of the most significant general auditing guidance and specialized cybersecurity and IT related auditing advice. We finished our attempt by examining the three basic types of cybersecurity internal controls mechanisms: 1) preventive, 2) detective, and 3) corrective, that entities develop and implement in order to protect and shield their NHS systems, IT applications and all the other relevant to cybersecurity concerns systems and materials from cybersecurity-related irregularities, anomalies, data breaches and unexpected malicious events, as those we examined in the relevant sub-section in this Chapter.

During this research course we had as guides the related provisions and frameworks deriving from International Auditing Standards, but also other standards and recognized auditing norms, that support and enrich our claims, and had been created by countries (UK, USA), international governmental institutions (EU), and other organizations, that provide internationally recognized auditing guidance, such as AICPA, PCAOB, CAQ and COSO. It is more than clear, that the more the number and complexity of frameworks, the more complicated, difficult, and demanding the auditing profession, both as practice and theory, is becoming, something that expects from auditors to constantly enrich and augment their

capacities, knowledge and abilities. It is difficult for modern auditors to have a solid grasp upon all the framework and emerging entity-related cybersecurity issues, that can influence proper financial reporting, a development that can have a significant negative impact in the accuracy and efficiency of IT/cybersecurity audits, as necessary part of general audits and audit reports. That is why, is of the outmost importance the phases of planning and execution of a cybersecurity auditing program to be conducted as more fully, efficiently and meritfully, as we are going to present in the following Chapter.

IV] CHAPTER 3: PLANNING AND EXECUTING A CYBERSECURITY AUDITING PROGRAM

IV] 1. The Cybersecurity Auditing Program and its Particles

Creating and executing a holistic, cost-effective, efficient and standards-complied cybersecurity audit program is by all means not an easy task, on the contrary, it is a very demanding and difficult one, due to the complexity, perplexity and the scalability of the whole process. Auditor(s) and/or auditing teams, belonging both to internal and external auditing systems, must formulate the whole audit process obeying in the requirement set by all the International Standards of Auditing (ISA). Planning and executing a cybersecurity auditing plan is based on the provisions the following ISA: *ISA 200 on Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing, ISA 210 on Terms of Audit Engagements, ISA 220 on Quality Control for an Audit of Financial Statements, ISA 230 on Audit Documentation, ISA 240 on The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements, ISA 250 on Consideration of Laws and Regulations in an Audit of Financial Statements, ISA 260 on Communication with Those Charged with Governance, ISA 265 on Communicating Deficiencies in Internal Control to Those Charged with Governance and Management, ISA 300 on Planning an Audit of Financial Statements, ISA 315 on Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement, ISA 320 on Materiality in Planning and Performing an Audit, ISA 330 on The Auditor's Responses to Assessed Risks, ISA 402 on Audit Considerations Relating to an Entity Using a Service Organization, ISA 450 on Evaluation of Misstatements Identified during the Audit, ISA 500 on Audit Evidence, ISA 501 on Audit Evidence-Specific Considerations for Selected Items, ISA 505 on External Confirmations, ISA 510 on Initial Audit Engagements-Opening Balances, ISA 520 on Analytical Procedures, ISA*

530 on Audit Sampling, ISA 540 on Auditing Accounting Estimates, Including Fair Value Accounting Estimates, and Related Disclosures, ISA 550 on Related Parties, ISA 560 on Subsequent Events, ISA 570 on Going Concern, ISA 580 on Written Representations, ISA 600 on Special Considerations-Audits of Group Financial Statements (Including the Work of Component Auditors), ISA 610 on Using the Work of Internal Auditors, ISA 620 on Using the Work of an Auditor's Expert, (ISQC) 1 on Quality Controls for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance and Related Services Engagements. These auditing standards provide detail provisions on how auditor(s) can succeed in the titanic sometimes job of planning, creating, performing and disseminate an audit program and consequently of an cyber-security audit program, as part of the overall audit program.

With the respect of the above-mentioned internationally recognized auditing standards, in general terms, every auditing tests and evidence gathering process, including this destine to track and mitigate cybersecurity risks, is consisted of three major one after the other steps/particles:

- (i) The first step, the *planning step*, includes the parts of understanding of the cybersecurity areas of concern, risk assessment on them and the development of the most applicable cybersecurity audit programme,
- (ii) The second step, the *execution step*, includes the collection of evidence, fieldwork, conducted mostly through in situ and in vitro testing and sampling, and documentation, and
- (iii) The last step includes the *formation and reporting of conclusions* based in the findings of the previous steps with the issuance of the auditing opinion and the following up.

Since the final step will be examined in the next chapter of this paper, we will examine here the first two steps and most prominently we will analyze them from the cybersecurity scope.

IV] 2. Compliance with Cybersecurity Auditing Frameworks

Due to the great demand for exact and trustworthy guidance in the matter of proper planning, and executing an audit program, a number of organizations had developed an extended list of voluntary standards to guide these processes. These standards are mostly

voluntary in nature, unless countries and international governmental organizations, like the EU, had decided to apply them in obligatory basis according to relevant national and EU laws. For the best fulfillment of the scope of this Master Thesis, we will examine only the cases of relevant to cybersecurity auditing standards that the two most important internationally recognized organizations, the International Standards Organization (ISO) and the Information Systems Audit and Control Association (ISACA), had created until so far. All the examined here standards aims from one side to provide to economic entities a clear framework about the protective mechanism that must implement in order to secure their NHS systems from cybersecurity risks, attacks, vulnerabilities or just the normal operational demands and from the other side provides a clear process on how a cybersecurity audit program must be articulated, and offers a concrete landscape about the capacities that IT auditors must possess in order to best perform their cybersecurity audit programs.

IV] 2. 1. The ISO Cybersecurity Auditing Framework

IV] 2. 1. A) The ISO Auditing and Auditing Management Standards

International Standards Organization (best known as ISO), as the body that creates and promotes standards in worldwide level upon a great variety of sectors in economy together with International Electrotechnical Commission (IEC) had established already a system of standards concerning the auditing sector. The first most important ISO standard of this system is the third edition²⁰⁶ of ISO's 19011 standard published on July 2018, best known as *ISO 19011:2018 - Guidelines for Auditing Management Systems Standard*. In its 46 pages, the Standard provides detailed guidelines upon the auditing principles, on how to

²⁰⁶ The first edition of this standard had been issued in 2002, *ISO 19011:2002 Guidelines for quality and/or environmental management systems auditing*, concerning mostly the conduction of internal and external audit, quality management system audits and environmental management system audits. The ISO 19011:2002 is actually the incorporated advancement of two other families of ISO standards, (a) the ISO 10011 (ISO 10011-1:1990 Guidelines for auditing quality systems — Part 1: Auditing, ISO 10011-2:1991 Guidelines for auditing quality systems — Part 2: Qualification criteria for quality systems auditors, and ISO 10011-3:1991 Guidelines for auditing quality systems — Part 3: Management of audit programmes) and (b) the ISO 14010 (ISO 14010:1996 Guidelines for environmental auditing — General principles, ISO 14011:1996 Guidelines for environmental auditing — Audit procedures — Auditing of environmental management systems, ISO 14012:1996 Guidelines for environmental auditing — Qualification criteria for environmental auditors) all of which had been replaced by the ISO 19011 Family of Standards. It was withdrawn in 2011 by the second edition, *ISO 19011:2011 Guidelines for auditing management systems*, which is applicable more to internal and external (financial) audits than the previous one. The 2011 edition is closer to the third edition mentality than to the 2002, since the last one was more applicable to quality and environmental audits. **ISO**, *ISO 19011:2002 Guidelines for quality and/or environmental management systems auditing*, <https://www.iso.org/standard/31169.html> (last retrieved 25/06/2019) & **ISO**, *ISO 19011:2002 Guidelines for auditing management systems*, <https://www.iso.org/standard/50675.html> (last retrieved 25/06/2019) .

manage and auditing process/programme, on how to conduct management system audits, on the best evaluation of the capacities and competences of the persons (both as individual auditors and audit teams) conducting the auditing activities. The applicability of the standard is extended, since it can be used not only on any planned or executed audit process (internal & external) on management systems, but also on the way an audit plan is managed and for all types of organizations.²⁰⁷

The second most important standard is the second edition of **ISO/IEC 17021-1:2015 Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements**, published in 2015 and which replaced the first edition of 2011. This Standard is consisted in total from seven parts or otherwise technical specifications, as it concerns the competences requirements for auditing and certification in different types of management systems: Part 1, sets general requirements, Part 2, concerns environmental management systems, Part 3, concerns quality management systems, Part 4, concerns sustainability management systems, Part 5, concerns asset management systems, Part 6, concerns business continuity management systems and Part 7, concerns road traffic safety management systems.²⁰⁸ For the purposes of this paper, we must explained that the most relevant parts are Part 1, 3, 5 and 6. Moreover, in section 3 of the document (“*Terms and definitions*”) of the Standard someone can read the definition on what is or must be considered as a certification audit (meaning a third-party certification audit): an audit carried out by an auditing organization independent of the client and the parties, that rely on certification, for the purpose of certifying the client's management system. They include a series of different audits: from initial audits, to surveillance audits, re-certification audits and even special audits. The Standard recognizes as four type of audits, (a) the **simple** one conducted only by one third-party accreditation body, (b) the **joint** one conducted by two or more auditing institutions in a cooperative way, (c) the **combined** one conducted on the provisions and requirements of two or more management system standards altogether and (d) the **integrated** one that takes place when there is the integration of applied requirements of two or more management systems standards into one cohesive management system. The set of requirements and any other additional clarification, that are provided by the ISO/IEC 17021-1:2015, must be presented by any institution and body

²⁰⁷ ISO, *ISO 19011:2018 Guidelines for auditing management systems*, <https://www.iso.org/standard/70017.html> (last retrieved 25/06/2019).

²⁰⁸ ISO, *ISO/IEC 17021-1:2015 Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements* <https://www.iso.org/standard/61651.html> (last retrieved 25/06/2019).

providing management systems certification, as it concerns their consistency, reliability and skillfulness. More specifically, ISO/IEC 17021-1:2015 sets at least seven principles (section 4 in the Standard) that accreditation institutions must have: impartiality, competence, responsibility, openness, confidentiality, responsiveness to complaints and the risk-based approach. In the next sections (Sections 5 to 10) the Standard provides the variety of requirements we mentioned. Those requirements are classified in the following categories: (a) *general requirements*, concerning legal and contractual demands, impartiality, liability and financing, (b) *structural requirements*, concerning not only the organizational structure and the highest levels of management, but also the operational control system of the client, (c) *resources requirements*, that deals with matters like the capacities of the workforce and its involvement in accreditation procedures, the use of external capacities, like external auditors and technical expertise, the quality of personnel records and provisions in case of outsourcing, (d) *information requirements*, about public distributed data, certification documents, confidentiality, the information that are exchanged between the accreditation institution and the client and how to refer to certification documents and how to best use of the marks, (e) *process requirements*, which refers to pre-certification actions, the planning activities, the initial certification processes, the conduction of the audits, the decision process of certification, the maintaining the certification demands, the process of appeals and complaints and finally the affairs on how to keep clients records and documentation, and (f) *management system requirements* for the certification institutions, which includes all the options between the general management requirements to specified ones in accordance with the provisions of ISO 9001²⁰⁹ .²¹⁰

IV] 2. 1. B) ISO/IEC 27000 Standards Family on Information Security Management Systems and Cybersecurity Auditing

A fundamental part of cyberpreparedness has to do with the best preparation of an economic entity to face efficiently and with the less possible cost (economic, functional, in fame, etc.) any cybersecurity attack through adopting well-established, even certified,

²⁰⁹ The ISO 9000 Family of Standards govern the Quality Management Systems.

²¹⁰ **ISO, ISO/IEC 17021-1:2015(EN): Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements**, <https://www.iso.org/obp/ui/#iso:std:iso-iec:17021:-1:ed-1:v1:en> (last retrieved 25/06/2019).

processes. It goes without saying, that International Organization of Standards, as the responsible international organization of creating and issuing worldwide standards, has a pivot role in the best cybersecurity auditing preparedness of economic entities. Indeed, ISO had recognized early on the great importance that information management and security play not only in the survival of an entity, but also in their long-lasting flourishing, by establishing in 1989 the ***ISO/IEC JTC 1/SC 27 Information Security, Cybersecurity and Privacy Protection Technical Committee*** (best known as SC 27). Among the aims of the SC 27 is to create and develop ISO type standards in order to address the issues of best protection of data/information and ICT infrastructure. This means that SC 27 produces not only generic methods, but also techniques and guidelines concerning and material security concerns and data privacy issues. More prominently, the Committee focusses on dealing with the following cybersecurity preparedness issues:

- Development of the methodological framework concerning the cybersecurity sphere,
- Creation of holistic approaches on information management and ICT security issues, like Information Security Management Systems (ISMS), cybersecurity processes, cybersecurity checks and controls balances and cybersecurity services,
- Especially as it concerns ISMS, the Committee develops the compliance demands and requirements concerning their assessment, accreditation, and auditing,
- Development of a framework concerning identity security, biometric data, and privacy demands,
- Development of mechanisms about cryptography and other cybersecurity mechanisms concerning the four basic values of information management: 1) accountability, 2) integrity, 3) availability and 4) confidentiality,
- Creation of the necessary cybersecurity support documentation, such as definitions and terminology documents, relevant guidelines and manuals and procedures concerning the registration process of cybersecurity themes, and
- Creation of cybersecurity evaluation frameworks and the relevant methodological systems.

The SC 27 has 49 participating members and 29 observing members, and its Secretariat is based in Berlin, Germany. Until so far, under the direct responsibility of SC 27 have been issued about 181 ISO cybersecurity preparedness standards, and about 65 relevant standards are under development.²¹¹

²¹¹ ISO, *ISO/IEC JTC 1/SC 27 - Information Security, cybersecurity and privacy protection: About*, <https://www.iso.org/committee/45306.html> (last retrieved 25/06/2019).

The concretization of ISO's response to businesses cyber-preparedness capacities came with the development of the 27000 Family of Standards about Information Security Management Systems (ISMS). ISO/IEC 27000 Family of Standards, first developed in 2009, aims to assist economic institutions/entities to maintain a high level of security as it concerns their information assets. As information assets are considered mostly non-tangible assets, such as a) financial data, b) intellectual property data, 3) human resources data and personnel information and 4) the knowledge and data provided in an entrusted way to the company by third party(ies) entity(ies).

The importance of ISMS is getting more and more enlarged nowadays, due to the fact that their holistic systematic approach targets to manage, secure and protect critical and sensitive data/information for economic entities. This holistic systematic approach is consisted in the application of risk management and assessing processes, that covers not only the IT systems and business processes and procedures, but also the people involved aiming to increase resilience and continuity. An ISMS, such as the one covered by ISO/IEC 27000 Standards Family, can be performed to an entity's NHS systems no matter their size (SMEs or larger companies) or the business sector they belong to. To be certified with an ISO/IEC 27000 Standard is not compulsory, but optionally. An organization can choose if it would like to implement an ISO/IEC 27000 Standard and get certified with the one that fits best in each entity's case. There are two main reasons why companies choose to adopt an ISO/IEC 27000 Standard: 1) to get familiar and to gain benefits from its best practice approach, and 2) to obtain an international recognized certification that will augment the trust of their future and existed customers, clients and other stakeholders.²¹²

The most important ISO/IEC 27000 Family Standards with a cybersecurity auditing importance are:

- **ISO/IEC 27000 on Information technology — Security techniques — Information security management systems — Overview and vocabulary:** first time issued on 2009 and enriched and replaced multiple times until so far (in 2012, in 2014, in 2016), with its fifth edition of 2018 to be the one in current force. The ISO/IEC 27000/2018 contains detailed guidelines and information for all types of economic entities, such as commercial enterprises, government agencies and non-profit organizations as it concerns the acquisition, support and implementation: (i) the understanding of the ISMS family of standards and the terms and definitions of

²¹² ISO, *ISO/IEC 27000 family - Information security management systems*, <https://www.iso.org/isoiec-27001-information-security.html> (last retrieved 25/06/2019).

the ISMS family of standards, (ii) the endorsement of an effective Plan-Do-Check-Act (PDCA) system, (iii) the providing of a sector-specific guideline system for ISMS, and (iv) the creation of an efficient conformity assessment for ISMS.²¹³

- **ISO/IEC 27001:2013 — Information technology — Security techniques — Information security management systems — Requirements:** first time issued on 2005 and the edition of 2013 is the second one with some enrichments conducted the following of 2013 years with ISO/IEC 27001:2013\Cor 1: 2014 and ISO/IEC 27001:2013\Cor 2: 2015. ISO/IEC 27001:2013 provides more clarification and specification regarding the requirements for establishing, applying, preserving, and constantly enhancing an entity-wide ISMS. Moreover, it also specifies further the requirements concerning the evaluation and handling of risk that information security possess and must be customized to the entities needs and capacities. All the provided by ISO/IEC 27001:2013 requirements are generic and applicable to all entities, indifferently their type, size, or nature.²¹⁴
- **ISO/IEC 27002:2013 — Information technology — Security techniques — Code of practice for information security controls:** as the previous standard, it was first time issued on 2005 and the edition of 2013 is the second one with some enrichments conducted the following of 2013 years with ISO/IEC 27002:2013\Cor 1: 2014 and ISO/IEC 27002:2013\Cor 2: 2015. ISO/IEC 27002:2013 provides extended guidelines concerning an entity's information security standards and the applied information security management practices, such as the choosing, deployment and management of controls upon the entity's information security risk environment(s). It is constructed in that way in order to be applicable to entities that aim to: (a) apply controls that comply with ISMS originating from ISO/IEC 27001, (b) apply widely accepted information security controls, and (c) aim to create their own information security management practices and guidelines.²¹⁵
- **ISO/IEC 27003:2017 — Information technology — Security techniques — Information security management systems — Guidance:** first issuance of this

²¹³ **ISO**, *ISO/IEC 27000:2009 Information technology - Security techniques - Information security management systems - Overview and vocabulary*, <https://www.iso.org/standard/41933.html> (last retrieved 25/06/2019).

²¹⁴ **ISO**, *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*, <https://www.iso.org/standard/54534.html> (last retrieved 25/06/2019).

²¹⁵ **ISO**, *ISO/IEC 27002:2013 — Information technology — Security techniques — Code of practice for information security controls*, <https://www.iso.org/standard/54533.html> (last retrieved 25/06/2019).

Guidance took place in 2010. As every ISO Guidance, offers further clarification on the implementation of a main standard, ISO/IEC 27001:2013 in this case.²¹⁶

- **ISO/IEC 27004:2016 — Information technology — Security techniques — Information security management — Monitoring, measurement, analysis, and evaluation:** first issuance of this standard took place in 2009 and this is the second edition of the standard. ISO/IEC 27004:2016 is another standard that can be implemented to entities of all types and sizes, and (a) provides guidelines regarding the monitoring and appraising of an entity's information security performance, (b) evaluates the effectiveness of the entity's ISMS, processes and controls in order to accomplish the requirements of ISO/IEC 27001:2013 and (c) analyzes and assesses the outcomes of (a) and (b).²¹⁷
- **ISO/IEC 27005:2018 — Information technology — Security techniques — Information security risk management:** the first edition of this standard was issued on 2008, the second on 2011 and the 2018 is the third and more recent edition of this standard. ISO/IEC 27005:2018 as other ISO's standards can apply to all types of organizations, such as commercial entities, government agencies, and non-profit organizations, that aim to manage risks able to impact the entity's information security capacities. This standard (a) provides assistance in the general aspects that ISO/IEC 27001 specialized and (b) offers support in the best application of the entity's risk management information security. For the best enforcements of this standard the user must have a solid understanding upon concepts, models, processes, and terminologies that ISO/IEC 27001 and ISO/IEC 27002 incorporate.²¹⁸
- **ISO/IEC 27006:2015 on Information technology — Security techniques Requirements for bodies providing audit and certification of information security management systems:** this standard has been updated, revised and enriched two times since 2007, when it first issued, in 2011 (second edition) and in 2015 (third edition), so now the applicable version is the third edition of this standard. The Standard is highly connected with the other standards of ISO that we described in the previously (a) the ISO/IEC 17021-1 and (b) the ISO 27001. Despite the fact that, this Standards was principally designed to assist the accreditation process of

²¹⁶ ISO, ISO/IEC 27003:2017 — Information technology — Security techniques — Information security management systems — Guidance, <https://www.iso.org/standard/63417.html> (last retrieved 25/06/2019).

²¹⁷ ISO, ISO/IEC 27004:2016 — Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation, <https://www.iso.org/standard/64120.html> (last retrieved 25/06/2019).

²¹⁸ ISO, ISO/IEC 27005:2018 — Information technology — Security techniques — Information security risk management, <https://www.iso.org/standard/56742.html> (last retrieved 25/06/2019).

organizations (called as “*bodies*”) that provide ISMS certifications, meaning to accredit the accreditors. The Standard can also be useful not only as “*criteria document for accreditation*”, but also as a tool for peer assessments and other audit performances. In its 35 pages contains specific requirements and guidelines on how institutions can provide audit and certification as it concerns an ISMS, additionally to the requirements and conditions that ISO/IEC 17021-1 and ISO 27001 provide. The logic of ISO/IEC 27006:2015 follows the relevant logic of ISO/IEC 17021-1, as it concerns the definition, the series of audits (initial, surveillance, re-certification and special audits, the types (simple, joint, combined and integrated), the principles, and the requirements (general requirements, structural requirements, resources requirements, information requirements, process requirements, management system requirements for the certification institutions), the way we described them previously, but it focus its attention to ISMS and not in management systems in general.²¹⁹

- **ISO/IEC 27007:2017 on Information Technology – Security Techniques – Guidelines for information security management systems auditing:** this is the second edition of the Standard with the first edition to be issued in 2011²²⁰. In its 41 pages the ISO/IEC 27007:2017 gives detailed guidelines about ISMS audit programs on how to perform and conduct audit trails and on the auditors’ capacities and competences, in supplementary conjunction to the relevant guidance provided by ISO 19011:2011, of which the structure follows. The Standard, that can be useful for institutions of all types and sizes, provides guidance not only for accredit bodies that provide relevant certification, but also to both internal (so called “first party”) and external and third-party auditing individuals, teams and firms (so called “second party”), according to ISMS audits complexity and magnitude, as well as the ISMS auditing schemes that must comply with ISO/IEC 27001. The Standard sets the criteria for best performance of auditors’ capacities, skills and evaluation. The Standard can be used even in cases of external audits upon ISMS compliance conducted for reasons apart a third-party management certification process. Moreover, ISO/IEC 27007:2017 can be an additional resource of guidance as it

²¹⁹ **ISO**, *ISO/IEC 27006:2015 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*, <https://www.iso.org/standard/62313.html> (last retrieved 25/06/2019). **ISO**, *ISO/IEC 27006:2015 (en): Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*, <https://www.iso.org/obp/ui/#iso:std:iso-iec:27006:ed-3:v1:en> (last retrieved 25/06/2019).

²²⁰ This standard is in the process to be updated in order to be enriched with the aspects of cybersecurity and privacy protection.

concerns the fulfillment of requirements under ISO/IEC 27006. ISO/IEC 27007:2017 can provide significant guidance to requirements derived from ISMS audits, such as: (i) those set by ISO/IEC 27001:2013, (ii) those set by policies and necessities given by parties with a related interest, (iii) those set by regulations and law, (iv) those set by the examined organization and all other related institutions within the an ISMS processes and control performances and (v) those set for ISMS plans having to deal with certain criteria of an ISMS audit, like those upon planning and conducting audit(s), achieving objectives plans, risk and opportunities dealing plans, project plans, keeping audit records, improving continuous process, reporting, etc.)²²¹

- **ISO/IEC 27008:2019 on Information technology — Security techniques Guidelines for auditors on information security controls:** the 91 pages of the second edition of this Standard (the first one was issued in 2011) contain extended guidance as it concerns the implementation and functionality of technical controls on information security provisions, such as IT controls and cybersecurity controls, concerning mostly technical assessment of those controls, in order to comply with all the set of requirements on information security the organization has set and must follow according to ISO/IEC 27001. The Standard follows the applicability fitness of other ISO standards and can be ideal to all types and sizes of institutions, no matter if those are public or private corporations, government or organizations, non-profit entities, as long as they perform technical assessment and compliance controls and evaluations on information security systems, such as IT controls, cybersecurity controls, servers, storage and network virtualizations controls, cloud services controls, physical and environmental security controls, incidence response controls, etc. The information security controls must be characterized by at least for major qualities: (i) the *fit-for-purpose requirement*, meaning that must be suitable for the purpose must deal with, for example appropriate enough for mitigating information risks, (ii) the *effectiveness requirement*, meaning that must be well-designed, specified, take place and dealt in the right way and time, and maintained in the most appropriate way, (iii) the *efficiency requirement*, meaning they must enhance institutions net value, and (iv) the *improvement requirement*, meaning to identify and implement the necessary advancing changes. The goals of these controls must be to offer a customized flexicurity, as it concerns not only an organizations mission, aims, policies and needs (general goal), but also to mitigate the risks deriving from

²²¹ ISO, ISO/IEC 27007:2017 *Information technology — Security techniques — Guidelines for information security management systems auditing*, <https://www.iso.org/standard/67398.html> (last retrieved 25/06/2019).

emerging threats and vulnerabilities, functionality and operational concerns and dependencies on ISMS (cybersecurity goal) in a cost-effective, added-value, business-friendly way.²²²

- **ISO/IEC 27009:2016 — Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements:** this is the first edition of this standard, that aims to provide further specification upon the requirements and the implementation of controls of ISO/IEC 27001, in order to be applicable to all sectors, such as the field, the application area, and the market sector. The standard targets that the set supplementary or enhanced requirements are in compliance and not in conflict with the requirements established by ISO/IEC 27001.²²³
- **ISO/IEC 27010:2015 — Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications:** the first edition of the standard was issued in 2012 and the current is the second edition of it. ISO/IEC 27010:2015 (a) offers guidelines that enrich the general framework established by ISO/IEC 27000 family of standards, as it concerns the application of information security management within information sharing environments, (b) delivers controls and guidance regarding the introduction, application, maintenance, and amelioration of information security in inter-organizational and inter-sector communications, by using established messaging and other technical communication methods and channels and (c) encourages international cooperation and growth of information sharing communities. This Standard can be implemented in all types of exchange and sharing of sensitive information, concerning not only public, but also private entities, irrelevantly if they function nation-wide or/and internationally and regardless if they operate within the same industry or in market sector or between any sector or if it is related to a nation's critical infrastructure.²²⁴
- **ISO/IEC 27011:2016 — Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations:** this is the second edition of this standard, while

²²² ISO, *ISO/IEC 27008:2019 Information technology — Security techniques — Guidelines for auditors on information security controls*, <https://www.iso.org/standard/67397.html> (last retrieved 25/06/2019).

²²³ ISO, *ISO/IEC 27009:2016 — Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements*, <https://www.iso.org/standard/42508.html> (last retrieved 25/06/2019).

²²⁴ ISO, *ISO/IEC 27010:2015 — Information technology — Security techniques — Information security management for inter-sector and inter-organisational communications*, <https://www.iso.org/standard/68427.html> (last retrieved 25/06/2019).

the first edition was issued in 2008. The standard (a) provides further guidelines as it concerns the implementation of information security controls in telecommunications entities, and (b) the standard assists those telecommunications organizations, that will choose to adopt it, to fulfil the basic information security management requirements of this sector and more precisely the principles of confidentiality, integrity, availability and any supplementary related security property principles.²²⁵

- **ISO/IEC 27017:2015 on Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services:** this Standard is in its first edition and provides guidelines as it concerns implementation and additional control of information security controls and cloud services, such as: (i) cloud specific concepts on cloud sector, (ii) information security policies, (iii) organization and information security, (iv) human resources security, (v) access controls, (vi) cryptography, (vii) physical and environmental security, (viii) operations security, (ix) communications security, (x) system acquisition, development and maintenance, (xi) relationship with suppliers, (xii) information security incident management, (xiv) information security and business continuity and (xv) compliance aspects. The implementation guidance about controls is connected to ISO/IEC 27002.²²⁶
- **ISO/IEC 27043:2015 on Information technology — Security techniques, Incident investigation principles and processes:** this standard is in its first edition and provides guidelines upon idealized models for ordinary incident investigation processes and principles, such as pre-incident preparation through investigation, general advice and warnings on such processes, security incident event management, forensic and governance investigations, electronic discovery investigation techniques, incident management, planning and preparation investigations, etc., applicable to various incident investigation scenarios involving handling, analysis and interpretation of digital evidence and digital evidence investigations, like unauthorized access incidents, data corruption, secure storage and storage

²²⁵ ISO, *ISO/IEC 27011:2016 — Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations*, <https://www.iso.org/standard/64143.html> (last retrieved 25/06/2019).

