POLITECNICO DI TORINO

Master's Degree in Computer Engineering

**Master's Degree Thesis**

# NIS2: Solutions and Strategies for Modern Cyber Governance

**Academic Tutor**

Prof. Luca Ardito

**Candidate**

Marco Chessa

**Company Tutor**

Claudio De Santis

Academic Year 2024-2025

# Contents

# List of Figures

# Summary

The present thesis examines the implications of *Directive (EU) 2022/2555 (NIS2)* for organisations operating in critical and highly critical sectors and handling sensitive data. The analysis aims to demonstrate the importance of compliance with the law in promoting cybersecurity resilience and, concomitantly, to provide operational guidelines and strategies that may be useful in containing and mitigating the impact of threats. The study is grounded in professional experience garnered at *KPMG Advisory S.p.A.*, Turin, in the Cyber and Tech Risk department, where an experiment was conducted on the creation of a cybersecurity framework and its application in a business context.

The initial section of the thesis provides a concise and essential description of the interventions that have been implemented by the national and international political system to address increasingly severe cybersecurity risk situations. This is done in order to provide the reader with knowledge of the regulatory and historical processes that led to the promulgation of *Directive (EU) 2022/2555.* The analysis commences with the initial significant threats that characterised the early 2000s and concludes with a description of the most sophisticated attacks of the present era. Among the legislative components that have defined this historical framework, some of the most important regulations implemented are illustrated, those that can be considered milestones in the European and international panorama. The initial provision under scrutiny, the *Budapest Convention on cybercrime*, constitutes a pivotal element of the international regulatory framework as the inaugural treaty endeavouring to harmonise the various legislative instruments enacted to combat cybercrime. This was followed by numerous documents, including the *General Data Protection Regulation (GDPR, 2016)*, which defines European standards on privacy and security, and *Directive (EU) 2016/1148 (NIS 1)*, the first legislation aimed at improving the security of networks and information systems. Subsequent analysis has exposed significant deficiencies in the latter, thus prompting the formulation and promulgation of *Directive*

*(EU) 2022/2555 (NIS2).* The present thesis provides extensive illustration of the provisions and contents of *NIS2 Directive*, which, in comparison with the previous directive, introduces more stringent requirements and obligations, covering a greater number of sectors. The new Directive strengthens management responsibility by requiring companies to have governance structures and clear roles for managing IT risks. The Directive imposes stringent incident reporting requirements, mandating that organisations establish and refine procedures for reporting security incidents to facilitate a coordinated response with national authorities. It promotes new provisions for risk management throughout the supply chain, extending the obligation of compliance to suppliers and external partners. The Directive establishes novel and stringent sanctions for non-compliance, with financial penalties calculated on the basis of fixed amounts or percentages of the organisation's global turnover.

The second part of the research illustrates the practical application of the *NIS2 Directive* within a client company, which in the specific case under examination, operates in the agri-food sector. The document describes the verification process used to assess the organisation's IT security status and the procedures adopted to ensure compliance with the provisions of the *NIS2 Directive*. The evaluation process was divided into four phases:

1. Document collection – The first phase involved the collection of relevant documents to determine their regulatory compliance. To this end, a Provided By Client List (PBC List) was prepared, which covered key aspects such as security governance, risk management, supply chain security and operational resilience. Concurrently, interviews were conducted with company representatives to proceed with the integration and verification of the information collected.

2. Readiness Assessment – The second phase involved an assessment of the company's cybersecurity readiness in relation to the requirements of the NIS 2 Directive. A Readiness Assessment Framework was developed, structured in thematic areas and specific controls, in order to ascertain the level of compliance. Following the dissemination of the collected data to the client, it was analysed to identify any gaps and areas for improvement. This analysis was conducted using a Readiness Assessment Report, which contained a mapping of critical issues, indications regarding areas for development and recommendations for filling the gaps.

3. Policy Review – The third phase entailed an analysis of the company's IT

security policies to identify any inconsistencies with the NIS 2 Directive. To address the identified gaps, a new set of cybersecurity policies was developed, integrating industry best practices.

4. Security Measures Implementation – The fourth phase involved the implementation of security measures. Preliminary indications and digital information content were provided to the Client to increase his awareness of cyber risks. Furthermore, a support programme was outlined for the implementation of security measures, which included the definition of business continuity plans, the organisation of attack tests and simulations, and the technical assessment of company vulnerabilities.

The analysis was conducted in accordance with ENISA guidelines, the National Framework for Cybersecurity and ISO/IEC standards, in order to ensure a structured and internationally recognised approach. The results demonstrate that organisations should not perceive compliance with NIS2 as a mere regulatory obligation, but rather as a valuable opportunity to enhance their cybersecurity strategies, fortify operational continuity and mitigate risks in an increasingly hostile digital landscape.

To achieve concrete and effective results, organisations must align their policies with the Directive, invest in advanced risk management technologies, activate continuous monitoring of sensitive elements and train employees to transform the human factor from a potential risk factor to a strength in the management of corporate threats. Finally, to guarantee operational continuity, it is essential to develop long-term resilience strategies, implementing disaster recovery plans capable of limiting the impact of any cyber attacks.

The purpose of this study is to provide possible, concrete and useful support to companies that are, or will be, active in critical sectors and that face, or will face, threats to their security. The thesis proposes a framework for the implementation of the *NIS2 Directive*, integrating key existing regulations and accommodating future updates. In general, all the tools created and used during the internship and presented in this paper provide objective data that can be integrated with security automation strategies to facilitate practical and timely risk management. In addition to serving as a model of the operational strategies that can be adopted for risk prevention and management, this thesis aims to emphasise that the future of cybersecurity in Europe depends on a coordinated effort between governments, businesses and cybersecurity professionals, who can only create a secure and resilient digital environment by working together and complying with current regulations.

# Chapter 1

# Introduction

## 1.1 Company Description

The choice of topic for this paper is based on my professional experience at the Turin office of KPMG Advisory S.p.A.. KPMG is a global network of independent professional services firms providing tax, legal, audit and management consulting services to businesses. The firm was founded over 150 years ago by Piet Klynveld, William Barclay Peat, James Marwick and Reinhard Goerdeler, from whose surnames the initials KPMG are derived. It has a global reach, with 142 countries and more than 275,000 professionals. In Italy, KPMG has been present for more than 65 years, with around 6,000 professionals in 25 offices and a portfolio of 6,000 clients. The firm works with leading technology partners such as Microsoft, Google, IBM, SAP, Oracle, Salesforce, Appian and ServiceNow to deliver innovative solutions and is considered one of the leading professional services platforms in our country. The federal management model allows the Italian network to maintain significant strategic and management autonomy in the domestic market. The fundamental principles that guide KPGM are leadership, teamwork, continuous updating, but also transparency and commitment to communities and its customers in providing them with innovative and quality solutions. Specifically, the services offered by KPMG include:

- Audit e Assurance
- M&A
- Risk Management
- Compliance

- Governance
- Corporate Restructuring
- Digital Solutions
- Cybersecurity
- Human Resources Transformation
- Transfer Pricing
- Global Mobility
- Tax and Legal Services

## 1.2 Risk Consulting - Cyber & Tech Risk

The content of this paper will cover the project I was involved in during my internship in the *Cyber and Tech Risk* department, which is responsible for helping companies deal with cybersecurity issues and identify strategies that will enable them to achieve economic growth and competitive advantage. The *Cyber and Tech Risk* division performs critical work for companies to ensure they have a level of security that matches the speed and complexity of today's risks. The department's key areas of focus are:

- **Strategy and Governance**: Turning risk into a competitive advantage through effective governance.
- **Security Transformation**: Accelerate transformation initiatives.
- **Cyber Defence**: Protecting business opportunities from security risks.
- **Cyber Response**: Responding effectively to cyber incidents, working to foster security in the digital world.

The analysis will mainly cover activities related to **Strategy and Governance**, which plays a crucial role in ensuring that companies address cyber risks systematically and effectively. An important part of my work in the department involved an in-depth examination of the client's operational processes and organizational structures, with the aim of identifying critical areas of vulnerability and areas for system improvement. Through my experience, I was able to help define strategies to mitigate the identified risks.

### 1.2.1 The Case Study

The company that was the specific subject of the study is a leader in the agribusiness market, specializing in the production, import, export and marketing of its food products. The sector in which it operates is of considerable importance and is regulated by current legislation, in particular the recent *NIS Directive 2 (Directive (EU) 2022/2555).* In order to enable the client company to adapt to the rapidly changing technological landscape and achieve regulatory compliance, it was necessary to provide it with valuable support through the creation of operational frameworks. This thesis aims to explore, through an account of work carried out in a state-of-the-art business context and in collaboration with an up-to-date and competent interdisciplinary team, the analysis of the interaction between business and technology with awareness of the challenges and opportunities related to cybergovernance.

## 1.3 Reason for the study

This paper is driven by the need to understand how today's organisations can navigate and be resilient in a landscape of evolving cyber threats.

To achieve its objective, the study therefore takes as its starting point an analysis of the regulatory environment in order to understand the security requirements established within the European Union. In this respect, it is important to note that the work takes shape at a crucial moment in the modern evolution of cyber governance: it is being developed in parallel with the introduction of the *"EU 2022/2555 (NIS 2)"* directive and its subsequent entry into force through the *"Decreto Legislativo N. 138"*.

This regulatory framework spans multiple business sectors, highlights the importance of cybersecurity in many operational areas, imposes rigorous risk management and incident response requirements. In short, it creates obligations for organisations, but also gives them the opportunity to develop a more structured and proactive approach to security.

The research aims to help organisations by providing a clear framework on how to comply with the Directive while strengthening their defences. The aim is therefore not only to guide organisations in meeting regulatory requirements, but also to combine technical solutions with best practices, supported by reference authorities in the field, through an engineering approach. The combination of regulation and the application of tools related to technological innovation thus makes it possible to develop a corporate infrastructure that effectively responds to both regulatory requirements and emerging cyber threats.

Overall, this thesis proposes to highlight how regulatory challenges can lead to the development of a culture of resilience, raising awareness that only through structural and cultural change can organisations build an innovative environment that can be trusted in the long term.

## 1.4 Methodology

The implemented operational methodology started from an objective analysis of the reference context as indicated in the NIS 2 Directive, took into account and combined qualitative and quantitative aspects in order to obtain a complete and exhaustive picture of the threats and related practices concerning *cybersecurity*. The study was divided into several phases. After analysing the regulatory framework and the best practices already mentioned, it focused on analysing and evaluating the data collected on the state of customers' infrastructures, the organisational risk management framework and the problem and incident reporting procedures, with the aim of identifying, in a second phase, areas of criticality and improvement in order to implement measures to ensure compliance with the requirements of the regulations. The final stage of the process was therefore to establish a structural plan for the implementation of the *NIS 2 Directive*. In detail, the situation analysis was carried out through the following steps:

1. **Data Collection**: Information on IT security policies and practices was collected from key individuals in IT departments and then supplemented with documentation requested from client companies for further investigation. This process provided the necessary elements to verify the compliance of practices with regulatory requirements.

2. **Risk Management Assessment**: The risk management framework of the audited company was then analysed through a detailed review of the risk assessment processes activated by the company. This made it possible to understand how risks are identified, assessed, mitigated and monitored by the company, to determine the compliance of the procedures in place with the requirements of NIS 2, and to identify areas of non-compliance.

3. **Compliance analysis**: A comparative assessment of the data collected against industry standards and the model defined by regulatory guidance was then undertaken to ensure that the organisation's practices met regulatory expectations.

4. **Validation and feedback**: Preliminary results were presented to key stakeholders within the organisation for validation. Feedback was incorporated into the final analysis as defined by NIS 2 for the implementation of the practices.

# Chapter 2

# Background

## 2.1 The Evolution of Cyber Governance and Cyber Threats in Europe

Over the past decades, the evolution of cyberthreats has experienced an unprecedented increase, making cybersecurity a priority for governments. The structuring of attacks and the increase in the number of related sectors affected by them have led the European Union to develop a comprehensive and robust regulatory framework, culminating in the adoption of the NIS 2 Directive. In order to fully understand today's regulatory environment, it is necessary to assess the trajectory of cybersecurity legislation in Europe over the years and the related threats. Therefore, this chapter will examine both aspects: on the one hand, the evolution of European cybersecurity initiatives will be described, and on the other hand, the evolution of cyber threats will be analyzed, focusing on the most relevant attacks and events.

### 2.1.1 The Worm Era

Since the early 2000s, the well-known proliferation of technologies has created an ecosystem in which the foundations of various essential services are cyber in nature. Between 2000 and 2004, the cyber landscape was marked by the spread of numerous worm attacks [1]. This type of attack had been known for some time, but during this period it took on global significance and caused so much operational damage that it has been referred to as "The Worm Era".

[1] a type of attack that creates copies of itself with the general purpose of infecting computers and networks

The magnitude of this period's damage is highlighted by the *ILOVEYOU* worm, which disseminated globally through email attachments within hours, leading to widespread disruption across personal and professional computers, with estimated damages reaching up to 15 billion, as reported by Sophos[14].

*"The Worm Era"* was therefore a pivotal moment in the history of information security, highlighting the need for a structured system to deal with this type of attack, but attackers had since moved on to other types of attack. The point was clear, it was not enough to fight individual attacks, but to identify the basis for developing an information security system with modern response strategies.

### Convention on Cybercrime

In this context, the first European treaty dedicated to the suppression of cybercrime comes into play: the Budapest Convention on Cybercrime, which was adopted by the Council of Europe in 2001 and entered into force on July 1, 2004[12]. Its main objective is to harmonize national laws while facilitating cooperation among signatory states.

The Convention is based on three pillars:

- **The Criminalization of Conduct**: the definition of crimes related to unauthorized access or computer fraud.
- **Procedural Powers**: The formulation of additional investigative procedures that allow for the collection and retention of electronic data related to computer crime.
- **International Cooperation**: The sharing of techniques and information through mutual assistance among signatory states.

In the context of cyber attacks, a Convention is needed that can address these challenges, specifically the identification of those responsible and the measurement of the consequences of cyber attacks, which can extend to multiple jurisdictions. Differences between national laws created the risk of legal gray areas, but this initiative has increased the effectiveness of criminal protection and created a fundamental basis for the development of harmonized procedures.

### European Network and Information Security Agency

An important next step was the publication of *Regulation (EC) No.460*[13], adopted on March 10 2004, which established the European Network and Information Security Agency (ENISA). This entity was created with the objective of assisting Member States in the management of cybersecurity. The Regulation outlines what are the main functions of the Agency including:

- **Risk Analysis**: through the collection of appropriate information, the Agency highlights current and emerging risks that could impact cybersecurity. These analyses produce results that are shared with a committee and member states.
- **Technical Support**: the Agency provides advice to states on best practices in cybersecurity. This support includes assistance in the implementation of regulations; this is relevant to the understanding of the NIS 2 Directive and will be discussed in more detail later.
- **Awareness and Training**: the Agency promotes initiatives aimed at raising awareness of cybersecurity. Target audiences for this type of training include citizens, businesses and institutions.
- **Cooperation between Member States**: the Agency assists States both in their dialogue with each other to develop common methodologies, and in their dialogue with industry to assess and address hardware or software security issues.

