UNIVERSITÀ DEGLI STUDI DI MILANO

Master di II livello in **CYBERSECURITY**

DIPARTIMENTO DI INFORMATICA "G. Degli Antoni"

DIPARTIMENTO DI SCIENZE GIURIDICHE "C. Beccaria"

DIPARTIMENTO DI ECONOMIA, MANAGEMENT E METODI QUANTITATIVI

CYBER RISK MITIGATION THROUGH AN ORGANIZATIONAL AND MANAGEMENT PROSPECTIVE IN A MULTIPLE LEGAL AND QUALITY ENVIRONMENT

Relatore Universitario: prof.ssa Maddalena Sorrentino

Laureando

dott. Gianluca Conte

(Matricola M03925)

Licenza selezionata

Attribuzione - Non commerciale - Non opere derivate 4.0 Internazionale

A. S. 2021-2022

All truth passes through three stages. First, it is ridiculed. Second, it is violently opposed. Third, it is accepted as being self-evident.

Arthur Schopenhauer (The World as Will and Representation)

Table of Contents

Acknowledgments

I thank Simone Piunno (CTO of Bocconi University) for giving me the opportunity to undertake the master, to better enter the new role that Bocconi has bestowed me.

I thank Prof.ssa Maddalena Sorrentino (University of Milan) for her guide, patience and availability.

I also thank the lawyer Michelangela Verardi (University of Pavia), a colleague for many years and now a friend, for the reflections concerning the legal aspects.

I dedicate this thesis to Paola, my life partner who has always been by my side and has always supported me even in the most difficult moments.

Preface

About candidate

Audit and compliance professional with plus than 13 years of experience achieved in Big4 (Deloitte), Big Pharma (Eli Lilly & Company) and in Higher Education University Management as staff member (Bocconi University and Bocconi SDA Business School, as University B.U.). Expert of vigilance concerning administrative liability pursuant to Italian Decree 231/01 as compliance auditor, member and secretary of Supervisory Body (Italian Decree 231/01 "*Organismo di Vigilanza*").

Specialized in auditing, control framework, organizational management, corporate governance, compliance advisory and risk management. Involved in organizational and corporate governance projects, design of internal control system, anti-corruption analysis, due diligence activities and business intelligence projects. | **2009 - 2022**

Graduated in game theory (field: asymmetric information in the labor market), qualified in statistics, econometrics and applied math (University of Pisa) | **2009**

Post-experience graduation in auditing and internal control (field: corruption risk management) (University of Pisa). | **2011**

Executive education in business management, leadership, governance, risk, compliance, audit, internal control, security, data protection and legal tech achieved at SDA Bocconi Business School, The Institute of Internal Auditors, European Academy for Taxes, Economy and Laws, Duke University, University System of Georgia, University of Michigan, University of California, Irvine, The Hong Kong University of Science and Technology, Yonsei University, Erasmus University Rotterdam, IE Business School, Politecnico di Milano, The State University of New York, Macquarie University, University of Colorado, University of Virginia. | **2014 - 2022**

About Thesis

The aims of the thesis are (1) to show that cyber and information security has multiple layers and that technology, while essential, is only one layer of a more complex picture (2) to propose an abstract and scalable model of Information Security Management System and Governance structure dedicated to cyber and information security, both of them coherent with different and complementary regulatory areas, national and European in order to move towards an integrated compliance system.

Introduction

Cyber and information security have recently emerged and have an enormous and growing importance for all social actors (individuals, companies, institutions, sovereign states) as they have a significant impact on individual freedoms, on obligations by legal persons, on economic balance both micro and macro and on the sovereignty of countries.

Cyber and information security is originally seen as a problem inherent to technology which, although fundamental, nevertheless represents only one among many links of a long chain. Each link in the chain represents a distinct disciplinary area that make the problem of cyber and information security deeply multidisciplinary.

The "human factor" is another of these links and it is often the weakest in the chain, exposing all social actors have significant risks. Human behaviors are, therefore, phenomena that must be understood and governed: in the corporate sphere this governance must take place through (1) the adoption of an adequate management system and (2) the introduction of suitable organizational structures used for its maintenance.

The adoption of these tools must consider (1) gaps in the scientific literature that hinder a single integrated vision of a multidisciplinary problem, (2) a complex, articulated and not-integrated compliance frameworks and (3) fragmented managerial practices and frameworks that address individually each area of compliance.

Even with these difficulties, companies have the ethical, social and administrative liability of approach the problem from a broad perspective. These activities, however, determine important costs that the company must evaluate with respect to the cost deriving from the aware and informed failure to adopt a solution. Companies must therefore find their own tailor-made solution (both from the point of view of management and organization) through a holistic, integrated approach with respect to all the regulatory requirements to which it is exposed and which represents the best solution to the trade-off between action and non-action.

The thesis analyzes cyber and information security issues from management system and organizational point of views.

The first chapter introduces the phenomenon of cybercrime, the definition of cyber risk, the types of perpetuating crimes and the economic effects on markets and the consequences for individual companies.

The second chapter defines the background of the problem, introducing the research questions and indicating the methodology adopted in the survey of the scientific literature.

The third chapter explores the governance of information security through an overview concerning the need for adequate cyber risk awareness, the influence that corporate culture and human behavior have on information security and the importance of policies, the rising role of CISO and globally recognized management systems (in particular ISO 27001).

The fourth chapter introduces some of the main compliance fields, with links to the cybersecurity and data protection area, to which Italian companies are exposed and have to manage, in particular GDPR, Legislative Decree 231/01, Legislative Decree 81/08 or to which it would be appropriate for them to be oriented, e.g. CoSO Report, in order to increase compliance assurance.

The fifth chapter is a methodological example of how to conduct an ISO 27001 implementation project and how to structure a CISO department: the chapter deals with the necessary requirements, the approach for setting up the project, the AS-IS reconnaissance phase, the Gap Analysis with respect to ISO controls, the formulation of recommendations to reach a TO-BE compliant situation with ISO controls.

In the last part of the chapter are described (1) an example (§5.3) of Information Security Management System, meeting the ISO requirements and (2) an example (§5.4) of a CISO department, hypothesized within an Italian company, with general characteristics assumed (as stated in the second chapter).

1. The Cyber Crime phenomenon

1.1 A brief overview of Cyber Crime history

The evolution of cybercrime has gone hand in hand with the evolution of information technology. Johannes Xingan Li[1] supposes that the cybercrime history can be divided in these four stages (1) germination (1940s-1960s), (2) rapid development (1970s-1980s), (3) broad expansion (1990s), (4) routinization (2000s) since increased the amplitude and the awareness inherent to cybercrime. In this environment, legislators have pursued these stages not in a timely manner.

Stage I: Germination (1940s-1960s)

In the first stages cybercrime was not a global phenomenon and involved a limited number of computers or concerned linked phenomena such as "phone phreaking": the dimension and the nature of the phenomena did not arouse the attention of the legislator and the judicial system had to deal with these events through the application of traditional law.

Greater attention was paid starting from the 1950s: starting from this period cybercrime has assumed greater importance in key areas for the social sphere, such as the military and finance sectors. For example, the first known cybercrime[2] in the financial sector occurred in the United States in 1958, through the manipulation of computer records by a bank employee who diverted a few cents from many depositors' interests.

The modern vision of hacking was introduced in the University environment: in the 1960s was published the first reference to malicious hacking in MIT's student's newspaper that investigated some programs in order to understand the way to improve them. During this stage, hacking had not financial, commercial, etc. scope but was only a social phenomenon that attracted curious students driven by the desire to contribute in technologies improvement. Big Corporate (such as IBM) used these

[1] Li, J. X. (2017). Cyber crime and legal countermeasures: A historical analysis. International Journal of Criminal Justice Sciences, 12(2), 196-207.
[2] Parker, D. B. (1989). Computer Crime: Criminal Justice Resource Manual.

desires, taking advance of young students' skills in order to improve software. This approach is still live and called Ethical Hacking.

Computers were initially very large in size. Only from the end of the 60's computers began to have smaller dimensions and more affordable prices. That was the beginning of the mass diffusion we know today.

At the same time, the world was experiencing the Cold War and ARPANET (Advanced Research Projects Agency Network) was created by U.S. Dept. of Defense (1960s): this event provided the military and research institutions with innovative and dematerialized coordination and command tools, particularly useful in case of physical war, guaranteeing a decentralized communication system. The other side of the coin was the implicit creation of cyber risks inherent to the fragility of the newborn system even if not yet open to global users. From that point on, cybercrime began to have military and scientific objectives.

As argued by Li[3], at that time real episodes of cybercrimes were starting but the law and regulatory framework was not adequate for the times and did not keep pace with the evolution of technologies and their improper use. In other words, cybercrimes were not prosecutable and there were not a duly deterrent and this certainly caused their proliferation. Existing laws were not suitable for stopping cybercriminals; for this reason, many ordinary criminals brought some of their activities online. Only at the end of the 1960s did legislators begin to update the system of laws and the trigger was the impact of new technologies on the protection of personal data.

Stage II: Rapid development (1970s-1980s)

In 1983 the cult film "Wargame" was released and the hacking phenomenon became globally known as well as the fragility of the IT systems and networks used up to then. During this period, new attack techniques were developed and spreaded, for example the Trojan Horses.

[3] Li, J. X. (2017). Idem

The US Dept. of Defense understood the relevance of the problem and began to establish defensive and protection criteria: in 1985 was published[4] the "Trusted Computer System Evaluation Criteria", in order to provide a first reference framework in the cyber field. In the same period, the American military system was compromised and the first case of data theft, sold to foreign secret services was known: well-known was the case of Marcus Hess who managed to compromise the Pentagon mainframe, selling information to the KGB.

At this stage, computers were increasingly popular even among end-consumers and global services began to take hold, such as e-mail, a simple, cheap and instant tool. At this stage, however, technologies remained fragile and easily exposed to manipulation, typically[5] for vandalism, theft of information, theft of services, theft of property, and fraud.

It was at this stage that legislators began to respond, albeit belatedly, to a need for legislative regulation. Li[6] describes that from this moment on, law deterrents were introduced and cybercrime was discouraged but this does not stop its growth.

Stage III: Broad expansion (1990s)

Starting in the 1990s, the whole world went online. Computers were now widespread in many countries, also characterized by different levels of economic well-being, and companies that would make the history of information technology were emerging and establishing themselves. Governments began to counteract the problem of cybersecurity by creating dedicated institutions (e.g. European Institute for Computer Antivirus Research).

The creation of the WWW[7] was the trigger that brought millions of interconnected people online. The targets of cyber criminals were no longer just institutions, corporations and governments but also ordinary people. In this phase, a huge number

[4] Lipner, S. B. (2015). The birth and death of the orange book. IEEE Annals of the History of Computing, 37(2), 19-31.
[5] Li, J. X. (2017). Idem
[6] Li, J. X. (2017). Idem
[7] Berners-Lee, T. J. (1989). Information management: A proposal(No. CERN-DD-89-001-OC).

of viruses were created that also began to be conveyed by email. For these reasons, the new anti-virus business was born at this stage.

Li[8] describes how it was from this stage that the regulatory systems began to harmonize globally, making it possible to achieve a sort of balance between deterrent tools and the growth of the phenomenon of cybercrime.

Stage IV: Routinization (2000s)

Since the 2000s, the economic and financial world has made the network one of its fundamental pillars, creating a situation from which, even if we wanted to, we could not go back. Cybercrime evolved and both large corporations and individuals were targeted. DoS attacks began to cause large loss of profits to large companies and in parallel the telematic frauds began to claim victims among the common people.

Cybercrime became a phenomenon with significant macroeconomic effects, causing damages for 455 million dollars in the early 2000s. Li[9] observes, in any case, that starting from 2004 there was a reduction in attacks and their economic significance: this decline is attributable to the strengthening of the tools to combat cybercrime.

More recent studies[10], detailed in the following paragraphs, show a resurgence of the phenomenon: in 2013, only in the USA, cyber-attack caused a peak of 564 million dollars in losses due to 180 day of unavailability of relevant online services.

Li also notes that, in any case, the enhancement of deterrents will always be a step behind the development of cybercrime. Cybercrime, as describe in the next chapters, has been transformed to the point of creating real criminal organizations that have very different aims and objectives. Entrepreneurship in cybercrime has allowed criminals to share and face off the increasing levels of risk.

[8] Li, J. X. (2017). Idem
[9] Li, J. X. (2017). Idem
[10] Dieye, R., Bounfour, A., Ozaygen, A., & Kammoun, N. (2020). Estimates of the macroeconomic costs of cyber-attacks. Risk Management and Insurance Review, 23(2), 183-208.

1.2 Definition of Cyber Crime, Cyber Risk and Cyber Resiliency

Cyber Crime seems to have simple definition, i.e. any criminal activities perpetuated using computer (as tool or as target[11]) and a network[12], perpetuated by natural persons.

Instead Cyber Risk seems to be more difficult to define and seems to depend on the context and the framework being considered, e.g. (as describe in the next chapters):

- ISO/IEC 27001 assumes a definition, focused on the safeguard of information themselves as Corporate assets,
- GDPR considers natural person's rights and freedoms as the most important value[13] so for the GDPR Cyber Risk can be defined as negative effect on natural persons rights and freedom, caused by other natural or juridical persons actions or omissions,
- Decree 231/01 consider Cyber Risk as the Corporate punishment, in the case of realization of a Cyber Crime that should be predictable and blocked by the Corporate, creating an interest/advantage for itself.

Beyond the juridical and philosophical question this point create a deep difference in the Cyber Risk Evaluation methodology, due to the different definitions, making hard to have an Integrated Cyber Risk Evaluation methodology.

G. Strupczewski[14] argues that

> *in the public discourse on cybersecurity, risk has been defined and redefined countless times in order to reflect those aspects that an author deemed important.*

Cyber risk must, therefore, concern the Enterprise Risk[15], being underlying and integrated with all risks of another nature. From this point of view, NIST's[16] definition of Cyber Risk is incomplete even to be "useless" in some compliance framework:

---

[11] Kruse II, W. G., & Heiser, J. G. (2001). Computer forensics: incident response essentials. Pearson Education.
[12] Moore, R. (2005). Cybercrime: Investigating high-technology computer crime. LexisNexis.
[13] Art. 1 GDPR Subject-matter and objectives
[14] Strupczewski, G. (2021). Defining cyber risk. Safety science, 135, 105143, 1-10.
[15] Committee of Sponsoring Organizations of the Treadway Commission (2017), Enterprise Risk Management. Integrated Framework.
[16] NIST Standard 800-160, Volume 2

the risk of depending on cyber resources, i.e., the risk of depending on a system or system elements which exist in or intermittently have a presence in cyberspace

Cyber Risk must have therefore a more complex and articulated definition; Strupczewski[17] analyzed many different definitions coming to formulate that:

Cyber risk is an operational risk associated with performance of activities in the cyberspace, threatening information assets, ICT resources and technological assets, which may cause material damage to tangible and intangible assets of an organisation, business interruption or reputational harm. The term 'cyber risk' also includes physical threats to the ICT resources within organisation

Strupczewski argues how difficult it is to provide a concise definition of cyber risk, formulating an ontological approach that allow to describe the "*functional interdependencies with other terms, conditions and factors that create the cyber risk framework and determine its nature"*. From this point of view, Strupczewski propose an ontological meta model of cyber risk concept as in Fig. 1[18]:

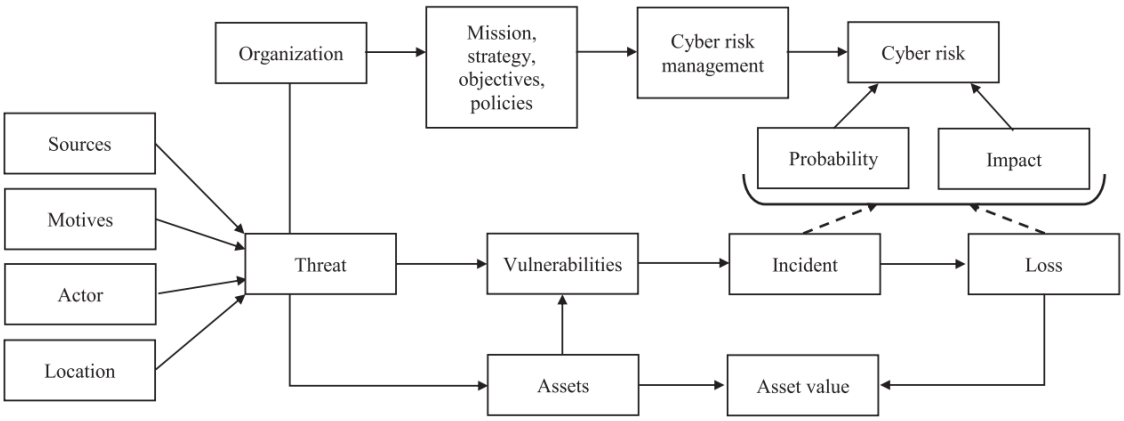


Fig. 1 – Cyber risk definition: ontological meta model

The definition of cyber risk changes according to the point of view and the context. A model based on an ontological approach has some advantages; as Strupczewski explains[19]:

It identifies four groups of factors that characterise the diverse nature of cyber threats (sources of cyber threats, actors, their motives, location). Another benefit of the meta model is placing cyber risk in the context of mission, strategy, risk

[17] Strupczewski, G. (2021). Idem
[18] Strupczewski, G. (2021). Idem
[19] Strupczewski, G. (2021). Idem

management policy and objectives of an organisation. And last but not least, the model indicates that, although cyber risk measures (probability of occurrence and potential impact) are abstract (i.e. determined using mathematical and statistical tools), they are estimated on the basis of historical data about the actual, not simulated, cyber incidents.

In any case, probably it is easier to have an Integrated Cyber Internal Control System, despite different definitions of Cyber Risk, embracing NIST's[20] Cyber Resiliency definition:

Cyber Resiliency is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

[20] NIST Standard 800-160, Volume 2

1.3 Typologies of Cybercrime

Cybercrime has evolved to cover several areas of typical analog crime, e.g. (1) organized crime has brought many of its activities online, (2) some terrorist environments have started operating on the web, (3) extortion have moved online both towards individuals and towards companies, public and governmental institutions, (4) up to online activities of real war between sovereign states.

With reference to organized crime, Etges and Sutcliffe explain[21] that

> *the Internet provides an opportunity for free enterprise without strict rules, and there is very limited monitoring and enforcement of laws in cyber-space. 'Services' such as child exploitation and human trafficking are offered in Websites and discussion groups with little concern for punishment, and organized crime groups practice fraud, cyber extortion, and money laundering using the quasi anonymity of e-currencies. Because digital gold currency providers are not banks, they are not legally required to perform the various types of "know your customer" background checks. […] different organized crime groups, using the latest communication technologies, establish connections, alliances, and business relations to optimize and expand their operations across the globe, they are generally labeled as Transnational Criminal Organizations.*

Instead, inherent in terrorist activities, Lee, Choi, Shandler and Kayser explain[22] that:

> *terror in cyberspace is ubiquitous, more flexible than traditional terrorism, and that cyberattacks mostly occurred within the countries of origin. […]*
> *This combination of ideology and technology means that terrorism in cyberspace, in the view of traditional conflict theory, could be attributed to a class struggle between different classes and ideologies, or an uneven world order, fueled by wealth, technology, ideology, and geopolitics. As the data show, cyberterror attacks tend to occur most often against wealthy democratic nations rather than poorer and non-democratic nations, which can result in a reversal of roles of victims and offenders […]. Terrorists who utilize cyber-resources to promote and propagate ideology and exercise power through global terrorism predominantly target Western democracies that do not share the same views, ideologies, and political systems of the perpetrators.*

Another significant area to mention is digital extortion: the development of cryptocurrencies, cryptolockers and the effectiveness of cyber-attacks that exploit the

[21] Etges, R., & Sutcliffe, E. (2008). An overview of transnational organized cyber crime. Information Security Journal: A Global Perspective, 17(2), 87-94.
[22] Lee, C. S., Choi, K. S., Shandler, R., & Kayser, C. (2021). Mapping global cyberterror networks: an empirical study of al-Qaeda and ISIS cyberterrorism events. Journal of Contemporary Criminal Justice, 37(3), 333-355.

technological immaturity of users (e.g. phissing) have determined the enormous growth of the phenomenon of online extortion.

With reference to Cyberextortion, Richardson and North argue[23] that

> *The FBI estimates that ransomware generated $209,000,000 in the first three months of 2016 and is on track to be a one-billion-dollar crime this year (Fitzpatrick & Griffin, 2016). During the first quarter, McAfee Labs measured 1.2 million ransomware attacks. This was a 24-percent increase over the fourth quarter of 2015 (McAfee Labs Threats Report, 2016).*

More recently, the cyber security company Sophos estimated[24], out of a sample of 5400 companies, that the average ransom paid by a medium-sized company was around 170k dollars in the year 2021. Paying the ransom is, however, only part of the cost that affected companies have to bear. From this point of view, Sophos argues[25] that in 2021:

> *Paying the ransom is just part of the cost of remediating an attack. While both the number of ransomware attacks and the percentage of attacks where adversaries succeed in encrypting data has declined since last year, the overall cost of remediating a ransomware attack has increased. Respondents reported that the average cost to rectify the impacts of the most recent ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc.) was US$1.85 million, more than double the US$761,106 cost reported last year*

Another area in which cyber activities are having a strong expansion is that of unconventional warfare between sovereign states. Eun and Aßmann argue[26] that

> *Attempting to define "cyberwar" brings even more confusion: when is a cyber-attack "merely" a nuisance and when can it be regarded as an act of aggression? […] Currently think-tanks and research institutions are engaging with this new phenomenon of cyber-attacks, trying to arrive at a usable definition of cyberwar, and provide practical government policies.*

The definition of cyberwarfare should probably be approached from an ontological point of view as was done for the definition of cyber risk. An ontological view of the

[23] Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. International Management Review, 13(1), 10.
[24] A Sophos Whitepaper. April 2021, The State of Ransomware 2021
[25] A Sophos Whitepaper, Ibidem
[26] Eun, Y. S., & Aßmann, J. S. (2016). Cyberwar: Taking stock of security and warfare in the digital age. International Studies Perspectives, 17(3), 343-360.

theme seems to have been provided by Wood and Winkle[27], analyzing how the insurance market has moved in relation to this phenomenon:

> *What constitutes war? Where is the threshold for hostility at which society can no longer tolerate the resulting damage? Ethical arguments suggest the answers can be found in reason. Realists assert that these questions are decided by the powerful. Constructionists argue shared expectations about reasonable behavior shape such decisions. Markets offer answers in the form of war clauses in insurance policies. Such clauses are used to withdraw coverage for losses related to military operations. Insurers draw the line between war and peace because the underwriting assumptions fundamentally differ. Doing so necessitates anticipating and defining which war-related events threaten the existence of a private market.*

Cybercrime therefore takes on different forms, it can have different purposes, it can be perpetuated by individuals and by both criminal and activist organizations but also carried out by sovereign states against other states. The theme is complex and in continuous and rapid expansion. The aim of this paragraph is to give only a very first smattering to help understand the profound transversality and complexity of the question.

[27] Woods, D. W., & Weinkle, J. (2020). Insurance definitions of cyber war. The Geneva Papers on Risk and Insurance-Issues and Practice, 45(4), 639-656.

1.4 Macroeconomics effect and microeconomics consequences for corporates

The global impact of cyber issues is evident to everyone and it seems increasingly appropriate to study the phenomenon also from an aggregate macroeconomic point of view.

A macroeconomic assessment on the cybercrime theme is an area that seems not yet sufficiently explored by the scientific and professional literature. Of particular note is the work of Dieye, Bounfour, Ozaygen and Kammoun[28]:

> *The idea is that when a disruptive event, such as a cyber-attack, hits a sector, it results in an inoperability state or production stoppage and/or slow-down. This inoperability state thus impacts that sector and diffuses to other sectors via the sector inter-dependencies matrix.*

They propose a dynamic inoperability input–output model as in Fig. 2[29]:

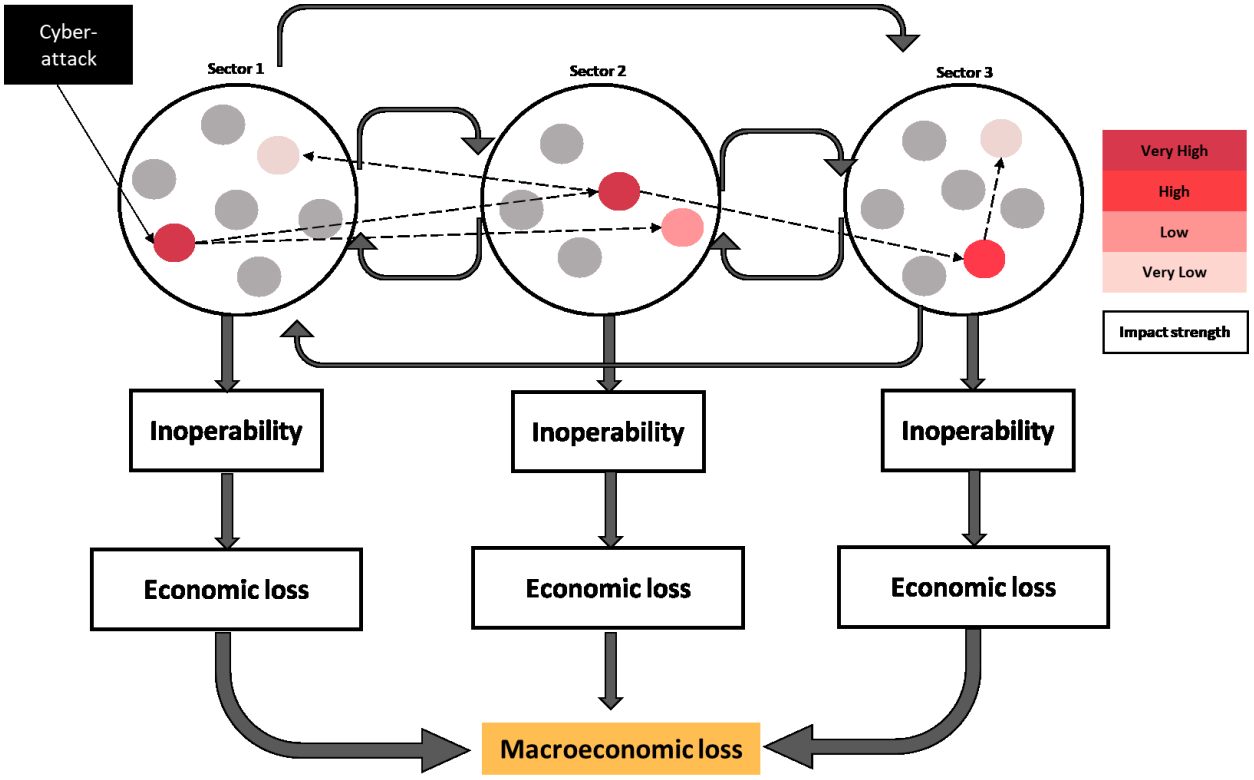


Fig. 2 – Macroeconomics inoperability input-output model

[28] Dieye, R., Bounfour, A., Ozaygen, A., & Kammoun, N. (2020). Idem
[29] Dieye, R., Bounfour, A., Ozaygen, A., & Kammoun, N. (2020). Idem

The analysis showed aggregate data of extreme interest: between 2000 and 2014 the worldwide macroeconomic effect, understood as economic losses, was estimated in a range between 2.2 and 7.2 billion US dollars, divided as follows in Tab. 1[30]:

	Inoperability ranges	
from	10%	40%
UK	66	194
US	131	394
Germany	23	70
Italy	29	88
France	23	68
China	1.476	4.889
Japan	62	193
Rest of World	435	1.378
Tot.	**2.245**	**7.274**

(million US dollars)

Tab.1 – Macroeconomics effect of cyber-attack (2000 – 2014)

1.4.1 Cyber-issues (e.g. data breach) costs and effects for a corporate

From a microeconomic point of view, following a cyber-attack that caused a data breach, a company will have to face a cost, as well as having to manage the reputational damage.