²²⁶ ISO, *ISO/IEC 27017:2015(en) Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*, <https://www.iso.org/standard/43757.html> (last retrieved 25/06/2019).

Cyber-security and Cyber-preparedness as a Necessary Part of the Auditing Process
sanitization, system crashes and intrusion prevention and detection, and corporate data breaches.²²⁷

IV] 2. 2. ISACA'S Cybersecurity Auditing Framework

Information Systems Audit and Control Association or best known from the acronym ISACA is a non-governmental, non-profit international independent association, that provides for more than 50 years qualitative creation, development, establishment, implementation and adoption of internationally accepted standards and practices upon IS audit and controls, providing at the same time training and certification schemes for professionals and enterprises that desire to augment their cybersecurity auditing and control performance skills and capacities. Moreover, ISACA's publications aims to raise awareness and provide guidance in domains related with the above-mentioned cybersecurity auditing critical points of focus. For example, as it concerns the steps of planning IS Audit Programs *ISACA's Five-Steps to Planning for an Effective Information Systems (IS) Audit Program*²²⁸, recognizes the following methodological steps:

1. *Determine audit subject*: such as the identification of the cyber-security areas that must be audit and vary from business functions, to NHS systems their physical protection.
2. *Define audit objective*: that shapes the identification of the audit scope and purpose or purposes
3. *Set audit scope*: that assists in the identification of the specific NHS systems, functions, operations, units of the client entity that must be part of the audit inspection program.
4. *Perform pre-audit planning*: is consisted of the conduction of the risk assessment performance, the identification of compliance and regulatory obligations of the client entity, and the determination of the resources and capacities needed, in order to best perform the audit program.
5. *Determine audit procedures and steps for data gathering*: that shapes the basic components of the overall audit strategy of the audit program and is consisted of activities like: understanding the departmental policies, practices, standards and codes,

²²⁷ ISO, ISO/IEC 27043:2015(en) *Information technology — Security techniques — Incident investigation principles and processes*, <https://www.iso.org/standard/44407.html> (last retrieved 25/06/2019).

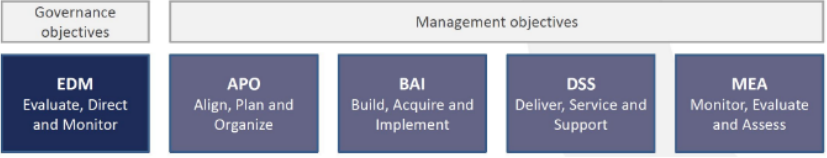
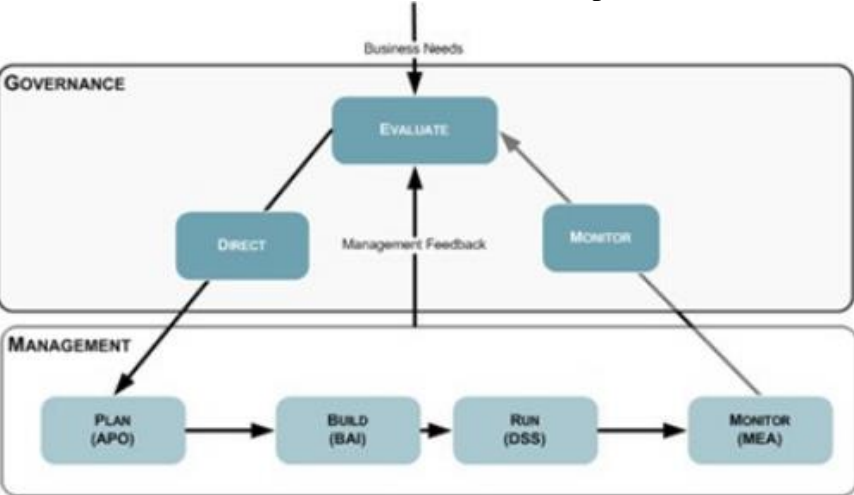
²²⁸ Cooke Ian (2017), *IS Audit Basics: Audit Programs*, ISACA Journal, Issue 2017, Volume 4, <https://www.isaca.org/resources/isaca-journal/issues/2017/volume-4/is-audit-basics-audit-programs> (last retrieved 25/06/2019).

additional to the requirement of compliance with regulatory obligations, identifying the individual that must be interviewed or external institutions, that must provide evidences, identifying and developing the methods and tools that will be applied for controls testing and verification, the creation of the necessary test scripts, detection of criteria for best examination and evaluation of the tests and lastly, the creation of methods and tools that will measure the accuracy and reliability of the performed tests, and where necessary to reperform the tests.

Moreover, ISACA had created and released specific guidelines frameworks for cyber-related professionals about the proper conduction of IS audit and controls inspections, that act as high-quality non-obligatory cyber(security) auditing standards for professionals, modern entities, and organizations. In the following pages we will examine two of these frameworks, the Control Objectives for Information and Related Technologies, best known as COBIT and Information Technology Assurance Framework, best known as ITAF and the accreditation schemes ISACA offers for experienced cyber-related professionals.

1] Control Objectives for Information and Related Technologies or COBIT: ISACA's COBIT is a framework developed for IT management in order to assist entities to create, optimize and apply the most appropriate strategies and policies for effective information management and governance. The first edition of COBIT was released in 1996, and in late 2018 ISACA released the newest edition, COBIT 2019, as the Table No 5 in this page indicates.

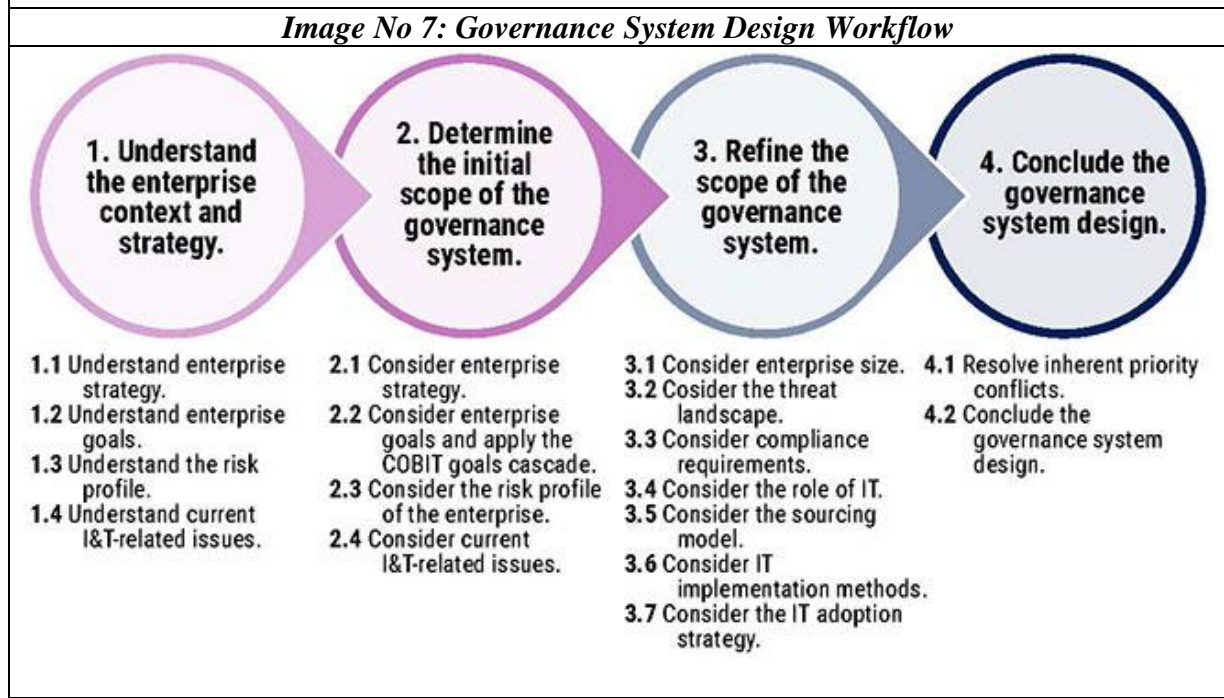
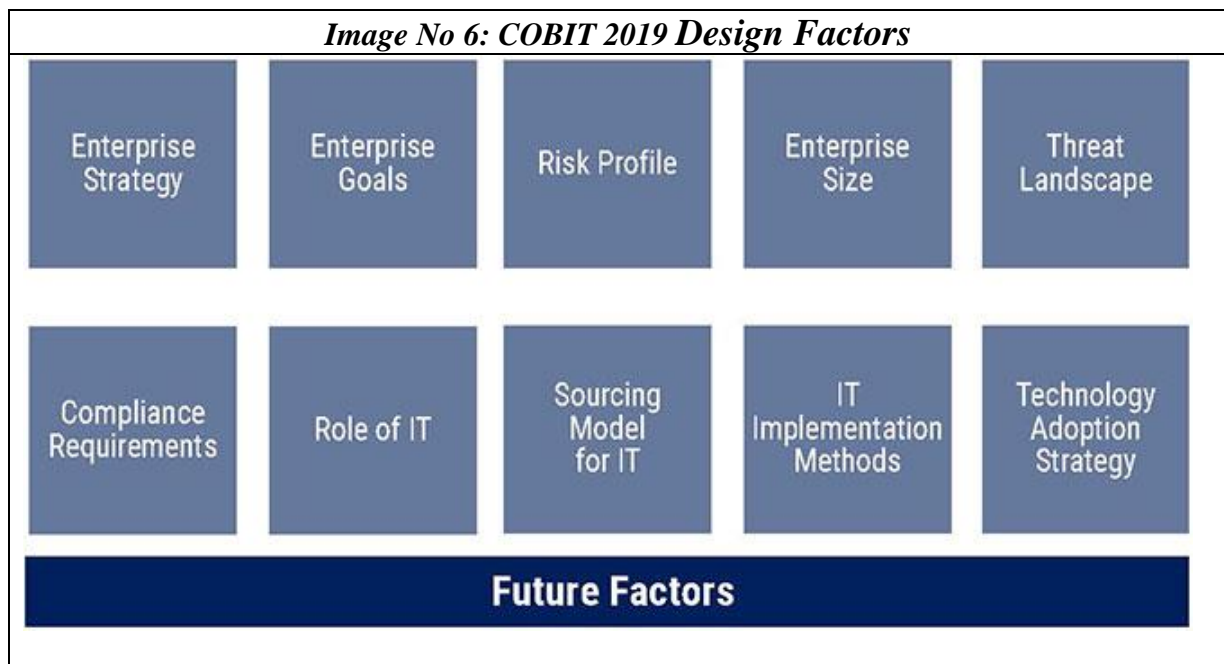
<i>Table No 5: Short History of COBIT Evolution</i>		
<i>Year of Release</i>	<i>Edition</i>	<i>What is New?</i>
1996	COBIT 1	Initially designed to provide guidance to auditors on how to better comprehend and assess IT landscapes and IT controls.
1998	COBIT 2	Expands the frameworks applicability beyond auditing community and auditing needs, due to demand from corporate audience and leadership for more guidance in internal controls inspections.
2000	COBIT 3	Introduces the IT management and information governance practices and qualities, that are present in the framework ever since.
2005	COBIT 4	Connects IT strategy and communication technologies governance with management, but the IT control objectives are considered quite complicate from the marketplace.
2007	COBIT 4.1	Due to the complexity and extension of COBIT 4 the 4.1 edition offered a reduced set of IT control objectives
2012	COBIT 5	Presents a comprehensive model for the IT governance, that aligns IT strategy with the overall management strategy on an entity, in connection with other internationally acknowledged standards, like ISO/IEC and ITIL. It promotes 37 processes in the following five governance and management objectives structure, according to the

		<p>scheme below:</p>  <p>Source: ISACA (2018)</p> <p>Governance objectives target to ensure that: (a) the stakeholder demands, terms and decisions are assessed in order to ascertain the entity’s reasonable, approved objectives, (b) priorities and proper decision making sets the leadership pathway and (c) adequate performance and compliance are supervised and monitored against agreed-on direction and objectives.</p> <p>Management objectives are guiding, creating, establishing and monitor all the actions according to target by an entity general objectives and goals.</p>
<p>2018</p>	<p>COBIT 2019</p>	<p>The newest edition keeps the five governance and management objectives approach of COBIT 5, but augments the number of processes to 40, and focus to areas, like information security, digital transformation, cloud concerns, robotics, DevOps, and more.</p>  <p>source: ISACA</p>
<p>Source: Tessin Peter (07/04/2016), <i>COBIT Celebrates 20 Years of Guidance</i>, https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2016/cobit-celebrates-20-years-of-guidance (last retrieved 25/06/2019). White Sarah K. (15/01/2019), <i>What is COBIT? A framework for alignment and governance</i>, https://www.cio.com/article/3243684/what-is-cobit-a-framework-for-alignment-and-governance.html (last retrieved 25/06/2019).</p>		

COBIT 2019, the newest and most advanced edition of this framework, introduces the enterprise governance of information and technology approach (also known as EGIT), by promoting a more customized and tailor-made IT governance in the entities, that aim to increase their value and integrity, to better optimize their resources and to deal more effectively with their risks. COBIT is consisted of the following framework materials:

- **COBIT® 2019 Framework: Introduction and Methodology:** is the main guide that provides assistantship about the basic COBIT principles and the structure of the framework.
- **COBIT® 2019 Framework: Governance and Management Objectives:** a companion guide that explains the COBIT Core Model and its 40 governance and management objectives. For each objective, it provides explanation about its purpose, its connection with enterprise goals and how it succeeds in achieving these goals.
- **COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution:** this is a companion guide, that provides in-depth guidance for the creation and establishment of customized and tailored-made dynamic IT governance system in entities, and the entity's size, sector, needs, mission, vision and goals, processes, organizational structure, technological choices, applications and IT role, compliance requirements, style of management style, potential threats, etc., based on a number of critical factors, also known as design factors, which are in reality all the factors that may impact an entity's governance system and the successful use of IT. In general terms, design factors can be categorized in the following classification: (a) *contextual design factors*: referring to those that can impact the entity but are outside its control, like the geopolitical and threat landscapes that an entity faces, (b) *strategic design factors*: that impact the decision-making processes of the entity, like an entity's strategies, the risk appetite of the management, the role of IT in general success and advancement, (c) *tactical design factors*: that impact the choices of the entity in implementation of resources (for example if the entity uses outsourcing, cloud services, etc.), IT technologies and technology adoption strategies, as the Image No 6 indicates. Moreover, this guide, as the Image No 7 below indicates, provides better understanding in the tailored-made design workflow IT governance system, that is consisted of four major steps: (a) the first step, provides better understanding in the entity's context, strategies, goals, risk appetite and present IT concerns, (b) the second step, provides better consideration and concretization upon the initial scope of the entity's governance system and how COBIT goals and structure can be implemented, (c) the next step, provides better enhancement upon the scope of the governance system, such as taking under consideration the entity's size, threat landscape, compliance obligations, role of IT and their implementation methods and adaptation strategies, and (d) the last step, provides

final conclusions upon the governance customized system design, by providing resolutions inherent conflicts and issues.²²⁹



Sources: Rafeq Abdul (04/02/2019), *COBIT Design Factors: A Dynamic Approach to Tailoring Governance in the Era of Digital Disruption*, ISACA, <https://www.isaca.org/resources/news-and-trends/newsletters/cobit-focus/2019/cobit-design-factors#:~:text=COBIT%202019%20also%20defines%20the,prioritize%20this%20content%20as%20required> (last retrieved 25/06/2019).

²²⁹ Rafeq Abdul (04/02/2019), *COBIT Design Factors: A Dynamic Approach to Tailoring Governance in the Era of Digital Disruption*, ISACA, <https://www.isaca.org/resources/news-and-trends/newsletters/cobit-focus/2019/cobit-design-factors#:~:text=COBIT%202019%20also%20defines%20the,prioritize%20this%20content%20as%20required> (last retrieved 25/06/2019).

➤ **COBIT® 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution:** the last companion guide provides assistantships as it concerns the implementation of the customized IT governance strategy that was developed in the previous section. It includes best practices, methods on how to avoid and solve hazards and difficulties and how to best adapt the designed COBIT 2019 into the previous applying COBIT 5 strategy.²³⁰

COBIT 2019 provides the following training and accreditation schemes, for individuals that desire to enrich and demonstrate their capacities and knowledge about the framework:

- ❖ ***COBIT Bridge Workshop:*** with this one-day course someone can grasp the basic concepts, models, and key definitions of COBIT 2019 and to understand better the differences between COBIT 5 and COBIT 2019.²³¹
- ❖ ***COBIT 2019 Foundation Certificate Program:*** provides verification about the skills, knowledge, and practical capacities on optimizing information and technology governance, based on the EGIT approach of COBIT 2019 and other leading internationally recognized relevant standards.²³²
- ❖ ***COBIT 2019 Design and Implementation Certificate Program:*** this certification is available from mid-2019 and provides skills upon on how to design and implement a customize appropriate fitted governance IT system using COBIT.²³³
- ❖ ***Implementing the NIST Cybersecurity Framework Using COBIT 2019 Training and Certificate Program:*** in general terms COBIT 2019 was being built in alignment and connection with the most important, leading and internationally recognized relevant cybersecurity standards models and good practices, such as NIST, ITIL, ISO/IEC 27000 Standards Family, CMMI, TOGAF, etc. More precisely, as it concerns NIST COBIT 2019 offers training and verification on how to best integrate

²³⁰ ISACA (2019), *COBIT 2019 Publications*, <https://www.isaca.org/resources/cobit> (last retrieved 25/06/2019).

²³¹ White Sarah K. (15/01/2019), *What is COBIT? A framework for alignment and governance*, <https://www.cio.com/article/3243684/what-is-cobit-a-framework-for-alignment-and-governance.html> (last retrieved 25/06/2019).

²³² ISACA (2019), *COBIT 2019 Foundation Certificate Program*, <https://www.isaca.org/credentialing/cobit/cobit-foundation> (last retrieved 25/06/2019).

²³³ ISACA (2019), *COBIT 2019 Design and Implementation Certificate Program*, <https://www.isaca.org/credentialing/cobit/cobit-design-and-implementation> (last retrieved 25/06/2019).

cybersecurity standards and concepts in the EGIT approach that COBIT 2019 applies.²³⁴

III Information Technology Assurance Framework or ITAF: ISACA's recognizes ITAF as a comprehensive professional practices framework for IS audit and assurance professionals to seek guidance, research policies and procedures, obtain audit and assurance programmes and develop effective reports. More precisely, ITAF provides compliance and good practices guidance upon the following areas: (a) the creation, execution and reporting of IS audits and assurance duties, (b) defining terms and concepts about IS assurance, and (c) establishing standards concerning IS audit and assurance professional roles and responsibilities, knowledge, skills and diligence, conduct, and reporting obligations. COBIT latest editions incorporate ITAF.

ITAF is from 2014 in its third edition and is consisted of

(a) *IS Audit and Assurance Standards*, which (i) specify required and mandatory controls of IS auditing/assurance processes, assisting like that professionals about the minimum level of acceptable performance that complies with ISACA's Code of Professional Ethics Standards²³⁵, (ii) provide proper information to the management and other interested parties about what they must expect professionally from practitioner,s and (iii) especially for holders of Certified Information Systems Auditor (CISA – see next sub-section about

²³⁴ ISACA (2019), *Implementing the NIST Cybersecurity Framework Using COBIT 2019 Training and Certificate Program*, <https://www.isaca.org/credentialing/cobit/implementing-the-nist-cybersecurity-framework-using-cobit-2019> (last retrieved 25/06/2019).

²³⁵ ISACA had set in its Code of Professional Ethics seven important principles for all its member and its certification holders that govern their behavior when the execute their duties: "1) Support the implementation of, and encourage compliance with, appropriate standards and procedures for the effective governance and management of enterprise information systems and technology, including: audit, control, security and risk management. 2) Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards. 3) Serve in the interest of stakeholders in a lawful manner, while maintaining high standards of conduct and character, and not discrediting their profession or the Association. 4) Maintain the privacy and confidentiality of information obtained in the course of their activities unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties. 5) Maintain competency in their respective fields and agree to undertake only those activities they can reasonably expect to complete with the necessary skills, knowledge and competence. 6) Inform appropriate parties of the results of work performed including the disclosure of all significant facts known to them that, if not disclosed, may distort the reporting of the results. 7) Support the professional education of stakeholders in enhancing their understanding of the governance and management of enterprise information systems and technology, including audit, control, security and risk management". Any failure to comply with this Code can lead to an investigation against a member or certification holder and even to disciplinary measures. Moreover, ISACA had introduced an anti-harassment policy," for any inappropriate verbal or physical conduct that shows hostility of a person's race, skin color, religion, gender, national origin, sexual orientation, gender identity, age, disability, veteran status or other such characteristic. Slurs, jokes, insensitive cultural references, use of stereotypes, hostility, insults and/or expressions of hatred or dislike directed at groups or individuals as members of groups within society can all be examples of prohibited harassing conduct." Last but not least, ISACA strictly prohibits any conduct that can be considered as sexual harassment in its Policy against sexual harassment. ISACA (2019), *Code of Professional Ethics*, <https://www.isaca.org/credentialing/code-of-professional-ethics> (last retrieved 25/06/2019).

accreditation schemes) provide description of their professional requirements and any failure to comply with these standards may end up with an investigation against the examined CISA holder by ISACA’s Board of Directors or any other appropriate committee may even result to disciplinary arrangement against the CISA holder, and (iv) are divided in three categories of guidance: general, performance and reporting, accordingly to the part of IS Audit/Assurance they try to facilitate,

(b) *IS Audit and Assurance Guidance*, which are designed to facilitate the standards implementation, recommendations, and best practices by following the same triple categorization as the Standards, and to assist practitioners in accomplishing alignment with the Standards,

(c) *IS Audit and Assurance Tools and Techniques*, which are documents (such as white papers, reference books, IS audit/assurance programs, glossary, COBIT 5 family of products) that provide step-by step instructions and additional guidance for IS audit and assurance professionals. In the following table, Table No 6, we present the full scheme of both Standards and Guidance:²³⁶

Table No 6: Presentation of ITAF’s 2014 Standards and Guidance System		
STANDARDS SERIES NUMBER	SUBJECT	GUIDELINES SERIES NUMBER
1000 series	General (provide broad guiding principles upon the ways IS assurance profession is conducted. They have a wide application about the proper execution of all IS audit and assurance professional duties, additional to related to professionals’ ethics, independence, objectivity and due care, capacities, competencies, and skills.)	2000 series
1001	Audit Charter	2001
1002	Organizational Independence	2002
1003	Professional Independence	2003
1004	Reasonable Expectation	2004
1005	Due Professional Care	2005
1006	Proficiency	2006
1007	Assertions	2007
1008	Criteria	2008
1200 series	Performance (Assist in more detailed parts of the IS audit assignment, such as planning and supervision, materiality, audit and assurance evidence, and the use of external experts, etc.)	2200 series

²³⁶ ISACA (01/05/2016), *Standards, Guidelines, Tools and Techniques*, ISACA Journal, Issue 2016, Volume 3, <https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/standards-guidelines-tools-and-techniques> (last retrieved 25/06/2019).

1201	Engagement Planning	2201
1202	Risk Assessment in Planning	2202
1203	Performance and Supervision	2203
1204	Materiality	2204
1205	Evidence	2205
1206	Using the Work of Other Experts	2206
1207	Irregularity and Illegal Acts	2207
	Sampling	2208
1400 series	Reporting (provide assistantship about the genres of IS audit and assurance reports, the means of communication and disclosure, and the data and information that must be included)	2400 series
1401	Reporting	2401
1402	Follow-up Activities	2402
Source: ISACA (01/05/2016), <i>Standards, Guidelines, Tools and Techniques</i> , ISACA Journal, Issue 2016, Volume 3, https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/standards-guidelines-tools-and-techniques (last retrieved 25/06/2019).		

III] Accreditation Schemes: ISACA, apart the COBIT accreditation programs, provides also the following highly distinguish and internationally accepted certifications for high-skilled cybersecurity professionals:

- **Certified Information Systems Auditor (CISA):** the most famous and rewarded standard of achievement among ISACA’s certifications with more than 151,000 CISA holders. This certification is best suitable for professionals with at least five years related experience, who audit, control, monitor and assess the information technology and business systems of an entity and allows them to be adequate prepared in implementing ISO/IEC 17024:2012. It signifies the knowledge and expertise of its holder in the following cybersecurity domains: (a) information systems auditing process, (b) IT governance and management, (c) acquisition, development and implementation of IS, (d) operability and business resilience of IS and (e) information assets protection.²³⁷
- **Certified in Risk and Information Systems Control (CRISC):** a quite specialized certification with more than 26,000 holders, focused in IT risks identification and management and IS controls maintenance. CRISC also provides adequate preparation for those involved with ISO/IEC 17024:2012 and signifies at least five years knowledge and

²³⁷ ISACA (2019), *Credentialing: CISA*, <https://www.isaca.org/credentialing/cisa> (last retrieved 25/06/2019).

expertise in the following domains: (a) IT risk identification, (b) IT risk assessment, (c) risk response and mitigation and (d) risk and control monitoring and reporting.²³⁸

- ***Certified in the Governance of Enterprise IT (CGEIT)***: a very specialized certification with just slightly more than 8,000 holders, that also provides adequate preparation for those involved with ISO/IEC 17024:2012. It signifies at least five years of knowledge and expertise in the following domains: (a) IT governance and management, (b) strategic management, (c) benefits realization, (d) risk optimization and (e) resources optimization.²³⁹
- ***Certified Data Privacy Solutions Engineer (CDPSE)***: with 80 countries in global scale to have established a kind of privacy and data protection legislation, CDPSE is the first experience-based, technical certification of that cybersecurity aspect. CDPSE aims to verify qualified professionals' effective privacy capacities, to demonstrate their ability of applying privacy by design solutions and their risks mitigation skills correlated with an entity's objectives, risk behavior, consumers' trust priorities and data privacy compliance demands. It signifies at least five years of working knowledge and expertise (minimum three for holders of the other mentioned here ISACA certificates) in the following domains: (a) privacy governance, (b) privacy architecture and (c) data lifecycle. CDPSE can be related with the following cybersecurity professional working roles: lead software engineer, data and system privacy engineer, privacy analyst, privacy advisor and consultant, security and privacy manager, lead privacy manager, security and privacy engineer, software engineer, back-end privacy engineer, management privacy engineering, domain architect, legal care compliance officer, privacy solutions architect, information security engineer, user data protection officer.²⁴⁰
- ***Cybersecurity Audit Certificate Program***: this novel ISACA's program aims to validate audit/assurance, security, and IT risk professionals upon: (a) capacities in understanding cybersecurity risks and applying mitigating controls, and (b) competences in planning and executing cybersecurity-related audits. More precisely, offers training²⁴¹ in the following cybersecurity auditing domains: (i) knowledge about security compliance

²³⁸ ISACA (2019), *Credentialing: CRISC*, <https://www.isaca.org/credentialing/crisc> (last retrieved 25/06/2019).

²³⁹ ISACA (2019), *Credentialing: GDEIT*, <https://www.isaca.org/credentialing/cgeit> (last retrieved 25/06/2019).

²⁴⁰ ISACA (2019), *Credentialing: CDPSE*, <https://www.isaca.org/credentialing/certified-data-privacy-solutions-engineer> (last retrieved 25/06/2019).