The European Agency acts as a hub of technical expertise in this field and provides coordination between Member States, a role that has been progressively strengthened over the years. Indeed, the regulation governing the Agency has been updated several times over the years, and additional resources have been proposed, which has led to a general strengthening of the Agency itself. In this regard, there is a wealth of documentation issued by the European Commission, including the most recent Regulation (EU) 2019/881, which ensured the permanence of the Agency through a mandate by establishing new tasks and resources.

## 2.1.2 The Monetization Era

As Europe lays the groundwork for an increasingly structured cybersecurity strategy, cybercrime continues to evolve rapidly, threatening the landscape with new threats.

In 2005, the so-called *"Monetization Era"* of cyber-attacks began. While in the past, attacks and malicious application development were done to cause disruption or gain notoriety, this phase has seen the growth of cyberthreats aimed at financial gain in a new market where professionals play different roles: among them, exploit producers who develop real attack kits with the goal of illegally obtaining data or selling the attacks themselves.

### The Zeus Trojan case

One of the most striking examples of this generation of malware is undoubtedly Zeus, a Trojan[2] that landed in banking in 2007 and was designed to steal financial credentials by infecting the Windows operating system. The company CrowdStrike describes the attack paths and specific targets of this virus[2]:

> *"There are two common attack vectors that open Windows computers to Zeus trojan malware attacks. Drive-by downloads require a user to visit a website that has the backdoor trojan code on it. They then download files into the user's computer without the user's knowledge. Modern browsers such as Google Chrome usually block these downloads and the sites they are found on, but hackers are constantly implementing new workarounds for this. Meanwhile, older web browsers like Internet Explorer may not block drive-by downloads at all. Zeus's other main mode of infection is through phishing attacks where users think they are downloading benign software from links in a phishing email or a post on social media. The two primary goals of the Zeus trojan horse virus are stealing people's financial information and adding machines to a botnet[3]. Unlike many types of malware, most Zeus variants try to avoid doing long-term damage to the devices they infect. Their aim is to avoid detection from antivirus software. The longer they last, the more likely the hacker is to pick up valuable information from your financial institution"*

[2] A type of malware that hides in a seemingly innocuous software object but can execute malicious code once inside the device

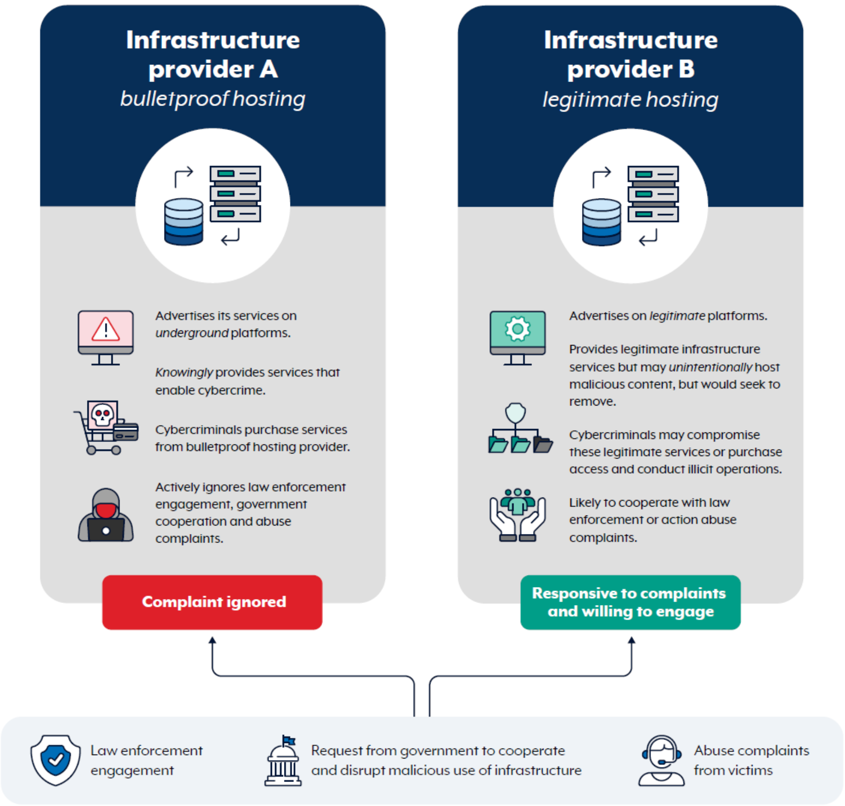
[3] A network of infected devices operating for a common purpose under the control of a single attacker

The analysis of this malware thus highlights the development of structured criminal operations that operate on multiple fronts and are difficult to detect, underscoring the importance of proper cyber hygiene with the correct information between governments and companies to train all relevant personnel on the necessary security practices.

### Bulletproof Hosting

An interesting phenomenon in this scenario that has further complicated the fight against attacks is the use of undetectable infrastructure that allows these criminals to remain hidden; this is referred to as *"Bulletproof Hosting (BPH)"*. The Australian Cybersecurity Centre defines BPH providers as[1]:

> *"A specific class of internet infrastructure service that enables malicious actors (including cybercriminals) to host illicit content and run operations on the internet".*



Infrastructure provider A
*bulletproof hosting*

Advertises its services on *underground* platforms.

*Knowingly* provides services that enable cybercrime.

Cybercriminals purchase services from bulletproof hosting provider.

Actively ignores law enforcement engagement, government cooperation and abuse complaints.

Complaint ignored

Infrastructure provider B
*legitimate hosting*

Advertises on *legitimate* platforms.

Provides legitimate infrastructure services but may *unintentionally* host malicious content, but would seek to remove.

Cybercriminals may compromise these legitimate services or purchase access and conduct illicit operations.

Likely to cooperate with law enforcement or action abuse complaints.

Responsive to complaints and willing to engage

Law enforcement engagement

Request from government to cooperate and disrupt malicious use of infrastructure

Abuse complaints from victims

Figure 2.1. Bulletproof Hosting. Source: [1]

Figure 2.1 in defining our evolutionary path is intended to highlight how companies that provide relevant services must also play an active role in detecting and combating cyber threats. This is done with a full understanding of the regulatory landscape and in cooperation with government authorities.

### Europe's Response

The general transformation of cybercrime threats into an organized and dangerous ecosystem required an immediate response from governments. Faced with these challenges, the European Union has introduced a number of key initiatives to strengthen security, including one of the first updates to the ENISA regulation. The following are some of the key initiatives.

**Identification and designation of European Critical Infrastructures:** "Directive 2008/114/CE"[6] establishes a common framework for the identification of European Critical Infrastructures, called ECIs, and considers how to improve their protection. It is therefore a key element in identifying and defining infrastructures in need of enhanced protection, as ECIs are defined as[6]:

> *"asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions"*

The Directive therefore aims to provide for the adoption of OSP security plans by operators, who will be responsible for identifying critical assets and their protection, designating those responsible for communication between operators and national authorities, and ensuring cooperation by exchanging information on vulnerabilities and protective measures

**Creation of CERT-EU:** Created in 2011, CERT-EU is a digital services body of the European Commission and aims to provide services to all EU institutions. It is currently chaired by the European Parliament and is composed of more than 60 cybersecurity experts to provide: [3]

> *"a wide range of services to our constituents spanning prevention, detection, response and cyber threat intelligence. For example, we*

> *coordinate response to cybersecurity incidents and ensure that information is efficiently exchanged with our constituents. We monitor and hunt for threats, perform technical assessments, Red Team and phishing exercises. We also organise cyber awareness sessions for our constituents and give them guidance as well as contribute to and participate in cyber exercises such Cyber Europe and Locked Shields."*

Overall, CERT-EU tracks the evolution of threats with the aim of improving the defenses of member states, and has structured cooperation with the aforementioned ENISA to ensure that research and action on multiple fronts work closely together.

### 2.1.3 The Ransomware Era

In the last two decades, there have been a number of very significant cases of cybersecurity threats, among which the proliferation of ransomware attacks has certainly played a prominent role, so much so that it has come to characterize this era. In fact, this type of attack has found in this historical period the right combination between what we can define as technological infrastructures and what has materialized as widespread social phenomena. The emergence of digital currencies and cryptocurrencies in the same period ensured the possibility of having easy payment methods with a high degree of anonymity[4], in addition, the wide spread of the Internet and social networks opened the door to a rapid spread of malware.

The proliferation of attacks on the security of different industries using different vectors should be seen as an important consideration. Sophos's report on this phenomenon and the accompanying chart (Figure 2.2) highlight the importance of security measures and cyber resilience in different categories of industry. Many of these, which are considered to be of particular importance, are in fact still under analysis at European level, with a view to being incorporated into existing legislation over time.

[4] The factor that had not allowed the spread of this type of attack in previous years was the possibility of being able to follow the flow of money in order to be able to detect possible culprits

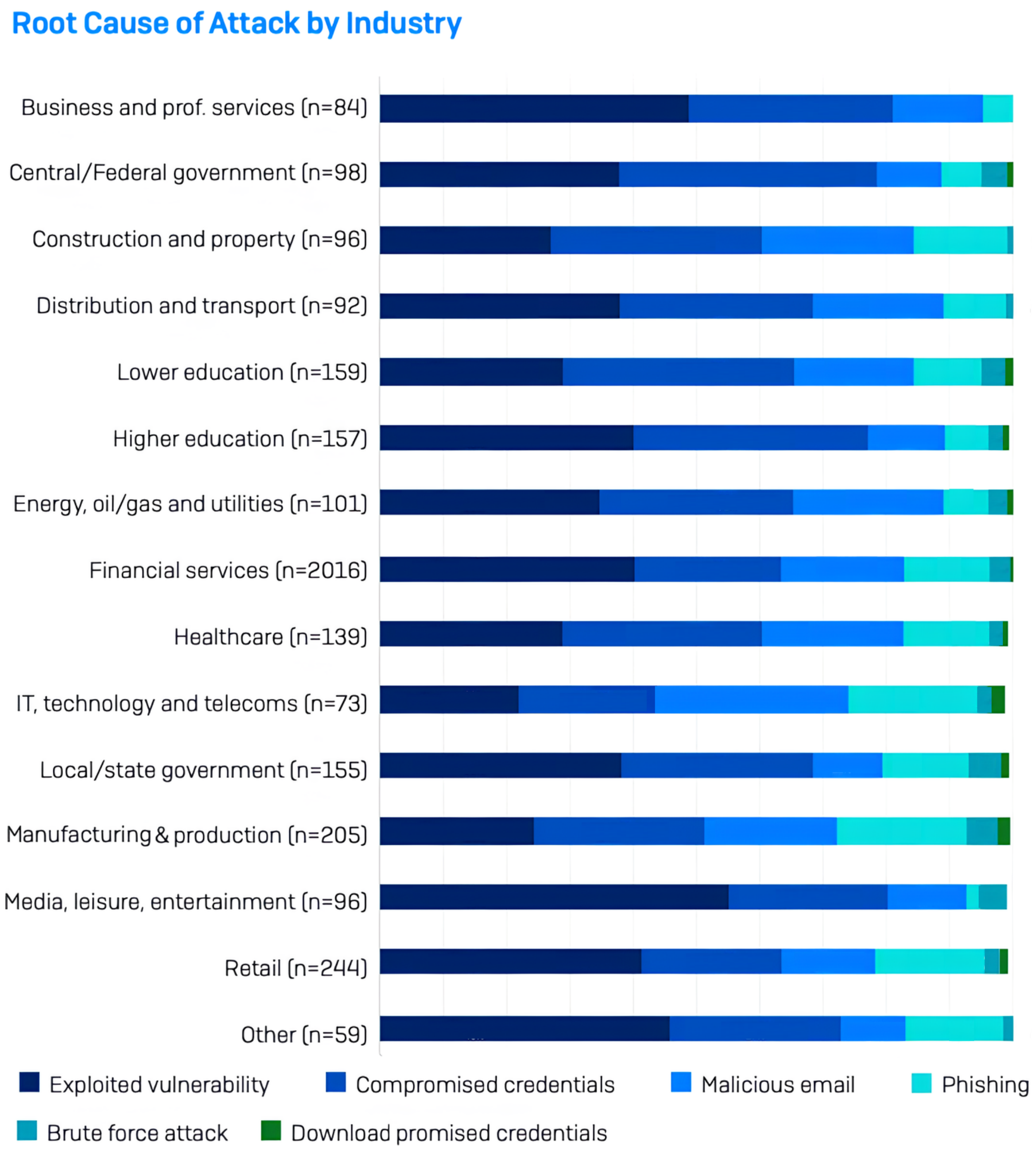


Figure 2.2. Rootcause of Attacks by Industry Source: [15]

### The Snowden Effect

In 2013, Edward Snowden, a former National Security Agency (NSA) analyst, leaked a number of classified documents with the intention of publicizing the existence of surveillance programs conducted by the United States. The leaked documents contained important details about the strategies used to collect and analyze vast amounts of private data derived from communications between citizens, companies, and political leaders. The documents produced also demonstrated the involvement of numerous intelligence agencies operating in a variety of countries.[7]

The revelations made by Snowden instigated a debate within the public sphere, wherein the necessity for surveillance of communications to ensure national security was acknowledged, while concurrently, the absence of transparency and the paucity of clear regulation governing data monitoring were identified as potential violations of citizens' privacy.

The phenomenon that has been termed the *"Snowden effect"* has precipitated considerable changes in the IT sector. Major companies such as Microsoft and Google, for example, have enhanced the security of their services by utilising end-to-end encryption.[5].

### The impact on European regulation

Aware of the growing importance of data protection, the European Union, in order to cope with this period of widespread cyber-attacks, has taken several policy and legislative measures to build resilient infrastructures and guarantee citizens' rights. Among these is the *General Data Protection Regulation (GDPR)*, which introduced new rules governing the processing of personal data.

At the same time as the GDPR, the first legal framework to strengthen the security of information systems, the *Network and Information Security (NIS) Directive,* was introduced in Europe. The evolving security threats and their serious consequences have necessitated a revision of the above legislation and led to the adoption of the *Directive (EU) 2022/2555 (NIS 2)*[9].

The main features of the above legislation are explained below.

## 2.1.4 The General Data Protection Regulation (GDPR) and its connection to cybersecurity

The *General Data Protection Regulation* (GDPR), formally known as Regulation (EU) 2016/679, came into force on May 25, 2018. The document was created with the aim of regulating, and thus ensuring, the protection of personal data within the European Union. This legislation has introduced significant changes and new restrictions for organizations that process personal data, imposing fundamental principles such as *correctness and transparency of processing* and *minimization of data.*

[5] A data protection method in which data is encrypted on the sender's device and can only be decrypted on the recipient's device

The GDPR has also regulated the organizational and operational dynamics of companies, imposing new obligations on them, including the implementation of adequate security measures for the protection of personal data. In fact, as an example, the *Article 32* of the regulation reports on risk management-oriented organizational measures[8]:

> *"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
>
> - *the pseudonymisation and encryption of personal data;*
> - *the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
> - *the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
> - *a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."*

This requires organizations to implement appropriate technical and organizational solutions to ensure the confidentiality, integrity and availability of information. The Regulation also introduced the obligation to notify supervisory authorities of personal *data breaches.*

### 2.1.5 The NIS Directive

The *Directive (EU) 2016/1148*, better known as the *Network and Information Security Directive* (NIS), was the first legislation in the European Union specifically addressing the security of networks and information systems. The Directive, which was adopted on July 6, 2016 and came into force in August of the same year, is a key act in establishing a common cybersecurity strategy within the EU.

