2015 Italian Cyber Security Report

A National Cyber Security Framework

Editors:
Roberto Baldoni
Luca Montanari

Cyber Intelligence and Information Security Center
Sapienza Università di Roma

cini
Cyber Security National Lab

2015 Italian Cyber Security Report

A National Cyber Security Framework

Research Center of Cyber Intelligence and Information Security
Sapienza Università di Roma

CINI Cyber Security National Laboratory
National Interuniversity Consortium for Informatics

Version 1.0
February 2016

Title: Italian Cyber Security Report 2015 – A National Cyber Security Framework
Online Version, February 2016

The 2015 Italian Cyber Security Report has been realized by:

CIS Sapienza
Cyber Intelligence and Information Security

cini
Cyber Security National Lab

Working group composed of:

AON

Deloitte.

Enel

eni

hermesbay

KPMG

INTELLIUM

in cooperation with:

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Ministero dello Sviluppo Economico

Computer Emergency Response Team
Pubblica Amministrazione
CERT - PA
Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

CERT nazionale Italia

and:

Microsoft

pwc

With the participation of the Presidency of Ministry Council – Security Intelligence Department

Editors: Roberto Baldoni and Luca Montanari
Translation by Carola Norcia
Authors (alphabetical order):

Luca Albertini
Stefano Armenia
Roberto Baldoni
Fabio Battelli
Luca Boselli
Stefano Buschi
Alfredo Caputi
Salvatore Carrino
Francesco Ceccarelli
Ludovica Coletta
Romina Colciago
Cosimo Comella
Fabrizio d'Amore
Ciro Di Carluccio
Rita Forsi
Luisa Franchina
Corrado Giustozzi
Davide Grassano
Michele Kidane Mariam
Alberto Marchetti Spaccamela
Carlo Mauceli
Antonino Mazzeo
Fabio Merello
Guido Milana
Luca Montanari
Paolo Prinetto
Leonardo Querzoni
Alfio Rapisarda
Andrea Rigoni
Massimo Rocca
Valeria Risuglia
Lorenzo Russo
Federico Ruzzi
Mario Terranova
Toto Zammataro
Andrea Zapparoli Manzoni

Contents

Executive Summary

Today, the economic and social systems of advanced countries are strongly dependent on *cyberspace*, meant as the combination of networks and data systems needed to provide essential services to citizens by governmental bodies, Critical Infrastructures, enterprises and the public sector.

IT systems have become a key factor also for the management of physical facilities such as electricity networks, industrial systems, transport systems, etc. However, cyberspace and its components are affected by a high number of potential risks. First of all, as they are complex and rapidly evolving systems, their vulnerability is always present. Despite the efforts, and as today there is no possibility to have non-vulnerable systems, also because of the many "0-day" attacks available on the black market, possible threats need to be steadily taken into consideration. One or more of these vulnerabilities can be exploited by an hacker to illegally access the IT systems of an organization, allowing him to read, steal or delete critical information or even take control of its IT or physical assets. These vulnerabilities, and the fact that the awareness about them is not yet so high at each and every community level, make the cyber risk much relevant for an organization, like the financial and the reputation risks.

IT attacks have increased drastically in recent years both in terms of complexity and of resources used and they cannot be stopped by single organizations, because they need a response at country level, as they tend to diminish its economic prosperity and independence. The cyber risk cannot be removed, but it is important that a developed country is equipped with a number of tools and methods to raise the awareness, establish a structured response and support the organizations, public and private bodies and organizations on its territory, in order to reduce the risk and to mitigate the effects of possible security accidents. This context poses the issue of responsibility of public and private organizations, and of the people with representation and managerial powers, in case of violation of the duties of diligence, prudence and expertise in the protection of guarantee positions that the system confers to natural and legal persons. The endorsement of the Framework, which represents the generally accepted and purposely validated practices, allows an easier demonstration of implementation of "due diligence", by relating to objective and measurable rationales, as it puts into practice what was duly expected within the

implementation of the "duty of care" principle.

This document introduces a *National Framework for cyber security* aimed at providing to organizations a homogeneous and volunteer approach to face up cyber security in order to reduce the risk linked to the cyber threat. The approach of this Framework is strinctly linked to a risk analysis and not to technology standards.

The Framework derives much from the Framework for Improving Critical Infrastructure Cybersecurity (NIST), targeted to Critical Infrastructures [15], also in order to favour International harmonization. Anyway this framework has been tailored according to the Italian production context with a specific focus on small and medium enterprises. The National Framework derives from the NIST Framework the basics of Framework Core, Profile and Implementation Tier, adding the priority and maturity levels to the 98 Subcategories of the Framework Core. The third concept introduced in this document is the notion of Framework contextualization. A company that would like to use the Framework should, firstly, identify a contextualization according to which it can evaluate its actual risk profile. A contextualization of the Framework implies the selection of subcategories of the Framework Core and the definition of the related priority and maturity levels. The contextualization is performed according to business profile, sector vulnerabilities, organization size and other company or sector characteristics. The contextualization of the Framework can be performed by various players, such as industry associations or by the same organization, if it has the competences to do so. In case of regulated production sectors, Framework contextualizations can be performed by the sector regulators so to harmonize them with the sector regulations related to cyber threats.

For example, this document provides a contextualization for small and medium enterprises, independently from a specific production sector.

Once the organization has adopted a Framework contextualization, it is able to assess its *current profile* against the cyber risk. Then, the organization should identify its *target profile*, which reflects the target of a company cyber strategy. The planned schedule and the methods of the organization to pass from its current profile to the target profile are up to the organization self.

It is important to remark that the Framework is not a security standard, but a common reference to identify existing and future sector standards and regulations. The task of standard definition is responsibility of national and international standardization bodies and institutions, as well as of industry regulators. The Framework endorsement is voluntary.

Besides the discussion about the relationship between the current Italian regulatory framework and the Framework Core Subcategories, this document introduces also new options to enhance protection against the cyber risk through the transfer of the residual risk to insurances. This way, insurance companies and insured subjects follow a virtuous path to reduce the economic consequences of risk materialization. The organization creates the preconditions to reduce the risk to an acceptable level for its security – even according to a cost-benefit, risk tolerance and risk appetite evaluation – and for the insurance market, which, in turn, shares with the organization a virtuous win-win process for both Parties (guarantee of balance protection for the organization; social role and profitability guarantee for the Market). In the end, the Framework helps the organization to describe the maturity and severity level of its cyber risk management practices.

This document is structured into three parts. Part I presents the National Framework, its motivations and guidelines for the use of the Framework for some particularly relevant players.

Part II presents the Framework Core, a contextualization of the Framework for small and medium enterprises and a series of recommendations for Large Enterprises on how to implement the cyber risk management process. Part III shows how the Framework related with the Italian

regulatory context and the specific sector regulations. In particular, it contains also a detailed analysis on cyber risk management and the relationship with the insurance market.

Considering the particular dynamic nature of cyberspace threats and the drastic technology development, this document will be steadily adjusted and regularly integrated according to feedback, best practices and lessons learnt over the time. The implementation of this Framework by the organizations in our country may strengthen the entire country system against cyber attacks.

1. Introduction and reading guide

Nowadays the entire economy and the welfare services of a developed country are based on facilities and services provided through the cyber space, a cluster of interconnected and heterogeneous networks, protocols and IT applications all around us. IT accidents impacting such facilities and services may have huge economic consequences at national, enterprise and single citizen level. Such accidents impact not just the cybernetic framework, because they may start there and then reach the physical facilities too, causing even primary services to be unavailable, therefore leading to an economic loss or even human loss. Accidents may be normal or caused by terrorists, cybercriminals, activists and by foreign countries (cyber-warfare). In those cases, if the victim is a company, beside the damage to its image, it may suffer a huge financial damage: From a simple loss of competitiveness up to the complete loss of the strategic asset control (IPR, process methodologies, IT systems, etc.). In the case of a country, it may lead to a reduction of defensive capacity or even a loss of independency. For a citizen, the cyber threat may cause damage to rights and constitutional concerns such as life, physical integrity, fundamental freedom, including the right to confidentiality, beside other economic impacts. In this document, cyber security is defined as follows:

Cyber security is the practice that allows an entity (as for example an organization, citizen, nation, etc.) to protect its own physical assets and confidentiality, integrity and availability of its own information against the threats posed by the cyberspace. In turn, *cyberspace is defined as the complex environment derived from the interaction of people, software and services on the Internet through technologies, devices and networks linked to it*[1].

Cyber threats certainly cannot be faced by giving up the potentials offered by the IT systems and their interconnection within the network, thus loosing the increase of productivity and efficiency linked with computerization. The answer should be systematic, aimed at raising the citizens' awareness, the "duty of care" of companies and the International "due diligence" of the country about the cyber threat. As reported in detail in an OECD document [23] and reiterated various times in our report in the last years [5, 6] , it is crucial that in this process of collective

[1] Compared to the definition introduced by the ISO/IEC 27000:2014 standard[10] and ISO/IEC 27032:2012[11], from which it derives, the definition includes also the protection of company physical assets, besides the IT ones.

raising awareness, we shift from an idea of "IT system security" or "IT security" to that of "cyber threat management". This means, among other things, to define a process that respects the Constitution principles regarding, for example, the business activity management in order neither to contrast the social benefit nor to affect safety, freedom and human dignity. This consideration implies that the cyber security perspective is not to be seen just in technologic terms, but rather requires taking into account the overall legal and formal duties and the principles of social interest, into which the public and private framework need to converge. For this reason, the duty of protection should become part of the top management responsibility of an organization, as it requires a specific and accurate evaluation by the ones who have the direction and management power[24].

As any company risk, the cyber risk cannot be eliminated and therefore requires a series of coordinated actions to be taken in order manage it. Such actions involve the organization and technology departments of the company, in addition to the financial management of the risk, also through the establishment of a residual risk management strategy and a strategy to protect the company balance. Furthermore, the cyber risk is intrinsically highly dynamic. It changes as threats, technology and regulations change. To start approaching this issue in a way which is useful for the country system (State, enterprises and citizens) it is necessary to define a common ground, a Framework, in which the various production sectors, government agencies and regulated sectors can recognize their business, so to align their cyber security policies in a steadily developing process. To reach this aim *a common Framework should be first of all neutral both in terms of business risk management policies and in terms of technology*, so that each player could keep on using its own risk management tools, managing its technology assets while monitoring at the same time the compliance with sector standards.

This document presents a National Framework for cyber security aimed, firstly, at creating a common language to compare the business practices to prevent and tackle cyber risks. The Framework may help an enterprise to plan a cyber risk management strategy, developed over the time according to its business, size and other distinguishing and specific elements of the enterprise. The Framework adoption is voluntary.

The Framework we present is based on the "Framework for Improving Critical Infrastructure Cybersecurity" issued by the NIST[15], from which it inherits key concepts such as Framework Core, Framework Implementation Tier and Framework Profiles. Thus, it adopts the Function and Category system of the Framework Core, which in facts represents that common ground, the meeting point between Framework and company standards, both technical and risk management standards.

The choice to use the US Framework is based on the idea that the answer to cyber threats should provide an alignment at international level, not only at national level. This is also to allow the corporation to align their cyber security management processes in an easier way at international level.

The NIST Framework offers a highly flexible framework, which is mostly targeted at crucial facilities; we developed it according to the characteristics of the social and economical system of our country, reaching a cross-sector framework that can be contextualized in specific production sectors or in company types with specific characteristics. This allows the transfer of practices and knowledge from one sector to another in an easy and efficient way. In this sense, we have introduced three important concepts in the National Framework:

Priority levels. The priority levels define which is the priority associated to every single Subcategory of the Framework Core. It should be noted that every organization is free to adapt its own priority levels according to type of business, size and own risk profile.

Maturity levels. The maturity levels define the various ways in which every single Subcategory of the Framework Core can be implemented. The selected maturity level is to be carefully evaluated by each single enterprise according to its business and size, as well as its risk profile. Typically, higher maturity levels require greater effort both in financial and management terms. For some Subcategories it is not possible to establish maturity levels.

Framework contextualization Creating a contextualization of the Framework (for a productive sector, for business type or a single business), means to select the Function, Category and Subcategory of the relevant Framework Cores, specifying the priority and maturity levels appropriate for the implementation context.

This document offers a context for Small and Medium Enterprises (SMEs), that is a context for each type of business, that is for whatever business sector (for details see Chapter 6). The choice to provide a context for SMEs is linked to the fact that these enterprises can be part of the food, manufacturing, logistic or mechanic sectors that can be particularly sensitive to cyber security topics. The aim is to provide to them the practical tools needed to initiate a virtuous path to strengthen their cyber protection. These SMEs develop services and/or products of higher quality, often through processes and methods that have been improved over the time and represent the true value of the company. If those strategic assets are threatened by cyber attacks, the company existence self is put at risk, and often it does not realizing on time what has happened.

Other contextualizations could be done specifically by trade associations and regulatory bodies, so that they are acknowledged by an entire production sector or by a regulated sector. As far as regulated sectors goes, in some cases the implementation priorities of some security controls at a basic maturity level could become compulsory according to sector regulations. Section 3.4 provides details about who can create a contextualization of the Framework and on how to do this.

Each organization can adjust its own cyber security policies to its own business, risk tolerance and available resources, by defining the residual risk management strategies. This concept is expressed by the notion of *current profile* of the organization. The current profile is created by comparing the existing cyber security practices with the Framework Subcategories and related maturity levels. Through this comparison, the Subcategories that are already implemented by the existing practices with related maturity level are selected. This selection creates the current profile, to be compared with the *target profile*. The target profile consists in the selection of Subcategories and of the desired maturity levels, according to the organization needs. To have a current and target profile favors the gap analysis process and the definition of a roadmap to be followed in order to obtain the target cyber security level. In establishing the roadmap, the Subcategories with *high priorities* are the first to be implemented. Subcategories with *medium priority* and *low priority* have to be selected according to one's own needs and then implemented.

Furthermore, the Framework supports the company in the evaluation of its own cyber risk management process through an assessment based on *implementation tiers*, that derives from the NIST Framework. Tier 1 identifies an ad-hoc risk management for cyber security. Tier 2 corresponds to the "risk informed" level, when the risk management processes work but are not integrated. Tier 3 corresponds to the "repeatable" level, in which formal policies for risk management work and are integrated and Tier 4, "adaptive", where the risk management processes are introduced within the company culture. Examples of contextualization of these Tiers have been elaborated by Intel [9], Langner [26] and by The Communications Security, Reliability and Interoperability Council [18]. Also in this case, the organizations have to evaluate

their risk management and plan a schedule in order to move gradually towards Tiers 3 and 4. For more details on the implementation tiers, see the Framework NIST document[15].

Figure 1.1 shows the relationship between the National Cyber Security Framework and the specific characteristics of an organization: implemented Enterprise Risk Management practices, applied IT security standards with related certifications, organization size and production sectors. In particular, the Framework, on a higher level of abstraction, serves as a bridge between the Enterprise Risk Management tools and the IT & Security Standards. The Figure shows the productive sector contextualization and the contextualizations based on the type of company. It should be noted that for each productive sector and each company type, various contextualization can be defined. As first step in the Framework implementation process, the company should select a contextualization to be used 3 for more details).

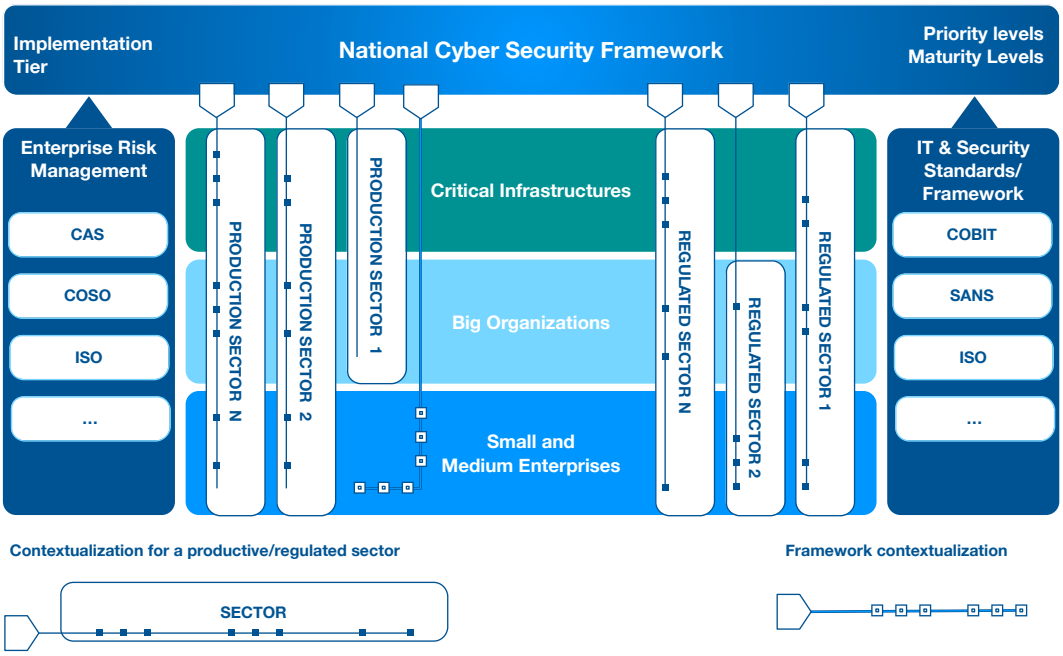

Figure 1.1: National Cyber Security Framework and its link to the enterprise risk management, IT security standard, enterprise size and production sectors

We point out that the National Cyber Security Framework is not a static document, but rather a live one, which has to be updated according to the evolution of the threat, of technologies, of cyber security and of the risk management techniques. Such update should be censure by institutional competent bodies for its maintenance over the time.

Document reading guidelines

This document is structured into three parts. Part I presents the National Framework, its motivations and guidelines for the use of the Framework for some particularly relevant players (Chapter 3 and Chapter 4). Part II presents the Framework Core (Chapter 6), a contextualization of the Framework for Small and Medium Enterprises and a series of recommendations for the Large Enterprises on how to implement the cyber risk management process. Part III provides some considerations linked to the context of national implementation of the Framework. In

particular, it contains details on the Enterprise Risk Management, an in-depth analysis of the insurance market and cyber policies, the relationship with the Italian regulation framework and an in-depth analysis related to specific regulated sectors.

Below some reading guidelines of Parts I and II of the document are identified for various types of readers:

Small and Medium Enterprises. Chapter 6 shows a contextualization of the Framework for Small and Medium Enterprises. The contextualization provided for the SMEs consists of: a selection of Subcategories (Section 6.1), of the various priority levels to be followed in the implementation of selected Subcategories (Section 6.2), maturity levels for high priority Subcategories (Section 6.3) and an implementation guide for them (Section 6.4). SMEs that are interested in establishing their own cyber security strategy and in implementing it, can benefit from such tools.

Large Enterprises, Critical Infrastructure and companies of national strategic relevance Chapter 7 provides suggestions on how a big enterprise can use the Framework. In this context we assume that Large Enterprises own the risk management competencies to adapt the Framework to the context. In particular, it contains some recommendations for the top management on how to manage the cyber risk and on how to organize the related process. It explains the difference between a Security Operations Center (SOC) and a Computer Emergency Readiness Center (CERT). Eventually, it presents an advanced cyber risk management process in a big enterprise.

Sector regulators. As far as sector regulators concerns, the Section 4.4 of the Chapter 4 presents a guide for the Framework implementation. Furthermore, Sections 11.1 and 11.2) provide two examples of positioning respect to the Framework of highly regulated sectors such as Government Agencies, bank sector and listed companies. Furthermore, it shows how such sectors can benefit from the Framework implementation.

In the final part, Chapter 8,9 and 10 are of general kind: The first deals with the topic of Enterprise Risk Management; the second with the transfer of risk to the insurance market; the third provides the link between the Framework subcategories and the Italian regulation context, in particular the one linked to the Privacy Code and the one derived from the DPCM of the 24/1/2013.

PART I – A National Framework

2. The need for a National Framework

Recently, public opinion has been exposed to many striking cases of cyber attacks, some of them with relevant effects. In some cases it was about attacks of players linked to governments, such as, for example, the attack to the Sony Pictures after the distribution of the movie "The Interview"; in other cases, it was about the use of cyber dimension for various activities and attacks (terrorism, intelligence operations, military interventions). Even Small and Medium Enterprises (SMEs) are realizing that the problem might involve them, although they do not always understand that the consequences could be devastating.

The awareness level has increased as a consequence and companies begin to ask themselves about their degree of preparedness. This process of raising the awareness, which is still extremely immature in our country, should be necessarily supported by methodological tools. Such tools should be simple, suitable to any user, able to provide a roadmap to reach a minimum readiness level to protect information and/or one's own image as well as the company image. This National Framework has been created exactly with this aim.

In the end, it is crucial to point out that the cyber threat requires a public-private response first of all at national level. None of the two players individually is able to provide a response to this threat, because the private sector is not able to control the threats coming from every part of the world and the public sector needs the private one because many primary services are now managed/provided by it and any attack may lead to direct consequences on citizens. As reported by the White Book "The Future of cyber security in Italy", published in November 2015 [3], the National Cyber Security Framework represents one of the essential tools to increase the domestic resilience of systems and networks against such threat. *The Framework implementation is therefore a crucial step even to improve one's own image, and so to promote international investments in our country.*

2.1 The advantages for the Italian context: SMEs, Large Enterprises and sector regulators

Small and Medium Enterprises.

The Italian framework is mostly made of SMEs, most of them have never faced the issue of IT security. This is generally due to a lack of cyber risk assessment: sometimes Small enterprises do not consider that they have information assets to protect, sometimes they do not know the many tools that modern hackers may use. The main issue for small enterprises, once they approach the security dimension, is represented by costs: They are not independently able to identify "quick-win" practices, which allow higher protection levels with minimum effort. As a consequence, these companies risk to make a wrong estimate of costs needed for their asset security, and this often make them give up the idea of improving security, with enormous consequent risks, which they are not aware of. The Framework provides a series of security practices that, especially for SMEs, are basic and economic at the same time. Such practices are called "high priority practices" (see Chapter 6) and correspond to that set of operations, which bring the level of awareness, protection and therefore security to a basic value, which is sufficient for most of the Italian SMEs.

Large Enterprises.

The National Framework does not pretend to guide Large Enterprises or to replace their complex risk management. It can be yet very useful to support, through a unique method, the company risk management programs and processes, so to make them evolve consistently and in a structured way (see Chapter 7). Furthermore, Large Enterprises can benefit from the Framework for two fundamental aspects: its international nature and the possibility to require security profiles to their contractors. The Framework, indeed, is based on the NIST Framework, therefore it is fully compatible with the security profiles and assumes the international nature of the latter. As a consequence, it can favour the communication of its own security levels and known standards (as for example the ISO standards), but in an extremely cheaper way. From the contractors' point of view, Large Enterprises and Critical Infrastructures may use the Framework to require given security levels to all or some of the players that form part of their supply chain, or just to the ones who have to deal with given resources. This mechanism increases the security of the entire enterprise environment and, as a consequence, minimizes the vulnerability to attacks.

Sector Regulators.

As far as sector regulators concerns, the National Framework provides ground for a clear and unique exchange, where it is possible to work consistently with regulatory companies as well as other regulators. The Framework may be used as a tool to define regulations and standards in a structured and compatible way together with other regulators. It enables the assessment of possible specific national, European and international regulations, general or specific ones, avoiding additional burdens and promoting the dialogue between regulator and regulated entities. Sector regulations, like all other regulations, remain effective, after their issue, for extremely long periods, compared to the evolution speed of the cyber threat. Therefore, it is important to establish review processes, especially for sectors, in which the security management is particularly crucial (e.g. bank sector, government agencies, etc.). The Framework can be used for a preliminary review of regulations at first, and then it is possible to follow the evolution of the Framework in order to update regulations and practices. Furthermore, establishing a mapping among sector rules and practices of the Framework represents a very useful exercise in order to point out the possible defects, which inevitably widen the attack territory for companies of one's own sector.

2.2 Framework and cyber risk management

The main task of cyber security is to protect and safeguard the organizations/companies' mission against the risks posed by cyberspace and IT systems. All organizations are exposed to many risks of various kinds. Even if there are many definitions, common sense shows that risk is nothing else but loosing something valuable: This value may be a physical object, money, health status, a social value, a degree of emotional wellbeing. Risk is therefore linked to uncertainty of foreseeable or sudden, direct or indirect, measurable and non-measurable events. Uncertainty is linked both to events and to their causes and effects that are not always definable and identifiable. Because of such uncertainty, the same risk can be perceived in a very different way according to the one who evaluates its characteristics.