²⁴¹ ISACA offers the following training choices according to individuals learning pathways and needs: an online, self-paced course, a virtual instructor-led course, an in-person training workshop, or onsite training for the whole enterprise.

frameworks and best practices, (ii) threats and vulnerabilities assessment and management tools, (iii) establishing procedures for secure authorization, (iv) clarification upon all aspects and features of cybersecurity governance, (v) knowledge about firewall and network security applications and technologies, (vi) knowledge about identification of identity and information access management, of security control implementation, of cloud strategies vulnerabilities, weaknesses and controls, and of legal and regulatory requirement and compliance evaluations, (vii) cybersecurity and third-party risks assessments and performance, (viii) assets management practice advancement, alignment and modification and (ix) understanding and identification of advantages and risks of containerization, a type of virtualization of operating system (OS), that use isolated spaces, known as containers, among the same applied OS.²⁴²

- **Cybersecurity Nexus (CSX):** ISACA from 2017 provides on-demand training and accreditation through performance testing in specific cybersecurity knowledge and real-world cybersecurity skills and capacities, like: (i) *advanced exploitation*, on in-depth system and network information collection methods, on identification and mapping networks of interest and vulnerable Transmission Control Protocol/Internet Protocol (TCP/IP) services, on assessing wireless and firewall security and technologies, etc., (ii) *forensic analysis and advanced forensic*, on file investigation and recovery, on evidence and processes documentation, on forensics reporting, etc., (iii) *cybersecurity fundamentals*, like cybersecurity architecture principles, protection and security of networks, systems, applications and data, incident response, security implications and adoption of evolving technologies, (iv) *Linux application and configuration*, (v) *network application and configuration*, (vi) *packet analysis*, like understanding the role of online communication packets, their components, applications, devices and wireless usage, defining protocol, ports and packet analysis, packets attack recognition, etc., (vii) *penetration testing overview*, (viii) *CSX Technical Foundations*: provided for individuals that had successfully passed all the following CSX Network Application and Configuration Certificate (v case), *CSX Linux Application and Configuration Certificate* (iv case) and *CSX Packet Analysis Course Certificate* (vi case), and (ix) *vulnerabilities and exploitation analysis*: on vulnerabilities scan and analysis performing, networks scanning, back-door implementation, exploitation tracks covering, etc.²⁴³

²⁴² ISACA (2019), *Credentialing: Cybersecurity Audit Certificate*, <https://www.isaca.org/credentialing/cybersecurity%20audit%20certificate> (last retrieved 25/06/2019).

²⁴³ ISACA (2019), *Credentialing: Certificates*, <https://www.isaca.org/credentialing/cybersecurity> (last retrieved 25/06/2019).

- ***CSX Cybersecurity Practitioner (CSX-P)***: is one of the Cybersecurity Nexus Training platform accreditations, the first and only wide-ranging performance certification scheme capable to test the adequacy and competence of an individual in conducting internationally authenticated cybersecurity capacities and skills, according to NIST Cybersecurity Framework five cybersecurity functions of Identification, Protection, Detection, Response and Recovery. More specifically in the field of Identification examines the capacity in recognizing and understanding the business and security environment, in the field of Protection examines the capacity of operational security preparedness and readiness, in the field of Detection examines the capacity of threat detection and evaluation, and in the fields of Response and Recovery examines the response and recovery capacities in case of an incident. CSX-P demands from candidates to demonstrate critical cybersecurity skills in live, virtual and proctored environments, additionally to the ability of presenting analytical skills in identifying assets, and to the capacity of resolving network and host cybersecurity issues by implementing significant cybersecurity knowledge and skills as an emerged cybersecurity first responder expert can perform. This hands-on, performing demonstrating confirmation process validates a variety of cybersecurity capacities for real-world cybersecurity situations and scenarios, ensures high level of professional performance, credibility and recognition among personnel, peers, colleagues, and firms. CSX-P examines the capacities of identification and documentation cybersecurity vulnerabilities assessment, critical assets specification and technical impacts recognition, multiple sources use and obtaining information (such as logs, data events, network reviews) in order (i) to track threat intelligence, (ii) to detect incident analytics and metrics (iii) to respond in anomalous events and incidents, (iv) to implement and evaluate cybersecurity controls (such as those related with security of NHS systems) according to the entity's policies, strategies and compliance requirements, (v) to detect and prevent from compromising any irregular potential or existing activity, intrusion and threat to NHS systems from internal, external and third-party sources, (vi) to carry out an initial attack assessment in order to define the pathways, intentions, extend and influence of an attack, and (vii) to perform specialized response plans in order to restrict negative impact and harm on damaged assets.²⁴⁴
- ***Certified Information Security Manager (CISM)***: another Cybersecurity Nexus Training Platform accreditation, a quite specialized certification with more than 46,000 holders, that also provides adequate preparation for those involved with *ISO/IEC 17024:2012*

²⁴⁴ **ISACA** (2019), *Credentialing: CSX-P*, <https://www.isaca.org/credentialing/csx-p> (last retrieved 25/06/2019).

Cyber-security and Cyber-preparedness as a Necessary Part of the Auditing Process upon Conformity assessment — General requirements for bodies operating certification of persons, a standard that provides principles and specified requirements regarding any body or institution, that certifies individuals, and includes provisions upon the proper creation and maintenance of a certification scheme for persons.²⁴⁵ It signifies at least five years knowledge and expertise in the following domains: (a) information security governance, (b) information risk management, (c) information security program development and management, and (d) information security incident management.²⁴⁶

IV] 3. Planning a Cybersecurity Auditing Program

The first step of every auditing process, including the cybersecurity one, is the planning step. This step is of the utmost importance because is the fundamental particle of every reliable, effective, and recognized auditing process. Mistakes and faults in this step mean bad quality and wrongful occurrence of the next step, the execution one, resulting working hours and important auditing resources to go wasted due to bad initial design. Moreover, *ISA 300 on Planning an Audit of Financial Statements, together with ISA 315 on Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement, ISA 320 on Materiality in Planning and Performing an Audit, ISA 330 on The Auditor's Responses to Assessed Risks*, provide detailed guidance about the scope, the process and the activities that must be incorporated in the planning phase.

International theory (like the one that above-mentioned standards provide) and practice of auditing in the cyber-security concerns, accepts a minimum of three basic steps/particles in the planning process:

1. Understanding the areas and the subjects of concern related to cybersecurity and setting of the scope of the Audit Programme,
2. Assessing Cybersecurity Risks and
3. Developing a detailed cybersecurity audit program based on the overall audit strategy.

Each step is consisted of sub-steps or sub-actions. Our approach in this master thesis follows this model of three major steps with sub-steps. Different recognized institutions

²⁴⁵ ISO (2018), *ISO/IEC 17024:2012 upon Conformity assessment — General requirements for bodies operating certification of persons*, <https://www.iso.org/standard/52993.html> (last retrieved 25/06/2019).

²⁴⁶ ISACA (2019), *Credentialing: CISM*, <https://www.isaca.org/credentialing/cism> (last retrieved 25/06/2019).

upon cyber-security matters had developed models of suggestion about planning audit programs with more steps, which usually is the expansion of one or more of the above-motivated steps into separated independent steps, according to what areas of cyber-security are about to be audit. A paradigm of that type is ISACA's Five-Steps to Planning for an Effective Information Systems (IS) Audit Program, that we examined previously in page 185. In this master Thesis we will follow the standard process of the three major steps accompanied by sub-steps, that actually includes the scope and steps of ISACA's proposed model.

IV] 3.1. Understanding the areas and the subjects of concern related to cybersecurity and setting of the scope of the Audit Programme

This first step of planning a cybersecurity audit plan is based in the solid configuration by the auditors (internal and external) of all the cyber-security and cyber-preparedness risks, vulnerabilities and demands (as we mentioned them in Chapter III) an entity faces, which is after all the heart of **ISA 315 on Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement**. Based on this procedure of configuration, the auditor(s) will create an initial general cybersecurity audit plan, which includes the audit actions, that are necessary, the time frame of the audit, the financial items and elements that must be inspected, and the impact of this audit performance. In order an auditor (or an auditing team) to best succeed in this task must first have a clear and holistic view about the object of its audit task and the relevant practices and procedures connected with this assignment.

IV] 3.2. Assessing Cybersecurity Risks²⁴⁷

Auditors must have a reliant knowledge about the whole spectrum of cybersecurity risks and the mechanisms, that the entity had imposed in order to track and neutralize these dangers, something that is in compliance with the requirements of **ISA 330 on The**

²⁴⁷ The creation of this sub-part of Chapter IV is based on information from: **Dr. Curtis Patchin and Mark Carey** (October 2012), *Risk Assessment in Practice*, Committee of Sponsoring Organizations of the Treadway Commission (COSO) and Deloitte & Touche LLP, <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dttl-grc-riskassessmentinpractice.pdf> (last retrieved 25/06/2019).

Auditor's Responses to Assessed Risks. This part of audit test planning is consisted of the following particles/steps:

I] Identification of Cybersecurity Threats: this step includes a deep knowledge about (i) the business model of the entity, (ii) the style of management of its directors team concerning risk taking mentality (risk lovers, or risk averters, etc.)²⁴⁸, (iii) the systems of protection of cybersecurity related data, (iv) the compliance and regulations (both internal, like internal policies, strategies, codes of ethics, code of governance, etc., and external, like national or/and international legal obligations, obligations from certification, etc.) requirements must be fulfilled by the entity²⁴⁹, (v) the general IT and NHS infrastructure architecture of the entity, (vi) the model and structure of its internal controls system(s), (vii) what are the lines of defense in case of an emergency, an internal fraud and an external attack, (viii) the business continuity plan of the entity, (ix) the deployment of third-party outsourcers and the risks by this deployment, (x) the key findings and most important concerns of previous years auditing reports, (xi) any other significant and with material impact change, etc.

II] Identification of the Impact of Cybersecurity Threats: there are five levels of impact in a typical cybersecurity impact identification analysis, where all the cybersecurity threats are categorized in one of the five levels according to the severity of any threat to effected people, to compromised NHS systems, to normal operations and to entity's environments (business and physical): 1) the *Negligible Impact Level*, with extremely low or unworthy to be taken under consideration impact concerns, 2) the *Minor Impact Level*, that usually signifies the first real level of consideration, 3) the *Moderate Impact Level*, which indicates threats that can be considered of having a reasonable effect to business functions. 4) the *Serious Impact Level*, for severe but still able to be handled effectively cybersecurity threats, and 5) the *Major Impact Level*, for extremely severe type of cybersecurity threats that can halt business continuity, and hurt existence and survival capacities of an entity. Is in the auditor(s) knowledge, analytical capacity, and experience to decide the level of impact of any occurred cybersecurity risk. A useful tool during this step can be the impact assessment that entities usually made for their interests. In Table No 7 we present the five levels of

²⁴⁸ That can lead to specific communication with the business management and assurance of its business model and risks strategies, according to *ISA 260 on Communication with Those Charged with Governance*, *ISA 265 on Communicating Deficiencies in Internal Control to Those Charged with Governance and Management*.

²⁴⁹ In accordance with *ISA 250 on Consideration of Laws and Regulations in an Audit of Financial Statements*.

impact as it concerns cybersecurity threats, accompanied with some useful examples from cybersecurity domain.

<i>Table No7: The five levels of impact analysis of cybersecurity threats</i>			
Impact Level	Impact on	Definition of Impact	Examples
1 Negligible	People	Negligible injury and effect	-Small injury (a minor cut or a wound) from using a device
	NHS systems	Negligible damage	-Destruction of a non- pivot cable -Loss of NHS manuals
	Operations	Negligible interruption	-extremely minor operation problems
	Environment	Negligible Impact	-Employees complaints or fatigue about technology use that goes unnoticed by management
2 Minor	People	Minor injury and effect	- Small number of personnel unfamiliar with used technologies -Severe trauma
	NHS systems	Minor damage	-Change place of a set of cables without inform
	Operations	Minor delays and interruption	-Unsuccessful espionage attempt
	Environment	Minor Impact	-Problems with NHS cooling system
3 Moderate	People	Major injury/health effect	-A moderate burning from NHS malfunction -Inexperienced and unfamiliar personnel with technologies used.
	NHS systems	Local Damage	- Temporarily Halt in NHS systems, due to electricity shortage
	Operations	Performance Reduction	-Small scale data breach - Successful but minor and controllable espionage attack -Bad choices from management about updating technologies, software licensees and accreditations
	Environment	Moderate but Controllable impact	-Bad publicity from a disclosure incident
4 Serious	People	Single Fatality or permanent disability	-Lost of an employee due to fire on NHS systems
	NHS systems	Serious and major damage	-Ransomware attacks -Small-scale DDoS attack -Severe Cyber-hacking attack to online servers, data centers and NHS

	Operations	Disruption of key operations	-Large-scale data breach -Permanent loss of IP due to attack or court decision -Bankruptcy or major incapacity to function properly of material third-party providers (data centers, supply chain participants, emerging technology providers, etc.)
	Environment	Major to mid-term damage	-Serious disruption in Blockchain, IoT, Cloud and Saas systems due to malicious attacks
5 Major	People	Multiple Fatalities or permanent total disability	-Multiple employees fatalities due to fire on NHS systems
	NHS systems	Extensive, uncontrollable and permanent damage	-Permanent and Long-term hult of NHS systems
	Operations	Major Disruption and destruction of core activities	-Severe or permanent halt of operations due to large scale malicious attacks
	Environment	Massive, long-term and irreparable damage	Total destruction of headquarter or other major building and data centers. -Complete and permanent loss of creditability and reputation due to a malicious attack
<p>Source: Dr. Curtis Patchin and Mark Carey (October 2012), <i>Risk Assessment in Practice</i>, Committee of Sponsoring Organizations of the Treadway Commission (COSO) and Deloitte & Touche LLP, https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dttl-grc-riskassessmentinpractice.pdf (last retrieved 25/06/2019).</p>			

III] Identification of the Probability Level of the Impact of Cyber-security Threats: in this part of the planning process the auditors must define the probability of having a risk or of a risk taken place, based usually in historical data. As in the impact scaling, in probability scaling determination auditors also usually are categorizing probability into five levels: 1) the *Very Unlikely Level of Probability*, in order to signify that an event has little or no chance at all to occur, 2) the *Unlikely Level of Probability*, that signifies a very limited probability of an event to take place at some time, but is still considered as mostly improbable to happen, 3) the *Possible Level of Probability*, for an event that is possible to occur at a point of time, 4) the *Likely Level of Probability*, that signifies that an event will probably take place, and 5) the *Probable Level of Probability*, that signifies that an event is expected to happen and is the level that shows the biggest certainty about an event to take place, as well as being at the same time the worst case scenario in a cyber-security threat: for

example in case of a hackers attack and penetration to NHS systems of a company, the auditors must expect that there will be a data breach and exposure, since this is the main reason why the hacking attack took place and because this is what the incidents from real world had showed. Again, as in the impact assessment process, the determination of how probable or not an event can occur is based on auditor(s) knowledge, analytical capacity and experience according of course to cyber-security and cyber-preparedness capacities of the client entity.

IV] Final Risk Assessment Conclusions Based on Risk Matrix: after having completed all the previous mentioned steps, auditor or auditing teams, internal and external, they must calculate the overall risk for every cyber-security threat. This estimation is calculated by the multiplication of the level of impact with the level of probability, in order to categorize any cyber-security event (threat) according to its impact and probability in what is called as the risk matrix, a practical tool that presents with biggest clarity the connection between the impact of a cyber-security event and its potentiality to occur, as the Table No 8 below indicates, and assist auditors in their decision of how they will develop their overall audit test program:

Table No 8: The Risk Rate Matrix for Cyber-security Threats							
(Probability × Impact = Overall Risk)							
		IMPACT					
		1. Negligible	2. Minor	3. Moderate	4. Serious	5. Major	
P R O B A B I L I	1. Very Unlikely	1	2	3	4	5	1-6 Low = minor event of little concern, impact and disruption
	2. Unlikely	2	4	6	8	10	7-14 Medium = important but not catastrophic event, that demands attention
	3. Possible	3	6	9	12	15	15-25 = material important event, demands (a) immediate attention and
	4. Likely	4	8	12	16	20	

T Y	5.	5	10	15	20	25	High	(b) introduction of a risk reduction control
	Probable							

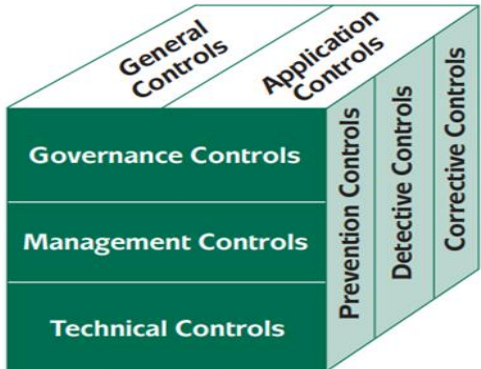
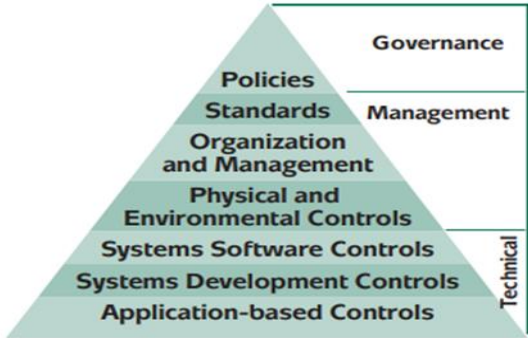
Source: Dr. Curtis Patchin and Mark Carey (October 2012), *Risk Assessment in Practice*, Committee of Sponsoring Organizations of the Treadway Commission (COSO) and Deloitte & Touche LLP, <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dttl-grc-riskassessmentinpractice.pdf> (last retrieved 25/06/2019).

IV] 3.3. Developing a detailed cybersecurity audit program

Developing an effective cybersecurity audit program, in order the execution phase not to present any defaults and mistakes, must be based in the provisions of *ISA 320 on Materiality in Planning and Performing an Audit*, *ISA 330 on The Auditor's Responses to Assessed Risks*, *ISA 402 on Audit Considerations Relating to an Entity Using a Service Organization*, *ISA 450 on Evaluation of Misstatements Identified during the Audit*, *ISA 500 on Audit Evidence*, *ISA 501 on Audit Evidence-Specific Considerations for Selected Items*, *ISA 505 on External Confirmations*, *ISA 510 on Initial Audit Engagements-Opening Balances*, *ISA 520 on Analytical Procedures*, *ISA 530 on Audit Sampling*, *ISA 540 on Auditing Accounting Estimates, Including Fair Value Accounting Estimates, and Related Disclosures*, *ISA 550 on Related Parties*, *ISA 560 on Subsequent Events*, *ISA 570 on Going Concern*, *ISA 580 on Written Representations*, *ISA 600 on Special Considerations-Audits of Group Financial Statements (Including the Work of Component Auditors)*, *ISA 610 on Using the Work of Internal Auditors*, *ISA 620 on Using the Work of an Auditor's Expert* and the findings of the previous steps. In this step the auditor(s) mostly must decide about the methods and tools that must be implemented for cybersecurity controls testing and verification and the effectiveness and accuracy of these methods and tools. This step is consisted of two sub-steps: (i) the first one is to determine what kind of cybersecurity controls must be implemented in the NHS systems and all other systems related to cybersecurity concerns and (ii) the second one is to determine the cybersecurity auditing process, which will be performed in the execution phase.

1] Identification and Determination of Cybersecurity Controls: in this step the auditors must decide what kind of controls must be performed on NHS systems and generally in any system is related to cybersecurity concerns according to the structure and the characteristics

of the examined entity. The **Institute of Internal Auditors (IIA)** in the second edition (March 2012) of its ***Global Technology Audit Guide (GTAG) 1: Information Technology Risk and Controls***, provides detailed guidance and advisory of what the most appropriate system of cybersecurity related controls must be. Even though, IIA had developed this tool mostly for chief audit executives (CAEs), their teams keep (consisting the internal auditors), the Board of Directors and its Audit Committee, chief information officer (CIO) and the entity’s IT management team, the tool can be the basis also for external auditors to develop and perform their audit program. Using the basic classification, we made in section III] 5. Understanding the Cybersecurity Risks’ Internal Controls System, concerning the fundamental three categories of internal controls, according to their purpose into (i) preventive, (ii) detective, and (iii) corrective, GTAG, suggests that we should additionally classify controls in two other classifications, related almost exclusively with the cybersecurity and IT points of view, (a) according to their fitting in the overall structure of an entity’s internal control system, so to separate them: (i) in general IT controls and (ii) in application controls, and (b) according to the individuals roles and responsibilities, and separate them: (i) in governance controls, (ii) in management controls and (iii) in technical controls. Image No 9 presents the three types of classification integrated. Moreover, as it concerns the classification of IT/cybersecurity internal controls according to individuals’ roles and responsibilities, those must be hierarchically listed, so in the level of *Governance*, which is the highest in the whole hierarchical pyramid, we have the policies controls, in the next level, the level of *Management*, we have standards controls, organizational and managerial controls and physical and environmental controls and as it concerns the *Technical* level, we have the systems software controls, systems development controls and application based controls, as Image No 10 indicates.

<p><i>Image No 8: The three Basic Categories of IT/cybersecurity Internal Controls</i></p>	<p><i>Image No 9: The Hierarchy of IT/cybersecurity Internal Controls</i></p>
	

Source: Institute of Internal Auditors (March 2012-Second Edition), *Global Technology Audit Guide (GTAG) 1: Information Technology Risk and Controls*, https://chapters.theiia.org/montreal/ChapterDocuments/GTAG%201%20-%20Information%20technology%20controls_2nd%20ed.pdf (last retrieved 25/06/2019).

But what are exactly each type of these IT and cybersecurity related controls and how they can enhance the internal and external auditors' duties? In the following paragraphs we will attempt to present the basic concepts upon each type of these IT controls, with the exemption of primary classification, meaning (i) preventive, (ii) detective, and (iii) corrective, since we already did this in section III] 5. Understanding the Cybersecurity Risks' Internal Controls System.

➤ **General IT Controls**: this variety of controls is applicable to the entire structure of an entity in an attempt to assure the adequacy of its structure and its systems to cybersecurity risks and malicious penetration attacks. In this category of controls are included: IT governance, risk management, resource management, IT operations, application development and maintenance, user management, logical security, physical security, change management, backup and recovery, and business continuity. While a part of them are business-related, such as those concerning segregation of duties or governance arrangements, others are very technical and infrastructure related, such as system software controls and network software controls. Since they functions as the basis of the IT control landscape of an entity, internal auditors (but also external auditors too), must give priority attention to them, since any weakness or inconsistency in them signifies that the auditors must either conduct further tests, either alternate his/hers test upon them. We must give special attention to the following types of general IT controls:

- **General Management Controls**: these controls are destined to estimate the productivity, effectiveness, and operability of the management of the entity and consequently of the entity itself. The areas of their focus are: (a) the quality of the structure and the effectiveness of the general long-term business plans of the management and their relation with cybersecurity concerns and risks, (b) the development of future plans and strategies about the creation of applications that will assist and improve the existed NHS systems, (c) the preparation and creation of short-term business cybersecurity related plans for the most appropriate assessment and acquisition of data, especially for those amounts of data that involve a lot and different teams, external providers and vendors cooperation and of which the coordination is a quite challenging but important task, (d) the estimation and

Cyber-security and Cyber-preparedness as a Necessary Part of the Auditing Process

evaluation of the efficacy and functionality of the above-mentioned cybersecurity related plans in periodical basis, and (e) the evaluation of the after development and use of the designed cyber-security applications and NHS systems and to what extent they achieve the set by management cybersecurity objectives.

- **Physical Access Controls:** physical access is referring to the right of only certain and authorized by management individual(s) to have access to material hardware and software capacities of an entity, with the aim to minimize the cybersecurity vulnerabilities of NHS systems and to achieve an adequate level of protection to the material parts of the NHS systems. These controls are focusing on the examination of: (a) the complete protection of material capacities, components and manuals of the NHS systems, (b) the assurance that standards and contracts of material protection are being respected according to the constructors or/and sellers indications/guidelines, (c) the updating and upgrading of material capacities according to constructors or/and sellers indications/guidelines, (d) the adoption of a security guarantee framework that will contain: the adoption of an entrance system with specific measures that will allow physical access only to authorized individuals with approved passwords, identity cards and personalized keys, the installation of security cameras and alarms in the buildings, even the installation of biometric security systems in order to prevent physical access to unauthorized and malicious behaving individuals, (e) the hiring of the right personnel or external contractor(s) that will manage in the most appropriate way the material integrity and physical protection of the hardware devices and systems.
- **Logical Access Controls:** logical access is about the right to have access and assess the software, data and network capacities of an entity but not to the hardware mechanisms that function as the storing home of these capacities, since this is the case of physical access controls. Securing data and software applications from any cybersecurity risk and vulnerability demands that logical access controls will test (a) the system of authorized and unauthorized users to software and data and how effectively limits the access to all unauthorized and malicious behaving individuals, (b) the system of personalized passwords and access codes/keys. Questions like: Does the entity use the same password(s) for multiple devices, accounts, communication networks? What is the level of passwords complexity? Does the entity applies a policy of simple and easy guessing passwords (for example passwords like the full name or nick name or the social security number of an employee, or just a number sequence like 12345...) which raise the level of cyber-

insecurity or applies a strong password and verification policy? The entity applies a periodically changing passwords policy, for example at least every six months, and always every time there is a suspicion of a cyber-attack and after an actual cyber-attack, (c) the integrity and security of network systems, like the Local Access Networks (LANs) and the worldwide connected networks like internet. The protection of these networks with the most suitable and appropriate anti-virus and firewall options is of the outmost importance, (d) like in the case of physical access the application and the installation of security cameras and alarms in the buildings, even the use of a biometric access system is quite important during auditing controls, and (e) the hiring of the right personnel or external contractor(s) that will manage the integrity and logical protection of the software, data applications and network devices and systems.

- **Application Controls:** are related with specific activities performed by NHS systems. For example, the controls performed on emerging technologies as we described them in Chapter III, are among the most characteristic example of application controls. These controls incorporate sub-controls of entrance (input control), of processing (process control) and of reporting (output control) according to the level of relevant data assessment data edits, segregation of business functions, balancing of processing totals, transaction logging, and error reporting. In the sub-control of entrance auditors must examine proper keeping/recording of coming and exiting invoices and their documentation, the accuracy of the invoices and documentation, the potentiality of not proper receiving and cataloging of the invoices and documentation, the potential existence of a daily record of defaults, mistakes and unprocessed items, etc. In a process sub-control, auditors must examine the accuracy, integrity and truthfulness of the data involved. A typical example of such type of sub-control is the verification control about the details and the balance of an application account. For example of an account related to blockchain technology and which had an abnormal performance, this can be an indication of a hacking or crypto-asset mining attack. In an output sub-control, auditors must reassure that the principle of proper presentation of information and the principle of disclosure only to the authorized stakeholders is fulfilled.
- **Governance Controls:** aim to oversee the role of the Board of Directors and its ability to safeguard a sufficient IT governance capacity. It is related with effective information management, with IT principles, IT policies, and IT processes and with ensuring of their proper establishment, conduction and performance, according to both organizational

goals and strategies, but also with outside the entity rules setting bodies, such as regulators and legal authorities. So, the main subcategory of governance controls is:

- **Policies Controls:** the establishing of goals and objectives through strategic plans and policy statements and procedures creation, is one of the basic governmental and top managerial tasks. Without clearly approved by management, recommended by the Board, and communicated to staff IT policies, entities risk to fell victims of disorientation and low quality and ineffective performing. Customization of the policy statements according to the entity's size, needs and IT deployment is necessary. For smaller organizations, a single but adequate policy statement can be sufficient, but for larger organizations better articulated, more detailed and specified policies must be the case. A proper IT policy statement must include: (a) a general entity-wide policy regarding the level of security and privacy protection according to relevant national and international legislation, including specifications upon the level of control and security according to applied systems and processed data sensitivity, (b) a statement regarding the data classification, access rights and limitations to access authorizations, (c) a clear definition of the notions of data, systems ownership, authority able to originate, modify, or delete information and users ability to produce their own applications, (d) personnel policies, regarding definitions and enforcement of conditions related to sensitive areas of concerns for staff in sensitive areas, the signing by staff of hiring agreements concerning their responsibilities and duties and to keep an adequate level of control, security, and confidentiality, as well as detailed disciplinary procedures, and (e) clarifications upon an entity's overall business continuity planning and disaster recovering provisions.
- **Management Controls:** concerning the responsibility of management to inspect all areas and sections of the organization, giving additional attention to issues like critical assets handling, sensitive information protection, and operational functions effectiveness, by ensuring the sufficient implementation and continuous application of proper IT controls, able not only to track and mitigate risks but also to protect the entity's processes, and assets. The are classified in three major categories:
 - **Controls on Standards:** concerns internal controls about written and approved by management standards, that must be available to all the individuals that implement them. These standards describe the manners to achieve the entity's objectives, by promoting the efficiency consistency of IT functions with overall operating capacities. Their proper development and application are related to an entity's size and resource capacities, since larger organizations tend to apply relatively more

Cyber-security and Cyber-preparedness as a Necessary Part of the Auditing Process

resources and create their own standards, but smaller organizations may not be able to apply the needed resources. The following aspects must be taken under account by an entity and more precisely by its IT management, when they create and/or apply IT standards: (a) systems development processes, (b) systems software configuration, (c) IT environment, (d) application controls, (e) data structures, and (f) proper standards documentation.