In the healthcare sector, Meisner[31] has carried out an impressive analysis aimed at estimating the final cost that a health-care company will have to bear due to the cyber incident. This cost is estimated in approx. 2.4 million of EUR.

The healthcare sector is particularly sensitive from a regulatory point of view, being particularly exposed to the risks inherent in the processing of sensitive personal data. This sensitivity is further increased in the European context where the GDPR has introduced one of the most protective regulatory frameworks for natural persons.

[30] Dieye, R., Bounfour, A., Ozaygen, A., & Kammoun, N. (2020). Idem

[31] Meisner, M. (2017). Financial consequences of cyber attacks leading to data breaches in healthcare sector. Copernican Journal of Finance & Accounting, 6(3), 63-73.

However, the health sector, while remaining among the most sensitive, has similarities with other sectors such as banks, insurance, research, university education.

In particular, Meisner constructs the estimate of the final cost through the following items and cost assumptions as in Tab. 2[32]:

Type of costs	Potential scenario	Estimated costs	Estimated costs in PLN*
Forensic investigation	3 weeks of engaging 3 experts (each working 8h/day). Rates: USD 200 per hour.	200 USD x 8h x 3 experts x 21 days = 100,800 USD	348,223.68 PLN
Breach notification	Notification of 3,000 patients. Cost of notification: USD 10 per victim.	3,000 patients x 10 USD = 30,000 USD	103,638 PLN
Post-breach patient protection	Post breach protection cost at the level of USD 15 per victim. Only 9% of victims – 270 patients – registered for such services.	270 victims x 15 USD = 4,050 USD	13,991.13 PLN
Attorney fees and litigation expenses	Costs of legal defence (USD 16,000) and cost of settlement in a class action civil lawsuit (USD 250,000).	16,000 USD + 250,000 USD = 266,000 USD	918,923.60 PLN
Regulatory compliance	The attacked hospital, i.e. the controller processing personal data, failed to notify about data breach as required in Article 33 of GDPR. Fine: EUR 2,000,000 according to Article 83 of GDPR. The data breach also showed that the hospital (being essential services operator) had not remedied non-compliance found during former audit. Fine: PLN 50,000 according to Article 57 of National Cybersecurity System Act (currently in draft version).	2,000,000 EUR + 50,000 PLN	8,341,400 PLN + 50,000 PLN = 8,391,400 PLN
Cybersecurity improvements	Cyber attackers gained access to patients data using presence of hospital system vulnerabilities. Cost of cybersecurity improvements: PLN 1,000,000.	1,000,000 PLN	1,000,000 PLN
Loss of reputation and patients churn	The attacked hospital was public healthcare provider and, despite loss of reputation, patients churn was almost unnoticeable.	–	–
Other potential costs	The hospital was refused to obtain insurance against cyber incidents, unless further cybersecurity improvements are made. Cost: PLN 300,000.	300,000 PLN	300,000 PLN
Total:			**11,076,176.40 PLN**

Tab.2 – Data Breach final cost for Corporate (an example)

In the healthcare sector a single episode of data breach can determinate a one-shoot cost equal to 11 million of PLN (approx. 2,4 million of EUR), that can be considered as an approximation (by excess) valid also for other sectors such as banks, insurance, research, university education.

[32] Meisner, M. (2017). Idem

There are many attempts to create a model for calculating the cost of data breach, but the scientific literature does not yet seem to have produced a predominant approach, more recognized than others. In any case, it is very important that companies address the problem and approach it from an operational point of view.

In this context another impressive contribution in the calculation of the final cost of a data breach was made by Algarni and Malaiya[33]. They argue that:

> *Estimates of the costs incurred in such data breaches are published frequently. However, those estimates vary widely. Without proper disclosure by the impacted organizations, it is hard to compare the risk of information loss and its potential costs. Thus, the collection and aggregation of such information is vital. A careful quantitative analysis of data from the disclosures can be used to allocate resources for prevention and recovery after a breach. […] The potential cost of information loss to businesses and society is increasing yearly.*

They propose a complex model that investigates the individual potential cost items that a company should incur[34]:

> *Utilizing an exhaustive range and combinations of inputs, we examine how each calculator computes the cost of data breaches for difference scenarios. We identify the factors that affect the costs of data breaches used in the various calculators and then classify those factors into logically related categories. […] We then model an approach needed to construct complete systemic models for data breach costs based on the calculators and actual data regarding data breach costs.*

Their "Overall risk evaluation model" can be represented briefly in a graphical way, as in Fig. 3[35]:

[33] Algarni, A. M., & Malaiya, Y. K. (2016, May). A consolidated approach for estimation of data security breach costs. In 2016 2nd International Conference on Information Management (ICIM) (pp. 26-39). IEEE.
[34] Algarni, A. M., & Malaiya, Y. K. (2016, May). Ibidem
[35] Algarni, A. M., & Malaiya, Y. K. (2016, May). Idem

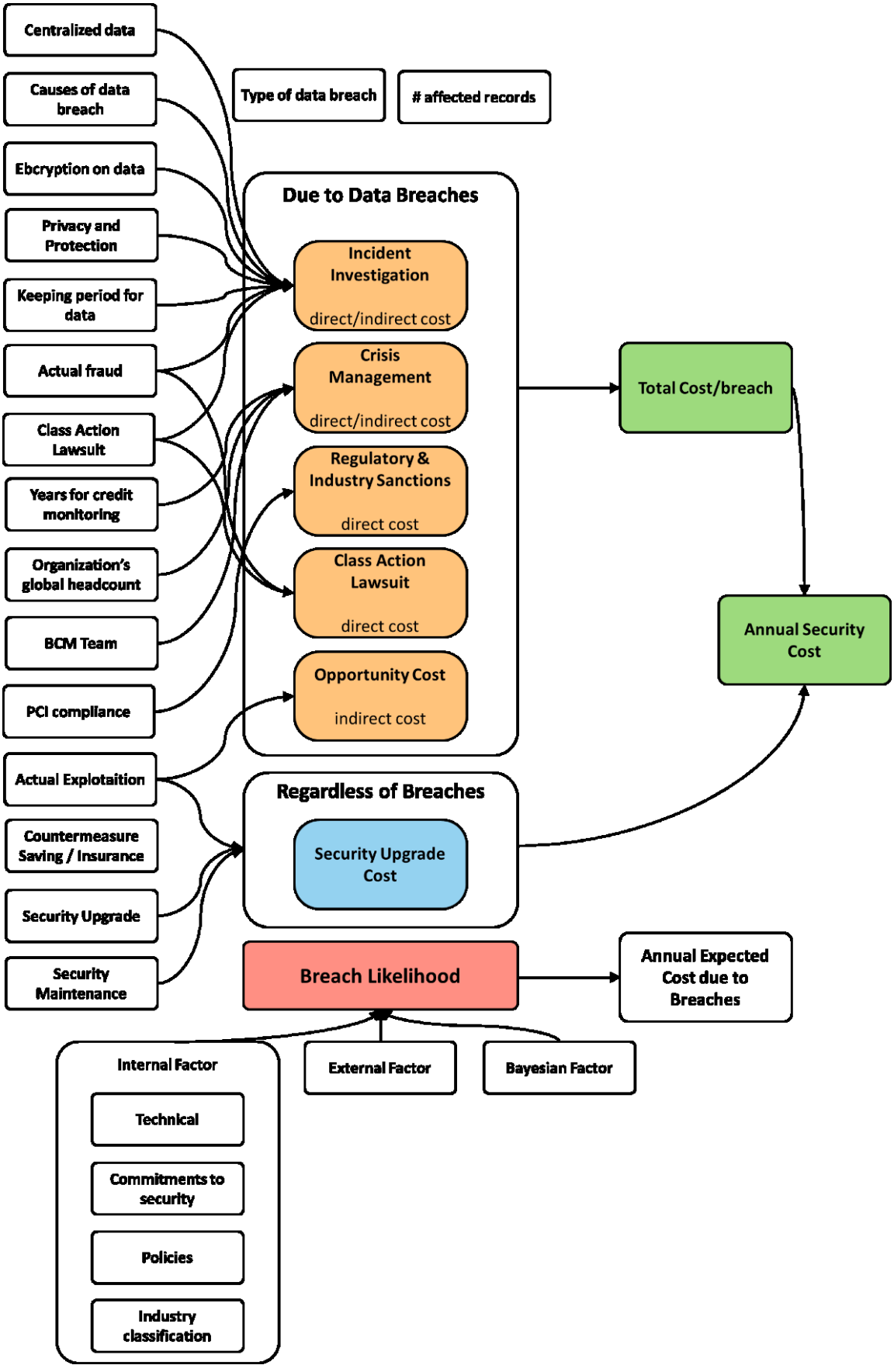


Fig. 3 – Overall risk evaluation model

In addition to the management costs due to a data breach, a company will have to make managerial and organizational choices, in order to send a message to the market and stakeholders. From this point of view Lending, Minnick and Schorno[36] conclude that

> *We also find significant responses from companies that are breached. These companies are more likely to have a change in both CEO and CTO. These changes may be due to the board seeing a need for a change in leadership or simply responding to the breached customers in a very visible manner […] There is […] an increase in the probability that the CEO and the CTO step down following the breach. Firms do make minor changes to their governance following the breach: there is a decrease in size of the board and entrenchment, which may indicate improvement in governance.*

Lending, Minnick and Schorno also point out that a company that has experienced a data breach also has long-term effects that need to be considered. In particular, they conclude their analysis by arguing that[37]:

> *While data breaches cause bad publicity to companies and negative stock returns, we also show there are long-term operational losses indicating declining customer perception. We find some evidence that poor corporate governance and environmental and community policies may increase the probability of a data breach, especially when the data is breached by hackers. […] Data breaches may be more likely in firms due to poor corporate governance leading to lack of controls or toward a specific company as a mechanism to enact change.*
> *[…] The financial impacts following the public announcement of a data breach are quite clear. While we and other researchers show negative announcement returns that indicate negative investor perception following a data breach, we also show real impacts on company revenues.*

from the point of view of revenues and stock returns/losses, they argue that[38]:

> *There is a decline in sales for nonbanks and a decline in deposits for banks from one year prior to the breach to one, two, and three years following the breach. We also find that firms with data breaches experience lower stock returns the year following the breach while efficient markets would not predict long-run stock losses, the operational declines may lead to long-run underperformance.*

[36] Lending, C., Minnick, K., & Schorno, P. J. (2018). Corporate governance, social responsibility, and data breaches. Financial Review, 53(2), 413-455.
[37] Lending, C., Minnick, K., & Schorno, P. J. (2018). Ibidem
[38] Lending, C., Minnick, K., & Schorno, P. J. (2018). Ibidem

It is evident that it is not a simple task to quantify the economic effect of a cyber incident: a widely shared framework does not yet seem to have established itself and companies can only proceed with common sense. Among the variables that make up the final effect of an accident, one that is not questionable is certainly represented by any fines.

From this point of view, it is interesting to see that between 2018 (July) and 2022 (April) the Privacy Guarantors, in the area of the GDPR, have imposed the following fines (aggregated by type of GDPR violation) as in Tab.3[39]:

	Violation	Sum of Fines
	Non-compliance with general data processing principles	**€ 815,779,144** (at 230 fines)
	Insufficient legal basis for data processing	**€ 435,961,231** (at 363 fines)
	Insufficient fulfilment of information obligations	**€ 235,791,595** (at 91 fines)
	Insufficient technical and organisational measures to ensure information security	**€ 100,312,319** (at 215 fines)
	Unknown	**€ 22,704,400** (at 6 fines)
	Insufficient fulfilment of data subjects rights	**€ 17,686,170** (at 106 fines)
	Insufficient fulfilment of data breach notification obligations	**€ 1,479,091** (at 22 fines)
	Insufficient data processing agreement	**€ 1,006,580** (at 6 fines)
	Insufficient involvement of data protection officer	**€ 350,600** (at 12 fines)
	Insufficient cooperation with supervisory authority	**€ 242,229** (at 43 fines)

Tab.3 – GDPR fines (between July 2018 and April 2022) aggregate by violation type

For the purposes of the thesis, particularly interesting are the fines relating to "*insufficient technical and organisational measures to ensure information security*" (as per art. 32 of the GDPR). This type of GDPR violation is directly related to the adoption (or failure to adopt) a suitable information management system managed by an information security structure.

[39] The following table is taken from https://www.enforcementtracker.com/?insights#violationstatistics (consultation date 23/04/2022)

1.4.2 Cost of cybersecurity in the corporate's financial statements

Cybersecurity is therefore a central topic in the management of a company: it represents a cost that must be considered and managed. It is for this reason that cybersecurity is a very relevant topic also for the CFOs: they must consider the strategies and accounting policies also in relation to this type of cost. According to the Board's Conceptual Framework for Financial Reporting[40]:

> *Expenses are decreases in economic benefits during the accounting period in the form of outflows or depletions of assets or incurrences of liabilities that result in decreases in equity, other than those relating to distributions to equity participants.*

The costs related to cybersecurity must also be considered in the preparation of the financial statements: cybersecurity therefore also becomes an important accounting topic. According to Antczak there are many kinds of costs related to cybersecurity, as in Tab. 4[41]:

INDIRECT COSTS	DIRECT COSTS
• purchasing a license for antivirus software • remuneration of cyber-security employee(s) • cyber-attack insurance policies • external data clouds • specialist advisory and legal services • costs related to data security – external drives, servers, etc. • training of employees in cyber-security	• court fees and lawyers' fees • contractual penalties • loss of money, e.g., hacking into bank accounts • costs for external parties restoring the system, data recovery • stagnation on the production line • lost value of customer relations • image loss • costs related to customer protection after stealing their data • loss of intellectual property • brand devaluation

Tab.4 – Cybersecurity direct and indirect costs (a proposal)

The costs inherent in cybersecurity must be evaluated in terms of risk and effects on the company's balance sheet. In addition to direct and indirect costs, there are also hidden costs that must be carefully evaluated by the CFO. Among the hidden costs[42]:

- *an increase in the insurance premium for buying or renewing a cyber-insurance policy,*
- *an increase in borrowing costs,*

[40] IASC's Framework for the Preparation and Presentation of Financial Statements, paragraph 70b
[41] Antczak, J. (2020). Cybersecurity Cost in an Enterprise Unit. Edukacja Ekonomistów i Menedżerów, 55(1), 82-94.
[42] Antczak, J. (2020). Ibidem

- *disruption of operations or loss of data,*
- *lost value of customer relations,*
- *value of lost revenues from contracts,*
- *brand devaluation – a devaluation of a trade name is a category of intangible costs related to the impairment of names, signs or symbols used by an organisation to distinguish its products and services,*
- *loss of intellectual property – the loss of IP is an intangible cost associated with the loss of sole control of trade secrets, copyrights, investment plans and other proprietary as well as confidential information that may lead to the loss of competitive advantage, the loss of revenue and permanent as well as potentially irreparable economic damage to the company.*

In order to reflect the cybersecurity cost on the corporate balance sheet, Antczak proposes the classification as in Tab. 5[43]:

Costs of cyber threats	Types of risks	Entry in the books
Costs related to the theft or phishing of confidential information for the purpose of using it to the detriment of the business entity.	• theft of identity, employee data • offensive and illegal content incidents involving employees or individuals • breach of security access within the system • computer hacking – bypassing system security and gaining unauthorised access to the information of a business entity • computer eavesdropping – unauthorised interception of all information of a business entity in cyberspace	• included in operating costs • presented in the profit and loss account
Costs related to destruction, damage to the property and information.	• unlawful damage, destruction or deletion of information, e.g., attacks using malicious virus software • hardware and software destruction • disruption of automatic information processing • computer sabotage – disrupting or paralysing the functioning of information system in an economic entity	• included in other operating costs • presented in the profit and loss account
Costs of litigation related to cybercrime.	• payment of a fee for hiring a law firm to write a statement of claim	• included in other operating costs or release of the provision (accrued expenses) • presented in the income statement or balance sheet
Costs of measures taken to protect against cybercrime.	• insurance policies • antivirus programs • remuneration of an employee responsible for cyber security	• included in the costs of basic operating activity or prepayments • presented in the income statement or balance sheet

Tab.5 – The effect of cyber threats' cost on balance sheet

[43] Antczak, J. (2020). Idem

Antczak[44] concludes the analysis sustaining that:

> *Costs related to cyber-security constitute a new category in the management of an entity at the accounting, both financial and management level, starting with the recognition of their accounts, then presentation in the statements to a significant category in the entity's management process.*

[44] Antczak, J. (2020). Idem

1.5 Phenomenon background summary

Information Security is a global phenomenon with significant macroeconomics impact and relevant effect for sovereign states, institutions, corporates and natural persons.

Cyber and Information security is a relatively new area and suffer from scarce interdisciplinary contamination and limited definition standardization (for example in the concept of cyber risk) which makes it difficult to approach the issue in a comprehensive and systemic way. These limitations generate limited awareness of the issue, of its repercussions on each individual, on corporates, on the country system and, in general, on the world-wide economic and social system.

Cyber and Information security are disciplinary fields that arise, in an extremely vertical way, from technological issues with technological point of view.

The technological aspects, although central, represent only a small part of the problem: cyber and information security require an organic and holistic approach taking into consideration non-technological dimensions such as, for example, the behavior and awareness of people and companies.

The issue is broad and, unfortunately, approached in a fragmented and non-organic way. Within a company, the organizational aspects (who, with what skills and with what responsibilities) and management (through which policies, procedures, … a company intends to pursue its objectives) take on prominence.

Best-practices and standards grow independently but their development, adoption and understanding are still affected by a limited multidisciplinary overview: some standards start to try to approach the problem considering all corporate layers (e.g. focusing also on HR layer) but the whole compliance needs are not evaluated as an unique, creating discrepancies and asymmetries between management systems created for different and mandatory reason.

With reference to corporates, Cyber and Information Security

(1) concerns technological, organizational, management and control layers,
(2) involves many different stakeholders (e.g. employees, collaborators, suppliers, …), and

(3) depends on many factors such as a full understanding of cybercrime phenomenon, risk awareness and corporate risk appetite, corporate culture, corporate commitment and accountability, technological threats and protections, human behavior, policies and procedures, ….

Consistent with these premises, a company should develop its cybersecurity program, in a suitably integrated way with respect to other areas of compliance and legal obligations.

This activity is difficult to do both (1) because companies are often complex and making changes requires many resources (as well as an active desire for change) and (2) because neither scientific literature nor business practices still address the problem of cyber and information security in an integrated way.

The challenge for the future is inevitably the creation of a compliance management system that (1) integrates each potentially relevant layer and (2) considers every type of regulatory compliance that companies must comply with.

2. Research questions and methodology

In the thesis are explored the themes of Information Security organization and management through a non-systematic scientific literature review inherent in (1) risk awareness, (2) corporate organizational culture, (3) human factor, (4) internal policies role, (5) organizational duties, competences, hierarchy, (6) management system.

The thesis' research questions are

- RQ.1 - How does the human factor affect information security?
- RQ.2 - What is meant by IS from an organizational and management point of view?
- RQ.3 - Which frameworks best reconcile the "human factor" with the organizational and management dimensions?
- RQ.4 - Basic principles can be distilled to define an abstract organizational and management model?

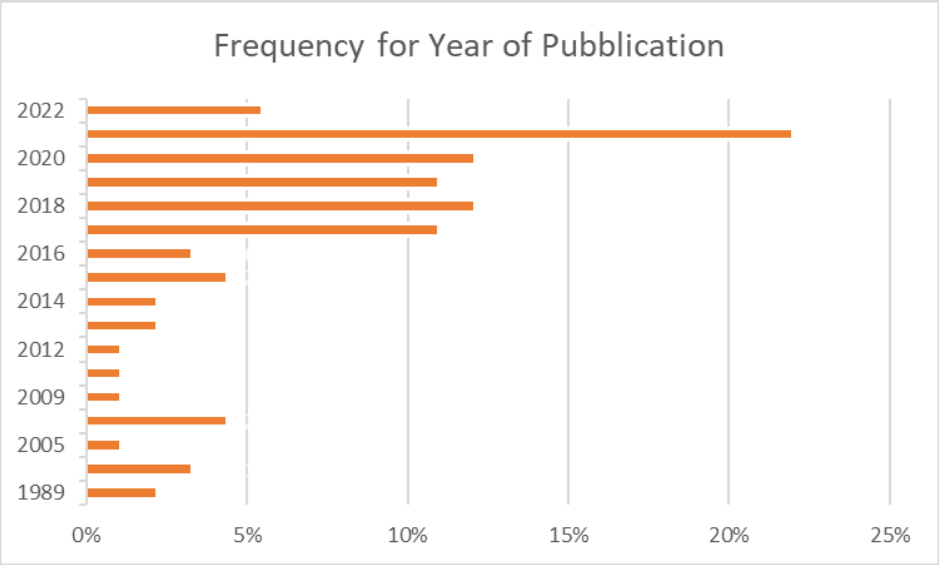
In order to answer the research questions was conducted a non-systematic scientific literature review.

The review was conducted by interrogating EBSCO discovery service

- during the period April - August 2022,
- using the keywords "data security", "data breach", "cyber security", "cyber risk", "information security", "IT security", "cyber governance", "CISO structure", "CISO department", "ISO 27001", "Information security management system", "cyber security awareness", "human factor cyber",
- search time range 1989 – 2022.

The search produced 510 results and among these, after an analysis of the abstracts, 77 bibliographic sources were investigated.

This set of bibliographic sources have the following frequency per year:



The set of 77 bibliographic sources consists in:

1	Algarni, A. M., & Malaiya, Y. K. (2016, May). A consolidated approach for estimation of data security breach costs. In 2016 2nd International Conference on Information Management (ICIM) (pp. 26-39). IEEE.	x
2	Allen, J. H., Crabb, G., Curtis, P. D., Fitzpatrick, B., Mehravari, N., & Tobar, D. (2015). Structuring the chief information security officer organization. CARNEGIE-MELLON UNIV PITTSBURGH PA PITTSBURGH United States, (pp. 1-33).	x
3	Amin, Z. (2019). A practical road map for assessing cyber risk. Journal of Risk Research, 22(1), 32-43.	x
4	Antczak, J. (2020). Cybersecurity Cost in an Enterprise Unit. Edukacja Ekonomistów i Menedżerów, 55(1), 82-94.	x
5	Badhwar, R. (2021). Simplified Approach to Calculate the Probability of a Cyber Event. In The CISO's Next Frontier (pp. 353-359). Springer, Cham.	x
6	Banga, G. (2020). Why is cybersecurity not a human-scale problem anymore? Communications of the ACM, 63(4), 30-34.	
7	Berners-Lee, T. J. (1989). Information management: A proposal (No. CERN-DD-89-001-OC).	x
8	Boehmer, W. (2008, August). Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001. In 2008 Second International Conference on Emerging Security Information, Systems and Technologies (pp. 224-231). IEEE.	x
9	Boehmer, W. (2009, March). Cost-benefit trade-off analysis of an ISMS based on ISO 27001. In 2009 International Conference on Availability, Reliability and Security (pp. 392-399). IEEE.	x
10	Cellerini, E. J., & Lang, C. (2018). Cyber Liability: Data Breach in Europe. Defense Counsel Journal, 85(3), 1-6.	
11	Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2020). Maximizing Employee Compliance with Cybersecurity Policies. MIS Quarterly Executive, 19(3), 183-198.	x
12	Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. The Geneva Papers on Risk and Insurance-Issues and Practice, 1-39.	
13	Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. The TQM Journal.	
14	Dalal, R. S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S. J., & Brummel, B. J. (2022). Organizational science and cybersecurity: abundant opportunities for research at the interface. Journal of business and psychology, 37(1), 1-29.	
15	Daneshmandnia, A. (2019). The influence of organizational culture on information governance effectiveness. Records Management Journal, 29(1/2), 18-41.	x
16	Deane, J. K., Goldberg, D. M., Rakes, T. R., & Rees, L. P. (2019). The effect of information security certification announcements on the market value of the firm. Information Technology and Management, 20(3), 107-121.	x
17	Dhillon, G., Smith, K., & Dissanayaka, I. (2021). Information systems security research agenda: Exploring the gap between research and practice. The Journal of Strategic Information Systems, 30(4), 101693.	
18	Dieye, R., Bounfour, A., Ozaygen, A., & Kammoun, N. (2020). Estimates of the macroeconomic costs of cyber-attacks. Risk Management and Insurance Review, 23(2), 183-208.	x
19	Dupuis, M., & Renaud, K. (2021). Scoping the ethical principles of cybersecurity fear appeals. Ethics and Information Technology, 23(3), 265-284.	
20	Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? European Journal of Operational Research, 272(3), 1109-1119.	