Specifically, the Directive and its provisions aim to:

- Strengthen the resilience of critical infrastructure and essential services against cybersecurity threats.
- Improve cooperation between Member States through common incident management strategies.
- Impose security and incident notification obligations on *operators of essential services* (OSEs) and *digital service providers* (FSDs).

Although the NIS Directive has made a significant contribution to the implementation of procedures to enhance cybersecurity, it has highlighted some critical issues, including the following:

- **Difference in implementation**: Member States have been given some discretion in implementing the rules set out in the Directive, which has led to significant differences in the implementation of the provisions in different national contexts.
- **Limited sectoral coverage**: Although the provisions of the Directive covered a wide range of sectors, some sections critical to cybersecurity were not included in the regulations.
- **Lack of uniform sanctions**: The Directive did not provide for common penalties to be adopted by the various Member States, leaving each Member State free to set penalties for non-compliance. This resulted in a great heterogeneity in the definition of penalties.

The critical issues outlined above highlighted the need for a regulatory update, which led to the creation of the *NIS 2 Directive*, which fills many of the gaps in the original version and broadens the scope of cybersecurity regulation in Europe.

### 2.1.6 The Path of the NIS 2 Directive

On November 10, 2022, the European Parliament approved the *Directive (EU) 2022/2555 (NIS 2)*[9], which aims to solve the aforementioned problems of the previous directive (NIS 1). The main goal of NIS 2 is to strengthen the overall level of European cybersecurity by expanding the sectors and critical infrastructure requirements covered. In Figure 2.3 we find the main stages that led to the development of the NIS 2 Directive and its implementation in the EU Member States. The birth of this paper comes within this line at a key moment in the transposition of the Directive at national level, in our case by Italy with the *"Legislative Decree No. 138"* that will be analyzed later.

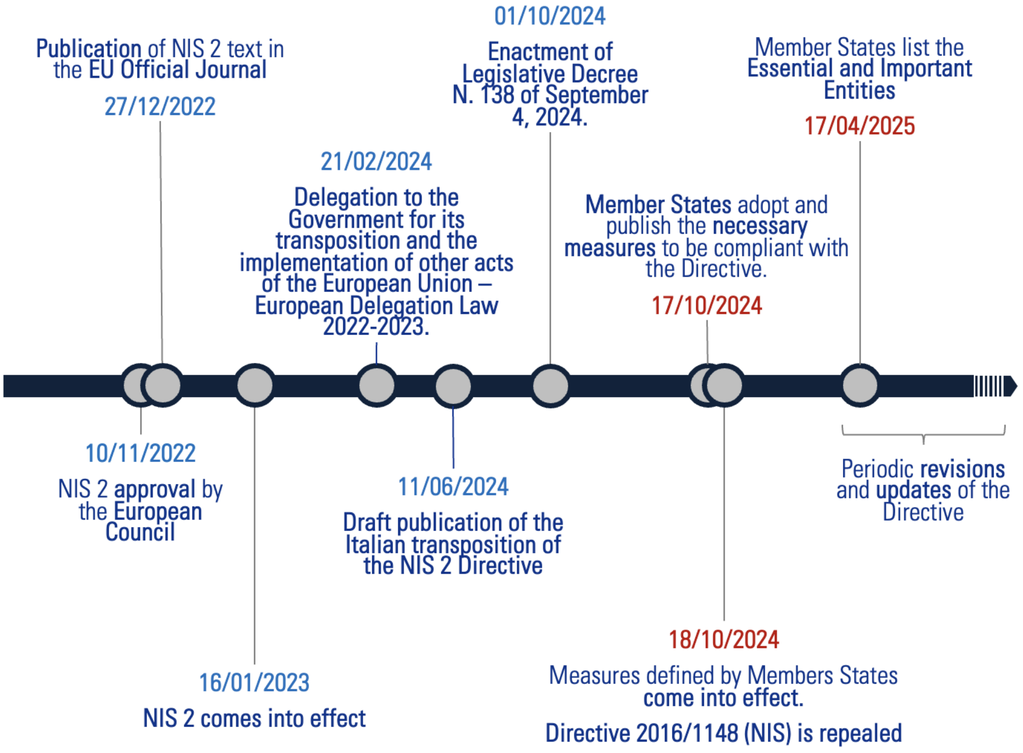

10/11/2022
NIS 2 approval by the European Council
Publication of NIS 2 text in the EU Official Journal
27/12/2022
16/01/2023
NIS 2 comes into effect
21/02/2024
Delegation to the Government for its transposition and the implementation of other acts of the European Union – European Delegation Law 2022-2023.
11/06/2024
Draft publication of the Italian transposition of the NIS 2 Directive
01/10/2024
Enactment of Legislative Decree N. 138 of September 4, 2024.
Member States adopt and publish the necessary measures to be compliant with the Directive.
17/10/2024
18/10/2024
Measures defined by Members States come into effect.
Directive 2016/1148 (NIS) is repealed
Member States list the Essential and Important Entities
17/04/2025
Periodic revisions and updates of the Directive

Figure 2.3. NIS 2 Timeline

NIS 2 expands the group of entities involved to include both public and private organisations operating in critical sectors. The total number of sectors in which these entities operate has been increased from that previously specified in NIS1, as reflected in the respective annexes to the Directives. The division of these entities is explained in *Article 3 of the Directive NIS 2*, where they are divided into essential and important entities according to their criticality and size. In turn, the thresholds defining the size of entities are defined in *Article 2 of the Annex to Recommendation 2003/361/EC* according to these parameters[5]:

1. *The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million.*

2. *Within the SME category, a small enterprise is defined as an enterprise which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million.*

3. *Within the SME category, a microenterprise is defined as an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million.*

Thus, essential entities are large enterprises in the sectors listed in Annex I, including public entities and other entities identified as critical by Member States. Important entities, on the other hand, are all other entities that fall under Annexes I and II but do not meet the criteria to be considered essential.

In figure 2.4 we find a diagram of the sectors involved, including the food sector, concerning the Client's company that we will analyze later.

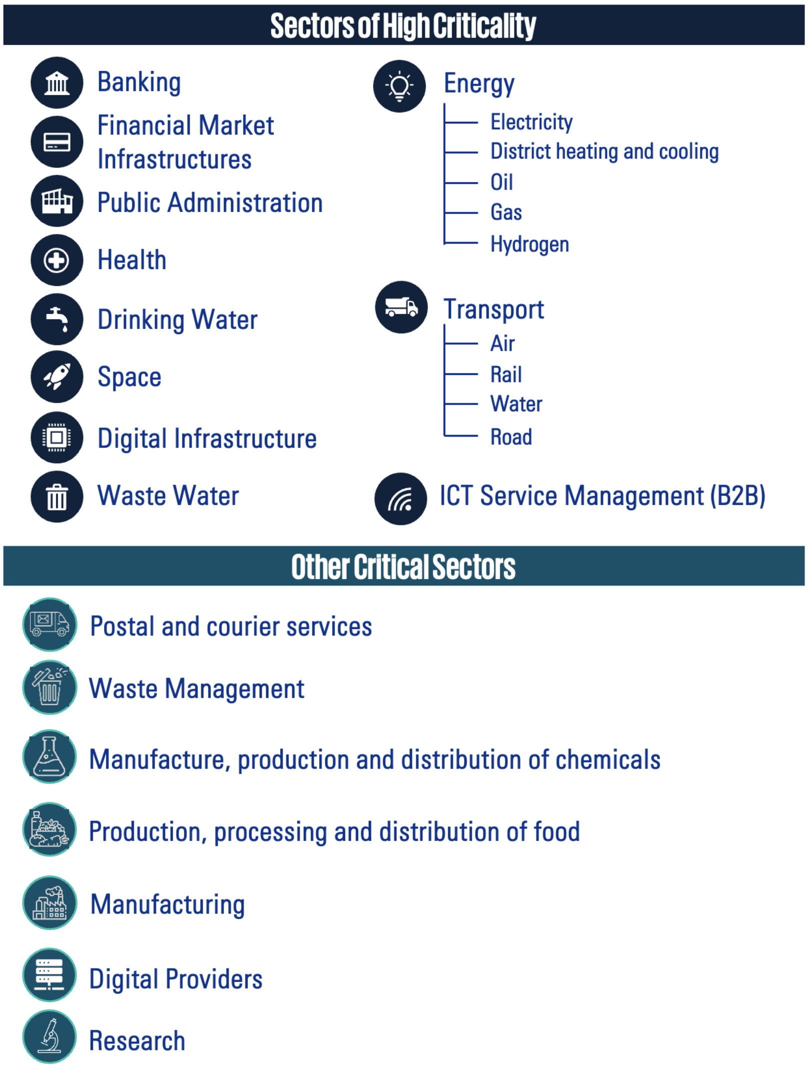

Sectors of High Criticality
Banking
Financial Market Infrastructures
Public Administration
Health
Drinking Water
Space
Digital Infrastructure
Waste Water
Energy
Electricity
District heating and cooling
Oil
Gas
Hydrogen
Transport
Air
Rail
Water
Road
ICT Service Management (B2B)
Other Critical Sectors
Postal and courier services
Waste Management
Manufacture, production and distribution of chemicals
Production, processing and distribution of food
Manufacturing
Digital Providers
Research

Figure 2.4. NIS 2 OSE

In addition, Article 3 clarifies that States are responsible for identifying and reporting these items in a list by April 17, 2025, and that this list is to be updated at least every two years[9]:

> *By 17 April 2025, Member States shall establish a list of essential and important entities as well as entities providing domain name registration services. Member States shall review and, where appropriate, update that list on a regular basis and at least every two years thereafter.*

Following an analysis of the Directive, key focus areas can be identified that will later serve as a reference point for the assessment of the Client's company to evaluate its compliance status. The following elements then represent the key focus areas from NIS Directive 2:

- **Governance**: *Article 20* states that senior management takes responsibility for cyber risk management, and specifically that the entities involved have obligations to approve risk management measures, oversee implementation, and consequently be liable in the event of a breach. In addition, the article emphasizes the importance for Member States to conduct training activities for their employees in order to provide them with appropriate skills for the risk management related services provided.

- **Incident Reporting**: *Article 23* requires companies to establish a process to ensure preliminary notification of significant incidents within 24 hours of discovery, full notification within 72 hours and a final report within 30 days.

- **Risk Analysis and Security Measures**: *Article 21* requires that a risk assessment be conducted to determine security measures to protect computer systems and information networks, including their physical environment.

- **Supply Chain Risk Management**: *Article 21* also adds details on strengthening the process of cyber risk management within one's supply chain, including aspects related to the security of relationships between each entity and its direct suppliers or service providers.

Finally, another important aspect of the Directive is that of penalties, which are intended to draw attention to the importance of the requirements of the NIS 2 Directive. Specifically, penalties are set in amounts and percentages based on the violation and the type of entity involved. Specifically, *Article 34* of the NIS 2 Directive provides that

> - *Member States shall ensure that where they infringe Article 21 or 23, essential entities are subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a maximum of at least EUR 10 000 000 or of a maximum of at least 2 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the essential entity belongs, whichever is higher.*
>
> - *Member States shall ensure that where they infringe Article 21 or 23, important entities are subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of*

> *a maximum of at least EUR 7 000 000 or of a maximum of at least 1,4 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the important entity belongs, whichever is higher*

These penalties, shown in Figure 2.5, have the inherent goal of incentivizing organizations to maintain high standards of cybersecurity.

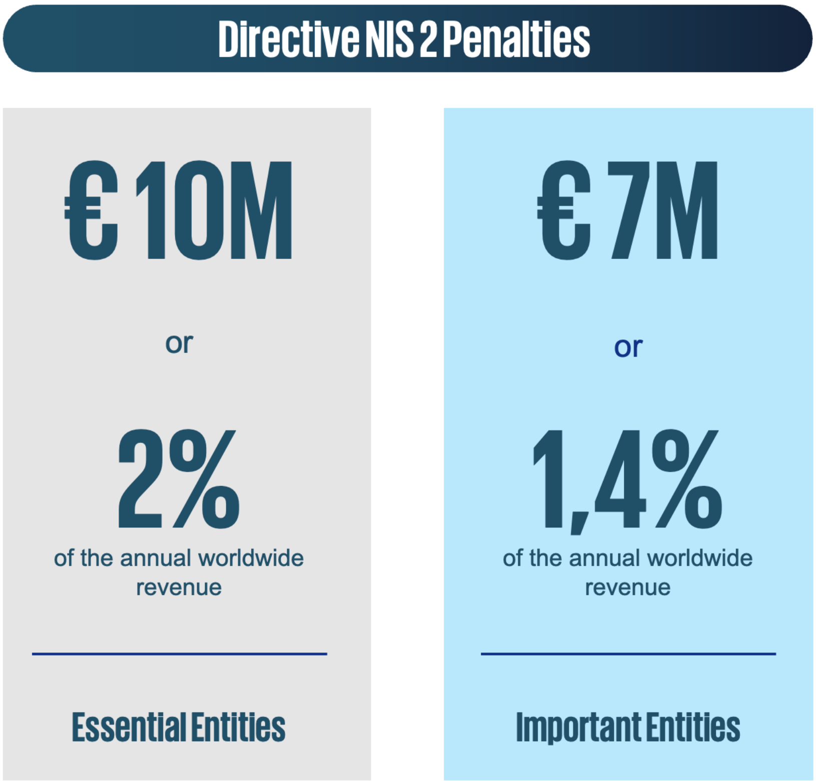

Directive NIS 2 Penalties
€ 10M
or
2%
of the annual worldwide revenue
Essential Entities
€ 7M
or
1,4%
of the annual worldwide revenue
Important Entities

Figure 2.5. NIS 2 Penalties

The context in which the NIS 2 Directive was born and how the threats have evolved to the present day allow us to understand the technical and practical aspects that need to be achieved in order to achieve regulatory compliance, but also to learn about additional tools that can lead to achieving a high level of security when upgrading business technologies and procedures.

### 2.1.7 National measures in Italy

The primary regulatory document that enabled Italy to implement Directive (EU) 2022/2555, also known as NIS 2, was Legislative Decree no.138 of

4 September 2024[11]. The Decree has facilitated enhanced security for network and information systems through a series of procedures, rules and duties, thereby contributing to the process of formulating cybersecurity strategies in Italy.

**Roles and governance of national cybersecurity** Legislative Decree no.138 formally acknowledges the pivotal role of the **National Cybersecurity Agency (ACN)**, entrusted with the execution of both strategic and operational responsibilities pertaining to national IT security, as outlined in Directive (EU) 2022/2555. The Agency is composed of several important structures that enable it to implement various services, including:

Decree no. 138, which serves to affirm the principles previously outlined in Directive (EU) 2022/2555, formally acknowledges the pivotal role of the **National Cybersecurity Agency (ACN)** in the context of national IT security. Since 2021, the ACN has been entrusted with the execution of strategic and operational responsibilities in this domain. Notably, the Decree designates the ACN as *the competent national authority and the NIS contact point*, a designation that bestows upon it extensive powers of supervision, oversight, and sanction. The Agency is composed of key structures that facilitate the implementation of various services.