- *Organizational and managerial controls*: a sufficient and effective organization and management structure permits better reporting and responsibilities' allocation. This type of controls is consisted of the following sub-categories: (a) *segregation of duties controls*: which ensures that all aspects of data collection and assessing are not conducted from only one person, and also the duties of data initiating, authorizing, entering, assessing, and examining are properly segregated to experienced, skillful and authorized employees, securing like that IT systems from errors, irregularities and malicious behaviors, (b) *financial controls*: budgetary and other related to financial resources controls must be applied in order to safeguard that the applied technologies can generate back to the company the investment costs payed for their deployment. Despite the fact that new IT deployments are quiet costly, without always deliver back to the entity the expected cost savings, managers must apply, assess and report controls concerning the financial aspect of IT, and (c) *change management controls*: aims to ensure that the IT landscapes, NHS and application systems, and data are applied in the proper way, that not only promotes duties segregation, but also protects the changed IT from being exploited due to malicious and fraudulent reasons, which can result a negative impact or even operational halting to an entity's system and service effectiveness and availability.
- *Physical and environmental controls*: due to IT systems relative high cost, their constant protection from accidental or deliberate damage, malfunction and loss must be properly guaranteed. Physical and environmental controls, are applicable to (a) large data centers, irrelevantly if they are established inside an entity or belong to a third-party provider, (b) web-based systems, such as data clouds, (c) servers, and (d) workstations. These controls must ensure: (i) proper and restricted access only to authorized people, (ii) proper application of fire detection and suppression equipment and proper implementation of fire escaping procedures by individuals, (iii) proper storage, accommodation and back-up of sensitive and crucial equipment, applications, and data away from physical and environmental dangers and threats,

such as floods, flammable liquids, natural disasters, etc., (iv) proper application of the entity's emergency plan and the after emergency business continuity plan.

➤ **Technical controls:** their importance is quite high since any weakness on technical controls is synonymous to negative operation to the overall internal control systems. As it concerns the aspect of protection against unauthorized access and interference, technical controls functions as the reasonable foundation that serves the principles of data integrity, data authenticity, business resilience, and IT infrastructures effectiveness. They mostly concern operating system controls, database controls, proper encryption, sufficient logging, and are categorized in the following types:

- **Systems software controls:** in general terms systems software products, such as operating systems (like Windows, Linux and UNIX), network and communications software, firewalls, antivirus products, and database management systems (or DBMS), provide to the application systems and users the ability to properly use IT equipment. IT audit experts must in regular base inspect and evaluate technical controls concerning systems software's, despite the fact that only large organizations can deploy such professional, while small organizations might not be able to bare the related cost. In this case, but also for all sizes entities, IT auditors might not belong to an entity's staff, but also can be deployed through a third-party vendor, usually due to the better expertise, that outsourced service providers have. The high complexity and the high level of sophistication of systems software demands high level of expertise and specialization, so the application of proper configuration techniques, such as logical access controls to authorized users only, segregation of duties controls, implementation of relevant specialized audit trails, promotion of data integrity controls through access control lists, filters, activity logs, and access recording systems is of the outmost importance. The well-being and effective management of IT systems software integrity can be ensured by the following controls: (a) proper allocation and control of the access rights according to the entity's related policies, (b) sufficient segregation of duties and responsibilities with the implementation of proper systems software and other configuration controls, (c) suitable implementation, evaluation, examination monitoring and reporting of the proper controls concerning cyber-attacks, penetrations and vulnerabilities prevention, and detection policies, (d) penetration testing must be conducted regularly, (e) encryption techniques must be in use, in order to ensure confidentiality and data integrity, (f) change management processes, such as patch management to NHS and data, must be constantly present, active and evaluated.

- *Systems development controls*: since there is a number of methodologies for all NHS systems purchase, establishment or creation, IT auditor should evaluate the adequacy of the method or methods used to obtain or create all the systems, applications and data an entity has, or acquires, and process. Important controls in this domain concerns: (a) proper documentation and measurement of user requirements, which must be designed through , processes within the system, (b) assurance of the proper structured and approved way for systems development processes, (c) individual system elements and system interfaces must be measured and function as expected, with relevant confirmation by the system owner, (d) application maintenance and change management processes must be implemented properly and in regular basis, (e) as it concerns the case of outsourced systems development the external vendor, outsourcer or provider, must ensure the application of similar controls, such as high quality project management controls, business continuity management controls, and development process controls, (f) time-sufficient and proper budgetary evaluation controls must be also in use, and (g) proper reporting controls, which ensures that executives have a sufficient knowledge of the current level and status of systems development must be also present.
- *Application-based controls*: as we stated previously the application controls are related with the way data (a) is inserted accurately, and with proper level of completeness, authorization and correctness (input controls), (b) is processed as expected (processing controls), (c) the proper storage and back-up of data (storage controls), (d) proper use and handling of the output data (output controls), (e) proper monitoring and examination upon data in process and/or storage, in order to safeguard the consistency and integrity of data (integrity controls), and (f) ability to track and record transactions and events from the source to the eventual end and backwards in order to identify defaults, anomalies and errors as close as possible to their sources and solve them as soon as possible (management trail controls).²⁵⁰

III Creation of the Most Suitable Cybersecurity Controls Audit Program: the creation of the best fitting auditing program for cyber-security concerns demands from auditor(s), internal and external, great experience and competences, since is the basis of the execution

²⁵⁰ Νεγκάκης Χρήστος Ι. Και Ταχυνάκης Παναγιώτης Δ. (2017), *Ελεγκτική- Εσωτερικός Έλεγχος: Θεωρία και Εφαρμογές (Auditing – Internal Auditing: Theory and Applications)*, Εκδόσεις Αειφόρος Λογιστική Μονοπρόσωπη ΙΚΕ, Θεσσαλονίκη, Σελ. 631-634. **Institute of Internal Auditors** (March 2012-Second Edition), *Global Technology Audit Guide (GTAG) 1: Information Technology Risk and Controls*, https://chapters.theiia.org/montreal/ChapterDocuments/GTAG%201%20-%20Information%20technology%20controls_2nd%20ed.pdf (last retrieved 25/06/2019).

step/phase. In the modern computerized auditing environments, the development of the necessary audit testing software is the everyday reality. Auditors use their own *Generalized Audit Software (GAS)* or/and *Computer Assisted Audit Techniques (GAATs)* that assist in the atomization of controls tests and promoted higher quality and objectivity of results.²⁵¹ Despite the fact that, those software applications had their own cybersecurity vulnerabilities, such as hacking attacks, internal structure problems, malicious attempts of destruction and penetration, a common ground of cybersecurity concern that auditors share with the client entities and should both mitigate, GAS and GAATS had gained more and more ground in auditors workload. In order to maximize the effectiveness, quality, applicability and correctness of the auditing software and at the same time minimize the potential vulnerabilities auditors use more computer based systematic approaches, like the *Software Development Life Cycle (SDLC)* about how to plan, construct, maintain and improve auditing software and how to achieve customers' expectations and demands, due to their internal quality characteristics. Suitable SDLC in GAS and GAATs can (a) ensure that implemented cybersecurity controls provide higher capacities of efficacy and mitigation of cybersecurity risks, (b) analyze different cybersecurity control testing situations and scenarios, in order to provide the most appropriate testing indications, explanations and recommendations for the NHS systems of examined entity case, (c) spot and frame the needed cybersecurity changes that must be implemented, their risks, cost and difficulties in implementation and (d) provide a mechanism for quality auditing planning, estimating, tracking, improving auditing speed, visibility and auditing failures track success and minimizes the use or abuse of auditing resources and capacities, (e) provide high quality and entity-customized deliverables, that will be used in the execution phase, (f) offer important explanation and guidance for post-implementation review and evaluation and (f) improve auditors relationships with the examined client entity, irrelevantly if it is an internal audit program or an external audit contract. A successful audit testing SDLC is usually characterized but the following phases:

➤ *Phase 1 – Planning and Feasibility Analysis Phase:* is the process to determine and document the software needs and specific requirements in order to design and develop the most appropriate software application. The approach used is more of a PESTEL-DG analysis²⁵² methodology but more customized to an entity's needs and dimensions, so

²⁵¹ Κωνσταντίνος Καραμάνης (2008), Ibid, Page 480.

²⁵² The **PESTEL-DG** acronym is derailing from Political, Economic, Social, Technical, Environmental, Legal, Demographic and Geographic feasibility aspects of any designed plan and project, including software creation applications projects. Is a very useful analytical tool, that identifies and shapes the so called as macro (or external) influences and implications, that may impact an entity operability and functionality. As the macro-

usually we have the following sub-feasibility evaluations: (a) the *economic feasibility*, that examines the budgetary and resources demands of the audit, (b) the *legal feasibility*, that examines the regulatory compliance requirements, (c) the *operational feasibility*, that examines the usefulness of the audit results to the client normal operations, (d) the *technical feasibility*, that examines the adequacy of technical –software, hardware, network, computational- capacities of the client entity and (e) the *time-framing feasibility*, that examines the scheduling and programming requirements of the audit program within a specific execution time frame.

- *Phase 2 – Design and Build Phase:* based on feasibility study and its components auditors identify and specify all the necessary requirements and demands, and design analogously their audit program in order to best articulate matters like: the description of tasks, criteria of performing specific tests and controls, operational capacities needed, how to interact with client entity, audit quality assurance identification, identification of audit risks and any other not anticipated risk during conducting an audit, provide guidelines and details about the whole process documentation, and generally any other relevant requirement for completing an effective audit program.
- *Phase 3 –Implementation and Testing Phase:* this phase is the practical expression of the execution phase that we will examine in the next section of this chapter. In general terms, this phase is about the examination of applicability and usefulness of customized audit tests according to the scale and needs of the entity, since exhausting auditing testing frameworks are resourcefully impossible.
- *Phase 4 – Reporting, Maintenance and Post Implementation Phase:* this phase is the practical expression of creation and issuance of final auditing reporting, and we will examine in the next chapter.²⁵³

IV] 4. Executing a Cybersecurity Auditing Program

After having acquired the necessary knowledge and understanding about the client entity's operating environment and the accompanied risk concerning cybersecurity, and after

implications in this particular case we can put all the cybersecurity risks and vulnerabilities that an entity face and auditor(s) must inspect during the cyber-security auditing programs.

²⁵³ ACCA Global (09/01/2019), *Agile audit of agile projects*, <https://www.accaglobal.com/gb/en/member/discover/cpd-articles/audit-assurance/agile-audit-of-agile-projects.html> (last retrieved 25/06/2019). Pearson Prentice Hall (2010), *The System Development Life Cycle (SDLC)*, https://wps.prenhall.com/bp_cis_careersinit_1/13/3452/883935.cw/index.html (last retrieved 25/06/2019).

having planned the most effective cybersecurity audit trail on the client entity's NHS and financial statements, according to *ISA 315 on Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*, *ISA 250 on Consideration of Laws and Regulations in an Audit of Financial Statements*, *ISA 300 on Planning an Audit of Financial Statements*, *ISA 320 on Materiality in Planning and Performing an Audit* and *ISA 330 on Auditor's Responses to Assessed Risks*, *ISA 402 on Audit Considerations Relating to an Entity Using a Service Organization*, auditors (we are now referring to external independent auditors mostly, but also internal auditor can be helped during their job by the indications we are about to present, as long as they adapt them to their role, responsibilities and duties necessities and requirements), must proceed to the execution phase of the planned audit program, that is mainly governed by *ISA 500 on Audit Evidence*, *ISA 501 on Audit Evidence-Specific Considerations for Selected Items*²⁵⁴, *ISA 505 on External Confirmations*, *ISA 520 on Analytical Procedures*, *ISA 530 on Audit Sampling*, *ISA 560 on Subsequent Events*, and *ISA 580 on Written Representations* and *ISA 620 on Using the Work of an Auditor's Expert*.

More precisely, *ISA 500 on Audit Evidence*²⁵⁵ and *ISA 501 on Audit Evidence-Specific Considerations for Selected Items*²⁵⁶, require from auditors to acquire sufficient and appropriate audit evidence upon the client entity's risk assessment and quality control procedures, accounting records and internal control systems, that is necessary to assist the auditor to properly and adequately form his/hers opinion and his/hers final audit report. The proposed by these ISA audit procedures to obtain the best qualitative and quantitative audit evidence are inspection, observation, (external) confirmation, recalculation, reperformance, and analytical procedures, and inquiry. After having a solid and workable audit evidence, which includes both internally produced by the client entity information, according to *ISA 500 on Audit Evidence*, *ISA 501 on Audit Evidence-Specific Considerations for Selected Items*, *ISA 520 on Analytical Procedures*, *ISA 560 on Subsequent Events*, *ISA 580 on Written Representations*, and *ISA 620 on Using the Work of an Auditor's Expert* and externally produced evidence, according to *ISA 505 on External Confirmations*, auditors must proceed to perform tests, that aim to spot any default in the financial statements results and accounts. Auditors must choose (a) either to test a whole population, such as payments, if that is

²⁵⁴ Those selected items are (a) inventory (b) litigation and claims, and (c) segment Information.

²⁵⁵ **IFAC** (2010), *International Standard on Auditing (ISA) 500 on Audit Evidence*, <https://www.ifac.org/system/files/downloads/a022-2010-iaasb-handbook-isa-500.pdf> (last retrieved 25/06/2019).

²⁵⁶ **IFAC** (2010), *International Standard on Auditing (ISA) 501 on Audit Evidence—Specific Considerations for Selected Items*, <https://www.ifac.org/system/files/downloads/a023-2010-iaasb-handbook-isa-501.pdf> (last retrieved 25/06/2019).

possible, for confirming certain characteristic, like authorization, in order the results of his/her tests to produce reliable results about the population proper functioning, (b) either to test selected items and perform one of the following three approaches: (i) selecting all items, meaning to perform a 100% examination, which is an extremely difficult task to be performed sufficiently but offers the best inspection rate, (ii) Selecting specific items, usually the most crucial and fundamental, or the items that in general terms produce the most cybersecurity audit issues, and (ii) conducting audit sampling, according to ***ISA 530 on Audit Sampling***.

IV] 4. 1. Performing Audit Tests in Internal Controls Systems

The major step of the execution phase is the designing, performing and evaluating of the proper tests in internal controls systems of the client entity's in actual real conditions, in order the auditors to achieve to their duties of (a) collecting sufficient and efficient evidence, (b) performing proper fieldwork and (c) developing the results documentation, that will help them enter in the final phase, the shaping and issuing of final audit report.

So, if from the step of risk assessment there is clear evidence that the entity does not have any reliable system of internal controls or its system is very weak, or of poor quality and poorly effective, then in this phase the auditor(s) must include in their audit program two types of testing: (a) the ***compliance testing***, which focus on determine whether a company must follow specific legal obligations and the level of this compliance performance by employees and management, and (b) the ***substantive testing***, which examines the financial records of the entity in order to identify errors, inaccuracies and defaults and includes the communication of auditors with the entity's banks/financial institutions, customers, suppliers, lenders, legal councilors, stock authorities, other stakeholders in order to confirm entity's data with theirs according to *ISA 505 on External Confirmations*.²⁵⁷ The cybersecurity-related controls testing phase can be characterized as the heart of the whole auditing program and performance, because the results of this phase is the basis of the final auditing report, as we stated previously. Both types of testing, compliance and substantive, aim to track and neutralize the most vital cybersecurity vulnerabilities and dangers, since as we stated previously exhausting testing frameworks are resourcefully impossible, unless the client entity is quite small and very easy inspectable.

²⁵⁷ **Bragg Steve** (29/05/2019), *Substantive testing*, Accounting Tools, <https://www.accountingtools.com/articles/what-is-substantive-testing.html> (last retrieved 25/06/2019).

For any other entity, the basic aim is to spot the most impactful dangers, those able to halt operations and hurt long-term existence.

This is a quite demanding task and can be performed with the use of proper audit sampling approach, according to *ISA 530 on Audit Sampling*.²⁵⁸ More precisely, part 5 of ISA 530 refers to “audit sampling” as “*the application of audit procedures to less than 100% of items within a population of audit relevance such that all sampling units have a chance of selection in order to provide the auditor with a reasonable basis on which to draw conclusions about the entire population*”, while as “population” we can identify an entity’s complete set of information, that will function as the basis of the sample deriving pathway and of which the auditor wants to have a better insight. As “sampling unit”, ISA 530 recognizes each individual objects/item, that formulate a population. As “statistical sampling” ISA 530 describes any methodology of sampling that is characterized by the following indicators: (a) the items for sampling are randomly selected, and (b) the evaluation of sample conclusions and sample risks measurement must be conducted with the use of probability theory and norms. As “sampling risk” the ISA 530 indicates the risk that is incorporated only after the assessment and conclusion of the sample population and may be distinct from the auditor’s assessment and conclusion upon the entire population. Sampling risk can end up into two kinds of erroneous conclusions: (a) in sampling tests upon controls, the possibility the controls to be more effective than what they really are, or as it concerns test of details, the material misstatement even though is present will not appear as such. This kind of erroneous conclusion demands from auditors special attention due to the fact that impacts the whole effectiveness of the audit procedure and might result to an incorrect audit opinion, and (b) in sampling tests upon controls, the possibility the controls to be less effective than what they really are or as it concerns test of details, the material misstatement even though is not present will appear as it actually exists. This kind of erroneous conclusion affects audit efficiency and usually demands from auditor additional work and effort in order to clear out the wrongness of primary conclusions. That is why, is of the utmost importance auditors to give special attention when they decide upon the sample design, size, the selected items for testing and the selection of the proper and most suitable sample assessment method and technique. ISA 530 provides the following possible sampling methods that auditors can select during the execution phase of their audit programs: (a) *random selection*, that is implemented by applying randomly picking up of

²⁵⁸ **IFAC** (2010), *International Standard on Auditing (ISA) 530 on Audit Sampling*, <https://www.ifac.org/system/files/downloads/a027-2010-iaasb-handbook-isa-530.pdf> (last retrieved 25/06/2019).

areas of the test population, for example randomly choose to inspect transactions that can be subject to cyber-malicious behaviors, like identity thefts, (b) *systematic selection*, that is achieved dividing the number of sampling units in the population according to the sample size in order to provide a sampling interval. For example, if the auditor chooses to inspect the first of every 100th related to cybersecurity transaction, then the first, the 101st, the 201st and so on will be selected to be tested. The selection of the chosen sampling interval is usually a random decision by the auditor, according to the computerized random number generator or random number tables of the software tools the auditor uses. While an auditor perform a systematic selection sampling, he/she must determine what is exactly the sampling units within the test population and must ensure that is not structured in such a way, so as not to lead to the correspondence of the sampling interval with a particular pattern in the population, (c) *monetary unit sampling or stratified sampling*, is a type of value-weighted selection, that divides a population into subpopulations, and each of subpopulations plays the role of a sampling unit, that share similar attributions and characteristics, usually counted in monetary values and amounts, (d) *haphazard selection*, a sampling method that uses no specific structured technique, but the auditor must evade from any conscious bias or predictability, such as avoiding difficult to trace items, or always selecting or circumventing from selection the first or last entries on a system, etc., as well as assure that all items within the population have at least an equal opportunity to be selected and tested. Haphazard selection cannot be used when statistical sampling is performed, (e) *block selection*, that is consisted of picking up a block(s) of connecting items within the population, a method that is usually not applicable to audit sampling, due to the fact that most populations are organized in such way that the populations' items are sequenced without having similar characteristics to each other, but are having different characteristics from items in a different place within the population, a situation able to compromise the validity of the complete sample population.

We must not neglect that the quality of audit evidence gathered from audit sample during audit tests must be according to ***ISA 500 on Audit Evidence*** without inconsistencies, or reliability doubts, even if they are obtained from different sources, with different ways and they are of a different nature, as long as the audit evidence is reliable and consistent with the audit evidence obtained from another source. For example, the cybersecurity related audit evidence must be consistent regardless if it came from sources like the management, or internal audit, or external partners, like banks and third-party service providers. In the next section of this Chapter, we will examine the most important paradigms of specialized

auditing test, according to the cybersecurity risks and vulnerabilities. Auditors should use these areas of concern in order to perform their audit test and to end up in important conclusions about the reliability, accuracy, and truthfulness of an entity's financial statements.

IV] 4. 2. Paradigms of Specialized Auditing Tests According to Specific Cybersecurity Risks and Vulnerabilities

In this section of the Master Thesis we would like to become more specialized as it concerns cybersecurity auditing tests by focusing in targeted areas of cybersecurity concern, as we described them in previous in section III] 3 in this Master Thesis. We will examine specific suggestions for effective and standards-complied type of auditing tests for the cybersecurity risks and vulnerabilities mentioned in Chapter III. The reader must always have in mind that these suggestions mentioned here are being collected by bibliography by the writer with the following international auditing standards in mind: *ISA 315 on Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement, ISA 250 on Consideration of Laws and Regulations in an Audit of Financial Statements, ISA 300 on Planning an Audit of Financial Statements, ISA 320 on Materiality in Planning and Performing an Audit, ISA 330 on Auditor's Responses to Assessed Risks, ISA 402 on Audit Considerations Relating to an Entity Using a Service Organization, ISA 500 on Audit Evidence, ISA 501 on Audit Evidence-Specific Considerations for Selected Items, ISA 505 on External Confirmations, ISA 520 on Analytical Procedures, ISA 530 on Audit Sampling, ISA 560 on Subsequent Events, and ISA 580 on Written Representations and ISA 620 on Using the Work of an Auditor's Expert.*

VI] 4. 2. 1 Malicious Code and Programs

During their audit trails, auditors must give special attention in the following situations: a) if the entity keeps updated and upgraded its firewall, anti-virus and other protective systems, b) if there are frequent unusually slow NHS systems performance, halts and crashes to an entity's NHS, or difficulties to restore capacities of the NHS systems, c) if the entity's email accounts are used to send mass emails inside and outside the entity with suspicious content or asking for irregular payments or with illegal content, etc., d)

unfamiliar programs that run at the same technology choice, when the NHS systems are turned on or during normal function and auditors can check through the active applications list of a computer, e) unusual change of passwords or the entity's homepage to be transferred in another website without an official notice from the management, or to be unable to restore the functionality of the entity's homepage, f) pop-up windows attached to official entity's homepage, g) risky use of social media (both entity's and personal) and external websites with open access downloads and attachments since they can carry viruses. Those are the most common signs that the NHS systems of the entity are suffering from malicious codes attacks. Moreover, during their audits they must ask for the reports produced after automatic and manual scans of the NHS systems, the reports created in case of a malicious code incident, the report or key findings after the implementation assessment of the above mentioned "anti-virus policy" and the information created in case the incident had been reported to authorities and law enforcement institutions.²⁵⁹ Last but not least, auditors must have a critical look on the report of any malicious data breach done to authorities and how those institutions had react and what kind of guidelines for further protection they had provide to the entity and how the entity implement them.²⁶⁰ This is a common practice for auditors for data breaches provoked not only from malicious code, but from all the vulnerabilities we are describing here.

VI] 4. 2. 2 Harmful Malwares

For both types of malicious software threats, it could be similar to the one we describe previously in the case of the malicious codes and programs, since both types of threats have common identification characteristics during audit trails. Moreover, internal and external auditors must show interest to explore and test the proper use of botnets inside the

²⁵⁹ **CISA**, 11/04/2019 (revised), Security Tip (ST18-004): Protecting Against Malicious Code, <https://www.us-cert.gov/ncas/tips/ST18-271> (last retrieved 25/06/2019). **CISA**, 04/11/2013, Security Tip (ST13-003) Handling Destructive Malware, <https://www.us-cert.gov/ncas/tips/ST13-003> (last retrieved 25/06/2019). **McDowell Midi** (for CISA), 11/10/2010, Security Tip (ST10-001) Recognizing Fake Antiviruses, <https://www.us-cert.gov/ncas/tips/ST10-001> (last retrieved 25/06/2019). **McDowell Midi** (for CISA), 19/03/2009, Security Tip (ST05-006) Recovering from Viruses, Worms, and Trojan Horses, <https://www.us-cert.gov/ncas/tips/ST05-006> (last retrieved 25/06/2019). **Durkota Michael D. and Dormann Will**, 2008, *Recovering from a Trojan Horse or Virus*, Carnegie Mellon University, <https://www.us-cert.gov/sites/default/files/publications/trojan-recovery.pdf> (last retrieved 25/06/2019). **CISA**, 08/09/2015, Securing Your Web Browser, <https://www.us-cert.gov/publications/securing-your-web-browser> (last retrieved 25/06/2019).

²⁶⁰ **Federal Trade Commission** (April 2019), *Data Breach Response: A Guide for Business*, <https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business> (last retrieved 25/06/2019).

normal function of a company and if any vulnerability on them can constitute them susceptible to external attacks and hijacking attempts.²⁶¹

VI] 4. 2. 3 Social Engineering and Phishing

Apart from checking the implementation of above-mentioned controls during their audit trails, auditors must also examine the amount of inside suspicious emails asking for internal data, information and credentials, that are characterized by a generic type of greeting or/and poor grammar and spelling quality, suspicious attachments, hyperlinks and websites. Moreover, they must take under serious consideration any relevant report of this type of incident both in inside administrators and also to outside important authorities, like police or related financial authorities (for example the Federal Trade Commission in United States of America).²⁶²

VI] 4. 2. 4 (Distributed) Denial of Service Attacks

IT department must report to internal auditors any large-scale technical problem especially in networks functionality, NHSs maintenance actions, cloud vulnerabilities, applications considerations and generally any indication of a (D)DoS attack. Any unexpected delay or insufficient performance on network and software systems must function as a red flag, a sigh of alert for both internal and external auditors. Network traffic inspections and monitoring, incidents of inaccessibility to certain websites or their unavailability to function proper must be tracked and reported by the IT department in cooperation with (internal or/and external) (D)DoS protection and clean up service to internal and external auditors, which must take them in serious consideration when they design their controls testing and reporting activities.²⁶³

²⁶¹ **McDowell Midi** (for CISA), 11/10/2010, *Security Tip (ST10-001) Recognizing Fake Antiviruses*, <https://www.us-cert.gov/ncas/tips/ST10-001> (last retrieved 25/06/2019). **McDowell Midi**, 24/09/2011, *Understanding Hidden Threats: Rootkits and Botnets*, <https://www.us-cert.gov/ncas/tips/ST06-001> (last retrieved 25/06/2019).

²⁶² **US Federal Trade Commission**, 2019, *Phishing*, <https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/phishing> (last retrieved 25/06/2019). **Luxembourg Bankers Association (ABBL)** (2019), *Phishing/Smishing/Vishing*, <https://www.abbl.lu/topic/phishing-smishing-vishing/> (last retrieved 25/06/2019).

²⁶³ **CISA**, 04/11/2009, *Security Tip (ST04-015): Understanding Denial-of-Service Attacks*, <https://www.us-cert.gov/ncas/tips/ST04-015> (last retrieved 25/06/2019).