No matter the sector or the type of risk, it is agreed to define the risk as the materialization of a negative event that can compromise the company targets. It can be seen as the result of three factors: threat, vulnerability and impact. The analysis of the three fundamental components can help an organization to reduce the risk with a number of techniques, from the reduction of vulnerability to the reduction of possible damage; in some cases it could also be possible to reduce the threat. Each organization has to evaluate its own risks according to its tolerance degree and decide what the countermeasures to be put in place are. In general, as it is a concept highly linked to the random nature of variables that cause it, it is not considered possible to reduce a risk to zero, therefore there is always a degree of residual risk to be taken into account. The organizations have to evaluate the balance between risk reduction, residual risk and their own risk "tolerance". Residual risk can therefore be accepted or transferred in its economic consequences outwards, for example through the use of insurance products. Another example is to turn to a Managed Security Services Provider (MSSP), in order to oversee the risks in a given security framework: e.g., the timely identification of suspected events or impairments that can compromise the integrity, availability and confidentiality of information. Such approach is particularly common for SMEs, for which it can be inconvenient to allocate human and technology resources in monitoring security events and therefore for the protection of that specific area. The practices of analysis and evaluation of risk mitigation, acceptance, transfer or avoidance options is called Risk Management. The evaluations linked to risk management may not be delegated: They represent a fundamental element in the organization management and their approval is inalienable responsibility of the top management.

The Cyber Security Risk Management is an implementation of the discipline o risk management in the cyberspace framework. As the three fundamental characteristics of the cyber risk (i.e. vulnerability, threat and damage) are often strongly interrelated with other risk domains, the cyber security risk management, like other types of risk analysis and management, cannot be considered as a stand-alone discipline, but as one of the key elements of the so called "Enterprise Risk Management". As we will see, the Framework provides a methodological system to design a process of cyber security risk management (an example of this process is described in Section 7.2).

2.3 Advantages for the country system: Towards an international due diligence

Considering that the economical, technologic and, consequently, the political aspects of cyberspace activities at international level will shortly become a crucial point of geopolitics, a national framework for cyber security is one of the elements that a country, as well as private companies under its jurisdiction, needs in order to secure the networks and IT systems. Beside the National Framework, further essential elements of a national system to increase the resilience to attacks are:

- an efficient CERT network: In 2014, Italy has created its own national CERT[1]. The national CERT supports citizens and enterprises through awareness raising, prevention and coordination of reaction to large scale cyber accidents. Furthermore, through a link with the other Government CERTs (CERT-PA for Public Administration and CERT-Defence), it can provide an updated overview on relevant events, that are useful to update and develop the enterprises' cyber security programs;

- a system to share public-private (with bidirectional exchange) following the US ISAC pattern, in which enterprises of the same production sector or with very similar cyber risk exposure gather around joint working tables [4]. These round tables aim at preventing the cyber threat through appropriate intelligence actions;

- an integrated system of interactions between public-private-national research made of technology programmes, joint research centres, etc. [3], in which to find a technology reference point for defense and crisis management operations.

The single organization, besides interfacing with the previous elements, should implement internally the technology best practices that are typical of the IT risk management, such as: disaster recovery systems and business continuity of systems and networks, audit, vulnerability research of systems and security certifications of its own systems.

This Framework of measures that go seamlessly from public to private, besides protecting our national economic interests, may be of crucial relevance within legal disputes between enterprises or international disputes among States, due to cyber attacks. Indeed, mitigating or worsening one's own position will depend on the "duty-of-care" or "negligence" that a State, company or both of them have followed over the time to minimize the cyber risk. From this point of view, the National Cyber Security Framework represents a tool to identify possible deficits within the cyber security management of an organization, both in the public and in the private sector and to define a risk management strategy that persists as the threat and technology change.

[1] The National CERT is available at `http://certnazionale.it`. The National CERT serves as aggregator and "certifier" of contributions, notification of highly reliable information coming from public and private, national and international entities. Enterprises can share, in a protected and safeguarded manner, all their information with the national CERT and with other validated subjects.

3. Basics

The National Framework as defined in this document is based on the ”Framework for Improving Critical Infrastructure Cybersecurity” [15], developed by the US National Institute for Standards and Technology (NIST), to be extended according to the national context. This choice is based on the fact that the Framework, deriving from the NIST, provides a full coverage and is at the state of the art of the life-cycle of information and system security, by maintaining the right abstraction degree that ensures to the companies freedom in the implementation and contextualizations of controls. As it has been created fro Critical Infrastructures, it introduces a complexity level which is not suitable for most of the companies of the Italian enterprise context. Even if it is a Framework, it needs to be updated according to the comments given by the companies implementing it, according to threat change and technology and organization development. Otherwise, regulators and standardization bodies may make their regulations and standards evolve. Furthermore, the fact that the National Framework, as defined here, is based on the NIST one, which has already been implemented in other countries, ensures its uniformity and ease of use, especially for corporations, which will not have to face different directions for each and every country.

The NIST Framework core is made up of 21 Categories and 98 Subcategories, structured into 5 Functions. Each Subcategory represents a recommendation area, that the organization may decide to implement, if necessary by referring to the specific sector standard or regulation. The NIST Framework provides references to existing standards and Frameworks for each Subcategory: It is a partial mapping that covers most of the references already implemented by International organizations, such as the NIST Standard, the ISO/IEC and the COBIT Standards.

The National Framework extends such structure by introducing two new concepts: priority levels and maturity levels. These two concepts allow to take account of the economic structure of our country, which is made of dozens of big companies and Critical Infrastructures and many small enterprises, therefore the Framework is suitable for SMEs, but remains targeted to Large Enterprises and Critical Infrastructures.

3.1 Framework Core, Profile and Implementation Tier

The Italian National Framework derives three fundamental concepts from the NIST Framework: Framework Core, Profile and Implementation Tier. Below they are briefly described, for further details, refer to the original document [15].

Framework Core. The core represents the life cycle structure of the management process of cyber security, both from a technical and organizational point of view. The core is structured hierarchically into Function, Category and Subcategory. Concurrent and continuous Functions are: Identify, Protect, Detect, Respond, Recover and they represent the main topics to deal with in order to strategically obtain an appropriate cyber risk management. Thus, the Framework, for each Function, Category and Subcategory, which provide information in terms of specific resources, defines the processes and technologies to be put in place in order to manage the single Function. Finally, the Framework core structure shows *informative reference*, informative references that link the single Subcategory to a number of known security practices by using sector standards (ISO, sp800-53r4, COBIT-5, SANS20 and others). The Framework Core structure of the NIST is showed by Figure 3.1.

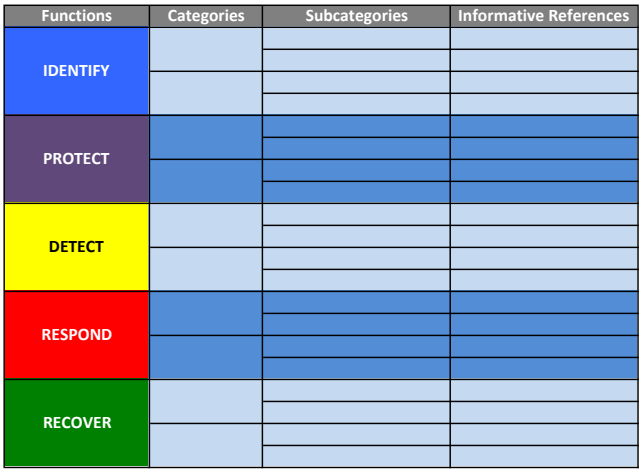

Figure 3.1: Framework Core structure (from [15])

The 5 Functions are briefly described below:
Identify. The *Identify* Function is linked to the understanding of the company context, of assets that support the critical business processes and relevant associated risks. Such understanding enables the organization to define resources and investments according to the risk management strategy and company objectives. The Categories within this Function are: Asset Management; Business environment ; Governance; Risk analysis; Risk management strategy.

Protect. The *Protect* Function is linked to the implementation of measures aimed at protecting the business processes and company assets, regardless of their IT nature. Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

Detect. The *Detect* Function is linked to the definition and implementation of appropriate activities aimed at identifying IT security accidents on time. Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes

Respond. The *Respond* Function is linked to the definition and implementation of appropriate activities in order to take action in case of detection of an cyber security event. The aim is to

reduce the impact of a potential cyber security event. Categories within this Function include: Planning; Communications; Analysis; Mitigation; and Improvements.

Recover. The *Recover* Function is linked to the definition and implementation of activities aimed at the management of plans and activities to restore processes and services impaired due to a cyber security event. The aim is to ensure the resilience of systems and facilities and, in case of accident, to support the timely recovery of business operations. Categories within this Function include: Recovery Planning; Improvements; and Communications.

Profile. Profiles represent the result of the selection made by an organization, of specific Subcategories of the Framework. Such selection can be performed according to various factors, that are mainly linked to risk assessment, business context and applicability of the various Subcategories. Profiles can be used as an opportunity to improve the security status by comparing an actual profile (also called current profile), with the wished profile (also called target). In order to develop a profile, an organization has to analyse each of the Subcategories and, according to the business driver and evaluation of one's own risks, to establish which ones have to be implemented and which ones are applicable to one's own context. Subcategories can be integrated with further practices, that are not provided by the Framework, for a complete risk management. The actual profile can therefore be used to define priorities and to measure the advancement towards the target profile. Profiles can be used also to perform a self-evaluation or to communicate one's own risk management level within or outside the organization. Finally, it should not be underestimated its use to define minimum profiles required by an organization in order to benefit from services provided by third parties. This use strengthens the entire supply chain in case of specific critical issues.

Implementation Tier. The implementation Tiers provide a context on how the company, as a whole, considers cyber risk and processes to manage it. There are four evaluation levels, from the softest to the hardest one: (1) Partial, (2) Informed, (3) Repeatable, (4) Adaptive. In particular:

Partial. The cyber security risk management of an organization is partial if it does not systematically take account of cyber risk and environmental threats.

Informed. The cyber risk management practices of an organization are informed if the organization has internal processes that take account of the cyber risk, but they do not cover the entire organization.

Repeatable. The cyber risk management model of an organization is repeatable if the organization regularly updates its own cyber security practices based on the risk management process output.

Adaptive. The cyber risk management model of an organization is adaptive if the organization frequently adjusts its cyber security practices by using its past experiences and risk indicators.

3.2 Priority levels

The priority levels help to support organizations and companies in the preliminary identification of Subcategories to be implemented in order to further reduce their risk levels, while balancing the effort to implement them. The Framework suggests the use of a priority scale of three levels among Subcategories. The objective is to:

- Simplify the identification of essential Subcategories to be immediately and binding implemented;
- Support the organizations in their risk analysis and management process.

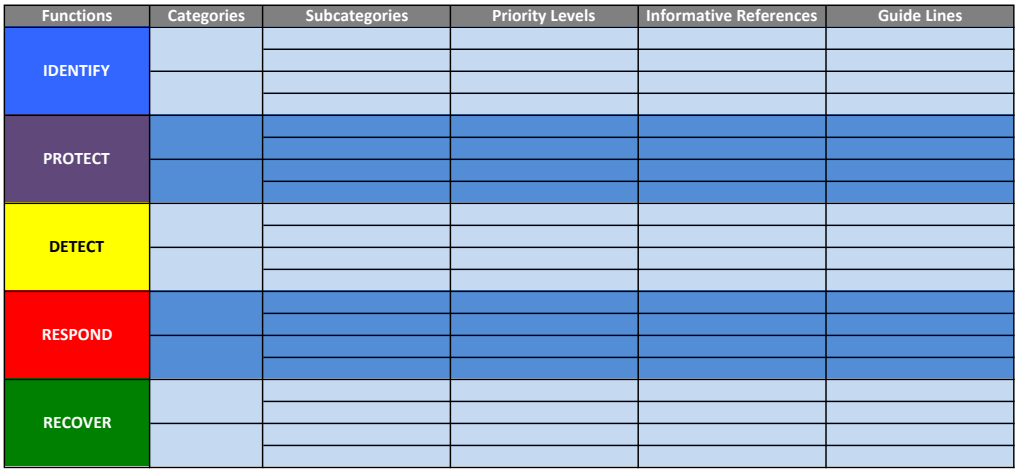

Figure 3.2: National Framework with priority levels related to Subcategories and with guidelines

The identification of priority levels assigned to Subcategories should be performed according to two specific criteria:

- Ability to reduce cyber risk, by working on one or more key factors for the identification, that is:
  - Exposure to threats, intended as the set of factors that increase or diminish the threat probability;
  - Occurrence Probability, that is the frequency of the possible event of a threat over the time;
  - Impact on Business Operations and Company Assets, intended as the amount of damage resulting from the threat occurrence;
- Ease of Subcategory implementation, considering the technical and organizational maturity usually required to put in place specific countermeasures.

The combination of these two criteria allows the definition of three different priority levels:

- High Priority: Actions that enable the slight reduction of one of the three key factors of cyber risk. Such actions are prioritized and must be implemented irrespective of their implementation complexity;
- Medium Priority: Actions that enable the reduction of one of the three key factors of cyber risk, that are generally easily implementable.
- Low Priority: Actions that make possible to reduce one of the three key factors of the cyber risk and that are generally considered as hard to be implemented (e.g. significant organizational and/or infrastructural changes).

Note that some Subcategories assume a specific priority for the used contextualization or assume a specific priority according to the organization context (possibly based on the associated risk evaluation), therefore, each organization, by implementing the Framework or during the contextualization activity, may redefine the specific priority levels for each Subcategory.
Appendix 6 presents a Framework contextualization for SMEs, by defining the priority level for each Subcategory and an implementation guide.

3.3 Maturity levels

Maturity levels enable the measurement of maturity of a security process, maturity of a specific technology implementation or an assessment of the amount of resources needed to implement a specific Subcategory.

Maturity levels provide a reference according to which each organization may evaluate its own Subcategory implementation and establish targets and priorities for their improvement. The levels must be incremental, from the lowest to the highest. Each level has to provide incremental practices and controls respect to the lower maturity level. Each organization will evaluate the satisfaction of control in order to identify the maturity level that has been reached (Figure 3.3). For some Subcategories it could not be possible to define maturity levels (see Subcategory ID.GV-3 in 6.3 for example).

Figure 3.3: National Framework with introduction of maturity levels.

Tables 3.1 e 3.2 provide two examples of maturity levels for two Subcategories of the Framework, while Section 6.3 reports the maturity levels for all high priority Subcategories of contextualization given for SMEs.

Table 3.1: Example of maturity levels for Subcategory “PR.AC-1: Identities and credentials are managed for authorized devices and users”.

Level and Description	
M1	Identities and credentials are administered locally on each device and IT system.
M2	Identities and credentials are administered through a company directory that allows the homogeneous implementation of rules and minimum security levels.
M3	Specific technology solutions are adjusted in order to specifically and appropriately manage privileged users (ee.g. System Administrators).

Within the definition of maturity levels, the following characteristics have to be taken into account:

- Specificity for Subcategory. An organization may have various maturity levels for different Subcategories;

Table 3.2: Example of maturity levels for Subcategory "ID.BE-3: Priorities for organizational mission, objectives and activities are established and communicated".

Livello	Descrizione
M1	M1.1. The company ha defined a cyber Security strategy.
M2	M2.1. Within the strategy, the objectives and activities of the company cyber Security are defined. M2.2. The strategy is aligned with the company strategic objectives and risks. M2.3. The strategy defines the approach for the Governance of cyber security. M2.3. The strategy defines the structure and organization to implement the program. M2.4. The strategy is approved by the Board of Directors.
M3	M3.1. The strategy is regularly updated in order to take account of business changes, operative context changes and risk profile changes.

- Completeness of security practices. The maturity level of a Subcategory corresponds at least to the one in which the related security practices are performed.

This enables to:

- Define partially or entirely one's own maturity level;
- Identify the target level: Partial or overall;
- Identify the necessary security practices in order to reach the target level.

In general, the Framework provides just the rules to define the maturity and priority levels, as these and their related controls are extremely linked to the company nature, the business sector, the its structure and size, as well as to the business model. In terms of SMEs context, this document presents a specific contextualization, the priorities for this company segment and the minimum maturity level to be provided in order to raise one's own ability to manage the Cyber risk.

3.4 How to contextualize the Framework

Framework contextualization for a production sector or an homogenous category of organizations means to specify its core (i.e. to select the Functions, Categories and Subcategories) and to specify the priority and maturity levels for the selected Subcategories. Up to now, all notions have been introduced regardless, for example, of the production sector, type of employees, size and position of the organization on the territory. When a Framework is contextualized, all or some of the previously described elements are taken into account. A Framework contextualization is performed following the steps below:

1. select the list of relevant Functions/Categories/Subcategories for the organization according to all or some of the previous elements (production sector, size and territorial position of the organization, etc.);
2. define the priority levels for the implementation of the selected Subcategories;
3. define the guidelines at least for high priority Subcategories;
4. specify the maturity levels at least for high priority Subcategories;

All organizations that implement a specific Framework contextualization, must always implement high priority Subcategories, at least at a minimum maturity level.

3.4.1 Who can perform a Framework contextualization

The above steps must be implemented according to the specific business characteristics of the organization. Below is a list of the ones who can carry on the task of Framework contextualization. The Framework can be contextualized:

1. by the single company for the management of its cyber security program. This implies that the company is enough mature to manage the above steps and the following associated risk management model. For example, Intel was one of the first to provide a case study on how to contextualize the NIST National Framework for cyber security [9].

2. by an association of a production sector, in order to make the Framework contextualization available to all companies of the sector. This contextualization can also take into account the company size. For example, the IV work group of the CSRIC (The Communications Security, Reliability and Interoperability Council) provided a Framework contextualization for the communication sector, including producers of satellites, TV networks, landline networks and wireless networks in the United States [18].

3. by a sector regulator in order to make the Framework contextualization available to all organizations of the sector. Contextualization can also take into account the company size, beside the specificity of the regulated sector.

4. by any player that defines a Framework contextualization according to one ore more characteristics that the companies have in common, as for example geographic location, size, staff type, etc. A typical case may be a local group of small and medium enterprises that use services provided by a consortium. The latter can contextualize the Framework for that companies. Finally, this document describes in Part II a contextualization of the Framework for SMEs made by a mixed group of academics and IT security professionals. This contextualization is therefore part of this category.

It should be noted that every single organization, even if a contextualization is provided by a regulator or a sector organization, may define and include further Subcategories or specialize the existing ones according to its own business and cyber security targets.

3.5 How to update the Framework

The Framework is a dynamic document and as such it is to be updated according to threat change and technological and organizational development. Therefore, the core (category and Subcategory), priorities, maturity levels and implementation Tier need to be reviewed from time to time. Institutions are responsible for the definition of the Framework contextualization and of their development and maintenance over time. The institutions are also responsible of establishing appropriate international relationships so to keep the Framework aligned with the development that could take place in other countries. Furthermore, such bodies should manage regular reviews by involving the main Italian companies and sector regulators. The identification of the specific subjects that may carry on these actions is not part of the scope of this document.

Professional associations of specific production sectors that choose to contextualize the Framework, should endorse the changes at institutional level and update their contextualization. This goes also for the regulatory bodies that have to issue specific regulations in order to specialize the updating processes. Companies should also adopt the new contextualizations directly from the institutions or the sector bodies and proceed with the framework implementation.

Lastly, during the Framework contextualization process, it could be possible to define the Subcategories that are not part of the original Framework Core. At this point, the one who extend the Framework should get in touch with the organization that manages the Framework in order to enter the Subcategory in a future version. Figure 3.4 summarizes the various update levels of the National Framework in the case of regulated sectors.

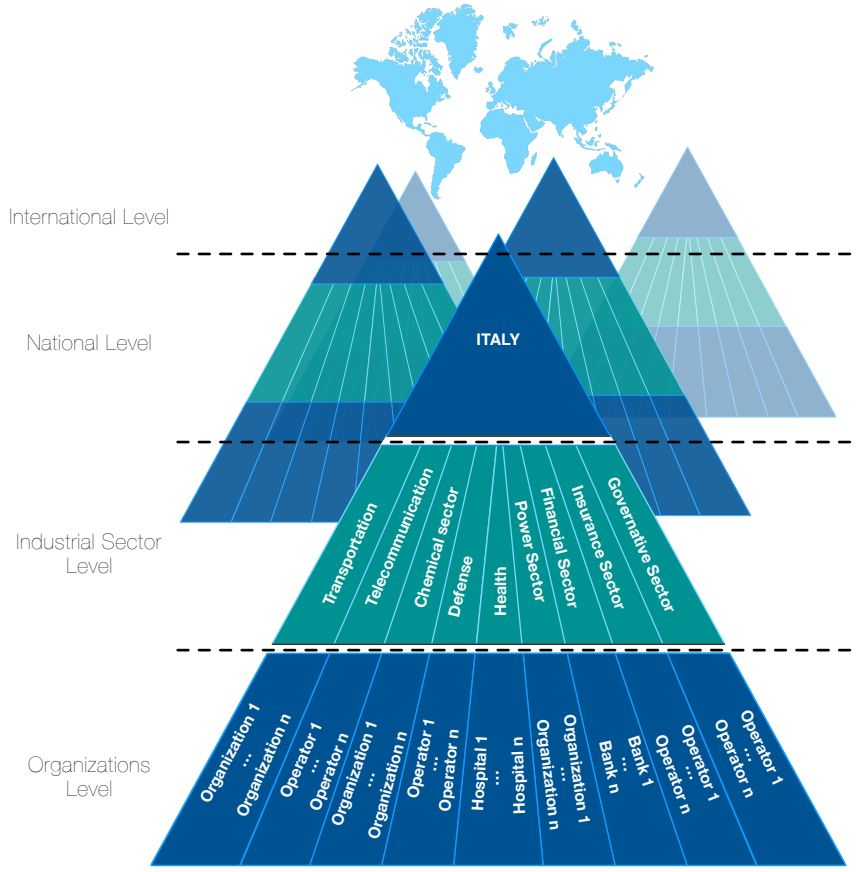

Figure 3.4: International, National, sector and company context for regulated sectors.

4. Guidelines for the implementation of the Framework

This chapter completes the previous one by providing guidelines on the use of the Framework by various players. In particular, SMEs, Large Enterprises, Critical Infrastructures of the country are taken into account. It is also explained how sector regulators can use the Framework.

4.1 Small and Medium Enterprises

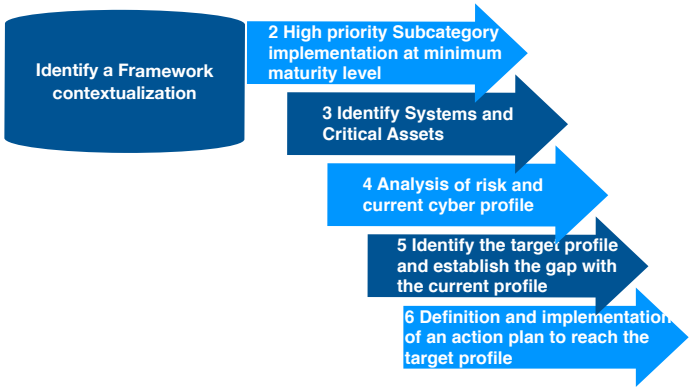

Figure 4.1: Process for the adoption of the National Cyber Security Framework by the SMEs

The implementation of the Framework by a SME should be performer in six steps, as showed by Figure 4.1. In particular:

1. *Identify a Framework contextualization.* The SME has to define the most appropriate contextualization for its business objectives and its criticalities. This activity can be performed also starting from a publicly available contextualization and adjusting it to the specific business context of the SMA. If the SME works in a regulated sector, it can refer to a contextualization possibly defined by the regulatory body.

2. *High priority Subcategory implementation*. The SME should start to use the Framework by implementing the "high priority" Subcategory (Section 6.2). Such Subcategories have to be implemented at least at the first maturity level (Section 6.3). This is a critical step in the Framework implementation and it makes possible to reach a degree of preparedness and awareness of the cyber risk.

3. *Identify Systems and Critical Assets*. The identification of ICT systems and information considered crucial or anyway critical by the SME to ensure its operations. This step is important especially for the following stages, as it makes possible to properly evaluate the impacts during risk analysis and it makes easier to understand the actual needed protection.

4. *Analysis of risk and current cyber profile.* To establish the *current profile* based on the Framework contextualization as adopted by the SME and to analyze the associated risk. Even if the Framework contains a list of priority security measures, each organization has its external peculiarities (as for example the market in which it operated, type of customer, etc.) and internal (as for example organizational and management model, offered products and solutions, territorial distribution, etc.). All the above defines the level of exposure to various risks for each organization that need to be identified through a specific analysis of cyber risks. It should be noted that the method to establish and assess the risks should be identified by each organization according to the specific organizational and specific market characteristics. Similarly, the SME should assess the level of implementation of each Framework Subcategory, in order to establish the actual protection profile.

5. *Identify the target profile and establish the gap with the current profile*. Once the current profile has been identified, according to the assessed risk levels, the SME should be able to establish its protection needs. This means to define a *target profile*: a set of Subcategories related, for each of them, to the target maturity level. The target profile represents the reference to compare the current profile, thus establishing the existing gaps within the cyber security management.

6. *Definition and implementation of an action plan to reach the target profile*. The last step of the process of Framework endorsement consists in defining the set of activities needed to reach the target protection profile as defined in the previous stage. This means to establish a specific plan to implement the Framework security practices, according to a schedule, that varies upon the actual identified risks and specific conditions of the SME business.

Clearly it is preferable to have a continuous evolution of the Framework implementation, even after having reached the target profile, in line with the cyclic risk assessment staged and following actions of steady improvement.