21	Eoyang, M., & Keitner, C. (2020). Cybercrime vs. Cyberwar: Paradigms for Addressing Malicious Cyber Activity. J. Nat'l Sec. L. & Pol'y, 11, 327.	
22	Etges, R., & Sutcliffe, E. (2008). An overview of transnational organized cyber crime. Information Security Journal: A Global Perspective, 17(2), 87-94.	x
23	Eun, Y. S., & Aßmann, J. S. (2016). Cyberwar: Taking stock of security and warfare in the digital age. International Studies Perspectives, 17(3), 343-360.	x
24	Fahey, E. (2014). The EU's cybercrime and cyber-security rulemaking: mapping the internal and external dimensions of EU security. European Journal of Risk Regulation, 5(1), 46-60.	
25	Fidler, B. (2017). Cybersecurity governance: a prehistory and its implications. Digital Policy, Regulation and Governance.	
26	Franke, U. (2020). IT service outage cost: case study and implications for cyber insurance. The Geneva Papers on Risk and Insurance-Issues and Practice, 45(4), 760-784.	
27	Govender, S. G., Kritzinger, E., & Loock, M. (2021). A framework and tool for the assessment of information security risk, the reduction of information security cost and the sustainability of information security culture. Personal and Ubiquitous Computing, 25(5), 927-940.	x
28	Grobler, J. (2018). Cyber risk from a chief risk officer perspective. Journal of Risk Management in Financial Institutions, 11(2), 125-131.	x
29	Gwebu, K. L., Wang, J., & Wang, L. (2018). The role of corporate reputation and crisis response strategies in data breach management. Journal of Management Information Systems, 35(2), 683-714.	
30	Inskeep, T. (2019). "How to Properly Position the CISO for Success", SecurityMagazine.com, 37.	x
31	Kappers, W. M., & Harrell, M. N. (2020). From Degree to Chief Information Security Officer (CISO): A Framework for Consideration, 22(11), 260-288	x
32	Karanja, E. (2017). The role of the chief information security officer in the management of IT security. Information & Computer Security.	
33	Karanja, E., & Rosso, M. A. (2017). The chief information security officer: An exploratory study. Journal of International Technology and Information Management, 26(2), 23-47.	
34	Kaspersky (2017), "The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within," Kaspersky daily, (https://www.kaspersky.com/blog/the-human-factor-in-it-security)	x
35	Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity Awareness Framework for Academia. Information, 12(10), 417.	x
36	King, Z. M., Henshel, D. S., Flora, L., Cains, M. G., Hoffman, B., & Sample, C. (2018). Characterizing and measuring maliciousness for cybersecurity risk assessment. Frontiers in Psychology, 9, 39.	x
37	Kobis, P. (2021). Human factor aspects in information security management in the traditional IT and cloud computing models. Operations Research and Decisions, 31, 61-76.	x
38	Kobis, P., & Karyy, O. (2021). Impact of the human factor on the security of information resources of enterprises during the COVID-19 pandemic. Polish Journal of Management Studies, 210-227.	
39	Kovalchuk, O., Shynkaryk, M., & Masonkova, M. (2021, September). Econometric Models for Estimating the Financial Effect of Cybercrimes. In 2021 11th International Conference on Advanced Computer Information Technologies (ACIT) (pp. 381-384). IEEE.	
40	Kruse II, W. G., & Heiser, J. G. (2001). Computer forensics: incident response essentials. Pearson Education, London.	x
41	Kshetri, N. (2010). Diffusion and effects of cyber-crime in developing economies. Third World Quarterly, 31(7), 1057-1079.	
42	Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. Neural Computing and Applications, 1-31.	x
43	Kweon, E., Lee, H., Chai, S., & Yoo, K. (2021). The utility of information security training and education on cybersecurity incidents: an empirical evidence. Information Systems Frontiers, 23(2), 361-373.	
44	Lankton, N., Price, J. B., & Karim, M. (2021). Cybersecurity Breaches and the Role of Information Technology Governance in Audit Committee Charters. Journal of Information Systems, 35(1), 101-119.	
45	Lee, C. S., Choi, K. S., Shandler, R., & Kayser, C. (2021). Mapping global cyberterror networks: an empirical study of al-Qaeda and ISIS cyberterrorism events. Journal of Contemporary Criminal Justice, 37(3), 333-355.	x
46	Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. Business Horizons, 64(5), 659-671.	x
47	Lending, C., Minnick, K., & Schorno, P. J. (2018). Corporate governance, social responsibility, and data breaches. Financial Review, 53(2), 413-455.	x
48	Li, J. X. (2017). Cyber crime and legal countermeasures: A historical analysis. International Journal of Criminal Justice Sciences, 12(2), 196-207.	x
49	Lipner, S. B. (2015). The birth and death of the orange book. IEEE Annals of the History of Computing, 37(2), 19-31.	x
50	Liu, P., Turel, O., & Bart, C. (2019). Board IT governance in context: Considering governance style and environmental dynamism contingencies. Information Systems Management, 36(3), 212-227.	
51	Lopes, I. M., Guarda, T., & Oliveira, P. (2019, June). How ISO 27001 can help achieve GDPR compliance. In 2019 14th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-6). IEEE.	x

52	Makridis, C., & Dean, B. (2018). Measuring the economic effects of data breaches on firm outcomes: Challenges and opportunities. Journal of Economic and Social Measurement, 43(1-2), 59-83.	
53	Mamonov, S., & Peterson, R. (2021). The role of IT in organizational innovation–A systematic literature review. The Journal of Strategic Information Systems, 30(4), 101696.	
54	Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. Journal of Marketing, 81(1), 36-58.	
55	Meisner, M. (2017). Financial consequences of cyber attacks leading to data breaches in healthcare sector. Copernican Journal of Finance & Accounting, 6(3), 63-73.	**x**
56	Moore, R. (2014). Cybercrime: Investigating high-technology computer crime. Routledge, London	**x**
57	Morrison, A., Kumar, G. (2018) "Corporate Boards May Be More Likely Than Regulators to Scrutinize Cybersecurity Program Effectiveness This Year", Journal of Health Care Compliance, 49-52.	**x**
58	Neal, R. (2008). Service-oriented security architecture and its implications for security department organization structures. Information Security Journal: A Global Perspective, 17(4), 188-200.	
59	Ngwenya, C., & Njenga, K. (2021). Evolving Information Security Governance Practices from Evolving Technologies: Focus on Covid-19 Lockdowns. The African Journal of Information Systems, 13(3), 3.	
60	Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. HOLISTICA–Journal of Business and Public Administration, 9(3), 71-88.	**x**
61	Palsson, K., Gudmundsson, S., & Shetty, S. (2020). Analysis of the impact of cyber events for cyber insurance. The Geneva Papers on Risk and Insurance-Issues and Practice, 45(4), 564-579.	
62	Parker, D. B. (1989). Computer Crime: Criminal Justice Resource Manual.	**x**
63	Poyraz, O. I., Canan, M., McShane, M., Pinto, C. A., & Cotter, T. S. (2020). Cyber assets at risk: monetary impact of US personally identifiable information mega data breaches. The Geneva Papers on Risk and Insurance-Issues and Practice, 45(4), 616-638.	
64	Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. International Management Review, 13(1), 10.	**x**
65	Richardson, R., Hiatt, M., Lowman, G. H., Napshin, S., & Perros, Y. (2021). Pay Rate Differentials. International Management Review, 17(2), 129-148.	**x**
66	Richardson, V. J., Smith, R. E., & Watson, M. W. (2019). Much ado about nothing: The (lack of) economic impact of data privacy breaches. Journal of Information Systems, 33(3), 227-265.	
67	Rios Insua, D., Couce-Vieira, A., Rubio, J. A., Pieters, W., Labunets, K., & G. Rasines, D. (2021). An adversarial risk analysis framework for cybersecurity. Risk Analysis, 41(1), 16-36.	
68	Ryczyński, J. (2019). Human factor as a determinant of reliability and safety of technical systems. Journal of KONBiN, 49(3), 195-220.	**x**
69	Schuetz, S. W., Benjamin Lowry, P., Pienta, D. A., & Bennett Thatcher, J. (2020). The effectiveness of abstract versus concrete fear appeals in information security. Journal of Management Information Systems, 37(3), 723-757.	
70	Shojaie, B., Federrath, H., & Saberi, I. (2014, September). Evaluating the effectiveness of ISO 27001: 2013 based on Annex A. In 2014 Ninth International Conference on Availability, Reliability and Security (pp. 259-264). IEEE.	
71	Smit, R., van Yperen Hagedoorn, J., Versteeg, P., & Ravesteijn, P. (2021). The Soft Skills Business Demands of the Chief Information Security Officer. Journal of International Technology and Information Management, 30(4), 41-59.	**x**
72	Sophos Whitepaper. April 2021, The State of Ransomware 2021	**x**
73	Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. Accounting, Organizations and Society, 71, 15-29.	
74	Strupczewski, G. (2021). Defining cyber risk. Safety science, 135, 105143, 1-10.	**x**
75	Venkatraman, S., MK Cheung, C., Lee, Z. W., D. Davis, F., & Venkatesh, V. (2018). The "Darth" side of technology use: an inductively derived typology of cyberdeviance. Journal of Management Information Systems, 35(4), 1060-1091.	
76	Weidman, J., & Grossklags, J. (2019). Assessing the current state of information security policies in academic organizations. Information & Computer Security, 28(3), 423-444.	**x**
77	Woods, D. W., & Weinkle, J. (2020). Insurance definitions of cyber war. The Geneva Papers on Risk and Insurance-Issues and Practice, 45(4), 639-656.	**x**

Following an initial analysis of the above bibliography, the sources indicated with an "**x**" have been investigated in deep. The other sources were excluded because they appeared (1) redundant, (2) inherent econometric-mathematical modelling of the problem (out of scope approach), (3) in my opinion uninteresting for research questions.

The final set of bibliographic sources is composed of 43 sources and can be divided into five main scientific sub-areas:

- definitions of cyber and information security problem,
- economic effects of cyber and information security events,
- individual and corporate culture and awareness,
- organization of cyber and information security (roles, responsibilities, competences, ...),
- management system of cyber and information security (policies, procedures, controls, …).

The review does not exhaust the complexity of the topic but the sources used seem to provide sufficient elements to frame the issue from an (1) organizational and (2) management point of view.

3. Information Security (IS) Governance and Management

The approach to cyber and information security has changed over time and it is still undergoing transformation[45]:

- originally it was believed that all possible causes of an accident could be foreseen and that the realization of an accident was an individual fault,
- subsequently the uncertainty deriving from not being able to foresee all the possibilities was accepted and a systemic vision began to develop, framing the individual dimension in an organizational context,
- the most recent developments pay increasing attention not only to the organizational context but also to its interconnections with the social system, moving towards an approach that is not only preventive but also reactive (the so-called resilience) with respect to the certainty that a negative event could always happen.

The path summarized above originates from the necessary awareness of a complex and multidisciplinary problem.

3.1 Risk awareness

The first step in dealing with a risk is to be aware of it, identifying it and estimating its relevance by means of its probability of realization and the impact that this would cause.

In the previous chapter we saw that cyber risk does not have a univocal definition and that the concept of risk changes according to the context in which it is considered.

In any case, companies must try to define cyber risks trying, in the most complete way, to identify them also from the point of view of regulatory compliance, in order to reach an integrated risk assessment methodology.

[45] Kaur, M., van Eeten, M., Janssen, M., Borgolte, K., & Fiebig, T. (2021). Human factors in security research: Lessons learned from 2008-2018. arXiv preprint arXiv:2103.13287.

According to Amid[46], it is essential to provide the competent bodies (e.g. risk management committee, executive committee, …) with a suitable roadmap aimed at assessing exposure to risks and resilience capabilities.

Amid identifies three stages:

> *(1) Phase I begins with the identification of where the organization is today in terms of cyber security. Cyber risk is heavily dependent on the specific nature of the organization and is closely linked to its cyber resilience. Thus, this step requires an understanding of the cyber security environment of the organization, its ability to prevent incidents, detect attacks, contain and respond to identified attacks, mitigate and recover from disruptions.*
>
> *(2) Where the organization needs to be in the future in terms of cyber security is identified in Phase II. What sort of cyber management culture does the organization wish to establish and what level of cyber resilience does the organization need to develop.*
>
> *(3) In this step (Phase III), we draw the route from where the organization is now to where it should be in the future. In this step, we provide the models to be used in assessing the full potential magnitude of cyber risks and its financial impacts on the company and in comparing and assessing alternative mitigation strategies.*

Risk assessment must necessarily be multidimensional and must include the dimensions that ontologically (G. Strupczewski, ibidem) define the concept of cyber risk.

It is not an easy job and, to date, cyber risk is assessed in many different ways vertically with respect to the scope of compliance analyzed.

The issue should, therefore, be addressed from different points of view through a multidisciplinary approach, in order to evaluate cyber-issues probability and, in particular, its business impact.

Badhware[47] suggests the typical risk formula:

$$Cyber\ Risk = Cyber\ Event\ Probability * Business\ Impact$$

[46] Amin, Z. (2019). A practical road map for assessing cyber risk. Journal of Risk Research, 22(1), 32-43.

[47] Badhwar, R. (2021). Simplified Approach to Calculate the Probability of a Cyber Event. In The CISO's Next Frontier (pp. 353-359). Springer, Cham.

emphasizing that the probability and the impact are not easy to determinate for a Company "*and requires extremely good self-visibility into*":

> *(a) Its technology debt (i.e., how current the technology stack is), including but not limited to all the vulnerabilities and weaknesses that may exist in its high-risk, external-facing and internal applications and systems,*
>
> *(b) Maturity of its (cyber) security stack and its incident response capability,*
>
> *(c) Data security, including but not limited to encryption and masking of its sensitive data,*
>
> *(d) The impact a cyber-event may cause to the processes and procedures used to conduct business for a given line of business […],*
>
> *(e) Its disaster recovery and business resilience capability,*
>
> *(f) Its reputational risk (depending upon the nature of the business and past track record),*
>
> *(g) Third-party and supply chain risk,*
>
> *(h) Its cyber adversaries or threat vectors including but not limited to insider threats.*

Badhware proposes an approach to determinate the Cyber Event Probability:

Cyber Event Probability (CEP) =

*Risk Score (rs) * Threat Score (ts) * Defensive Score (ds)*

where:

- *rs is assigned to each application or system. It encompasses the risk from vulnerabilities, currency (N-?), exploitability and occurrence of vulnerabilities, and other security issues such as data and network security that increase the risk of application, system, or network breaches. […]*
- *ts is assigned to each application or system. It measures the risk from advanced malware, sophisticated threat actors, or malicious entities (e.g., criminals, nation states), and other forms of advanced persistent threat, and insider threat. […]*
- *ds is assigned to each application and system, measures a range of defense related capabilities: countermeasures deployment against malware and other advanced threats, as well as insider threat; monitoring and mitigating controls deployment; the hiring of educated and well-trained cyber security professionals[…].*

Badhware supposes these standard ranges:

- rs: 1 (Critical), 0.7 (High), 0.5 (Medium), 0.1 (Low)
- ts: 1 (Advanced), 0.7 (High), 0.5 (Medium), 0.2 (Low)

- ds: 0.5 (Excellent), 0.6 (Good), 0.5 (Medium), 0.8 (Poor), 0.9 (None)

According to Badhware, the final CEP for an entire IT ecosystem is:

$$CEP = \sum_{x=1}^{x=n} \frac{rs(x)}{x} * \sum_{x=1}^{x=n} \frac{ds(x)}{x} * \sum_{x=1}^{x=n} \frac{ts(x)}{x}$$

Badhware doesn't approach the estimation of business impact, much more complex to determinate: corporate should consider every possible effect, quantifying them as financial outflow.

Among the possible effects, as seen in the previous chapter, there are those of compliance, reputational, technical costs, ...

The assessment of cyber risk, and its subsequent management, is a complex issue that does not only concern technological aspects.

Many standards have tried to define frameworks for cyber risk assessment and management. For example: ISO 31000 stresses that any risk assessment must consider the business context, ISO 27005 proposes a risk prioritization approach based on sensitive processes, ISO 27001 defines information security management controls, NIST 800-29 introduces a holistic approach to cyber risk assessment.

In this context, Kure, Islam, and Mouratidis propose an integrated cyber security risk management framework as in Fig. 4[48]

[48] Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. Neural Computing and Applications, 1-31.

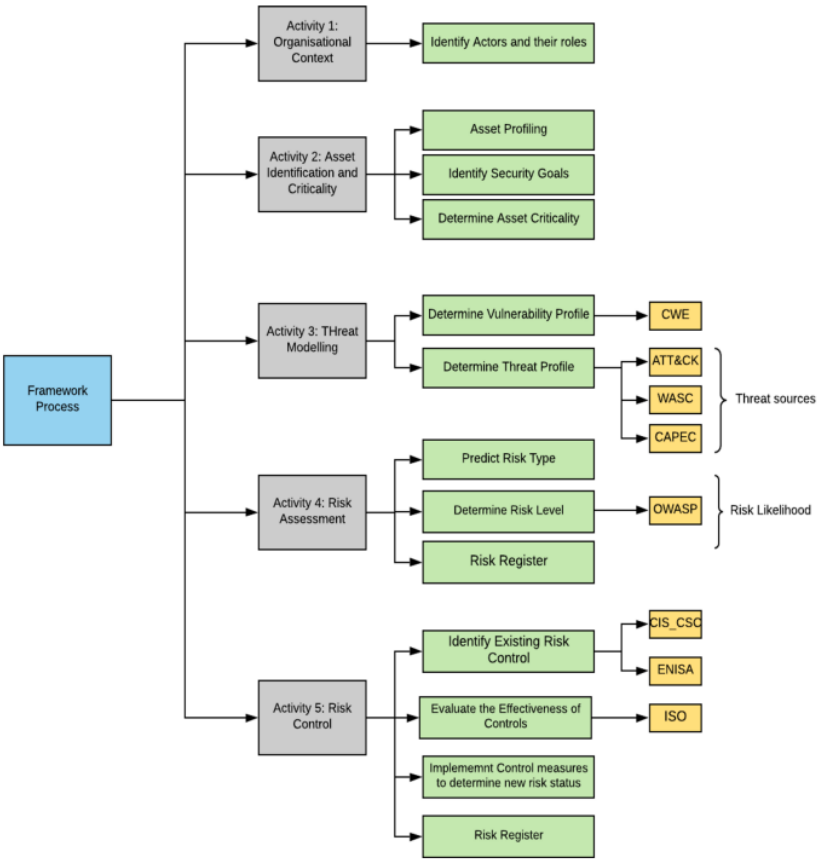


Fig. 4 – Integrated cyber security risk management framework

where:

> *Activities 1 and 2 focus on the context of the risk assessment and in particular an organisation's scope. This helps to gain a comprehensive understanding of supported assets, functions, goals and essential security requirements. Activity 3 gathers vulnerability and threat information from multiple sources through various means, to address vulnerabilities protect assets and respond to threats. Activity 4 determines the risk level and provides a risk register with the previous activities' data. Activity 5 implements control measures and evaluate the effectiveness of the existing control.*

Approaching the estimation of risk presupposes, which is not to be taken for granted, an already matured abstract awareness of the risk itself. Awareness is a real project that every company must develop.

Khader, Karam and Fares[49] describe same best practices in order to create security awareness about cyber risks:

- *Build an institution-wide culture and participation where decision-making and application of cybersecurity best practices become daily pursuits for end-users at all levels,*
- *Clearly communicate to upper-level management and all end-users that it is critical to understand the value and purpose of cybersecurity education before implementing training,*
- *Gauge program success by conducting a comparative study to see if there is a reduction in institutional employee-driven cybersecurity incidents over time,*
- *Conduct regular, ongoing assessments and training so that end-users are given the benefit of regular cybersecurity education, and the opportunity to learn over time and develop new skills,*
- *Create a clear link between assessments and training,*
- *Maintain awareness of cybersecurity best practices for end-users by revisiting topics on a regular basis and incorporating ongoing awareness activities; without reinforcement, the institution must regularly rebuild rather than build upon,*
- *Be consistent in tracking and reporting progress,*
- *Keep the end-user motivated and engaged by applying gamification techniques that use rewards and positive reinforcement to raise end-user interest and participation and elevate the effectiveness of your program.*

From these premises, Khader, Karam and Fares propose a cybersecurity awareness framework as in Fig. 5[50]:

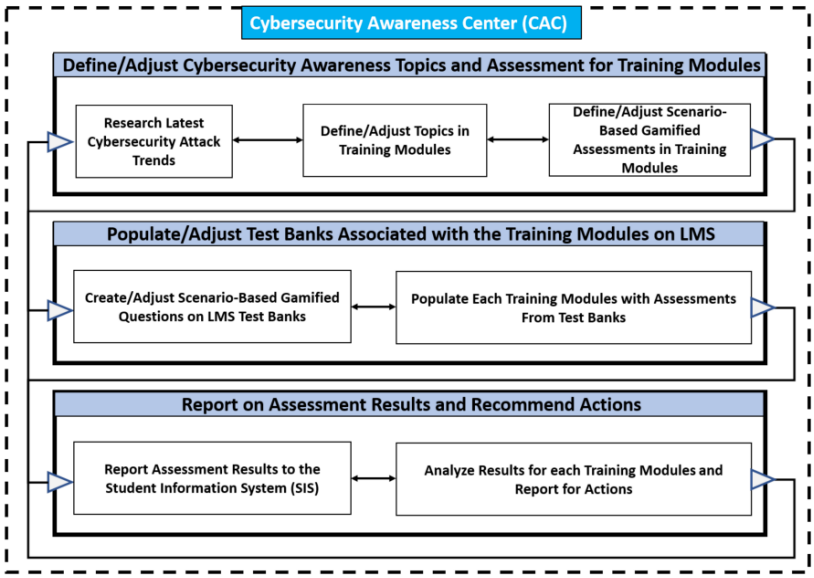


Fig.5 – Cybersecurity awareness framework

[49] Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity Awareness Framework for Academia. Information, 12(10), 417.
[50] Khader, M., Karam, M., & Fares, H. (2021). Idem

Consistently with the works analyzed, Lee[51] believes that cyber risk management must focus on both technological and human aspects, approached in a holistic way.

In particular, Lee proposes a cyber risk management framework, not a substitute but supplementary to the globally frameworks (e.g. NIST, ISO 27k, COBIT, ...), as in Fig. 6[52]:

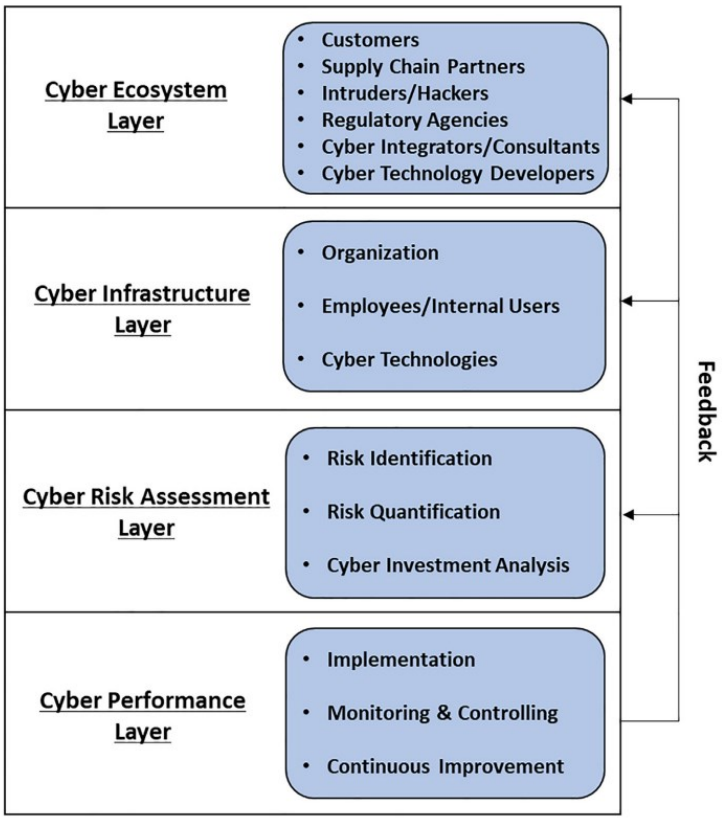


Fig. 6 – Cyber risk management framework

From these premises, Lee[53] argues that:

> *The organization is responsible for identifying the need for cyberacquisition and the best technology to meet that need. By prioritizing technologies that improve cybersecurity protection, organizations can reduce the consequences of cybercrime and unlock future economic value as higher levels of trust encourage more business from customers [...]. We must keep the basic tenet of the four-layer framework in mind. If we want to make a sound justifiable*

[51] Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. Business Horizons, 64(5), 659-671.
[52] Lee, I. (2021). Idem
[53] Lee, I. (2021). Idem

cyberinvestment to protect our IT assets and services from threats, then we need to address each layer appropriately. We must:

1. *Understand our external environment through the cyber ecosystem layer,*
2. *Evaluate the organization, employees/internal users, and existing cybertechnologies through the cyberinfrastructure layer,*
3. *Assess cyber risks through the cyber risk assessment layer, and*
4. *Conduct cybersecurity activities at the cyber performance layer.*

All the four layers are strongly intertwined and referenced to the cyber risk management framework so that holistic cyber risk management is achieved.

Knowing the risks is mandatory as well as making executive managers aware and informed through adequate analyzes and informing all employees through adequate training. Every company must introduce an approach for creating the necessary awareness.

Lastly, the definition and awareness of the risk described so far is inherent to the so-called "second level of control" (e.g. corporate Compliance functions)[54]. It is interesting to see that even the so-called "third level of control" (e.g. audit functions) have developed specific methodologies for the assessment of cyber risks. This arises, in particular, from the requirements of the Sarbanes Oxley Act (section 404) which determine the need to evaluate the effect of the failure of IT controls and IT security measures that can lead to significant failures in business controls with possible repercussions on the reliability of the financial statements. The topic will not be explored in depth, but it is interesting to show the principles of the GAIT (Guide to the Assessment of IT Risk, supplemental guidance to IPPF[55]) methodology developed by the IIA (The Institute of Internal Auditors):

1. *The identification of risks and related controls in IT general control processes (e.g., in change management, deployment, access security, operations) should be a continuation of the top-down and risk based approach used to identify significant accounts, risks to those accounts, and key controls in the business processes,*
2. *The IT general control process risks that need to be identified are those that affect critical IT functionality in financially significant applications and related data,*

[54] Committee of Sponsoring Organizations of the Treadway Commission (2013), Internal Control. Integrated Framework.

[55] International Standards for the Professional Practice of Internal Auditing (IPPF Standards)

3. *The IT general control process risks that need to be identified exist in processes and at various IT layers: application program code, databases, operating systems, and network,*
4. *Risks in IT general control processes are mitigated by the achievement of IT control objectives, not individual controls.*

[…]

In short, the GAIT methodology guides you through asking three questions in sequence:

1. *What IT functionality in the financially significant applications is critical to the proper operation of the business process key controls that prevent/detect material misstatement (i.e., what is the critical IT functionality)?*
2. *For each IT process at each layer in the stack, is there a reasonable likelihood that a process failure would cause the critical functionality to fail — indirectly representing a risk of material misstatement (i.e., if that process failed at that layer, what effect would there be on the critical functionality? Would it cause the functionality to fail such that there would be a reasonably likely risk of material misstatement)?*
3. *If such ITGC (IT General Control) process risks exist, what are the relevant IT control objectives (i.e., what IT control objectives need to be achieved to provide assurance over the critical functionality)?*

This approach makes it possible to establish the risk-based priorities of the audits to be carried out in order to create an Auditplan compliant with the Sarbanes Oxley regulation.

The next steps are (1) the adequate assignment of organizational roles and responsibilities in order to assign suitable, clear and formal (e.g. through proxies and powers of attorney) accountability to all organizational levels (employees, middle-management, directors, executives), (2) the introduction of an understandable, simple and robust internal rules system, duly empowered by competent body and based on the organizational culture.

3.2 Organizational culture, the "human factor" and the role of internal policies

Cyber security and information security are, first of all, dependent on organizational culture and individual behavior. Cram, Proudfoot and D'Arcy[56] argue that:

> *Although deploying technical solutions to "lock down" systems and data provides an important form of defense, it is well established that humans are the weakest link in cybersecurity.*

According to Kaspersky[57] the top three cybersecurity issues originate from human behaviors, in particular:

> *1) inappropriate sharing of data via mobile devices,*
> *2) physical loss of mobile devices exposing organizations to risk, and*
> *3) inappropriate IT resource use by employees.*

Organizational culture is fundamental for driving human behaviors and for the effectiveness of information governance. According to Daneshmandnia[58] information governance starts and concerns:

- *promotion of technique (technological and organizational innovations),*
- *identification of risks according to key players (stakeholders, CIO, etc.), and*
- *employment of rules to govern information practices as they correspond with internal and external guidelines.*

This complexity must be governed from several points of view, starting from a coherent corporate culture and a system of published, recognized, used and controlled rules, through audit activities, e.g. policies, procedures, … managed by a robust organization structure with suitable accountability, duly empowered.

Ryczynski identifies these corporate factors that influence cyber incidents as in Fig. 7[59]:

---

[56] Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2020). Maximizing Employee Compliance with Cybersecurity Policies. MIS Quarterly Executive, 19(3), 183-198.

[57] Kaspersky (2017), "The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within," Kaspersky daily, (https://www.kaspersky.com/blog/the-human-factor-in-it-security)

[58] Daneshmandnia, A. (2019). The influence of organizational culture on information governance effectiveness. Records Management Journal, 29(1/2), 18-41.

[59] Ryczyński, J. (2019). Human factor as a determinant of reliability and safety of technical systems. Journal of KONBiN, 49(3), 195-220.