VI] 4. 2. 5 Ransomware

Audit trails must give special significance to these incidents, because usually they are an identification of general poor cybersecurity capacity of an organization and must not hesitate to include their findings to their final report. Tests upon areas like: (a) is the exposed amount of data of sensitive kind?, (b) are the ransoms paid with the return of stolen data and what is the impact of the ransom in overall resources of the entity?, (c) are the stolen data also sold in darkmarkets?, (d) did the entity ask for the help of law enforcement authorities and what was the outcome of their intervention?, (e) is now the entity better prepared from analogous events? are some of key questions that auditors must investigate.²⁶⁴

VI] 4. 2. 6 CEO/CFO scams or Whaling and Identity Thefts

Auditors must be informed in case of these types of incidents took place in order to judge their severity and how they can have a significant impact in entities health and longevity. Auditors must also take under serious consideration the bank statements and relevant account activity in their trails in order to spot any peculiar activity that might signify an identity theft attack, and had passed unnoticed from IT management of the entity. Any abnormality concerning accounts activity, such as (a) suspicious, unexpected and difficult to explain charges in transaction bills, (b) malfunction or unexplainable denial of credit cards in online and offline spots of payments, (c) peculiar, usually new and unauthorized accounts and transactions included on semester or annual credit and bank reports, (d) unable to receive the semester or annual credit and bank report or bills and emails from bank, customers and relevant stakeholders and (e) peculiar phone calls or emails and other communication for bills and accounts for offers, product and services that the entity does not sell or/and buy. Due to severity of the situation and its consequent

²⁶⁴ US Federal Trade Commission, 2019, *Ransomware*, <https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/ransomware> (last retrieved 25/06/2019).

crimes, countries had adopted relevant reporting systems²⁶⁵, so auditors must always be notified for the submission of these reports and what authorities responded to them.²⁶⁶

VI] 4. 2. 7 Keylogger

Auditors must pay special attention to any reported incidence of keylogging during their controls. What is more, internal and external auditors, when the design and perform their internal controls tests, must examine not only if they relevant by entity policies exist and function properly and effectively, but also if the keylogger applications do not shown signs of vulnerability and other problems, capable to constitute them easy targets to external attack and internal misbehaviors.²⁶⁷

VI] 4. 2. 8 Financial Information Disclosure and Use of Social Media Vulnerabilities

Since disclosure of material financial information in media and mostly in social media can have a significant impact, negative and positive, on (a) an entity's reputation, leading sometimes to the so-called phenomenon of brand sabotage due to social media fiascos and compliance penalties, (b) an entity's compliance with legislation and other lawful requirements, (c) stocks' liquidity and investors' attractivity as a way to decrease information asymmetry²⁶⁸, (d) investors' and customers' behavior towards the entity, especially in cases of product recall crisis²⁶⁹ or extended negative criticism incidents, even if

²⁶⁵ For example, in United States of America an entity can report a identity theft in Federal Trade Commission in its specially for that purpose designed website <https://www.identitytheft.gov> and get significant help as it concerns the process of recovering from such an incident. Moreover, US' IRS has a relevant reporting system for tax-related identity thefts and frauds. **IRS**, 2019, *Identity Theft Central*, <https://www.irs.gov/identity-theft-central> (last retrieved 25/06/2019).

²⁶⁶ **CISA**, 21/11/2018 (revised), *Security Tip (ST05-019): Preventing and Responding to Identity Theft*, <https://www.us-cert.gov/ncas/tips/ST05-019> (last retrieved 25/06/2019). **United States Department of Justice**, 07/05/2017, *Identity Theft*, <https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud> (last retrieved 25/06/2019).

²⁶⁷ **McAfee**, 23/07/2013, *What is a Keylogger?*, <https://www.mcafee.com/blogs/consumer/family-safety/what-is-a-keylogger> (last retrieved 25/06/2019).

²⁶⁸ **Blankespoor Elizabeth, Miller Gregory S., and White Hal D.** (January 2014), *The Role of Dissemination in Market Liquidity: Evidence from Firms' Use of Twitter*, *The Accounting Review* (2018) by American Accounting Association, Volume 89, Issue 1, Pages 79–112, <https://aaapubs.org/doi/abs/10.2308/accr-50576> (last retrieved 25/06/2019).

²⁶⁹ **Lee Lian Fen, Hutton Amy P., and Shu Susan** (May 2015), *The Role of Social Media in the Capital Market: Evidence from Consumer Product Recalls*, *Journal of Accounting Research*, Volume 53, Issue 2, Pages 367-404, <https://onlinelibrary.wiley.com/doi/abs/10.1111/1475-679X.12074> (last retrieved 25/06/2019).

this criticism is coming from third-party social media users,²⁷⁰ auditors must show significant interest in assessing relevant risks during their controls trials, since the risks related with this vulnerability can be constant and in daily base, having to face not only truthful but also malicious and faulty comments and posts inside and outside the entity. Auditing the reputation risk might increase the cost of performing audits and auditing risk assessments, especially for internal auditing departments. Auditing the operational effectiveness risks can be a quite demanding effort for auditors, internal and external, but can be corelated with other IT audits on NHS, dealing mostly with requirements like the social media risk assessment and their inherent risk, the applicable controls to minimize this risk, the impact, probability and velocity concerns of this risk, which organizational goals, objectives and parts of the business model can be affected by this risk and if the existed (if there is any) media and social media strategic plan is reliant and effective enough to deal with any type of demanding disclosure and social media incidents and emergency situations or it needs modifications.²⁷¹

VI] 4. 2. 9 Supply Chain Vulnerabilities

It is particularly important for auditors (internal and external) to have a strong understanding of the way and the complexity of supply chain management systems, about the opportunities and their weaknesses, so to conduct a realistic and accurate Strengths/weaknesses/Opportunities/Threats Analysis, or best known from the acronym SWOT analysis, in order to apply the most suitable audit trail controls that will raise corporate efficiency and cost reduction. In this framework, the role of internal auditors gain significant importance, because in cooperation with the entities supply chain department can assist not only in the development of cybersecurity high-quality performance monitoring and compliance processes that will identify critical, material important, vulnerable and perhaps cases of potential succumb to bankruptcy suppliers and stakeholders, but also to implement the required control procedures and analytical tools in order to mitigate all possible risks. This added-value internal auditing supply chain performance tests can advance at least five core value domains in an entity: (a) by achieving the strategic goals and business model, that accomplish business objectives and raise profitability and customers experience, (b) by empowering organizational effectiveness and partners commitment, (c)

²⁷⁰ **Cade Nicole L.** (July 2018), *Corporate Social Media: How Two-way Disclosure Channels Influence Investors*, Accounting, Organizations and Society Journal, Volumes 68-79, Pages 63-79, <https://www.sciencedirect.com/science/article/abs/pii/S0361368218300837> (last retrieved 25/06/2019).

²⁷¹ **Prof. Singleton Tommie** (2012), *Ibid*, Page 13 and **Deloitte** (2013), *Ibid*.

by promoting processes' excellence and operations' effectiveness, (d) by enhancing reliability and dependability of supply chain planning, executing and information quality and technological capacities and (e) by increasing general performances in supply chain abilities, cash liquidity, shareholders returns, cost-reduction and reputation.²⁷²

VI] 4. 2. 10 Intellectual Property Cyber-thefts and Industrial Cyberespionage

Auditors not only must controls and inspection all the capacities an entity had impose to protect its intellectual properties from thefts, concerning mostly the protection of NHS system from the traditional malicious cyber threats (such as viruses, trojans, DDoS, rootkits, etc.), but they must also in their system of cybersecurity controls incorporate the intellectual property vulnerability concern, by: (a) making sure that in case of use of a SCIF, this is conducted with the most effective and applicable way, (b) assuring that no unauthorized individuals and devices can have access to the whole process of development, testing, patenting and application of IP data, (c) the effective implementation of confidentiality and non-disclosure agreements between IP personnel and/or external IP services providers, (d) if there is an updated IP protection insurance and what this insurance cover, (e) if the entity has any IP breach recovery plan and if yes, if it is updated and suitable? is personnel quite familiar with it? Perhaps, the auditor might propose to the entity to make proactive emergency incidents exercises or automated vulnerability assessments in order (i) to spot any vulnerabilities, anomalies in its NHS systems and (ii) to prepare its personnel better. If the entity does not have one, auditors can propose its creation, (f) in case of an actual IP theft, how the entity react? What were the implications? What kind and size of resources are lost because of it? What will be the expenses in order to return to the status quo ante, if that is possible? How the entity calculates the loss of an IP incident and how it transferred this estimation in its financial statements according to relevant accounting standards? Did the company make all the necessary provisions and adjustments (disclosures) to its financial statements after the incident according to relevant accounting standards? Did the report the incident to the authorities (especially if the entity is obliged to do so) and how

²⁷² **Pasula Milan, Nerandžić Branislav and Radošević Milan** (2013), *Internal Audit of the Supply Chain Management in Function of Cost Reduction of the Company*, Journal of Engineering Management and Competitiveness (JEMC), Volume 3, Issue No. 1, 2013, Pages 32-36 ISSN 2217-8147 University of Novi Sad, <https://www.researchgate.net/publication/320819794> Internal audit of the supply chain management in function of cost reduction of the company (last retrieved 25/06/2019).

authorities deal with this? etc. must be among the priority questions and indications of concern for the auditors.²⁷³

VI] 4. 2. 11 Vulnerabilities due to Emerging Technologies:

VI] 4. 2. 11. A) Blockchain, Smart Contracts and Crypto-assets

Since there is no universally accepted standard for Blockchain technology regulation and auditing, only guidelines from related national authorities and institutional bodies²⁷⁴, compliance requirements derail from other national legal frameworks against fraud and fraudulent reporting. Among the areas that auditor must give special attention and perform tests, regarding blockchain and crypto-assets domains are: (i) *Blockchain Development, Deployment and Data Management Concerns*: the audit control tests in this category aim to secure that the creation, establishment, usage and data generation of the decided by management type of blockchain technology used in the most appropriate and effective way for an entity's needs. Auditors, therefore, must base their controls assessment findings in the following potential areas of risk: (a) is the structure of the blockchain used the most appropriate? Does the smart contracts methods used the most applicable and inclusive for all transactions demands and vulnerability scenarios? (b) is the level of protection (digital and physical) and ownership of public keys and public DLTs the most assuring, according to standards and efficient? (ii) *Operation, Access, Maintenance and Continuity Concerns*: this domain of audit controls provides feedback to the following audit concerns: (a) is the system of access to sensitive data and codes about the blockchain systems effective and protective enough, not to permit entrance to unauthorized individuals inside (management, employees, third-party contractors, etc.) and outside (cybercriminals, rival companies, cyber-spies, etc.) the entity? (b) does the entity deploy the right monitoring system capable to track any security vulnerability, anomaly and default in the blockchain network? Is time

²⁷³ **Gelinne John, Fancher J. Donald and Mossburg Emily** (25/07/2016), *The hidden costs of an IP breach: Cyber theft and the loss of intellectual property*, Deloitte Review Issue 19, <https://www2.deloitte.com/us/en/insights/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html> (last retrieved 25/06/2019). **KPMG** (2016), *Securing Industrial Control Systems*, <https://assets.kpmg/content/dam/kpmg/ca/pdf/2016/11/ca-kpmg-cyber-securing-industrial-control-systems.pdf> (last retrieved 25/06/2019).

²⁷⁴ Such as the relevant guidelines the US Financial Industry Regulatory Authority (FINRA) had developed about the impact of the blockchain and Distributed Ledger technologies (DLT) on securities, capital markets and broker-dealers. **FINRA** (31/03/2017), *Report on Distributed Ledger Technology: Implications of Blockchain for the Securities Industry*, <https://www.finra.org/rules-guidance/guidance/faqs/report-distributed-ledger-technology-implications-blockchain-securities-industry> , (last retrieved 25/06/2019).

effective and resources saving too? Is it able to spot early-on and effectively any hacking and malicious malware penetration attempts, or DDoS attacks? Is it able to neutralize these threats on time and protect core systems and operations? Can estimate their latency? (c) Does the entity makes periodical tests, updates and upgrades in business continuity and recovery plans, in cooperation with its external blockchain vendors and stakeholders, in case of an extended problem in its blockchain NHS systems? (d) Is the documentation and controls assurance reports of the normal functionality and operability of the whole blockchain processes conducted periodically, available and easy to produced? Is the access in this data protected from unauthorized individuals? (e) Does the entity apply the best security backup practices and standards to minimize any data breach of private keys, invoices, transactions, on-line and off-line data, especially if third-party vendors are involved? (f) Does the company maintain, protect and periodically review and assess blockchain passwords, private keys, permissions and other sensitive information, and (iii) *Achieving Business Goals and Strategies Concerns.*²⁷⁵

VI] 4. 2. 11. B) Electronic commerce or e-commerce and e-governance

First of all, auditors must gain a clear view about the usage level and the generating income level of the e-commerce inside an entity. The higher the level of incoming derailing from e-commerce activities the more the cybersecurity risks are so consequently more controls must be conducted. Secondly, they must inspect if the e-signatures and e-contract obligations according to international, peripheral, European and national laws and relevant certifications are updated and functional, since this is an area of inspection according to *ISA 315 on Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement and ISA 250 on Consideration of Laws and Regulations in an Audit of Financial Statements.*

VI] 4. 2. 11. C) Artificial Intelligence

The great extension and use of AI applications to all industries and sectors had led front-line leading auditing firms to invest significantly in AI and create their own AI auditing risks frameworks. For example, in 2015 **Deloitte** won prestigious “Audit Innovation of the Year” award by the International Accounting Bulletin, for developing and

²⁷⁵ Maguire Eamon, Nagaraj Kiran, Wyner Sam and Goens LaDarius (2017), Ibid.

using the *Argus* AI cognitive technology system to process and recognize information of material accounting significance in electronic databases and documentation.²⁷⁶ In 2017, **PriceWaterCoopers** (best known as pwc), had won the same award for developing *GL.ai*, an AI algorithmic software able to work as an experienced auditor capable to identify frauds, errors and misconducts in transactions during audit trails.²⁷⁷ At the same period, **KPMG** had created a relevant risks and controls framework upon 17 domains of AI related managing risks and controls, able to identify 78 risks and 106 controls, in areas such as IT operations, strategy and governance, human resources management and security management.²⁷⁸ Also, KPMG had created *Clara*, an analytical, data driven, AI risk assessment tool platform that enhance audit quality.²⁷⁹ In general terms, (internal and external) auditors actions concerning AI audit inspections must focus on: (a) parameterizing the materiality of existing and potential risks of AI applications may impose to normal and effective operationality and functionality of an entity, and its ability to achieve successfully strategic goal, (b) the resources allocated for its use, but also those that are saved by it and how properly are estimated and articulated in financial statements, and in which category of assets must be incorporated, (c) authentication, authorization and standard access of personnel to AI applications, (d) physical protection of AI-related NHS systems and (inter)connection with other NHS systems, (e) in case of usage of AI outsourced capacities, to identify the risks of using a third-party AI contractor, since the vendors cyber and all other types of vulnerabilities can effect negatively and the entity's AI and other NHS systems, especially in case of an extended sophisticated attack to a third-party contractor can lead to penetration and destructions to analogous NHS systems of all its clients and providers.²⁸⁰

²⁷⁶ **Deloitte** (2019), *Deloitte wins 'Audit Innovation of the Year' at 2015 International Accounting Bulletin awards*, <https://www2.deloitte.com/ch/en/pages/audit/articles/deloitte-wins-iab-audit-innovation-award.html> (last retrieved 25/06/2019).

²⁷⁷ **PWC** (2019), *Harnessing the power of AI to transform the detection of fraud and error*, <https://www.pwc.com/gx/en/about/stories-from-across-the-world/harnessing-the-power-of-ai-to-transform-the-detection-of-fraud-and-error.html> (last retrieved 25/06/2019).

²⁷⁸ **Holland Paul, Rae Shamus and Taylor Paul** (2018), *Why AI must be included in audits*, KPMG, <https://assets.kpmg/content/dam/kpmg/uk/pdf/2018/06/why-ai-must-be-included-in-audits.PDF> (last retrieved 25/06/2019).

²⁷⁹ **KPMG International** (June 2018), *KPMG Clara: A smart audit platform*, <https://assets.kpmg/content/dam/kpmg/xx/pdf/2017/05/kpmg-clara-a-smart-audit-platform.pdf> (last retrieved 25/06/2019).

²⁸⁰ Prof. **Klous Sander** (08/06/2018), *In AI we trust?: Assurance is more important than ever in the age of machines*, KPMG, <https://home.kpmg/xx/en/home/insights/2019/04/in-ai-we-trust.html> (last retrieved 25/06/2019). **Kokina Julia and Davenport Thomas H.** (2017), *The Emergence of Artificial Intelligence: How Automation Is Changing Auditing*, American Accounting Association: Journal of Emerging Technologies in Accounting, Volume 14, Issue 1, available at <https://meridian.allenpress.com/jeta/article-abstract/14/1/115/116001/The-Emergence-of-Artificial-Intelligence-How?redirectedFrom=fulltext> (last retrieved 25/06/2019). **Brennan Bill, Baccala Mike, and Flynn Mike** (02/02/2017), *Artificial Intelligence Comes to Financial Statement Audits*, CFO online, <https://www.cfo.com/auditing/2017/02/artificial-intelligence-audits/> (last retrieved 25/06/2019). **Issa Hussein, Sun Ting, and Vasarhelyi Miklos** (2016),

VI] 4. 2. 11. D) Internet of Things (or IoT)

Auditors must take under serious consideration when the designing their assessment controls on IoT NHS systems all the three types of risks we just mentioned. They must create risk scenarios during their pre-auditing planning based on their identification and selection of the IoT devices and software that they must be inspected and which of them possess greater risks due to their importance for business operations and continuity, their potentiality of being hacked, their difficulty of risk mitigation, their access concerns, the easiness and cost-effectiveness of their updates and upgrades, the ability to be efficiently monitored, the data privacy, data ownership, data collection, data protection and data retention and disclosure issues they might impose, and with concerns about the storage and sharing of the data IoT systems produce. Since there is not universally accepted definition and standards about the quality, performance, operability, and safety of IoT, there are now relevant audit performance programs on IoT that are accepted and recognized worldwide apart a series of guidelines, like Open Web Application Security Project (OWASP) IoT Security Guidance, Global System for Mobile Communications Association (GSMA) IoT Security Assessment, ISACA's COBIT 5, etc. In indirect way, we can have the application of obligatory legal requirements concerning mostly data privacy and handling, like the European Union's General Data Protection Regulation. Auditors must take under consideration these frameworks, obligatory and voluntarily, when they create their IoT risk scenarios. Among the necessary steps during an audit process must include can be the following: (a) a minimum general type of controls, that are typical to all technological related audits, IoT included, concerning the risk of IoT technology, the possibility to be hacked (b) data-related and data-specified controls concerning the IoT applicability, like those we mentioned previously, (c) analytical and ensuring controls, that analyze and provide useful data about the functionality and results of IoT, that will aid and shape relevant decision-making and (d) controls concerning the fulfilment of business and general organizational goals and strategies from the implementation of IoT, including the demands of resilience, business continuity and recovery in case of an enlarge problem in IoT capacities.²⁸¹

Research Ideas for Artificial Intelligence in Auditing, The Formalization of Audit and Workforce Supplementation, American Accounting Association: Journal of Emerging Technologies in Accounting, Volume 13, Issue 2, available at <https://meridian.allenpress.com/jeta/article/13/2/1/115980/Research-Ideas-for-Artificial-Intelligence-in> (last retrieved 25/06/2019).

²⁸¹ **Cooke Ian and Raghu R. V.** (01/09/2018), *IS Audit Basics: Auditing the IoT*, ISACA Journal, Issue 2018: Volume 5, <https://www.isaca.org/resources/isaca-journal/issues/2018/volume-5/is-audit-basics-auditing-the-iot>

VI] 4. 2. 11. E) Cloud Services and Software as a Service (SaaS)

First of all, auditors, internal and external (individuals, teams and firms), must have a strong understanding of what is a cloud and SaaS?, their components, scalability, performance, results, pros and cons. Both ISACA's and ISO's Frameworks provides detailed guidelines on how auditors and IT specialists can acquire relevant accreditations and the necessary knowledge they should have in order to perform the best their auditing duties. Moreover, they must (a) to identify the type of cloud, external data storage, IaaS and SaaS service the entity uses and its risks of using these technologies, (b) to perform adequate risk mitigating controls, (c) to ask and incorporate in their IT controls any incident, attack and data-breach took place to the third-party providers storage systems and how these situations had negatively affect the client's entity data intactness, next to reports about the updates and upgrades to their storage systems.²⁸² The realization of importance of proper data gathering for auditing purposes by using cloud platforms and thus the incorporation of cloud services in auditing practices had become more and more present in auditing firms, which develop their own similar innovations. For example, **Deloitte** had developed a cloud-powered data platform *Cortex*, that permits an effective data acquisition, organization and assessment respecting cybersecurity and analytical auditing concerns, winning for its development the 2018 'Audit Innovation of the Year' at The Digital Accountancy Forum & Awards.²⁸³

VI] 4. 2. 12 Outdated Technology Vulnerabilities

Auditors must always check if an entity implements a variety of sophisticated controls as it concerns the necessary or/and obligatory updates and upgrades in software

(last retrieved 25/06/2019). **Protiviti** (2016), The Internet of Things: What is It and What Should Internal Audit Care?, https://www.protiviti.com/sites/default/files/united_states/insights/internal-audit-and-the-internet-of-things-whitepaper-protiviti.pdf (last retrieved 25/06/2019). **Salman Syed** (29/10/2015), *Auditing the Internet of Things: The rise of Internet-connected devices and systems bring both new opportunities and risk for modern organizations*, Institute of Internal Auditors, <https://iaonline.theiia.org/2015/auditing-the-internet-of-things> (last retrieved 25/06/2019).

²⁸² **Signleton Tommie W** (01/05/2010), *IT Audits of Cloud and SaaS*, ISACA Journal, <https://www.isaca.org/resources/isaca-journal/past-issues/2010/it-audits-of-cloud-and-saas> (last retrieved 25/06/2019).

²⁸³ **Deloitte** (05/10/2018), *Deloitte Wins 2018 'Audit Innovation of the Year' at The Digital Accountancy Forum & Awards: Two-time award winner Deloitte recognized for its Audit-Transforming "Cortex" data platform*, <https://www.prnewswire.com/news-releases/deloitte-wins-2018-audit-innovation-of-the-year-at-the-digital-accountancy-forum--awards-300724977.html> (last retrieved 25/06/2019).

protocols and hardware capacities and assure that at least the most sensitive data are not handled by non-high-qualified and unauthorized employees in outdated NHS systems.

VI] 4. 2. 13 Compliance with Cybersecurity National and International Regulatory Norms

Auditors must examine thoroughly all the requirements deriving from obligatory cybersecurity norms, as those we represent in the previous Chapter. Especially, they must give proper attention to requirements like securities market proper function, anti-laundry money issues, data protection and privacy, cybersecurity accreditations, cybersecurity protection of critical infrastructure, proper following of recognized cybersecurity and auditing standards, such as ISO's and ISACA's, when the entity admits that will implement a relevant standard, proper reporting of data breaches, examination of any imposed penalty, existed or potential, such as those included in EU's GDPR and their implication to proper functionality of the company, especially if the penalty is a hefty one to money capacities of an entity, and any other related regulatory requirement, as those we described in the previous Chapter.

VI] 5. Conclusions

The phase of planning and executing a sound, reliable, accurate, productive, trustworthy and effective audit program is an extremely difficult and complex task, but the successful conduction of it provides to the auditor all the necessary audit evidence for best formulation of its final audit opinion and the issuance of its final audit report, a process examined in the next Chapter. Any wrongdoing in any of the sub-phases of the two major particles, meaning the planning and the execution phase, might lead to a number of problems, such as: (a) reconduction of the designing phase of planning and execution, (b) reconstruction and reconduction of the audit evidence collection process, by resetting the testing requirements and the sampling procedures, and (c) tracking of any informalities and inconsistencies in the whole process, even after its reconstruction and reperformance. This hefty duty signifies more allocation of audit resources and drawbacks from the auditor(s), such as (i) potential appointment of more auditors or better qualified, (ii) extra working hours for the reperformance of the same tasks, (iii) use of more advanced and sophisticated software, that perhaps must be purchased, (iv) use of external cybersecurity experts, cyber-

related legal counsels, and cybersecurity investigators, such as “white hat” hackers, which are individuals that have superior hacking capacities, but they use them to help entities and not against them, (v) additional communication with the management and internal auditors, that might lead to loose of faith and trust from top executives of the entity towards the auditor(s) or audit firm performing the audit program, (vi) better communication and exchange of information with law enforcement and imposing penalties authorities, to get a better understanding in cybersecurity incidents and events, like data breaches, identity thefts, and intellectual property thefts, especially if these incidents are accompanied with heavy fines and penalties, as in the case of GDPR and NIS Directive in EU market, or result significant loose of the entity’s money capacities, and there were not taken under account during the initial phases of auditing planning and execution, or they took place after them, but they have a significant impact to the entities proper creation of financial statements, etc.

In the next Chapter and final as it concerns the main analysis of the this Thesis before the Chapter of Final Conclusions, we will examine how all the data and articulations received from the phases of audit program planning and execution assist auditors to formulate their audit opinion, with the issuance of their final audit report. Any weakness and mistakes in the phases of audit program planning and execution will result a final report, also problematic and inconsistent to the reality of operations of the entity. So, auditors must always bear in mind that as it concerns the processes of planning and execution of their audit program, the devil is on the details, and in this particular case the details are the proper conduction of sampling and testing, external verification, etc., while the devil is any cybersecurity and cyber-preparedness risk and vulnerability, that is not handled, tested, mitigated and reported properly. In any case, both the “devil” and “its details” must be included ai the most accurate and reliable way in the final audit report, that auditors provide to the client entity and to the public.

V] CHAPTER 4 : ISSUANCE OF CYBERSECURITY AUDITING REPORT

The final step in every auditing process, also known as the reporting and follow-up phase, is the issuance of the final auditing report, in which the assigned auditor must (a) gather all the necessary documents and required data for a sound audit report, (b) prepare an outline of the report, also known as draft, (c) create the final edition of the report, (d) disclose and communicate the final version of the audit report to the client entity and (e) permits follow-up when is necessary, according to *ISA 700 on Forming an Opinion and Reporting on Financial Statements*, *ISA 705 on Modifications to the Opinion in the Independent Auditor's Report*, *ISA 706 on Emphasis of Matter Paragraphs and Other Matter Paragraphs in the Independent Auditor's Report*, *ISA 710 on Comparative Information-Corresponding Figures and Comparative Financial Statements*, and *ISA 720 on The Auditor's Responsibilities Relating to Other Information in Documents Containing Audited Financial Statements*, that provide detail provisions about the best conduction of this step. *ISA 800 on Special Considerations-Audits of Financial Statements Prepared in Accordance with Special Purpose Frameworks*, *ISA 805 on Special Considerations-Audits of Single Financial Statements and Specific Elements, Accounts or Items of a Financial Statement*, on *ISA 810 on Engagements to Report on Summary Financial Statements and International Standard on Quality Control*, offer further guidance upon special purposes and elements of an audit inspection, engagement concerns, quality control, and other aspects of proper audit in an entity's financial statement.