The Framework endorsement may be further simplified by using specific IT tools that can guide the companies to correctly carry the described steps. Eventually, is should be noted that within SMEs it is important to also identify the ones who are responsible for the implementation of the Framework steps. In effect, SMEs may not have staff such as the CISO, dedicated to this are within Large Enterprises. In this case, the CEO should designate the ones responsible for this implementation within the company.

4.2 Large Enterprises

Large Enterprises may use the Framework as a tool to support the cyber risk management and processing. It is reasonable that cyber security programs have been already introduced in such

contexts, that is why the Framework in not intended as a replacement of what already exists, but rather a further reference in order to:

- Improve or define a cyber security program, if not available, in a structured and integrated way, based on risk management, that could be implemented even in case of existing security governance models;
- Enable the easy establishment of maturity level of cyber security activities, identifying, as the case may be, improvement actions or security cost rationalization for a reasonable re-distribution of resources;
- complete the benchmark among companies and organizations operating in specific sectors or with similar characteristics that, at national level, may favor security level improvement, at the same time enabling cyber insurance;
- support and facilitate the communication with the top management (for example administrators and boards of directors, shareholders, etc.) and with external players (as for example rating agencies, suppliers and partners), so to clearly present the cyber risk levels, which the organization are exposed to, and in order to establish investments and resources to be put in place for an appropriate risk reduction.

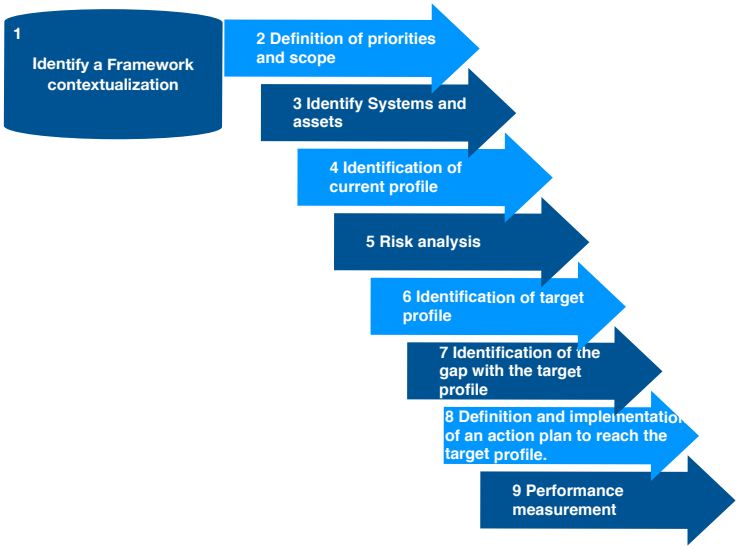

Figure 4.2: Process for the adoption of the National Cyber Security Framework by Large Enterprises and Critical Infrastructures

As shown in Figure 4.2, the Framework implementation should be carried out in nine steps, as explained below:

1. *Identify a Framework contextualization.* If the big enterprise is part of a regulated sector, it should use the contextualizations provided by its sector regulator. If the big enterprise is not part of a regulated sector, it should identify among the available contextualizations, the one to be used in the Framework implementation process. It should be noted that the selected contextualization is not a regulation to be followed, but rather a guideline. It could be modified according to own business objectives and criticalities. It should also be noted that the big enterprise, unlike SMEs, might have the ability to define its own Framework contextualization.

2. *Definition of priorities and scope*. To identify periodically the strategic objectives and organization business priorities in order to select key areas and functions that need a specific focus.

3. *Identify Systems and assets*. Identify information and IT systems (both in the IT and in the industrial fields) that the organization considers vital and critical in order to ensure the organization activity. This step is important especially for the following stages, as it makes possible to properly evaluate impacts during risk analysis and it makes easier to understand the actual needed protection;

4. *Identification of current profile*. The implementation status and maturity level of each Framework Subcategory need to be evaluated. This makes possible to define one or more current profiles related to areas/functions provided to implement the program;

5. *Risk analysis*. Establishing and evaluating risks by using an appropriate method, according to the specific characteristics of the organization and its reference market. Some prompts relating to the risk analysis and management process are reported in section 7.2.

6. *Identification of target profile*. Through the risk treatment process, the organization should be able to define a target profile that, unlike the current one, represents the target implementation and maturity level for each Framework Subcategory. It is preferable that the selection of such levels could be made after the introduction of cyber security risk management into the enterprise risk management program, so that cyber risk management may benefit from the decisions takes at a higher organization level (i.e., top management), taking advantage of a comprehensive systematic view that supports the decision process.

7. *Identification of the gap with the target profile*. To carry out a comparison between target and current profile in order to identify the existing gap within the cyber security management;

8. *Definition and implementation of an action plan to reach the target profile*. The implementation stage of the process of Framework endorsement consists in defining the set of activities needed to reach the protection profile as defined in the previous stage. This means to establish a specific plan to implement the Framework single controls, according to a schedule, that varies upon actual identified risks and specific activity conditions of each organization.

9. *Performance measurement*. In order to carry out a periodic review of the target profile effectiveness and to steadily improve it, monitoring measures need to be established, also in order to point out its operating costs. The evaluation of the current profile effectiveness should be used to define the new target profile.

The Framework is supposed to be implemented to evaluate the maturity level of cyber security activities and processes. This use, which completes the previous one, consists in a simpler process to evaluate more rapidly the existing gap and to define an action plan for its improvement. The process stages are similar to the ones described above, except for the risk evaluation.
A wide use of the Framework by Large Enterprises may provide new criteria for risk analysis and mitigation, starting from the direct feedback coming from the learned lessons. These indications ensure the actuality and relevance of the Framework. Each organization involved is therefore invited to participate in the development, validation and implementation of the Framework.

4.3 Critical Infrastructures

Critical Infrastructures, like Large Enterprises, may implement the Framework to support the cyber risk management and treatment process, besides implementing adequate cyber intelligence activities to be carried out privately and/or in collaboration with authorities, according to the methods provided for the sector of business. Inoltre, potranno adottare il Framework al fine di:

- Monitoring the threat, that should be considered as a dynamic element, through the activation of proper cyber intelligence channels and cooperation with authorities;
- increase the security of the services supply chain. Critical Infrastructures may require to their service providers to have a specific minimum profile or to link a minimum profile to each service;
- To present to the designated authorities a brief and harmonized view of exposure level of Critical Infrastructures, in order to facilitate corrective actions on the protection plan and the regulations in force.

The Framework implementation stages for Critical Infrastructures are the same as the ones provided for Large Enterprises, with some important differences:

- As far as phase 3 is concerned, “identify systems and assets”, in addition to what is provided for Large Enterprises, the critical infrastructure has to identify sensitive targets of its activity and interconnections with other Critical Infrastructures that in effect represent systemic interdependencies. Through this stage, and the use of specific tools to analyze the scenario, to evaluate impacts and support decisions, specific impacts (e.g. impact on safety) can be properly assessed during the risk analysis stage, once the potential domino effect scenarios have been outlined and the actual protection needs have been understood.
- As far as stage 6 is concerned, “Definition of target profile”, in addition to the provisions related to Large Enterprises, at this stage, the critical infrastructure and in particular its management, should adopt a comprehensive systemic view to support the decision making process, taking into account the balance between systematic protection strategy of Critical Infrastructures and intrinsic objectives of civil defense.

4.4 Sector regulators

A regulator may play two roles during the life cycle of the Framework. The first is described by the previous Chapter, and consists in holding its framework contextualizations aligned with the institutional Framework. The other is to update the sector regulations by using the Framework Categories and Subcategories as reference. This applies even better for the regulation bodies at national level. Once the regulation has been updated with reference to the Framework, a mapping between Subcategories and regulations is to be created and the priority and maturity levels need to be updated. Then the updated Framework is to be notified to the organizations belonging to the regulated sector. The Framework therefore represents also a way to make the regulations of various regulatory bodies evolve in homogenous and consistent way.

PART II – Framework support documents

5. Framework Core

This Chapter provides the list of Functions, Categories and Subcategories of the NIST Framework. Enumeration, sequence and topic of each Subcategory is consistent with the NIST Framework, as a consequence there is full compatibility with the Framework presented here and the original NIST Framework. This compatibility implies the fact that a profile provided by any organization at global level (there are already some examples online) is perfectly comparable with the National Framework. It should be noted that the National Framework allows the creation of more complex profiles thanks to the concept of maturity levels.
It should also be noted that the column "Informative References" contains the same references to the NIST Framework, includes in bold type, just as an example and not limited to some of the main obligations deriving from the Italian regulations governing privacy. Where such obligations are provided, the column indicates for each Subcategory the related regulation and when this is to be taken into account (e.g. in case of personal data processing by the organization). In these cases, there is no need to stress that, regardless of the provided Priority Level, the control is to be considered as compulsory and the related maturity level should match the one provided by the relevant regulation. Such column includes also the obligations for Government Agencies[1] as provided by the Code of Digital Administration (CAD) with related article, according to the description of Section 11.1. Further details on the Italian regulation context related to the Framework are reported in Section 10.

[1] Note that, as far as Subcategory ID.AM-5 concerns, the mandatory character derives from the need to prepare a plan that should provide a census of resources and a kind of esteem and consequent prioritization.

Function	Category	Subcategory	Informative References
	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	· CCS CSC 1 · COBIT 5 BAI09.01, BAI09.02 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	· CCS CSC 2 · COBIT 5 BAI09.01, BAI09.02, BAI09.05 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: Organizational communication and data flows are mapped	· CCS CSC 1 · COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.2.3.4 · ISO/IEC 27001:2013 A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	· COBIT 5 APO02.02 · ISO/IEC 27001:2013 A.11.2.6 · NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	· COBIT 5 APO03.03, APO03.04, BAI09.02 · ISA 62443-2-1:2009 4.2.3.6 · ISO/IEC 27001:2013 A.8.2.1 · NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14 · **Mandatory for the Governative Agencies according to 50-bis, comma 3, lett. A of CAD**
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	· COBIT 5 APO01.02, DSS06.03 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1 · NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	· COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 · ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 · NIST SP 800-53 Rev. 4 CP-2, SA-12
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	· COBIT 5 APO02.06, APO03.01 · NIST SP 800-53 Rev. 4 PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	· COBIT 5 APO02.01, APO02.06, APO03.01 · ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 · NIST SP 800-53 Rev. 4 PM-11, SA-14
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	· ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 · NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Resilience requirements to support delivery of critical services are established	· COBIT 5 DSS04.02 · ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 · NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established	· COBIT 5 APO01.03, EDM01.01, EDM01.02 · ISA 62443-2-1:2009 4.3.2.6 · ISO/IEC 27001:2013 A.5.1.1 · NIST SP 800-53 Rev. 4 -1 controls from all families · **To be done if classified information are processed, according to DPCM 6 november 2015**
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	· COBIT 5 APO13.12 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.1 · NIST SP 800-53 Rev. 4 PM-1, PS-7
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	· COBIT 5 MEA03.01, MEA03.04 · ISA 62443-2-1:2009 4.4.3.7 · ISO/IEC 27001:2013 A.18.1 · NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1) · **Mandatory according to D.Lgs. 196/2003** · **Mandatory according to Data Protection Authority's directives** · **To be implemented if classified information are processed (according Da eseguirsi per coloro che trattano informazioni classificate ai sensi del DPCM 6 november 2015 and decrees n. 4/2015 e n.5/2015)**

Function	Category	Subcategory	Informative References
		ID.GV-4: Governance and risk management processes address cybersecurity risks	· COBIT 5 DSS04.02 · ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 · NIST SP 800-53 Rev. 4 PM-9, PM-11
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	· CCS CSC 4 · COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 · ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 · ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 · NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	· ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 · ISO/IEC 27001:2013 A.6.1.4 · NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5
		ID.RA-3: Threats, both internal and external, are identified and documented	· COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 · ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 · NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Potential business impacts and likelihoods are identified	· COBIT 5 DSS04.02 · ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 · NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	· COBIT 5 APO12.02 · ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16
		ID.RA-6: Risk responses are identified and prioritized	· COBIT 5 APO12.05, APO13.02 · NIST SP 800-53 Rev. 4 PM-4, PM-9
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	· COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 · ISA 62443-2-1:2009 4.3.4.2 · NIST SP 800-53 Rev. 4 PM-9
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	· COBIT 5 APO12.06 · ISA 62443-2-1:2009 4.3.2.6.5 · NIST SP 800-53 Rev. 4 PM-9
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	· NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14

Function	Category	Subcategory	Informative References
	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	· CCS CSC 16 · COBIT 5 DSS05.04, DSS06.03 · ISA 62443-2-1:2009 4.3.3.5.1 · ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 · ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 · NIST SP 800-53 Rev. 4 AC-2, IA Family · **To be implemented if classified information are processed (according Da eseguirsi per coloro che trattano informazioni classificate ai sensi del DPCM 6 november 2015 and decrees n. 4/2015 e n.5/2015)** · **Mandatory if personal data are processed using electronic devices (according to All. B) D. Lgs. 196/2003 Rules 1-10)**
		PR.AC-2: Physical access to assets is managed and protected	· COBIT 5 DSS01.04, DSS05.05 · ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 · ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 · NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9 · Mandatory if personal data are processed using electronic devices (according to All. B) D. Lgs. 196/2003)
		PR.AC-3: Remote access is managed	· COBIT 5 APO13.01, DSS01.04, DSS05.03 · ISA 62443-2-1:2009 4.3.3.6.6 · ISA 62443-3-3:2013 SR 1.13, SR 2.6 · ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1 · NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20 · **To be implemented if classified information are processed (according Da eseguirsi per coloro che trattano informazioni classificate ai sensi del DPCM 6 november 2015 and decrees n. 4/2015 e n.5/2015)** · **Mandatory if personal data are processed using electronic devices (according to All. B) D. Lgs. 196/2003 Rules 1-10)**
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	· CCS CSC 12, 15 · ISA 62443-2-1:2009 4.3.3.7.3 · ISA 62443-3-3:2013 SR 2.1 · ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 · NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16 · Mandatory if personal data are processed using electronic devices (according to All. B) D. Lgs. 196/2003 Rules 12,13,14)

Function	Category	Subcategory	Informative References
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	· ISA 62443-2-1:2009 4.3.3.4 · ISA 62443-3-3:2013 SR 3.1, SR 3.8 · ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, SC-7
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	· CCS CSC 9 · COBIT 5 APO07.03, BAI05.07 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.7.2.2 · NIST SP 800-53 Rev. 4 AT-2, PM-13 · **Mandatory if personal data are processed using electronic devices (according to All. B) D. Lgs. 196/2003 Rules 4, 9, 18, 21, 27, 28)**
		PR.AT-2: Privileged users understand roles & responsibilities	· CCS CSC 9 · COBIT 5 APO07.02, DSS06.03 · ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 · NIST SP 800-53 Rev. 4 AT-3, PM-13 · **Directive of Data Protection Authority of 27 november 2008** · **Mandatory if personal data are processed using electronic devices (according to All. B) D. Lgs. 196/2003)**
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	· CCS CSC 9 · COBIT 5 APO07.03, APO10.04, APO10.05 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 · NIST SP 800-53 Rev. 4 PS-7, SA-9
		PR.AT-4: Senior executives understand roles & responsibilities	· CCS CSC 9 · COBIT 5 APO07.03 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, · NIST SP 800-53 Rev. 4 AT-3, PM-13

Function	Category	Subcategory	Informative References
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	· CCS CSC 9 · COBIT 5 APO07.03 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, · NIST SP 800-53 Rev. 4 AT-3, PM-13
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	· CCS CSC 17 · COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06 · ISA 62443-3-3:2013 SR 3.4, SR 4.1 · ISO/IEC 27001:2013 A.8.2.3 · NIST SP 800-53 Rev. 4 SC-28 · **To be implemented if classified information are processed (according Da eseguirsi per coloro che trattano informazioni classificate ai sensi del DPCM 6 november 2015 and decrees n. 4/2015 e n.5/2015)** · **Mandatory if personal data are processed using electronic devices (according to All. B) D. Lgs. 196/2003 Rules 16,17, 20)**
		PR.DS-2: Data-in-transit is protected	· CCS CSC 17 · COBIT 5 APO01.06, DSS06.06 · ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 · ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 SC-8 · **Mandatory if personal data are processed using electronic devices (according to All. B) D. Lgs. 196/2003)**
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	· COBIT 5 BAI09.03 · ISA 62443-2-1:2009 4. 4.3.3.3.9, 4.3.4.4.1 · ISA 62443-3-3:2013 SR 4.2 · ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 · NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16
		PR.DS-4: Adequate capacity to ensure availability is maintained	· COBIT 5 APO13.01 · ISA 62443-3-3:2013 SR 7.1, SR 7.2 · ISO/IEC 27001:2013 A.12.3.1 · NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5

Function	Category	Subcategory	Informative References
PROTECT (PR)		**PR.DS-5:** Protections against data leaks are implemented	· CCS CSC 17 · COBIT 5 APO01.06 · ISA 62443-3-3:2013 SR 5.2 · ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 · **Mandatory if personal data are processed using electronic devices (according to All. B) D. Lgs. 196/2003)**
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	· ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 · ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 SI-7
		PR.DS-7: The development and testing environment(s) are separate from the production environment	· COBIT 5 BAI07.04 · ISO/IEC 27001:2013 A.12.1.4 · NIST SP 800-53 Rev. 4 CM-2
		PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	· CCS CSC 3, 10 · COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 · ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 · ISA 62443-3-3:2013 SR 7.6 · ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	· COBIT 5 APO13.01 · ISA 62443-2-1:2009 4.3.4.3.3 · ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 · NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8
		PR.IP-3: Configuration change control processes are in place	· COBIT 5 BAI06.01, BAI01.06 · ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 · ISA 62443-3-3:2013 SR 7.6 · ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10

Function	Category	Subcategory	Informative References
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-4:** Backups of information are conducted, maintained, and tested periodically	· COBIT 5 APO13.01 · ISA 62443-2-1:2009 4.3.4.3.9 · ISA 62443-3-3:2013 SR 7.3, SR 7.4 · ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 · NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9 · **Mandatory if personal data are processed using electronic devices (according to All. B) D. Lgs. 196/2003 Regola 18)**
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	· COBIT 5 DSS01.04, DSS05.05 · ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 · ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 · NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Data is destroyed according to policy	· COBIT 5 BAI09.03 · ISA 62443-2-1:2009 4.3.4.4.4 · ISA 62443-3-3:2013 SR 4.2 · ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 · NIST SP 800-53 Rev. 4 MP-6
		PR.IP-7: Protection processes are continuously improved	· COBIT 5 APO11.06, DSS04.05 · ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 · NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	· ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	· COBIT 5 DSS04.03 · ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1 · ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2 · NIST SP 800-53 Rev. 4 CP-2, IR-8 · **Mandatory if personal data are processed using electronic devices (according to All. B) D. Lgs. 196/2003)**
		PR.IP-10: Response and recovery plans are tested	· ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 · ISA 62443-3-3:2013 SR 3.3 · ISO/IEC 27001:2013 A.17.1.3 · NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14 · **Mandatory for the Governative Agencies according to 50-bis, comma 3, lett. B of CAD**

Function	Category	Subcategory	Informative References
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	· COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 · ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 · ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4 · NIST SP 800-53 Rev. 4 PS Family
		PR.IP-12: A vulnerability management plan is developed and implemented	· ISO/IEC 27001:2013 A.12.6.1, A.18.2.2 · NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	· COBIT 5 BAI09.03 · ISA 62443-2-1:2009 4.3.3.3.7 · ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5 · NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	· COBIT 5 DSS05.04 · ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 · ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 · NIST SP 800-53 Rev. 4 MA-4
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	· CCS CSC 14 · COBIT 5 APO11.04 · ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 · ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 · ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 · NIST SP 800-53 Rev. 4 AU Family
		PR.PT-2: Removable media is protected and its use restricted according to policy	· COBIT 5 DSS05.02, APO13.01 · ISA 62443-3-3:2013 SR 2.3 · ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 · NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7 · **Mandatory if personal data are processed using electronic devices (according to All. B) D. Lgs. 196/2003)**
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	· COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4

Function	Category	Subcategory	Informative References
			· ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 · ISO/IEC 27001:2013 A.9.1.2 · NIST SP 800-53 Rev. 4 AC-3, CM-7 · **Mandatory if personal data are processed using electronic devices (according to All. B) D. Lgs. 196/2003)**
		PR.PT-4: Communications and control networks are protected	· CCS CSC 7 · COBIT 5 DSS05.02, APO13.01 · ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 · ISO/IEC 27001:2013 A.13.1.1, A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7
	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	· COBIT 5 DSS03.01 · ISA 62443-2-1:2009 4.4.3.3 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 · ISO/IEC 27001:2013 A.16.1.1, A.16.1.4 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	· ISA 62443-3-3:2013 SR 6.1 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Impact of events is determined	· COBIT 5 APO12.06 · NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI -4
		DE.AE-5: Incident alert thresholds are established	· COBIT 5 APO12.06 · ISA 62443-2-1:2009 4.2.3.10 · NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8
		DE.CM-1: The network is monitored to detect potential cybersecurity events	· CCS CSC 14, 16 · COBIT 5 DSS05.07 · ISA 62443-3-3:2013 SR 6.2 · NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4

Function	Category	Subcategory	Informative References
DETECT (DE)	**Security Continuous Monitoring (DE.CM):** The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-2:** The physical environment is monitored to detect potential cybersecurity events	· ISA 62443-2-1:2009 4.3.3.3.8 · NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	· ISA 62443-3-3:2013 SR 6.2 · ISO/IEC 27001:2013 A.12.4.1 · NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 · **To be implemented according to art.23 of D.Lgs n.151/2015**
		DE.CM-4: Malicious code is detected	· CCS CSC 5 · COBIT 5 DSS05.01 · ISA 62443-2-1:2009 4.3.4.3.8 · ISA 62443-3-3:2013 SR 3.2 · ISO/IEC 27001:2013 A.12.2.1 · NIST SP 800-53 Rev. 4 SI-3
		DE.CM-5: Unauthorized mobile code is detected	· ISA 62443-3-3:2013 SR 2.4 · ISO/IEC 27001:2013 A.12.5.1 · NIST SP 800-53 Rev. 4 SC-18, SI-4. SC-44
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	· COBIT 5 APO07.06 · ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 · NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	· NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Vulnerability scans are performed	· COBIT 5 BAI03.10 · ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 · ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 RA-5
		DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	· CCS CSC 5 · COBIT 5 DSS05.01 · ISA 62443-2-1:2009 4.4.3.1 · ISO/IEC 27001:2013 A.6.1.1 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14

Function	Category	Subcategory	Informative References
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-2:** Detection activities comply with all applicable requirements	· ISA 62443-2-1:2009 4.4.3.2 · ISO/IEC 27001:2013 A.18.1.4 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4
		DE.DP-3: Detection processes are tested	· COBIT 5 APO13.02 · ISA 62443-2-1:2009 4.4.3.2 · ISA 62443-3-3:2013 SR 3.3 · ISO/IEC 27001:2013 A.14.2.8 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4
		DE.DP-4: Event detection information is communicated to appropriate parties	· COBIT 5 APO12.06 · ISA 62443-2-1:2009 4.3.4.5.9 · ISA 62443-3-3:2013 SR 6.1 · ISO/IEC 27001:2013 A.16.1.2 · NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4 · **Mandatory if personal data are processed (according to artt. 19-22, 25-27, 32-bis and 39 of D. Lgs. 196/2003)**
		DE.DP-5: Detection processes are continuously improved	· COBIT 5 APO11.06, DSS04.05 · ISA 62443-2-1:2009 4.4.3.4 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	· COBIT 5 BAI01.10 · CCS CSC 18 · ISA 62443-2-1:2009 4.3.4.5.1 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	· ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 · ISO/IEC 27001:2013 A.6.1.1, A.16.1.1 · NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Events are reported consistent with established criteria	· ISA 62443-2-1:2009 4.3.4.5.5 · ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 · NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8 · **Mandatory if personal data are processed (according to artt. 19-22, 25-27, 32-bis and 39 of D. Lgs. 196/2003)**

Function	Category	Subcategory	Informative References
RESPOND (RS)		**RS.CO-3:** Information is shared consistent with response plans	· ISA 62443-2-1:2009 4.3.4.5.2 · ISO/IEC 27001:2013 A.16.1.2 · NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4 · **Mandatory if personal data are processed (according to artt. 19-22, 25-27, 32-bis and 39 of D. Lgs. 196/2003)**
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	· ISA 62443-2-1:2009 4.3.4.5.5 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	· NIST SP 800-53 Rev. 4 PM-15, SI-5 · **Mandatory if personal data are processed (according to artt. 19-22, 25-27, 32-bis and 39 of D. Lgs. 196/2003)**
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	· COBIT 5 DSS02.07 · ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISA 62443-3-3:2013 SR 6.1 · ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: The impact of the incident is understood	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 CP-2, IR-4
		RS.AN-3: Forensics are performed	· ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 · ISO/IEC 27001:2013 A.16.1.7 · NIST SP 800-53 Rev. 4 AU-7, IR-4
		RS.AN-4: Incidents are categorized consistent with response plans	· ISA 62443-2-1:2009 4.3.4.5.6 · ISO/IEC 27001:2013 A.16.1.4 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	· ISA 62443-2-1:2009 4.3.4.5.6 · ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 IR-4

Function	Category	Subcategory	Informative References
		RS.MI-2: Incidents are mitigated	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 · ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 · NIST SP 800-53 Rev. 4 IR-4
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	· ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	· COBIT 5 BAI01.13 · ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RS.IM-2: Response strategies are updated	· NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event	· CCS CSC 8 · COBIT 5 DSS02.05, DSS03.04 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	· COBIT 5 BAI05.07 · ISA 62443-2-1 4.4.3.4 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated	· COBIT 5 BAI07.08 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 · **Mandatory for the Governative Agencies according to 50-bis, comma 3, lett. B of CAD**
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed	· COBIT 5 EDM03.02 · **Mandatory if personal data are processed (according to artt. 19-22, 25-27, 32-bis and 39 of D. Lgs. 196/2003)**
		RC.CO-2: Reputation after an event is repaired	· COBIT 5 MEA03.02
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	· NIST SP 800-53 Rev. 4 CP-2, IR-4

6. A Framework contextualization for SMEs

This Chapter presents a Framework contextualization of Italian SMEs (hereinafter called *CONTEXT-PMI*). The contextualization is presented regardless of business domain and, for example enterprise size. The steps presented by Section 3.4 are applied: Selection of Subcategories, attribution of priority values to them, definition of maturity levels (in this case just for high priority Subcategories). Eventually, this Chapter reports an implementation guide for high priorities Subcategories.