The following list details the most significant of these:

- **NCS (Nucleo per la Cybersicurezza - Cybersecurity Unit)**, which carries out prevention and preparation functions for potential crisis situations and is responsible for activating alert procedures.

- **CSIRT (Computer Security Incident Response Team) Italia**, the national team for responding to cyber incidents.

The provisions of the Decree serve to strengthen the inspection and verification powers established by the National Cybersecurity Agency, through the introduction of additional obligations and constraints regarding documentary material, control through periodic audits, and a strict system of sanctions that follows the provisions of Article 34 of NIS 2, with fines that can be as much as 2% of turnover for essential subjects, and as much as 10 million euros *(Article 38 Legislative Decree no.138[11])*.

**Obligations for the organisations involved** Organisations affected by the provisions of *Legislative Decree No.138* must:

- Adopt all the technical, organisational and procedural measures provided for the management of IT risk contemplated in the document.

- Prepare adequate documentation that includes a cybersecurity policy, with rules and standards that must be subject to a system of continuous risk assessment and provide procedures for the management of any incidents.

- Notify the National Cybersecurity Agency of any incident deemed important as soon as possible, within twenty-four hours of detection with any updates within the following seventy-two hours. and a final report within 30 days of detection.

- In line with *Article 20 of NIS 2*, assign greater responsibility for the supervision and implementation of security measures to company management.

- Prepare and apply measures for third-party risk management, i.e. implement interventions that allow for the prediction, assessment and mitigation of risks caused by one's supply chain.

**Integration with the national crisis system** *Legislative Decree 138/2024* imposes further obligations on organisations, mandating the integration of their IT crisis management framework with that provided by the national system. It also necessitates coordination with the *Cybersecurity Unit (NCS)* and the direct involvement of the Presidency of the Council.

**Alignment with existing regulations** Another salient aspect of *Legislative Decree 138/2024* that deserves highlighting is its coordination with other significant provisions that have been adopted over time, such as *Legislative Decree 105/2019* (National Cyber Security Perimeter), which deals with the protection of strategic infrastructures and *Legislative Decree 82/2005 (Digital Administration Code)* which regulates the digital transformation and security of public administrations. The synergy between the aforementioned regulatory provisions has allowed the establishment of a multi-level cybersecurity ecosystem, in which all the subjects involved, companies, the Public Administration and digital service providers are called upon to operate in compliance with shared security and resilience standards.

**Relevance for documentary analysis** The focus on the Decree is warranted by its status as a foundational element of current legislation, anticipated to offer strategic direction to organisations seeking to attain regulatory compliance. The Decree meticulously delineates measures and provisions aimed at ensuring IT security, thus establishing itself as a comprehensive framework that organisations can adopt. The following documents are of particular relevance for the purpose of demonstrating compliance and are thus highlighted for explanation:

- Risk management plans.
- Incident and vulnerability logs.
- Documentation regarding compliance audits.
- Contracts regarding security agreements with third-party suppliers.
- Incident notification and management reports.

The obligatory compilation of the aforementioned documentation, as well as the verification of the provisions it contains, are essential factors in demonstrating to the control authorities that organisations are in compliance with current regulations and in allowing for eventual checks and inspections by the NAC. The present thesis aims to underscore the fundamental importance of the documentation in question for the purpose of verifying the Client company's compliance with current legislation. This is achieved through a detailed analysis of the content of the documentation and its conformity with the requirements of *NIS 2* and the Italian implementing decree.

**Final considerations** In summary, it can be posited that *Legislative Decree 138/2024* should not be regarded as a mere formal instrument for the implementation of *NIS 2 Directive*, but rather as a valid regulatory document whose provisions have had a profound impact on corporate governance and cyber risk management, rendering it crucial for IT security in our country.

In the subsequent chapter, a case study of the client company will be specifically analysed. This will entail an examination of the data from its internal documentation, followed by a comparison with the requirements of *NIS 2* and *Legislative Decree 138/2024*. The focus will then be on evaluating the results and, as part of a gap analysis process, identifying and proposing any corrective measures necessary to achieve full compliance.

# Chapter 3

# Case Study

## 3.1 Preliminary Analysis

This phase entailed an exhaustive examination of the NIS 2 Directive, the consequent Legislative Decree No.138, and the associated technical and regulatory documentation. The objective of this analysis was to compare the aforementioned directives with the provisions adopted by the client company, thereby assessing its level of conformity and ensuring the provision of targeted and valid technical support.

Specifically, the preliminary phase involved the following activities:

- Exploration of the regulatory scenario concerning security requirements, risk management and protection of critical infrastructures.

- Examination of operational guidelines and *frameworks* related to cybersecurity and data protection in order to identify *best practices* and practical implications to be adopted.

- Identification of points of convergence between European legislation and specific business needs, in order to strategically orientate the adoption of the measures necessary for regulatory compliance.

## 3.2 Sources and Materials

The development of a security framework and the implementation of related and subsequent activities was influenced by the knowledge of best practices adopted over time in the field of IT security. The formulation of the security framework was achieved by integrating the contents of the guidelines[10] provided by the *European Union Agency for Cybersecurity* with the cybersecurity framework[4] defined at national level, which in turn take into account the principles of the *NIST (National Institute of Standards and Technology) framework.*

### 3.2.1 ENISA in the Case Study

In the course of the compliance framework's implementation for the client during the intervention of the Case Study, it is specifically noted that the guidelines contained in the document Implementation Guidance on Security Measures, published as a draft by ENISA, were of support. The document in fact provides a valid operational reference for the implementation of the required security measures and is able by its structure to offer organisations both general principles and practical guidance. ENISA's guidelines were instrumental in the earlier activity with the client, facilitating the identification of the necessary evidence for demonstrating compliance with specific requirements and, through the elaboration of further parameters, facilitating an important mapping capable of correlating regulatory requirements to international standards.

It is important to note that both the ENISA guidance and the framework it has created are subject to change, as the foundations upon which they rest, namely the national cybersecurity frameworks and international standards, are subject to change over time. The structure of the framework lends itself to changes in content and possible additions that the periodic evaluations and reviews, to which the work is subject, require. Similar review procedures, at regular intervals, are in fact contemplated by the European Commission and the NIS cooperation group also in relation to the ENISA document under consideration.

The document provides a detailed description of security measures and includes suggestions for the adaptation of several important areas, including:

- **Risk Management**: which provides definitions for the assessment and adoption of appropriate security policies and procedures.
- **Operational Protection**: which includes technical security guidelines such as data protection measures.
- **Incident Response**: which provides guidelines for the detection and management of attacks or security breaches.

- **Monitoring**: consisting of specific recommendations in the area of auditing for the continuous verification of the measures adopted.

### 3.2.2 The National Cybersecurity and Data Protection Framework

The National Cybersecurity and Data Protection Framework is another important supporting document that is worthy of analysis. This document contains the structure of a framework developed by the CINI National Cybersecurity Laboratory and CIS-Sapienza. This is based on the NIST Cybersecurity Framework and aims to provide Italian organisations with a practical reference for the implementation of cybersecurity and data protection measures.

**Structure and Fundamental Principles** The most useful element for its contribution to the realisation of the work was the skeleton used in the structure of the National Framework for Cybersecurity and Data Protection. Specifically, the Framework Core proved to be highly informative, as it contains references for all categories related to cybersecurity management and the various links to international standards. Each category is subdivided into subcategories that can be organised and customised according to their relevance to the individual organisation. Finally, for each of these subcategories, there is a section dedicated to assessing the company's level of maturity.

**Application in the context of NIS 2 compliance** In the course of developing the NIS 2 compliance framework, the National Framework was employed for the following purposes:

- The establishment of security measures in a clear and consistent manner with regulatory requirements.
- The facilitation of the integration of security practices into existing business processes.
- The provision of a nationally recognised reference model useful for communication with stakeholders and supervisory authorities.

The utilisation of this framework facilitated the translation of the general indications of the NIS 2 directive into a set of practical and operational controls. The work did not result in a mere transposition of the existing model; instead, a structure was developed with integrative elements that enriched the original one. In particular, each sub-category is accompanied by a set of guiding questions, which are designed to facilitate and clarify the self-assessment process for the client. The self-assessment system itself, the description of which will be provided in detail in the following chapters, allows one to express one's level of maturity in a structured manner, with a correlated justification. Finally, for each result obtained, a dedicated section has been integrated, providing the customer with immediate feedback capable of guiding them in the subsequent planning phases of internal improvement interventions.

The contents indicated by the European Guidelines enabled an assessment of the general security measures for the management of infrastructure risks and the criticalities in the management of information systems, while the national regulations provided more detailed operational indications, specifically adapted to the local context. The integration of these sources of information allowed the creation of a security framework that was considered complete and effective, making the framework not only an analysis tool, but also a real operational support in the definition of concrete and customised improvement roadmaps. Collaboration with the corporate team was fundamental in identifying the practical needs of the client companies and finding suitable solutions, proposals that were actually applicable to their specific operational context. Critical points concerning the integration of regulatory requirements, procedures for collecting the necessary data, and the definition of an action plan that not only met compliance obligations, but was also able to adapt and respond effectively to today's security risks and the specific needs of each company involved, were always examined and discussed as a team.

### 3.2.3 ISO/IEC 27001:2022 in the Analysis Process

During the Preliminary Analysis Process, together with the aforementioned *ENISA Guidelines*, the *National Framework for Cybersecurity and Data Protection*, another important regulatory reference was adopted, the *Standard ISO/IEC 27001:2022.*

The latter has proved to be a valid operational and methodological support as the structured information management system (ISMS) it is accompanied by has allowed the updating of the controls necessary for the evaluation of the level of company maturity in terms of cybersecurity and has favoured greater compliance of the system with the *NIS 2 Directive***.**

#### Structure of the Standard

The main purpose of the standard is to guarantee the protection of the confidentiality, integrity and availability of information; in fact this model is defined as **Confidentiality, Integrity, Availability (CIA),** as illustrated in the figure below (*Figure 3.1*).

Confidentiality
Availability
CIA
Integrity

Figure 3.1. Confidentiality, Integrity, Availability

The above-mentioned objective is achieved through a systematic approach to risk management that allows companies to adopt measures appropriate to the specific risks affecting their operational context.

The Standard consists of two main parts, one relating to the Clauses and the other to the table Annex A:

1. **Clauses 0-10**: Specifically, these concern, from 0 to 3: the Introduction, the Scope, the Normative References, the Terms and Definitions. The following clauses cover the general requirements for information security management. Among other things, these describe the organisational context, leadership, risk assessment and what continuous improvement should be.

2. **Annex A**: The annex contains a list of non-mandatory controls that supplement the clauses. There are 93 controls for information security, as shown below (*Figure 3.2*), and they are divided into four categories:

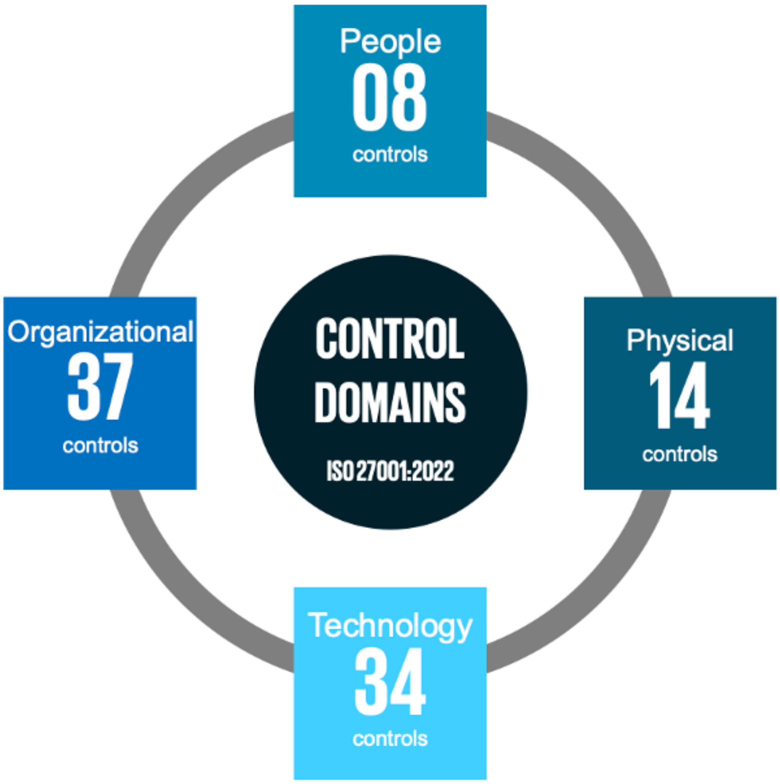


Figure 3.2. ISO 27001:2022 Control Domains

- **Organisational controls:** which through 37 specific controls affect governance, risk management and relations with third parties.
- **Physical Controls:** which concern 14 building security controls, through the regulation of physical access.

- **People:** which includes 8 controls relating to security training, management of roles and responsibilities.
- **Technological Controls:** 34 controls concerning Network Protection, encryption and IT access management.

### Role of ISO/IEC 27001 in the Case Study

Due to the characteristics outlined above, the adoption of the *standard ISO/IEC 27001:2022* proved to be an effective tool for various stages of work in the case study under examination. Some of these are described below, by way of explanation:

- **Definition of the security evaluation criteria** → The risk management practices required by ISO 27001 facilitated the identification of gaps and vulnerabilities in compliance with the requirements of NIS 2.
- **Mapping security measures**→ The controls listed in Annex A **of** ISO 27001:2022 were used to compare the security measures adopted by the Client with international best practices.
- **Strategic guidance for compliance**→ The structure of the standard facilitated the security processes and procedures with respect to the governance obligations imposed by the NIS 2 Directive.
- **Support in drafting the corporate** self-assessment framework and subsequent **policies**→ The ISO 27001 categories and controls provided practical references that proved to be a valid support for the construction of a security management model suited to the specific operational reality of the client company.

As can be easily seen from the above description, the structure of the *ISO/IEC 27001:2022 standard* allows for the implementation of an effective security system that can be adapted to the specific needs of different organisations.

### Convergence between ISO 27001 and NIS 2 in the Business Context

For a more explicit analysis of ISO 27001:2022, it is important to compare it with the NIS 2 Directive to highlight how they have fundamental points of convergence *(Table 3.1)*.

This correlation during the intervention process, relating to the Customer case in question, allowed for the adoption of an integrated approach to compliance that favoured the optimisation of strategies for responding to security threats and regulatory compliance.

| Area | NIS 2 Requirements | ISO 27001 Controls |
|---|---|---|
| **Risk management** | Continuous threat assessment and mitigation measures | Risk management, vulnerability assessment, third-party management |
| **Critical infrastructure protection** | Security measures to prevent cyber attacks | IT system protection, access management, network security |
| **Incident monitoring and response** | Reporting obligations and proactive attack management | Logging, incident management, cyber attack response |
| **Security governance** | Structured approach to IT security | Implementation of ISMS, role and responsibility definition |

Table 3.1. Mapping of NIS 2 Requirements to ISO/IEC 27001:2022 Controls

### Application of ISO/IEC 27001 in the Case Study

In the case study, ISO/IEC 27001:2022 was specifically used as an operational reference to:

1. **Structure the customer's compliance framework.** The framework structure allowed for a valid systematic view of information security.