In general terms, *ISA 700 on Forming an Opinion and Reporting on Financial Statements*, referred to the proper technical and contextual aspects that the final audit report, including the cybersecurity aspect, that the audit report must have in order to fulfil its objectives of (a) providing an opinion on the soundness and fair presentation of the client entity's financial statements, prepared in all their material aspects according to the

applicable financial reporting frameworks, based on the examination and evaluation of the acquired audit evidence, which must be sufficiently obtained and appropriate, and (b) expressing evidently that opinion provided on a written report, which additionally describes the basis for that opinion. As it concerns the technical aspects of the final audit report, that includes the auditor final opinion, those are referred to the proper presentation of the report, that not only (a) must be in a written form, but also must include (b) the specification and the status of the financial statements that had been audited, (c) the date or period that financial statements cover, (d) the relevant responsibilities of the management, (e) the auditor's responsibility, (f) the auditor opinion's analysis, (g) the date of issuance of the audit report, (h) the signature of the auditor and (i) the auditor's address. As it concerns the contextual aspects of the final audit report, those include (a) the expression of the auditor's responsibility, (b) the expression of assurance that the audit program and the audit opinion had been performed and developed according to the applied, laws or regulations, ISAs or/and auditing standards of a specific jurisdiction, providing a true and fair view of the examined financial statements, and (c) the potential inclusion of explanation about the application of other explanatory material, such as qualitative aspects of the entity's accounting practices, disclosure of the effect of material transactions and events on the information conveyed in the financial statements, and the description of the applicable financial reporting framework, that can assure material inconsistencies, and material misstatements of fact, according to *ISA 720 on The Auditor's Responsibilities Relating to Other Information in Documents Containing Audited Financial Statements*.²⁸⁴

ISA 705 on Modifications to the Opinion in the Independent Auditor's Report indicates that auditors can proceed to modification of their original opinion in the following two cases: (a) when the entity's financial statements as a whole are not free from material misstatement, despite the acquired evidence, or (b) when the auditor realizes his/hers inability to acquire sufficient appropriate audit evidence, in order to properly decide whether the financial statements as a whole are free from material misstatement or not. The possible modified auditor's opinion, as Image No 10 indicates, can be of three types: (i) *a qualified opinion*, which is expressed in the following two situations: (a) when the auditor had acquired sufficient and appropriate audit evidence, and has the opinion that financial

²⁸⁴ **IFAC** (2010), *International Standard on Auditing (ISA) 700 on Forming an Opinion and Reporting on Financial Statements*, <https://www.ifac.org/system/files/downloads/a036-2010-iaasb-handbook-isa-700.pdf> (last retrieved 25/06/2019). **IFAC** (2010), *International Standard on Auditing (ISA) 720 on The Auditor's Responsibilities Relating to Other Information in Documents Containing Audited Financial Statements*, <https://www.ifac.org/system/files/downloads/a040-2010-iaasb-handbook-isa-720.pdf> (last retrieved 25/06/2019).

statement contain material, but not pervasive²⁸⁵ misstatements, individually or aggregately, or (b) when the auditor realizes his/hers inability to acquire sufficient and appropriate audit evidence, but formulates the opinion that the possible impact of unobserved and potential misstatements on the financial statements could be of material kind and still remain not pervasive, (ii) an *adverse opinion*, which is expressed when the auditor despite having acquired sufficient and appropriate audit evidence, formulates the opinion that misstatements (individually or aggregately) on the financial statements are both of material

kind, and pervasive, and (iii) a *disclaimer of opinion*, when the auditor realizes his/hers inability to acquire sufficient and appropriate audit evidence, but formulates the opinion that possible impacts and effects of unobserved misstatements (if any) on the financial statements could be both of material kind, and pervasive. The case of disclaiming an opinion, must be given only in extremely rare

Image No 10: Types of Modified Opinions

Nature of Matter Giving Rise to the Modification	Auditor's Judgment about the Pervasiveness of the Effects or Possible Effects on the Financial Statements	
	Material but Not Pervasive	Material and Pervasive
Financial statements are materially misstated	Qualified opinion	Adverse opinion
Inability to obtain sufficient appropriate audit evidence	Qualified opinion	Disclaimer of opinion

Source: IFAC (2010), *International Standard on Auditing (ISA) 705 on Modifications to the Opinion in the Independent Auditor's Report*, <https://www.ifac.org/system/files/downloads/a037-2010-iaasb-handbook-isa-705.pdf> (last retrieved 25/06/2019).

situations characterized by numerous uncertainties, when the auditor despite having acquired sufficient and appropriate audit evidence, concerning every single of the uncertainties, still it is impossible for him/her to formulate an opinion on the financial statements due to the potential interactivity between those uncertainties and their probable collective effect on the accuracy of financial statements.²⁸⁶ Cybersecurity extended incidents, such as those we examined in relevant section of Chapter III, like hefty data breaches, or intellectual property thefts, or disruption to supply chain management systems, etc., can provoke a disclaimer of

²⁸⁵ The term of pervasiveness of misstatements on financial statements according to ISA 705 “describes the existed or potential impact and effects on the financial statements of misstatements that are undetected due to an inability to obtain sufficient appropriate audit evidence. Pervasive effects on the financial statements are those that, in the auditor's judgment: (i) Are not confined to specific elements, accounts or items of the financial statements; (ii) If so confined, represent or could represent a substantial proportion of the financial statements; or (iii) In relation to disclosures, are fundamental to users' understanding of the financial statements.” IFAC (2010), *International Standard on Auditing (ISA) 705 on Modifications to the Opinion in the Independent Auditor's Report*, <https://www.ifac.org/system/files/downloads/a037-2010-iaasb-handbook-isa-705.pdf> (last retrieved 25/06/2019).

²⁸⁶ IFAC (2010), *International Standard on Auditing (ISA) 705 on Modifications to the Opinion in the Independent Auditor's Report*, <https://www.ifac.org/system/files/downloads/a037-2010-iaasb-handbook-isa-705.pdf> (last retrieved 25/06/2019).

opinion, due to the fact that not only they incorporate a lot of hefty uncertainties, such as destruction or permanent loss of sensitive databases, reputation costs, repairing costs, reparation costs for individuals and entities negatively affected, compliance costs and penalties, etc., but also their cumulative impacts can exceed the examined time period and last for years. We should not forget the case of Yahoo!/ Alibaba data breach (in pages 121-122 of the Master Thesis) that USA's SEC, issued in April, 2018, its first ever action against an entity for a cybersecurity disclosure violation with the Accounting and Auditing Enforcement Release No. 3937, but also years later Verizon Communications, Inc. used the breach in order to lower the acquisition price by 7.25 percent, as well as the company's obligation to pay a settlement of \$29 million as fiduciary duties concerning the non-proper handling of its users' data during a series of cyberattacks taking place from 2013 until 2016, affecting more than three billion Yahoo! users in a historical decision of Santa Clara's, California Superior Court, since it was the first time that shareholders have been granted monetary damages after winning a derivative lawsuit regarding a cybersecurity issue against their own company.²⁸⁷

Cybersecurity incidents, risks and vulnerabilities, may not only provoke the modification of the auditors opinion, but also might provoke the formulation of an opinion on the financial statements of a paragraph of an emphasis matter, according to *ISA 706 on Emphasis of Matter Paragraphs and Other Matter Paragraphs in the Independent Auditor's Report*, that is important enough as the auditors want to draw users' attention on it, by creating an emphasis paragraph on a matter (a) that must be appropriately presented or disclosed in the financial statements, due to either its fundamental importance fundamental to users' understanding of the financial statement or (b) that is not presented or disclosed in the financial statements, but according to auditor's verdict, is related to users' understanding upon the audit, the auditor's responsibilities or the auditor's report²⁸⁸

After having formulate his/hers final cybersecurity related opinion and articulated with the proper presentation elements on his/hers final written report, the auditor must disseminate and disclose the report to the examined entity's top management and to the public according to the applied legal frameworks. The report, apart from the key findings and conclusion(s) as it concerns IT/cybersecurity issues, can also contain relevant

²⁸⁷ Newman Craig A. (23/01/2019), *Lessons for Corporate Boardrooms From Yahoo's Cybersecurity Settlement*, <https://www.nytimes.com/2019/01/23/business/dealbook/yahoo-cyber-security-settlement.html> (last retrieved 25/06/2019).

²⁸⁸ IFAC (2010), *International Standard on Auditing (ISA) 706 on Emphasis of Matter Paragraphs and Other Matter Paragraphs in the Independent Auditor's Report*, <https://www.ifac.org/system/files/downloads/a038-2010-iaasb-handbook-isa-706.pdf> (last retrieved 25/06/2019).

recommendations and even reservations, for which the auditor must provide the related audit evidence in order to draw the attention of the management, readers and users of the audit report to important cybersecurity concerns on the financial statements. This will allowed to the auditor to have a proper follow-up in the future, either if the same individual or firm, must perform for another economic period the IT/cybersecurity audit inspection of the company, either if this task is conducted by another individual and firm, which will use the previous economic periods general audit reports and specialized cybersecurity audit reports as a guide that provides areas of further focus, concern and inspection.

Last but not least, we must mention that any errors, misstatements, cooperation with the client entity's management to present a better situation that what actually is, and defaults in the proper conduction and reporting of the IT/cybersecurity audit opinion by the auditor can be synonymous to hefty disciplinary penalties from each country's national authority of overseeing audit professionals upon the proper conduction of the audit service and profession.

V I] C H A P T E R 5 : FINAL CONCLUSIONS ON HOW CYBERSECURIT HAD TRANSFORMED AUDITING SERVICE

In this Master Thesis we set as our primary goal, already through its title, the necessity of integration of aspects of cybersecurity and cyber-preparedness into the auditing processes, audit profession, internal and external, audit service, internal and external, audit practice, and auditing science evolvement. We start this journey from the Introductory Chapter, by presenting exactly the fundamental question of this Master Thesis, meaning how important and necessary is the incorporation of cybersecurity and cyber-preparedness in the auditing processes, as well as presenting the two major thematics, the cybersecurity and the cyber-preparedness, and their components, and how these thematics are related to modern economic entities functions and to their obligation of proper financial reporting without misstatements, defaults and irregularities, regarding cybersecurity concerns.

In the next part of the Master Thesis, Chapter One, we attempt to examine the reasons why is important to incorporate cybersecurity and the cyber-preparedness into the auditing service. We choose to conduct this attempt in two forms, the first one is concerning the historical and philosophical perspective and how technological advancements and their constant usage by corporations and entities of all sizes, sectors and natures (private, public, mix, non-profit) constitutes cybersecurity and the cyber-preparedness concerns among the fundamental ones, the second one is correlated with the modern business risk model, that demands from entities to be adequately prepared against a great variety of risks and vulnerabilities in order to offer to the public and related authorities financial statements, that are free from mistakes, defaults and errors. Modern entities cannot be completely riskproof, if they do not incorporate in their risk assessment, analysis and mitigation the dangers and misappropriations, that cybersecurity and cyber-preparedness can bring in the their

operational, financial and survival instincts and capacities. Despite the fact that the level of cybersecurity risk taking is analogous to the risk mentality and tolerance of every entity, the role of auditors and more precisely of cybersecurity or IT auditors, internal and external, is gaining more and more importance in tracking, neutralize and properly disclose cyber-related dangers to internal audiences, but also and more significantly to external audiences, like shareholders, existed or potential investors, resources lenders, providers/suppliers, related authorities and rest stakeholders. That is why, the implementation and existence of a sufficient, effective and defaults-recognizing cybersecurity audit program, as part of the general overall audit program, must be faced and considered not only as a pure necessity but also as a demand too, becoming an entity's goal on its own.

In Chapter Two, we try to analyze the first two parts of any sufficient, effective, and defaults-recognizing cybersecurity audit program, which is the proper appointment of the IT/Cybersecurity auditor by the client entity. This audit engagement mandate must contain all the needed from the side of entity goals and resources for the best conduction of the IT/Cybersecurity audit program, as well as from the side of the auditor the proper and fruitful understanding of the entity's cybersecurity risks and cybersecurity functional environment. Is of the outmost importance for the auditor to have a solid and productive understanding upon the correlation between cybersecurity dimension and the entities' internal controls systems, in order to design and conduct the most appropriate audit program. These cybersecurity landscapes and dangers understanding by the auditors is a quite challenging and complex task, since it involves the deep insight and identification, from one side of most important cybersecurity risks and vulnerabilities to the entities' internal controls systems, such as malicious code and programs, harmful malwares, social engineering and phishing, (distributed) denial of service attacks, ransomware, CEO/CFO scams or whaling and identity thefts, keylogger issues, financial information disclosure and use of social media vulnerabilities, supply chain vulnerabilities, intellectual property cyber-thefts and industrial cyberespionage, outdated technology vulnerabilities, and vulnerabilities due to emerging technologies, like blockchain, smart contracts and crypto-assets, electronic commerce or e-commerce and e-governance, artificial intelligence, internet of things, and cloud services and software as a service, and from the other side the deep grasp and awareness upon the obligatory legal cybersecurity compliance frameworks in every country the entity's operates. Even though, we would like to offer a detailed presentation of all the national legal cybersecurity compliance frameworks and norms, this task will exceed by far the scope and extension of this Master Thesis, so for technical and research reasons we

narrow this presentation to the three most important relevant frameworks: in national level, we examined the case of Great Britain (UK) and the United States of America (USA) and in the level of an international intergovernmental organization with obligatory norms for natural and legal persons, we examined the case of European Union (EU). We choose these particular frameworks, because they are considered as the most advanced, sophisticated and leading in the examined here domains. What we must refer as the basic conclusions upon the examination of these frameworks is (a) that they contain an extended series of laws on subjects like promotion of markets and securities stability and integrity, protection of data, data holders and privacy, freedom of information promulgation, computer fraud and abuses handling and punishing, cybersecurity certification schemes, protection of critical infrastructure, networks and information systems, (b) that some norms are accompanied by hefty fines and penalties, such as those imposed by EU's GDPR and NIS Directive, or/and even prison time, such as USA's Computer Fraud and Abuse Act, and (c) that the examined here countries and the EU also had created the proper mechanism, meaning institutions and regulatory bodies, such as USA's SEC, AICPA, PCAOB, FBI, CISA, etc., and EU's ENISA, and Europol/European Cybercrime Centre, in order not only to oversee, inspect, investigate and impose adequate fines, and penalties in entities, accountants and auditors upon cybersecurity actions and violations, but also to provide cybersecurity guidance and consultancy concerning the appropriate execution of entities, accountants and auditors tasks and operations, and critical infrastructure protection against cybersecurity risks and vulnerabilities. Are these developments enough to protect entities and auditors from cybersecurity attacks and mistakes or misstatements? Probably not! The huge amount of almost everyday cyber-attacks, regardless if they are successful or not, indicates that protection systems are never enough to stop malicious cyber-behaviors. The application of effective and efficient internal controls systems by entities, that aim to prevent, detect, and correct cyber-related risks and defaults is the first line of defense from the entities' side, but also the landscapes where IT auditors will designed and execute their audit program and tests.

In Chapter Three, we aimed exactly to examine the third phase of an audit program, that is consisted of two sub-phases, the phase of planning and the phase of executing a cybersecurity auditing program. We examined that every phase of planning and execution is consisted of sub-phases, but the important is that internationally recognized institutions, such as ISO and ISACA, IIA, had developed standards, guidelines, accreditation schemes, tools and programs, in order to support entities and auditors in their cybersecurity, cyber-

preparedness duties. As it concerns the design and planning sub-phase of an audit program, auditors, must always bear in mind, that in order to perform with high quality and adequacy this sub-phase, they must (a) acquire a profound understanding upon the areas and the subjects of concern related to cybersecurity, that will help them articulate better the set scope of their audit programme, (b) assess those areas of concern according to their impact and their level of probability to take place, in order to create the risk matrix of overall risk for every cyber-security threat, that will assist auditors in their decisions-making upon the development of their overall audit test program and (c) develop an effective cybersecurity audit program, in order the execution phase not to present any defaults and mistakes, consisted of (1) proper identification and determination of cybersecurity controls that must be performed on NHS systems and generally in any system is related to cyber-security concerns according to the structure and the characteristics of the examined entity and includes types of controls according (i) to their purpose (preventive, detective, and corrective), (ii) to their fitting in the overall structure of an entity's internal control system (general IT controls and application controls), and (iii) to the related individuals' roles and responsibilities (governance controls, management controls and technical controls) and their sub-categories of controls, and (2) proper creation of the most suitable cybersecurity controls audit program, based in the use of most adequate, suitable and competent Generalized Audit Software (GAS) or/and Computer Assisted Audit Techniques (GAATs), that assist in the atomization of controls tests and promotion of a higher quality and objectivity of results, as well as the use of an effective Software Development Life Cycle (SDLC), that will assist auditors to plan, construct, maintain and improve their auditing programs. As it concerns the sub-phase of execution, this phase must be conducted taking under consideration the applicability and usefulness of customized audit tests according to the scale and needs of the entity, since exhausting auditing testing fieldworks are resourcefully impossible. It is consisted mostly of proper and sufficient acquisition of (a) appropriate audit evidence, through the processes of inspection, observation, (external) confirmation, recalculation, reperformance, and analytical procedures, and inquiry, (b) proper qualitative and quantitative testing, and (c) adequate sampling gathering, upon the client entity's risk assessment and quality control procedures, accounting records and internal control systems, that will assist auditors in the formulation of their professional audit opinion and the issuance of their final audit report. We finish the section of execution of the audit program by presenting a series of specialized audit tests in internal controls systems according to the examined in Chapter Two cybersecurity risks, vulnerabilities, and compliance obligations.

In Chapter Four, the last Chapter of our main analysis upon the research theme, we examined the process of formation of auditor (s) final opinion and the issuance of the final audit report, regarding cybersecurity and cyber-preparedness, that must be distributed to the top management, to shareholders, to the public and to related stakeholders, according to regulatory norms and provisions. The auditor(s) has the capability either to give a positive opinion, which is the best level of assurance as it concerns an adequate level of cybersecurity protection and related financial reporting, either to provide a qualified opinion, and either to give adverse opinion or even a disclaimer of opinion, if the cybersecurity situation is of crucial importance to the entity's survival and the later had done nothing to prevail the forthcoming cyber-disaster, either to provide an emphasis matter paragraph, for cybersecurity issues that demands further attention from the users' of financial statements.

In a nutshell, IT/cybersecurity auditing, from its first phase of engagement through its last one, the issuance of the cybersecurity audit report, provides significantly crucial functions, such as (a) problems and defaults spotting, mitigation and reporting, (b) compliance checking and achieving assurance and promulgation, (c) data integrity and privacy promotion and protection, (d) operational capacities assessment and assuring, (e) internal controls effectiveness evaluation, (f) examination and monitoring upon financial and operational adequacy and appropriateness of internal controls, (g) business-wide risk management, (h) positive change and best practices adoption facilitation, and a great variety of other functions, that assist entities and their management to achieve their mission and objectives.

The final conclusion we would like to make as it concerns the necessity of inclusion of cybersecurity and cyber-preparedness concerns in modern audit programs, procedures, regardless if they are provided by internal and/or external auditors, evolution of the profession and enrichment of the audit practice and science, is that the cybersecurity aspect is not only remarkable important and demanding to be incorporated in audit processes, but also shapes and transforms the general financial audit reporting, so as in the near future we might not discuss about the incorporation of cybersecurity audit part to the main general financial audit program, but the reverse situation, the inclusion of financial audit processes to the overall cybersecurity audit program, because as much digitalized the modern economic, social and even political environments are becoming, the more necessary and pivot will be first to secure the integrity, operability and effectiveness of NHS systems and (perhaps) then examine the financial performance of them.

V I I] B I B L I O G R A P H Y

I] BOOKS

Αποστόλου Απόστολος Κ. (2015), *Ανάλυση Λογιστικών και Χρηματοοικονομικών Καταστάσεων (Analysis of Accounting and Financial Statements)*, Association of Hellenic Academic Libraries.

Bateson Gregory (1972), *Steps to an Ecology of Mind*, Paladin Publishing, London.

Gordo-López Ángel J. & Parker Ian (editors) (2008 for Greece-1999 first edition in English for Macmillan Press LTD) *Κυβερνοψυχολογία (Cyberpsychology)*, Published by Εκδόσεις Παπαζήση (Papazisi Publishing Company), Αθήνα (Athens).

Bradley Gunilla (2017), *The Good ICT Society: From Theory to Actions*, Routledge Publishing, London and New York.

Glenny Misha (2012 for Greek edition, 2011 the original), *DarkMarket: CyberThieves, CyberCops and You*, Papiros Publishing, Athens.

Konstantinos Karamanis (Κωνσταντίνος Καραμάνης) (2008–1st Greek edition), *Σύγχρονη Ελεγκτική: Θεωρία και Πρακτική Σύμφωνα με τα Διεθνή Ελεγκτικά Πρότυπα (Modern Auditing: Theory and Practice according to International Auditing Standards)*, Εκδόσεις ΟΠΑ, Αθήνα.

Κυριαζόγλου Ιωάννης (2001), *Έλεγχος Συστημάτων Πληροφορικής, EDP/IT Auditing*, Εκδόσεις Anubis, Αθήνα.

Λάιος Λάμπρος (2001), *Διοίκηση Εφοδιασμού (Supply Chain Management)*, Εκδόσεις HUMANTEC, Πειραιάς.

Νεγκάκης Χρήστος Ι. & Ταχυνάκης Παναγιώτης Δ. (2017), *Ελεγκτική- Εσωτερικός Έλεγχος: Θεωρία και Εφαρμογές (Auditing – Internal Auditing: Theory and Applications)*, Εκδόσεις Αειφόρος Λογιστική Μονοπρόσωπη ΙΚΕ, Θεσσαλονίκη.

Weiner Norbert (1948 & 1961), *Cybernetics or Control and Communication in the Animal and the Machine*, MIT Press, 2nd edition, Cambridge.

Weiner Norbert (1954), *The Human Use of Human Beings: Cybernetics and Society*, Anchor Publishing, New York.

II] WEBSITES

ACCA Global (09/01/2019), *Agile audit of agile projects*, <https://www.accaglobal.com/gb/en/member/discover/cpd-articles/audit-assurance/agile-audit-of-agile-projects.html> (last retrieved 25/06/2019).

Action Fraud (2019), *What is Action Fraud?*, <https://www.actionfraud.police.uk/what-is-action-fraud> (last retrieved 25/06/2019).

Action Fraud (2019), *Who reports fraud to us*, <https://www.actionfraud.police.uk/who-reports-fraud-to-us> (last retrieved 25/06/2019).

AICPA (2019), *About the AICPA*, <https://www.aicpa.org/about.html> (last retrieved 25/06/2019).

AICPA (2019), *SOC for Service Organizations: Information for CPAs*, <https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/cpas.html> (last retrieved 25/06/2019).

AICPA (26/04/2017), *AICPA Unveils Cybersecurity Risk Management Reporting Framework*, <https://www.aicpa.org/press/pressreleases/2017/aicpa-unveils-cybersecurity-risk-management-reporting-framework.html> (last retrieved 25/06/2019).

AICPA (2018), *Cybersecurity risk management reporting fact sheet*, <https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/cybersecurity-fact-sheet.pdf> (last retrieved 25/06/2019).

AICPA (2019), *Exploring Cybersecurity*, <https://www.aicpa.org/interestareas/privatecompanies/practicesection/qualityservicesdelivery/exploring-cybersecurity.html> (last retrieved 25/06/2019).

AICPA (May 2017), *CGMA Cybersecurity Risk Management Tool*, <https://www.cgma.org/content/dam/cgma/resources/tools/downloadabledocuments/cgma-cybersecurity-tool.pdf> (last retrieved 25/06/2019).

AICPA (2019), *About the Cybersecurity Practical Applications Certificate Program*, <https://certificates.aicpastore.com/certificates/cybersecurity-practical-applications> (last retrieved 25/06/2019).

AICPA (2019), *About the Cybersecurity Fundamentals for Finance and Accounting Professionals Certificate Program*, <https://certificates.aicpastore.com/certificates/cybersecurity-fundamentals-finance-accounting-professionals> (last retrieved 25/06/2019).

AICPA (2019), *About the Cybersecurity Advisory Services Certificate Program*, <https://certificates.aicpastore.com/certificates/cybersecurity-advisory-services> (last retrieved 25/06/2019).

AICPA (2019), *About the SOC for Cybersecurity Certificate Program*, <https://certificates.aicpastore.com/certificates/soc-for-cybersecurity> (last retrieved 25/06/2019).

AICPA (2019), *Credentials: CITP Overview*, <https://www.aicpa.org/membership/join/credentials.html?tab-1=4> (last retrieved 25/06/2019).

AICPA (2019), *Cybersecurity Resources for CPAs Providing Advisory Services*, <https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/cybersecurity-resources-for-cpas-providing-advisory-services.html> (last retrieved 25/06/2019).

AICPA (2019), *SOC for Cybersecurity: Information for CPAs*, <https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/cybersecurityforcpas.html> (last retrieved 25/06/2019).

AICPA, (29/04/2019), *The audit risk model: your first step in risk assessment*, <https://blog.aicpa.org/2019/04/the-audit-risk-model-your-first-step-in-risk-assessment.html#sthash.0WWnE3fn.dpbs> (last retrieved 25/06/2019).

Appelbaum Deniz and Smith Sean Stein(2018) *ICYMI: Blockchain Basics and Hands-on Guidance: Taking the Next Step toward Implementation and Adoption*, CPA Journal, Issue June 2018, <https://www.cpajournal.com/2019/06/27/icymi-blockchain-basics-and-hands-on-guidance/> (last retrieved 25/06/2019).

Axelos (2019), *What is ITIL?*, <https://www.axelos.com/best-practice-solutions/itil/what-is-itil> (last retrieved 25/06/2019).

Bank of England's Prudential Regulatory Authority (2019), *Rulebook*, <http://www.prarulebook.co.uk> (last retrieved 25/06/2019).

BBC (29/12/2017), *Exmo Bitcoin exchange manager freed by kidnappers*, <https://www.bbc.com/news/business-42518235> (last retrieved 25/06/2019).

Bragg Steve (29/05/2019), *Substantive testing*, Accounting Tools, <https://www.accountingtools.com/articles/what-is-substantive-testing.html> (last retrieved 25/06/2019).

Blankespoor Elizabeth, Miller Gregory S., and White Hal D. (January 2014), *The Role of Dissemination in Market Liquidity: Evidence from Firms' Use of Twitter*, The Accounting Review (2018) by American Accounting Association, Volume 89, Issue 1, Pages 79–112, <https://aaapubs.org/doi/abs/10.2308/accr-50576> (last retrieved 25/06/2019).

Boillet Jeanne (01/04/2018), *Why AI is both a risk and a way to manage risk*, https://www.ey.com/en_us/assurance/why-ai-is-both-a-risk-and-a-way-to-manage-risk (last retrieved 25/06/2019). Prof.

Boillet Jeanne (28/09/2018), *How can you build trust when emerging technologies bring new risks?*, https://www.ey.com/en_us/digital/how-can-you-build-trust-when-emerging-technologies-bring-new-risks (last retrieved 25/06/2019).

Brennan Bill, Baccala Mike, and Flynn Mike (02/02/2017), *Artificial Intelligence Comes to Financial Statement Audits*, CFO online, <https://www.cfo.com/auditing/2017/02/artificial-intelligence-audits/> (last retrieved 25/06/2019).

Cade Nicole L. (July 2018), *Corporate Social Media: How Two-way Disclosure Channels Influence Investors*, Accounting, Organizations and Society Journal, Volumes 68-79, Pages 63-79, <https://www.sciencedirect.com/science/article/abs/pii/S0361368218300837> (last retrieved 25/06/2019).

C.E. Shannon (1948), *A Mathematical Theory of Communication*, The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, October, 1948, Reprinted with corrections from Harvard,

<http://math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf> (last retrieved 25/06/2019).

CAQ (2019), *Our Mission: Serving Investors, Public Company Auditors & the Markets*, <https://www.thecaq.org/about-us/> (last retrieved 25/06/2019).

CAQ (21/03/2014), *CAQ Member Alert No 2014-3: Cybersecurity and the External Audit*, https://www.thecaq.org/wp-content/uploads/2019/03/caqalert_2014_03.pdf (last retrieved 25/06/2019).

CAQ (May 2017), *CPA's Role in Addressing Cybersecurity Risk: How the Auditing Profession Promotes Cybersecurity Resilience*, https://www.thecaq.org/wp-content/uploads/2019/03/caq_cpa_role_in_addressing_cybersecurity_risk_2017-05.pdf (last retrieved 25/06/2019).

CAQ (April 2018), *Cybersecurity Risk Management Oversight: A Tool for Board Members*, https://www.thecaq.org/wp-content/uploads/2019/03/caq_cybersecurity_risk_management_oversight_tool_2018-04.pdf (last retrieved 25/06/2019).

CAQ (December 2018), *Emerging Technologies: An Oversight Tool for Audit Committees*, https://www.thecaq.org/wp-content/uploads/2019/03/caq_emerging_technologies_oversight_tool_2018-12.pdf (last retrieved 25/06/2019).

CAQ (May 2019), *Emerging Technologies, Risk, and the Auditor's Focus: A Resource for Auditors, Audit Committees, and Management*, https://www.thecaq.org/wp-content/uploads/2019/05/caq_emerging_technologies_risk_auditors_focus_2019-05.pdf (last retrieved 25/06/2019).

Chartered Institute of Internal Auditors (08/10/2014), *Risk Based Internal Auditing*, <https://global.theiia.org/standards-guidance/topics/Documents/201501GuidetoRBIA.pdf> (last retrieved 25/06/2019).

CISA (06/07/2009), *Protected Critical Infrastructure Information (PCII) Program*, <https://www.cisa.gov/pcii-program> (last retrieved 25/06/2019).

CISA (23/07/2007), *Cybersecurity Division Mission And Vision*, <https://www.cisa.gov/cybersecurity-division> (last retrieved 25/06/2019).

CISA (07/12/2012 original edition, 06/03/2019 revised), *Suspicious Activity Reporting Tool*, <https://www.cisa.gov/suspicious-activity-reporting-tool> (last retrieved 25/06/2019).

CISA (2019), *What Does CISA Do?*, <https://www.cisa.gov> (last retrieved 25/06/2019).

CISA (08/09/2015), *Securing Your Web Browser*, <https://www.us-cert.gov/publications/securing-your-web-browser> (last retrieved 25/06/2019).

CISA, (06/05/2014 original, 06/03/2019 revised), *Infrastructure Protection Gateway*, <https://www.cisa.gov/ip-gateway> (last retrieved 25/06/2019).

CISA (2019), *Downloading and Installing CSET*, <https://www.us-cert.gov/ics/Downloading-and-Installing-CSET> (last retrieved 25/06/2019).

CISA (2019), *Industrial Control Systems*, <https://www.us-cert.gov/ics> (last retrieved 25/06/2019).

CISA (11/04/2019) (revised), *Security Tip (ST18-004): Protecting Against Malicious Code*, <https://www.us-cert.gov/ncas/tips/ST18-271> (last retrieved 25/06/2019).