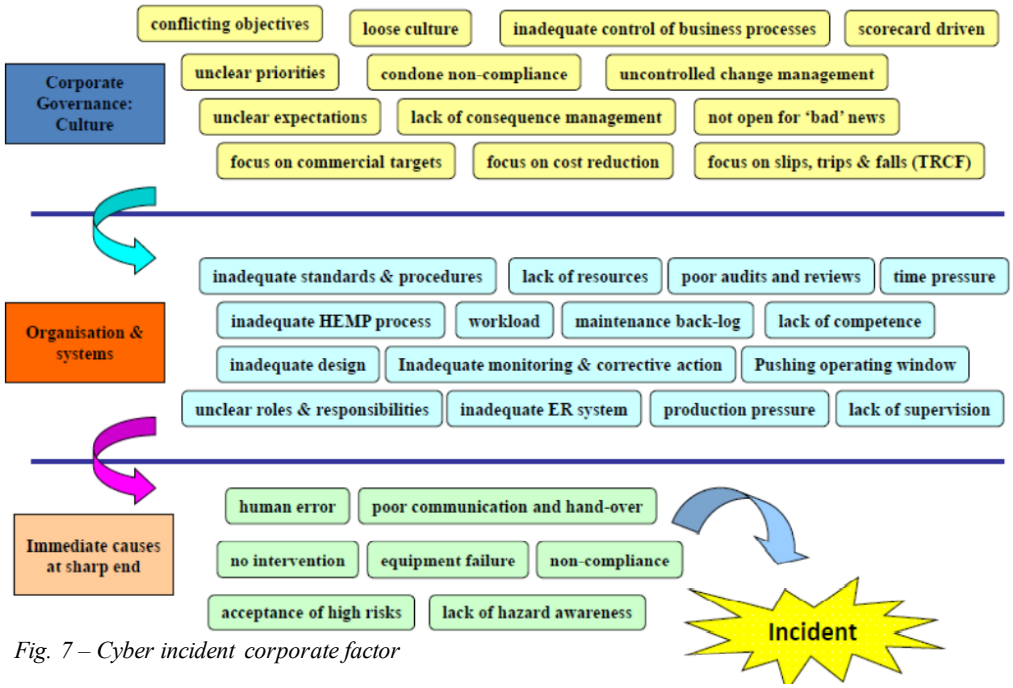


Fig. 7 – Cyber incident corporate factor

King, Henshel, Flora, Cains, Hoffman and Sample, in particular, propose a Human Factors Framework as in Fig. 8[60]:

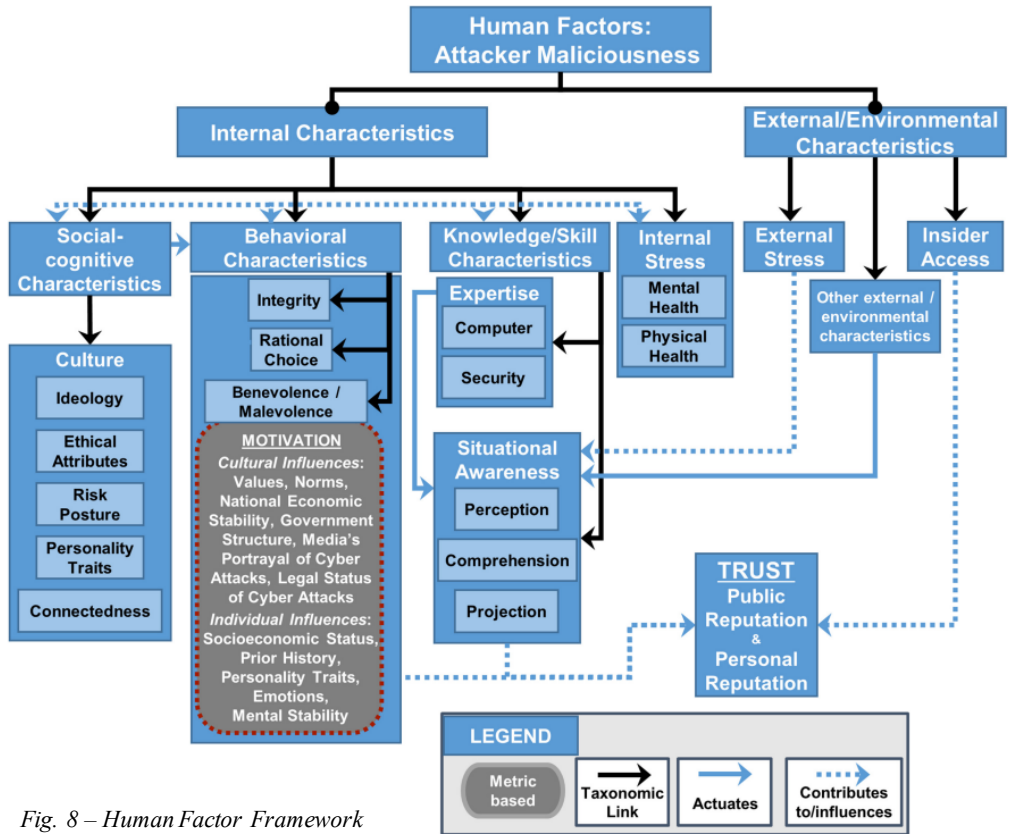


Fig. 8 – Human Factor Framework

[60] King, Z. M., Henshel, D. S., Flora, L., Cains, M. G., Hoffman, B., & Sample, C. (2018). Characterizing and measuring maliciousness for cybersecurity risk assessment. Frontiers in Psychology, 9, 39.

With their Human Factor Frameworks, King, Henshel, Flora, Cains, Hoffman and Sample[61] argue:

> *[...] that maliciousness for attackers is a function of personality traits, mental instability, emotions, self-perception, attitudes, biases, interpersonal behavior, marginality, values (individual and subcultural), norms, national economic stability, government structure, media portrayal of cyber attacks, legal status of cyber attacks, and intergroup behavior.*

Another model to enhance information security culture is proposed by Govender, Kritzinger and Loock as in Fig. 9[62]:

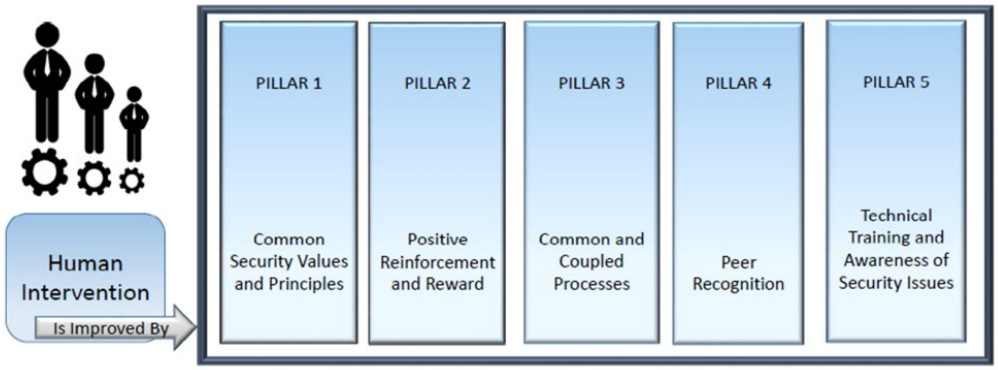


Fig. 9 – Human Intervention: corporate pillar

According to by Govender, Kritzinger and Loock, corporate culture is influenced by the factors as in Fig. 10[63]:

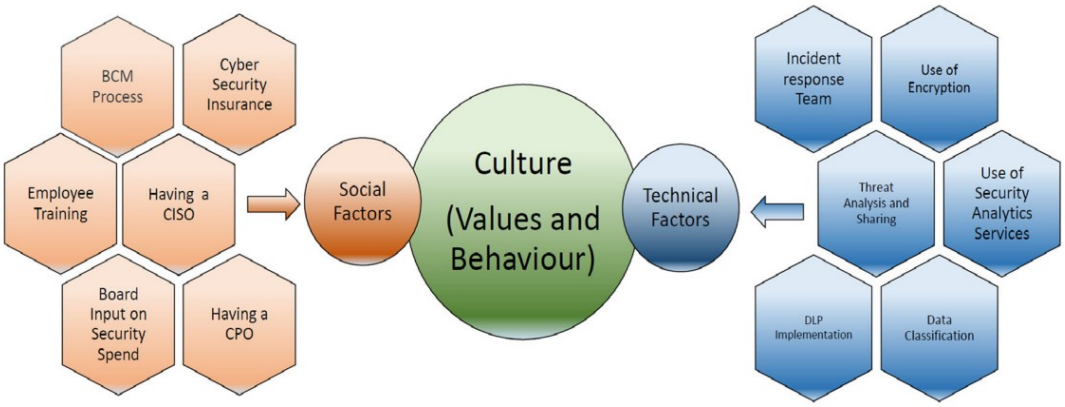


Fig. 10 – Corporate culture influence factor

[61] King, Z. M., Henshel, D. S., Flora, L., Cains, M. G., Hoffman, B., & Sample, C. (2018). Idem
[62] Govender, S. G., Kritzinger, E., & Loock, M. (2021). A framework and tool for the assessment of information security risk, the reduction of information security cost and the sustainability of information security culture. Personal and Ubiquitous Computing, 25(5), 927-940.
[63] Govender, S. G., Kritzinger, E., & Loock, M. (2021). Idem

Govender, Kritzinger and Loock also propose a model that correlates the technological factor with the human component, showing how the technology components necessarily derive from human intervention as in Fig. 11[64]:

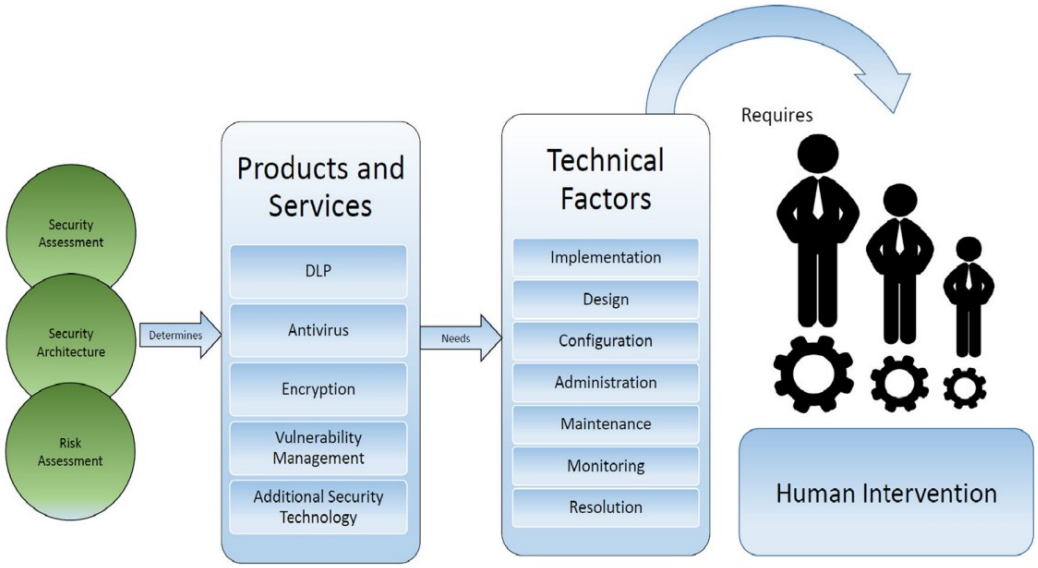


Fig. 11 – Technological factor and human intervention

Govender, Kritzinger and Loock[65] conclude their analysis arguing that:

> *Organizations have focused their security management efforts on technology at significant cost and complexity. Organizations have however neglected the consideration that the number of devices and therefore the amount and variety of threats is far greater than ever before. Incorporating information security into the culture of the IT staff members that support these technologies is a key function that must be considered in parallel to improved security technology. Understanding the threats, security landscape and gaps in information security is also key. […] The framework proposed […] considers focusing on cost-reducing products, services and structures, while building the correct behaviour and values in IT staff members, and strengthening their ability to improve information security assessment capabilities in the organization, to better support information security management.*

Cybersecurity is therefore strongly affected by human behaviors that derive from the corporate culture: the management of these two aspects has a cost that the company must be aware of and must manage in order to achieve also a social control system.

[64] Govender, S. G., Kritzinger, E., & Loock, M. (2021). Idem
[65] Govender, S. G., Kritzinger, E., & Loock, M. (2021). Idem

Consider this evidence Cram, Proudfoot and D'Arcy[66] argue that it is mandatory to find the most effective way to engage employees compliance with policies inherent cybersecurity.

In particular, they identify the following practices to be adopted or not adopted in order to maximize compliance through a wise use of cybersecurity policies as in Tab. 6[67]:

Start Using (or Continue Using)	Stop Using (or Avoid Using in the Future)
• Hiring employees with a positive attitude and ethical orientation toward cybersecurity activities	• Using rewards to encourage cybersecurity policy compliance
• Walking and talking a commitment to cybersecurity initiatives	• Using punishments to discourage non-compliance with the cybersecurity policy
• Providing cybersecurity training that builds employee skills and confidence	• Using the same approach to improve policy compliance and reduce policy violation
• Helping employees follow through on their compliance intentions	• Prioritizing efficiency in the design of the cybersecurity policy
• Highlighting the benefits of compliance	

Tab.6 – Best and worst practices for policies effectiveness

Their recommendations are particularly noteworthy as the analysis is based on a very large representative sample. Cram, Proudfoot and D'Arcy[68] define further actions aimed at achieving effective compliance with cybersecurity policies:

- *Be Open-minded About How You Can Cultivate Employee Compliance with the Policy,*
- *Be Proactive in Instilling Compliant Behaviors,*
- *Provide Employees with the Resources to Help them Comply with the Cybersecurity Policy,*
- *Ensure Employees Understand the Rationale for the Policy Rules,*
- *Rethink the Approach Used to Enforce the Cybersecurity Policy,*
- *Don't Prioritize Efficiency in Cybersecurity Policy Design,*
- *Recognize that Policy Requirements May Be Perceived Differently.*

But why is it so important to govern human behavior? The answer is in the historical evidence. According to Kobis[69] the main human mistakes inherent the cybersecurity includes:

- *excessive trust in global network contents,*
- *lack of developed self-control mechanisms when using electronic mail,*
- *lack of habit of systematic updating of operating systems and application software,*

[66] Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2020). Idem
[67] Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2020). Idem
[68] Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2020). Idem
[69] Kobis, P. (2021). Human factor aspects in information security management in the traditional IT and cloud computing models. Operations Research and Decisions, 31, 61-76.

- *using low-level security measures (weak passwords, failure to use authorization),*
- *levels for the access to data and information,*
- *using security software in free or insufficient versions to meet current needs (willingness to make savings on security software),*
- *connecting mobile devices to unsecured networks (hot spots in airports, restaurants, etc.),*
- *hiding mistakes concerning ensuring information security.*

Kobis[70] argues also Kaspersky Lab analysis (2017), describing that:

- *46% of incidents in 2016 were related to accidental breach of the security policy by employees,*
- *among business entities that fell victim to malware, 53% reported that the reason for the infection was a careless employee and as many as 36% of cases were due to social engineering manipulation of the employees,*
- *in 40% of the cases of security breaches, employees tried to conceal the incident, thereby exposing the business to even greater losses,*
- *nearly 50% of the respondents believed that employees in their company may inadvertently disclose corporate information using mobile devices while working.*

Considering the centrality of human behavior, Nobles[71] identifies the following actions aimed at mitigating the effects of improper actions by employees:

a) Seek the expertise of human factors specialists and behavioral analysts,
b) Mandate an executive-led committee to address human factors in information security,
c) Conduct a risk assessment solely based on human factors,
d) Integrate human factors objectives into the information security strategy,
e) Make humans centric to the foundation of information security and cybersecurity practices,
f) Leverage human factors lessons learned from the aviation, nuclear power, and safety industries,
g) Design training and awareness programs to include gamification,
h) Train personnel on human factors,
i) Develop metrics to capture the changes after implementing human factors objectives,
j) Sponsor human factors research projects with universities and colleges,
k) Integrate human factors course material into information security certification program,

[70] Kobis, P. (2021). Ibidem
[71] Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. HOLISTICA – Journal of Business and Public Administration, 9(3), 71-88.

l) Advocate for colleges and universities to develop and teach human factors courses.

In this highly articulated context, dependent on many factors (cultural, behavioral, technological, ...), corporate policies take on a fundamental role for an adequate governance of IT security (and more). According to Weidman and Grossklags[72]:

> *Policy within any organization continues to be a critical component of that organization's infrastructure. When done correctly, various policies should dictate the function of an entire organization, as well as of those individuals operating within it. One of the principle goals of any organization is to protect its own assets; a topic almost entirely addressed by technical policy, which guides the technical and non-technical security operations of an organization.*

They propose a simple framework inherent the correlation among corporate internal rules, as in Fig. 12[73]:

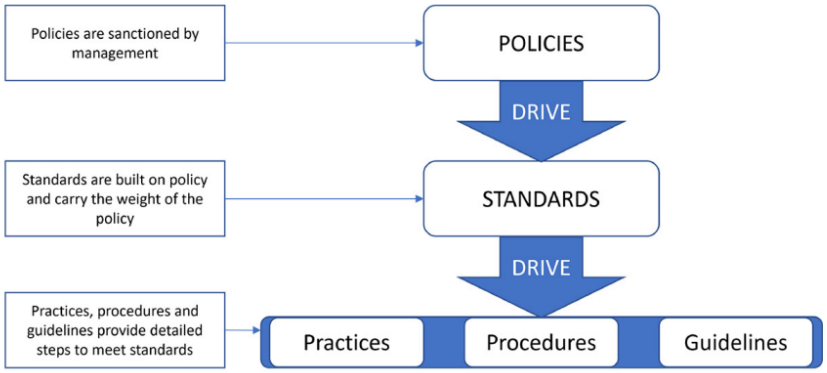


Fig. 12 – Policy, Standard, Procedures, ... correlation framework

Purely technological measures are essential but are completely insufficient if inserted in a context where corporate culture, leadership policy and human behavior are lax, ungoverned and not regulated by internal rules (policies, procedures, ...) which must necessarily and adequately empowered by competent body (e.g. Board of Director, Executive Committee, …) and managed by a duly organizational structure with a concrete accountability and a public mandate.

[72] Weidman, J., & Grossklags, J. (2019). Assessing the current state of information security policies in academic organizations. Information & Computer Security, 28(3), 423-444.
[73] Weidman, J., & Grossklags, J. (2019). Idem

3.4 IS organization, the example of CISO

Cybersecurity and information security can be guaranteed only through multiple layers that must be implemented and managed by companies. The technological layer is mandatory as well as the regulatory layer (policy, procedures, ...) and the organizational layer. Regulatory and organizational layers, more than the technological one, need a suitable empowerment (clear responsibility, public mandate, adequate budget, ...) and derive from a duly awareness of risks and from the corporate culture. In turn, each layer is made up of sub-layers: the organizational layer includes every level of the company, each employee having a responsibility, proportional and increasing with respect to their role and accountability. Within the organizational sub-layer, the CISO function increasingly represents an international reference standard that should be introduced and must be tailored to the actual needs but which must meet minimum requirements.

Allen, Crabb, Curtis, Fitzpatrick, Mehravari and Tobar[74] defines a CISO model starting from the study of some accepted, credible and reputable standard[75]. From these premises, they define these pillar inherent CISO's responsibilities:

- ***Protect, Shield, Defend, and Prevent***

Ensure that the organization's staff, policies, processes, practices, and technologies proactively protect, shield, and defend the enterprise from cyber threats, and prevent the occurrence and recurrence of cybersecurity incidents commensurate with the organization's risk tolerance.

- ***Monitor, Detect, and Hunt***

Ensure that the organization's staff, policies, processes, practices, and technologies monitor ongoing operations and actively hunt for and detect adversaries, and report instances of suspicious and unauthorized events as expeditiously as possible.

- ***Respond, Recover, and Sustain***

---

[74] Allen, J. H., Crabb, G., Curtis, P. D., Fitzpatrick, B., Mehravari, N., & Tobar, D. (2015). Structuring the chief information security officer organization. CARNEGIE-MELLON UNIV PITTSBURGH PA PITTSBURGH United States, (pp. 1-33).

[75] CERT Resilience Management Model, version 1.1 [Caralli 2011], U. S. National Institute of Standards and Technology Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations [NIST 2015], U.S. Department of Energy Cybersecurity Capability Maturity Model (C2M2) [DOE 2014], U. S. National Institute of Standards and Technology Framework for Improving Critical, Infrastructure Cybersecurity [NIST 2014], National Initiative for Cybersecurity Education (NICE) The National Cybersecurity, Workforce Framework Version 1.0 [NICE 2013]1 and the Office of Personnel Management extensions to it [OPM 2014]
SANS Critical Security Controls [SANS 2015]

When a cybersecurity incident occurs, minimize its impact and ensure that the organization's staff, policies, processes, practices, and technologies are rapidly deployed to return assets to normal operations as soon as possible. Assets include technologies, information, people, facilities, and supply chains.

- ***Govern, Manage, Comply, Educate, and Manage Risk***

Ensure that the organization's leadership, staff, policies, processes, practices, and technologies provide ongoing oversight, management, performance measurement, and course correction of all cybersecurity activities. This function includes ensuring compliance with all external and internal requirements and mitigating risk commensurate with the organization's risk tolerance.

More specifically they define the following operational roles and responsibilities as in Tab. 8-10[76]:

➢ Protect, Shield, Defend, and Prevent

Department	Subfunction	Activity
Security Engineering (all asset lifecycle-related activities)	Security requirements	Specify and allocate/assign confidentiality, integrity, and availability requirements.
	Security architecture	Develop and maintain a security architecture.
	Secure lifecycle	Address security throughout the development lifecycle.
	Secure lifecycle	Address security throughout the acquisition lifecycle.
	Certification and accreditation	Perform certification and accreditation prior to releasing new systems to production.
Identity Management	Identity and access management	Define and manage identities and access controls based on identities (password management, single sign on, two-factor authentication, PIN management, digital signatures, smart cards, biometrics, Active Directory, etc.)
Application Security (operations, not development lifecycle)	Software and application inventories	Develop and maintain software and application inventories
	Software and application controls	Define, implement, assess, and maintain controls necessary to protect software and applications in accordance with security requirements (operating systems, applications, database management systems, web-based PCI applications, COTS; maintenance)[4]
	Configuration management	Manage configurations for software and applications
	Change management	Manage changes for software and applications
	Host and network inventories	Develop and maintain network, hardware, device, and system inventories (including wireless)
	Host and network controls	Define, implement, assess, and maintain controls necessary to protect networks, hardware, and systems in accordance with security requirements (intrusion prevention/detection)
	Network perimeter controls	Define, implement, assess, and maintain controls necessary to protect the network/Internet perimeter in accordance with security requirements (firewalls, DMZ, network connections, third-party connectivity, remote access, VPNs)[5]
	Configuration management	Manage configurations for networks (including wireless), hardware, and systems
	Change management	Manage changes for networks, hardware, and systems
Information asset security	Information asset categorization	Designate and categorize information and vital assets (including PII[6]) (includes privacy requirements)
	Information asset inventories	Develop and maintain information asset inventories
	Information asset controls	Define, implement, assess, and maintain controls necessary to protect information and vital assets (including media) in accordance with security requirements (includes privacy requirements, PII, encryption, PKI, backups, DLP, data retention/destruction)[7]
Physical access control	Physical access controls	Define and enforce access controls for facilities and other physical assets (such as networks and hosts)

Tab.7 – CISO responsibilities (area: Protect, Shield, Defend, and Prevent)

[76] Allen, J. H., Crabb, G., Curtis, P. D., Fitzpatrick, B., Mehravari, N., & Tobar, D. (2015). Idem

- Monitor, Detect, and Hunt

Department	Subfunction	Activity
Security operations center	Intelligence collection and threat management	Collect, analyze, triage, and disposition information from all threat sources
	Situational awareness and common operating picture	Collect, analyze, and report information in (near) real time that provides situational awareness and a common operating picture
	Logging	Perform audit logging (includes review and retention) of users, applications, networks, systems, and access to physical assets
	Monitoring	Monitor users, applications, networks, systems, and access to physical assets (includes intrusion prevention/detection, email/spam filtering, web filtering)
	Vulnerability management	Scan for, analyze, and disposition vulnerabilities
	Virus and malicious code management	Detect, analyze, and eliminate viruses and malicious code
	Information security help desk (a.k.a. CIRT[8])	Accept, triage, assign, and disposition all reported suspicious events and security incidents
	Incident management and response	Detect, triage, analyze, respond to, and recover from suspicious events and security incidents

Tab.8 - CISO responsibilities (area: Monitor, Detect and Hunt)

- Respond, Recover and Sustain

Department	Subfunction	Activity
Emergency operations and incident command centers	Incident management and response	Detect, triage, analyze, respond to, and recover from suspicious events and security incidents
	Business continuity	Plan for business continuity
	IT disaster recovery	Plan for disaster recovery
	Test/exercise/drill response plans	Test and exercise BC, DR, and incident management plans (penetration testing, etc.)[9]
	Problem management, root cause analysis, and post mortem reports	Perform problem management, analyze root causes, and develop after action reports for high-profile, high-impact incidents
	Investigations	Perform forensic analysis and support investigations (includes interfaces with law enforcement)

Tab.9 – CISO responsibilities (area: Respond, Recover and Sustain)

- Govern, Manage, Comply, Educate and Manage Risk

Department	Subfunction	Example Activity
Program management office	Information security program/plan	• Develop, implement, and maintain an information security program and plan • Allocate adequate trained/skilled resources to implement the information security program and plan • Measure and monitor cost, schedule, and performance
Governance, risk, and compliance	Information security program/plan	Define, implement, and enforce information security policies
	Risk management	Establish an information security risk management strategy, process, and program
	Governance and compliance	• Govern/oversee the information security program and plan (includes CCB and other oversight boards/groups) • Ensure that controls are adequate to meet legal, regulatory, policy, standards, and security requirements (PCI, SOX,[10] etc.) • Conduct audits
Personnel and external relationships	External relationship management	• Manage relationships with third parties (vendors, suppliers, contractors, partners, and critical infrastructure owners/operators) • Manage relationships with external stakeholders (for example, NCCIC, NSA, DHS, US-CERT, FBI, and the press)[11]
	Personnel management	• Manage the employment lifecycle and performance of personnel in accordance with security requirements (background checks, vetting, transfers, risk designations, succession planning, disciplinary action, and termination) • Manage knowledge, skills, capabilities, and availability of the information security team • Implement an enterprise-wide role-based information security awareness and training program

Tab.10 - CISO responsibilities (area Govern, Manage, Comply, Educate and Manage Risk)

From these premises they arrive to propose the following organization chart as in Fig. 13[77]:

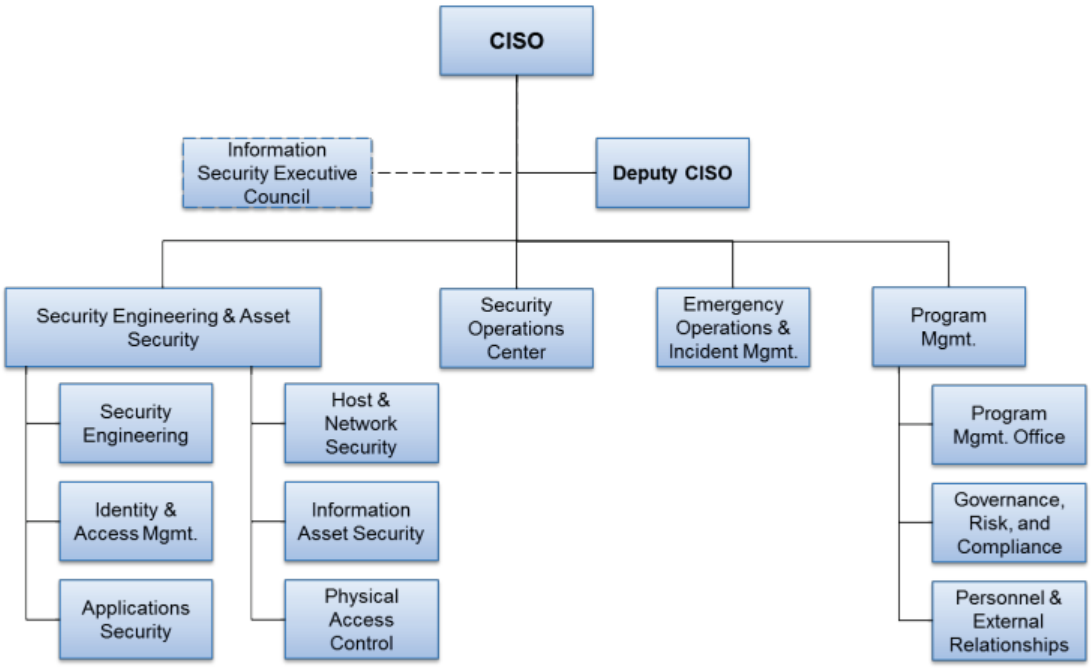


Fig. 13 – CISO Organization Chart (Carnegie-Mellon University)

It is therefore evident that the responsibilities of the CISO are very broad and concern both technological, process and organizational aspects. It is for this reason that the CISO must have specific (1) hard skills and (2) soft skills.

About hard skills, Kappers and Harrel[78] propose this general model:

- *Work Experience: […] 10 years of experience in the IT security area, […] 5 years of security management and team administration;*
- *Education: Master's degree, or greater, in IT Security […]*
- *Skill and Certification: programming languages (C, C++, C#, Java and/or PHP), enterprise architecture, firewall and intrusion/detection/prevention protocol, […] third-party audit, […] cloud risk assessment methodology, ISO 27002, COBIT, ITIL, network security architecture development and definition, PCI, HIPAA, NIST, GLBA and SOX compliance assessments, Practices and methods of IT strategy, secure coding practices, ethical hacking and threat modeling, security architecture, security concept related to DNS, routing, authentication, VPN, Proxy services and DDOS mitigation technologies, TCP/IP, computer networking, routing and switching, Windows, Unix, Linux*

[77] Allen, J. H., Crabb, G., Curtis, P. D., Fitzpatrick, B., Mehravari, N., & Tobar, D. (2015). Idem
[78] Kappers, W. M., & Harrell, M. N. (2020). From Degree to Chief Information Security Officer (CISO): A Framework for Consideration, 22(11), 260-288

About soft skills, Yperen Hagedoorn, Versteeg and Ravesteijn [79] argue that the most important and required skills (ranked in order of importance) are:

- *Communication,*
- *Leadership,*
- *Interpersonal skills,*
- *Professionalism,*
- *Integrity,*
- *Work ethics,*
- *Responsibility,*
- *Teamwork skills,*
- *Positive attitude,*
- *Flexibility,*
- *Courtesy.*

Therefore, the CISO must be an "all-round manager", progressively (1) further away from the technical aspects (which he must know but can / must delegate internally to his own structure) (2) closer to a strategic-directional top manager.