2. **Support company self-assessment.** By means of a set of controls provided to them, the Client was able to correctly measure and assess the level of maturity of their company with respect to the NIS 2 Directive.

3. **Integrate security measures into business processes.** The interventions were implemented in such a way as to ensure that cybersecurity strategies were aligned with the Customer's operational needs.

4. **Provide a security governance model.** The latter was structured in such a way as to be a valid tool for sustainable and scalable management over time.

In summary, it can be argued that the ISO/IEC 27001:2022 Standard has proved to be a fundamental element in the construction of the compliance framework that has been created for the client company and that, through this, it has been possible to offer the organisation valid and concrete support for the implementation of the measures required by the NIS 2 Directive.

## 3.3 Customer Assessment and Customization Cycle

Following the delineation of the project's scope, a collaborative relationship was initiated with the Client's managerial personnel. The primary objective of this initiative was to evaluate the company's cybersecurity risk mitigation strategies, with a particular focus on their alignment with the stipulations outlined in the NIS 2 Directive. The assessment process was meticulously executed through a series of systematic steps, the details of which will be elucidated in the subsequent paragraphs.

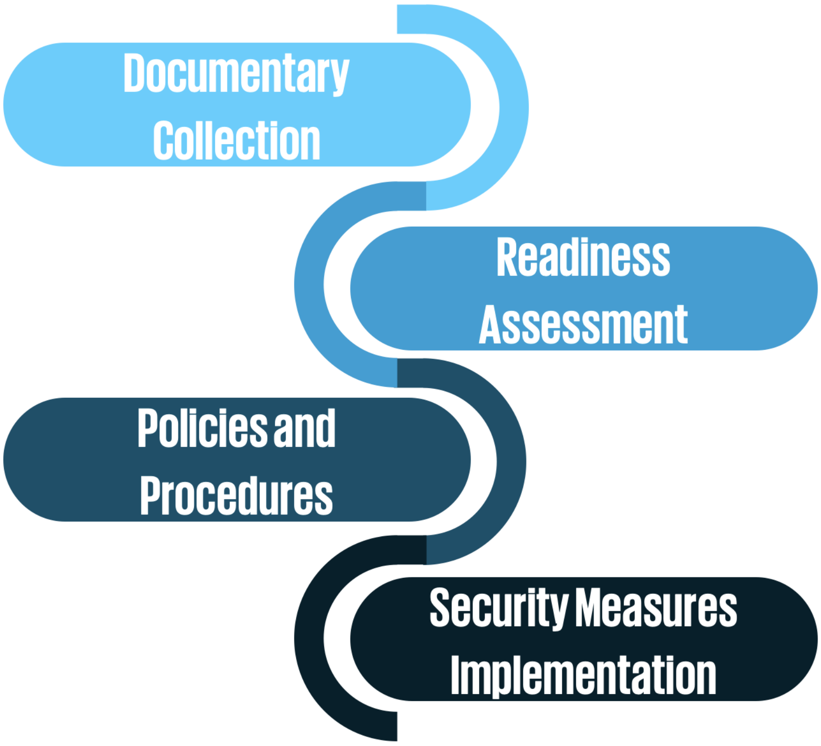


Figure 3.3. Phases of the work

### 3.3.1 Documentary collection

Following the framing of the evolution of the phenomenon of cybersecurity in Europe within its historical context, and the examination of the consequent regulatory responses aimed at containing it and the main operational support tools, a series of company documents were collected. These were considered pertinent and therefore functional for the evaluation of the organisation's level of compliance with the current regulatory system.

The objective of this phase was twofold:

- to verify the presence of the documentation in the company's possession and its completeness in relation to regulatory obligations
- to assess the organisation's overall level of maturity with regard to its governance and level of security.

In order to provide the Client with a valid tool for collecting and cataloguing the necessary documentation, a Provided By Client List (PBC) has been prepared. This consists of a detailed list of the required documents, divided into subject areas. The list has been structured in accordance with the regulatory analysis process, specifically the requirements of the *NIS 2 Directive*, *Legislative Decree 138/2024*, the guidelines for the creation of internationally established frameworks and the best practices explained in the previous section of this document.

The documentation collection phase is considered an essential part of the process of intervention in favour of computer security. This is because, in addition to representing a first indicator of regulatory compliance, it also denotes the starting point for subsequent evaluation activities. In order to better explain its structure, the PBC List used will be illustrated below, and in detail, the areas of documentation that were the subject of request and analysis.

#### Structure of the PBC List

The PBC List, as previously stated, consists of macro-areas that have been defined to represent the complete IT security management cycle, and take into account the entire process, which reflects the cyber risk management process, both in its organisational and strategic aspects and in its operational and methodological aspects. The subdivision has been designed to cover various aspects, such as:

1. **The organisational structure and governance roles**: knowledge of the aspects relating to these components can be considered the focal point for assessing whether duties and responsibilities are clearly assigned as required by the regulations.

2. **Training and corporate culture on security**: staff awareness of regulations and operational strategies is an essential requirement for the defence of security; the NIS 2 Directive requires management to be directly involved in the process and provides training courses for them.

3. **Incident handling and recovery planning**: the ability to implement a timely response to a cyber incident is an important indicator of the maturity level of a security system.

4. **Structured risk management**: is the core of any security system is its ability to promptly identify, assess and mitigate risks.

5. **Supply chain security**: is a key priority for NIS 2, which has emphasised the need to extend security governance to suppliers and critical partners.

6. **The adoption of technical and organisational security measures**: this operational phase involves requesting documentation from organisations that certify the concrete application of the foreseen protection measures, for example, for access management, backup, vulnerability management, logging, encryption, etc.

7. **The operational resilience of IT systems**: is the area that guarantees the **operational continuity** of security, allowing organisations to **quickly restore** their services in the event of a serious incident.

### A risk-based approach

As previously mentioned, the structure of the **PBC List** reflects a risk-based approach, consistent with the provisions of Article 21 of the *NIS 2 Directive* and *Legislative Decree 138/2024*. It is important to note that this list should not be regarded as a static or standardised document collection. Instead, it should be adapted to the specific risk profile of the organisation under analysis. This process involves taking into account various factors, including the sector to which the organisation belongs, the size of the company, technological and organisational complexity, and the presence of regulated processes or critical activities.

The PBC List is a key operational instrument for the systematic compilation of corporate documentation, enabling the identification of existing documentation and the determination of any document-related discrepancies with the requirements of the *NIS 2 Directive* and *Legislative Decree 138/2024*.

It is proposed as a valid tool capable of facilitating subsequent documentary analysis and providing an effective operational trace that favours direct comparison and possible additions during interviews with company representatives.

### Interviews with company representatives

Concurrently with the collection of documentation, interviews were conducted with company representatives, following a PBC List structure, in order to integrate and clarify the information provided by the client. The questions concerned technical aspects such as:

- Updating the organisation chart and defining cybersecurity responsibilities.
- Recruitment procedures, with a focus on assessing IT security skills.
- The existence of confidentiality agreements and formal information security policies.
- Supplier management processes, including security requirement checks.
- The way in which security incidents, backups and vulnerabilities are managed.

These interviews allowed for the identification of gaps in the documentation and verification of the consistency between formal policies and operational practices adopted by the company.

# Chapter 4

# Readiness Assessment

This phase involves the assessment of the company's readiness, which is achieved through the analysis of the documentation provided by the Client and the procedures described during the interviews. The objective of this stage is to catalogue potential issues and define them in a concrete and, where possible, measurable way. The activity is carried out in various areas of IT security, with particular attention to the requirements of the NIS 2 directive.

To achieve this objective, specific activities were undertaken, the main ones being the following:

1. **Assessment Framework**
   In this phase, the readiness assessment framework is designed and developed, aligned with the requirements of the NIS 2 Directive. The framework consists of a series of questions that have been structured and categorised into thematic areas, sub-areas and specific controls. This structure is designed to verify company compliance with regulatory requirements and best practices in IT security. The flexibility of the framework, within the specific context of analysis, has enabled adaptation to the company's particular characteristics while ensuring methodological consistency with the criteria established at a European level.

2. **Roll-out and Sharing**
   After development, the framework is shared with the client company through a structured questionnaire accompanied by instructions on how to fill in each section of the document. In this phase, the functioning of the AS-IS evaluation process is explained, as well as the criteria for assigning maturity levels and the need to justify the assigned evaluations. The assessment, which was based on the analysis of the data provided

by the framework relating to the client company, initially concerned only aspects relating to the Italian context as the main operational reference, and subsequently referred to the comparison of the requirements in European locations. This approach facilitated the verification of compliance with European regulatory requirements.

3. **Drafting of the Readiness Assessment Report**
   The critical issues and potential for each location examined by the client company were established, and a Readiness Assessment Report was subsequently drawn up, which clearly and in detail outlined the state of compliance found. The document included: a detailed analysis of the deficiencies identified, a summary of the results obtained, also relating to areas for improvement, and recommendations and indications that could help address and manage the problems identified and enhance the areas for development instead.

4. **Dissemination of results**
   The results of the analyses carried out were then shared with the client, through dedicated sessions. During these meetings, the findings were presented in a clear and detailed manner, supported by the collected documentation, and the strategies necessary to fill the gaps found and achieve compliance with the requirements were indicated. In summary, the objective was to support the company in defining a concrete action plan, based on targeted interventions capable of promoting the safety conditions of the system in the shortest possible time and guaranteeing its compliance with current regulations.

## 4.1 Framework Architecture

The *assessment framework* is a foundational document for the analysis of the company context, as it is structured in such a way as to provide clear and precise information for the collection of the necessary data. This framework for verifying the security conditions of the client company has been designed in a modular way, dividing the scope of analysis into six main macro-areas, in line with the main sections of the industry's best practices.

These macro-areas are then further categorised into thematic sub-areas, addressing specific safety aspects and containing specific controls that are defined in a clear and precise manner. The framework enables the accurate analysis of each control, facilitating the identification of gaps in the system and the determination of the degree of compliance with the requirements of NIS 2. Consequently, the implementation of necessary measures to enhance cyber resilience can be facilitated.

The specific areas and sub-areas of intervention of the framework are indicated below 4.1:

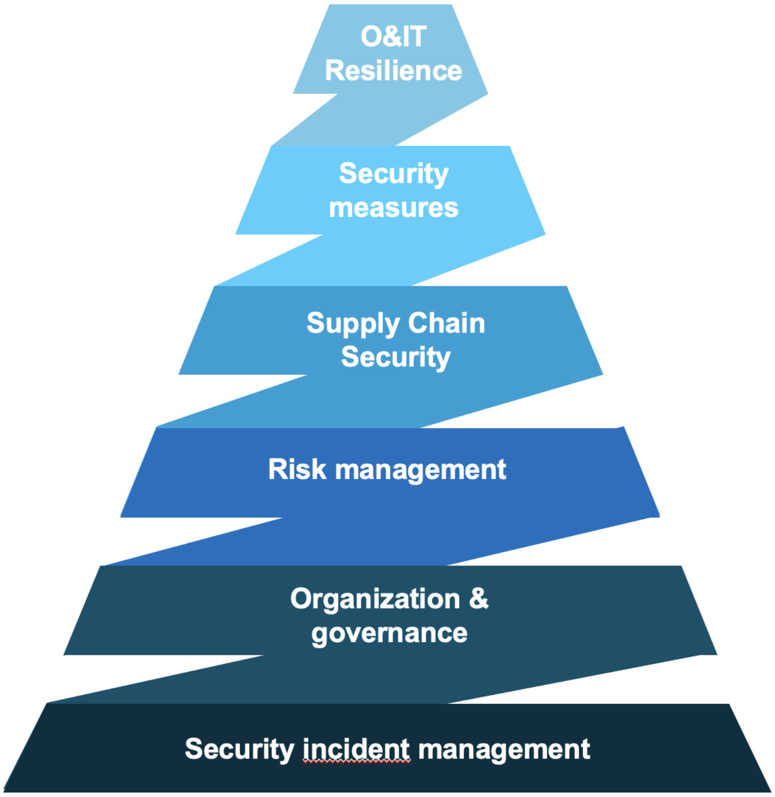


Figure 4.1. Focus Areas

### 4.1.1 The Areas

The areas and sub-areas are as follows:

1. **Operational Resilience and IT**: this concerns operational resilience and IT, backup processes, disaster recovery and operational continuity.
2. **Security measures**: this includes network control, cloud security, change management and logical and physical access management, criteria for logging and encryption systems and for asset protection.
3. **Supply Chain Security**: this assesses the security of critical suppliers and supply chain management processes, ensuring that they are aligned with security requirements.
4. **Risk Management**: this analyses risk assessment and treatment processes, vulnerability management and management involvement in threat management.
5. **Organisation & Governance**: which verifies the organisational structure, security policies, management of responsibilities and training and awareness processes.
6. **Security Incident Management**: which assesses incident management capabilities, including detection, response and reporting processes.

Each element of the framework control is directly associated with one or more requirements of the NIS 2 Directive, thereby ensuring that the framework does not function as a rudimentary self-assessment instrument, but rather as a structured, guided pathway to compliance.

## 4.2 Roll-out and sharing

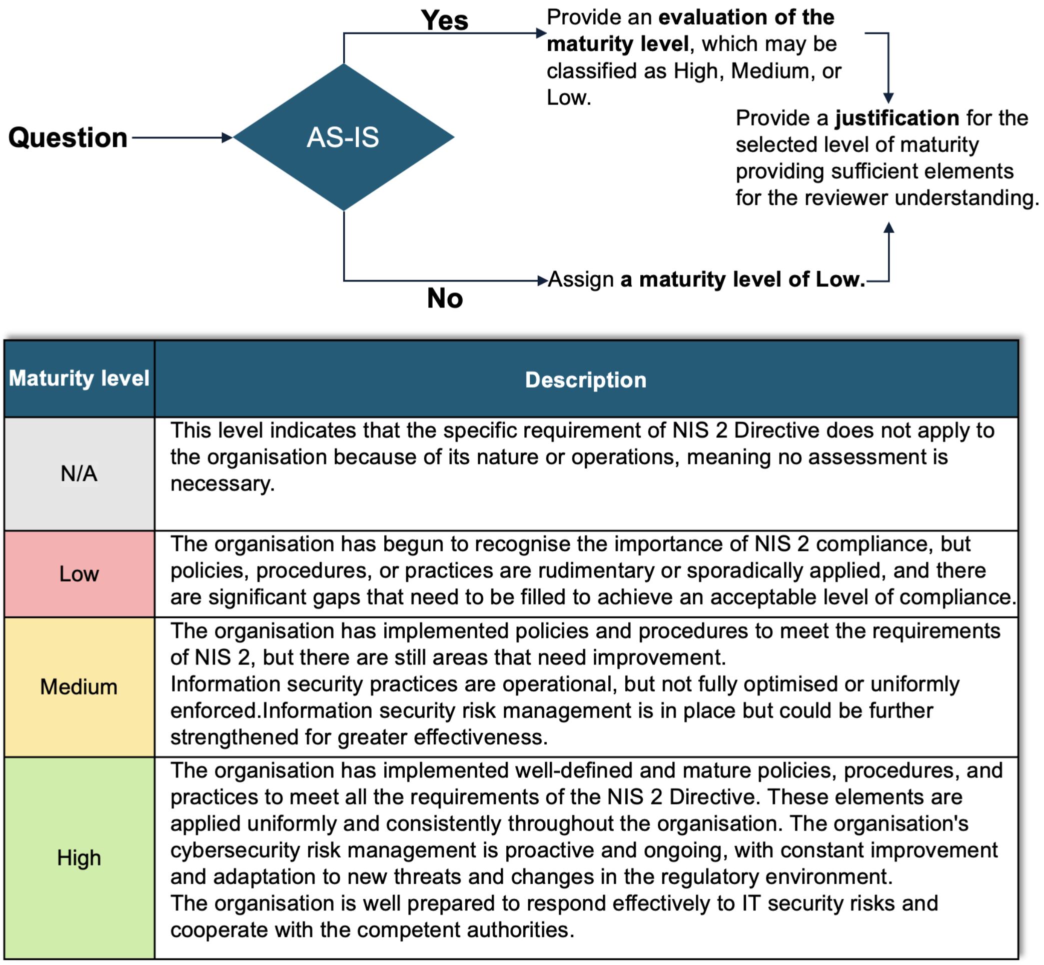
The outcome of the initial phase of development qualifies as a pivotal operational instrument that enables the client company to execute a legitimate self-assessment process.