CISA (04/11/2009), *Security Tip (ST04-015): Understanding Denial-of-Service Attacks*, <https://www.us-cert.gov/ncas/tips/ST04-015> (last retrieved 25/06/2019).

CISA, 04/11/2013, *Security Tip (ST13-003) Handling Destructive Malware*, <https://www.us-cert.gov/ncas/tips/ST13-003> (last retrieved 25/06/2019).

CISA, 08/09/2015, *Securing Your Web Browser*, <https://www.us-cert.gov/publications/securing-your-web-browser> (last retrieved 25/06/2019).

CISA, 04/11/2009, *Security Tip (ST04-015): Understanding Denial-of-Service Attacks*, <https://www.us-cert.gov/ncas/tips/ST04-015> (last retrieved 25/06/2019).

CISA, 21/11/2018 (revised), *Security Tip (ST05-019): Preventing and Responding to Identity Theft*, <https://www.us-cert.gov/ncas/tips/ST05-019> (last retrieved 25/06/2019).

Congress (2002), *Public Law No: 107-204 (07/30/2002)- 107th Congress (2001-2002): Sarbanes-Oxley Act Of 2002*, <https://www.congress.gov/bill/107th-congress/house-bill/3763/text> (last retrieved 25/06/2019).

Congress (2002), *Public Law No: 107-204 (07/30/2002)- 107th Congress (2001-2002): Sarbanes-Oxley Act Of 2002*, <https://www.congress.gov/bill/107th-congress/house-bill/3763/text> (last retrieved 25/06/2019).

Congress (26/04/2016), *Text: H.R.5069 — 114th Congress (2015-2016): Cybersecurity Systems and Risks Reporting Act*, <https://www.congress.gov/bill/114th-congress/house-bill/5069/text> (last retrieved 25/06/2019).

Congress (24/06/2014), *Text: S.2521 — 113th Congress (2013-2014), Public Law No: 113-283 (12/18/2014): Federal Information Security Modernization Act of 2014*, <https://www.congress.gov/bill/113th-congress/senate-bill/2521> (last retrieved 25/06/2019).

Congress (14/05/2008), *H.R.6060 — 110th Congress (2007-2008): Identity Theft Enforcement and Restitution Act of 2008*, <https://www.congress.gov/bill/110th-congress/house-bill/6060> (last retrieved 25/06/2019).

Congress (03/10/1986), *TEXT H.R.4718 — 99th Congress (1985-1986): H.R.4718 - Computer Fraud and Abuse Act of 1986*, <https://www.congress.gov/bill/99th-congress/house-bill/4718> (last retrieved 25/06/2019).

Congress (30/06/2016), *TEXT S.337 — 114th Congress (2015-2016): Public Law No: 114-185 (06/30/2016), FOIA Improvement Act of 2016*, <https://www.congress.gov/bill/114th-congress/senate-bill/337/text> (last retrieved 25/06/2019).

Congress (30/06/2016), *TEXT: H.R.16373 — 93rd Congress (1973-1974): Privacy Act*, <https://www.congress.gov/bill/93rd-congress/house-bill/16373> (last retrieved 25/06/2019).

Congress (01/10/2015), *Text: H.R.3664 - Promoting Good Cyber Hygiene Act of 2015*, <https://www.congress.gov/bill/114th-congress/house-bill/3664> (last retrieved 25/06/2019).

Congress (21/09/2016), *TEXT H.R.6066 — 114th Congress (2015-2016): H.R.6066 - Cybersecurity Responsibility and Accountability Act of 2016*, <https://www.congress.gov/bill/114th-congress/house-bill/6066> (last retrieved 25/06/2019).

Congress (06/06/2016), *TEXT S.3024 — 114th Congress (2015-2016): Small Business Cyber Security Improvements Act of 2016*, <https://www.congress.gov/bill/114th-congress/senate-bill/3024> (last retrieved 25/06/2019).

Congress (15/03/2016), *Text: H.R.4743 — 114th Congress (2015-2016): National Cybersecurity Preparedness Consortium Act of 2016*, <https://www.congress.gov/bill/114th-congress/house-bill/4743> (last retrieved 25/06/2019).

Congress (10/02/2016), *Text: H.R.4528 — 114th Congress (2015-2016): ENCRYPT Act of 2016*, <https://www.congress.gov/bill/114th-congress/house-bill/4528> (last retrieved 25/06/2019).

Congress (14/09/2016), *Text: H.R.6032 — 114th Congress (2015-2016): Data Breach Insurance Act*, <https://www.congress.gov/bill/114th-congress/house-bill/6032> (last retrieved 25/06/2019).

Congress (07/06/2016), *Text: H.R.5390 — 114th Congress (2015-2016): Cybersecurity and Infrastructure Protection Agency Act of 2016*, <https://www.congress.gov/bill/114th-congress/house-bill/5390> (last retrieved 25/06/2019).

Congress (27/10/2015), *Text: S.754 — 114th Congress (2015-2016): To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes*, <https://www.congress.gov/bill/114th-congress/senate-bill/754> (last retrieved 25/06/2019).

Congress (14/09/2016), *Text: H.R.5823 — 115th Congress (2017-2018): Secure Data Act of 2018*, <https://www.congress.gov/bill/115th-congress/house-bill/5823> (last retrieved 25/06/2019).

Congress (26/02/2018), *Text: H.R.4943 — 115th Congress (2017-2018): Clarifying Lawful Overseas Use of Data Act or the CLOUD Act*, <https://www.congress.gov/bill/115th-congress/house-bill/4943/text> (last retrieved 25/06/2019).

Congress (11/03/2019), *Text: S.734 — 116th Congress (2019-2020): Internet of Things Cybersecurity Improvement Act of 2019*, <https://www.congress.gov/bill/116th-congress/senate-bill/734> (last retrieved 25/06/2019).

Congress (31/01/2019), *Text: S.315 — 116th Congress (2019-2020): DHS Cyber Hunt and Incident Response Teams Act of 2019*, <https://www.congress.gov/bill/116th-congress/senate-bill/315/text> (last retrieved 25/06/2019).

Cooke Ian (2017), *IS Audit Basics: Audit Programs*, ISACA Journal, Issue 2017, Volume 4, <https://www.isaca.org/resources/isaca-journal/issues/2017/volume-4/is-audit-basics-audit-programs> (last retrieved 25/06/2019).

Cooke Ian and Raghu R. V. (01/09/2018), *IS Audit Basics: Auditing the IoT*, ISACA Journal, Issue 2018: Volume 5, <https://www.isaca.org/resources/isaca-journal/issues/2018/volume-5/is-audit-basics-auditing-the-iot> (last retrieved 25/06/2019).

COSO (May 2013), *Internal Control—Integrated Framework: Executive Summary*, <https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf> (last retrieved 25/06/2019).

Council of Economic Advisers of the Executive Office of the President of United States (February 2018) *The Cost of Malicious Cyber Activity to the U.S. Economy*, <https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf> (last retrieved 25/06/2019).

Council of Europe (2019), *Details of Treaty No.185: Convention on Cybercrime of 2001*, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185> (last retrieved 25/06/2019).

Dr. Curtis Patchin & Mark Carey (October 2012), *Risk Assessment in Practice*, Committee of Sponsoring Organizations of the Treadway Commission (COSO) and Deloitte & Touche LLP, <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dttl-grc-riskassessmentinpractice.pdf> (last retrieved 25/06/2019).

Cyber Essentials, 2019, *Cyber Essentials*, <https://www.cyberessentials.nesc.gov.uk> (last retrieved 25/06/2019).

Cybersecurity Forensic Analyst (CSFA) Certification, <http://www.cybersecurityforensicanalyst.com/> (last retrieved 25/06/2019).

Durkota Michael D. and Dormann Will, 2008, *Recovering from a Trojan Horse or Virus*, Carnegie Mellon University, <https://www.us-cert.gov/sites/default/files/publications/trojan-recovery.pdf> (last retrieved 25/06/2019).

Deloitte (July 2016), *RBI Guidelines for Cyber Security Framework*, <https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-risk-rbi-guidelines-for-cyber-security-framework-noexp.pdf> (last retrieved 25/06/2019).

Deloitte (2013), *The digital grapevine: Social media and the role of Internal Audit*, <https://www2.deloitte.com/global/en/pages/risk/articles/social-media-internal-audit.html> (last retrieved 25/06/2019).

Deloitte & Touche LLP and Forbes Insights (2012), *Aftershock Adjusting to the new world of risk management*, https://deloitte.wsj.com/cfo/files/2012/10/Aftershock_Adjusting-to-the-new-world-of-risk-management.pdf (last retrieved 25/06/2019).

Deloitte (05/10/2018), *Deloitte Wins 2018 'Audit Innovation of the Year' at The Digital Accountancy Forum & Awards: Two-time award winner Deloitte recognized for its Audit-Transforming "Cortex" data platform*, <https://www.prnewswire.com/news-releases/deloitte-wins-2018-audit-innovation-of-the-year-at-the-digital-accountancy-forum--awards-300724977.html>

Deloitte, *What is a Blockchain?*, <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-what-is-blockchain-2016.pdf>, (last retrieved 25/06/2019).

Deloitte (2019), *Deloitte wins 'Audit Innovation of the Year' at 2015 International Accounting Bulletin awards*, <https://www2.deloitte.com/ch/en/pages/audit/articles/deloitte-wins-iab-audit-innovation-award.html> (last retrieved 25/06/2019).

Dickey Gabe, Blanke Sandra and Seaton Lloyd (June 2019), *Machine Learning in Auditing: Current and Future Applications*, <https://www.cpajournal.com/2019/06/19/machine-learning-in-auditing/> (last retrieved 25/06/2019).

Doyle Charles (15/10/2014), *Congress Research Service: Cybercrime: A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Laws*, <https://fas.org/sgp/crs/misc/RS20830.pdf> (last retrieved 25/06/2019).

Durkota Michael D. and Dormann Will, 2008, *Recovering from a Trojan Horse or Virus*, Carnegie Mellon University, <https://www.us-cert.gov/sites/default/files/publications/trojan-recovery.pdf> (last retrieved 25/06/2019).

Eaglesham Jean and Vigna Paul (28/022/2018), *Cryptocurrency Firms Targeted in SEC Probe: Regulator issues subpoenas to parties engaged in booming market for initial coin offerings*, Wall Street Journal, <https://www.wsj.com/articles/sec-launches-cryptocurrency-probe-1519856266> (last retrieved 25/06/2019).

Encyclopedia Britannica (2019), *Artificial intelligence*, <https://www.britannica.com/technology/artificial-intelligence/Reasoning> (last retrieved 25/06/2019).

Ernst & Young LLP (2018), *Cryptocurrencies and cryptoassets: Managing the new asset class*, [https://www.ey.com/Publication/vwLUAssets/ey-cryptocurrencies-and-cryptoassets-managing-the-new-asset-class/\\$File/ey-cryptocurrencies-and-cryptoassets-managing-the-new-asset-class.pdf](https://www.ey.com/Publication/vwLUAssets/ey-cryptocurrencies-and-cryptoassets-managing-the-new-asset-class/$File/ey-cryptocurrencies-and-cryptoassets-managing-the-new-asset-class.pdf) (last retrieved 25/06/2019).

Ethereum (2019), *What is Ethereum?*, <https://ethereum.org/what-is-ethereum/> (last retrieved 25/06/2019).

European Commission (2018), *COM 109/2 Communication From The Commission To The European Parliament, The Council, The European Central Bank, The European Economic And Social Committee And The Committee Of The Regions: FinTech Action plan: For a more competitive and innovative European financial sector*, https://ec.europa.eu/info/sites/info/files/180308-action-plan-fintech_en.pdf (last retrieved 25/06/2019).

European Commission (17/09/2017), *State of the Union 2017: The Commission scales up its response to cyber-attacks*, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_3194 (last retrieved 25/06/2019).

European Commission (2019), *Auditing of companies' financial statements: The EU provides regulations on statutory auditing to improve the integrity of financial statements*, https://ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/auditing-companies-financial-statements_en (last retrieved 25/06/2019).

European Court of Auditors (2019), *Audit Methodology*, <https://www.eca.europa.eu/en/Pages/AuditMethodology.aspx> (last retrieved 25/06/2019).

EUROPOL (2019), *EUROPEAN CYBERCRIME CENTRE - EC3: Combating crime in a digital age*, <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3> (last retrieved 25/06/2019).

European Securities and Market Authority –ESMA (09/01/2019), *ESMA50-157-1391: Advice on Initial Coin Offerings and Crypto-Assets*, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf (last retrieved 25/06/2019).

FCA (2019), *FCA Handbook*, <https://www.handbook.fca.org.uk/handbook> (last retrieved 25/06/2019).

Financial Conduct Authority (27/02/2019), *Initial Coin Offerings*, <https://www.fca.org.uk/news/statements/initial-coin-offerings> (last retrieved 25/06/2019).

FINRA (31/03/2017), *Report on Distributed Ledger Technology: Implications of Blockchain for the Securities Industry*, <https://www.finra.org/rules-guidance/guidance/faqs/report-distributed-ledger-technology-implications-blockchain-securities-industry> , (last retrieved 25/06/2019).

FOIA.GOV (2019), *Freedom of Information Act Statute*, <https://www.foia.gov/foia-statute.html> (last retrieved 25/06/2019).

Gargano Antonello (30/09/2011), *Managing Privacy Risk in a Social Media-Driven Society*, Protiviti, Page 19-20, http://www.aiea.it/sites/default/files/attivita/sds/roma_30_settembre_2011_gargano.pdf (last retrieved 25/06/2019).

Gelinne John, Fancher J. Donald and Mossburg Emily (25/07/2016), *The hidden costs of an IP breach: Cyber theft and the loss of intellectual property*, Deloitte Review Issue 19, <https://www2.deloitte.com/us/en/insights/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html> (last retrieved 25/06/2019).

Ghost Shona (6/11/2017), *Estonia has frozen its popular e-residency ID cards because of a massive security flaw*", Business Insider, <https://www.insider.com/estonia-freeze-e-residency-id-cards-id-theft-2017-11> (last retrieved 25/06/2019).

GOV.UK (2019), *Data Protection*, <https://www.gov.uk/data-protection> (last retrieved 25/06/2019).

GOV.UK, 16/01/2018, *Guidance - Cyber Essentials Scheme: overview*, <https://www.gov.uk/government/publications/cyber-essentials-scheme-overview> (last retrieved 25/06/2019).

Holland Paul, Rae Shamus and Taylor Paul (2018), *Why AI must be included in audits*, KPMG, <https://assets.kpmg/content/dam/kpmg/uk/pdf/2018/06/why-ai-must-be-included-in-audits.PDF> (last retrieved 25/06/2019).

Houben Robby and Snyers Alexander (June 2018), *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion*, EU European Parliament, <https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf> (last retrieved 25/06/2019).

Iansiti Marco and Lakhani Karim R. (2017), *The Truth About Blockchain*, Harvard Business Review: January-February 2017 Issue, <https://hbr.org/2017/01/the-truth-about-blockchain> (last retrieved 25/06/2019).

IFAC (2010), *International Standard on Quality Control (ISQC) 1 on Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance and Related Services Engagements*, <https://www.ifac.org/system/files/downloads/a007-2010-iaasb-handbook-isqc-1.pdf> (last retrieved 25/06/2019).

IFAC (2010), *International Standard On Auditing 200 Overall Objectives Of The Independent Auditor And The Conduct Of An Audit In Accordance With International Standards On Auditing*, <https://www.ifac.org/system/files/downloads/a008-2010-iaasb-handbook-isa-200.pdf> (last retrieved 25/06/2019).

IFAC (2010), *International Standard On Auditing 210 Agreeing The Terms Of Audit Engagements*, <https://www.ifac.org/system/files/downloads/a009-2010-iaasb-handbook-isa-210.pdf> (last retrieved 25/06/2019).

IFAC (2010), *International Standard On Auditing 220 Quality Control for an Audit of Financial Statements*, <https://www.ifac.org/system/files/downloads/a010-2010-iaasb-handbook-isa-220.pdf> (last retrieved 25/06/2019).

IFAC (2010), *International Standard On Auditing 230 Audit Documentation*, <https://www.ifac.org/system/files/downloads/a011-2010-iaasb-handbook-isa-230.pdf> (last retrieved 25/06/2019).

IFAC (2010), *International Standard On Auditing 240 The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements*, <https://www.ifac.org/system/files/downloads/a012-2010-iaasb-handbook-isa-240.pdf> (last retrieved 25/06/2019).

IFAC (2010), *International Standard On Auditing 250 on Consideration of Laws and Regulations in an Audit of Financial Statements*, <https://www.ifac.org/system/files/downloads/a013-2010-iaasb-handbook-isa-250.pdf> (last retrieved 25/06/2019).

IFAC (2010), *International Standard On Auditing 260 Communication with Those Charged with Governance*, <https://www.ifac.org/system/files/downloads/a014-2010-iaasb-handbook-isa-260.pdf> (last retrieved 25/06/2019).

IFAC (2010), *International Standard On Auditing ISA 265 on Communicating Deficiencies in Internal Control to Those Charged with Governance and Management govern the procedure of this appointment*, <https://www.ifac.org/system/files/downloads/a015-2010-iaasb-handbook-isa-265.pdf> (last retrieved 25/06/2019).

IFAC (2010), *International Standard On Auditing 315 on Understanding the Entity and its Environment and Assessing the Risks of Material Misstatement* <https://www.ifac.org/system/files/downloads/a017-2010-iaasb-handbook-isa-315.pdf> (last retrieved 25/06/2019).

IFAC (2010), *International Standard on Auditing (ISA) 500 on Audit Evidence*, <https://www.ifac.org/system/files/downloads/a022-2010-iaasb-handbook-isa-500.pdf> (last retrieved 25/06/2019).

IFAC (2010), *International Standard on Auditing (ISA) 501 on Audit Evidence—Specific Considerations for Selected Items*, <https://www.ifac.org/system/files/downloads/a023-2010-iaasb-handbook-isa-501.pdf> (last retrieved 25/06/2019).

IFAC (2010), *International Standard on Auditing (ISA) 530 on Audit Sampling*, <https://www.ifac.org/system/files/downloads/a027-2010-iaasb-handbook-isa-530.pdf> (last retrieved 25/06/2019).

IFAC (2010), *International Standard on Auditing (ISA) 700 on Forming an Opinion and Reporting on Financial Statements*, <https://www.ifac.org/system/files/downloads/a036-2010-iaasb-handbook-isa-700.pdf> (last retrieved 25/06/2019).

IFAC (2010), *International Standard on Auditing (ISA) 705 on Modifications to the Opinion in the Independent Auditor's Report*, <https://www.ifac.org/system/files/downloads/a037-2010-iaasb-handbook-isa-705.pdf> (last retrieved 25/06/2019).

IFAC (2010), *International Standard on Auditing (ISA) 706 on Emphasis of Matter Paragraphs and Other Matter Paragraphs in the Independent Auditor's Report*, <https://www.ifac.org/system/files/downloads/a038-2010-iaasb-handbook-isa-706.pdf> (last retrieved 25/06/2019).

IFAC (2010), *International Standard on Auditing (ISA) 720 on The Auditor's Responsibilities Relating to Other Information in Documents Containing Audited Financial Statements*, <https://www.ifac.org/system/files/downloads/a040-2010-iaasb-handbook-isa-720.pdf> (last retrieved 25/06/2019).

IFRS Foundation (2019), *IAS 38 Intangible Assets*, <https://www.ifrs.org/issued-standards/list-of-standards/ias-38-intangible-assets/> (last retrieved 25/06/2019).

IGI Global (2019), *What is Cyber Preparedness*, <https://www.igi-global.com/dictionary/cyber-preparedness/51238> (last retrieved 25/06/2019).

Information Commissioner's Office (2019), *Who we are?*, <https://ico.org.uk/about-the-ico/who-we-are/> (last retrieved 25/06/2019).

Investopedia (2019), *Blockchain explained*, <https://www.investopedia.com/terms/b/blockchain.asp> (last retrieved 25/06/2019).

Institute of Internal Auditors (March 2012-Second Edition), *Global Technology Audit Guide (GTAG) 1: Information Technology Risk and Controls*, https://chapters.theiia.org/montreal/ChapterDocuments/GTAG%201%20-%20Information%20technology%20controls_2nd%20ed.pdf (last retrieved 25/06/2019).

IRS, 2019, *Identity Theft Central*, <https://www.irs.gov/identity-theft-central> (last retrieved 25/06/2019).

IRS (2019), *Virtual Currencies*, <https://www.irs.gov/businesses/small-businesses-self-employed/virtual-currencies> (last retrieved 25/06/2019).

ISA (2019), *Mission and Goals*, <https://isalliance.org/about-isa/mission-and-goals/> (last retrieved 25/06/2019).

ISACA (2019), *COBIT 2019 Foundation Certificate Program*, <https://www.isaca.org/credentialing/cobit/cobit-foundation> (last retrieved 25/06/2019).

ISACA (2019), *COBIT 2019 Design and Implementation Certificate Program*, <https://www.isaca.org/credentialing/cobit/cobit-design-and-implementation> (last retrieved 25/06/2019).

ISACA (2019), *Implementing the NIST Cybersecurity Framework Using COBIT 2019 Training and Certificate Program*, <https://www.isaca.org/credentialing/cobit/implementing-the-nist-cybersecurity-framework--using-cobit-2019> (last retrieved 25/06/2019).

ISACA (2019), *Code of Professional Ethics*, <https://www.isaca.org/credentialing/code-of-professional-ethics> (last retrieved 25/06/2019).

ISACA (01/05/2016), *Standards, Guidelines, Tools and Techniques*, ISACA Journal, Issue 2016, Volume 3, <https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/standards-guidelines-tools-and-techniques> (last retrieved 25/06/2019).

ISACA (2019), *Credentialing: CISA*, <https://www.isaca.org/credentialing/cisa> (last retrieved 25/06/2019).

ISACA (2019), *Credentialing: CRISC*, <https://www.isaca.org/credentialing/crisc> (last retrieved 25/06/2019).

ISACA (2019), *Credentialing: GDEIT*, <https://www.isaca.org/credentialing/cgeit> (last retrieved 25/06/2019).

ISACA (2019), *Credentialing: CDPSE*, <https://www.isaca.org/credentialing/certified-data-privacy-solutions-engineer> (last retrieved 25/06/2019).

ISACA (2019), *Credentialing: Cybersecurity Audit Certificate*, <https://www.isaca.org/credentialing/cybersecurity%20audit%20certificate> (last retrieved 25/06/2019).

- ISACA** (2019), *Credentialing: Certificates*, <https://www.isaca.org/credentialing/cybersecurity> (last retrieved 25/06/2019).
- ISACA** (2019), *Credentialing: CSX-P*, <https://www.isaca.org/credentialing/csx-p> (last retrieved 25/06/2019).
- ISACA** (2019), *Credentialing: CISM*, <https://www.isaca.org/credentialing/cism> (last retrieved 25/06/2019).
- ISACA** (2019), *COBIT 2019 Publications*, <https://www.isaca.org/resources/cobit> (last retrieved 25/06/2019).
- ISO**, *ISO 28000:2007 on Specification for security management systems for the supply chain*, <https://www.iso.org/standard/44641.html> (last retrieved 25/06/2019).
- ISO**, *ISO 19011:2002 Guidelines for quality and/or environmental management systems auditing*, <https://www.iso.org/standard/31169.html> (last retrieved 25/06/2019) & **ISO**, *ISO 19011:2002 Guidelines for auditing management systems*, <https://www.iso.org/standard/50675.html> (last retrieved 25/06/2019) .
- ISO**, *ISO 19011:2018 Guidelines for auditing management systems*, <https://www.iso.org/standard/70017.html> (last retrieved 25/06/2019).
- ISO**, *ISO/IEC 17021-1:2015 Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements* <https://www.iso.org/standard/61651.html> (last retrieved 25/06/2019).
- ISO**, *ISO/IEC 17021-1:2015(EN): Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements*, <https://www.iso.org/obp/ui/#iso:std:iso-iec:17021:-1:ed-1:v1:en> (last retrieved 25/06/2019).
- ISO**, *ISO/IEC JTC 1/SC 27 - Information Security, cybersecurity and privacy protection: About*, <https://www.iso.org/committee/45306.html> (last retrieved 25/06/2019).
- ISO**, *ISO/IEC 27000 family - Information security management systems*, <https://www.iso.org/isoiec-27001-information-security.html> (last retrieved 25/06/2019).
- ISO**, *ISO/IEC 27000:2009 Information technology - Security techniques - Information security management systems - Overview and vocabulary*, <https://www.iso.org/standard/41933.html> (last retrieved 25/06/2019).
- ISO**, *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*, <https://www.iso.org/standard/54534.html> (last retrieved 25/06/2019).
- ISO**, *ISO/IEC 27002:2013 — Information technology — Security techniques — Code of practice for information security controls*, <https://www.iso.org/standard/54533.html> (last retrieved 25/06/2019).
- ISO**, *ISO/IEC 27003:2017 — Information technology — Security techniques — Information security management systems — Guidance*, <https://www.iso.org/standard/63417.html> (last retrieved 25/06/2019).

ISO, ISO/IEC 27004:2016 — *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*, <https://www.iso.org/standard/64120.html> (last retrieved 25/06/2019).

ISO, ISO/IEC 27005:2018 — *Information technology — Security techniques — Information security risk management*, <https://www.iso.org/standard/56742.html> (last retrieved 25/06/2019).

ISO, ISO/IEC 27006:2015 *Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*, <https://www.iso.org/standard/62313.html> (last retrieved 25/06/2019).

ISO, ISO/IEC 27006:2015 (en): *Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*, <https://www.iso.org/obp/ui/#iso:std:iso-iec:27006:ed-3:v1:en> (last retrieved 25/06/2019).

ISO, ISO/IEC 27007:2017 *Information technology — Security techniques — Guidelines for information security management systems auditing*, <https://www.iso.org/standard/67398.html> (last retrieved 25/06/2019).

ISO, ISO/IEC 27008:2019 *Information technology — Security techniques — Guidelines for auditors on information security controls*, <https://www.iso.org/standard/67397.html> (last retrieved 25/06/2019).

ISO, ISO/IEC 27009:2016 — *Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements*, <https://www.iso.org/standard/42508.html> (last retrieved 25/06/2019).

ISO, ISO/IEC 27010:2015 — *Information technology — Security techniques — Information security management for inter-sector and inter-organisational communications*, <https://www.iso.org/standard/68427.html> (last retrieved 25/06/2019).

ISO, ISO/IEC 27011:2016 — *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations*, <https://www.iso.org/standard/64143.html> (last retrieved 25/06/2019).

ISO, ISO/IEC 27017:2015(en) *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*, <https://www.iso.org/standard/43757.html> (last retrieved 25/06/2019).

ISO, ISO/IEC 27043:2015(en) *Information technology — Security techniques — Incident investigation principles and processes*, <https://www.iso.org/standard/44407.html> (last retrieved 25/06/2019).

ISO (2018), ISO/IEC 17024:2012 upon Conformity assessment — *General requirements for bodies operating certification of persons*, <https://www.iso.org/standard/52993.html> (last retrieved 25/06/2019).

Issa Hussein, Sun Ting, and Vasarhelyi Miklos (2016), *Research Ideas for Artificial Intelligence in Auditing, The Formalization of Audit and Workforce*

Supplementation, American Accounting Association: Journal of Emerging Technologies in Accounting, Volume 13, Issue 2, available at <https://meridian.allenpress.com/jeta/article/13/2/1/115980/Research-Ideas-for-Artificial-Intelligence-in> (last retrieved 25/06/2019).

Jung Michael J., Naughton James P. Tahoun Ahmed & Wang Clare (2018), *Do Firms Strategically Disseminate? Evidence from Corporate Use of Social Media*, The Accounting Review (2018) by American Accounting Association, Volume 93, Issue 4, Pages 225–252, <https://meridian.allenpress.com/accounting-review/article-abstract/93/4/225/53582/Do-Firms-Strategically-Disseminate-Evidence-from?redirectedFrom=fulltext> (last retrieved 25/06/2019).

Kaspersky Lab (2019), *What is Cyber-Security?*, <https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security> (last retrieved 25/06/2019).

Kaspersky (2019), *4 Common Cryptocurrency Scams and How to Avoid Them*, <https://www.kaspersky.com/resource-center/definitions/cryptocurrency-scams> (last retrieved 25/06/2019).

Kirwan Grainne and Power Andrew (2012), *The Psychology of Cyber Crime: Concepts and Principals*, IGI Global.