CONTEXT-PMI is a possible Framework contextualization. Other contextualizations could be created by different operators (some of them are reported in Section 3.4.1). In this regard, it should be noted that the choice to use 3 priority levels (low, medium, high) and of 3 maturity levels is typical of the contextualization and not of the Framework: The various contextualizations may have more o less priority and maturity levels. It should be noted that Implementation Tiers for SMEs are not part of the scope of this contextualization.

6.1 Selection of Subcategories

The Subcategories selection implies the identification of the Subcategories that the ones who extended the contextualization do not consider adequate suitable for the target companies, which the contextualization is made for. It should be recalled that the NIST Framework has been designed to improve cyber security practices in Critical Infrastructures. Thus, it makes sense to assume that some Subcategories could not be relevant for the companies that the contextualization is targeted to. However, the selection process could lead to the conclusion that all Subcategories are relevant for the number of companies taken into account.

This selection step should be carried out by the ones who extend the contextualization, taking into account the fact that eliminating a Subcategory could increase the cyber risk. Therefore, the Subcategories that are not relevant for companies targeted by the contextualization, for example because of business type, size, structure, etc. have to be removed. The exclusion of Subcategories should be carefully considered, while excluded categories need to be included again if, for example, the SME, even if it is not a Critical Infrastructure, plays a crucial role in the service supply chain for one or more Critical Infrastructures. Nevertheless, a SME might

include again in the contextualization some excluded subcategories according to its business and cyber security objectives.

Lastly, as described in Section 3.5, a contextualization could also define Subcategories that are not part of the Framework Core, in this case, the ones who extend the contextualization should contact the organization that manages the Framework in order to include the Subcategory in the Framework review.

In *CONTEXT-PMI*, the following Subcategories have been marked as "non selected", as they are considered not particularly suitable to most of the Italian SMEs. However, each SME should evaluate the possible applicability in their own context, also according to the size and characteristics of the organization and in general according to its own risk profile.

- ID.AM-4: External information systems of the organization are classified
- ID.BE-1: The organization role within the production chain is identified and communicated
- ID.BE-2: The organization role as critical infrastructure and within the reference industry sector is identified and communicated
- PR.DS-3: The physical transfer, removal or destruction of data saving devices are managed through a formal process
- DE.CM-6: The monitoring of external service provider activities is performed in order to identify potential cyber security events.

Below are reported the reasons why such Subcategory selection took place.
DE.CM-6 requires an effort that is not commensurate to the use of service providers made by the SMEs. As a consequence, the cost and management of such practice could be higher than the benefits obtained by SMEs. PR.DS-3 requires the definition of a formal process that could result in an excessive overhead for a SME compared with its business activities. ID.BE-1 and ID.BE-2 are clearly dedicated to Critical Infrastructures or highly regulated organizations, which have to report to their regulators also their role and functional dependencies. ID.AM-4 requires the creation of a set of non proprietary IT systems of SMEs. Except for cloud services, rarely such systems can be found in the Italian SME context.

6.2 Priority levels

This Section presents the priorities associated with the selected Subcategories according to the description of Chapter 3 for the contextualization *CONTEXT-PMI*. For the sake of completeness, the column of informative references is reported once again. It should be noted that If in the informative references column a mandatory Subcategory is specified, such Subcategory is to be considered as the highest priority by the specified subjects, regardless of what is indicated in the Priority column.

Function	Category	Subcategory	Priority	Informative References
	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	**HIGH**	· CCS CSC 1 · COBIT 5 BAI09.01, BAI09.02 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	**HIGH**	· CCS CSC 2 · COBIT 5 BAI09.01, BAI09.02, BAI09.05 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: Organizational communication and data flows are mapped	**LOW**	· CCS CSC 1 · COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.2.3.4 · ISO/IEC 27001:2013 A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**NOT SELECTED**	· COBIT 5 APO02.02 · ISO/IEC 27001:2013 A.11.2.6 · NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	**MEDIUM**	· COBIT 5 APO03.03, APO03.04, BAI09.02 · ISA 62443-2-1:2009 4.2.3.6 · ISO/IEC 27001:2013 A.8.2.1 · NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14 · **Mandatory for the Governative Agencies according to 50-bis, comma 3, lett. A of CAD**
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	**HIGH**	· COBIT 5 APO01.02, DSS06.03 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1 · NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11

Function	Category	Subcategory	Priority	Informative References
IDENTIFY (ID)	**Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	**NOT SELECTED**	· COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 · ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 · NIST SP 800-53 Rev. 4 CP-2, SA-12
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**NOT SELECTED**	· COBIT 5 APO02.06, APO03.01 · NIST SP 800-53 Rev. 4 PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**MEDIUM**	· COBIT 5 APO02.01, APO02.06, APO03.01 · ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 · NIST SP 800-53 Rev. 4 PM-11, SA-14
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**MEDIUM**	· ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 · NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Resilience requirements to support delivery of critical services are established	**MEDIUM**	· COBIT 5 DSS04.02 · ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 · NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established	**MEDIUM**	· COBIT 5 APO01.03, EDM01.01, EDM01.02 · ISA 62443-2-1:2009 4.3.2.6 · ISO/IEC 27001:2013 A.5.1.1 · NIST SP 800-53 Rev. 4 -1 controls from all families · **To be done if classified information are processed, according to DPCM 6 november 2015**
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	**MEDIUM**	· COBIT 5 APO13.12 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.1 · NIST SP 800-53 Rev. 4 PM-1, PS-7

Function	Category	Subcategory	Priority	Informative References
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	**HIGH**	· COBIT 5 MEA03.01, MEA03.04 · ISA 62443-2-1:2009 4.4.3.7 · ISO/IEC 27001:2013 A.18.1 · NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1) · **Mandatory according to D.Lgs. 196/2003** · **Mandatory according to Data Protection Authority's directives** · **To be implemented if classified information are processed (according Da eseguirsi per coloro che trattano informazioni classificate ai sensi del DPCM 6 november 2015 and decrees n. 4/2015 e n.5/2015)**
		ID.GV-4: Governance and risk management processes address cybersecurity risks	**LOW**	· COBIT 5 DSS04.02 · ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 · NIST SP 800-53 Rev. 4 PM-9, PM-11
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	**MEDIUM**	· CCS CSC 4 · COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 · ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 · ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 · NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	**LOW**	· ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 · ISO/IEC 27001:2013 A.6.1.4 · NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5
		ID.RA-3: Threats, both internal and external, are identified and documented	**LOW**	· COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 · ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 · NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Potential business impacts and likelihoods are identified	**LOW**	· COBIT 5 DSS04.02 · ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 · NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	**LOW**	· COBIT 5 APO12.02 · ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16
		ID.RA-6: Risk responses are identified and prioritized	**LOW**	· COBIT 5 APO12.05, APO13.02 · NIST SP 800-53 Rev. 4 PM-4, PM-9

Function	Category	Subcategory	Priority	Informative References
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	**LOW**	· COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 · ISA 62443-2-1:2009 4.3.4.2 · NIST SP 800-53 Rev. 4 PM-9
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	**LOW**	· COBIT 5 APO12.06 · ISA 62443-2-1:2009 4.3.2.6.5 · NIST SP 800-53 Rev. 4 PM-9
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	**LOW**	· NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14
	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	**HIGH**	· CCS CSC 16 · COBIT 5 DSS05.04, DSS06.03 · ISA 62443-2-1:2009 4.3.3.5.1 · ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 · ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 · NIST SP 800-53 Rev. 4 AC-2, IA Family · **To be implemented if classified information are processed (according Da eseguirsi per coloro che trattano informazioni classificate ai sensi del DPCM 6 november 2015 and decrees n. 4/2015 e n.5/2015)** · Mandatory if personal data are processed using electronic devices (according to All. B) D. Lgs. 196/2003 Rules 1-10)
		PR.AC-2: Physical access to assets is managed and protected	**MEDIUM**	· COBIT 5 DSS01.04, DSS05.05 · ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 · ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 · NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9 · **Mandatory if personal data are processed using electronic devices (according to All. B) D. Lgs. 196/2003)**

Function	Category	Subcategory	Priority	Informative References
		PR.AC-3: Remote access is managed	**HIGH**	· COBIT 5 APO13.01, DSS01.04, DSS05.03 · ISA 62443-2-1:2009 4.3.3.6.6 · ISA 62443-3-3:2013 SR 1.13, SR 2.6 · ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1 · NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20 · **To be implemented if classified information are processed (according Da eseguirsi per coloro che trattano informazioni classificate ai sensi del DPCM 6 november 2015 and decrees n. 4/2015 e n.5/2015)** · **Mandatory if personal data are processed using electronic devices (according to All. B) D. Lgs. 196/2003 Rules 1-10)**
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	**HIGH**	· CCS CSC 12, 15 · ISA 62443-2-1:2009 4.3.3.7.3 · ISA 62443-3-3:2013 SR 2.1 · ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 · NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16 · Mandatory if personal data are processed using electronic devices (according to All. B) D. Lgs. 196/2003 Rules 12,13,14)
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	**MEDIUM**	· ISA 62443-2-1:2009 4.3.3.4 · ISA 62443-3-3:2013 SR 3.1, SR 3.8 · ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, SC-7
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	**HIGH**	· CCS CSC 9 · COBIT 5 APO07.03, BAI05.07 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.7.2.2 · NIST SP 800-53 Rev. 4 AT-2, PM-13 · **Mandatory if personal data are processed using electronic devices (according to All. B) D. Lgs. 196/2003 Rules 4, 9, 18, 21, 27, 28)**

Function	Category	Subcategory	Priority	Informative References
		PR.AT-2: Privileged users understand roles & responsibilities	**HIGH**	· CCS CSC 9 · COBIT 5 APO07.02, DSS06.03 · ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 · NIST SP 800-53 Rev. 4 AT-3, PM-13 · **Directive of Data Protection Authority of 27 november 2008** · **Mandatory if personal data are processed using electronic devices (according to All. B) D. Lgs. 196/2003)**
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	**MEDIUM**	· CCS CSC 9 · COBIT 5 APO07.03, APO10.04, APO10.05 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 · NIST SP 800-53 Rev. 4 PS-7, SA-9
		PR.AT-4: Senior executives understand roles & responsibilities	**HIGH**	· CCS CSC 9 · COBIT 5 APO07.03 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, · NIST SP 800-53 Rev. 4 AT-3, PM-13
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	**MEDIUM**	· CCS CSC 9 · COBIT 5 APO07.03 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, · NIST SP 800-53 Rev. 4 AT-3, PM-13
		PR.DS-1: Data-at-rest is protected	**MEDIUM**	· CCS CSC 17 · COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06 · ISA 62443-3-3:2013 SR 3.4, SR 4.1 · ISO/IEC 27001:2013 A.8.2.3 · NIST SP 800-53 Rev. 4 SC-28 · **To be implemented if classified information are processed (according Da eseguirsi per coloro che trattano informazioni classificate ai sensi del DPCM 6 november 2015 and decrees n. 4/2015 e n.5/2015)** · **Mandatory if personal data are processed using electronic devices (according to All. B) D. Lgs. 196/2003 Rules 16,17, 20)**

Function	Category	Subcategory	Priority	Informative References
PROTECT (PR)	**Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-2:** Data-in-transit is protected	LOW	· CCS CSC 17 · COBIT 5 APO01.06, DSS06.06 · ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 · ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 SC-8 · **Mandatory if personal data are processed using electronic devices (according to All. B) D. Lgs. 196/2003)**
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	NOT SELECTED	· COBIT 5 BAI09.03 · ISA 62443-2-1:2009 4. 4.3.3.3.9, 4.3.4.4.1 · ISA 62443-3-3:2013 SR 4.2 · ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 · NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16
		PR.DS-4: Adequate capacity to ensure availability is maintained	MEDIUM	· COBIT 5 APO13.01 · ISA 62443-3-3:2013 SR 7.1, SR 7.2 · ISO/IEC 27001:2013 A.12.3.1 · NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5
		PR.DS-5: Protections against data leaks are implemented	LOW	· CCS CSC 17 · COBIT 5 APO01.06 · ISA 62443-3-3:2013 SR 5.2 · ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 · **Mandatory if personal data are processed using electronic devices (according to All. B) D. Lgs. 196/2003)**
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	LOW	· ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 · ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 SI-7
		PR.DS-7: The development and testing environment(s) are separate from the production environment	MEDIUM	· COBIT 5 BAI07.04 · ISO/IEC 27001:2013 A.12.1.4 · NIST SP 800-53 Rev. 4 CM-2

Function	Category	Subcategory	Priority	Informative References
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	**HIGH**	· CCS CSC 3, 10 · COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 · ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 · ISA 62443-3-3:2013 SR 7.6 · ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	**MEDIUM**	· COBIT 5 APO13.01 · ISA 62443-2-1:2009 4.3.4.3.3 · ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 · NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8
		PR.IP-3: Configuration change control processes are in place	**MEDIUM**	· COBIT 5 BAI06.01, BAI01.06 · ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 · ISA 62443-3-3:2013 SR 7.6 · ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	**HIGH**	· COBIT 5 APO13.01 · ISA 62443-2-1:2009 4.3.4.3.9 · ISA 62443-3-3:2013 SR 7.3, SR 7.4 · ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 · NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9 · Mandatory if personal data are processed using electronic devices (according to All. B) D. Lgs. 196/2003 Regola 18)
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	**MEDIUM**	· COBIT 5 DSS01.04, DSS05.05 · ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 · ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 · NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Data is destroyed according to policy	**MEDIUM**	· COBIT 5 BAI09.03 · ISA 62443-2-1:2009 4.3.4.4.4 · ISA 62443-3-3:2013 SR 4.2 · ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 · NIST SP 800-53 Rev. 4 MP-6

Function	Category	Subcategory	Priority	Informative References
		PR.IP-7: Protection processes are continuously improved	**LOW**	· COBIT 5 APO11.06, DSS04.05 · ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 · NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	**LOW**	· ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	**MEDIUM**	· COBIT 5 DSS04.03 · ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1 · ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2 · NIST SP 800-53 Rev. 4 CP-2, IR-8 · **Mandatory if personal data are processed using electronic devices (according to All. B) D. Lgs. 196/2003)**
		PR.IP-10: Response and recovery plans are tested	**LOW**	· ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 · ISA 62443-3-3:2013 SR 3.3 · ISO/IEC 27001:2013 A.17.1.3 · NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14 · **Mandatory for the Governative Agencies according to 50-bis, comma 3, lett. B of CAD**
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	**LOW**	· COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 · ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 · ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4 · NIST SP 800-53 Rev. 4 PS Family
		PR.IP-12: A vulnerability management plan is developed and implemented	**MEDIUM**	· ISO/IEC 27001:2013 A.12.6.1, A.18.2.2 · NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	**LOW**	· COBIT 5 BAI09.03 · ISA 62443-2-1:2009 4.3.3.3.7 · ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5 · NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	**HIGH**	· COBIT 5 DSS05.04 · ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 · ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 · NIST SP 800-53 Rev. 4 MA-4

Function	Category	Subcategory	Priority	Informative References
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	**MEDIUM**	· CCS CSC 14 · COBIT 5 APO11.04 · ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 · ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 · ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 · NIST SP 800-53 Rev. 4 AU Family
		PR.PT-2: Removable media is protected and its use restricted according to policy	**MEDIUM**	· COBIT 5 DSS05.02, APO13.01 · ISA 62443-3-3:2013 SR 2.3 · ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 · NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7 · **Mandatory if personal data are processed using electronic devices (according to All. B) D. Lgs. 196/2003)**
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	**MEDIUM**	· COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 · ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 · ISO/IEC 27001:2013 A.9.1.2 · NIST SP 800-53 Rev. 4 AC-3, CM-7 · **Mandatory if personal data are processed using electronic devices (according to All. B) D. Lgs. 196/2003)**
		PR.PT-4: Communications and control networks are protected	**HIGH**	· CCS CSC 7 · COBIT 5 DSS05.02, APO13.01 · ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 · ISO/IEC 27001:2013 A.13.1.1, A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7
	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	**LOW**	· COBIT 5 DSS03.01 · ISA 62443-2-1:2009 4.4.3.3 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4

Function	Category	Subcategory	Priority	Informative References
DETECT (DE)		**DE.AE-2:** Detected events are analyzed to understand attack targets and methods	LOW	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 · ISO/IEC 27001:2013 A.16.1.1, A.16.1.4 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	MEDIUM	· ISA 62443-3-3:2013 SR 6.1 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Impact of events is determined	MEDIUM	· COBIT 5 APO12.06 · NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI -4
		DE.AE-5: Incident alert thresholds are established	MEDIUM	· COBIT 5 APO12.06 · ISA 62443-2-1:2009 4.2.3.10 · NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	MEDIUM	· CCS CSC 14, 16 · COBIT 5 DSS05.07 · ISA 62443-3-3:2013 SR 6.2 · NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity	LOW	· ISA 62443-2-1:2009 4.3.3.3.8 · NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	LOW	· ISA 62443-3-3:2013 SR 6.2 · ISO/IEC 27001:2013 A.12.4.1 · NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 · **To be implemented according to art.23 of D.Lgs n.151/2015**
		DE.CM-4: Malicious code is detected	HIGH	· CCS CSC 5 · COBIT 5 DSS05.01 · ISA 62443-2-1:2009 4.3.4.3.8 · ISA 62443-3-3:2013 SR 3.2 · ISO/IEC 27001:2013 A.12.2.1 · NIST SP 800-53 Rev. 4 SI-3
		DE.CM-5: Unauthorized mobile code is detected	LOW	· ISA 62443-3-3:2013 SR 2.4 · ISO/IEC 27001:2013 A.12.5.1 · NIST SP 800-53 Rev. 4 SC-18, SI-4. SC-44

Function	Category	Subcategory	Priority	Informative References
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	**NOT SELECTED**	· COBIT 5 APO07.06 · ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 · NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	**MEDIUM**	· NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Vulnerability scans are performed	**MEDIUM**	· COBIT 5 BAI03.10 · ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 · ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 RA-5
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	**LOW**	· CCS CSC 5 · COBIT 5 DSS05.01 · ISA 62443-2-1:2009 4.4.3.1 · ISO/IEC 27001:2013 A.6.1.1 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14
		DE.DP-2: Detection activities comply with all applicable requirements	**MEDIUM**	· ISA 62443-2-1:2009 4.4.3.2 · ISO/IEC 27001:2013 A.18.1.4 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4
		DE.DP-3: Detection processes are tested	**LOW**	· COBIT 5 APO13.02 · ISA 62443-2-1:2009 4.4.3.2 · ISA 62443-3-3:2013 SR 3.3 · ISO/IEC 27001:2013 A.14.2.8 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4
		DE.DP-4: Event detection information is communicated to appropriate parties	**MEDIUM**	· COBIT 5 APO12.06 · ISA 62443-2-1:2009 4.3.4.5.9 · ISA 62443-3-3:2013 SR 6.1 · ISO/IEC 27001:2013 A.16.1.2 · NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4 · **Mandatory if personal data are processed (according to artt. 19-22, 25-27, 32-bis and 39 of D. Lgs. 196/2003)**
		DE.DP-5: Detection processes are continuously improved	**LOW**	· COBIT 5 APO11.06, DSS04.05 · ISA 62443-2-1:2009 4.4.3.4 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

Function	Category	Subcategory	Priority	Informative References
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	LOW	· COBIT 5 BAI01.10 · CCS CSC 18 · ISA 62443-2-1:2009 4.3.4.5.1 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	LOW	· ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 · ISO/IEC 27001:2013 A.6.1.1, A.16.1.1 · NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Events are reported consistent with established criteria	LOW	· ISA 62443-2-1:2009 4.3.4.5.5 · ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 · NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8 · **Mandatory if personal data are processed (according to artt. 19-22, 25-27, 32-bis and 39 of D. Lgs. 196/2003)**
		RS.CO-3: Information is shared consistent with response plans	LOW	· ISA 62443-2-1:2009 4.3.4.5.2 · ISO/IEC 27001:2013 A.16.1.2 · NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4 · **Mandatory if personal data are processed (according to artt. 19-22, 25-27, 32-bis and 39 of D. Lgs. 196/2003)**
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	LOW	· ISA 62443-2-1:2009 4.3.4.5.5 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	LOW	· NIST SP 800-53 Rev. 4 PM-15, SI-5 · **Mandatory if personal data are processed (according to artt. 19-22, 25-27, 32-bis and 39 of D. Lgs. 196/2003)**
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	LOW	· COBIT 5 DSS02.07 · ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISA 62443-3-3:2013 SR 6.1 · ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: The impact of the incident is understood	MEDIUM	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 CP-2, IR-4

Function	Category	Subcategory	Priority	Informative References
		RS.AN-3: Forensics are performed	**LOW**	· ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 · ISO/IEC 27001:2013 A.16.1.7 · NIST SP 800-53 Rev. 4 AU-7, IR-4
		RS.AN-4: Incidents are categorized consistent with response plans	**LOW**	· ISA 62443-2-1:2009 4.3.4.5.6 · ISO/IEC 27001:2013 A.16.1.4 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	**HIGH**	· ISA 62443-2-1:2009 4.3.4.5.6 · ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 IR-4
		RS.MI-2: Incidents are mitigated	**HIGH**	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 · ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 · NIST SP 800-53 Rev. 4 IR-4
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	**HIGH**	· ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	**LOW**	· COBIT 5 BAI01.13 · ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RS.IM-2: Response strategies are updated	**LOW**	· NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event	**MEDIUM**	· CCS CSC 8 · COBIT 5 DSS02.05, DSS03.04 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	**LOW**	· COBIT 5 BAI05.07 · ISA 62443-2-1 4.4.3.4 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated	**LOW**	· COBIT 5 BAI07.08 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 · **Mandatory for the Governative Agencies according to 50-bis, comma 3, lett. B of CAD**

Function	Category	Subcategory	Priority	Informative References
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed	**LOW**	· COBIT 5 EDM03.02 · **Mandatory if personal data are processed (according to artt. 19-22, 25-27, 32-bis and 39 of D. Lgs. 196/2003)**
		RC.CO-2: Reputation after an event is repaired	**LOW**	· COBIT 5 MEA03.02
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	**MEDIUM**	· NIST SP 800-53 Rev. 4 CP-2, IR-4

6.3 Maturity levels

This Section reports the maturity levels for the Subcategories marked with “high priority” in the contextualization *CONTEXT-PMI*. For each of these Subcategories, also a reference to the implementation guide for high priority Subcategories is given in Section 6.4. It should be noted that it makes sense to define three increasing maturity levels, therefore, some Subcategories report just one or two maturity levels. Furthermore, it should be noted that high priority Subcategories are the ones that should be implemented for first and at least at a minimum maturity level. According to business context, risk assessment and other factors, lower priority Subcategories need to be implemented in the contextualization as well as the target maturity levels.