Consistent with this view, Grobler[80] argues that

> *The CISO of the future must be able to effectively communicate and influence at all levels in the organisation. It is absolutely crucial that he or she is able to influence not only technical resources, but also C-suite executive management to ensure cyber risk becomes part of normal risk management and business management practices. The CISO is a crucial change agent in the organisation and his or her role in education at all levels is very important to ensure a better understanding of cyber risk.*

Considering these premises, the issue of reporting the CISO is relevant, in order to ensure adequate empowerment. In this regard, the analysis conducted by SecurityMagazine.com appears very interesting, as in Tab. 11[81]:

[79] Smit, R., van Yperen Hagedoorn, J., Versteeg, P., & Ravesteijn, P. (2021). The Soft Skills Business Demands of the Chief Information Security Officer. Journal of International Technology and Information Management, 30(4), 41-59.
[80] Grobler, J. (2018). Cyber risk from a chief risk officer perspective. Journal of Risk Management in Financial Institutions, 11(2), 125-131.
[81] Inskeep, T. (2019). "How to Properly Position the CISO for Success", SecurityMagazine.com, 37.

Tab.11 – CISO's report position (an analysis)

CISO Reporting to the CIO ***Rationale:*** The CIO is responsible for information and the CISO is responsible for securing that information.	**Benefits** • Allows technical CISOs to obtain greater exposure to the business. • Natural tie between security and technology.	**Risks** • If security plans threaten to stall an IT project, the CIO might overrule the plan. • CIO may limit the CISO's budget, choosing instead to fund his or her own projects or goals.
CISO Reporting to the CFO ***Rationale:*** Cyberattacks and data breaches measurably impact the bottom line.	**Benefits** • Demonstrates leaderships commitment to security. • Provides CISO a "friendly" voice at the leadership table. • Enables CFO to better understand where new risks lie. • Provides CISO an alternate funding channel for cybersecurity efforts. • Enables CISO to get closer to business operations.	**Risks** • CFOs are numbers-based while security investments are still mostly qualitative. • CFO could constrain security budget. • CFOs traditionally have less interest or acumen with security. • Parties may not have common backgrounds or goals.
CISO Reporting to the CRO ***Rationale:*** Security is an enabler for reducing business risk.	**Benefits** • CRO is already a recognized leader and could help foster security agenda. • Provides an alternate funding channel for cybersecurity efforts. • Moves security out of CIO/CTO technology-centric organizations, making it clear cyber risk is part of the broader risk management agenda.	**Risks** • Without soft skills, the CISO may not thrive in this scenario. • Cyber risk is often wrongly perceived as IT risk. • CRO budget may not be able to adequately support the CISO budget.
CISO Reporting to the General Counsel ***Rationale:*** GC and CISO have shared goals. Both have an incentive to confirm that the policies do not violate laws and enable the company to meet legal obligations.	**Benefits** • General Counsel can be a valuable ally to the CISO. • Enables CISO to gain greater exposure to other aspects of the organization.	**Risks** • Legal teams tend to be less technologically focused than the security group.
CISO Reporting to the CEO ***Rationale:*** CEO takes security seriously and perceives security as key to business operations.	**Benefits** • Demonstrates management's commitment to the strategic importance of the CISO's role. • Working closely with the CEO helps ensure best alignment of security with business imperatives. • Provides CISO positional authority to drive security agenda. • Positions CISO equal to other revenue generating parts of the business. • Increases the chance of having security a priority for all aspects of the business.	**Risks** • Could create division between CISO and the IT team as IT team has to implement and manage security technologies and policies. • Positions CISO equal to other revenue-generating parts of the business, creating potential tension. • CISO no longer has a boss to help champion his or her cause. • CIO and CISO may compete for the same dollars.
CISO Reporting to the Board ***Rationale:*** The company has a mature security program and security is core to the business.	**Benefits** • Demonstrates commitment to the security agenda and value of the CISO.	**Risks** • Demands that the CISO must be able to interact effectively with the board and present security in terms the board understands. • Could create tension between the CISO and the CEO.

The issue of the CISO report was also addressed by an analysis conducted by Deloitte and reported on "Journal of Health Care Compliance" which shows the orientation of the market in this regard as in Fig. 14[82]:

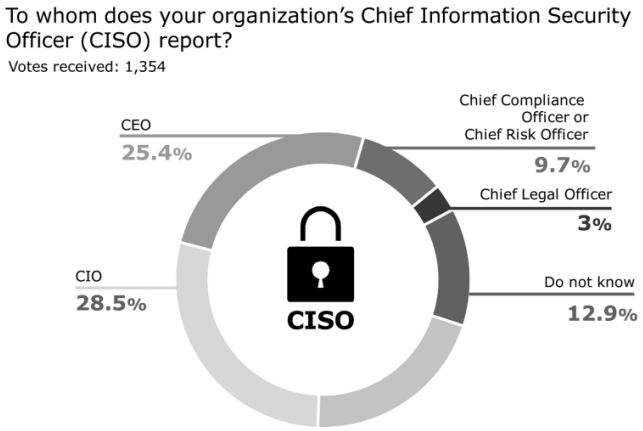


Fig. 14 – Organization's CISO report survey

There is probably no correct answer in absolute terms: different hierarchical positions of the CISO can be effective based on the specificities of the company in which it is inserted. However, there must be awareness that, as for other corporate structures (e.g. audit, compliance, ...), the CISO must be able to act with strong empowerment, clear accountability and with adequate resources (budget and staff): these assessments can only be realized from time to time in individual contexts.

[82] Morrison, A., Kumar, G. (2018) "Corporate Boards May Be More Likely Than Regulators to Scrutinize Cybersecurity Program Effectiveness This Year", Journal of Health Care Compliance, 49-52.

3.5 IS management, the example of ISO 27001

ISO/IEC 27001 is an (1) IT Security, (2) Environmental and (3) Organizational Security and Control Framework: these three areas are deeply connected, with equivalent relevance, and originate from natural and juridical persons behaviors and culture.

Organizational and Environmental areas need much more commitment and empowerment, from the Board of Director, than the "simple" IT Security: it is the reason why ISO/IEC 27001 implementation required (as we will see in the next chapters) consistent resources both financial (it is very recommended to engage, at least, an ISO expert advisor) and qualified personnel time.

ISO/IEC 27001 consists in ten section and an Annex:

1. Scope,
2. Regulatory References,
3. Terms and Definitions,
4. Organizational context, stakeholders and needs understanding,
5. Information Security Leadership and C-level empowering,
6. Planning: opportunity and risk treatment, scope,
7. Support: resources, competence, awareness, communication and documentation,
8. Operational Activities: planning, risk evaluation and management,
9. Reviewing the system's performance,
10. Corrective action.

Annex A: List of controls and their objectives

The Annex have 114 controls that can be clustered in:

- **A.5 Information security policies** (2 controls), about policies empowerment, how the policies are written and reviewed in accordance with the Board of Director information security practices
- **A.6 Organization of information security** (7 control), about the assignment of responsibilities, in order to be sure that Board of Director has established a framework that could adequately implement and update information security

practices (**A.6.1**), concerning smart/remote working and the use of mobile device, in order to be sure anyone follows appropriate practices from the offices, home and on the go (**A.6.2**)

- **A.7 Human resources security** (10 controls), controls before to employment (**A.7.1**), during (**A.7.2**), and after the employment or positions changes (**A.7.3**)
- **A.8 Asset management** (10 controls), inventory of information assets (**A.8.1**), definition of acceptable use and appropriate protection according to information classification (**A.8.2**), media handling, in order to be sure that sensitive information is not modified, removed, destructed or disclosure without authorization (**A.8.3**)
- **A.9 Access control** (14 controls), access Control Policy to information assets and elaborations system (**A.9.1**), user access management (**A.9.2**), system and application access control (**A.9.3**), and user responsibilities (**A.9.4**)
- **A.10 Cryptography** (2 controls), use of cryptography to protect data confidentiality, integrity and availabity
- **A.11 Physical and environmental security** (15 controls), controls defining secure areas, entry controls, protection against threats (**A.11.1**), equipment security, secure disposal for hardware and software, Clear Desk and Clear Screen Policy (**A.11.2**)
- **A.12 Operational security** (15 controls), information management conducted by operational procedures and proper responsibilities (**A.12.1**), defences to mitigate malware's infection risk (**A.12.2**), backup system to mitigate data loss risk (**A.12.3**), logging and monitoring system for security events documented evidence (**A.12.4**), operational software protection (**A.12.5**), technical vulnerability management to protect from exploit system weaknesses (**A.12.6**), audit activities an operations system and theirs minimizations (**A.12.7**)
- **A.13 Communications security** (7 controls), network security for confidentiality, integrity and availability of information in those networks (**A.13.1**), information security in transit towards different organization parts or towards third party (such as customers, suppliers or another interested party) (**A.13.2**)

- **A.14 System acquisition, development and maintenance** (13 controls), information security is an integral part of information systems across the entire lifecycle, including requirements for information systems that provide services over public networks. (**A.14.1-2**), ensure the protection of data used for testing (**A.14.3**).

- **A.15 Supplier relationships** (5 controls), protection of information assets that are accessible to or affected by providers (**A.15.1**), monitoring of the agreed level of information security and services delivery (**A.15.2**)

- **A.16 Information security incident management** (7 controls), controls for reporting events and weaknesses, defining responsibilities, response procedures, and collection of evidence

- **A.17 Information security aspects of business continuity management** (4 controls), controls requiring the planning of business continuity (**A.17.1**), procedures, verification and reviewing, and IT redundancy (**A.17.2**)

- **A.18 Compliance** (8 controls), controls requiring applicable law and regulations in order to avoid breaches of legal, statutory, regulatory or contractual obligations related to information security (**A.18.1**), controls to be sure that information security is effectively implemented in accordance with corporate policies and procedures (**A.18.2**)

The Integrated Cyber Internal Control System must cover all these areas, describing and regulating them with Policies and Procedures (1) approved by management, (2) published, (3) communicated to any interested subjects, (4) object of training activities and (5) auditable.

The scope of application of the ISO is therefore very broad and has a large area that overlaps with other compliance areas (e.g. GDPR). According to Lopes, Oliveira and Guarda[83]:

> *Our findings allow concluding that any organization that has already implemented or is in the process of implementing ISO/IEC 27001 is in an excellent position to show compliance with the new GDPR requirements. The*

[83] Lopes, I. M., Guarda, T., & Oliveira, P. (2019, June). How ISO 27001 can help achieve GDPR compliance. In 2019 14th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-6). IEEE.

new regulation of data protection introduces a set of rules, which require organizations to implement controls. The implementation of ISO 27001 will help organizations respond to these requirements.

In order to implement an ISMS pursuant to ISO 27001, Boehmer identifies four different level for constructing end empowering the management system that must be considered and approached, as in Fig. 15[84]:

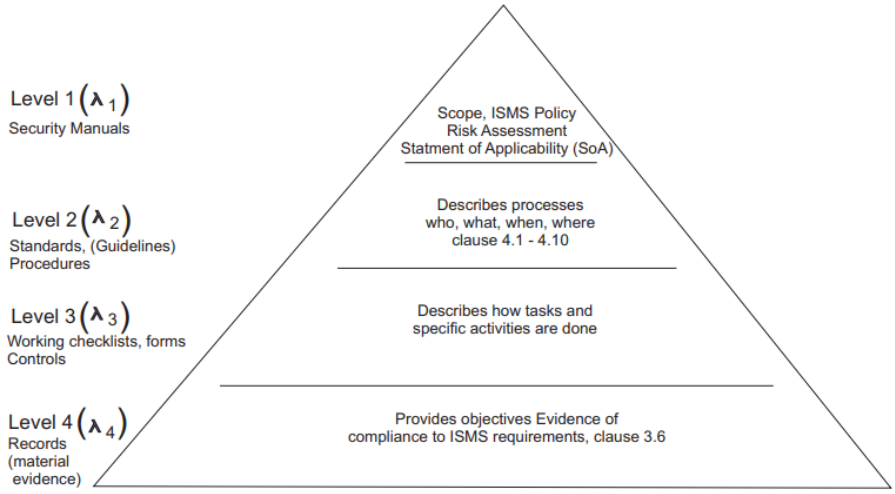


Fig. 15 - General example of an Internal Regulatory Framework logical

Boehmer[85] also believes that implementing an ISO project is not necessarily worthwhile for a company: the implementation and maintenance of a control system has a cost.

Boehmer underlines how the effectiveness and efficiency of the control system represent a trade-off:

In this contribution, we showed that there is a new discussion on security investment estimation, which is based on the KPI of effectiveness and the KPI of economic efficiency. The two KPIs are a trade-off. An alignment in favor of the one KPI is necessarily done at the expense of the other. […] we argued that an Information Security Management System (ISMS) based ISO 27001 is equivalent to risk management, which, in turn, is equivalent to cost/benefit management. Consequently, this risk approach of ISO 27001 is of interest for those companies that want to avoid wasting investments in their information security.

[84] Boehmer, W. (2008, August). Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001. In 2008 Second International Conference on Emerging Security Information, Systems and Technologies (pp. 224-231). IEEE.
[85] Boehmer, W. (2009, March). Cost-benefit trade-off analysis of an ISMS based on ISO 27001. In 2009 International Conference on Availability, Reliability and Security (pp. 392-399). IEEE.

Obtaining ISO 27001 certification certainly entails a cost but can also lead to an increase, not insignificant, of the company's market value. Deane, Goldberg, Rakes[86] conducted a study on this and concluded that:

> *Using ISO 27001 certifications as evidence that firms have successfully developed such a program; we employ the event study methodology to examine empirically the abnormal returns associated with the announcements of these certifcations. We observe positive and statistically significant abnormal returns in the 2-day window comprising the day of and the day preceding these announcements, indicating that the market perceives significant value in commitments to information security risk management. Furthermore, we observe that firms in the historically vulnerable manufacturing and financial services industries derived greater beneft from these certifcations, indicating a greater level of differentiation between these firms and their competitors.*

Obtaining ISO 27001 certification may be appropriate, or even necessary, also for (1) access to business networks, (2) enter into business with entities subject to specific sector regulations, (3) increase the level of assurance towards stakeholders.

This "opportunity-cost" assessment should be carried out by the C-levels (Board of Directors, Executive Committee) expressed in the strategic plan and reported, in terms of objectives, to the top management of the company.

[86] Deane, J. K., Goldberg, D. M., Rakes, T. R., & Rees, L. P. (2019). The effect of information security certification announcements on the market value of the firm. Information Technology and Management, 20(3), 107-121.

4. Major Compliance Frameworks (an overview)

Corporates are exposed to many compliance requirements both legal (mandatory) or quality (optional). Legal requirement must be answered in order to avoid sanctions, limitations or blocks in business continuity (e.g. as defined in administrative sanctions pursuant to Decree 231/01).

Quality requirement are opportunities, not mandatory, that can help corporate to potentiate its reputation, assurance for stakeholders, costs saving and business continuity strategy. Quality requirement alignment can also protect from legal issues, underlining Corporate's will to be compliant.

Same example of traditional legal requirement in Italy are:

- General Data Protection Regulation (UE Reg. 679/16),
- Measures for a high common level of security of network and information systems (UE Directive 1148/16),
- Italian Decree 231/01 inherent corporate liability,
- Italian Decree 81/08 inherent health and safety in working place.

Particular industries can have also specific legal requirement, e.g. "UE Directive MiFID II 65/14", "UE Reg. 600/14" for financial industry or "Italian Law 27/2012" and "Italian Law 135/2012" for assurance industry.

Same examples of quality requirement are:

- ISO/IEC standard,
- NIST Standard,
- CoSO Report, Enterprise Risk Management: Integrated Framework,
- CoSO Report, Internal Control: Integrated Framework.

The management of technological services is the subject of many other standards that address the same problems by proposing similar but different approaches and results. Among these standards, not detailed in the thesis, COBIT and ITIL are among the most famous and most used.

Additional to these legal requirement (such as GDPR, 231/01, 81/08), Companies have to manage also a myriad of specific regulation and law concerning e.g. (1) labor law, (2) fiscal law, (3) company law, (4) copyright law, (5) Civil Code, (6) accounting principles, … that are to be considered in the compliance needs evaluation.

4.1 General Data Protection Regulation (UE Reg. 679/16)

GDPR requires companies and public authorities to abide by security and privacy rules. The Regulation applies to any entity that collects, processes or handles personal data of "natural persons" (data subjects).

The European Legislator describe the principles relating to processing personal data (Art.5 GDPR), the lawfulness of processing (Art.6 GDPR), the condition for consensus (Art.7 GDPR). Moreover, The European Legislator identify specific and severes case-law for that need deeper protection for data subjects (Art.8-11 GDPR).

The GDPR purpose is to:

1. create an Internal Control System suitable for preventing privacy risks relating to personal data, enhancing the existing controls, in terms of adequacy to legal requirements and effective operation of the same,
2. promptly manage possible critical issues,
3. provide highlight the control system implemented, avoiding liability and penalties envisaged.

The pillars of an effective Privacy Internal Control System are:

a. procedure for managing (1) the Data Breach, (2) Data Retention and (3) company data,
b. organizational and governance model,
c. risk assessment metodology (Privacy Impact Assessment),
d. the updating of the relevant privacy documentation (e.g. treatment register, information, consents, internal and external appointments),
e. documented training activity,
f. audits to assess the effectiveness of the system.

Corporates must implement an Internal Regulatory System that describe, with an effective empowerment given by the Board of Director, how to draw up procedures. GDPR requires:

- a Data Breach procedure in order to define how Corporate (Data Controller) must (1) manage possible situation of Data Breach, (2) notify to Supervisory Authority and (3) inform (when applicable) the data subjects,
  This procedure must describe roles and responsibility of the involved staff, in coherency with Corporate privacy organization hierarchy.
- Data retention procedure in order to describe (1) what kind of data should be stored or archived, (2) where that should happen, and (3) for how long, depending on the lawfulness of processing,
- data management procedure in order to ensure that Corporate's data are managed consistently and properly used, through (1) quality, (2) access and (3) security usage criteria.

An example of effective organizational and governance model can contemplate (hierarchy order):

- Data Controller (Corporate),
- Data Protection Officer (if mandatory),
- Privacy Committee,
- Business Unit coordinator,
- Business Unit Privacy contact,
- Processors,
- IT Department,
- System Administrator,
- External Processor,
- Sub-supplier of External Processor,
- Data subject.

For an effective accountability, corporate listed roles need specific, tailor-made and tracked training activities.

The adoption of a risk management methodology allows the definition of plans for intervention (organizational, managerial and control) aimed at mitigating the principal

risks which derive, in particular, from data (1) destruction, (2) loss, (3) modification, (4) unauthorized disclosure or access.

Key Risk Indicator (KRIs) depends on:

- Analysis of the types of data and of the context,
- Calculation of the impact on confidentiality, integrity and availability.

For GDPR the risk consists in any situation that undermine rights or freedom of data subject ("natural person").

Relevant privacy documentation (such as treatment register, information, consents, internal and external appointments) must be periodically updated in order to (1) improve possible shortcomings and (2) receive possible regulatory evolution.

Training activities are mandatory for the effectiveness of the Privacy Internal Control System. These activities must be (1) documented (e.g. tracking online for e-learning contents) and (2) tailormade according to the role, the organizational and governance hierarchy.

Audit activities are mandatory for the effectiveness of the Privacy Internal Control System: only with audits it is possible to test the continuous effectiveness of policy and procedures in order to identify possible shortcomings and areas for improvement.

4.2 Security of network and information systems (UE Directive 1148/16)

The EU NIS directive (implemented by Italian Decree 65/18) is the first important example of community legislation, developed by the EU member states, concerning the security of networks and information systems in industrial sectors identified as critical for the functioning of the "country-system".

Therefore, the directive does not apply to all industrial sectors that lack legal frameworks established by the Italian or European legislator. This causes a problem since other regulations (e.g. GDPR, Legislative Decree 231/01, ...) establish penalties for any non-fulfillment, but with respect to which legislation? This question will be taken up again in the next chapter.

From ENISA website[87]

> *As part of the EU Cybersecurity strategy the European Commission proposed the EU Network and Information Security directive. The NIS Directive [...] is the first piece of EU-wide cybersecurity legislation. [...]. EU directives give EU countries some level of flexibility to take into account national circumstances, for example to re-use existing organizational structures or to align with existing national legislation.*
>
> *The NIS Directive has three parts:*
>
> *1. National capabilities: EU Member States must have certain national cybersecurity capabilities of the individual EU countries, e.g. they must have a national CSIRT, perform cyber exercises, etc.*
>
> *2. Cross-border collaboration: Cross-border collaboration between EU countries, e.g. the operational EU CSIRT network, the strategic NIS cooperation group, etc.*
>
> *3. National supervision of critical sectors: EU Member states have to supervise the cybersecurity of critical market operators in their country: Ex-ante supervision in critical sectors (energy, transport, water, health, digital infrastructure and finance sector), ex-post supervision for critical digital service providers (online market places, cloud and online search engines)*

In particular, the directive includes the following elements:

- systematic and continuous management of networks and information systems,
- mapping of information systems,

[87] https://www.enisa.europa.eu/topics/nis-directive

- definition of an appropriate set of policies relating to IT security management, including risk analysis, human resources, security of operations, security architecture, life cycle management of protected data and systems and encryption and its management (if necessary),
- physical and environmental safety,
- risk-based measures aimed at protecting the networks and information systems of digital service providers from damage, system errors, human errors, malicious acts and natural phenomena,
- security of supply-chain, through the introduction and maintenance of policies to ensure the accessibility and traceability of critical supplies,
- access controls to networks and information systems, understood as measures aimed at ensuring that physical and logical access to networks and information systems are authorized, based on actual business needs and based on the principles of segregation of roles and least privilege.

The companies that fall within the scope of application of the directive also have the obligation to notify, without undue delay, accidents that have an impact relevant, inherent to continuity and supply of the service, to the national Computer Security Incident Response Team (CSIRT), also informing the competent national authority Reference NIS. These authorities change according to the nature of the supply (e.g. in Italy: Health Sector -> Ministry of Health, Transport Sector -> Ministry of Infrastructure and Transport, Energy Sector -> Ministry of Economic Development, ...).

The directive is currently under review and a new version will be issued which, among other innovations, will extend the industrial sectors considered critical and, therefore, which fall within the scope of application of the legislation.

While representing an important step forward in the definition of regulatory standards, established by the European legislator, this legislation is nevertheless (1) not applicable to most industrial sectors and (2) does not define control standards, therefore companies having to seek compliance with the directive through the adoption of quality management systems, such as ISO ones.

4.3 Administrative Liability (Italian Decree 231/01)

The Decree introduced the administrative liability of Companies for certain offences explicitly listed in the Decree and perpetrated, in their own interest or for their own benefit, by their directors, employees and/or representatives in general, together with the related monetary and prohibitive sanctions to be imposed upon the Companies themselves. The Decree provides that Companies may be exempted from such liability should they be able to prove that they have (1) adopted and effectively implemented an Organisational, Management and Control Model (OMM), which is capable of reasonably preventing those offences set out in the Decree; (2) entrusted to a Supervisory Body, vested with autonomous powers of initiative and control, the task of supervising the functioning of and compliance with the Model and ensuring that it is updated with a consistent empowerment given by the Board of Director.

In a logic of continuous improvement, OMM aims to formalize:

- legislative updates within the scope of Decree 231/01,
- the evolution of the regulatory framework on matters of interest,
- any developments in Courts' decisions and legal literature,
- any changes in corporate organization,
- any considerations arising from the application of the Model 231, including any experience from criminal proceedings,
- the practical experience of Italian and foreign companies with regard to compliance models,
- the results of supervision activities and the findings of internal audit activities,
- the "Sensitive Activities and specific control standards of OMM" which dictates the controls that must be set out in the corporate regulatory instruments.

Key Risk Indicator (KRIs) depends on:

- probability to commit a listed crime,
- impact of criminal behavior or aware omissions (administrative sanction).

In Decree 231/01 compliance, the risk is commonly defining as the effect of potential realization of a listed crime.

The offenses contemplated by the legislator in Decree 231/01 concerning the liability of offending entities may be grouped as follows:

- Wrongful receipt of funds, fraud against the Government or a public body or for the obtaining of public funds and computer fraud to the detriment of the Government or any public body,
- IT offenses and unlawful processing of data,
- Organized crime offenses,
- Extortion, wrongful inducement to give or promise other benefits and bribery,
- Counterfeiting of currency, public funding documents, tax stamps and instruments or identifying marks,
- Offenses against industry and commerce,
- Corporate offenses,
- Crimes for purposes of terrorism or subversion of the democratic order contemplated by the criminal code and by the special laws,
- Practices of mutilation of female genital organs,
- Offenses against the individual person,
- Market abuse offenses,
- Crimes of manslaughter and serious or very grave wrongful acts, committed through breach of the regulations on workplace accident prevention and health and safety,
- Receipt, laundering and use of money, goods or benefits of unlawful origin, as well as "self-laundering,
- Copyright infringement offenses,
- Inducement not to make statements or to make false statements to the judicial authorities,
- Environmental offenses,
- Employment of illegally-staying foreign nationals,
- Racial, ethnic and religious discrimination,
- Transnational offenses,

The thesis concerns "**IT offenses and unlawful processing of data**", where data is a legal asset subject to protection:

- Computer fraud of the electronic signature certifier (art. 640-quinquies of the Italian criminal code),
- Wrongful access to a computer or electronic system (art. 615-ter of the Italian criminal code),
- Falsehood in a public computer document or document having evidentiary effect (art. 491-bis of the Italian criminal code),
- Wrongful possession and dissemination of access codes to computer or data interchange systems (art. 615-quater, Italian criminal code),
- Dissemination of equipment, devices or computer programs with intent of damaging or interrupting a computer or data interchange system (art. 615-quinquies, Italian criminal code),
- Interception, impediment or unlawful interruption of computer or data interchange communications (art. 617-quater, Italian criminal code),
- Installation of equipment intending to intercept, impede or interrupt computer or data interchange communications (art. 617-quinquies, Italian criminal code),
- Damage to information, data and computer programs (art. 635-bis, Italian criminal code),
- Damage to information, data and computer programs used by the Government or any public body or, in any case, of public interest (art. 635-ter, Italian criminal code);
- Damage to computer or data interchange systems (art. 635-quater, Italian criminal code),
- Damage to computer or data interchange systems of public interest (art. 635-quinquies, Italian criminal code).

The preconditions for the advent of administrative liability are:

- the commission by a natural person (whether of senior management or subordinate) of one of the offenses listed in Decree 231/01,
- the offense's having been committed or not prevented in the interest/advantage of the entity,
- the offense's originating from an "organizational fault" of the entity.

These kinds of preconditions lose their validity in other compliance field, e.g. GDPR where is not necessarily corporate advantage for receiving a punishment.

Some regulatory areas, such as the Consolidated Law on Health and Safety in the workplace (Italian D.lgs 81/08 Italian) define by law the standards to be adopted. In these contexts, the jurisprudence[88] is clear in identifying an administrative liability, also pursuant to the Italian Law 231/01, under these conditions:

1. criminal behavior or aware omissions by senior management or subordinate,
2. aware non-existence or laxity of typical controls (defined by law).