Klous Sander (08/06/2018), *In AI we trust?: Assurance is more important than ever in the age of machines*, KPMG, <https://home.kpmg/xx/en/home/insights/2019/04/in-ai-we-trust.html> (last retrieved 25/06/2019).

Kokina Julia and Davenport Thomas H. (2017), *The Emergence of Artificial Intelligence: How Automation Is Changing Auditing*, American Accounting Association: Journal of Emerging Technologies in Accounting, Volume 14, Issue 1, available at <https://meridian.allenpress.com/jeta/article-abstract/14/1/115/116001/The-Emergence-of-Artificial-Intelligence-How?redirectedFrom=fulltext> (last retrieved 25/06/2019).

Konrad Martin (2018), *Embracing Compliance for the Sake of Cybersecurity: Looking Beyond Legal Requirements to Find Best Practices*, CPA Journal, <https://www.cpajournal.com/2018/07/06/embracing-compliance-for-the-sake-of-cybersecurity/> (last retrieved 25/06/2019).

KPMG (2016), *Securing Industrial Control Systems*, <https://assets.kpmg/content/dam/kpmg/ca/pdf/2016/11/ca-kpmg-cyber-securing-industrial-control-systems.pdf> (last retrieved 25/06/2019).

KPMG International (June 2018), *KPMG Clara: A smart audit platform*, <https://assets.kpmg/content/dam/kpmg/xx/pdf/2017/05/kpmg-clara-a-smart-audit-platform.pdf> (last retrieved 25/06/2019).

LAW INSIDER (2019), *Definition of Data asset*, <https://www.lawinsider.com/dictionary/data-asset> (last retrieved 25/06/2019).

Lee Lian Fen, Hutton Amy P., and Shu Susan (May 2015), *The Role of Social Media in the Capital Market: Evidence from Consumer Product Recalls*, Journal of Accounting Research, Volume 53, Issue 2, Pages 367-404,

<https://onlinelibrary.wiley.com/doi/abs/10.1111/1475-679X.12074> (last retrieved 25/06/2019).

Loop Paula (13/09/2018), *Blockchain: What Boards Need to Know*, National Association of Corporate Directors (NACD), <https://blog.nacdonline.org/posts/blockchain-boards-need-to-know> (last retrieved 25/06/2019).

Luxembourg Bankers Association (ABBL) (2019), *CEO Fraud*, <https://www.abbl.lu/topic/ceo-fraud/> (last retrieved 25/06/2019).

Luxembourg Bankers Association (ABBL) (2019), *Phishing/Smishing/Vishing*, <https://www.abbl.lu/topic/phishing-smishing-vishing/> (last retrieved 25/06/2019).

Luxembourg Bankers Association (ABBL) (2019), *Phishing/Smishing/Vishing*, <https://www.abbl.lu/topic/phishing-smishing-vishing/> (last retrieved 25/06/2019).

Maguire Eamon, Nagaraj Kiran, Wyner Sam and Goens LaDarius (2017), *Securing the Chain*, KPMG International, <https://advisory.kpmg.us/content/dam/advisory/training/pdf/securing-the-chain.pdf> (last retrieved 25/06/2019).

Mandjee Tara (2015), *Bitcoin, its Legal Classification and its Regulatory Framework*, Journal of Business & Securities Law, Volume 15, Issue 2, Page 165, Published by Digital Commons at Michigan State University College of Law, 2016, <https://digitalcommons.law.msu.edu/jbsl/vol15/iss2/4/> (last retrieved 25/06/2019).

McAfee, 23/07/2013, *What is a Keylogger?*, <https://www.mcafee.com/blogs/consumer/family-safety/what-is-a-keylogger> (last retrieved 25/06/2019).

McAfee and Center for Strategic International Studies (CSIS) (February 2018), *Economic Impact of Cybercrime— No Slowing Down*, https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email (last retrieved 25/06/2019).

McDowell Midi (for CISA), 11/10/2010, *Security Tip (ST10-001) Recognizing Fake Antiviruses*, <https://www.us-cert.gov/ncas/tips/ST10-001> (last retrieved 25/06/2019).

McDowell Midi (for CISA) (19/03/2009), *Security Tip (ST05-006) Recovering from Viruses, Worms, and Trojan Horses*, <https://www.us-cert.gov/ncas/tips/ST05-006> (last retrieved 25/06/2019).

McDowell Midi (for CISA) (11/10/2010), *Security Tip (ST10-001) Recognizing Fake Antiviruses*, <https://www.us-cert.gov/ncas/tips/ST10-001> (last retrieved 25/06/2019).

McDowell Midi, 24/09/2011, *Understanding Hidden Threats: Rootkits and Botnets*, <https://www.us-cert.gov/ncas/tips/ST06-001> (last retrieved 25/06/2019).

Murray Joe (June 2019), *ICYMI : The Coming World of Blockchain: A Primer for Accountants and Auditors*, CPA Journal, Issue June 2018,

<https://www.cpajournal.com/2019/06/20/icymi-the-coming-world-of-blockchain/> (last retrieved 25/06/2019).

National Cyber Security Centre, 2019, *About Cyber Essentials*, <https://www.ncsc.gov.uk/cyberessentials/overview> (last retrieved 25/06/2019).

Newhouse William, Keith Stephanie, Scribner Benjamin, Witte Greg (08/2017), *NIST Special Publication 800-181: National Initiative For Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf> (last retrieved 25/06/2019).

Newman Craig A. (23/01/2019), *Lessons for Corporate Boardrooms From Yahoo's Cybersecurity Settlement*, <https://www.nytimes.com/2019/01/23/business/dealbook/yahoo-cyber-security-settlement.html> (last retrieved 25/06/2019).

NIST (14/07/2017), *About NIST*, <https://www.nist.gov/about-nist> (last retrieved 25/06/2019).

NIST (16/04/2018), *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.0416.2018.pdf> (last retrieved 25/06/2019).

NIST (2019), *Questions and Answers*, <https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics#federal>, (last retrieved 25/06/2019).

NIST (11/2016), *NISTIR 7621 Rev. 1-Small Business Information Security: The Fundamentals*, <https://csrc.nist.gov/publications/detail/nistir/7621/rev-1/final> (last retrieved 25/06/2019).

NIST (12/2018), *NIST Special Publication 800-37 Revision 2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf> (last retrieved 25/06/2019).

NIST (12/2014), *NIST Special Publication 800-53A revision 4- Assessing Security and Privacy Controls in Federal Information Systems and Organizations Building Effective Assessment Plans*, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf> (last retrieved 25/06/2019).

NIST & Joint Task Force Transformation Initiative (03/2011), *NIST Special Publication 800-39 Managing Information Security Risk: Organization, Mission, and Information System View*, <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf> (last retrieved 25/06/2019).

Official Journal of the European Union (27/05/2014), *Directive (EU) Directive 2014/56/EU of the European Parliament and of the Council of 16 April 2014 amending Directive 2006/43/EC on statutory audits of annual accounts and consolidated accounts (Text with EEA relevance)*, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0056> (last retrieved 25/06/2019).

Official Journal of the European Union (27/05/2014), *Regulation (EU) No 537/2014 of the European Parliament and of the Council of 16 April 2014 on specific requirements regarding statutory audit of public-interest entities and repealing Commission Decision 2005/909/EC Text with EEA relevance*, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0537> (last retrieved 25/06/2019).

Official Journal of the European Union (19/07/2016), *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (last retrieved 25/06/2019).

Official Journal of the European Union (07/06/2019), *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)*, <https://eur-lex.europa.eu/eli/reg/2019/881/oj>

Official Journal of the European Union (10/05/2019), *Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.123.01.0018.01.ENG (last retrieved 25/06/2019).

Official Journal of the European Union (04/05/2016), *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*, <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (last retrieved 25/06/2019).

Official Journal of the European Union (19/06/2018), *Directive (EU) 2018/843 of The European Parliament and of The Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance)*, L 156/43, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN> (last retrieved 25/06/2019).

Oxford Dictionaries (2019), *Definition: Cybersecurity*, <https://en.oxforddictionaries.com/definition/cybersecurity> (last retrieved 25/06/2019).

Pasula Milan, Nerandžić Branislav and Radošević Milan (2013), *Internal Audit of the Supply Chain Management in Function of Cost Reduction of the Company*, Journal of Engineering Management and Competitiveness (JEMC), Volume 3, Issue No. 1, 2013, Pages 32-36 ISSN 2217-8147 University of Novi Sad, https://www.researchgate.net/publication/320819794_Internal_audit_of_the_supply_chain_management_in_function_of_cost_reduction_of_the_company (last retrieved 25/06/2019).

PCAOB (2018), *Strategic Plan 2018-2022*, <https://pcaobus.org/About/Administration/Documents/Strategic%20Plans/PCAOB-2018-2022-Strategic-Plan.pdf> (last retrieved 25/06/2019).

PCAOB (2019), *Changes in Use of Data and Technology in the Conduct of Audits*, <https://pcaobus.org/Standards/research-standard-setting-projects/Pages/data-technology.aspx> (last retrieved 25/06/2019).

PCAOB (2019), *Data and Technology Task Force*, <https://pcaobus.org/Standards/research-standard-setting-projects/Pages/Data-Technology-Task-Force.aspx> (last retrieved 25/06/2019).

PCAOB (5-6/06/2018), *Standing Advisory Group Meeting: Panel Discussion*, <https://pcaobus.org/News/Events/Documents/Cybersecurity%20Briefing%20Paper.pdf> (last retrieved 25/06/2019).

PCAOB (April 2016), *Staff Inspection Brief: Vol. 2016/1*, <https://pcaobus.org/Inspections/Documents/Inspection-Brief-2016-1-Auditors-Issuers.pdf> (last retrieved 25/06/2019).

PCAOB (November 2017), *Staff Inspection Brief: Vol. 2017/4*, <https://pcaobus.org/Inspections/Documents/inspection-brief-2017-4-issuer-results.pdf> (last retrieved 25/06/2019).

Pearson Prentice Hall (2010), *The System Development Life Cycle (SDLC)*, https://wps.prenhall.com/bp_cis_careersinit_1/13/3452/883935.cw/index.html (last retrieved 25/06/2019).

Prestigiacomio Lorenzo (October 2017), *What Is The "Gaap" In Regard To Digital Currency?*, Mazars-USA, <https://mazarsusa.com/ledger/what-is-the-gaap-in-regard-to-digital-currency/> (last retrieved 25/06/2019).

Protiviti (2016), *The Internet of Things: What is It and What Should Internal Audit Care?*, https://www.protiviti.com/sites/default/files/united_states/insights/internal-audit-and-the-internet-of-things-whitepaper-protiviti.pdf (last retrieved 25/06/2019).

PWC (2019), *Harnessing the power of AI to transform the detection of fraud and error*, <https://www.pwc.com/gx/en/about/stories-from-across-the-world/harnessing-the-power-of-ai-to-transform-the-detection-of-fraud-and-error.html> (last retrieved 25/06/2019).

PWC (2017), *Blockchain: a catalyst for new approaches in insurance*, <https://www.pwc.com/gx/en/insurance/assets/blockchain-a-catalyst.pdf> (last retrieved 25/06/2019).

Queensland Government Chief Information Office (2019), *Information Asset (Definition)*, <https://www.qgcio.qld.gov.au/publications/qgcio-glossary/information-asset-definition> (last retrieved 25/06/2019).

Rabinovitch Ari & Cohen Tova (25/6/2019), *Hackers steal data from telcos in espionage campaign: cyber firm*, Reuters, <https://www.reuters.com/article/us-cyber-telecoms-cyberreason/hackers-hit-global-telcos-in-espionage-campaign-cyber-research-firm-idUSKCN1TQ0BC> (last retrieved 25/06/2019).

Rafeq Abdul (04/02/2019), *COBIT Design Factors: A Dynamic Approach to Tailoring Governance in the Era of Digital Disruption*, ISACA, <https://www.isaca.org/resources/news-and-trends/newsletters/cobit-focus/2019/cobit-design-factors#:~:text=COBIT%202019%20also%20defines%20the,prioritize%20this%20content%20as%20required> (last retrieved 25/06/2019).

Rajeev Ronanki, Ashish Verma, David Pierce & Mark Shilling (24 February 2016), *Deloitte Insights: Industrialized analytics: Data is the new oil. Where are the refineries?* <https://www2.deloitte.com/insights/us/en/focus/tech-trends/2016/data-assets-and-analytics.html> (last retrieved 25/06/2019).

Raphael Jon (01/04/2017), *Rethinking the audit: Innovation is transforming how audits are conducted—and even what it means to be an auditor*, Journal of Accountancy, <https://www.journalofaccountancy.com/issues/2017/apr/rethinking-the-audit.html> (last retrieved 25/06/2019).

Radcliff Debrach (01/03/2004), *MEECES to pieces*, Network World, <https://www.networkworld.com/article/2330885/meeces-to-pieces.html> (last retrieved 25/06/2019).

Republic of Estonia (2019), *E-residency: The New Digital Nation*, <https://e-resident.gov.ee> (last retrieved 25/06/2019).

R. E. Kalman (1960), “On the General Theory of Control Systems”, on **IFAC Proceedings Volumes, Volume 1, Issue 1**, August 1960, Pages 491-502, Available in the following website: <https://www.sciencedirect.com/science/article/pii/S1474667017700948> (last retrieved 25/06/2019).

Ripple (2019), *Instantly Move Money to All Corners of the World*, <https://ripple.com> (last retrieved 25/06/2019).

Ross Ron, Dempsey Kelley, Viscuso Patrick, Riddle Mark, Guissanie Gary (20/02/2018), *NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, <https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final> (last retrieved 25/06/2019).

Ross Ron, Dempsey Kelley & Pillitteri Victoria (June 2018), *NIST Special Publication 800-171A on Assessing Security Requirement for Controlled Unclassified Information* <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171a.pdf> (last retrieved 25/06/2019).

Salman Syed (29/10/2015), *Auditing the Internet of Things: The rise of Internet-connected devices and systems bring both new opportunities and risk for modern organizations*, Institute of Internal Auditors, <https://iaonline.theiia.org/2015/auditing-the-internet-of-things> (last retrieved 25/06/2019).

SEC (10/06/2013), *What We Do*, <https://www.sec.gov/Article/whatwedo.html> (last retrieved 25/06/2019).

SEC (21/02/2018), *Release Nos. 33-10459; 34-82746: Securities And Exchange Commission 17 CFR Parts 229 and 249 on Commission Statement and Guidance on Public*

Company Cybersecurity Disclosures, <https://www.sec.gov/rules/interp/2018/33-10459.pdf> (last retrieved 25/06/2019).

SEC (24/04/2018), *Accounting and Auditing Enforcement Release No. 3937: Order Instituting Cease-And-desist Proceedings Pursuant To Section 8A Of The Securities Act Of 1933 And Section 21C Of The Securities Exchange Act Of 1934, Making Findings, And Imposing A Cease-And-Desist Order*, <https://www.sec.gov/litigation/admin/2018/33-10485.pdf> (last retrieved 25/06/2019).

SEC (16/10/2018), *Release No. 84429: Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements*, <https://www.sec.gov/litigation/investreport/34-84429.pdf> (last retrieved 25/06/2019).

SEC Release 2018-226 (29 September 2018), *Elon Musk Settles SEC Fraud Charges; Tesla Charged With and Resolves Securities Law Charge*, <https://www.sec.gov/news/press-release/2018-226> (last retrieved 25/06/2019).

SEC Release 2013-51 (02 April 2013), *SEC Says Social Media OK for Company Announcements if Investors Are Alerted*, <https://www.sec.gov/news/press-release/2013-2013-51.htm> (last retrieved 25/06/2019).

SEC (18/07/2002), *Release No. PA-32 ; File No. S7-27-02: Privacy Act of 1974, Amended System of Records for Enforcement Files*, <https://www.sec.gov/rules/other/pa-32.htm> (last retrieved 25/06/2019).

SEC (2019), *Spotlight on Initial Coin Offerings (ICOs)*, <https://www.sec.gov/ICO> (last retrieved 25/06/2019).

SEC (25/07/2017), *Securities Exchange Act Of 1934, Release No. 81207, Report of Investigation: Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*, <https://www.sec.gov/litigation/investreport/34-81207.pdf> (last retrieved 25/06/2019).

SEC: Divisions of Enforcement and Trading and Markets (07/03/2018), *Statement on Potentially Unlawful Online Platforms for Trading Digital Assets*, <https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading> (last retrieved 25/06/2019).

Son Hugh (28/02/2017), *JPMorgan software does in seconds what took lawyers 360,000 hours*, <https://www.independent.co.uk/news/business/news/jp-morgan-software-lawyers-coin-contract-intelligence-parsing-financial-deals-seconds-legal-working-a7603256.html> (last retrieved 25/06/2019).

Sterley André (2019), *Cryptoassets: Accounting for an Emerging Asset Class*, CPA Journal, Issue June 2019, <https://www.cpajournal.com/2019/06/21/cryptoassets-accounting-for-an-emerging-asset-class/> (last retrieved 25/06/2019).

Singleton Tommie (2012), *What Every IT Auditor Should Know About Auditing Social Media*, ISACA Journal, Volume 5: 2012, Page 12-13, http://www.isacajournal-digital.org/isacajournal/2012vol5?article_id=1077872&pg=NaN#pgNaN (last retrieved 25/06/2019).

Singleton Tommie W (01/05/2010), *IT Audits of Cloud and SaaS*, ISACA Journal, <https://www.isaca.org/resources/isaca-journal/past-issues/2010/it-audits-of-cloud-and-saas> (last retrieved 25/06/2019).

SpaceDaily (24/06/2019), *Governments must regulate social networks: Facebook's Clegg* http://www.spacedaily.com/reports/Governments_must_regulate_social_networks_Facebooks_Clegg_999.html (last retrieved 25/06/2019).

Steven Wertheim (June 2019), *Auditing for Cybersecurity Risk*, *CPA Journal: The Voice of the Profession*, June 2019 Issue, by New York State Society of Certified Public Accountants (CPA), <https://www.cpajournal.com/2019/06/19/auditing-for-cybersecurity-risk/> (last retrieved 25/06/2019).

Swinhoe Dan, 11/12/2018, *What is a keylogger? How attackers can monitor everything you type*, CSO, <https://www.csoonline.com/article/3326304/what-is-a-keylogger-how-attackers-can-monitor-everything-you-type.html> (last retrieved 25/06/2019).

UK Legislation National Archives, *UK Public General Acts: The Telecommunications (Data Protection and Privacy) Regulations 1999*, <http://www.legislation.gov.uk/uksi/1999/2093/contents/made> (last retrieved 25/06/2019).

UK Legislation National Archives, *UK Public General Acts: The Privacy and Electronic Communications (EC Directive) Regulations 2003*, <http://www.legislation.gov.uk/uksi/2003/2426/contents/made> (last retrieved 25/06/2019).

UK Legislation National Archives, *UK Public General Acts: Computer Misuse Act 1990*, <https://www.legislation.gov.uk/ukpga/1990/18/contents> (last retrieved 25/06/2019).

UK Legislation National Archives, *UK Public General Acts: Data Protection Act (DPA) 1998*, <http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted> (last retrieved 25/06/2019).

United Nations Conference on Trade and Development: Trade and Development Board Investment, Enterprise and Development Commission (2015), *Cyberlaws and regulations for enhancing e-commerce: Case studies and lessons learned*, UNCTAD, https://unctad.org/meetings/en/SessionalDocuments/ciem5d2_en.pdf (last retrieved 25/06/2019).

US Federal Bureau of Investigation (2019), *Cyber Crime*, <https://www.fbi.gov/investigate/cyber> (last retrieved 25/06/2019).

US Federal Bureau of Investigation (2019), *National Cyber Investigative Joint Task Force*, <https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force> (last retrieved 25/06/2019).

US Federal Bureau of Investigation and IC3, *Internet Crime Report 2018*, https://pdf.ic3.gov/2018_IC3Report.pdf (last retrieved 25/06/2019).

US Federal Bureau of Investigation (26/10/2016), *National Cyber Security Awareness Month: FBI Deploys Cyber Experts to Work Directly with Foreign Partners*, <https://www.fbi.gov/news/stories/fbi-deploys-cyber-experts-to-work-directly-with-foreign-partners> (last retrieved 25/06/2019).

US-CERT, *United States Computer Emergency Readiness Team*, https://www.us-cert.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf (last retrieved 25/06/2019).

US Department of Justice (07/05/2017), *Identity Theft*, <https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud> (last retrieved 25/06/2019).

US Department of Justice (2019), *Computer Crime and Intellectual Property Section (CCIPS)*, <https://www.justice.gov/criminal-ccips> (last retrieved 25/06/2019).

US Department of Justice (2019), *Cybersecurity Unit*, <https://www.justice.gov/criminal-ccips/cybersecurity-unit> (last retrieved 25/06/2019).

US Federal Trade Commission (10/04/2014), *Department Of Justice And Federal Trade Commission: Antitrust Policy Statement On Sharing Of Cybersecurity Information*, <https://www.ftc.gov/public-statements/2014/04/departement-justice-federal-trade-commission-antitrust-policy-statement> (last retrieved 25/06/2019).

US Federal Trade Commission (April 2019), *Data Breach Response: A Guide for Business*, <https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business> (last retrieved 25/06/2019).

US Federal Trade Commission (2019), *Phishing*, <https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/phishing> (last retrieved 25/06/2019).

US Federal Trade Commission (October 2018), *Consumers Information: What to know about Cryptocurrency*, <https://www.consumer.ftc.gov/articles/what-know-about-cryptocurrency>, (last retrieved 25/06/2019)

US Federal Trade Commission (2019), *Ransomware*, <https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/ransomware> (last retrieved 25/06/2019).

US Federal Trade Commission (April 2006), *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying> (last retrieved 25/06/2019).

Vasarhelyi Miklos A. and Rozario Andrea M. (June 2018), *How Robotic Process Automation Is Transforming Accounting and Auditing*, CPA Journal, <https://www.cpajournal.com/2018/07/02/how-robotic-process-automation-is-transforming-accounting-and-auditing/> (last retrieved 25/06/2019).

Verizon (2019), *2019 Data Breach Investigations Report*, <https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf> (last retrieved 25/06/2019).

Waldron Amy & Hallstrom David (01/09/2013), *A breach of client data: Risks to CPA firms*, Journal of Accountancy,

<https://www.journalofaccountancy.com/issues/2013/aug/20138003.html> (last retrieved 25/06/2019).

White House: Office of the Press Secretary (12/02/2013), Presidential Policy Directive - Critical Infrastructure Security and Resilience, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil> (last retrieved 25/06/2019).

White House (11/05/2017), *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/> (last retrieved 25/06/2019).

White Sarah K. and Greiner Lynn (18/01/2019), *What is ITIL? Your guide to the IT Infrastructure Library*, CIO, <https://www.cio.com/article/2439501/infrastructure-it-infrastructure-library-itil-definition-and-solutions.html> (last retrieved 25/06/2019).

Wollmert Peter (10/04/2019), *How to prepare for the digital transformation of reporting*, EY, https://www.ey.com/en_gl/assurance/are-you-prepared-for-the-digital-transformation-of-reporting (last retrieved 25/06/2019)

World Economic Forum (2019), *Global Risks Report of 2019: 14th edition, Pages 5 & 8*, http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf (last retrieved 25/06/2019).

Yaga Dylan, Mell Peter, Roby Nik & Scarfone Karen (October 2018), *NISTIR 8202: Blockchain Technology Overview*, NIST, <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf> (last retrieved 25/06/2019)

III] BIBLIOGRAPHY OF TABLES AND IMAGES

<i>T A B L E S</i>		
N o	Title	Source
1	The Audit Risk Equitation in Modern Business Risk Model	Κωνσταντίνος Καραμάνης (2008–1 st Greek edition), <i>Σύγχρονη Ελεγκτική: Θεωρία και Πρακτική Σύμφωνα με τα Διεθνή Ελεγκτικά Πρότυπα (Modern Auditing: Theory and Practice according to International Auditing Standards)</i> , Εκδόσεις ΟΠΑ, Αθήνα.
2	The Basic Steps of Cybersecurity Audit Process	Κωνσταντίνος Καραμάνης (2008–1 st Greek edition), <i>Σύγχρονη Ελεγκτική: Θεωρία και Πρακτική Σύμφωνα με τα Διεθνή Ελεγκτικά Πρότυπα (Modern Auditing: Theory and Practice according to International Auditing Standards)</i> , Εκδόσεις ΟΠΑ, Αθήνα.
3	The four Tiers of NIST’s Cybersecurity Framework Version 1.1	NIST (2019), <i>Framework Documents</i> , https://www.nist.gov/cyberframework/framework (last retrieved 25/06/2019).

4	Analytical Presentation of the Five Core Functions and their Categories of NIST's Cybersecurity Framework Version 1.1	NIST (16/04/2018), <i>Framework for Improving Critical Infrastructure Cybersecurity Version 1.1</i> , https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (last retrieved 25/06/2019).
5	Short History of COBIT Evolution	Tessin Peter (07/04/2016), <i>COBIT Celebrates 20 Years of Guidance</i> , https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2016/cobit-celebrates-20-years-of-guidance (last retrieved 25/06/2019). White Sarah K. (15/01/2019), <i>What is COBIT? A framework for alignment and governance</i> , https://www.cio.com/article/3243684/what-is-cobit-a-framework-for-alignment-and-governance.html (last retrieved 25/06/2019).
6	Presentation of ITAF's 2014 Standards and Guidance System	ISACA (01/05/2016), <i>Standards, Guidelines, Tools and Techniques</i> , ISACA Journal, Issue 2016, Volume 3, https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/standards-guidelines-tools-and-techniques (last retrieved 25/06/2019).
7	The five levels of impact analysis of cybersecurity threats	Dr. Curtis Patchin and Mark Carey (October 2012), <i>Risk Assessment in Practice</i> , Committee of Sponsoring Organizations of the Treadway Commission (COSO) and Deloitte & Touche LLP, https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dttl-grc-riskassessmentinpractice.pdf (last retrieved 25/06/2019).
8	The Risk Rate Matrix for Cyber-security Threats	
I M A G E S		
1	The correlation between Inherent Risk, Residual Risk and Risk Appetite in Risk Based Internal Audits	Chartered Institute of Internal Auditors (08/10/2014), <i>Risk Based Internal Auditing</i> , https://global.theiia.org/standards-guidance/topics/Documents/201501GuidetoRBIA.pdf (last retrieved 25/06/2019).
2	Blockchain Technology Applications according to World Economic Forum	WEF , 2019, <i>Strategic Intelligence: Blockchain</i> , https://intelligence.weforum.org/topics/a1Gb00000038qmPEAQ?tab=publications (last retrieved 25/06/2019).
3	The Three Primary Components of NIST's Cybersecurity Framework Version 1.1	NIST (2019), <i>Framework Documents</i> , https://www.nist.gov/cyberframework/framework (last retrieved 25/06/2019).
4	The Core Elements of NIST's Cybersecurity Framework Version 1.1	NIST (2019), <i>Framework Documents</i> , https://www.nist.gov/cyberframework/framework (last retrieved 25/06/2019).
5	Presentation of COSO's Internal Control—Integrated Framework (2013 edition) and its Components	COSO (May 2013), <i>Internal Control—Integrated Framework: Executive Summary</i> , https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf (last retrieved 25/06/2019).
6	COBIT 2019 Design Factors	Rafeq Abdul (04/02/2019), <i>COBIT Design Factors: A</i>

7	Governance System Design Workflow	<i>Dynamic Approach to Tailoring Governance in the Era of Digital Disruption</i> , ISACA, https://www.isaca.org/resources/news-and-trends/newsletters/cobit-focus/2019/cobit-design-factors#:~:text=COBIT%202019%20also%20defines%20the,prioritize%20this%20content%20as%20required (last retrieved 25/06/2019).
8	The Three Basic Categories of IT/cybersecurity Internal Controls	Institute of Internal Auditors (March 2012-Second Edition), <i>Global Technology Audit Guide (GTAG) 1: Information Technology Risk and Controls</i> , https://chapters.theiia.org/montreal/ChapterDocuments/GTAG%201%20-%20Information%20technology%20controls_2nd%20ed.pdf (last retrieved 25/06/2019).
9	The Hierarchy of IT/cybersecurity Internal Controls	
10	Types of Modified Opinions	IFAC (2010), <i>International Standard on Auditing (ISA) 705 on Modifications to the Opinion in the Independent Auditor's Report</i> , https://www.ifac.org/system/files/downloads/a037-2010-iaasb-handbook-isa-705.pdf (last retrieved 25/06/2019).