Function	Subcategory	Reference to the Guide	Level 1	Level 2	Level 3
IDENTIFY (ID)	ID.AM-1: Physical devices and systems within the organization are inventoried	Table 6.1: Assets identification (IA)	Assets inventory, classification and update (intended as information, applications, available systems and equipment) are performed mainly manually according to a defined and controlled process	Assets inventory, classification and update are performed in part in automatic mode that allows at least to automate the "discovery" phase of systems connected to the network, by detecting their characteristics (installed hardware, software, configurations, etc.) and registering the target inventory in a central repository	Inventory, classification and update of assets is done completely in automatic mode, allowing to manage the entire lifecycle of an asset (identification, assignment, status changes, removal, etc.)
	ID.AM-2: Software platforms and applications within the organization are inventoried	Table 6.1: Assets identification (IA)	See ID.AM-1	See ID.AM-1	See ID.AM-1
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Table 6.2: Responsibility assignment (AR)	The Company Owner and/or the Top Management designates the representative for Cyber Security, formally defining its tasks. They also establish technical specifications for an adequate use of information and IT tools by all involved parties (e.g. employee, consultants, third	A Company Policy document for the Cyber Security defining and clearly formalizing roles, responsibilities and activities required to all involved parties, clearly communicating to them the commitment of the Owner and of the Company Top Management with respect	N/A

Function	Subcategory	Reference to the Guide	Level 1	Level 2	Level 3
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	Table 6.3: Compliance with laws and regulations (CLR)	Compliance with laws and regulation is achieved and assessed, also with the help of specialists and external suppliers, where considered necessary, so to facilitate the identification and management of regulation and compliance aspects, above all if directly or indirectly linked with Cyber	N/A	N/A
PROTECT (PR)	PR.AC-1: Identities and credentials are managed for authorized devices and users	Table 6.6: Access Controls (CA)	The life-cycle of identities and authentication credentials is managed and administered locally on each device or IT system according to a defined and controlled system	Identities and credentials are managed through a company directory that allows the homogeneous application of rules and minimum security levels	Specific technical solutions are adopted to specifically manage in an appropriate way the privileged users (e.g. System Administrators)
	PR.AC-3: Remote access is managed	Table 6.6: Access Controls (CA)	Remote access to resources is possible through the use of secure communication channels (e.g. VPN with communication cryptography) and in line with the criteria provided by the control implementation guide	Remote access to resources by using secure communications channels and two-factor authentication systems	Remote access to resources is permitted only if the system setup specific criteria are fulfilled (i.e. antivirus, status update patch available, etc.)

Function	Subcategory	Reference to the Guide	Level 1	Level 2	Level 3
PROTECT (PR)	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	Table 6.6: Access Controls (CA)	Access to IT systems is allowed upon registration of the main existing roles, in order to identify the action perimeter of each role and pointing out possible existing incompatibilities between them. Then activation profiles and access credentials must be assigned according to a defined authorization procedure and attribution of minimum privilege needed to exercise the only functions for each role	Segregation rules need to be established in order to prevent the assignment of incompatible roles and related automatic control tools need to be implemented, also to assess the authorization procedure compliance as defined in order to prevent and identify the possible occurrence of frauds, abuses, mistakes of users	A periodic certification process of assigned privileges is to be defined and related assessment activities are needed to ensure that assigned privileges are valid (i.e. persistence of conditions that have lead to their assignment)
	PR.AT-1: All users are informed and trained	Table 6.9: Staff Basic Training (FBP)	Basic staff training on cyber security risks is performed according to established plan and schedule and with the help of appropriate training techniques and tools (e.g. e-learning, classroom training, tutorial material) in line with the specific characteristics of each organization (e.g. staff territorial distribution, prevailing use of external supplier)	Training initiatives on cyber security are distinguished in their objectives according to the specific role played by the involved resources	Training initiatives on cyber security are carried out for specific user categories and provide a training to identify and react to cyber security risks

Function	Subcategory	Reference to the Guide	Level 1	Level 2	Level 3
PROTECT (PR)	PR.AT-2: Privileged users understand roles & responsibilities	Table 6.9: Staff Basic Training (FBP)	Cyber security training for expert staff is carried out through external training courses, in order to ensure appropriate technical and professional abilities in line with played roles (e.g. system administrators)	Specialist staff training on cyber security is carried out for specific user categories with the support of specialized external organizations, providing possible Professional Certification procedures	N/A
	PR.AT-4: Senior executives understand roles & responsibilities	Table 6.9: Staff Basic Training (FBP)	Owner and company top management support awareness raising of the staff on cyber security through the al location of specific resources and communicate its relevance through formal references (e.g. general security policy, internal communication, company bulletin board)	The Owner and Company Management participate actively to awareness raising programmes, through the direct participation to workshops and targeted training activities to improve cyber risk perception and practices to be implemented in order to better address th	N/A
	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	Table 6.7: System Secure Configuration (CCS)	Secure setup of systems is carried out by the IT responsible staff (if applicable) and/or by external designated companies (if applicable) by complying with the criteria specified in the control implementation guide	The secure system setup is carried out by implementing operational guidelines and procedures that formalize the criteria and modalities according to market standards	Secure setup of systems is carried out also by using automatic tools and solutions developed to facilitate the setup and control of IT system connected to the company network. Security standards need to be regularly updated

Function	Subcategory	Reference to the Guide	Level 1	Level 2	Level 3
PROTECT (PR)	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	Table 6.10: Backup and Restore (BR)	Backup and Restore of data is performed through the use of specific technology solutions that are able to automate the main required activities (planning of savings, monitoring of results, etc.) and in line with the other criteria specified in the control implementation guide. Backups are regularly tested according to a defined process	Solutions to maintain the operation continuity have to be assessed according to the objectives of restoring and safeguard identified information. Continuity plans have to be defined to restore operation continuity	Restore and backup objectives need to be regularly reviewed Continuity plans have to be tested and updated regularly
	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Table 6.6: Access Controls (CA)	Enter a preventive authorization and documentation process of the action taken	See PR.AC-3	See PR.AC-3

Function	Subcategory	Reference to the Guide	Level 1	Level 2	Level 3
	PR.PT-4: Communications and control networks are protected	Table 6.5: Perimetral protection (PP)	Perimeter protection of networks is obtained through appropriate hardware and software solutions in line with the criteria specified in the control implementation guide	Company internal communication networks (including the ones in which virtual systems are present) that play a particular relevant role for business operations must be properly protected through the use of firewall devices that segregate networks and restrict traffic just to the authorized one. Company wireless networks must be set up so to prevent non authorized accesses	Perimeter and internal communication networks must be protected with advanced solutions to protect the net traffic, in order to extend the basic functions of Firewall solutions. Access to company networks must be granted only after an assessment of compliance with the company standards
DETECT (DE)	DE.CM-4: Malicious code is detected	Table 6.4: Protection against Virus (PV)	Protection against Malware takes place through the implementation of dedicated technology solutions	The protection solution against malware (e.g. software antivirus and/or endpoint protection solutions) are managed and monitored at central level	Protection against malware is achieved by combining more technology solutions so to cover systems and networks (host based and network based)

Function	Subcategory	Reference to the Guide	Level 1	Level 2	Level 3
RESPOND (RS)	RS.MI-1: Incidents are contained	Table 6.11: Security Event Response (RI)	The response to Cyber Security events takes place at least through the establishment of a company procedure, written according to the criteria defined in the control implementation guide and communicated to all involved parties (e.g. employees, consultants, third parties)	The event management process must provide criteria for the definition of event priorities, modalities of event reduction and operation restoration. It must be possible to identify events through the analysis of events generated by security solutions and registered systems	The event management process must provide the registration of events and performed activities in order to manage them. The analysis on occurred events is to be carried out in order to establish the causes and to reduce the occurrence likelihood. A plan for the external communication of events is to be provided
	RS.MI-2: Incidents are mitigated	Table 6.11: Security Event Response (RI)	See RS.MI-1	See RS.MI-1	See RS.MI-1
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	Table 6.8: System update (AS)	The systems are automatically updated for the workstations and devices of final users, through technology solutions and according to the criteria defined in the control implementation guide. Servers are periodically updated	The systems are automatically updated for the workstations and devices of final users, through technology solutions and according to the criteria defined in the control implementation guide. Servers are periodically updated	Vulnerability Assessment activities have to be carried out regularly on all systems and company networks. Identified vulnerabilities have to be solved according to priorities based on the involved Assets relevance. Penetration Test activities

6.4 Guidelines to implement high priority Subcategories

The Framework implementation by the SME has been simplified – as anticipated in Chapter 4 – compared to the approach proposed for big enterprises and organizations. This provides, firstly, that all Framework high priority Subcategories are implemented. These represent, in effect, the essential actions to be performed in order to contrast the main and most common cyber threats and to protect the generally exposed SME systems. This Chapter aims at supporting SMEs in performing this first step.

This guide is made up of 4 use areas, each divided into eleven subsections, as reported below:

1. Identification of assets and security governing

   1.1 Asset identification (IA)

   2.2 Responsibility assignment (AR)

   3.3 Compliance with Laws and Regulations (CLR)

2. Identification of threats

   2.1 Protection against Malware (PM)

3. Protection of systems and infrastructures

   3.1 Perimeter protection (PP)

   3.2 Access Controls (CA)

   3.3 System Secure Configuration (CCS)

   3.4 System update (AS)

   3.5 Staff Basic Training (FBP)

   3.6 Backup and Restore (BR)

4. Security event management

   4.1 Security Event Response (RI)

For each subarea are indicated procedural, organizational and technical controls to be put in place and references to fulfilled Framework high priority Subcategories. All high priority Subcategories are addressed by the guide.

Identification of assets and security governing

Table 6.1: **Asset identification (IA)**

Description:	The implementation of countermeasures to reduce cyber risk should take place on all company systems and computers and in particular on the ones considered as critical for the business of the company. It is therefore essential to have an inventory of all assets represented by information, applications, IT systems and equipment within the company. To register important attributes, as for example the physical position, the owner, reference function, dependencies, etc. is functional to the cyber security governing and management. For example, an inventory of resources may activate the identification of systems that require the application of a specific software update.
Subcategory:	■ ID.AM-1: Systems and physical equipment used in the organization are registered ■ ID.AM-2: Platforms and software applications used in the organization are registered
Applicable controls:	IA.1 An inventory of information, applications, systems and equipment available in the company, both at IT level and in terms of Industrial Control Systems, if available IA.2 The inventory has to meet the following criteria: (a) For the inventory assets are provided at least type of information addressed, position, reference direction/function, the responsible, reference staff involved in various capacities in the management and maintenance activities, dependencies and further useful details for the implementation of the mentioned controls in the following sub-area (e.g. hardware type, software versions, processed information, service contracts, etc.) (b) Systems with greater relevance in terms of company business objectives to be achieved as well as the ones involved in various capacities in the compliance with cogent regulation duties are identified. (c) All status changes related to assets are recorded, such as acquisitions, installations, efficiency and withdrawal. IA.3 The inventory must be steadily updated, in particular whenever a change takes place and a history of changes has to be maintained

Table 6.2: **Responsibility Assignment (AR)**

Description:	The assignment of roles and responsibilities is an essential aspect to ensure a correct risk management and enables an efficient operation, intended as implementation of controls to prevent and/or contrast cyber security threats, which the companies are exposed to. It is important that the staff is aware of the roles and security responsibilities linked with the working activities performance. To the top company management, the CEO and the board of directors, more in general to the "owners" is assigned a key role in defining the priorities and assigning the resources linked to cyber security initiatives. These are in effect ultimate responsible for cyber risks within the company.
Subcategory:	■ ID.AM-6: Roles and responsibilities related to cyber security are defined and communicated for the entire staff and possible relevant third parties (e.g. suppliers, customers, partners) ■ PR.AT-4: Managers and directors understand roles and responsibilities
Applicable controls:	AR.1 The company top management (i.e., CEO, board of directors and managers) has to be aware and understand the responsibilities associated to cyber security risks. This should be clear at least within the board of directors (if present/applicable) AR.2 Roles and responsibilities linked to cyber security, as for example the one provided for the protection of systems and infrastructures or the ones linked to the correct use of IT tools have to be established and made official, for the entire staff and involved third parties (e.g. suppliers, customers, partners). AR.3 Within the organization, should be identified the reference representative for cyber security (i.e. the responsible for cyber security), whose task is to coordinate the various cyber security initiatives and to contact authorities and National CERT in case of wide scope events AR.4 All assigned responsibilities should be duly formalized

Table 6.3: **Compliance with laws and regulations (CLR)**

Description:	The sharp growth of information technology and actual digitalization process implied and will imply also in the future the possibility for the companies to steadily adjust themselves to specific laws and regulations in order to protect users and organization within the cyberspace. The organization has the duty to be aware and comply with the law and regulations applicable to their context, above all with reference to its market and the type of used and/or provided IT services.
Subcategory:	■ ID.GV-3: Legal requirements in matters of cyber security, including the duties related to privacy and civil freedom have to be understood and managed
Applicable controls:	CLR.1 Identify laws and regulations that directly or indirectly impact cyber security (es. Computer Crime, Data Breach Notification, intellectual property), by regularly updating the inventory CLR.2 Identifying, through a regular monitoring activity, each possible non-compliance with the provisions of laws and regulations and preparing a specific adjustment plan to address such non-compliances, by sharing specific impacts and implications with the company top management CLR.3 Taking the measures established in the adjustment plan, as approved by the company top management CLR.4 Assessing over time the actual implementation of necessary measures to ensure the compliance with laws and regulations, sharing with the designated company responsible staff the gaps and/or criticalities that can imply non-compliance or legal consequences of civil and/or criminal nature.

Identification of threats

Table 6.4: **Protection against Viruses (PV)**

Description:	It systems are generally exposed to malevolent software, also called malware, especially in case of Internet connection. Impairment through malware may happen in various ways, as for example by opening an infected e-mail, by surfing in impaired websites, by opening files on local devices or contained in external mass storage devices (as for example USB Storage). Specific protection solutions should be adopted in order to monitor, identify and remove the malware.
Subcategory:	▪ DE.CM-4 The malevolent code is detected
Applicable controls:	PV.1 Malware protection solutions (e. g. antivirus software and/or solutions for endpoint protection) should be used on all company systems such as computers, servers and company mobile devices, including the ones related to industrial control systems (e.g. SCADA systems) PV.2 The protection against malware must be effective in contrasting all kinds of malware: Virus, Worm, Trojan, Spyware, Rootkit, Botnet, Keystroke Loggers, Adware. PV.3 The protection against malware must me kept constantly updated over time, by using as far as possible to automatic update mechanisms of at least daily controls; PV.4 The malware protection must always be active and not able to be deactivated by users. It should also be set up for: (a) Remove or isolate (quarantine) files infected by malware (b) Perform regular scan of all files (c) Provide notifications in case of suspected malware identification PV.5 The solution must ensure protection in the following cases: (a) Access to locally saved files and data on external devices or centralized servers (e. g. file server) (b) Access to an e-mail or related attachments (c) Access to web sites while surfing on the Internet, by preventing the connection to malevolent sites (d) Access to Instant Messenger and to any other communication form that enables the exchange of files and information

Protection of systems and infrastructures

Table 6.5: **Perimeter protection (PP)**

Description:	The computer networks of an organization, connected to Internet or interconnected with other nets, must be protected by hackers trying to get access to systems, computer and information. A net security device like firewall installed on the net perimeter is able to protect the net against basic cyber threats – attacks that require limited capabilities and techniques, and therefore are widely spread – by limiting the net incoming and outbound traffic only to authorized connections. Such restrictions are obtained by applying the setup settings known as rules (or policy) of the firewall. This solution is to be properly installed, set up and managed over time, in order not to nullify the achievement of specific targets.
Subcategory:	▪ PR.PT-4: Communication and control networks are protected
Applicable controls:	PP.1 One or more firewalls (or similar protection devices) must be installed on the outer net perimeter of the organization (as for example between the Internet and the internal net) PP.2 Each rule that allows traffic through the firewall, linked to IT communications, must be approved by a company responsible PP.3 Non approved services or typically vulnerable services must be deactivated or blocked through specific firewall rules PP.4 Firewall rules that are no longer needed (for example because the service is no longer needed) must be removed or disables immediately PP.5 Passwords associated to firewall administration credentials must be modified as an alternative to the basic ones provided by the producer and attributed to single-user accounts PP.6 The administration interface used to manage the system must be protected against unauthorized access through Strong Authentication techniques (e.g. based on two independent authentication factors) or robust passwords if accessed only from the internal net. Users have to be blocked after a maximum number of unsuccessful access attempts

Table 6.6: **Access Control (CA)**

Description:	Access control methods must be established in order to limit access to information, apps, systems nets and IT devices in general by all user types. The objective is to ensure that only actual authorized users can access such systems or data, by ensuring a minimum privilege system needed to exercise their functions.
Subcategory:	■ PR.AC-1: Digital identities and access credentials for users and authorized devices are administered ■ PR.AC-3: Remote access to resources is administered ■ PR.AC-4: Access to resources is administered according to the minimum privilege principle and separation of functions ■ PR.AT-2: Privileged users (e. g. System Administrators) include roles and responsibilities ■ PR.MA-2: Remote maintenance of resources and systems is approved, documented and performed so to avoid unauthorized accesses
Applicable controls:	CA.1 Access control measures must address: (a) All types of roles (employees, suppliers, partners, etc.) (b) All kind of information, services or systems, which the staff has to interact with CA.2 The entire staff (internal and external) should be univocally identified and authenticated in order to access services, systems and company information through the use of nominal IDs (accounts) CA.3 In case of authentication credentials like username and password, they have to comply with the following criteria: (a) Use of robust passwords (at least 8 alphanumeric characters and special characters like $, #, !,?,"), possibly implemented through setup mechanisms and automatic controls (b) Regular update of passwords at intervals no longer than 60 days CA.4 The assignment of access credentials and related privileges must undergo an approval process according to the following principles: (a) Minimum privilege, that is assignment of minimum privileges needed to perform one's tasks (i.e. Least Privilege) (b) Access just to the information strictly needed to perform one's tasks (i.e. Need-to-Know) (c) Segregation of roles, in order to separate incompatible activities among various players CA.5 Credentials used for specific activities, such as the administration of systems and IT apps must be managed by complying with the following criteria: (a) Limited to a strict number of previously authorized persons and managed in compliance with the regulations in force (b) Distinguished from the ones used for other purposes CA.6 Accounts and access privileges must be disabled when they are no more necessary (e.g. change of structure, drop out from the organization)

Table 6.7: **Secure Configuration of Systems (CSS)**

Description:	Computers and net devices cannot be considered secure with the initial standard factory settings. In effect, admin credentials, or in general factory settings, are frequently public or not safe and could be used for unauthorized access to company systems and to related information. By implementing some simple precautions during setup of new computers and IT systems, it is possible to considerably reduce risks and likelihood of successful IT attack.
Subcategory:	▪ PR.IP-1: Reference practices (so called baselines) are defined and managed to setup IT systems and industrial control
Applicable controls:	CSS.1 Deactivate users that are not strictly necessary, above all the ones characterized by high privileges (e.g. admin and system users) CSS.2 Immediate modification of nominal users and any preset factory standard password, using univocal users and robust passwords CSS.3 Remove and disable the software and unnecessary services (including applications and admin tools) CSS.4 Disable "automatic" function in order to prevent for example the possibility that a software is automatically executed if an external device (e. g. USB Storage) is connected to a computer CSS.5 Using a personal firewall (or equivalent) on PCs, laptops and other IT devices for personal or company production, blocking unauthorized net connections CSS.6 Using encoded net protocols for the remote control of servers and net devices (e. g.. SSH, SSL) CSS.7 Setting up technical users (application to application or machine to machine) so that the interactive use by the users is not possible CSS.8 Activating the logging function on systems. In case of personal data processing, the provisions of the relevant regulation have to be complied with CSS.9 Setting up the systems so that the final user is not able to independently modify setup configurations

Table 6.8: **System update (AS)**

Description:	The software of all computers and more in general on IT systems may present errors or flaws, generally known as "vulnerabilities". They represent intrinsic weaknesses that can be exploited by single persons or group of hackers, as well as by malware and other malevolent programs. Since the time of detection and until the time in which they are exploited, vulnerabilities must be identified and managed through appropriate countermeasures, as for example the installation of updated released by the software developers, in order to solve one or more vulnerabilities. Software developers are responsible for the supply of remedies for the detected vulnerabilities, as rapidly as possible, in form of software update, also known as "Security patches" and released to the customers within the license framework. In order to reduce information and IT system impairment risks taking advantage of the software vulnerabilities, companies and organizations must effectively manage such software update processes.
Subcategory:	▪ RS.MI-3: New vulnerabilities are mitigated and documented as accepted risk
Applicable controls:	AS.1 Software installed on company systems like computers, servers, net devices, mobile devices, etc., must provide a manufacturer license so to guarantee the availability of security updates and other updated that may impact security AS.2 Companies need to identify and obtain the Patch (including critical updates, service packs), once available in order to correct the detected vulnerabilities, by interacting with the software producers or completing their recovery from the official or authorized websites AS.3 Updates have to be promptly installed and, if possible, after an impact analysis carried out through mechanisms of automatic update AS.4 The software that is no more supported (i.e. Out-of-Date) must be removed from the company systems and replaced by more recent versions (for which the producer releases the related updates)

Table 6.9: **Basic staff training (FBP)**

Description:	Company users, who interact with IT systems represent the main cyber risk source. Inappropriate or wrong behaviors can nullify the most sophisticated security measures implemented by a company. To raise the awareness of users about the appropriate use of IT tools and information, the organization has to plan specific awareness raising and training programs in order to improve the cyber risk perception and to promote an appropriate conduct. Specific awareness raising and training programs must be targeted to the entire internal and external staff that accesses directly or indirectly to the organization IT systems and information. Such programs must be targeted at creating a cyber security culture in order to prevent inappropriate behavior and to reduce the consequent exposure to risks.
Subcategory:	▪ PR.AT-1: All users are informed and trained
Applicable controls:	FPB.1 Full involvement and approval of staff training and awareness raising plans by the top management, which stresses their importance and monitor their full performance FPB.2 Performance of sessions at least one a year through classroom training and/or using e-learning platforms FPB.3 References to cyber security during daily activities, through various techniques and communication modes (e.g. informative poster in offices, awareness raising e-mails about the risks and correct behaviors, distribution of specific brochures, dedicated sections on websites and internal portals). FPB.4 Addressed topics should include at least also: (a) Security principles (b) Appropriate use of company tools (PCs, mobile devices, etc.) and risks related to their inappropriate and incorrect use (c) How to proceed in case of suspicious events (e.g. suspicious e-mails received, unusual behaviors of company tools) or in case of security events (e. g. system and external support impairments) (d) Specific roles and responsibilities related to cyber security (e) Applicable laws and regulations and consequences in case of violation FPB.5 Dedicated and specialized training for users with higher privileges (e.g. IT system administrators), so to increase and maintain updated the specific competences on cyber risks and the related protection techniques over time

Table 6.10: **Backup & Restore (BR)**

Description:	Availability of information and systems is essential to guarantee the business of a company on the market. The primary control to be implemented is represented by the storage of business information and system setup on dedicated supporting devices, to be used in case of disasters, human errors and failures, by favoring normal operations.
Subcategory:	▪ PR.IP-4: Backups of information are regularly executed, administered and assessed
Applicable controls:	BR.1 Appropriate mechanisms and tools for the storage and recovery of data and information need to be used BR.2 The type (partial or total) and frequency of saving need to be defined. These have to be established according to the organization business needs, information security requirements, obligations provided by the law and criticality of information processed in order to maintain the operational performance BR.3 The positive results of information and data saving and recovery activities is to be assessed regularly (e. g. through test activities) BR.4 Backups need to be remotely stored, at a sufficient distance from the headquarters, or through cloud services with the same purpose, in order to avoid impairments in case of disaster. They have to be protected with similar measures of physical and logic kind compared to the ones taken at headquarters

Response to security events

Table 6.11: **Response to security events (RI)**

Description:	If security measures are not able or are just limitedly effective in preventing negative security events (e.g. system impairment, unauthorized access to information), the organization needs to be able to rapidly and effectively react to a potential security event, by reducing impacts and limiting the future occurrence likelihood.
Subcategory:	▪ RS.MI-1: In case of incident, procedures to reduce the impact are put in place ▪ RS.MI-2: In case of incident, procedures to reduce the impact are put in place
Applicable controls:	RI.1 Describe and communicate to the entire involved staff the procedure to be implemented in case of suspected violation or security event (i.e. event management process) RI.2 Incident management procedure must define at least: (a) General criteria to be adopted in order to identify an event (b) Types of events and related severity scale, needed to make a first classification (c) Internal reference staff list (e. g. Information System responsible, Communication responsible, Legal responsible, Company Management) and external ones (e. g. Judicial Police bodies, external suppliers) to be contacted in case of incident (d) Event notification criteria for the various reference staff and response criteria, related roles and responsibilities, aimed at reducing impacts and/or mitigate the effects according to type and severity (e) Criteria, roles and responsibilities, procedures to restore the previous status before the event

7. Recommendations for Large Enterprises

In the last decades, the company net asset value has gradually increased with a shift from the tangible to the virtual dimension. In may sectors, virtual assets, like intellectual property, reputation and online confidence, online customers and other intangible assets have overcome tangible ones in terms of economic value, sometimes even of criticality. Furthermore, the use of Information Communication & Technologies (ICT) in the production processes involved numerous key sectors of domestic economy, from the financial sector to energy, transport and telecommunications, chemical sector, organized large retail and so on. Furthermore, after the introduction of "Industry 4.0", also the traditional production processes have evolved so that the ICT has become a strategic and essential element.

This new scenario exposes all companies and institutions to new risks, such as intellectual property theft, data tampering, operation interruptions or even impact on the quality and safety of production plants. All of the above may considerably impact the company competitiveness and value, including the share price and the value for shareholders.