With reference to the "IT offenses and unlawful processing of data" and, more generally, to the topic of "Information Security" and "Cybersecurity" (governed also by GDPR), the standards that must be applied are not fully[89] defined by law, although other laws and regulations (Italian Law 231/01, GDPR, ...) provide for the case of "inadequacy" of controls.

In the event of disputes, how should the potential inadequacy of control be assessed, if there is no regulation (emanate from national or EU legislator) on controls to be adopted?

Although in the absence of related jurisprudence, it should be clear how qualitative standards (e.g. ISO) must be considered by the public prosecutor as mandatory substitutes of national or EU regulations.

In the event of non-alignment or inadequacy with these standards, therefore, an administrative liability of the entity could be configured: the activation of administrative responsibility should be possible making a logical interpretation of recent jurisprudential developments (sentence of the Italian Court of Cassation n. 22256/2021), ensuring a proper parallelism with Italian D.lgs 81/08 disputes.

The sentence indicates that the advantage requirement occurs when (1) managerial decisions have resulted in a reduction in costs with consequent maximization of profit,

[88] Sentence of the Italian Court of Cassation n. 22256/2021

[89] E.g. UE Directive 1148/16 applies to specific industrial sectors and does not cover all types of businesses

(2) the savings derive from non-compliance (voluntary or not voluntary) of norms, (3) the saving is not insignificant.

Referring to "IT offenses and unlawful processing of data", should be a corporate liability for example under these conditions:

1. criminal behavior or aware omissions by senior management or subordinate,
2. aware non-existence or laxity of typical controls (defined by standard).

From these premises, in case of cyber or data-protection issues, in addition to any problems pursuant to the GDPR[90], the aware failure to adopt a robust ISMS, duly managed by an effective organization structure (elements understood together as "typical controls"), should ignite a corporate liability pursuant to Italian law 231/01 subsisting (1) informed and aware non-existence or laxity of typical controls (defined by standard) and (2) corporate's advantage represented by a significant cost-saving.

[90] E.g. pursuant to art. 32 GDPR, inherent in "Insufficient technical and organisational measures to ensure information security", case that, in the GDPR area, resulted in approx.100 million euros in fines between 2018 and 2022 (https://www.enforcementtracker.com)

4.4 Health and safety on work (Italian Decree 81/08)

This Legislative Decree pursues to implement rules, ensuring uniformity of the protection of workers and workers on national territory by respecting the essential levels of social and civil rights benefits.

The pillars of an effective Health and Safety Internal Control System are:

a. compliance with the technical-structural standards of the law relating to equipment, plants, workplaces, chemical, physical and biological agents,
b. risk assessment and preparation of prevention and protection measures,
c. organizational activities, such as emergencies, first aid, procurement management, periodic safety meetings, consultations with workers' safety representatives,
d. health surveillance activities,
e. the information and training of workers,
f. supervisory activities with reference to workers' compliance with procedures and instructions for work in safety,
g. the acquisition of documents and certifications required by law,
h. periodic audits of the application and effectiveness of the procedures adopted.

Cyber-security is out of scope respect Decree 81/01 purpose but, depending on the specifics Company, Health and Safety Internal Control System could regards also the environmental security, one pillar of ISO/IEC 27001 standard.

Italian Decree 81/08 requirement could be accomplished within the implementation of ISO/IEC 45001:2018, concerning Occupational Health and Safety Management System.

4.5 Risk and Internal Control Integrated Framework (CoSO Report and ERM)

According to CoSO Report[91], **Internal Control** is

> *a process, carried out at different levels of the organization, aimed at providing reasonable certainty as to the attainment of the objectives of: effectiveness and efficiency of operating activities; reliability of information in financial statements; compliance with applicable laws and regulations*

The pillars of **Internal Control** System are:

1. Control environment regarding HR policies (e.g. Code of Conduct, Regulation, Policy, Procedures, Reward System, Training Activities, definition of incompatibility situations, …),
2. Risk assessment inherent (1) the business activities, (2) the effectiveness of adopted measures, (3) the purpose of risk mitigation,
3. Control Activities, design and implementation of specific procedures inherent (1) Organizational control mechanisms (e.g. Segregation of Duties, Least Privilege), (2) IT control mechanism for traceability of process and activities,
4. Information and Communication processes,
5. The Monitoring, carried out by (1) any actors with roles of responsibility for management and control processes and (2) by Audit, Regulatory Body, … in order to evaluate the control system's adequacy.

According to CoSO Report**, Enterprise Risk Management** aims to:

> **- *Align risk appetite and strategy*** *– Management considers the entity's risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.*
> **- *Enhance risk response decisions*** *– Enterprise risk management provides the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance.*

[91] Committee of Sponsoring Organizations of the Treadway Commission (2017), Enterprise Risk Management. Integrated Framework.

- Reduce operational surprises and *losses – Entities gain enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses.*

- Identify and manage multiple and cross-enterprise risks *– Every enterprise faces a myriad of risks affecting different parts of the organization, and enterprise risk management facilitates effective response to the interrelated impacts, and integrated responses to multiple risks.*

- Seize opportunities *– By considering a full range of potential events, management is positioned to identify and proactively realize opportunities.*

- Improve deployment of capital *– Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation*

The pillars to obtain ERM's aims are:

*1. **Governance and Culture**: Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviors, and understanding of risk in the entity.*

*2. **Strategy and Objective-Setting**: Enterprise risk management, strategy, and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.*

*3. **Performance**: Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritized by severity in the context of risk appetite. The organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.*

*4. **Review and Revision**: By reviewing entity performance, an organization can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed.*

*5. **Information, Communication, and Reporting**: Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization.*

5. Proposal for IS organizational and management models

Following what has been seen in the previous chapters, the last chapter aims to

(1) represents the ISO-project complexity, focusing on awareness of the top-level decision-makers (Board of Director, Executive Committee), accountability of the Head of the Company (CEO, Directors), empowerment of the Project Management Team,
(2) propose an abstract model of ISMS pursuant to ISO 27001, managed by an effective CISO organizational structure, for a theoretical company hypothesized as follow:
    - Italian Company,
    - B2B and B2C trading and/or services activities,
    - middle-exposition to compliance requirement (hyper-regulated industrial sectors such as financial, chemical, pharmaceutical, energy, ... are excluded),
    - big-size dimension (600-1200 employees and 500 external collaborator),
    - on global market,
    - annual revenue 200-300 mln euros/year, operating costs 170-270 mln euros/year, net income ~ 30 mln euros/year,
    - positive long-run outlook,
    - no legal or compliance issues,
    - large scale personal data usage through (as per art. 35 of the GDPR),
    - use of standard-leader ERP solution and other software solution (both on market and custom),
    - significant number of IT providers (both market leader and middle-little software-house) (20-30 providers),
    - significant number of IT user (all employees and external collaborator, 1100-1700 natural persons).

ISO 27001 project is not only technological but also organizational, management and control; this wide scope makes mandatory to consider all the legal and quality requirement asked to the company: otherwise it is concrete the risk to formalize Policy or Procedures pursuant to ISO standard but (1) affected by explicit non-compliancy

respect others regulatory fields or (2) too generic to be effective also for the other different legal frameworks, that Corporate have to manage and respects in any case.

The ISMS must be represented by an Internal Regulatory Framework, (1) intended as a formal set of Policies and Procedures empowered by the Board of Director and (2) in common with non-Cyber business processes internal regulations.

The ISMS can be built after (1) an AS-IS recognition, (2) gap analysis between actual situation and standard, (3) the definition of recommended action to manage the gaps, (4) concreate implementation of these actions (and their manteinance); these four steps are typical project management's phases.

ISO/IEC 27001 project show off many operational risks that can nullify an effective ISMS implementation: this complexity requires awareness of the C-level (Board of Director, Executive Committee) in order to create accountability of the Head of the Company (CEO, Directors) and to give empowerment to Project Management Team.

For facing these needs, and for managing possible "unpleasant" results, there are necessary (1) a clear and public project mandate that clarify the project scope, (2) a consistent Project Management Hierarchy, (3) financial resources, (4) multidisciplinary external advisory team and (5) lung-run ISMS manteinance and improvement strategy.

ISO/IEC 27001 project needs the allocation of significant resources that Board of Directors have to guarantee for covering one-shoot costs (pilot phase Advisory) and long-run costs (manteinance and improvement).

5.1 Internal Regulatory Framework as mandatory requirement

An **Internal Regulatory Framework** (IRF) must be establish for the management of Policies, Procedures and for supporting relevant Corporate documentations, that in order to be easier aligned to legal and quality requirements.

IRF can be considering as a continuous process that needs effective empowerment from the Board of Directors in order to manage obligations and compliance risks in an effective and efficiently ways.

IRF is a set of regulatory documents, commonly Policies and Procedures:

- Policies are concise formal statements of high levels principles, regulating action and conduct,
- Procedures describe, in sequential order, a process that declines Policies, describing roles and ownership of the organizational, management and control model applied in the specific process.

ISO Standard give these definitions:

> *3.4.5 - **Procedure**: specified way to carry out an activity or a process (ISO 9000:2015)*
> *3.5.8 - **Policy**: intentions and direction of an organization as formally expressed by its top management (ISO 9000:2015)*

IRF represents concretely how Corporate intends to be committed to comply with legal and quality requirement, proving a clear separation between governance and management responsibility.

For being consistent, an IRF must regulate formal features such as e.g. (1) necessary requirement in the Policy/Procedure drafting, (2) the hierarchy of IRF management and its governance, (3) the publishing and sharing of Policy/Procedure, (4) the improvement processes, (5) audit activities, ….

ISO 27001:2017 needs, as exogenous and mandatory requirement, an IRF:

> *5.1.1 - **Information security policy document**: An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties. (ISO 27001:2017)*

In other words, ISO 27001:2017 takes for granted the existence of an IRF without witch it is not possible to seriously approach ISO implementation.

The IRF must be applied on the several legal and quality requirements in order to have an internal regulatory System, made by Policy and Procedures that talk the same language even if with different risks definitions and different compliance management approaches.

Typically, an IRF born Bottom-up but, at some point, a Top-down commitment became mandatory in order to make IRF much closer to a "compliancy-proof" situation, otherwise IRF remains, in the best case, only a set of good-practices.

If a Company does not have (or not planning to have) an IRF, it is not possible to talk seriously about ISO 27001 implementation.

5.2 Life-cycle project implementation

5.2.1 Project Establishment

Project Governance is a critical success factor. The PMI explains the reason[92]:

> *Project governance needs to be tailored to an organization's specific needs, and there are eight components that must be considered. These components will influence how you create and implement as well as monitor and control the governance framework […].*
> *Project governance is an "oversight function that is aligned with the organization's governance model and encompasses the project life cycle[93]". There are two critical elements in this statement that need to be emphasized:*
> *- **Alignment with organization's governance**: There needs to be an understanding of the project's environment to ensure that there is a right fit with the established organization's governance. This alignment is a crucial factor and must be considered when defining (1) the project governance framework, (2) roles and responsibilities and (3) stakeholder engagement and communication. These prerequisites need to be met at the onset of the project kick-off.*
> *- **Longevity, monitoring and controlling of the governance plan**: These three components come to fruition during the life cycle of your project. The project/program manager needs to make sure the governance plan is implemented throughout the project and must also monitor and control the effectiveness of the governance plan. When monitoring and controlling the project governance framework, the project manager needs to ensure that there are adequate (4) meetings, (5) reporting, (6) risk and issue management, (7) assurance, and (8) project management control processes.*

An ISO/IEC 27001 project must have an effective governance close to this:

- Project Sponsor (Board of Director, Executive Committee) that give the mandate, establishing the scope,
- Steering Committee, composed by this Departments/Committee:
  - ICT,
  - Legal,
  - Audit,
  - Compliance,
  - HR,

[92] Alie, S. S. (2015). Project governance: # 1 critical success factor. Project Management Institute.
[93] A Guide to the Project Management Body of Knowledge (2013) (PMBOK® Guide). Fifth Edition (Project Management Institute)

  - Risk Committee (if any),
  - Privacy Committee (if any),
  - another competent Committee (if any),
- Operational Committee composed, at least, by this departments:
  - ICT,
  - Compliance,
- ISO Project Leader (1 FTE) who responds to Operational Committee and manage independent Consultants specialized in:
  - Policy & Procedures Quality Framework Advisory,
  - Overall (GDPR, Decree 231/01, CoSO Framework, …) Compliance Advisory,
  - Overall (Administrative Liability, Labor Law, …) Legal Advisory.

Consultants independency is mandatory in order to have (1) a non-biased project outcome and (2) more assertiveness in the needs' representation that can be "uncomfortable" for the management. Consultants effort must be budgeting.

The project Hierarchy must be publicly and formally empowered by the Board of Director: the strength of empowerment must be directly proportional to the scope's width. ISO/IEC 27001 certification can concern the entire Corporate environment or a part of this: it is easier to approach ISO project for single area (e.g. ICT Department), in this way instead we have a reduction of ISO/IEC 27001 assurance's scope for Corporate stakeholders.

ISO/IEC 27001 Scope is a Board of Director's aware and informed decision and must be formalized in the public mandate of the Project Management Hierarchy.

Next steps are planning the activities than can be summarized in these four phases:

- AS-IS analysis,
- GAP analysis,
- Recommendation definition,
- Implementation of Recommendation.

All of this step must to be (1) planned and (2) budgeted.

The planning has to consider project scope and organizational, management and control Corporate complexity: e.g. in the AS-IS analysis can be necessary to interview about 30-40 persons. This activity is very time-consuming.

These persons must be well-engaged because they are the same that will validate GAP analysis, Recommendations and that have to carry-out the concrete implementation of the recommended action.

Let's suppose that (1) the four phases need the same effort (25% for phases) and (2) AS-IS analysis needs 55 labors full-day (front/back-end activities) equivalent to approx. three labor full-months. The entire project will need 1 labor full-year (approx. in 220 labor full-day) that can be smeared on more than one solar year: it depends on the Board of Directors' mandate. The phase "Implementation of Recommendations" is optimistically estimated: these costs will depend on the "aggregate Gap Level" between actual situations and the minimum compliance situation.

Let's suppose also that (1) it is need, at least, a Consultant in every labor full-day and (2) the relative effort of independent Consultants is hypothesized as follow:

- 50% for Policy & Procedures Quality Framework Advisory,
- 30% for Overall Compliance Advisory,
- 20% Overall Legal Advisory.

Considering a middle-rate, for a Consultancy day, about 900euros + VAT we will have an economical effort of 198k euros + VAT divided as follow:

- 99k euros + VAT for Policy & Procedures Quality Framework Advisory,
- 59,4k euros + VAT for Overall Compliance Advisory,
- 39,6k euros + VAT for Overall Legal Advisory.

It must be underline that, in this phase, we are not considering the costs of (1) personnel, (2) fine-tuning implementation and (3) manteinance: these costs are fixed and pluriannual while the 198k euros + VAT is related only to the one-shoot costs for pilot consultancy and go-live phase.

5.2.2 AS-IS analysis

AS-IS analysis is a documented recognition of the situation actually encountered. The analysis usually involves (1) carrying out interview with key-role and (2) analyzing of company's internal regulatory sources. All results must be formalized in a report (named "AS-IS Analysis") shared with the project governance.

Typical key-role to be interviewed are:

1. Chief Information Technology Officer,
2. OS administrator,
3. Network administrator,
4. Data centers maintenance and security environmental systems staff,
5. Technical project manager involved in the design, development, go-live and maintenance of software application,
6. A representative sample of IT systems users,
7. Health and Safety Officer for physical and environmental security of offices,
8. HR involved in selection processes, placement, training and exit of any kind of personnel (i.e. permanent/temporary employees, collaborators, interns, consultants, …),
9. Procurement involved in the selection and management of suppliers.

The internal regulatory sources usually include:

1. Company Statute,
2. Decree 231/01 Model,
3. Privacy Model,
4. Regulation, Policy, Procedures,
5. Act of delegations, power of attorney.

AS-IS analysis is aim to understand and represent in a consistent report:

1. organizational structure, roles, responsibilities, proxies, powers of attorney (with particular focus on IT and safety management),

2. HR administration (with particular focus on technical skills management and development and regarding communications about safety rules),
3. Procurement administration (with particular focus on IT security and safety requirements during the life-cycle of services purchase),
4. updating processes relating to the applicable legislation,
5. reviewing processes for policies and procedures and them sharing with personnel, users, system administrator and technical operator,
6. physical security of offices, data centers and servers,
7. management of IT (system, application, administrative) and physical authorizations,
8. requirements for the development of applications and related processes of design, development, testing, making available for the applications developed, web or not,
9. IT Systems and them supplier census,
10. security measures relating to IT systems and network,
11. management of incidents and communication to interested parties (data breach),
12. business continuity and disaster recovery plan.

More in details:

1. <u>Organizational structure, roles, responsibilities, proxies, powers of attorney (with a focus on IT and safety management)</u>

It is necessary to understand and formally represents how a Company works. This point can be easily analyzed thanks to the "Organizational, Management and Control Model pursuant to Decree 231/01", if any, and checked with key Top-Manager interviews. A Company is made by organizational structure and natural persons that have specific roles and responsibility in that specific structures and between them: this assessment is mainly oriented to evaluate (1) if key principles are applied, such as "Segregation of Duties", "Least Privilege", "Conflict of Interest Policy" and (2) how the Company manage relevant activities such as "Contact with authorities", "Internal Regulation and Law enforcement Policies".

2. HR administration (with particular focus on technical skills management and development and regarding communications about safety rules)

HR have to take care of employment life-cycle through (1) CV screening, (2) terms and conditions of employment, (3) disciplinary process, (4) personnel duties and responsibilities definition and (5) termination of employment.

In particular, the use (as simple user or admin) of an IT System (such as ERP Solution) must be preceded by specialist training activities promoted by HR.

3. Procurement administration (with particular focus on IT security during the life-cycle of services or goods purchase)

Procurement administration must be regulated by a related Policy, as part of Corporate's IRF. Procurement Policy have to discipline the eligibility criteria for entering in the suppliers register: the criteria concern many fields (e.g. labor law, health and safety, financial sustainability, references, …) in order to be sure that the chosen supplier respects legal, compliance, cost-benefit and cost-utility requirements.

IT security requirement of Technological supplier must be (1) formally predicted the eligibility criteria, (2) inserted in the supply contract as binding clauses and (3) auditable by the client.

4. Updating processes relating to the applicable legislation

Corporate must monitoring legal and compliance requirement evolution related to all the fields Company are exposed to. Corporate have to manage a myriad of regulation and law concerning a wide range of requirement, e.g. (1) privacy (GDPR), (2) Decree 231/01 (Administrative Liability), (3) Decree 81/08 (Health and Safety), (4) Labor Law, (5) Fiscal Law, (6) Corporate Law, (7) Civil Code, (8) Accounting Principles, …

This monitoring is very complex and time-consuming and must be conducted by a professional structure such as "Compliance Department".

5. Reviewing processes for policies and procedures and them sharing with personnel, users, system administrator and technical operator

The Internal Regulatory Framework (IRF) must be consider as a continuous process, conducted by a professional structure such as "Organization & Processes Department". The review process must be regulated by the IRF itself as specific Policy.

6. Physical security of offices, data centers and servers

The Company must apply a compliance framework concerning Health and Safety on working places. The Physical security requirement considered by the ISO 27001 is generally out of scope respect Health and Safety regulation's aim: a Company must have specific rules that regulate (1) authorized personnel and how (2) to access to offices, (3) the data center and (4) server room.
Physical security regards also the uses and practices adopted by the employees' workstation: Company must have a Policy that describe the best and the worst practices to (or not) attend e.g. in desk management. This Policies should be auditable.

7. Management of IT (system, application, administrative)

Corporate must have a User Life-Cycle Policy that describe, consistently with HR employees Life-Cycle and Job Profile Policies, who are eligible to receive (1) Corporate email (such as @corporate_name.com or @corporate_collab.com for external collaborator) and (2) IT System users according to Segregation of Duties and Least Privilege principles. User policy must be auditable.

8. Requirements for the development of applications and related processes of design, development, testing, making available for the applications developed, web or not

Software development must conduct by (1) professional employees (checked by HR department) under ICT department coordination and/or (2) IT provider (check by Procurement department) under ICT department coordination. All development phases must be documented and respect project management and cyber-security Framework. In software development, Corporate must use a compliance-by-design approach in order to ex-ante evaluate possible compliance issues. Compliance-by-design approach should be regulated by specific Policy, as part of IRF.

9. IT Systems and them supplier census

IT Systems census is a common sense and mandatory requirement. The census should consider, at least, (1) supplier (with technical and commercial references), (2) business owner (Corporate personnel that are in charge on the business process regulated by the IT System), (3) technical owner, (4) hosting details, (5) technical and functional documentation.

10. Security measures relating to IT systems and network

IT Systems and network security must be manned by ICT department through (1) most recently security technology, (2) personnel with specific qualification and (3) technology professional provider. Technologic measures must be documented, shared, formalized expected in a Policy and describe in a Procedure, as parts of IRF.

11. Management of incidents and communication to interested parties (data breach)

Corporate must have a Policy and/or a Procedure, as part of IRF, that describe how to (1) manage (role, responsibility, …) and (2) communicate data breach to any interested parties (Authorities, natural person, ...). This is a requirement strongly established by General Data Protection Regulation that must to be incorporate in the Privacy Management System.

12. Business continuity and disaster recovery plan

Business continuity is "the capacity of the capability of an organization to continue the delivery of products or services at pre-defined acceptable levels following a disruptive incident[94]".

The capacity must be declinate in a Policy and/or a Procedure, that establish the disaster recovery plan that describe (1) roles and responsibility, (2) prevention action and activities, (3) risk detection and (4) tool for risk management.

The description of the above, which emerged during the interviews and the analysis of the documents, must be documented (1) on-going after the conclusion of interviews,

[94] ISO 22300:2012 - Societal security

(2) in a final report, edited by common recognized consultancy Framework or best-practices. All documentation must be shared and fine-tuned with the interviewed, business/process owner and department Director.

The AS-IS analysis must be objective and must not provide any kind of judgment or evaluation about detected situations. AS-IS document must be (1) wide shared with interviewed and theirs Director and after (2) officialized to the Project Management Governance.

5.2.3 GAP analysis

Starting from a consistent AS-IS analysis, Gap Analysis is pretty easy to technically carry out, in particular exploiting Consultants expertise and standing. Much harder can be the results sharing with project stakeholders.

Gap Analysis has the same structure of AS-IS Analysis, describing the "gap" (what is missing) respect the standard prediction. The gap can concern (1) technology, (2) organization, (3) management or (4) control and can be inherent to legal or quality standard requirement (also out of scope of ISO 27001 itself).

The main difficult in the Gap Analysis phase is the results sharing. Same results can be "unpleasant" for the Top Management and for the Board of Director: Gap Analysis show the distance between the actual situation and the minimum compliant situations. The width of this distance can be (1) physiological, (2) pathological (potentially showing that same internal practices are close to worst-practices) or (3) in the middle.

Gap Analysis is the main risk phase for the Project Leader that must guarantee an ethical equilibrium between the accuracy of the results and Corporate's mandate. For Project Leader's protection is crucial the consistency of Project Governance and the ongoing clarifying about what "expected results" are.

Considering some theoretical situations of "unpleasant" result that could emerge from Gap Analysis and that could be not easy to manage:

Example 1

- the Company (as hypothesized) makes use of external collaborators,
- collaborators receive and use institutional emails "@corporate_name.com",
- there is not Policy related to (1) the attribution and (2) the use of institutional technological devices or services,
- there is not Policy related to the collaborator recruitment,
- there is not Policy related to the IT identity HR life-cycle,
- collaborators have fixed workstation,
- same collaborators are engaged independently by different Business Units (these collaborators have more than one contract at the same time),
- the same collaborators have been continuously engaged since more than 3 years,

- the HR department only manages the contracts from an acritical administrative point of view, regardless of labor law risks.

Example 2

- the Company makes use of interns,
- interns receive and use institutional emails "@corporate_name.com",
- interns' duties include Corporate IT System use, core-business processes,
- the activities on IT System are conduct with nominal IT User,
- same interns have IT User with the same IT Right of same permanent employee,
- among these IT User, some IT Right correspond to Admin profile,
- there is not Policy related to the IT identity HR life-cycle.

ISO 27001 needs the existence of consistent (1) organizational, management and control structures, (2) HR administration processes (natural person labor life-cycle) and (3) User IT life-cycle. ISO 27001 does not talk about or define what "consistent" means, implicitly referring to common Best Practices Frameworks.

The non-compliancy (and so the related risks), in theoretical examples, derive from legal and quality requirements (e.g. Labor Law, Decree 231/01, Decree 81/08) that are independent but necessary strictly correlated with ISO 27001 standard prediction. In the event of a crime being committed, the company may have administrative liability pursuant to Decree 231/01, where the benefit it represents by the Corporate saving for not having adopted suitable control misures.

Example 3

- the Company uses a standard-leader ERP solution and other software solution (both on market and custom),
- many software are connected each-other among public-services (e.g. API, web-services, …),
- public-services was created and are developing by middle-little software-house,
- public-services respect traditional ICT standard, but some of these do not respect Cybersecurity standard (e.g. encryption, strong authentication, IT profile modelling, …),
- some personal-data are transmitted among these public-services,

Example 4

- the Company uses a standard-leader ERP solution and other software solution (both on market and custom),
- the on-market software has a native IT profile modelling system,
- custom software was created and are developing by middle-little software-house,
- the custom software has an IT profile modelling system, based on the functional requirements expressed by the business units to the software-house, through ICT dept.,
- the functional requirements are evaluated by ICT dept. but not analyzed from a Compliance structure,
- same functional requirements do not respect principles of Segregation of Duties and Least Privilege,
- same functional requirements are inherent personal-data processing.

Example 4.1

- some on-market software was customized through a non-standard IT profile modelling system,
- there is not IT profile modeling approach consistent with IT system technical features and HR job-profiling system,
- some IT profile modelling system do not respect principles of Segregation of Duties and Least Privilege,
- some IT profiles concerns personal-data processing.

Example 4.2

- some IT user profile are assigned to external collaborator, interns and/or suppliers,

Example 4.3

- some IT profiles are assigned through cloning existing profiles,
- there is an acritical stratification of IT profiles with a massive use of super-users/admin users,

Example 4.3

- some IT profiles (standard user, super-user and admin) are assigned and governed by Business Unit independent of ICT dept. and/or HR dept.

Example 5

- the Company use a standard-leader ERP solution and other software solution (both on market and custom),
- there are few functional documentations, inherent specific software's uses,
- there are no HR training activities inherent software's uses,
- HR dept. has not a detailed job-profiling system,
- HR flow inherent tour-over and resignation are not formalized for ICT dept.

Example 6

- the Company use a standard-leader ERP solution and other software solution (both on market and custom),
- Company's software are used by employee, external collaborator, interns and suppliers,
- Company's does not have a formalized HR life-cycle policy,
- ICT dept. receive late or does not receive formalized HR flow.

The non-compliancy (and so the related risks), in theoretical examples, derive from the aware no-adoption of standard security practices inherent (1) software development, (2) IT profile modelling and (3) HR life-cycle management and mandatory training, producing a saving for the Corporate. In the event of a crime being committed, the company may have administrative liability pursuant to Decree 231/01.

In ISO 27001 Gap Analysis should be mandatory to consider the entire set of legal and quality requirement, otherwise it is concrete the risk to formalize Policy or Procedures pursuant to ISO standard but (1) affected by explicit non-compliancy respect others regulatory fields or (2) too generic to be effective also for the other different legal frameworks, that Corporate have to manage and respects in any case.

The Gap Analysis consists in a professional evaluation about detected situations respect to a benchmark (legal and quality standard requirement).

Due to possible “unpleasant” results, Gap Analysis document should be (1) discussed with the Project Management Governance and after (2) communicated to the interviewed and their Directors. After these steps, the Gap Analysis document can be considered officialized and it is possible to define the Recommendations.