The framework in this phase comprises the following:

- **Area**: the general category to which the control belongs.
- **Sub area**: a more specific sub-category within the main area.

- **Control number**: a numerical identifier assigned to each control.
- **Control description**: a detailed description explaining the content and purpose of the control.
- **Maturity level**: an indication of the level of maturity associated with the control, which can range from *Low* to *High*, providing an indication of the degree of implementation and compliance.
- **Justification**: a section dedicated to a brief description that motivates the indicated maturity level.
- **Evidences**: general documents necessary to demonstrate the implementation of the control.

The client is provided with instructions (Figure 4.2) for filling in the document and for facilitating the understanding of the various maturity levels:



Provide an **evaluation of the maturity level**, which may be classified as High, Medium, or Low.

Provide a **justification** for the selected level of maturity providing sufficient elements for the reviewer understanding.

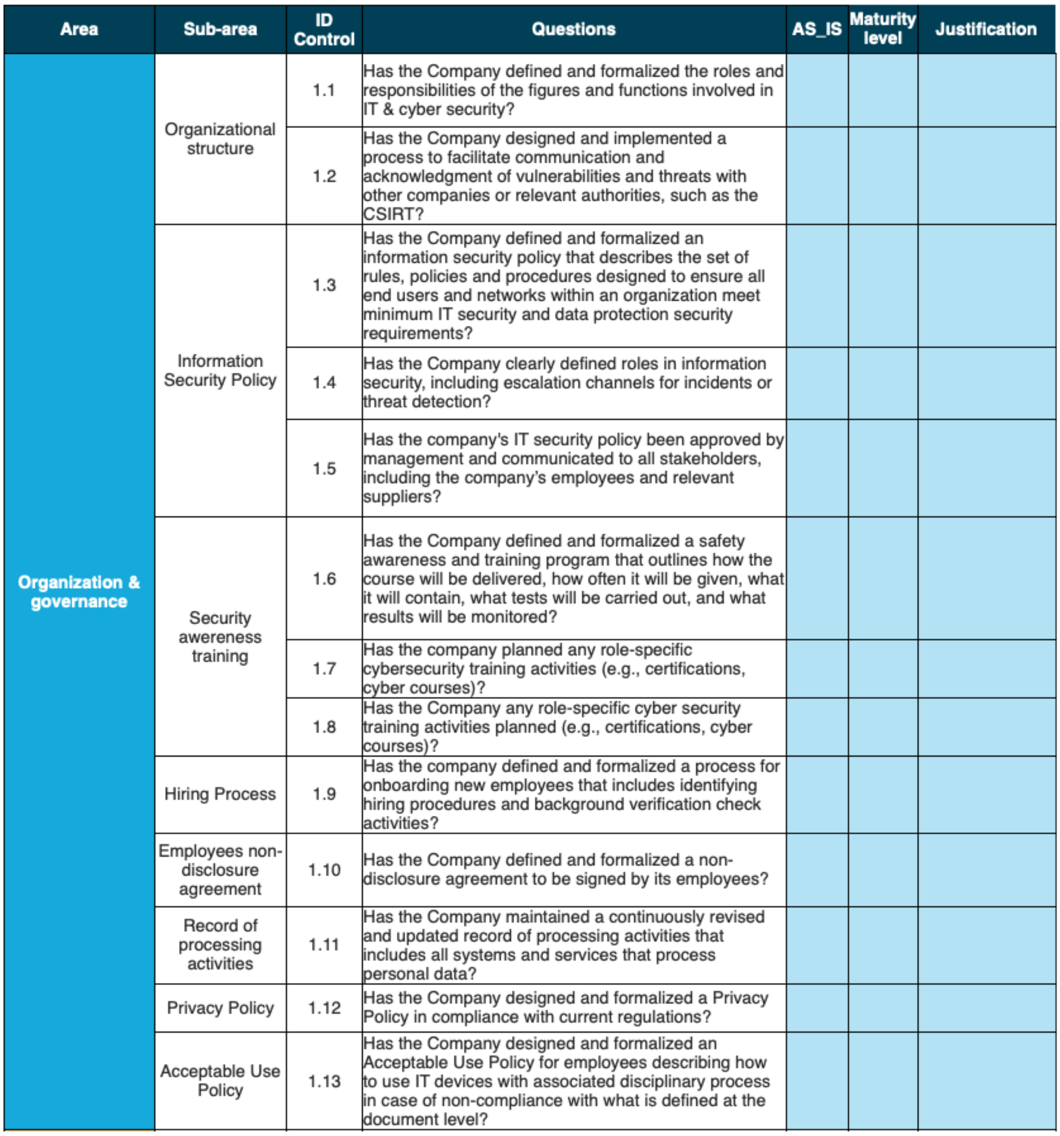
Assign **a maturity level of Low.**

| Maturity level | Description |
|---|---|
| N/A | This level indicates that the specific requirement of NIS 2 Directive does not apply to the organisation because of its nature or operations, meaning no assessment is necessary. |
| Low | The organisation has begun to recognise the importance of NIS 2 compliance, but policies, procedures, or practices are rudimentary or sporadically applied, and there are significant gaps that need to be filled to achieve an acceptable level of compliance. |
| Medium | The organisation has implemented policies and procedures to meet the requirements of NIS 2, but there are still areas that need improvement.<br>Information security practices are operational, but not fully optimised or uniformly enforced.Information security risk management is in place but could be further strengthened for greater effectiveness. |
| High | The organisation has implemented well-defined and mature policies, procedures, and practices to meet all the requirements of the NIS 2 Directive. These elements are applied uniformly and consistently throughout the organisation. The organisation's cybersecurity risk management is proactive and ongoing, with constant improvement and adaptation to new threats and changes in the regulatory environment.<br>The organisation is well prepared to respond effectively to IT security risks and cooperate with the competent authorities. |

Figure 4.2. Client Instructions

The investigation process was initiated with a focus on the Italian context, the client company's primary operational reference point, and was subsequently expanded to encompass the European offices, with the objective of ensuring compliance at an international level.

Below (Figure 4.3) is an extract from the **self-assessment framework** for the *Organization & Governance* area.



| Area | Sub-area | ID Control | Questions | AS_IS | Maturity level | Justification |
|---|---|---|---|---|---|---|
| Organization & governance | Organizational structure | 1.1 | Has the Company defined and formalized the roles and responsibilities of the figures and functions involved in IT & cyber security? | | | |
| | | 1.2 | Has the Company designed and implemented a process to facilitate communication and acknowledgment of vulnerabilities and threats with other companies or relevant authorities, such as the CSIRT? | | | |
| | Information Security Policy | 1.3 | Has the Company defined and formalized an information security policy that describes the set of rules, policies and procedures designed to ensure all end users and networks within an organization meet minimum IT security and data protection security requirements? | | | |
| | | 1.4 | Has the Company clearly defined roles in information security, including escalation channels for incidents or threat detection? | | | |
| | | 1.5 | Has the company's IT security policy been approved by management and communicated to all stakeholders, including the company's employees and relevant suppliers? | | | |
| | Security awereness training | 1.6 | Has the Company defined and formalized a safety awareness and training program that outlines how the course will be delivered, how often it will be given, what it will contain, what tests will be carried out, and what results will be monitored? | | | |
| | | 1.7 | Has the company planned any role-specific cybersecurity training activities (e.g., certifications, cyber courses)? | | | |
| | | 1.8 | Has the Company any role-specific cyber security training activities planned (e.g., certifications, cyber courses)? | | | |
| | Hiring Process | 1.9 | Has the company defined and formalized a process for onboarding new employees that includes identifying hiring procedures and background verification check activities? | | | |
| | Employees non-disclosure agreement | 1.10 | Has the Company defined and formalized a non-disclosure agreement to be signed by its employees? | | | |
| | Record of processing activities | 1.11 | Has the Company maintained a continuously revised and updated record of processing activities that includes all systems and services that process personal data? | | | |
| | Privacy Policy | 1.12 | Has the Company designed and formalized a Privacy Policy in compliance with current regulations? | | | |
| | Acceptable Use Policy | 1.13 | Has the Company designed and formalized an Acceptable Use Policy for employees describing how to use IT devices with associated disciplinary process in case of non-compliance with what is defined at the document level? | | | |

Figure 4.3. Client Framework

## 4.3 Readiness Assessment Report

Following the completion of the framework by the client, the team involved in the investigation initiated a comprehensive analysis to verify the completeness, consistency and adequacy of the responses with respect to regulatory and operational requirements. This analysis culminated in the formulation of a report. Each piece of information in the framework was examined to identify any inconsistencies or gaps, which were then discussed with the client. Where necessary, additions were provided to ensure a more precise and structured evaluation.

Based on this review, the framework was used as a basis for providing the client with a structured and timely report. The following sections were included in the document:

- **Maturity level assessment**: an assessment by the work team of the level of maturity associated with the control provided in the self-assessment phase

- **Assessment procedures**: the procedures used to assess the control, which may include document analysis, interviews and technical reviews.

- **Reference Documents**: the specific reference documents used for the control, such as previously provided guidelines or internal policies.

- **Improvement points**: the areas for improvement identified during the assessment.

- **Recommendation**: specific recommendations aimed at improving that specific business area.

Through the described process, it was therefore possible to identify the level of correspondence of the evidence provided with respect to the requirements indicated in the framework, the critical issues and the opportunities for improvement. The specific solutions were designed to align with national guidelines and the requirements of the NIS 2 Directive. The operational approach adopted proved effective, as it allowed the recommendations for improvement to be technically adequate. That is to say, the recommendations aimed to fill the gaps that emerged and strengthen the overall level of security and compliance.

## 4.4 Dissemination of results

The evaluation process of each of the implemented controls, carried out in collaboration with the IT manager of the client company, allowed the definition of the level of maturity achieved by the organisation in relation to its security system. This phase, described in the previous paragraphs, produced data based on concrete evidence, which was subsequently shared with the Company in order to provide it with valid support to redefine methods or strategies that presented critical issues or, on the other hand, to strengthen the areas for improvement identified.

The presentation of the results to the client was accompanied by graphic representations that facilitated a clearer and more immediate interpretation of the information contained in the document. These graphs will be illustrated below to better explain, through their structure and content, the role of facilitators they played in the client's process of understanding the information collected.

The first graph offers a comprehensive overview of the organisation's compliance with the entire set of checks conducted, illustrating the percentage distribution of maturity levels achieved in relation to all evaluated requirements. Through the balancing of these levels, the critical areas are identified.

The distribution analysis enables the customer to comprehend, with ease and in a timely manner, the quantity of evaluation results that have achieved low levels of maturity and therefore necessitate urgent intervention to address the identified gaps, and those that, in contrast, have attained medium or high levels and signify the implementation of correct practices. The correct interpretation of the data relating to the distribution of maturity levels enables the customer to identify the priorities on which to focus their intervention plan to enhance the overall level of compliance. The predominance of findings necessitates the implementation of specific actions, such as:

- **The predominance of the percentage relating to low maturity levels**: highlights the need to define and implement best practices to develop procedures and controls, aiming to increase security and compliance with current regulatory obligations.

- **A balanced distribution between low and high**: this presents potential margins for improvement while also demonstrating a solid operational foundation.

- **A high percentage of low levels**: indicates the presence of strong management of security systems and consolidated compliance with current regulations.

The subsequent graph *(Figure 4.4)* pertains to the method of data dissemination within the organisation, with the removal of specific data elements to ensure the confidentiality of Client information.

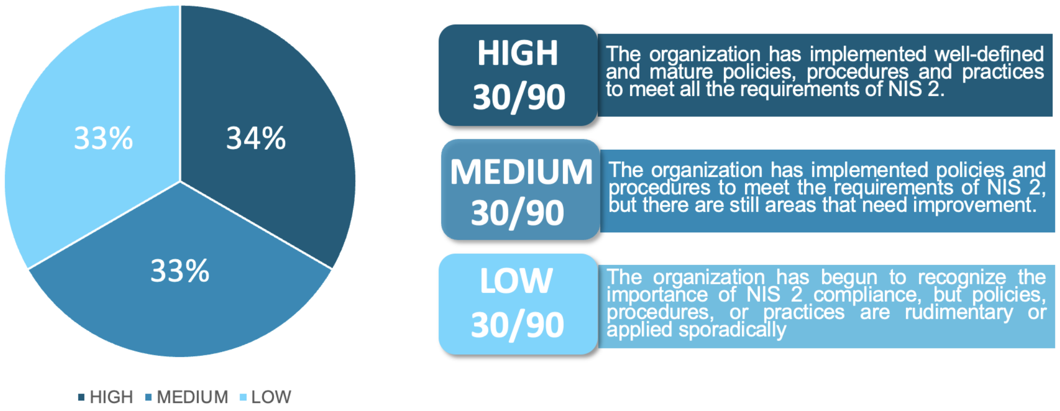


Figure 4.4. Distribution of maturity levels

The second graph *(Figure 4.5)* facilitates further analysis of the results produced by the first one above by allowing for the more specific sub-division of the levels of maturity achieved by the company into different control categories. This representation enables the client to examine in detail the specific areas in which there are critical issues or strong points and to quickly and specifically evaluate the strategies to be implemented.

Using these data, the customer can swiftly ascertain the extent to which the various operational areas contribute to achieving an adequate level of maturity. The graph enables the client to:

- Identify specific categories with low levels of maturity, necessitating urgent action to address compliance gaps and enhance safety.

- Identify categories with intermediate levels, which require action to optimise processes and practices, or even consolidate them.

- Ensure categories with a high level of maturity, where results are positive and interventions are managed appropriately.

The presentation of data divided by category is an effective method of sharing results with the client, who can easily obtain a comprehensive view of the situation through the graphic representation, allowing them to swiftly plan intervention strategies aimed at enhancement.