The evolution towards information technologies came also with a diversification and spread of cyber threats: In few years, cyber attacks committed by various players – for example activists, criminals and groups supported by Governments – took place in addition to the physical ones. The consequence of this scenario, among others, was the so called "hybrid war", in which typical security elements as well as new ones of the cyber war combined and, first of all, directly involved national Critical Infrastructures.

Companies and organizations may initiate a process to improve their security through specific initiatives and plans. In order to support the identification and introduction of strategic initiatives, some recommendations for the top management and some plan proposals are reported here to help companies to widely address the improvement of their own protection and defense capacity, by extending the scope of their controls as well as their maturity level.

7.1 The top management role in managing cyber risk

Companies are more and more targeted by sophisticated threats and for that reason they began to raise huge technology and financial resources to defend themselves. Threats involve all companies: Not just big ones, but also small and medium enterprises have become usual target, considering the intangible asset variety and low protection level. Damages are not just linked to intellectual property theft, but also to the company reputation. More and more frequently, it is because of these attacks that some managers loose their position. The increasingly spread Corporate Governance rules provide that directors are responsible for their activity management and protection. For the above mentioned reasons, it is necessary that the board of directors and top management of companies/institutions/organizations understand and evaluate new risks, by balancing growth and market profitability with company protection and risk mitigation. This task is already provided in the mandate of the Board of Directors, which, even with the help of a Control and Risk Committee, if available, has the duty to define the nature and risk level compatible with the company strategic objectives, also considering all risks that may be relevant for the medium-long term sustainability of the company business. Furthermore, the Board has also the duty to assess the adequacy of the organization, administration and accounting structure. Such principles are already provided by the self-discipline code of the Italian Stock Exchange [8]. Undoubtedly, cyber risk should be considered as potential "main risk" for companies and public organizations, as pointed out in the Annual Report 2014 of the Presidency of the Council of Ministries about the Security Policy of the Republic [22].

Undoubtedly, considering the extent and effects of the cyber threat, this should be considered among high relevance risks that every company and organization has to evaluate and manage. By implementing these Corporate Governance principles and in line with the provisions of the Strategic Plan and the National Plan, companies should introduce the following initiatives/practices at the Board of Directors and top management level:

1. **The cyber risk** – The Board of Directors and top management (hereinafter called "top management") consider cyber (or IT) risks among high level risks. Risks have to be assesses in an accurate and analytic way, identifying impacts on companies, customers and external players (other sector players, citizens/civil society, Government). The assessment of these risks is supported by the Control and Risk Committee (CCR), where applicable, through an appropriate investigation activity both of consulting and propulsive nature. The top management has to address cyber security as a general risk management issue (Enterprise risk management) and not exclusively as an "Information Technology" issue.

2. **Cyber security as strategic element in company governance policies** – The company Governance consists in the set of rules of any level (laws, regulations, etc.) that regulate the management and direction of a company (or, more in general, of a public or private organization) and includes the relationships among involved stakeholder and the organization objectives. The main players are the shareholders, the board of directors and the management. More in general, company governance consists of a set of rules, relationships, processes and company systems, through which the trust authority is exercised and controlled. The company governance structure represents the rules and processes, through which company decisions are taken, as well as the way, in which company objectives and means to achieve and measure achieved results are defined.

   All company departments cooperate in drawing up the guidelines to define the organization governance and, in this regard, also cyber security must be considered in a shared systemic perspective, according to which it is not considered as a superfluous or disturbing element,

but is embedded as one of the fundamental elements in the definition of risks, therefore it is considered as one of the strategic tools of the company vision expression.

Therefore, the top management draws up a governance plan including cyber security, which involves all the company roles and functions and all the operation risk areas, by clearly defining roles and responsibilities and their appropriate separation (task segregation principle), so to identify three control levels: Primary level control, under the direct responsibility of who exercise the function (production, IT, sales, etc.); second level controls, under the responsibility of a security function, external to the production/business functions; third level controls, under the responsibility of the internal control functions (audit). The function responsible for the second level controls deals with the definition of company security policies and the assessment of their correct implementation (compliance). Furthermore, the top management ensures that the integrated governance plan fulfill the following needs:

(a) alignment between risk management and company strategic objectives;

(b) definition of an organization model that provides coverage of security processes and domains of the entire company;

(c) definition, within the organization model, of an integrated risk management process in order to identify and contextualize, assess, react and monitor risks related to the organization and its assets, services, staff, other organizations and the State;

(d) efficient and effective allocation of the required resources by a systemic company management, including risk management;

(e) definition of a monitoring and efficient and effective organization reporting process (according to the wished metering shared with the top management) as well as a change management process in case of need to modify one's own company structure, by adopting adequate analysis approaches (e.g.: System Dynamics) that take into account the dynamicity and intrinsic "systematic nature" of the organization;

(f) provision of an assessment, monitoring and presentation process of risk management within this process.

The top management ensures that the governance model and cyber security plan is embedded in the company plan for risk management (Enterprise risk management) and crisis management plan or "crisis management". More and more frequently, impacts derived from cyber threat are classifiable as crisis, thus a consistent and integrated management is needed, possibly by using tools and methods to support the decision making process, which provide an integrated perspective of the system model and considers all company dynamics (e. g. Model-based Governance). Among the aspects the top management is to be drawn the attention to, there are also the ones related to risk management in case of outsourcing and cloud contracts. Often one believes that the risk is handed over, but this is not the case: There is only a different way of operation security management that requires a careful assessment both by the top management, the CISO and the facilities involved in the service management.

3. **Roles and responsibilities** – A correctly integrated company Governance, i.e. a comprehensive vision, shared by its management, related to interdependencies among the various company functions and to the impacts that some issues in one of these functions could cause on other ones in cascade, must provide the definition of a correct organization structure that includes on the one side a steady improvement both of processes and policies

and therefore the elimination of wrong mental patterns of the function representatives, reaching the virtuously called Learning Organization. For instance, it is already well known that some social aggressive strategies (through the manifold phenomenon known as Insider Threat) proved to be particularly effective to bypass special technology controls, to the detriment of security procedures related to the introduction of IT material coming from outside the company, or through the external staff dissimulation (as in the well-known Mall Target case in the US). Therefore, cyber security is an issue that involves the entire company, from the top management to operation facilities, and thus it should be systematically assessed and steadily monitored. Often, companies make the mistake of assigning cyber security management exclusively to the ICT structure. Although the ICT plays a relevant role in managing security, this approach implies some possible problems, below are listed some of them:

(a) cyber risk is seen mainly from an IT system point of view, and often inadequate countermeasures are taken;

(b) it is implicitly assumed that there is a limited combination between the business needs and risk reduction needs of the entire organization;

(c) intrinsic organizational difficulties ma impact the implementation of security processes and countermeasures within the various company functions (of business, production, administration, etc.);

(d) security management plans are incomplete;

(e) possible tension between ICT investments and security investments (often ICT budget cuts directly impact cyber security budgets).

In order to guarantee a complete coverage of the company, it would be useful to support the security functions within the ICT division with "logic" security functions outside the ICT (generally a report of the Chief Security Officer or the Chief Risk Officer, or in some cases a direct report of the General Director, of the Chief Operating Officer or of the CEO). This logic security function is driven by the CISO - Chief Information Security Officer. This approach ensures the responsibility segregation principles and allows the distinction between first level control (assigned to the ICT or to the business/production functions from the second level ones (carried out by the CISO and/or the logic security function).

4. **The CISO role** – The Chief Information Security Officer or CISO is established by the top management, which ensures that the role is assigned to somebody who has the due relevant competencies and experience. The CISO responsibilities include: a) Introduction/development of a company IT risk management, in line with the general process of risk management (Enterprise risk management) b) Monitoring of risk development and consequent adjustment to the plan c) Analysis of the main events, of their consequences and actions taken to mitigate future occurrences d) Periodic report to the top management e) Connection function between top management, company functions and domestic and foreign institutions. In companies of medium/big size, this role should be assigned to a dedicated responsible to this aim.

5. **Integrated monitoring** – The top management regularly assesses identified risks, together with the comprehensive ERM, and the mitigation plan. The top management has the task to take a decision about the choices related to the cyber risk mitigation/acceptance/transfer strategies, as it is the case for all other risks the company is exposed to.

6. **Resources** – The top management has to assess adequate economic and relevant staff resources support the security plan. Allocated resources must be consistent and in line with the company risk management plan (Enterprise risk management). The possible residual risk must be correctly evaluated and, if not in line with general guidelines, a risk treatment plan is to be drawn up by assessing the possibility of risk reduction through the implementation of countermeasures, by preventing the risk and removing risk sources, or by transferring the risk.

7. **Awareness and cyber security culture** – The top management must carry out activities to promote the awareness and cyber security culture at all company levels. The CISO will arrange a program to increase the internal and external staff awareness in order to reduce risks deriving from the inappropriate or wrong use of the organization IT tools and processes. Furthermore, internal and/or sector and national training sessions may be arranged in order to test and improve the capacity of the top management and of operation structure to manage cyber events.

8. **Information exchange and cooperation** – The top management must promote and support initiatives aimed at establishing and strengthening cooperation relationships with other organization of the same sector and with the institutional bodies in charge for the fight the cyber threat. The participation in Sector CERT or institutional CERT (like the National CERT) and the cooperation with other organizations allows to improve the threat under standing, to share fighting practices and tools and, in some cases, to develop common capacities.

7.2 The cyber security risk management process

As a consequence of the cyber threat evolution, it is necessary to adjust also the approach towards the IT assets protection, of IT facilities and business processes, by passing from a static paradigm to a dynamic risk view. Figure 7.1 shows a traditional process of information security risk management, with limited risk integration at enterprise level, often assigned to IT technical staff. The process is completed within the company context, without any interaction, if not just rare and unstructured, with the external environment. Unlikely, cyber security risk management is a continuous and dynamic process, from which to derive actions to be implemented in order to consciously implement risk management, adjust to the assets to be protected and in line with the organization changes in terms of time, as well as environmental, technology changes regarding the company, internally as well as externally. Without this process, the company risks to invest and spend money in non-priority areas and/or not to invest adequately in high risk areas.

By focusing on the steadily evolving attack scenarios, one of the possible evolved cyber risk management processes is presented below. It is based on the introduction of new important elements:

- Cyber intelligence – analysis of threats in the “real world” through a steady safeguard and predictive analysis of information mostly coming from external sources; this component of cyber intelligence can be supported by an information gathering process base on institutional sources (CERT, Intelligence, Postal Police, etc.) and private sources (business information agencies) that serve also as information quality certifiers.

- Continuous monitoring – steady analysis of information coming from the company internal context (for example CERT and SOC), in order to improve and contextualize the threat event occurrence likelihood, by acting as activation factor for the dynamic risk calculation;

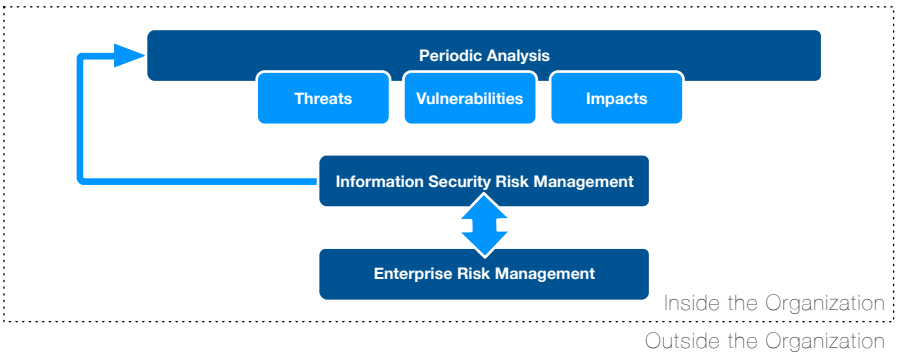

Figure 7.1: A traditional approach to IT risk management.

- Threat modelling – identification and selection of factors (threats, vulnerabilities and impacts) able to represent potential threat scenarios with detailed evaluation of risks based on under standing capacities and intentions of potential attackers;

- Information Sharing – relevant and timely information exchange in order to prevent and/or fight against the cyber threat affecting public and private governance actors (as for example the National CERT or the US-ISAC), after the definition of sharing agreements.

Figure 7.2 shown such evolved cyber risk management process, consistent with the above mentioned principles. In particular, the process implies that the organization implements information gathering policies and information sharing policies in order to support a cyber intelligence component and that it shares a piece of this information through the same information sharing channels. This way, the organization does not only consider the potential risks related to the internal company context, but also assesses the potential risks related to the outside context, above all the ones related to the interconnection level of one's own information system with the external environment. The Figure also point out the new role played by the cyber security risk management process that now is integral part of a global risk management and in which the top management plays a crucial role. With this approach, the cyber security risk management process receives information and data from the cyber intelligence components and from the IT structure steady monitoring to define, in a cyclic and continuous process, the best strategies to manage cyber risk.

The basic purpose is to shift the cyber threat management from a reactive approach to a proactive one, through a dynamic model that makes possible to consider the organization as an independent system of activities, processes, technologies, data, people, relationships, etc., which is customizable and gradually implementable according to the specific organization nature. In this new vision, it is essential to carry out a cyber risk analysis within a more general systematic analysis of the organization dynamics, in order to start an evolution path from Information Security Risk Management to cyber security risk management, so that the strategic choices and/or policies to be implemented are correctly considered.

In general, an appropriate cyber security risk management process must be strictly matched with the main business processes and it requires, firstly, the involvement of the organization Board, of the staff having experience and vertical competencies regarding risk and security, as well as appropriate qualifying technical tools. In this regard, it is crucial to implement a process of analysis and selection of the most adequate technical and operation solutions, even with the help of highly specialized external consulting services, which, starting from the situation *AS*

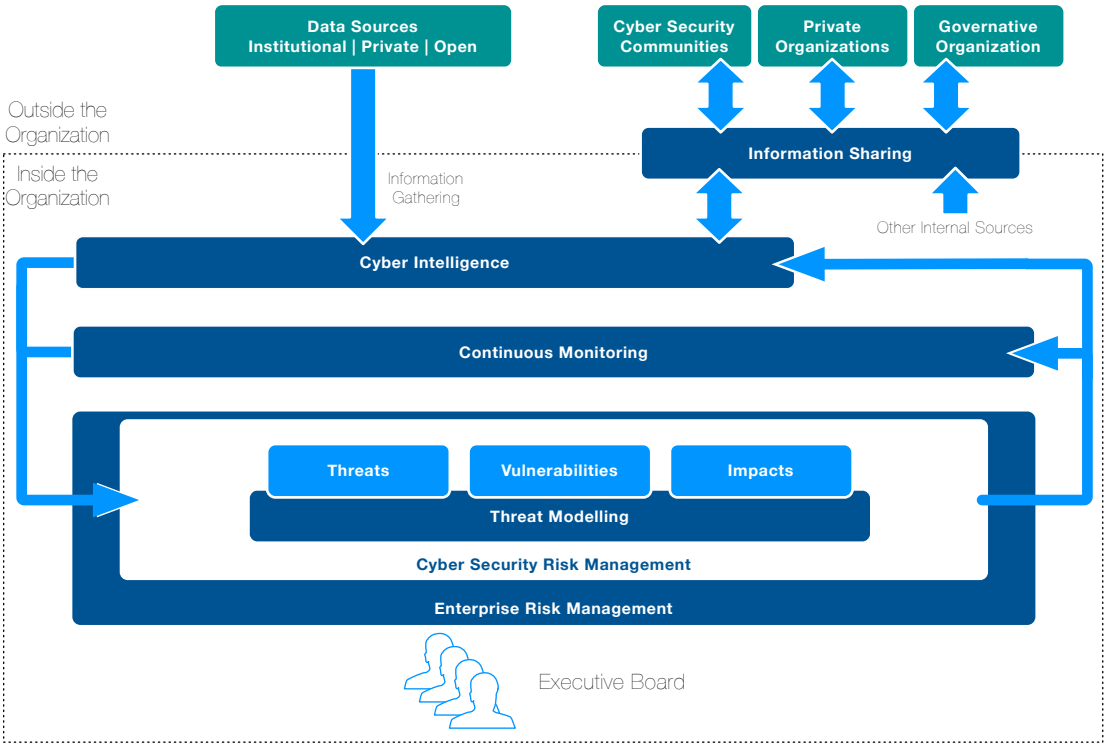

Figure 7.2: An evolved approach to cyber risk management.

IS identify the most appropriate solutions for the organization context according to the model requirements *TO BE*.

In defining the cyber security risk management process, the organization should achieve the following objectives:

- To establish univocal criteria for the evaluation and identification of cyber risks;
- Standardization of a uniform analysis method in order to achieve comparable results over time;
- Be aware of the risk exposure level of each company information system component;
- Assess if the identified risk is acceptable or if, instead, it is necessary to plan appropriate processes to mitigate the risk.
- To provide an adequate and flexible method to identify technical-organizational protection needs in order to balance in the best way the possible preventive and detective security countermeasures;
- Allow the monitoring and analysis of security events in order to put in place improvement actions;
- Assess all potential risks in defining and implementing new IT services;
- Identify a company function that coordinates all activities;

- Embed the cyber security risk management process within the Enterprise Risk Management process (if already available in the organization), according to a common Framework that makes possible to put together information in order to obtain a systematic perspective of company risks as well as a selection of specific actions within the IT scope in terms of mitigation priorities.

- perform a unique reporting for the company management.

The activation of the cyber security risk management process would allow to the organization to achieve a set of benefits, among them:

- Comply with national and international laws and regulations that expressly require that the organization is equipped with an IT risk Analysis method or process;

- Ensure the compliance of the IT governance with the company business objectives, in terms of sustainable evolution, operation excellence and cost competitiveness, through the risk exposure reduction;

- To plan appropriate response actions to potential cyber attacks in order to minimize possible impacts and therefore ensure the continuity of supplied services;

- Enable the organization to minimize security costs, ensuring an appropriate risk reduction at acceptable levels by the organization self. In other words, to avoid costs for implementing a security level, which is higher than the appropriate one and which applies to information system components with low impact for the organization.

The design and activation of the cyber security risk management process requires a series of initiatives that, even if strongly dependent on the initial situation, imply a considerable effort (human resources, time, etc.). Therefore, its implementation should take place in different project stages.

7.3 Computer Emergency Readiness Team (CERT)

Consistently with the National and International orientations, the establishment of a centre for critical cyber security events, commonly known as CERT, has become an essential and spread practice in order to effectively prevent and react to this kind of events. The CERT represents the main contact point of the organization in matter of cyber security, both in terms of prevention in order to avoid or reduce the effects o fan impairment and in terms of reaction and timely response in case of specific critical event; in this sense, it works actively to favor the information exchange with other CERTs and security communities, belonging to the same sector as well as in case of specific excellence centers in this context. Among the main capacities that a CERT should have, there are:

- identification and proactive analysis of the main threats, in order to promptly assess known or emergent impairment scenarios that may have a direct impact on the Constituency;

- definition of processes and structured methods for the event management, in order to favor a rapid and appropriate reaction to possible impairments, by cooperating, if needed, with other organizations (e.g. other companies of the same sector) or institutions and reference communities (e. g. armed forces, National CERT);

- development of the capacity to promptly identify security relevant events, also through the integration with other cyber security protection tools within the organization, as for example the Security Operations Center (SOC)[1];
- availability of central tools (e. g. Web Portal, Blog, secure e-mail, Information Sharing platform, etc.) in order to favor the exchange and dialogue with the Constituency and the other involved parties (e. g. Bodies, Institutions, cyber security communities, etc.);
- development and participation to internal and external simulations to identify the robustness degree of event response processes and procedures;
- support to the definition and supply of security awareness programs aimed at raising the awareness regarding cyber risks and to favor correct behaviors in terms of risk prevention.

The development and establishment of a CERT should take place through the following main activities:

- Definition of objectives and reference Constituency through the formal identification of purposes set by the CERT and the precise identification of (internal and external) user community targeted by the CERT services;
- Accurate choice of services to be supplied, by assessing benefits and expectations linked to each service. This evaluation should be based on criteria and modes that make the services effectively appropriate and able to supply the highest benefits to the Constituency;
- Identification of the reference organization model, considering the possible synergies and internal integrations, needed to reach the established objectives and to maintain the quality indexes for the supplied services (e. g. reaction times in case of incident, security bulletin frequency);
- Development of technical and operational capacities needed to supply the services, according to a reference model that takes into account, on the one side, the sector best practice, on the other side the need of gradual progress of CERT services and capacities over time;
- Definition of sharing, cooperation and coordination model needed to maximize the benefits deriving from the information exchange and in general from the spread capacity to fight and reduce impacts after a possible cyber attack;
- Definition of the Investment plan and related action roadmap with the aim to prioritize the release of services and related capacities in a cost/benefit perspective and considering the intrinsic complexity linked to the topics (e.g. need for professional specialist competencies, integration and use of technical platforms, relationships with the Constituency and with other reference entities, selection and management of third parties)

[1] Compared to the CERT, the SOC role is to constantly monitor the cyber threats that can directly impact the organization ICT structures, as well as to effectively manage the security devices in place for the protection of the same infrastructures. The CERT works in strict coordination with the SOC, mainly supplying information (e. g. Security Intelligence) and comprehensive coordination services in the framework of critical event management (or unknown ones). The interaction between SOC and CERT is usually censure by a shared event prevention and management process, based on specific criteria of mutual “engagement”, aimed at ensuring strict cooperation between the two functions.

PART III – Aspects related to the application context

8. Enterprise Risk Management: reference context

The enterprise business is characterized by an indissoluble link with the risk. Risk is an intrinsic characteristic of company business and risk identification, evaluation and management capacities are at the base of company success. The interest in the risk management has assumed crucial importance since the nineties: Gradually its value has increased, booming in recent years. However, initially risk was considered, in practice and in literature, merely as a secondary element within the enterprise managing, as risk management was usually restricted to simple separated actions aimed at reducing the uncertainty deriving from specific activities. The limits of this orientation became evident by the end of the nineties, when the greater uncertainty showed by the economic context and financial markets has deeply changed the context, in which the enterprise works. The increasing competitiveness, the new organization models, impacts deriving from technical development on business competitive dynamics, financial collapses recently affecting some listed Large Enterprises, the increasing social, economic and political instability increased the degree of instability, uncertainty and the set of variables impacting the achievement and maintenance of company results. Real estate markets, credit institutes, rating agencies and investors became aware of the increasing relevance of risk in company activities asking the companies to take more into account such issue as well as to take appropriate measures to manage it, pointing out the need to improve internal control systems of the companies in order to anticipate and manage the change and, therefore, to strengthen and increase their capacity to create value for the stakeholders. The traditional risk-insurance approach is being given up in favor of an integrated management process related to generally accepted organization solutions shared by the whole organization. The crises in 2008 contributed furthermore to spread among the companies the awareness about how even apparently irrelevant risks could cause serious damage if not managed adequately, and this is even truer if various types of risk events interact. The result is that a good risk management model should make possible to understand the potential positive and negative aspects of all factors that can impact the organization, by increasing the success likelihood of the strategy and reducing the uncertainty of achieving the general objectives of the company. Therefore, the risk becomes a further productive factor in the company framework, to be managed according to the common entrepreneurship and

management principles [12]. The economic situation development, like the changed risk consideration led to the establishment of innovative management models within the company context. one example is the Enterprise Risk Management – Integrated Framework defined and developed by the Committee of Sponsoring Organisations of Treadway Commission (COSO) [14]. This Framework, published in September 2004, defines the Enterprise Risk Management (ERM) as a process put in place by the board of directors by the top management and other company staff; applied to develop the company strategy of the entire organization, planned to identify and manage events that could have a positive or negative impact on the company; focused on maintaining the company risk level within an acceptable risk appetite threshold; designed to provide a reasonable guarantee to the company related to the achievement of its objectives. In this model, risk management goes with a regular operative activity and becomes integral part of the company organization structure. Furthermore, the ERM adopts a comprehensive risk vision that proves to be essential in order to identify the possible interconnections between the various risk types. As a matter of fact, just by considering the company as a unique entity, in which various interconnected areas and activities are organized. Therefore, the Enterprise Risk Management (ERM) model proposed by the COSO promoted the organic and integrated management paradigm of all types of company risk, where the ERM goes with any company activity and process in order to better evaluate the risk assumed by the enterprise both in detail and as a whole. An evaluation of the global risk profile enables the management to assess and analyze the consistency of taken decisions, and on the other side to align the company risk level to the acceptable risk level. A complete and detailed evaluation of the company risk is crucial and essential for a correct assessment and selection of company strategies and related objectives. Therefore, the integrated risk management acquires a strategic tactic and competitive nature, able to positively influence the entire process of creating value for the company. Another significant and niche approach, as it is specifically addressed to the cyber security aspects of small and medium enterprise, is represented by “A simplified approach to Risk Management for SMEs”, an initiative of 2007 promoted by the European Agency for the Security of Networks and Information (ENISA). As indicated in the title, the European Union body decided to equip the management staff that is not expert in matter of security, with a simple tool to perform a guided and modular risk self-evaluation. In this regard, security aspects have been simplified and acceptable target security levels have been established, identifying, as provided by the National Framework, a target risk profile to tend to[27].