5.2.4 TO-BE actions

Borrowing audit standard, according to IPPF[95] (2410 – Criteria for Communicating):

> *Final communication of engagement results must include applicable conclusions, as well as applicable recommendations and/or action plans. Where appropriate, the internal auditors' opinion should be provided. An opinion must take into account the expectations of senior management, the board, and other stakeholders and must be supported by sufficient, reliable, relevant, and useful information*

Recommendations derive from Gap-Analysis results: every gap must be analyzed in order to define (1) technological, (2) organizational, (3) management and (4) control actions able to cover it. Recommendations are based on the Advisor professional judgment and proposed by ISO Project Leader. The recommended action could concern:

- adoption of technological solution,
- establishment of organizational development,
- implementations of management tool,
- design of control environment.

These points must be expressed in regulatory documents (Policy or Procedure) compliant with the Internal Regulatory Framework adopted by the Company: this set of regulatory documents will constitute the ISMS pursuant to ISO 27001 standard.

Recommendations are formulated with a proposal, shared with Project Management Hierarchy and approved by the Board of Directors, of the B.U./Directions in charge to carry out these activities.

Recommendations must be considered as a standalone project that needs specific (1) Awareness of the top-level decision-maker, (2) Accountability of the Head of the Company, (3) Empowerment of project management team and (4) a project governance hierarchy. Every single project must be budgeted: in the projectwork we

[95] International Standards for the Professional Practice of Internal Auditing (IPPF Standards)

are assuming a standard cost concerning non-pathological situation, “easy” to manage and resolve.

ISO Project Leader is not responsible for the concrete adoption of the actions recommended but he could be involved, as internal consultant, in some actions.

Recommendations must be concern also (1) communication, (2) mandatory training activities and (3) sanctioning system, addressed to the entire Corporate extended community, potentially involved.

5.3 An example of IS Management System

The ISMS Policy and Procedures should consider and cover all Corporate's "layers", if related to the use or adoption of any kind of technologies. Trying an overall merge of the frameworks previously described, focusing on the use or adoption of technologies, Corporate's "layers" could be so represented:

Layer	II level	III level
Technology	**Hardware, Device, IoT**	HW, Device, IoT Census
		HW, Device, IoT Management
		Supplier Governance
		Security Measures
		Assignment Eligible Criteria
		Identity and Authentication Management
	Application, Services and Network	Security Architecture
		Security Application
		IT System Census
		IT Management
		Supplier Governance
		Security Development Standard
		Security Measures
		Assignment Eligible Criteria
		Identity and Authentication Management
Organization	**Leadership Model**	Accountability, Empowering
		Business Strategy
		Organization Design
		Strategic Plan / Business Goals
		System of Work Design (welfare and workforce capability)
	Structures, Roles, Responsability	ICT Dept.
		HR Dept.
		Compliance Dept. (II e III level CoSO report)
		Procurement Dept.
		Business Unit

	Proxies, Powers of Attorney	Third-Party Relations
		Supplier Relations
	Physical Security of spaces	Offices
		Server, Datacenter
Management	**Statute, Code of Conduct, Sanctionary System**	
	Internal Regulatory Framework -IRF (Policy and Procedures)	Law and Framework Monitoring
		IRF Empowering
		IRF Writing, Reviewing, Sharing and Training
	Management System	GDPR System
		Incident Management and Business Continuity
		Decree 231/01 System
		HR Administration
		Procurement Administration
		Reward System
		User Education and Training Activities
		Information and Communication Activities
		Incompatibility Situations
Control	**Risk Evaluation**	Applicable Legislation Review
		Business Activities Analysis
		Risk Assessment Metodology
		Recommendations and Action Plans
	Internal Control System	Awareness, training, information and communication
		Ongoing Application and Monitoring
		Segregation of Duties
		Least Privilege
		Processes and activities traceability
		Compliance by Design (II Level Control, CoSO Report)
		System Adequacy Evaluation (Audit)

Tab.12 – General representation of Corporate's layers

The "Information Security Management System" is one of the Management System that Corporate should adopt. All the Management System must be developed through the Internal Regulatory Framework (IRF) that represents "common factor rules":

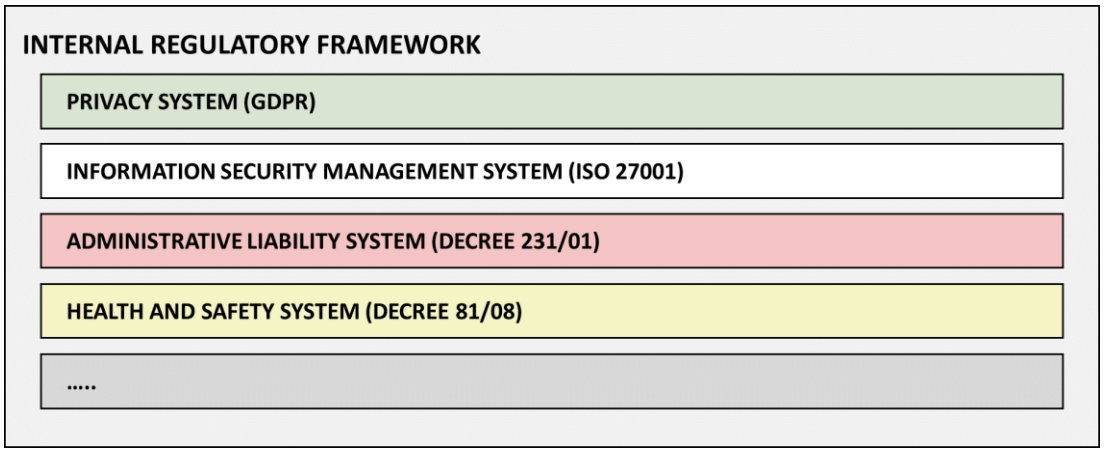


Fig.16 – General example of an Internal Regulatory Framework logical structure

The ISMS are composed by Policy and Procedures, connected each other, that are IT specific focused or can be borrowed (or be in common) from (with) other Management System (e.g. physical security policy, privacy policies, cybercrime policies, …):

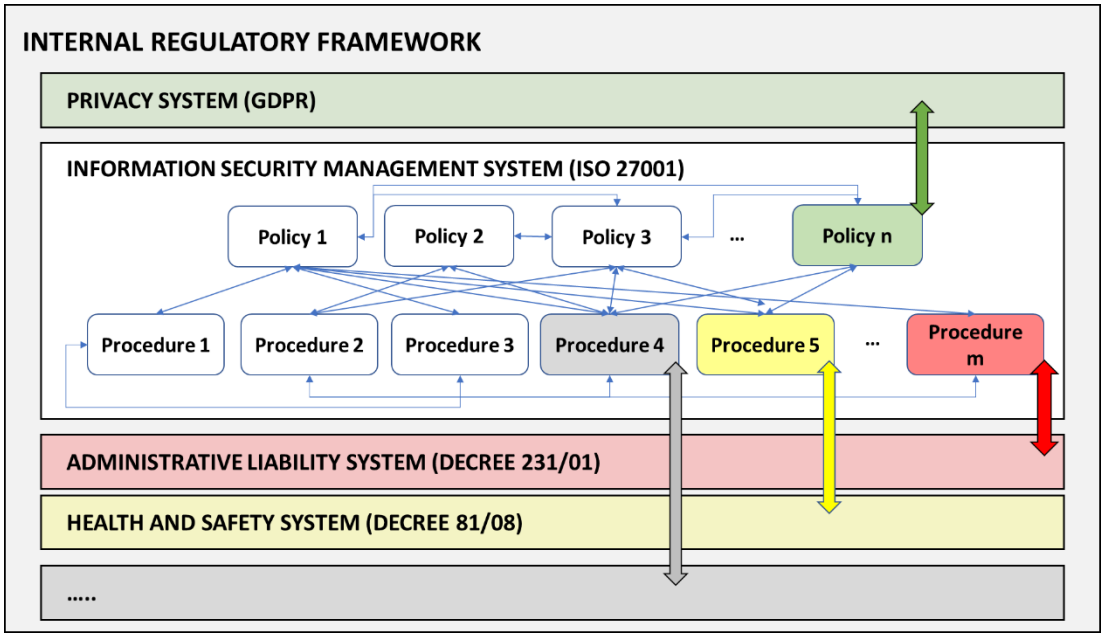


Fig.17 - General example of Policies and Procedures interaction in an Internal Regulatory Framework

ISMS Policies and Procedures should be developed according to the "least regulation principle": a regulatory document must describe only the information necessary to

know legitimate actions and behaviors, explicitly leading to others regulatory documents for complementary and related information, actions and behaviors.

In this way ISMS Policies and Procedures are interconnected (also with other Management System), without overlapping and guaranteeing effectiveness in their updating process.

According to ISO 27001 controls and considering traditional legal and quality frameworks, an ISMS should have this overall structure and these minimum contents:

Source		Internal regulatory document	ISO 27001 Controls Ref.
Policies (PO) (Approved by Board of Directors)	**1**	**IT Governance, Risk and Compliance (IT GRC) Model**	A.5 Information Security Policies A.6 Organization of information security A.16 Information security incident management A.17 Information security aspects of business continuity management A.18 Compliance
	2	**Information, Communication and Training Activities**	A.6 Organization of information security A.7 Human resources security A.8 Asset management A.9 Access control
	3	**Data Classification and Protection**	A.8 Asset management A.10 Cryptography
	4	**IT Security Standard**	A.9 Access control A.11 Physical and environmental security A.12 Operational security A.13 Communications security A.16 Information security incident management A.17 Information security aspects of business continuity management

	5	**Acceptable Use of Corporate IT goods and services**	A.6 Organization of information security A.7 Human resources security A.8 Asset management A.9 Access control
	6	**IT goods and services standard Equipment (Eligible Criteria and Life Cycle for Employees and Collaborators)**	A.6 Organization of information security A.7 Human resources security A.8 Asset management A.9 Access control
	7	**IT goods and services purchasing and IT provider management**	A.14 System acquisition, development and Maintenance A.15 Supplier relationships
	8	**Privacy Compliance**	A.18 Compliance
	9	**Intellectual Property Compliance**	A.18 Compliance

Tab.13 – Abstract Policies' list pursuant to ISO 27001

Source		Internal regulatory document	Policy Ref. (PO.)
Procedures (PR) (Approved by B.U. and reviewed by Compliance Dept.)	**1**	**Application, Database and Network Security Management**	PO.1, PO.4
	2	**Identity Governance System and Users Life Cycle**	PO.1, PO.4, PO.5, PO.6
	3	**Authentication Security Management**	PO.1, PO.4, PO.5, PO.6

	4	**IT goods and services assignment**	PO.1, PO.2, PO.4. PO.5, PO.6, PO.7
	5	**Protection of Information in work activities**	PO.1, PO.2, PO.3, PO.4, PO.5, PO.6, PO.8
	6	**Cryptographic Tools for Information Processing**	PO.1, PO.3, PO.4
	7	**Application Logs and Privileged Access Management**	PO.1, PO.2, PO.5, PO.6
	8	**Security Incidents, Business Continuity and Disaster Recovery**	PO.1, PO.2, PO.4, PO.5
	9	**IT System and Provider Census Management**	PO.1, PO.4, PO.7, PO.8, PO.9
	10	**Contractual Compliance regarding Cybesecurity, Data Protection & Privacy**	PO.1, PO.4, PO.7, PO.8, PO.9
	11	**Contractual Compliance regarding Intellectual Property Rights**	PO.1, PO.7, PO.8, PO.9
	12	**Software and Hardware not included in the standard equipment (Use or Purchase)**	PO.1, PO.7, PO.8, PO.9
	13	**Software Development: Security Standard, Source Code and Public Services Management**	PO.1, PO.3, PO.4, PO.7, PO.8, PO.9

Tab.14 - Abstract Procedures' list pursuant to ISO 27001

More in details:

Internal Regulatory Documents	
Policies	
IT Governance, Risk and Compliance (IT GRC) Model	IT Governance, Risk and Compliance (GRC) Model is a representation of IT Corporate strategy for managing overall Governance, ERM and compliance with legal and quality Framework. GRC scope is to aligning IT strategy and management with business objectives, having also an effective risk management approach and regulatory compliancy.
Information, Communication and Training Activities	The ISMS must be transmitted and know by all stakeholder (e.g. employees, collaborator, …, provider) potentially involved. This document describes how Corporate want to concrete manage these kinds of obligations through an effective knowledge and awareness path, mandatory, documented and tailormade for different roles and responsibility.
Data Classification and Protection	Data Classification is a formal process that aims to assess Corporate Information in order to define the duty level of protection. The classification approach should be risk based: information with a higher risk level must receive higher level of confidentiality. The Key Risk Indicator should be based on different fields: e.g. GDPR, Decree 231/01, …, Core Business information. Confidentiality is the typical terms of classification and a Corporate should have different level that correspond to different level of risk, e.g.: - Confidential (only few employees have access), - Restricted (most employees have access), - Internal (all employees have access), - Public information (everyone has access).

IT Security Standard	Corporate assets (IT Goods and Services) managed and manteinance. Technological assets include computer, mobile, servers, internet, applications, …, official email, … Corporate must establish the technological security standard of IT assets to ensure the safety, security, integrity of data, information, services or product used by the Corporate or offered on market.
Acceptable Use of Corporate IT goods and services	Corporate assets (IT Goods and Services) must be property used. Technological assets include computer, mobile, servers, internet, applications, …, official email, … Corporate must establish the behavioral security standard and the acceptable and ethical use of IT assets to ensure the safety, security, integrity of data, information, services or product used by the Corporate or offered on market.
IT goods and services standard Equipment (Eligible Criteria and Life Cycle for Employees and Collaborators)	Corporate assets must be assigned to employees, collaborator, … according to standard eligible criteria and a public life cycle inherent HR management. Corporate must establish the standard equipment related to specific figures (employees, collaborator) and roles, defining also the minimum criteria that allow the assignment (in order to be compliant with legal requirement, e.g. labor law) and the life cycle that describe when an asset can be assigned or must be regained by ICT dept. on HR dept. trigger. Particular attention must pay for collaborator that must have special equipment (if considered necessary) that make explicit the nature of collaborations (e.g. the assignation of email as @collab.corporate-name.com)

IT goods and services purchasing and IT provider management	The IT Goods and Services must be central managed by Dept. endowed with adequate accountability. Procurement and ICT Dept. must have the central and exclusive ownership inherent the IT assets purchasing process and the provider and third-parties' relations (such as negotiation). This policy should describe the IT assets purchasing process, detailing the different kind of IT Goods (e.g. Laptop, smartphone, …, Server, …) or Services (e.g. Cloud, SW on market, SW development, …) identifying ownership both for standard and exceptional needs.
Privacy Compliance	A Corporate should have a Privacy Management Systems pursuant to the GDPR. These policies can be borrowed from the Privacy Management System in order to integrate the mandatory regulation asked to an ISMS pursuant to ISO 27001.
Intellectual Property Compliance	Company should manage the Intellectual Property Compliance with a specific set of regulation that can be borrowed by the ISMS pursuant to ISO 27001. Otherwise, Corporate must discipline how to protect intellectual property rights in business activities.

Internal Regulatory Documents

Procedures

Procedures are the second level of the Internal Regulatory Framework and decline Policies. Procedures describe how to obtain the respect of the Policies general principles and dispositions, defining the operative action, step, activities that everyone have to carry out in business processes**.** The set of Procedures derives from the needs expressed by the Gap-Analysis and should cover all the Corporate "layers" related to use or adoption of any kind of technologies. Procedures must describe the process phase, the input and output elements and the organizational, management and control ownerships. Procedures must be auditable in order to evaluate their effectiveness. Procedures can be borrowed (or be in common) from (with) other Management System (e.g. Privacy, Health and Safety, …).

Typically, ISMS Procedures should cover these areas in order to formalize the minimum compliance requirement from legal and quality Frameworks:

Procedures	
Application, Database and Network Security Management	ICT Dept. must define the minimum-Security Standard (both technological and behavioral) to respect and apply in the use or adoption of application, database and networking system. This ownership derives from Policies and give to ICT Dept. the exclusive accountability to evaluate the best solutions based on market analysis and renewed standards.
Identity Governance System and Users Life Cycle	ICT Dept. and HR Dept. must manage the access to IT System and Services through a process that guarantee the identity of resources, in compliance with labor law requirement and coherently with the HR life cycle, Segregation of Duties and Least Privilege principles. To guarantee the traceability of all action, it is necessary to

	describe the system logs management adopted by the Corporate. IT Users (e.g. IT System User, Corporate email) are a type of IT services that needs specific governance. As IT standard equipment, IT Users must be assigned according to related Policies and through a process that clarify roles, responsibility and operative step for obtain, manage and terminate IT Users. The access to IT System is sensible and must be agreed after an HR process aims to evaluate the consistency between IT user and job profile and after specific training (promoted by HR dept.) in order to duly operate in the IT System. The assignation of Corporate email must be governed strictly according to HR life circle (in order to avoid Labor Law risk among external collaborator management).
Authentication Security Management	Password and Authentication requirement must be defined by ICT Dept. in order to align to the international best-practices and renewed standards. Password complexity and strong authentication (e.g. 2-factor) must be evaluated by the ICT Dept. and imposed top-down according to risk evaluation and standard analysis.
IT goods and services assignment	IT standard equipment must be assigned according to related Policies and through a process that clarify roles, responsibility and operative step for obtain, manage and get back the IT asset, coherently with the HR life cycle.
Protection of Information in work activities	Physical protection of Corporate's spaces must be defined and described in order to have both technological (e.g. physical access control) and behavioral (e.g. use or misuse of workplace) misures. This procedure can be partially borrowed (e.g. for physical access) from Health and Safety

	Management System and integrated for ISO 27001 requirements.
Cryptographic Tools for Information Processing	Data classification define the duty level of protection. Cryptographic tool must be use in the processing of confidential data and/or in the high risk's cases. ICT Dept. have to define the standard process and tools that all B.U. must use in the case established by the related Policy.
Application Logs and Privileged Access Management	This procedure has the same object of "Identity Governance System and Users Life Cycle" procedure but focused on IT Administrator, their Life Cycle characterized by specific duties and obligations. Procedure describe how Admin User are formally designed in compliancy with GDPR requirement. This procedure describe also how Administrator activities are tracked.
Security Incidents, Business Continuity and Disaster Recovery	This procedure can be borrowed from the Privacy Management System that must describe how the Company manage Incidents situations, guarantee Business Continuity and the Disaster Recovery approach, according to the GDPR requirements.
IT System and Provider Census Management	ICT Dept. must have and update a list of IT System in order to trace functional referent (employees at B.U. in charge for data processing), technical referent (employees at ICT Dept. in charge for technical data management and provider coordination), Provider referents (both technical that commercial), hosting details and all IT System

	documentations, both functional (how IT System work from all type Users point of view) and technological (how the IT System work from technological point of view). ICT Dept. and Procurement must have and update a list of IT Provider with the indications of the security standard required and provisioning details flow. This list is a part of vendor list managed by Procurement in accordance to common best practices and Procurement Policy or Procedure.
Contractual Compliance regarding Cybesecurity, Data Protection & Privacy	ICT Dept., Procurement Dept. and Legal Dept. must develop standard contract clause to apply top-down to IT Provider in order to regulate Intellectual Property Right (in compliancy also with the specific – if any – inherent regulation)
Contractual Compliance regarding Intellectual Property Rights	ICT Dept., Procurement Dept. and Legal Dept. must develop standard contract clause to apply top-down to IT Provider in order to regulate Privacy aspect (in compliancy also with Privacy Management System)
Software and Hardware not included in the standard equipment (Use or Purchase)	ICT Dept. has the exclusive ownership, deriving from Policies, to value the best technological solution for standard equipment. Any requests concerning the purchase or the use of non-standard equipment Software or Hardware must be evaluated by ICT Dept. from cybersecurity point of view and must be authorized by ICT Dept., Procurement Dept. and a C-Level with duly power of attorney.

Software Development: Security Standard, Source Code and Public Services Management	According to related Policies, ICT Dept. must have the exclusive ownership to engage and coordinate IT Provider. For Software development ICT Dept. must guarantee the adoption of security standard by Providers, the production of the functional and technical documentations, the repository of the Source code and, in particular, the documented evidence inherent public services (e.g. web services). The procedure describes also how manage technical and services users, necessary in software development, that must be regulated in the contracts between Corporate and IT provider

5.4 An example of CISO Department

In a complex organization, a robust structure is mandatory to ground an effective Information Security Management System pursuant to ISO 271001 standard.

The following model is strongly inspired by the work of Allen, Crabb, Curtis, Fitzpatrick, Mehravari and Tobar[96], customized on the scope and methods of reference standard, scientific literature overviewed and analyzed benchmark and scalable on a company as assumed at the beginning of chapter 5.

From these premises a hypothetical organizational structure for the secure management of information should be close to:

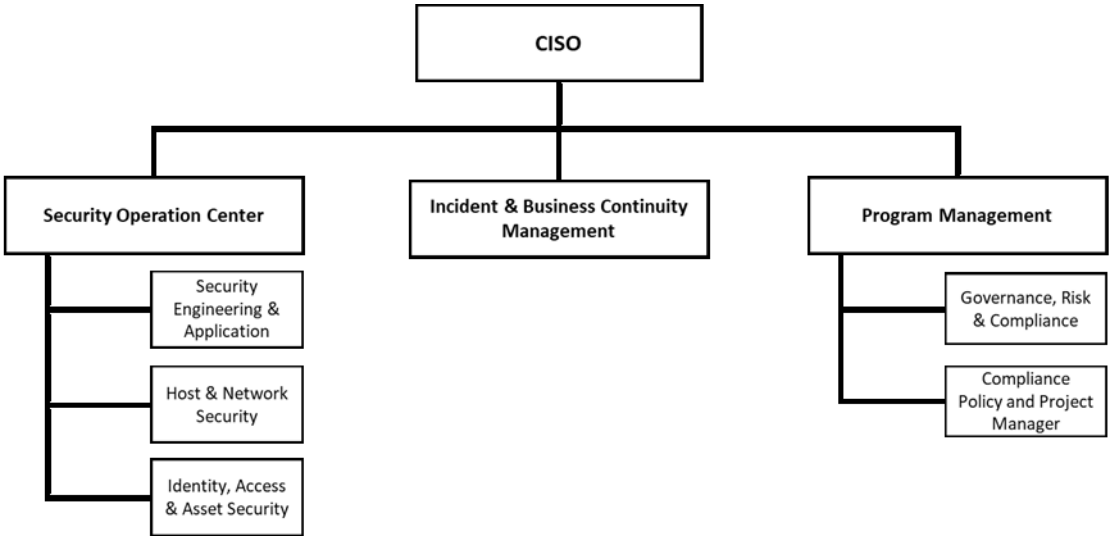


Fig.18 – Abstract CISO organizational structure, based on standard hypothesis.

The CISO have to create and manage a corporate program inherent data protection through the definition of a Management and Monitoring System. He must have deep knowledge of legal, regulatory, policy and procedures and standard related to information security. The CISO:

- supports corporate governance in order to guarantee an effective information security management,
- analyzes corporate processes and aims in order to evaluate risks,
- monitors legal, regulatory and quality framework development,

[96] Allen, J. H., Crabb, G., Curtis, P. D., Fitzpatrick, B., Mehravari, N., & Tobar, D. (2015). Idem

- introduces compliance-tech by design methodology in policy/procedures design and in project management activities,
- defines incident and crisis management standard management in order to guarantee business continuity through a formal strategy,
- conducts continuous control on IT System in order to increase protection in accordance with recognized standard,
- introduces and develops host and network protection in accordance with recognized standard,
- defines information access criteria, behavioral rules and technical measures,
- manages Identity Governance Access and corporate asset life-cycle in accordance with HR eligible criteria.

➢ **Security Operation Center**

- **Security Engineering & Application**, in charge for guarantying the adoption of security standard in any software development, stimulating the continuous updating and alignment with standard evolution in coordination with developer both internal then external (as technological suppliers),
- **Host & Network Security**, in charge for guarantying (1) the adoption of security standard and defences settings in Server OS and Host OS (as employee's devices), (2) the creation of an infrastructure for devices, applications and users,
- **Identity, Access & Asset Security**, in charge for (1) enabling and securing digital identities (in accordance with HR eligible criteria and compliance requirement) for all users, applications, data and technology assets (as corporate device, institutional email, …), (2) managing access (IT system, information, …) and asset life-cycle, applying Segregation of Duties and Least Privileged rules defined by the Corporate.

➢ **Incident Management, Business Continuity & Resiliency Planning**

Incident management aims to restore normal technological service operation as quickly as possible to minimize the impact to business operations, responding to incidents when they occur, taking any necessary step to restore involved services and interacting with employees, provider and customers if necessary.

Business continuity and resiliency planning is the corporate approach for managing operational risks in order to guarantee standard level of products or services delivery in case of a disruptive incident.

- **Program Management**

– **CISO Program Manager**, in charge for (1) coordinating corporate compliance by design metodology, (2) guarantying continuous alignment with all compliance corporate functions, (3) establishing information, communication and training activities and contents inherent cybersecurity and data protection, (4) transposition of internal needs inherent cybersecurity and data protection,

– **Governance, Risk & Compliance**, in charge for (1) analyzing the set of internal regulatory sources established by the directors or the board of directors and that reflect organization's structure and how it is managed, (2) predicting risk that could affect corporate achievement, reputation, …, (3) examining mandatory (as law, regulations, …) and voluntary (quality certification, …) fulfillments, (4) harmonizing previously sets of information for face offing with uncertainty and acting with integrity with an efficient and effective approach,

– **Compliance Policy and Project Management,** in charge for (1) internal regulatory documents (policy, procedures, labor instructions, …) maintenancing and developing in accordance with fulfillments and organizational and corporate changes, (2) participating in technological corporate project, supporting guarantying compliance by design approach.

According to supposed organizational chart, Corporate FTEs needs will be:

- CISO, 1 FTE senior manager,
- SOC manager, 1 FTE manager,
    - Security, Engineering & Application, 1 FTE senior associate,
    - Host & Network Security, 1 FTE senior associate,
    - Identity, Access & Asset Security, 1 FTE senior associate,
- Incident Management, Business Continuity & Resiliency Planning, 1 FTE middle-senior manager,
- Program Manager, 1 FTE manager,

- Governance, Risk & Compliance, 1 FTE senior associate,
- Compliance Policy and Project Management, 1 FTE senior associate.

We have also to consider the FTE related to audit activities in order to have an independent evaluation of the effectiveness of (1) ISMS and (2) information security governance.

It should be noted that the business cost for 1 FTE is not the Gross Annual Salary (GAS) but the cost that the company incurs considering ancillary expenses, such as:

- social security contributions (e.g. Italian INPS),
- welfare contributions (e.g. Italian INAIL),
- wages revaluation,
- holiday allowance in lieu,
- severance indemnity,
- individual awards,
- supplementary pension,
- optional health insurance,
- food stamps,
- …

With respect to GAS, the above values are estimated in this way:

% on GAS:	
Social security contributions (e.g. Italian INPS)	33,2%
Welfare contributions (e.g. Italian INAIL)	8,0%
Wages Revaluation	2,0%
Holiday allowance in lieu	4,8%
Individual awards	10,0%
total	**58%**
Severance indemnity coefficient (SIC) > GAS/SIC	**13,5**
Other items (for 1 FTE):	
Supplementary pension	1.000 €
Optional health insurance	1.000 €
Food stamps	2.000 €
total (for 1 FTE)	**4.000 €**

Tab.15 - Coefficients for calculating the HR company cost

From these premises and basing on Richardson, Hiatt, Lowman, Napshin and Perros analysis[97], inherent manager and director wages, the final cost of CISO department, as well as assumed, is approx. 1,4 mln euros / year so detailed:

	GAS (euro)	CORPORATE COST (euro)		
CISO (1FTE)	115.000	194.219	HR Cost (Senior Manager)	fixed cost
Security Operation Center (1FTE)	92.000	156.175	HR Cost (Middle Manager)	fixed cost
Security Engineering & Application (1FTE)	66.000	113.169	HR Cost (Senior Associate)	fixed cost
Host & Network Security (1FTE)	66.000	113.169	HR Cost (Senior Associate)	fixed cost
Identity, Access & Asset Security (1FTE)	66.000	113.169	HR Cost (Senior Associate)	fixed cost
Incident Management, Business Continuity & Resiliency Planning (1FTE)	100.000	169.407	HR Cost (Middle-Senior Manager)	fixed cost
Program Manager	92.000	156.175	HR Cost (Middle Manager)	fixed cost
Governance, Risk & Compliance (1FTE)	66.000	113.169	HR Cost (Senior Associate)	fixed cost
Compliance Policy and Project Management (1FTE)	66.000	113.169	HR Cost (Senior Associate)	fixed cost
Audit activities (1FTE) (external to CISO Dept.)	66.000	113.169	HR Cost (Senior Associate)	fixed cost
Tot	**795.000**	**1.354.989**		fixed cost
Specialist Training (hp 6k euro/year for 1 FTE * 8 FTE)	48.000	48.000	+ VAT (on market services opex)	fixed cost
Tot	**843.000**	**1.402.989**		

Tab.16 – Final CISO organizational structure cost, based on standard hypothesis

[97] Richardson, R., Hiatt, M., Lowman, G. H., Napshin, S., & Perros, Y. (2021). Pay Rate Differentials. International Management Review, 17(2), 129-148.