The graph below *(Figure 4.5)* relating to the method of sharing data with the company, is presented with some data omitted to ensure the confidentiality of the customer's information.

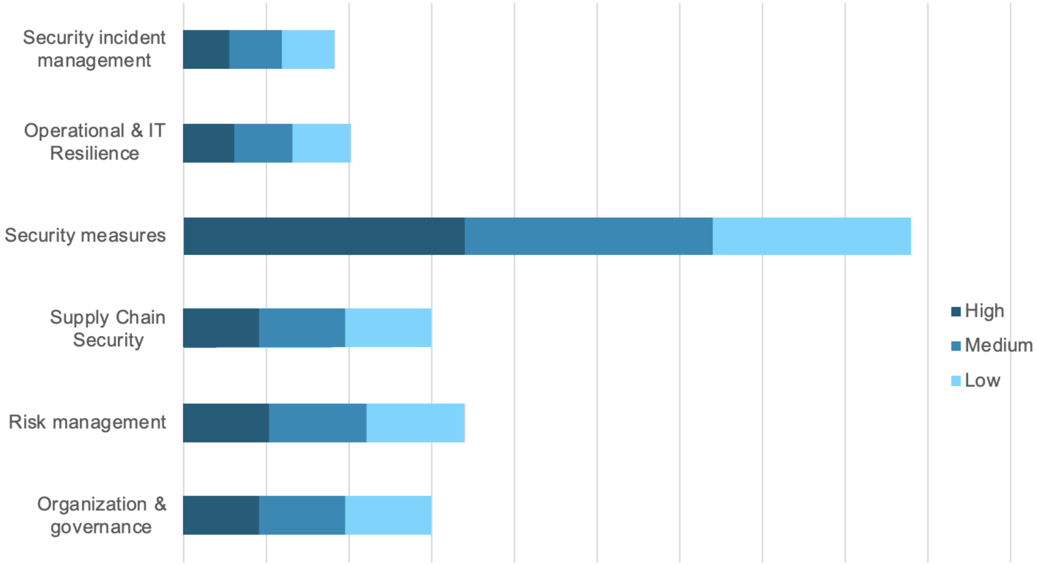


Figure 4.5. Detail of maturity by category

# Chapter 5

# Policy Review

As part of the analytical process, the interventions also included an in-depth examination of the data provided by the Client in relation to the set of cybersecurity regulations in order to verify their compliance with current obligations and, in case of any inconsistencies or gaps, to propose appropriate improvements.

## 5.1 Analysis of existing policies

Specifically, the analysis of the security policies used by the organisation under study has allowed the identification of several critical issues, some of which are listed below, by way of example:

- Non-compliance with the obligations established by the NIS Directive 2, which made it necessary to review and update existing policies in order to ensure compliance with the new provisions.

- The absence of standardised procedures, which are essential for the effective implementation of security measures at company level.

- The absence of a structured framework for risk management, necessary to promote the company's ability to respond proactively to cyber threats.

Following the clarifying discussion with the client, the mapping of the deficiencies detected was initiated, and subsequently, the definition of an intervention plan aimed at overcoming them was pursued.

## 5.2 Security Policies Development

In this phase, in order to support the organisation in its process of adaptation to the NIS 2 Directive, the work involved the development of a set of security policies, integrated with the leading practices in the sector.

The compliance policy encompasses all critical aspects of IT security and its implementation, offering companies the possibility of creating a governance framework with defined roles and responsibilities. In this specific case, the policy covered the following macro areas of intervention:

- **Governance and Risk Management**: Defines the procedures for establishing strategies and processes capable of identifying risks and implementing the necessary measures to mitigate them. Risk management, structured according to the methods indicated in the policy, promotes a proactive approach in IT infrastructure protection.

- **Protection of Assets and Information**: Outlines the criteria for secure data management through data classification procedures, regulation of access to critical resources, and the definition of practices for the secure disposal of IT assets.

- **Management of Third Parties**: Regulates the monitoring of suppliers and external collaborators to ensure that their security standards align with those adopted by the organisation. This procedure helps prevent potential vulnerabilities and reduces risks associated with third-party relationships.

- **Management of Vulnerabilities and Incidents**: Defines the necessary procedures for the timely identification of vulnerabilities and their resolution, if found. The implementation of the proposed practices allows for an effective response to security incidents, limiting their impact.

- **Protection of Communications and Data**: Describes the implementation of encryption mechanisms and backup procedures to ensure the integrity and availability of corporate information.

- **Continuous Monitoring and Improvement**: Establishes procedures to ensure that policies are regularly reviewed and updated to align with regulatory changes and the development of new cyber threats.

As can be deduced from the above, adopting a structured approach in these macro areas of intervention is crucial for the client company to enhance risk control and mitigation. Cybersecurity policies, therefore, represent essential tools for ensuring the protection of organisations' data and facilitating compliance with current regulations.

The aforementioned policies are reported below (Figure 5.1), by way of explanation.

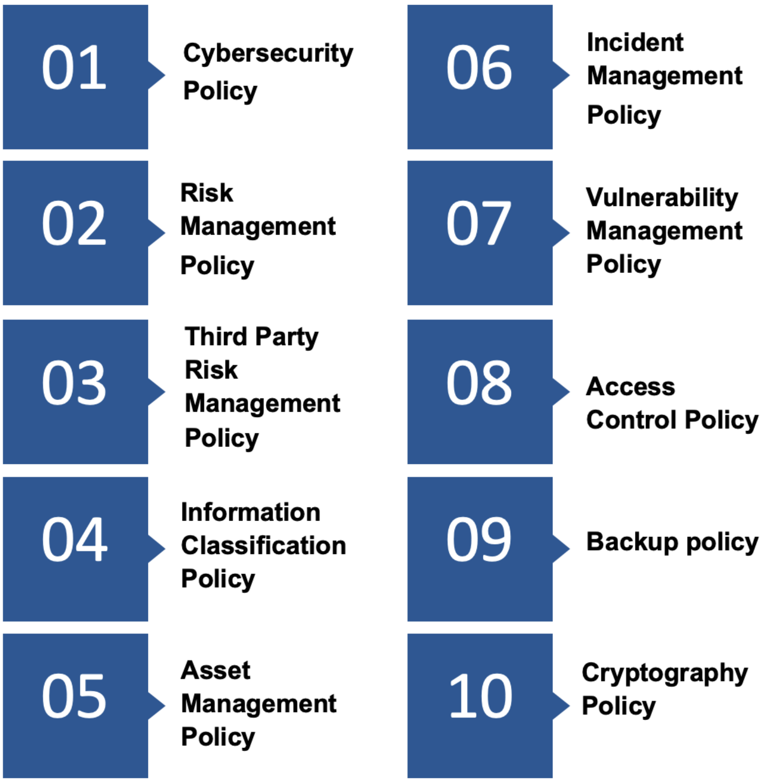

01 Cybersecurity Policy
02 Risk Management Policy
03 Third Party Risk Management Policy
04 Information Classification Policy
05 Asset Management Policy
06 Incident Management Policy
07 Vulnerability Management Policy
08 Access Control Policy
09 Backup policy
10 Cryptography Policy

Figure 5.1. Cybersecurity Policy

### 5.2.1 Cybersecurity Policy

This document is the main guideline, reference for the use and implementation of other corporate policies and for the definition of additional policies capable of ensuring corporate security. The Cybersecurity Policy has been explained and delivered to the corporate client to be used as a reference for the implementation of the procedures necessary to ensure the confidentiality, integrity and availability of corporate data in various aspects. This policy is a cornerstone of security and can be applied to all systems, people, and business processes.

#### Main Objectives

The specific objectives of the policy are:

- Define roles and responsibilities for information protection.
- Establish practices to prevent unauthorized access to data and systems.
- Ensure compliance with applicable regulations.
- Provide a *framework* to protect the confidentiality, integrity and availability of corporate information.

#### Security Policy Framework

The document is divided into a number of sections covering the main topics listed below:

1. **Introduction and Purpose**: Emphasizes the importance of the *policy* and outlines the regulatory context to which it relates.
2. **Policy, Procedures, Guidelines**: Clarifies and outlines what can be identified as acceptable practices and appropriate procedures for security management.
3. **Scope**: Defines what may be included in the *policy*.
4. **Roles and responsibilities**: Describes what may be the key functions for implementing and monitoring the *policy*.

The IT Security Policy can be seen as a key tool for managing the following critical business processes:

- **Human Resources Security**: Provides guidance to ensure the training, information, and safety of personnel by promoting the reduction of risks that may be identified in personnel management procedures.
- **Physical and Environmental Security**: Provides guidance on protecting the organization's information systems from unauthorized access and/or natural disasters.
- **Business Continuity Management**: Provides plans and strategies to protect activities from disruption in the event of unforeseen events

This is followed by a detailed description of the *corporate policies* mentioned above, highlighting their objectives and main components.

### 5.2.2 Risk Management Policy

The **Risk Management Policy** establishes the basic principles for identifying, assessing, mitigating and monitoring all information security risks, and is thus described as fundamental to ensuring the protection of business objectives.

#### Main Objectives

The main objectives of the Risk Management Policy are listed below:

- Implementation of strategies, structured processes of risk management, including the identification of risks, their assessment and treatment for the purpose of resolving the issues highlighted.
- Periodic audits and assessments of information systems to ensure data protection, integrity and confidentiality.
- Ongoing updating of its standards so that they can be aligned with international standards and *best practices*.

#### Risk assessment and management

Information systems should always be periodically audited to identify any risks associated with business processes. Identified risks must be contained, avoided or even possibly accepted and contained with strategies that can be defined based on the results of the assessments performed.

### 5.2.3 Third Party Supplier Management Policy

The purpose of the **Third Party Supplier Management Policy** is to define the policies and processes necessary to identify, assess, and mitigate risks associated with third party suppliers that interact with the company's systems by sharing practices and information.

#### Main Objectives

The purpose of the Third Party Supplier Management Policy is to:

- Identify and assess supply chain risks through a dedicated working group and operational process.
- Implement controls to prevent and/or mitigate supplier-related cybersecurity risks. Procedural activities include, for example, those related to:
  - Planning and identifying third parties that interact with the company.
  - Ongoing monitoring and management of offboarding steps.
  - Establishing confidentiality agreements and information management procedures to secure contracts with suppliers.

#### Risk Assessments and Monitoring

To implement effective risk monitoring and assessment, it is important to establish risk management criteria. All suppliers interacting with the Client company are evaluated and ranked according to the level of risk they represent on a scale of 1 to 4, taking into account some specific parameters, such as:

- the sensitivity of the data they manage.
- the frequency of compliance audits performed.
- the security measures implemented.

Assessments are based on frameworks such as *NIST 800-53* and include internal and technical audits.

### 5.2.4 Information Classification Policy

.

The **Information Classification Policy** deals with the classification of business data based on its value, the sensitivity of the content being processed, or what has been identified as critical risk issues. Based on the assessment, a structured *framework* for data management and protection is defined.

#### Main Objectives

The key objectives can be summarized in the objectives below:

- Classify business data to determine appropriate levels of protection, taking into account the categories to which it belongs and which it may belong:
  - **Public**: Public information that does not require restrictions because it is not subject to any form of confidentiality.
  - **Internal**: Internal information that, because it is not characterized by confidential data, may have minimal impact in the event of disclosure.
  - **Confidential**: Sensitive information that, as such, is confidential and therefore access to it is restricted to authorized users.
  - **Restricted**: Highly sensitive information that can only be accessed through regulated access on a *need-to-know* basis.
  - **Personal Information**: Characterized by personal data that requires a high level of protection in accordance with the provisions of privacy legislation.
- Ensure that security controls are proportionate to the level of sensitivity assigned to the data.
- Manage business standards information in compliance with regulations.

#### Data Governance Roles

This policy assigns specific roles to those involved in information management, such as:

- **Data Owner**: One who is assigned responsibility for classifying, protecting, and managing corporate data.

- **Data Controller**: The person responsible for overseeing data handling processes to ensure compliance.
- **Data Processor**: The person responsible for the operational management and protection of information.
- **Data Custodian**: One who is responsible for the technical management of data through backup, protection, and secure destruction activities.
- **Authorized User**: The person responsible for compliance with classification and security policies.

### 5.2.5 Asset Management Policy

La **Asset Management Policy** is responsible for defining the use of *technological assets* by defining them at all stages, from their acquisition to their disposal. It is responsible for ensuring the protection and traceability of assets in order to guarantee the effective management of the Client company's technological assets.

#### Main Objectives

The purpose expressed above is expressed through the implementation of the following procedures:

- Implement a structured programme that regulates the life cycle of technological assets, their acquisition, their use, the maintenance they require and finally their disposal.
- Ensure the traceability of the *assets* through an updated and detailed inventory.
- Implement risk mitigation strategies to protect the *assets* against risks such as theft, unauthorised access or data loss.

#### Asset Lifecycle Management

The management program for *assets* shall cover all phases of their life cycle and shall therefore address various aspects such as:

- **Procurement e provisioning**:Technology assets must be formally approved before they are purchased and must be traceable through tools such as the Configuration Management Database (CMDB).
- **Inventory**: The asset must be registered with established and detailed criteria considering, for example, its traceability, owner information, compliance data, etc.
- **Acceptable Use**: The users authorized to access the asset shall be identified and the procedures by which they may use it shall be specified.
- **Maintenance and monitoring**: The asset shall also be monitored by automated systems capable of ensuring its integrity and compliance.

### Disposal and destruction of assets

With respect to the disposal of *assets* containing sensitive data, it is important that procedures are in place in order eliminate the risk of data dissemination. Measures may include:

- The sanitization of storage media to eliminate sensitive data.
- The physical destruction of *assets* using techniques such as shredding, disintegrating, or degaussing.
- The certification of destruction by authorized vendors.

### 5.2.6 Incident Management Policy

The **Incident Management Policy** defines the process for managing cybersecurity incidents by identifying appropriate strategies that, through timely and effective response, can minimize the negative impact they may have on technology assets and corporate data.

#### Main Objectives

In particular, this policy seeks to:

- Establish a structured incident management program that includes reporting, containment, criticality assessment, and eventual recovery..
- Ensure a rapid and orderly response to incidents, including identification of additional unauthorized access.
- Establish criteria for action consistent with privacy regulations, such as timely notification of appropriate authorities in the case of significant incidents.

#### Incident Management

The program shall cover all phases of incident response, including:

- **Preparation**: Establishing detailed plans and procedures for incident management.
- **Identification and Detection**: Continuously monitor the situation and identify any critical issues.
- **Containment**: Implementing appropriate action strategies to contain the growth of the incident.
- **Eradication and Recovery**: Identify and remediate the possible causes of the incident.
- **Lessons Learned**: Evaluating the post-incident dynamics put in place to improve future processes.

### Incident Management Roles

Identifies individuals with specific incident management responsibilities:

- **Cyber Incident Response Team (CIRT)**: Responsible for incident coordination and management, working with internal and external support teams.
- **Core Team**: Manages high severity incidents.
- **Extended Team**: Supports the Core Team and focuses on minimizing business impact during the incident.
- **Business Continuity Coordinator**: Has the authority to activate the Business Continuity Plan when deemed necessary.