8.1 Risk analysis

Risk Appetite and Risk Tolerance

In the risk management analysis, primary relevance is given to the definition of the internal environment and company strategic objectives. The internal environment represents the essential identity of an organization, establishes the modes in which the risk is considered and addressed by the company staff, the ethical values and the general working environment. In this framework it is crucial to define the company risk management philosophy. This represent the common attitudes of the company risk approach, the way it is considered in all activities, identified and managed. It results then in the identification of the company Risk Appetite that is the inclination to the risk that reflects the way in which events are perceived and identified, what kinds of risk are accepted or not and how they are managed. Risk Appetite is identified and is the result of a dialogue between the management and the board of directors, as it impacts both the strategic choices addressed to the board and the operative ones related to the directors of various units. The Risk Appetite choice is at the base of decisions taken related to the strategy to follow as well as the allocation of resources among the various business divisions. However,

as said before, the ERM purpose is to give reasonable certainty of achieving the strategic objectives. It is therefore necessary to quantify such reasonability. The tolerable risk threshold is to be established according to the activity performed by the organization that implements it and according to a wide set of other variables. Such confidence threshold establishes the acceptable deviation levels compared to the objective achievement, it is called Risk Tolerance and is measurable with the same unit of measure chosen for other objectives.

Risk Assessment

The risk analysis process begins with the identification of risk events that could impact the achievement of company objectives. Each of them identifies risks is subject to two assessments: Before and after the mitigation actions put in place by the management. The first assessment defines the inherent (or intrinsic) risk that is the maximum possible risk level, without any applied mitigation action. The second assessment defines the residual risk that is the part of risk remaining to the company after having put in place the existing control activities on the inherent risk. Mitigating actions are all the activities put in place to reduce the likelihood of risk event and/or linked impact. Risk assessment regards two aspects:

- impact;
- likelihood.

The identification of the risk impact consists in defining the type of potential loss and measuring the size of the risk event. Considering that each risk is related to a specific objective and that this is qualitative as well as quantitatively measurable, risks may be quantified by using the same measurement of the reference objectives. Typically, the criteria for the risk impact assessment are:

- Economic: The risk effect in terms of lower profit and higher costs is assessed. Such criterion is applicable to all those risks having a quantifiable effect on the income statement of the Company and they require the definition of specific thresholds based on a reference parameter (Costs, Revenues, Margin);
- Market: Possible loss of market shares as a consequence of risks related to inability to fulfill customer needs in terms of product/service quality;
- Reputational: Based on the occurrence of possible events that could damage the Company image;
- Competitive advantage: It measures the loss of competitive advantage acquired by a Company in case of occurrence of risk events.

The likelihood of risk occurrence is the possibility that an identified event/risk occurs in a given period of time. This aspect remains one of the most complex and controversial in the risk analysis process. Without precise quantitative information that may derive from the analysis of similar previous experiences or from the specific analysis of relevant phenomena, it is possible to identify the occurrence likelihood based on the staff sensitivity and experiences in their competence function scope. It is also possible to establish and create a risk matrix, similar to the one showed by Figure 8.1, that is a brief representation of the positioning related to single risks compared to the company risk appetite and risk tolerance, enabling the management to identify action priorities and possible risk response strategies.

Risk assessment, given by the multiplication of occurrence likelihood and impact, generates three risk levels:

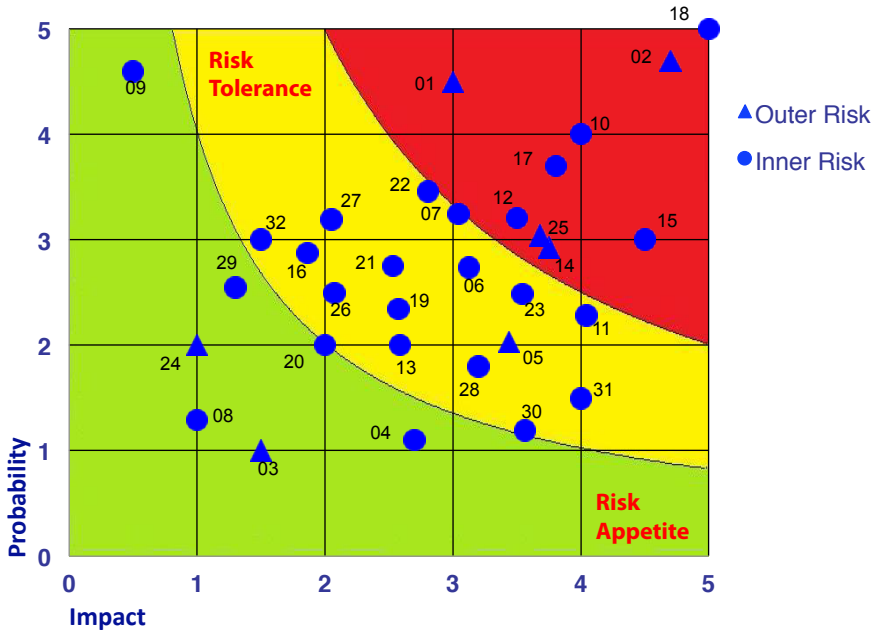

Figure 8.1: Example of Company Risk Matrix

- Low Risk – Irrelevant: The risk remains within the company risk appetite and, as a consequence, neither control measures nor further mitigation strategies are needed.
- Medium Risk – Monitoring: Risk overcomes risk appetite but remains within the risk tolerance. This kind of risk is usually steadily monitored/managed by the organization.
- High Risk – Avoid/Reduce: Risk overcomes both risk appetite and risk tolerance levels. It requires higher care by the management, which has to decide which treatment strategies have to be implemented: Risk reduction/mitigation, risk transfer or risk source elimination.

Risk response

The company management, once understood the residual risks, establishes how to align them to the target risk appetite level through a risk treatment plan. Possible answers to risk may be classified according to the following categories:

- Risk avoidance: It was not possible to find a valid option that reduces risk impact and likelihood to an acceptable degree, therefore the source of risk is eliminated;
- Risk reduction: Actions to reduce risk likelihood or impact or both are taken at a level in line with target risk tolerance. In other words, further risk mitigation action are implemented;
- Risk sharing/insurance: Risk likelihood and impact are reduced by transferring or sharing part of the risk (e.g. insurance policy, coverage measures against price or currency fluctuation risks, outsourcing);
- Risk acceptance: No action has been taken to affect the risk likelihood and impact, as the risk is already within the tolerance range.

Monitoring over time and risk prevention: i Key Risk Indicator

Once impact and likelihood values are defined and considering that a risk is made up of many steadily evolving factors, an effective ERM process requires a steady monitoring of these factors in order to ensure that relative risks are kept under control. In this context it is crucial to identify the most appropriate metrics, indicators in the description of concurrent factors of a given risk and to define how they affect the impact and likelihood values. In this case, these indicators are generally defined as Key Risk Indicators. The identification and use of accurate Key Risk Indicators (KRI) plays a crucial from a strategic point of view, as they improve the risk management process, facilitate the identification of vulnerabilities and improve the risk monitoring process. In order for risk indicators to be considered effective, they need to be repeatable and significant to such an extent as to create a risk development database, useful to compare the efficiency of taken countermeasures and investment return (in terms of avoided losses). The KRI are statistics and measurements able to offer a perspective regarding the company positioning respect to the risk, they use to be regularly reviewed in order to ensure the correct and heterogeneous risk assessment and they inform about the changes that can imply an increase or the occurrence of a risk.

8.2 The advantages of the ERM process implementation

The inadequacy of the traditional risk management forms has been understood also by the regulatory authorities, which, during the last decade, have gradually implemented stricter and stricter bonds in matter of company risk management and awareness. The same risk understanding underwent a significant change: Initially it was just attributed to negative situations, now it is considered as a company success factor, if the company is able to draw its intrinsic value. Risk is therefore not just a burden to be born, but, if duly managed, it can become a crucial success factor and provide a competitive advantage able to guarantee the company activity development and protection. The implementation of an ERM company system implies a set of indirect not negligible advantages. In effect, considering that the balance between assumed risks and company net asset solidity is an essential requirement for the business continuity and that company capital and debt level directly impact such balance, a better company risk management makes possible to reduce the likelihood of incurring in difficult financial situations by positively influencing the company value. Furthermore, credit institutes consider as positive the presence of an ERM system in the company context, as it provides a reasonable certainty that the company will maintain its economic balance unchanged. Such approval by the financiers may considerably reduce the cost of capital raising by the company and therefore it may positively impact its profit and loss. In the actual economic scenario, the definition and implementation of a company risk management system becomes a driving factor for the company improvement and growth as well as a crucial competitiveness factor.

9. Cyber risk policies

As said before, the cyber risk topic represents nowadays a critical aspect in the risk analysis and mitigation process that a company has to face in the framework of its business management. In effects, widespread technology and business models, more and more based on networks, on sensitive information exchange/possession and virtual space sharing (social media, cloud computing, etc.) certainly offers new possibilities, but has to imply also a higher attention of the companies to the risks deriving from these changes.

Cyber risks can indeed imply huge economic damages, mainly due to:

- Theft/corruption of sensitive and/or third party data;
- Asset damage deriving from activity interruption (e. g. operation stop and/or online transactions);
- Asset damage deriving from financial frauds;
- Material damage to the company asset;
- Material damage to customers (in particular in the healthcare sector);
- Damage to the image.

The need for an integrated risk management process and the insurance role.
To address these threats, Companies have to arrange an integrated Risk Management process that includes the Cyber framework. This approach ensures the most effective method for an IT risk impact prevention/mitigation, thanks to the development of an appropriate awareness, while optimizing the process of transferring the risk to the insurance market. The insurance coverage of such risks is indeed the last step of a structured process that starts with the analysis of the specific company situation: From the type of business to the type of implemented activity, up to the IT infrastructure characteristics. As an example, some critical aspects to be taken into account are listed below:

- Reference market;

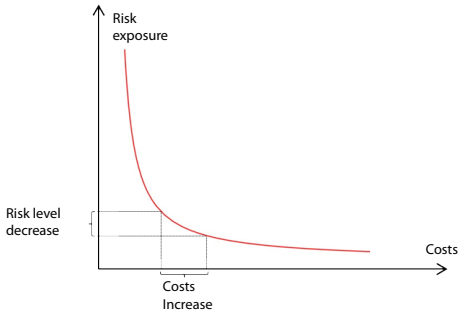

Figure 9.1: Each new reduction of exposure to the cyber risk requires increasing costs.

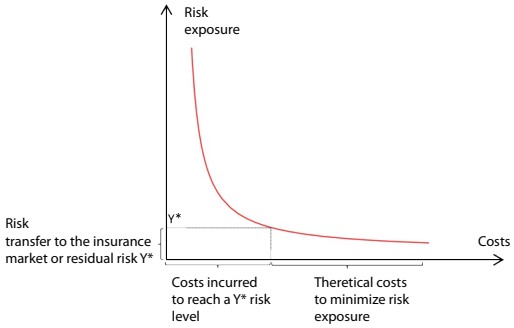

Figure 9.2: The company establishes a threshold, beyond which residual risk is to be transferred to the insurance market.

- Geographic context of business;
- IT infrastructure peculiarities (server room location, value of IT resources, intra/extra net networks, etc.);
- Type of processed data/information;
- Online based services and channels;
- Access possibilities (physical/virtual), even remotely, to company systems/networks;
- cyber security policies and implemented prevention/protection measures.

In effects, it should be noted that Cyber Insurance has to serve as a toll to protect the company balance, by covering the so called “catastrophic risks”, also based on the company risk appetite and risk tolerance. Furthermore, it should be noted that incremental benefits deriving from further prevention/protection actions gradually diminish beyond a certain threshold, therefore, the cost required to further increase security levels would be unbearable compared to its benefits. The company should therefore establish which is the most appropriate threshold of transfer ring the residual risk to the insurance market and, at the same time, evaluate the best trade-off between the insurance coverage price and level of exposure to residual risk (see Figures 9.1 and 9.2).

Insurance market and indemnity methodologies.
The insurance market of cyber risk policies is rapidly evolving and offers the possibility to create ad hoc customer protection. Such customization offers a very good level of matching the real cyber risk to which the company is exposed, of course it implies a previous analysis and evaluation process, as described above. However, it should be noted that, even if rapidly evolving, the Italian insurance market is still at an early stage. This is because, as usual in this kind of market, the reaction to a risk takes place when such risk becomes known and measurable. This new situation regards just the Italian market as, in the countries of North America and in the UK, the issues related to cyber risks have been addressed during the last decade. However, this implies the fact that the contract structure of most coverage policies follows the indemnity approach for privacy data violation, which is such a beloved topic in English-speaking countries. Out of 50 insurance companies in Europe, which declare to be specifically ready to undersign cyber risk policies, only one third is Italian, the rest works mainly in the United Kingdom (and covers Italian risks).

The insurer market is characterized by two approaches:

1. First Party Damages: the damage suffered by the company affected by a cyber event;
2. Third Party Damages: That is the insured company responsibility of violation of third party data that the insured company owns.

These two approaches imply two different indemnity methods: In the first case, in facts, the insurer indemnifies the costs needed to address the emergency crisis, meant as costs borne by specialized IT companies for IT security, lost, encrypted or destroyed data recovery, legal costs for investigation by control authorities, profit loss linked to insured company activity interruption and, furthermore, in case, IT fraud suffered by the company and damage caused to third parties.

The second approach, instead, is symmetrical and basically indemnifies damage claim of third parties because of the violation of third party data owned by the company, by adding the further costs for data recovery, damage to the insured company image, legal costs to address a damage claim or investigation, in case of effective loss of third party data outflow. In this case, it will not be indemnified, except for the profit loss suffered by the insured company, according to the relevant agreement.

The difference between the two indemnity approaches finds confirmation in two different coverage activation stages; in the first party method case, the factor that triggers the coverage is the insured company damage detection, whether it is about a tangible, intangible or asset damage. In the second case, instead, coverage is triggered by the damage indemnity claim by third parties as a consequence of the violation of third party data held by the insured company, for which the insured entity is responsible.

9.1 Risk perception and spread of cyber policies

The Ponemon report 2015 on cyber risk pointed out how risk transfer to the insurance market is extremely widespread, although the degree of awareness of tangible damage to assets and intangible damage to intangible assets (data) remains the same. The survey shows that the perceived value of tangible as well as intangible assets is relatively similar with just a 3% difference. On average, the total value of tangible assets reported by the survey is of 872 millions USD, compared to 845 millions USD of intangible assets. By estimating the loss or destruction average value of all intangible assets (or maximum likely loss, PML), the result was similar (638 millions USD for intangible assets, against 615 millions USD for tangible assets). On the contrary, both the impact of business interruption linked to intangible assets and the

likelihood of data or intangible asset violation are considered as significantly higher compared to the same event affecting tangible assets. The estimated impact of business interruption linked to intangible assets is of 168 millions USD, 63% higher than 103 millions USD in case of tangible assets; while the likelihood of facing a loss is of 4.7% compared to 1.5% for tangible assets (for damages of no more than 50% of the PML within the next 12 months).

Despite this increasing cyber risk awareness, there is wide insurance gap. If we compare tangible and intangible assets, EMEA Business Leaders say that intangible assets are more exposed by 38% compared to tangible assets in terms of insurance coverage. About half of potential losses (49%) of tangible assets is covered by the insurance company, while this value is of 11% for intangible assets. On the contrary, as far as intangible assets are concerned, self-insurance – considered as the risk retention within the specific balance post related to insurance policy purchase - is much more widespread. In general, it is observed that damage to data is considered more dangerous for the reputation compared to a tangible damage to assets. This implies that, in absence of notification duty provided by the law, companies are less inclined to declare to have suffered data loss instead of declaring to have suffered damage to tangible assets. Talking about legal obligations, nowadays only three company categories are obliged to notify data violations: Telecommunication companies and internet providers, banks, healthcare companies. Furthermore, according to the provisions of the Decree of the 2nd of July 2015, government agencies are obliged to notify personal data breaches to the Authority. As far as telecommunication companies concerns, the Authority for the Protection of Personal Data has provided also a procedure to notify the Authority and customers about data breaches. For the other two categories, today there is no regulated customer notification procedure concerning banks, while a notification duty is provided for patients, but just towards the Authority, as far as healthcare companies is concerned.

Insurance market capacity and risk assessment need

We should add that, while the theoretical market capacity for each single company is of about 200.000.000 Euros, if we want to restrict the coverage to first party particular cases, the limit decreases drastically to a range of 25-80 millions Euros. This limit undoubtedly favors risk selection by the insurer. Furthermore, the already pointed out regulation implies that there is no standard that insurers should anyway comply with, so that risk anti-selection phenomenon is exacerbated. The complex capacity, apparently limited may look like a limit for Companies, especially for the bigger ones. Indeed, all insured entities are trying to develop coverage against cyber risks. The very fact that insurers are still assessing the extent of this industry may represent an opportunity for Companies that want to protect themselves. Almost all insurance companies are taking measures in their organization in order to offer also, as insurance plan collateral guarantees, coverage for their intellectual property (trade mark breach, etc.) and against reputational damage, even with sublimities of policy main maximum coverage and only upon external IT breach, or fraudulent internal one. Once the distinction between the various operation sectors and therefore between the main risk factors is clear, it is important – in order to plan an insurance coverage – to carry out an assessment process able to evaluate and value the most significant financial risks. The final benefit that companies can draw from this kind of coverage – designed according to an accurate risk evaluation – basically consists in the Enterprise financial balance protection, against a residual risk, which cannot be further reduced, if not through too high investments, as explained above.

9.2 Guidelines to a cyber risk insurance coverage implementation

For the purposes of implementing a cyber risk insurance coverage, the company should follow 4 steps:

1. Involvement of an Insurance Consultant: As anticipated, the cyber risk sector is not yet ripe nor has reference standards (in the insurance field). The risk peculiarity and sector immaturity make it essential to have knowledge of the market and the technical-commercial levers of insurance sector players. The involvement of one or more consultants specialized in risk transfer to the insurance market becomes crucial in order to transfer the necessary specifications to insurers. The direct consultation of insurance companies could lead them to supply products that do not match the insured needs.

2. Risk Assessment: In order to properly isolate the maximum likely damage and to correctly estimate risk exposure, it would be appropriate, before signing the Policy, to carry out a risk analysis and calculation. Very often, Companies – even of medium-big size – find it hard to quantify their exposure, above all direct damages, as the economic impact of an adverse IT event is hard to be forecasted. Even in this case, the support of an acknowledged consultant to the insurance market becomes very important. Risk assessment should furthermore enable to gather useful information to fill in an insurance questionnaire. A structured Risk Assessment is strongly recommended to Large Enterprises and Critical Infrastructures, besides all SMEs greatly depending on Systems and working in defined contexts (e.g. on-line trade, retail, healthcare, medium publishing industry, broker, IT service companies, etc.).

3. Filling in an insurance questionnaire: Insurance questionnaires are aimed at gathering basic information needed for a first risk assessment by insurers. Filling-in questionnaires results in the possibility to value the various indemnity limit hypothesis, on which the insurance contract is based, and to make the insured person aware of his/her strengths and weaknesses. It should be pointed out that the questionnaire gathers standardized information (availability of certifications, standard protections, subjects having access to company system, contracts between insured entity and third parties) and therefore the in-depth analysis level is not so high. However, questionnaires imply the benefit for the insured entity to allow the insurer to provide a premium range that may be improved by following the negotiation; as far as the insurer is concerned, the questionnaire (even without any assessment) provides the certainty of some crucial data, as it is undersigned by the company requesting insurance coverage.

4. Insurance Coverage implementation: Once the assessment process through questionnaires and/or structured risk assessment is complete, it will be possible to request a formal quotation to the insurance market. Also in this case, the contribution of a specialized Consultant to the negotiation is at least recommendable, as the sector knowledge and negotiation capacity of the ones who constantly work in this field enable to reach higher performing results compared to the ones that can be achieved by single Customers directly with insurers, or by a non specialized Consultant with the insurers.

10. Privacy aspects linked to the Framework

This Chapter presents some aspects related to privacy, classified documents and State secret, to be taken into account when the Framework is implemented. It is mainly based on the provisions of the Privacy Code and to a lower extent on the Decree of the President of the Council of Ministries of the 6th of November 2015, which contains the "Regulation on digital signature of classified documents" (Decree no. 4/2015) and the "Provisions about the administrative protection of State secret and classified and exclusively divulgated information" (Decree no. 5/2015). However, within the following Framework reviews, this Chapter will have to take account of some European provisions undergoing the approval process. the general Regulation on data protection[1] and the Directive on data protection in the sector of tackling activities[2], which imply changes to the Privacy Code and are planned to enter into force in spring 2018, as well as the NIS directive (Network and Information Security) which enters into force in spring 2016[3].

10.1 The Privacy Code

The National Framework is implemented in compliance with the Italian regulations and, in particular, with the provisions of the Privacy Code (hereinafter called the"Code"). In this sense, Subcategory "ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations are understood and managed" provides that all regulations in force in terms of cyber security and personal data protection are identified and analyzed according to type of business of an organization and nature of processed date. Generally, the Code identifies as responsible of data processing: "the natural person, legal person, government agency or any other body, association or body, even jointly with another responsible, who is in charge of taking decisions according to purposes, personal data processing modalities and used tools, including security profile" (art. 4). These subjects have to comply with following

[1] http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52012PC0011&from=EN
[2] http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%205833%202012%20INIT
[3] http://data.consilium.europa.eu/doc/document/ST-15229-2015-REV-2/en/pdf

obligations:

- security (articles 31-34);
- communication (articles 19-22, 25-27, 32, 32-bis e 39).

Below, such obligations and the relationship with the Framework Subcategories that they imply for the identified subjects are described:

Security and communication obligations

Security obligations related to processed personal data, are provided by article 31 of the Code, according to which data have to be "supervised and controlled [...] so to minimize the risk of data loss or destruction, even if accidental, of unauthorized access or processing of data, or not in compliance with information collection purposes, through appropriate and preventive security measures". Some of these obligations are explained by article 34 and in the technical reference attachment B as minimum security measures (intended as "the set of technical, IT, organizational, logistic and security procedural measures that set up the minimum required protection in case of data destruction or loss risks, even accidental, of unauthorized data access or processing or not in compliance with their collection purposes"). These measures include:

a) IT authentication;

b) Implementation of procedures to manage authentication credentials;

c) Use of authorization system;

d) Regular update (at least once a year) of identification of authorized processing scope allowed to single persons in charge of managing and maintaining electronic tools;

e) protection of electronic tools and data against illicit data processing, unauthorized access and given IT programs (electronic tools to be updated at least every 6 months; at least an annual update of programs to prevent electronic system vulnerabilities);

f) Implementation of procedures to store security copies (at least weekly data savings), recovery of data and system availability (within 7 days);

g) Implementing procedures for removable support media management and use;

h) Use of encoding techniques or identification codes for data processing able to reveal health status or sexual habits by healthcare bodies.

These provisions make the five Framework Subcategories be considered as mandatory for those organizations that process personal data through electronic tools. These Subcategories are:

- PR.DS-1: Data-at-rest is protected;
- PR.IP-9: Response plans are active and managed (Incident Response e Business Continuity) as well as recovery plans (Incident Recovery e Disaster Recovery) in case of incident/disaster;
- PR.PT-2: Removable storage supports are protected and their use is limited according to policies;
- PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality;

- PR.AC-2: Physical access to assets is managed and protected.

The performance of the above minimum measures does not diminish in any case the relevance of general security duties to be fulfilled by personal data processing holders pursuant to article 31 of the Code. These are indeed responsible in judicial proceedings (pursuant to article 2050 of the Italian Civil Code in matters of responsibilities in performing dangerous activities) in case of possible damage caused by breaching the above mentioned article 31 and in order to avoid compensation, they are obliged to comply with security duties pursuant to the principle of reversal of the burden of proof.
Communication duties vary according to processing holder and type of processed personal data. More in detail:

- for public bodies (excluding economic public bodies) and for non sensitive and judicial data (articles 19 e 39):
  - communication by a government body or other public bodies is allowed if provided by the law or by a regulation. In case of lack of such regulation, the communication is allowed in any form if it is anyway required in order to exercise institutional functions, upon communication to the Guarantor. The consequent data processing may start after a term of 45 days after the communication has been sent to the Guarantor (unless otherwise provided, even afterwards);
  - the communication by the public body to privates or economic government bodies and the divulgation by a government subject are allowed uniquely if provided by the law or regulations.
- for public subjects (excluding economic public bodies) and for sensitive and judicial data (articles 20-22):
  - processing of sensitive and judicial data by government subjects is allowed only if authorized according to express law provision or Guarantor regulation;
  - sensitive and judicial data contained on lists, registers or databases, stored through electronic tools, are processed with encoding techniques or through the use of identifying codes or other solutions that, considering the number and nature of processed data, make them temporarily unintelligible even to the those who have authorized access to them and allow to identify the affected subjects only if required;
  - data revealing health status may not be divulgated. In any case, the divulgation of sensitive and judicial data is allowed only if expressly provided by the law.
- for private entities and economic government bodies (articles 25-27):
  - without prejudice of required data communication and divulgation, in compliance with the law, the judicial authority, information and security bodies and other public entities, for State defense and security purposes or for the prevention, investigation or repression of crimes;
  - sensitive data can be processed with or without written consent of the affected person and upon the Guarantor's authorization. Data revealing health status may not be divulgated;
  - judicial data processing by privates and economic government bodies is allowed only if expressly provided by the law or any Guarantor's regulation specifying the relevant processing purposes, the kind of processed data and possible allowed operations.