Conclusion and Final Remarks

Cyber and Information Security are a global phenomenon with heavy macroeconomics impact and relevant effects (operational, financial, reputational, …) for sovereign states, institutions, corporates and natural persons. It can be tempting to consider Information Security, and Cybersecurity more generally, as a purely technological problem. This is a mistake that exposes all social actors (individuals, companies, institutions, sovereign states) to significant risks. Indeed, technological security measures are fundamental but not sufficient: cyber and Information Security is, first of all, a behavioral issue that must be governed through appropriate organizational and management measures.

In this thesis a non-systematic review of the scientific literature related to the following areas was conducted:

- definitions of cyber and information security problem,
- economic effects of cyber and information security events,
- individual and corporate culture and awareness,
- organization of cyber and information security (roles, responsibilities, competences, ...),
- management system of cyber and information security (policies, procedures, controls, …).

The aim of the thesis was to answer the following questions:

- RQ.1 - How does the human factor affect information security?
- RQ.2 - What is meant by IS from an organizational and management point of view?
- RQ.3 - Which frameworks best reconcile the "human factor" with the organizational and management dimensions?
- RQ.4 - Basic principles can be distilled to define an abstract organizational and management model?

With reference to the first question (RQ.1)

Human behaviors represent one of the links, probably the weakest, in a long chain. Human behaviors (both of action and of omission) determine the main risks in the field of cyber and information security and can, e.g., completely nullify purely

technological security measures even if they are valid and effective in themselves. Human behaviors are difficult (probably impossible) to fully map as human imagination, creativity and gullibility are endless.

However, the need arises to govern the human factor in order to try to minimize related risks. Within the company, the management of the human factor can take place through the adoption of suitable management systems maintained by adequate and dedicated organizational structures.

With reference to the second question (RQ.2)

In the business environment, cyber and information security have many layers and among these there are the management and the organizational ones.

The management layer needs social awareness of the problem and it is made up of a set of rules (policies, procedures, etc ...) that are adequately communicated, concretely accepted, duly applied and effectively monitored.

These rules are aimed at describing the roles, responsibilities and behaviors to be held in company processes, in order to minimize the probability of realizing a risk. A management system, however, is neither born nor evolves autonomously but must be managed by an appropriate organizational structure that has a mission dedicated to this purpose.

With reference to the third question (RQ.3)

There are many standards and frameworks that can help the company to equip itself with a management system and an organizational structure. With reference to the management system, the ISO 27001 standard was studied in depth which, unlike others (e.g. NIST, COBIT, ITIL, ...) deals with security in a fairly broad perspective, considering not only the technological dimension but also that of organization, management and control.

Approaching an ISO 27001 project is, however, complex and requires high specific internal and / or consultancy skills with the risk, I fear, of a "consultancy commodification" that undermines the effectiveness of its adoption.

With reference to organizational frameworks, the CISO was studied in depth: this role is increasingly widespread internationally and has been transformed from a "technical" profile to a c-level profile, where managerial skills are much more important than technical ones. The introduction of a CISO department, however, is very expensive and requires a complete awareness of the risks on the part of the Board of Directors and its active desire for managerial change.

Both the organizational and management model must be developed in such a way as to include all company levels, not only the technological one, potentially exposed (or related) to cyber and information risks. Furthermore, the cybersecurity program must be coherent with the entire set of legal and compliance obligations that the company have to comply with (e.g. GDPR, D.lgs 231/01, …, Labor Law, Health and Safety, …).

With reference to the third question (RQ.4)

From the evidence gathered, the following elements of reference can be distilled.

An Information Security Management System pursuant to ISO 27001 should describe, engage and govern (or being governed by) these corporate layers:

- Technology
  - Hardware, Device, IoT (HW, Device, IoT Census/Management, Supplier Governance, Security Measures, Assignment Eligible Criteria, Identity and Authentication Management),
  - Application, Services and Network (Security Architecture, Security Application, IT System Census, IT Management, Supplier Governance, Security Development Standard, Security Measures, Assignment Eligible Criteria, Identity and Authentication Management),
- Organization
  - Leadership Model (Accountability, Empowering, Business Strategy, Organization Design, Strategic Plan / Business Goals, System of Work Design (welfare and workforce capability)),
  - Structures, Roles, Responsability (ICT Dept., HR Dept., Compliance Dept., Procurement Dept., Business Unit),

    - Proxies, Powers of Attorney (Third-Party Relations, Supplier Relations),
    - Physical Security of Spaces (Offices, Server, Datacenter),
- Management
    - Statute, Code of Conduct, Sanctionary System,
    - Internal Regulatory Framework - IRF (Policy and Procedures) (Law and Framework Monitoring, IRF Empowering, IRF Writing, Reviewing, Sharing and Training),
    - Management System (GDPR System, Incident Management and Business Continuity, Decree 231/01 System, HR Administration, Procurement Administration, Reward System, User Education and Training Activities, Information and Communication Activities, Incompatibility Situations),
- Control
    - Risk Evaluation (Applicable Legislation Review, Business Activities Analysis, Risk Assessment Metodology, Recommendations and Action Plans),
    - Internal Control System (Awareness, training, information and communication, Ongoing Application and Monitoring, Segregation of Duties, Least Privilege, Processes and activities traceability, Compliance by Design (II Level Control, CoSO Report), System Adequacy Evaluation (Audit)).

The analysis of these layers must lead the Corporate to the adoption of a set of regulatory documents (Policies, Procedures, …) which will constitute the Information Security Management System (ISMS) pursuant to ISO 27001.

The issuance of the ISMS must be carried out by of suitable bodies (e.g. Board of Directors, Executive Committee, ...) considering the transversality of the areas (many of which are non-technological) and in order to guarantee the necessary empowering.

The ISMS can be subject to certification but, in any case, it must be subject to continuous audit activities in order to verify its continuous adequacy. The evidence of the application of the ISMS must be shared at all organizational levels and with all compliance bodies, including external ones, in order to strengthen an integrated approach to compliance.

From the organizational point of view, the CISO should have the following main areas of responsibility:

- Protect, Shield, Defend, and Prevent (ensure that the organization's staff, policies, processes, practices, and technologies proactively protect, shield, and defend the enterprise from cyber threats, and prevent the occurrence and recurrence of cybersecurity incidents commensurate with the organization's risk tolerance),
- Monitor, Detect, and Hunt (ensure that the organization's staff, policies, processes, practices, and technologies monitor ongoing operations and actively hunt for and detect adversaries, and report instances of suspicious and unauthorized events as expeditiously as possible),
- Respond, Recover, and Sustain (when a cybersecurity incident occurs, minimize its impact and ensure that the organization's staff, policies, processes, practices, and technologies are rapidly deployed to return assets to normal operations as soon as possible. Assets include technologies, information, people, facilities, and supply chains),
- Govern, Manage, Comply, Educate, and Manage Risk (ensure that the organization's leadership, staff, policies, processes, practices, and technologies provide ongoing oversight, management, performance measurement, and course correction of all cybersecurity activities. This function includes ensuring compliance with all external and internal requirements and mitigating risk commensurate with the organization's risk tolerance).

From these premises, starting from scratch, in the thesis it was deepened that (1) the start-up phase of ISMS implementation can cost up to 198k euros + VAT (as one-shoot costs for pilot consultancy and first go-live) while (2) the final cost of a CISO department, as well as assumed, could be approx. 1,4 mln euros / year.

The Board of Directors should evaluate these costs comparing to potential consequences and costs that could result from the non-adoption of cybersecurity program, such as the costs that the company should incur in case of cyber issues (up to 2 mln euro for single event of data breach) and consequent compliance issues.

For example, between July 2018 and April 2022, in GDPR area, Privacy Guarantors have imposed fines for approx. 100 mln euros due to "*insufficient technical and organizational measures to ensure information security*" (as per art. 32 of the GDPR).

In the event of disputes, how should the potential inadequacy of control be assessed, if there is no regulation (emanate from national or EU legislator) on controls to be adopted? Although in the absence of related jurisprudence, it is reasonable to think that qualitative standards (e.g. ISO 27001) should be considered by the public prosecutor as mandatory substitutes of national or EU regulations.

Indeed, the Board of Directors of Italian corporate should be conscious that the aware failure to adopt an Information Security Management System, duly managed by an organization structure, could ignite a corporate liability pursuant to Italian D.lgs 231/01. The entire set of legal and compliance obligations that the company have to comply with (e.g. GDPR, Legislative Decree 231/01, ...) must be considered as a puzzle: if there is a hole in the puzzle, there is an administrative liability pursuant to the Italian decree 231/01.

Frequently, therefore, the adoption of a cybersecurity program is necessary to access business networks, apply public tenders or to be accredited as suppliers, ... Cyber and Information Security starts to be a barrier to entry on the market: e.g. some industry, exposed to a pervasive sector legislation (e.g. banks, insurance, pharma, ...), need and require cybersecurity standard in their supply-chain.

In this context, it is a mandatory responsibility of the management to make the Board of Directors fully aware and informed about the real situation concerning cyber risks and corporate cybersecurity measures.

It is also the responsibility of the Board of Directors to stimulate in-depth analysis in the cyber area, starting from a clear declaration in the Strategic Plan, providing adequate resources and guaranteeing an unequivocal and continuous commitment, to be translated also among all level management's business objectives.

What has been explained up to now seems to indicate that there are some open questions to which the scientific and professional literature, standards, best practices or jurisprudence have not yet given an answer:

1. how to ensure that the Management Systems are natively developed in line and integrated with other regulatory and compliance needs?

   The compliance areas to which a company is exposed are many (e.g. GPDR, Directive 1148/16, Legislative Decree 231/01, …, and more[98]) and often address the same issue in a different way, as occurs, for example, in the definition of IT risk that each compliance area evaluates differently.

   Furthermore, the ISO 27001 Management System, for example, should not only refer to other internal regulatory areas but should be developed, even in its specific parts, in line with all the compliance areas that a company is required to respect: for example (1) from the point of view of labor law it is a risk to provide a policy that attributes company assets (laptops, mobile phones, ..., accounts for access to IT systems or for the use of institutional email, ...) to external collaborators, (2) the life cycle of the purchase and assignment of hardware and software has accounting and fiscal implications and the policies that describe these processes must take this into account, ...

   The above requires a broad and multidisciplinary overview, which is very expensive but unavoidable to provide the company with appropriate assurance.

2. how to guarantee an adequate attribution of accountability for the maintenance and development of the Management System?

   For example, an ISO 27001 Management System defines roles and responsibilities inherent to the disciplined processes, but does not seem to address the ownership of maintenance, updating and development of the Management System itself: Compliance Dept. (if any) may not have the necessary skills, ICT Dept. is in

[98] Additional to these legal requirement, Companies have to manage also a myriad of specific regulation and law concerning e.g. (1) labor law, (2) fiscal law, (3) company law, (4) copyright law, (5) Civil Code, (6) accounting principles, … that are to be considered in the compliance needs evaluation. Particular industries can have also specific legal requirement, e.g. "UE Directive MiFID II 65/14", "UE Reg. 600/14" for financial industry or "Italian Law 27/2012" and "Italian Law 135/2012" for assurance industry.

conflict of interest (since it is itself subject to control in this area), the Central Direction has too broad accountability, …

The use of specialized consultants may appear to be a solution but the company would become dependent on them. Another solution could consist in the introduction of independent organizational structures used only for this purpose: the CISO can be an example.

It would therefore seem appropriate and necessary to deepen the link between the information security organization and the related management systems.

3. In the event of legal disputes, e.g. as per art. 32 of the GDPR, with respect to which requirements is the "*insufficiency of technical and organizational measures*" assessed if there are no legal references (issued by the Italian or European legislator) that define them?

   With respect to what is the administrative liability triggered as per Italian Decree 231/01? This liability is triggered in the event of an advantage (e.g. significant economic savings) for the entity following the non-adoption, conscious and informed, of suitable measures (such as in health and safety security as per Italian Decree 81/08): however, until now in the IT security field the law does not establish how to evaluate these measures.

   This void seems to require intervention by the legislature and, in the meantime, in the appeal by the public prosecutor to reference quality standards as terms of comparison.

In closing, the limitations of the research in the thesis are summarized as following: (1) the above is the result of a non-systematic review of the scientific literature, (2) the scientific literature identified was selected by excluding, in personal judgment, some publications considered out of scope, redundant or of little interest for the research questions, (3) the practical development of the management system model and the organizational structure are modeled on the basis of standard hypotheses formulated in personal judgment, (4) the implementation costs are assumed based on personal experience and refined on the basis of thematic scouting concerning the HR cost.

Bibliography

A Guide to the Project Management Body of Knowledge (2013) (PMBOK® Guide). Fifth Edition (Project Management Institute)

Algarni, A. M., & Malaiya, Y. K. (2016, May). A consolidated approach for estimation of data security breach costs. In 2016 2nd International Conference on Information Management (ICIM) (pp. 26-39). IEEE.

Alie, S. S. (2015). Project governance: # 1 critical success factor. Project Management Institute.

Allen, J. H., Crabb, G., Curtis, P. D., Fitzpatrick, B., Mehravari, N., & Tobar, D. (2015). Structuring the chief information security officer organization. Carnegie-Mellon Univ Pittsburgh PA Pittsburgh United States, (pp. 1-33).

Amin, Z. (2019). A practical road map for assessing cyber risk. Journal of Risk Research, 22(1), 32-43.

Antczak, J. (2020). Cybersecurity Cost in an Enterprise Unit. Edukacja Ekonomistów i Menedżerów, 55(1), 82-94.

Badhwar, R. (2021). Simplified Approach to Calculate the Probability of a Cyber Event. In The CISO's Next Frontier (pp. 353-359). Springer, Cham.

Berners-Lee, T. J. (1989). Information management: A proposal (No. CERN-DD-89-001-OC).

Boehmer, W. (2008, August). Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001. In 2008 Second

International Conference on Emerging Security Information, Systems and Technologies (pp. 224-231). IEEE.

Boehmer, W. (2009, March). Cost-benefit trade-off analysis of an ISMS based on ISO 27001. In 2009 International Conference on Availability, Reliability and Security (pp. 392-399). IEEE.

Committee of Sponsoring Organizations of the Treadway Commission (2013), Internal Control. Integrated Framework.

Committee of Sponsoring Organizations of the Treadway Commission (2017), Enterprise Risk Management. Integrated Framework.

Control Objectives for Information and related Technology (COBIT)

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2020). Maximizing Employee Compliance with Cybersecurity Policies. MIS Quarterly Executive, 19(3), 183-198.

Daneshmandnia, A. (2019). The influence of organizational culture on information governance effectiveness. Records Management Journal, 29(1/2), 18-41.

Deane, J. K., Goldberg, D. M., Rakes, T. R., & Rees, L. P. (2019). The effect of information security certification announcements on the market value of the firm. Information Technology and Management, 20(3), 107-121.

Decree 231/01 – Administration Liability

Decree 81/08 – Health & Safety Liability

Decree 65/18 – Measures for a high common level of security of network and information systems across the Union,

Dieye, R., Bounfour, A., Ozaygen, A., & Kammoun, N. (2020). Estimates of the macroeconomic costs of cyber-attacks. Risk Management and Insurance Review, 23(2), 183-208.

Etges, R., & Sutcliffe, E. (2008). An overview of transnational organized cyber crime. Information Security Journal: A Global Perspective, 17(2), 87-94.

Eun, Y. S., & Aßmann, J. S. (2016). Cyberwar: Taking stock of security and warfare in the digital age. International Studies Perspectives, 17(3), 343-360.

European General Data Protection Regulation n 679/2016

Govender, S. G., Kritzinger, E., & Loock, M. (2021). A framework and tool for the assessment of information security risk, the reduction of information security cost and the sustainability of information security culture. Personal and Ubiquitous Computing, 25(5), 927-940.

Grobler, J. (2018). Cyber risk from a chief risk officer perspective. Journal of Risk Management in Financial Institutions, 11(2), 125-131.

IASC's Framework for the Preparation and Presentation of Financial Statements, paragraph 70b

Information Technology Infrastructure Library (ITIL)

Inskeep, T. (2019). "How to Properly Position the CISO for Success", SecurityMagazine.com, 37.

International Standards for the Professional Practice of Internal Auditing (IPPF Standards)

ISO 22300:2012 – Societal Security Management Systems

ISO 27001:2017 – Information Security Management Systems

ISO 45001:2018 – Occupational Health and Safety Management Systems

ISO 9000:2015 – Quality Management Systems

Kappers, W. M., & Harrell, M. N. (2020). From Degree to Chief Information Security Officer (CISO): A Framework for Consideration, 22(11), 260-288

Kaspersky (2017), "The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within," Kaspersky daily, (https://www.kaspersky.com/blog/the-human-factor-in-it-security)

Kaur, M., van Eeten, M., Janssen, M., Borgolte, K., & Fiebig, T. (2021). Human factors in security research: Lessons learned from 2008-2018. arXiv preprint arXiv:2103.13287.

Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity Awareness Framework for Academia. Information, 12(10), 417.

King, Z. M., Henshel, D. S., Flora, L., Cains, M. G., Hoffman, B., & Sample, C. (2018). Characterizing and measuring maliciousness for cybersecurity risk assessment. Frontiers in Psychology, 9, 39.

Kobis, P. (2021). Human factor aspects in information security management in the traditional IT and cloud computing models. Operations Research and Decisions, 31, 61-76.

Kruse II, W. G., & Heiser, J. G. (2001). Computer forensics: incident response essentials. Pearson Education, London.

Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. Neural Computing and Applications, 1-31.

Lee, C. S., Choi, K. S., Shandler, R., & Kayser, C. (2021). Mapping global cyberterror networks: an empirical study of al-Qaeda and ISIS cyberterrorism events. Journal of Contemporary Criminal Justice, 37(3), 333-355.

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. Business Horizons, 64(5), 659-671.

Lending, C., Minnick, K., & Schorno, P. J. (2018). Corporate governance, social responsibility, and data breaches. Financial Review, 53(2), 413-455.

Li, J. X. (2017). Cyber crime and legal countermeasures: A historical analysis. International Journal of Criminal Justice Sciences, 12(2), 196-207.

Lipner, S. B. (2015). The birth and death of the orange book. IEEE Annals of the History of Computing, 37(2), 19-31.

Lopes, I. M., Guarda, T., & Oliveira, P. (2019, June). How ISO 27001 can help achieve GDPR compliance. In 2019 14th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-6). IEEE.

Measures for a high common level of security of network and information systems across the Union, EU Directive 1148/16

Meisner, M. (2017). Financial consequences of cyber attacks leading to data breaches in healthcare sector. Copernican Journal of Finance & Accounting, 6(3), 63-73.

Moore, R. (2014). Cybercrime: Investigating high-technology computer crime. Routledge, London.

Morrison, A., Kumar, G. (2018) "Corporate Boards May Be More Likely Than Regulators to Scrutinize Cybersecurity Program Effectiveness This Year", Journal of Health Care Compliance, 49-52.

NIST Standard 800-160, Volume 2

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. HOLISTICA–Journal of Business and Public Administration, 9(3), 71-88.

Parker, D. B. (1989). Computer Crime: Criminal Justice Resource Manual.

Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. International Management Review, 13(1), 10.

Richardson, R., Hiatt, M., Lowman, G. H., Napshin, S., & Perros, Y. (2021). Pay Rate Differentials. International Management Review, 17(2), 129-148.

Ryczyński, J. (2019). Human factor as a determinant of reliability and safety of technical systems. Journal of KONBiN, 49(3), 195-220.

Sentence of the Italian Court of Cassation n. 22256/2021

Smit, R., van Yperen Hagedoorn, J., Versteeg, P., & Ravesteijn, P. (2021). The Soft Skills Business Demands of the Chief Information Security Officer. Journal of International Technology and Information Management, 30(4), 41-59.

Sophos Whitepaper. April 2021, The State of Ransomware 2021

Strupczewski, G. (2021). Defining cyber risk. Safety science, 135, 105143, 1-10.

Weidman, J., & Grossklags, J. (2019). Assessing the current state of information security policies in academic organizations. Information & Computer Security, 28(3), 423-444.

Woods, D. W., & Weinkle, J. (2020). Insurance definitions of cyber war. The Geneva Papers on Risk and Insurance-Issues and Practice, 45(4), 639-656.

List of figures and tables

Figures

Table

Online Resources Reconnaissance

➢ ISO/IEC 27001, implementation examples:

Higher Education

https://magazine.unibo.it/archivio/2021/10/01/sicurezza-dei-dati-l2019alma-mater-e-il-primo-grande-ateneo-in-italia-ad-ottenere-la-certificazione-iso-27001
https://www.imperial.ac.uk/admin-services/ict/about-ict/governance/certifications/
https://www.brookes.ac.uk/it/information-management/iso-27001/
https://www.unibz.it/it/services/ict-services/iso-certification/
https://docs.hpc.cam.ac.uk/srcp/isms-docs/information-policy.html
https://www.gla.ac.uk/media/Media_591661_smxx.pdf
https://vsix.unipd.it/certificazione-iso-27001

Other Industries

https://www.eng.it/corporate-governance/certificazioni
https://www.digitalpa.net/about-us/
https://www.oracle.com/it/corporate/cloud-compliance/
https://www.ibm.com/support/pages/ibm-iso-27001-certifications-europe-middle-east-africa
https://www.dssecurity.it/en/certifications/
https://www.onetrust.com/company/news/press-releases/onetrust-achieves-worlds-first-iso-27701/
https://www.wolterskluwer.com/en/solutions/cch-tagetik/governance-certifications
https://aws.amazon.com/it/compliance/iso-certified/
https://www.lantechlongwave.it/iso-iec-20000-27001-non-ci-fermiamo/
https://italy-vms.ru/home/
https://www.fisvi.com/en/iso-certification
https://cloud.google.com/security/compliance/iso-27001
https://www.doxee.com/about-us/certifications/
https://onit.it/en/company
https://www.asp-italia.com/sicurezza-certificata-2/
https://financeactive.com/it/stampa/finance-active-e-certificata-iso-27001/
https://en.spazioaste.it/Pages/Content/certificazioni
https://www.3d2b.com/about-us/iso-27001.html
https://www.apkappa.it/en-gb/about-us
https://www.unigum.it/en/certifications
https://www.namirial.com/en/company/certifications/

➢ Information Security Policy, implementation examples:

Higher Education

https://ist.mit.edu/about/it-policies
https://cybersecurity.yale.edu/policies-standards/yales-information-security-policy-base
https://policy.security.harvard.edu/
https://uit.stanford.edu/security
https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/data-and-system-security-policy.html
https://london.ac.uk/sites/default/files/governance/ISP-001-information-security-policy.pdf
https://www.gs.unsw.edu.au/policy/documents/itsecuritypolicy.pdf
https://www.cqu.edu.au/policy/sharepoint-document-download?file_uri=%7BBE8380F3-F86D-4C55-AC0D-84A81EAFD6A2%7D/Information%20Security%20Management%20Policy.pdf
http://www.bristol.ac.uk/infosec/policies/
https://ts.sunderland.ac.uk/csig/information-governance/information-governance-policies/information-security-policy/
https://intranet.birmingham.ac.uk/it/documents/public/Information-Security-Policy.pdf
https://policy.unimelb.edu.au/MPF1270

https://sites.cardiff.ac.uk/isf/policies/information-security-policy/
https://www.liverpool.ac.uk/media/livacuk/computingservices/regulations/informationsecuritypolicy.pdf
https://documents.manchester.ac.uk/display.aspx?DocID=6525
https://www.lancaster.ac.uk/media/lancaster-university/content-assets/documents/strategic-planning--governance/publication-scheme/5-our-policies-and-procedures/Information-Security-Policy.pdf
https://warwick.ac.uk/services/sim/
https://policy.vu.edu.au/document/view.php?id=136
https://www.ct.edu/files/it/BOR_IT-003.pdf

Other Industries

https://www.cityofpensacola.com/DocumentCenter/View/1680/Information-Security-Policy-PDF
http://www.qehkl.nhs.uk/IG-Documents/information-security-policy.pdf
https://www.janabank.com/images/policies/info-security-policy.pdf
https://www.ecips.org/ecips-infosec.pdf
https://www.cmpdi.co.in/docfiles/Approved_IT_Policy_CIL_and_Subsidiaries.pdf
https://investor.ryanair.com/wp-content/uploads/2021/12/Ryanair_Information-Security-Policy.pdf
https://www.temenos.com/wp-content/uploads/2019/07/governance-policy-information-systems-security-2019-jul-03.pdf
https://tdra.gov.ae/userfiles/assets/PvFNAE8d.pdf
https://www.celsia.com/wp-content/uploads/2021/05/information-security-policy.pdf
https://www.vakrangee.in/pdf/Policies-PDF/Information%20Security%20&%20Management%20Policy%20v3.pdf
https://www1.nyc.gov/assets/doitt/downloads/pdf/P-AS-01-Citywide-Application-Security-Policy.pdf
https://s25.q4cdn.com/701614211/files/doc_downloads/policies/Cyber-Security-Policy.pdf
https://www.uclahealth.org/compliance/workfiles/HS%20Policies/HS9450-InformationSecurity.pdf
https://www.cihi.ca/sites/default/files/document/information-security-policy-en.pdf
https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/OtherRegulatoryDocuments/Documents/CITC_Information_Security_Policies_and_Procedures_Guide_En.pdf
https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-example-data-security-policies-na.pdf
https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0_en.pdf
https://www.fujitsu.com/global/documents/about/ir/library/integratedrep/IntegratedReport2016-pdf-25.pdf
https://www.ffiec.gov/press/PDF/FFIEC_IT_Examination_Handbook_Management_Booklet_2015Final.pdf

➢ CISO dept., implementation examples:

https://resources.sei.cmu.edu/asset_files/technicalnote/2015_004_001_446198.pdf
https://www.dayblink.com/wp-content/uploads/2019/04/Structuring-the-InfoSec-Org_vFINAL_04.pdf
http://jcsitnet.com/journals/jcsit/Vol_7_No_1_June_2019/1.pdf
https://it.cornell.edu/sites/default/files/Office%20of%20the%20CIO/2021-12-15%20IT%20Security.pdf
https://media.kasperskydaily.com/wp-content/uploads/sites/92/2018/10/25062436/What-it-takes-to-be-a-CISO-%E2%80%94-Success-and-leadership-in-corporate-IT-security.pdf
https://www.mitre.org/sites/default/files/pdf/10_3710.pdf
https://www.cio.gov/assets/resources/CISO_Handbook.pdf
https://www2.deloitte.com/content/dam/insights/us/articles/ciso-next-generation-strategic-security-organization/DR19_TheNewCISO.pdf
https://fenix.tecnico.ulisboa.pt/downloadFile/1970719973966321/Extended%20Abstract_82662_Eugenio%20Tchipako.pdf
https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Charting-Your-Course-Governance-Step-2-Nov-2019.pdf
https://www.heidrick.com/-/media/heidrickcom/publications-and-reports/upendingtraditionmodelingtomorrowscybersecurityorganization.pdf
https://www.nzism.gcsb.govt.nz/pdf/index/289
https://sansorg.egnyte.com/dl/p6YbmrhJy6
https://resources.trendmicro.com/rs/945-CXD-062/images/ESG-eBook-TrendMicro-Cyber-C-Suite-Boardroom-Dec2020.pdf