### Notification and Reporting

All incidents must be reported promptly according to agreed criteria and mechanisms. The *CIRT* is responsible for reporting incidents to the appropriate authorities. Each incident must be documented and evaluated in order to identify improvements in any new response processes.

### 5.2.7 Vulnerability Management Policy

The **Vulnerability Management Policy** defines the procedures necessary for the identification, assessment, management, and remediation of vulnerabilities found in enterprise systems. Its purpose is to ensure the security of corporate information.

#### Main Objectives

In order to ensure the security of corporate information, the vulnerability management policy shall achieve the following objectives:

- Plan a structured criticality and vulnerability management program that includes periodic testing of access to security systems.
- Identify and mitigate discovered vulnerabilities in a timely manner.
- Establish remediation priorities for critical issues based on their vulnerability and negative impact on the business system.

#### Vulnerability Management Program

The vulnerability management program shall include the following activities:

- **Vulnerability Scan**: The Cyber Defense Operations Manager will ensure that periodic audits are conducted to identify any critical issues with enterprise assets such as IT, web applications, and database configurations.
- **Penetration Testing**: Security Assessment Managers are responsible for performing penetration tests and other assessments and providing appropriate reports to explain identified vulnerabilities.
- **Results Management**: Identified vulnerabilities should be reported to asset owners on a regular basis, with automated reports.

#### Vulnerability remediation

Vulnerability management involves various risk mitigation activities, such as:

- **Patch e Updates**: The periodic updating of operating systems, databases, and applications with identified and approved patches.

- **Configuration Changes**: hanging the configuration of asset when vulnerabilities are found.
- **Source Code Modification**: The correction of application code that is deemed inadequate.
- **Remediation Prioritization and Planning**: The implementation of systematic compensating controls when it is not possible to modify the configuration found to be vulnerable.

### Prioritisation and planning of remediation

Vulnerabilities found should be ranked according to their CVSS score, which determines their priority for remediation. For those considered serious and urgent critical issues, the *Product Manager* coordinates immediate action. The execution of the remediation plan is monitored by the *Cyber Defense Operations Manager*, who validates the possible resolution of vulnerabilities and/or coordinates any new scans. The *Product Manager* and teams involved in remediation must ensure that the resources needed to resolve critical issues are available, including requesting support from external vendors and teams as necessary.

### 5.2.8 Access Management Policy

The **Access Management Policy** establishes the policies that govern the control of access to corporate systems to ensure data security. It is responsible for defining what the access criteria should be and what actions should be taken against any unauthorized access.

#### Main Objectives

The main objectives to be achieved include:

- Manage corporate resources so that only authorized users can access data and systems.
- Establish an access management plan that governs access from enrolment to revocation.
- Establish secure and compliant authentication methods that ensure the protection of corporate data.

#### Access Management

The management program shall cover various aspects related to the management of user access to data and shall therefore establish criteria for:

- **Authentication and credential management**: Authentication and credential management must be carried out correctly. For example, it would be advisable for users to use a unique ID and a secure password.
- **Authorization and controls based on business needs**: Access to business resources should be authorized only for specific needs that are justified and approved by managers.
- **Monitor and review access**: Access should be monitored regularly to detect any anomalies, and access rights should be reviewed periodically (every 180 days).

#### Exception and privilege management

Permissions to access restricted areas are governed by specific rules and granted only to authorized personnel or with valid justification. Access to critical systems, such as databases and network devices, is subject to validation and control. This privileged access must be protected by advanced authentication methods, such as multi-factor authentication.

### 5.2.9 Backup Management Policy

The **Backup Management Policy** defines the policies for protecting and restoring corporate data, ensuring that the necessary information is available in the event of an emergency. The *policy* defines the roles and responsibilities and the processes required to ensure that data is regularly backed up and can always be quickly recovered and used.

#### Backup Management Roles

- **Backup Operations Manager**: Responsible for overseeing the backup management process, approving exceptions to the policy, managing backup configurations, and evaluating the effectiveness of backups based on data criticality. They are also responsible for classifying systems and identifying potential recovery targets.

#### Main Objectives

The actions and operational objectives of this policy include the following:

- **Data Protection and Recovery**: Ensure the rapid protection and recovery of critical business information to enable business continuity and minimize the negative impact of incidents.

- **Definition of Responsibilities**: Assign responsibility for overseeing the backup process, managing configurations, and approving any exceptions to the policy.

- **Regular Planning and Monitoring**: Ensure that backups are performed with established and appropriate schedules to avoid disruption to business operations.

- **Continuous Testing and Updating**: Perform regular updates to backup and recovery plans to maintain their effectiveness.

- **Risk Assessment and Impact Analysis**: Implement measures to adapt backup strategies to technological advances.

- **Secure Backup Management**: Design a storage strategy with local, cloud, and immutable solutions to protect corporate data from risks posed by system failures or, for example, *ransomware* attacks.

- **Respond effectively to incidents**: Integrate rapid response strategies into backup plans to ensure timely recovery.

### 5.2.10 Encryption Policy

The **Encryption Policy** establishes guidelines to ensure that sensitive data is protected by encryption in accordance with regulations.

#### Main Objectives

- Protect sensitive data by using encryption so that only authorized users can read it.
- Securely manage encryption keys and provide robust protection and recovery systems in the event of loss.
- Ensure compliance with applicable regulations regarding the use of encryption, key management, and privacy.
- Implement encryption protection solutions for data in transit, at rest, and on mobile or removable devices.
- Ensure the security of facilities that manage public keys, digital certificates, and sensitive information.

## 5.3 Presentation of Results

In the final phase of the process, the results were presented to the client. This was done in order to provide the client with a clear and detailed description of the results obtained. It was also done to make the client aware of the level of compliance achieved by the company with the regulatory requirements of the NIS 2 Directive.

During the presentation, the necessity for a periodic review of all security policies adopted by the organisation was emphasised, with the aim of guaranteeing their effective application over time. It was also specified that in the absence of significant changes to the regulations or to the company's information systems, this review can be carried out only once a year. However, in the event of significant changes, such as the introduction of new technologies, regulatory updates or the emergence of new cyber threats, a timely update is essential to ensure continuity of protection and compliance.

In order to facilitate the implementation of the aforementioned procedures, a structured policy review and update process was proposed to the Client Company. This process included the appointment of a team dedicated to managing verification activities, the use of monitoring tools to detect any need for adjustment, and the definition of an effective action plan for the implementation of any necessary changes.

The observations that emerged were discussed directly with the client during a scheduled meeting, which allowed for the clarification of any doubts and the planning of an effective path for compliance.

The discussion proved successful in raising the customer's awareness of the importance of proactive IT security management and the need to continuously update the measures adopted in order to adapt to the evolution of the regulatory and technological context.

# Chapter 6

# Security Measures Implementation

## 6.1 Introduction

The implementation of security measures is imperative to ensure the protection of company systems and compliance with current cybersecurity regulations. However, for these measures to be effective, it is essential that the organisation develops an adequate awareness of cyber risks and mitigation strategies.

In the context of the project, preliminary indications were provided to the client to increase their knowledge of the main cyber threats and good security practices. In particular, the sharing of so-called 'digital pills' was proposed: short informative contents focused on key aspects such as credential protection, physical and digital security, 'phishing' and other common threats. The objective of this initiative was to furnish practical tools to enhance corporate security, thus facilitating future implementation of the necessary measures.

## 6.2 Implementation of security measures

In addition to the provision of information material, the customer was offered the possibility of receiving dedicated support in the subsequent phases of implementation of the security measures. This support could include various activities aimed at strengthening the organisation's security posture and ensuring adequate protection of information systems. The following activities were identified:

- **Definition of business continuity plans**: provision of assistance in formulating strategies to ensure the resilience of business systems in the event of cyber incidents or critical events.
- **Organisation of tests and simulations**: planning of activities to evaluate the effectiveness of the security measures adopted, such as simulations of cyber-attacks or exercises in response to incidents.
- **Technical identification of areas for improvement**: analysis of vulnerabilities and suggestions on possible corrective actions to increase the level of security.

In summary, the measures proposed and the approach adopted so far have laid the foundations for future support in the integration of more advanced protection strategies, helping to strengthen the organisation's awareness and improve its cybersecurity preparedness.

# Chapter 7

# Conclusion

## 7.1 Objectives Achieved

The principal purpose of the analysis conducted during the case study and illustrated in this document was to outline operational tools and strategies capable of clearly and effectively supporting organisations, specifically the Client Company, in their process of adaptation to the provisions of the NIS 2 Directive. In fact, the aim was to provide valid content and skills to encourage a structured approach to the evaluation and implementation of security measures. A thorough examination of the indications, prescriptions and obligations of NIS 2, and their application, was conducted, followed by an analysis of the cybersecurity best practices of the organisation under investigation.

Ultimately, an evaluation framework was developed, serving as a practical instrument for assessing the maturity level of companies in relation to the requirements, identifying any existing gaps, and proposing suitable improvement strategies. The primary interventions that were implemented can be outlined as follows:

- **Analysis of current legislation**: this involved an in-depth analysis of the content of the NIS 2 Directive and Legislative Decree no. 138 was carried out to understand the possible operational implications of their provisions for companies.
- **Definition of an assessment framework**: We proceeded to create a framework, a structured tool capable of allowing the detection of the level of compliance of companies with regulatory requirements.
- **Assessment of the level of maturity**: Using the aforementioned framework, the company security processes were evaluated, identifying

the critical aspects of the system, but also its strong points and possible areas of improvement.

- **Preparation of a Readiness Assessment Report**: The results obtained were then summarised in a detailed report, which highlighted the critical issues encountered and provided concrete recommendations for improving their security system.

- **Review and integration of company policies**: During the process, existing policies were analysed and additions deemed necessary to bring them into line with regulatory standards were proposed.

- **Awareness and training**: To help raise staff awareness of cybersecurity risks, training tools such as *digital pills* were proposed.

The approach adopted has facilitated a systematic management of cybersecurity concerns, thereby ensuring the client receives support from tangible tools that can enhance the security level of the company and ensure compliance with regulatory obligations.

## 7.2 Future Development of the Framework

The creation of several tools for the assessment and mitigation of cybersecurity risks is projected, and the framework will undoubtedly be a significant component of this. The framework is currently employed to evaluate and ascertain the maturity of cybersecurity, and its utilisation may be expanded and refined in the near future. Potential developments of the framework may pertain to the following processes:

- **Automation of the assessment process**: the integration of additional software tools with the framework could allow for a faster and more accurate analysis of the collected data, reduce the margin of error and facilitate data management.

- **Continuous updating**: as has been repeatedly emphasised in this paper, cybersecurity is a constantly evolving sector. Therefore, the framework needs to be updated periodically in order to include any new regulatory requirements and emerging best practices.

- **Adaptability to different industrial sectors**: the framework utilised in the present analysis was developed with consideration for the provisions of the NIS 2 Directive. However, it possesses the potential for expansion through interactions that respond to the indications of other regulations, such as the Digital Operational Resilience Act (DORA) specific to the financial sector.

- **Integration with monitoring systems**: combining the framework with additional security monitoring tools could enable an effective approach to cyber risk management.

## 7.3 Further Development of the Work

In addition to the interventions aimed at improving the framework, as described above, there are other areas of research and development that could be investigated in the future and used to increase the effectiveness of interventions in favour of cybersecurity. The following section outlines some of these areas:

- **Comparative analysis with other cybersecurity models**: a comparison between the developed framework and other international models could facilitate a comprehensive study of the differences and provide valuable insights for the development of more effective application strategies

- **Study on the effectiveness of the security measures adopted**: a well-organised collection of data on companies that have implemented the suggested measures could allow for a greater understanding of the effectiveness of the security strategies adopted.

- **Development of operational guidelines for companies**: the creation of a manual with a detailed description of valid processes for the implementation of security measures could support organisations in the process of adapting to the NIS 2 Directive.

- **In-depth study of legal and regulatory aspects**: taking into account the sudden evolution of cybersecurity regulations, continuous updating and detailed analysis of the legal implications for companies governed by the regulations could be beneficial.

## 7.4 Final Conclusions

The present thesis delineates a methodical approach to achieving and maintaining the requisite levels of compliance with the NIS 2 Directive. The proposed process is substantiated by concrete exemplars, and it is argued that the adoption of a structured assessment and the implementation of adequate security measures is a fundamental step in strengthening the cyber resilience of companies.

Despite the issuance of significant amendments and the attainment of substantial operational outcomes over the years, cybersecurity concerns persist as a primary issue for all organisations. Cybersecurity is an ever-evolving field, necessitating unwavering dedication to address the perpetual threat landscape and ensure the continuous updating of provisions to align with emerging regulations. The present paper proposes a process that, if expanded and improved over time, could contribute to the development of increasingly effective tools and action strategies for the protection of critical infrastructures and company data.

This research is not limited to providing technical and regulatory solutions, but also promotes a vision of cybersecurity as a strategic element for the growth and security of organisations.

# Bibliography

[1] Australian Cyber Security Centre. Bulletproof hosting providers, 2024. URL: https://www.cyber.gov.au/about-us/view-all-content/publications/bulletproof-hosting-providers.

[2] Kurt Baker. The zeus trojan malware - definition and prevention, 2023. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/malware/zeus-malware/.

[3] CERT-EU. About us. Accessed: 2025-02. URL: https://cert.europa.eu/about-us.

[4] CINI Cybersecurity National Lab, CIS-Sapienza. Framework nazionale per la cybersecurity e la data protection, February 2019. URL: https://www.cybersecurityframework.it/sites/default/files/framework2/Framework_nazionale_cybersecurity_data_protection.pdf.

[5] European Commission. Commission recommendation of 6 may 2003 concerning the definition of micro, small and medium-sized enterprises, 2003. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32003H0361.

[6] Council of the European Union. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, 2008. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008L0114.

[7] G.Dance E.Macaskill. Nsa files decoded: Edward snowden's surveillance revelations explained. *The Guardian*, November 2013. URL: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded.

[8] European Parliament and Council. Regulation (eu) 2016/679 of the european parliament and of the council, April 2016. URL: https://gdpr-info.eu.

[9] European Parliament and Council. Directive (eu) 2022/2555 of the european parliament and of the council, December 2022. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555.

[10] European Union Agency for Cybersecurity (ENISA). Implementation guidance on security measures, October 2024. URL: https://www.enisa.europa.eu/sites/default/files/2024-11/Implementation%20guidance%20on%20security%20measures_FOR%20PUBLIC%20CONSULTATION.pdf.

[11] Repubblica Italiana. Decreto legislativo 4 settembre 2024, n. 138, 2024. Gazzetta Ufficiale della Repubblica Italiana, Serie Generale n. 230 del 1° ottobre 2024. URL: https://www.gazzettaufficiale.it/eli/id/2024/10/01/24G00155/SG.

[12] Council of Europe. The budapest convention on cybercrime, 2001.

[13] European Parliament and Council of the European Union. Regulation (ec) no 460/2004, 2004.

[14] John Shier. Report cyberthreats: A 20-year retrospective. Technical report, Sophos, December 2020. Senior Security Advisor, Sophos.

[15] Sophos. The state of ransomware 2023, 2023. Whitepaper.