- for electronic communication services, upon suffered breach (art. 32-bis):
  - in case of personal data breach, the supplier of publicly accessible electronic communication services notifies the breach to the Guarantor without undue delay. If the personal data breach risks to cause prejudice to personal data or the contractor's or any other party's confidentiality, the supplier shall notify the breach to them without any delay;
  - communication is not due if the supplier proved to the Guarantor to have implemented the protection technical measures that make data unintelligible to any unauthorized person and that such measures have been implemented also for the data affected by breach.

This implies that in the proposed Framework, Subcategories related to communications have to be considered as high priority for the above mentioned subject category and type of processed data, independently from what is indicated in the contextualization that such subjects have taken as reference. Concerned practices are:

- DE.DP-4: Event detection information is communicated to appropriate parties;
- RC.CO-1: After an incident, public relations are managed;
- RS.CO-2: Criteria for incidents/events documentation are established;
- RS.CO-3: Information is shared consistent with response plans;
- RS.CO-4: Coordination with stakeholders occurs consistent with response plans;
- RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.

Employees Monitoring

Before the reform introduced by the "Jobs Act", article 4, clause 1 of the Workers Statute set forth the prohibition of using "audiovisual devices and other equipment for the remote control of the employees' activity". The reforming Legislative Decree no. 151/2015 modified such provision in line with the Guarantor's decisions in this regard, by establishing that "audiovisual devices and other tools enabling remote control of the employees' activity may be used exclusively for organizational and production purposes, for the work safety or the company asset protection and may be installed upon collective agreement signed by the unitary union representatives or company union representatives". These provisions have to be taken into account in implementing the Subcategory

- DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.

10.2 Classified information and State secret

The Decree of the President of the Council of Ministries of the 6th of November 2015, including the "Regulation on digital signature of classified documents" (Decree no. 4/2015) and the "Provisions about the administrative protection of State secret and classified and exclusively divulgated information" (Decree no. 5/2015), introduces new elements to protect such documents, considering cyber risks and in relation to the personal data protection needs. This results in the fact that the provisions contained in these acts have to be duly taken into account by all public and private entities that manage via computer issues covered by state secret as well as classified information, while implementing the following Subcategories;

- ID.GV-1: Organizational information security policy is established;
- ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed;
- PR.AC-1: Identities and credentials are managed for authorized devices and users;
- PR.AC-3: Remote access is managed;
- PR.DS-1: Data-at-rest is protected.

11. Sector Regulators

In this Chapter we discuss the positioning of some regulated sectors in respect to the Framework that is government agencies, the bank sector and companies listed on a stock exchange and how these sectors could implement the Framework to their advantage. The proposed sections are examples: Each regulated sector has its more or less mature regulation peculiarities in the cyber sector and therefore will have to get in position and implement the Framework in the most appropriate way.

11.1 Government agencies

Government agencies may be considered as strongly regulated organizations, as their activity takes place within the scope and limits of regulations having legal effect; however, the regulatory framework has paid too little attention to cyber security until now. The most relevant regulations in this regard are the ones provided by the Code of Digital Administration (CAD - DLgs. 7th March 2005 s.m.i.), which in article 17, clause 1, points out the need to concentrate in a single office the strategic coordination of IT and phone system development (letter A) and the orientation, planning, coordination and monitoring of IT security regarding data, systems and infrastructures (letter C). The following articles 50, 50 bis and 51 deal with the issues of data integrity and availability, by assigning to the AgID a primary role in re leasing technical regulation in the field of IT security, as well as IT security incident management. This role is strengthened by the National Strategic Framework for Cyberspace Security, whose tasks are explicitly defined by the Agency:

- It provides directions, technical rules and guidelines in matters of IT security,
- It ensures the technical quality and public IT system security and related interconnection net security in order to safeguard the IT assets of government agencies and guarantee the integrity, availability and confidentiality of services supplied to citizens,
- It manages the CERT-PA, CERT of government agencies, which ensures the IT system cyber security of government agencies as well their interconnection network security

through the coordination of security management structures ICT – ULS, SOC and CERT working within their scope.

It is therefore the Agency task to differentiate the Framework so to specialize it for the Italian government agencies, taking into account the fact that they have substantially different characteristics, structure and objectives compared to the company ones, in which the damage, and therefore the risk, is easily quantifiable. Often, their status and the nature of services supplied to citizens is similar to the ones of Critical Infrastructures, not least because of the fact that services supplied by the private sector depend on the government authoritative ones. In any case, the Framework represents an extremely useful chance also for government agencies that can use it to various purposes:

- Awareness: Raising one's own awareness in matters of cyber security through a self-evaluation and the creation of one's own profile. In facts, the Framework, regardless of the organization nature and size, allows to identify high priority security practices that at present are not directly considered. This contributes to fill the gaps showed by the government agencies showed (see Cyber Security Report 2013[5] and 2014[6]) and allows to identify high impact action on the cyber risk management of government agencies.
- Target profile: According to various factors, the definition of the process to increase one's own security rarely represents an easy to solve issue. Identifying the practices to carry out to reach the target status, without any guidance, could imply a waste of energy and financial resources. The definition of a target profile that identifies security practices that the government agency would like to achieve, compared with the current profile, represent a useful tool in order to define a security roadmap for government agencies.
- Supply chain: Increasing the security of the entire supply chain of services for government agencies. Government agencies may require their service providers to have a minimum profile: A set of security practices required for particularly critical data processing, or in order to interact with the government systems and so on. The government agency may define specific profiles for single services and attach such profile to tender notices for the supplier selection.

The Framework is part of the process initiated by the Agency to adjust the organization, awareness and robustness level of government agencies regarding cyber risk. The "Technical rules in matters of data, system and infrastructure security of government agencies", drawn up by the Agency and soon to be released, give expression to the CAD provisions by assigning to government agencies the obligation of implementing an appropriate Information Security Management System (SGSI, corresponding to the Italian ISMS), based on a precise assignment of roles and responsibilities. If the Technical Rules are mainly focussed on the organization, from an operative point of view, they are based on the Guidelines on ICT Security in government agencies. In this regard a security control system has been made available and is derived from the SANS 20, in which these are qualified according to priority, impact and cost. This way the minimum set of measures to be implemented is identified and may be compared to the "High Priority" system provided by art. 5.1 and representing minimum security measures for all government agencies. The implementation of further controls is here presented as a tool to achieve higher security levels, but, in the Framework perspective, it corresponds to increasing maturity levels. The Framework implementation should follow a terminology alignment, with the harmonization of the control identification system and a wider structure f the implementation guide that take into account the government agency size, its organizational complexity, type of processed data, also according to the privacy regulation, without overlooking the level of exposure to cyber risk that depends also on political and environmental factors.

11.2 Bank and financial sector

In recent years, the main Italian banks and financial brokers have defined and initiated cyber security programs aimed at arranging government measures, security management and control in order to prevent, reduce and react to the IT security threats the company IT assets are exposed to. Among various factors that result in a complex situation of higher maturity in the cyber risk approach there are:

- The substantial change observed in the way bank services are offered and supplied. The implementation of a multichannel approach to interact with existing or potential customers, beside the increasing digitalization of operative processes, implied the implementation of IT security controls and the protection of data and transactions processed by financial and credit brokers, together with privacy protection.

- An evolved culture and sensitivity of risk within the institutes. In effect, for long these institutes have arranged approaches, systems and tools for risk assessment, among which also operative and reputational ones, which facilitated the introduction of cyber risk management systems.

- The duty to comply with regulations and specific sector provisions released at national and international level in matters of information security, IT systems and operation continuity. Compliance programs initiated by institutes, besides including the implementation of required measures, gave the chance, in general, of a comprehensive review of one's own IT management and governance structures and for the implementation of best practices and security controls within company processes.

- Resilience of financial services is a strategic aspect directly impacting on the core business of banks that always paid great attention to operation continuity and ICT security.

National initiatives

A central role is played by the Bank of Italy, responsible for the release of cross-regulations applicable to the entire financial sector. In facts, only recently the provisions of relevant prudential supervision for the IT risk management, IT security governance and bank operation continuity entered into force (see Circ. 285 of the 17th December 2013, 11th update, Tit. IV). Specifically, a new chapter dedicated to the Information System (Chapter 4) has been added, while the chapters that rules internal controls and operation continuity protection measures (respectively Chapter 3 and 5) have been updated.

The particular new aspect is exactly the relevance attributed to the IT risk assessment, integrated in the comprehensive company risk management process (RAF Risk Assessment Framework), in order to enable supervision and management bodies to benefit from a comprehensive vision of the company risk profile. The regulation entered into force in February 2015 in order to allow to the brokers to adjust IT systems to the regulatory provisions. To this purpose, in July 2013, the issue of the regulation came with the requirement for companies to perform a self-assessment in order to identify possible deficits (gap Analysis) and to define an action plan to achieve full compliance with the regulation within the following 18 months. The same Regulation leads broker to consider, among others: "the IT security policy; the measures taken to ensure data security and access control, including the ones aimed at the security of telecommunication services for customers; the management of changes and security incidents; the availability of information and ICT services". Furthermore, starting from February 2015, brokers are also obliged to promptly notify relevant security incidents to the Bank of Italy. In 2003, the Bank of Italy ha established CODISE, a facility in charge of coordinating the

operative crisis of the Italian financial market. It is lead by the Bank of Italy and the CONSOB and systemically relevant operators of the financial sector take part of it. The CODISE, which operates in agreement with similar structures at International level, organizes and take part to a test and to national and European simulations. As periodic discussion meeting among the participants, it favors the analysis of the development of threats to the system operative continuity and the analysis of prevention and risk control methods, including cyber security.

European initiatives

During 2015, the ECB (European Central Bank, which in November 2014 assumed the responsibility of direct supervision on the most significant EU bank brokers) has initiated a program to assess cyber security of supervised European institutes, including the Italian ones[1]. The "Orientations in matters of online payment security", implemented by the European Bank Authority (ABE) on the 18th of December 2014, in course of implementation, which specify the security measures required to all suppliers of services against payment, specifically with regard to electronic services against payment supplied online.

Global initiatives

The Committee on Payments and Market Infrastructures (CPMI) and the International Organisation of Securities Commissions (IOSCO) have submitted to public consultation a guide [2] to improve the resilience of Financial Market Infrastructures (FMI)[2] in case of cyber threats. The guide, addressed to FMI and their overseer:

- It does not provide further requirements respect to the Principles for financial market infrastructures (PFMI) of 2012 and is aimed at supporting some critical objectives for the financial stability, in particular the rapid FMI recovery;
- Defines principles and not rules, also to avoid the fact that its recommendations become rapidly dated and it does not dictate rigidity in terms of implementation of the same principles.
- It highlights the importance of robust ICT controls, but does not go in detail in order to allow flexibility to operators, also given the numerous existing standards of the market.
- It uses a legible and understandable language for the FMI top management, considering the fundamental role that the company top management has in strengthening cyber resilience;
- It is divided in chapters that identify five main categories to manage risks (1.Governance; 2.Identification; 3.Protection; 4.Detection; 5 Response and Recovery) and three cross-components (1.Testing; 2.Situational Awareness; 3.Learning and Evolving);
- defines the concept of "cyber governance" putting it at the core of the efforts to improve the FMI cyber resilience. Cyber governance mechanisms must ensure that cyber risks are properly taken into account at all levels within the FMI and that appropriate resources and competences are allocated to manage such risks. The guide encourages the involvement of the company top management to create a company philosophy in which the staff, at all levels, is aware of its role and responsibility in matters of cyber resilience;

[1] The Bank of Italy has extended such charge to 12 Italian banks of medium size ("High priority banks").

[2] The FMI are payment systems of systemic relevance, systems to settle securities, the main counterparts, central depositaries, trade repositories. For a wider definition see `http://www.bis.org/cpmi/publ/d101a.pdf`

- It points out the fact that an efficient mitigation of cyber risks requires an identification and prioritization of critical processes, as well as understanding the threats, no just generically but specifically for each single FMI. The guide encourages the FMI to have a clear and correct perception – in real time – of what happened, of what is happening and will happen in the near future (situational awareness), also through the participation to information sharing initiatives;

- It invites the FMI to implement processes - not just of technology kind - in line with the best international practices. In particular, the FMI must have advanced capacities to monitor, promptly detect and reduce the impacts of cyber attacks;

- It invites the FMI to get prepared to extreme but plausible cyber threats and orientates FMI towards actions needed to create a recovery capacity within two hours from each destructive event (consistently with principle 17 of the PFMI). Even realizing how difficult it is to achieve this goal, the guide points out that there are technical and organizational options that may support the achievement of such objective.

- It point out that market resilience depends on the entire FMI environment and therefore that a collective effort is needed to ensure financial stability, which excludes the performance of trainings.

- It highlights that cyber resilience requires a steady adjustment and improvement.

11.3 Listed companies on regulated markets

The Self-discipline Code, in line with the experience on the main International markets, defines the best practice in matters of company governance recommended to the Committee for the Corporate Governance of Listed Companies. Among the articles of the Self-discipline code, art. 7 provides the Principles, Implementation Criteria and Comments on the internal control and risk management System (SCIGR). The Code assigns a central role to the "identification, measurement, management and monitoring of the main risks" to contribute to a company management that is consistent with the goals and aware decision-taking in a context in which also cyber risk are becoming more and more relevant. The same renaming from "internal control system" to "internal control and risk management system" ("SCIGR") and from "committee for internal control" in "control and risk committee" confirm the specific attention paid by the ones who extended the Code to such topics. The above mentioned choices seem to be the result of the fact that the authors of the Self-discipline Code have realized that "the modern understanding of controls focus on the notions of company risks, their identification, assessment and monitoring". It is also for this reason that the "regulation and the Code refer to the internal control and risk management system as a harmonized system, of which the risk represents only the underlying principle". Art. 7 of the Self-discipline code provides also a clear definition of SCIGR, in line with the provisions of the CoSO ERM Integrated Framework, that is "the set of rules, procedures and organization structures aimed at enabling the identification, measurement, management and monitoring of the main risks". In case of reference to the experience of other countries, the SEC (US-Security Exchange Commission) has issued guidelines on cyber security for listed companies that affect also primary Italian groups. Companies are required to consider cyber risk and take account of all relevant available information, among which previous incidents, their seriousness degree and frequency. Furthermore, incident likelihood is to be assessed and the quantitative and qualitative scope of such risk is to be evaluated, including potential costs and other consequences deriving from the misappropriation of sensitive goods and information, data

corruption or operation interruption. Among specific factors mentioned by the SEC to be taken into account in cyber risk assessment, there are:

- Suitability of preventive actions taken to reduce cyber risk within the company context and the company activity sector;
- Attack vulnerability and threats that the company knows about, suffered incident and, in case of single events or more relevant and substantial events;
- Aspects of business operation giving rise to relevant cyber risks;
- Potential costs and consequences of such risks.

Going back to Italian requirements, Principle 7.P.3, consistently with the international Frameworks guidelines, identifies also the players involved in several respects in addressing, managing, assessing and monitoring the SCIGR, each according to their own competence. We refer, more precisely, to:

- The Board of Directors, both collectively in its role of guiding and defining the system guidelines, and through the identification of representatives (the manager in charge of the internal and risk management control system) and of its internal committees (control and risk committees);
- the management;
- Company functions of first and second level with management tasks of SCIGR;
- the internal audit function as third level security line;
- The Statutory Board of Auditors as control body.

The central sole is undoubtedly assigned to the Board of Directors that, among others, "defines the guidelines of the internal control and risk management system, in a way that the main risks related to the issuer and its holdings are correctly identifies, as well as adequately measured, managed and monitored" and cyber risks have to be considered within such scope. The Board of Directors is also responsible, pursuant to the implementation criterion 1.C.1, of defining "risk nature and level compatible with the strategic objectives of the issuer". It is easily recognizable in this provision the reference to the risk appetite concept (that is the comprehensive risk level that the issuer is ready to take in order to reach its objectives), in line with the approach suggested by the Framework in assessing cyber risks. Notwithstanding the above, in general it seems that: "a control system, in order to be effective, has to be "integrated": this presumes that components are coordinated and interdependent among them and that the system, comprehensively, is in turn integrate in the general company organization, management and accountability structure" (see Comment to art. 7). Furthermore, the already mentioned Principle 7.P.3 recommends to issuers the identification of coordination procedures among the various involved players in the SCIGR: "in order to maximize the internal control and risk management system efficiency and to reduce the activity duplication". In particular, the Board of Directors plays its central role in defining the limits of admissible risk and of risk management guidelines, whose actual implementation is assigned to the entire organization structure, through:

- the definition of company strategic, financial and industrial plans, in order to ensure consistency of strategies and objectives defined with admissible risk levels, and to provide SCIGR guidelines related to acceptable risk levels (that can be reviewed according to the results of monitoring activities);

- assessment of the SCIGR suitability and effectiveness in respect to the enterprise and the Group characteristics and the accepted risk profile;
- the delegation system related to the assignment of powers to the management, which is given the accepted risk control by the Board of Directors.

In order for the Board of Directors to collect the required information to define expected objectives consistently with the sustainable risk levels, as well as to monitor their achievement and control and risk management system effectiveness, the information flows between SCIGR players should be essentially reliable, clear, complete and timely; they represent therefore the crucial element on which the entire risk oversight system is based. In view of all the above, it becomes clear that the National Framework for Cyber Security in the context of listed companies may provide elements supporting the Self-discipline Code, enabling ad appropriate cyber risk assessment and management.

Acknowledgements

The editors of this volume would like to thank the authors fro the time dedicated to this work. It was a great public-private team that worked in perfect harmony and synchrony. A special thank goes to the authors and organizations that participated in drawing up the text and chose not to be mentioned. Finally, the document has been submitted to public consultation, this fact contributed enormously to improve the text and contents thanks to specific comments and accurate amendments. Each of the approximately five hundreds received amendments and comments has been carefully assessed by a specific working group. Thanks to all the authors of such comments and amendments. Lastly, a special thank goes to the authors of comments and amendments accepted and therefore integrated in the text. Below are listed the name of those who accepted to be publicly acknowledged:

Romano Stasi (ABI Lab)

Liberato Pesticcio (Almaviva)

Panfilo Ventresca (Almaviva)

Alessandro Vinciarelli (Almaviva)

Giancarlo Butti (Banco Popolare)

Claudio Ciccotelli (CIS-Sapienza)

Federico Lombardi (CIS-Sapienza)

Mauro Alovisio (CSIG Ivrea Torino)

Riccardo Abeti (CSIG Ivrea-Torino, Unione Avvocati Europei)

Marco Baldassari (CSIG Ivrea-Torino)

Raoul Chiesa (CSIG Ivrea-Torino)

Selene Giupponi (CSIG Ivrea-Torino)

Giulio Cantù (Comitato AICQ)

Antonio Rassu (Comitato AICQ)

Valerio Teta (Comitato AICQ)

Francesco Di Maio (ENAV)

Maria Doris Di Marco (ENAV)

Wang Yujun (Huawei Technologies Italia SRL)

Pier Luigi Rotondo (IBM Italia S.p.A.)

Glauco Bertocchi (ISACA)

Alberto Piamonte (ISACA)

Petro Caruso (Palo Alto Networks)

Palma Ombretta (Poste Italiane)

Rocco Mammoliti (Poste Italiane)

Riccardo Roncon (RSA Assicurazioni)

Damiano Bolzoni (Security Matters)

Enrico Cambiaso (Università degli studi di Genova)

Sandro Bologna

Luigi Carrozzi

This work is part of the research activities financed within the framework of the Italian project MIUR TENACE.

The editors would like to thank the following organizations that supported the presentation event of 4th February 2016

Bibliography

[1] Maria Cristina Arcuri, Roberto Baldoni, Marina Brogi, Giuseppe Di Luna, Attacchi alle infrastrutture finanziarie attraverso armi cibernetiche. Franco Angeli Editore, 20 pages, ISBN: 9788820440145, 2013.

[2] Bank for International Settlement (BIS), Guidance on cyber resilience for financial market infrastructures - consultative paper, Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions, November 2015 http://www.bis.org/cpmi/publ/d138.htm

[3] Roberto Baldoni, Rocco De Nicola Editors, Il Futuro della Cyber Security in Italia, Consorzio Interuniversitario Nazionale Informatica, November 2015 https://www.consorzio-cini.it/labcs-home/libro-bianco

[4] Roberto Baldoni, Luisa Franchina, Luca Montanari. Verso una struttura nazionale di condivisione ed analisi delle informazioni. Franco Angeli Editore, 20 pages, ISBN 9788891706881, 2014.

[5] Roberto Baldoni, Luca Montanari Editors. 2013 Italian Cyber Security Report - Critical Infrastructure and Other Sensitive Sectors Readiness. Università degli Studi di Roma La Sapienza. 2014 ISBN 978-88-98533-13-8 http://www.dis.uniroma1.it/~cis/media/CIS%20Resources/2013CIS-Report.pdf

[6] Roberto Baldoni, Luca Montanari Editors. 2014 Italian Cyber Security Report - Awareness, Defense and Organization in the Public Sector. Università degli Studi di Roma La Sapienza. November 2015 http://www.cis.uniroma1.it/csr2014

[7] Roberto Baldoni, Gregory Chockler: Collaborative Financial Infrastructure Protection - Tools, Abstractions, and Middleware. Springer 2012 http://www.springer.com/us/book/9783642204197

[8] Borsa italiana - Codice di Autodisciplina, July 2015 http://www.borsaitaliana.it/borsaitaliana/regolamenti/corporategovernance/corporategovernance.htm

[9] Tim Casey, Kevin Fiftal, Kent Landfield, John Miller, Dennis Morgan, Brian Willis. The Cybersecurity Framework in Action: An Intel Use Case. Intel 2014 http://www.intel.com/content/www/us/en/government/cybersecurity-framework-in-action-use-case-brief.html

[10] ISO/IEC 27000:2014 Information technology – Security techniques – Information security management systems – Overview and vocabulary http://www.iso.org

[11] ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity http://www.iso.org

[12] Confindustria, Università Cà Foscari, Demos & Pi, Afferrare il futuro! Strategie di risk management per l'impresa di domani, 2011 http://www.giovanimprenditori.org/confindustria_afferrare_ilfuturo.pdf

[13] Stephen Coraggio, John Rogers, Nicholas Hilgeman NIST Cybersecurity Framework: Implementing the framework Profile. Booz-Allen-Hamilton, 2014 https://www.boozallen.com/insights/2015/07/nist-cybersecurity-framework

[14] COSO Enterprise Risk Management - Integrated Framework 2004 http://www.coso.org/

[15] Framework for Improving Critical Infrastructure Cybersecurity (Version 1.0) National Institute of Standards and Technology. 2014 http://www.nist.gov/cyberframework/

[16] Douglas Gray, et al. "Improving Federal Cybersecurity Governance Through Data-Driven Decision Making and Execution." TECHNICAL REPORT, CMU/SEI-2015-TR-0112015, September 2015 http://resources.sei.cmu.edu/asset_files/TechnicalReport/2015_005_001_444963.pdf

[17] Alexander Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn 2012

[18] Robert Mayer, Brian Allen (editors). Cybersecurity Risk Management and best practices:Final Report The Communications Security, Reliability and Interoperability (CSRIC) Council - Working Group 4, 2015 https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf

[19] Presidency of the Council of Ministries: Strategic Framework for cyberspace security http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/quadro-strategico-nazionale-cyber.pdf

[20] Presidency of the Council of Ministries: Strategic Framework for cyber protection and IT security http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/piano-nazionale-cyber.pdf.

[21] Presidency of the Council of Ministries: Decree of the 24th of January 2013 – Directive of indications for cyber protection and National IT security, 2013 http://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg

[22] Presidency of the Council of Ministries, Information system for the security of the Republic, Report about the Republic security policy, 3rd Part, pages 81-87, 2014, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2015/02/relazione-2014.pdf

[23] Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris, 2015

[24] David Patt. Cyber security is not just the IT department's problem. Financial Times. November 2015. http://www.ft.com/intl/cms/s/0/f6b50038-92a1-11e5-bd82-c1fb87bef7af.html?desktop=true#axzz3srZntwJX

[25] 2015 Cost of Cyber Crime: Global. Ponemon Institute, 2015 http://www.ponemon.org/

[26] Perry Pederson. A RIPE Implementation of the NIST Cyber Security Framework. Langner 2014 http://www.langner.com/en/wp-content/uploads/2014/10/A-RIPE-Implementation-of-the-NIST-CSF.pdf

[27] ENISA, A simplified approach to Risk Management for SMEs, ENISA Deliverable: Information Package for SMEs, febbraio 2007, https://www.enisa.europa.eu/publications/archive/RMForSMEs

[28] Shackelford, S. et al. Toward a Global Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices. Texas International Law Journal, 2015 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2446631