**NIS PLATFORM**

**WG1-CHAPTER1** **FINAL DRAFT 220515**

# NETWORK AND INFORMATION SECURITY RISK MANAGEMENT ORGANISATIONAL STRUCTURES AND REQUIREMENTS

# Table of Contents

## 1. INTRODUCTION

The Cybersecurity Strategy for the European Union was established in 2013.The Network and Information Security Platform (NISP), is a platform of European public and private stakeholders to identify good cybersecurity practices for security of information and communication technologies (ICT), creating favourable market conditions for the development and adoption of secure ICT solutions.

Businesses and public administrations need to invest in Network and Information Security (NIS) to protect their key assets and ensure the continuity of the services they provide. As a starting point, they should implement proper risk management processes, including dynamic risk assessment and risk mitigation, but also participate in the exchange of information on threats and vulnerabilities while recognising the potential benefit of collaboration in incident response. These practices are essential safeguards to cope with a rapidly evolving threat and technology landscape. The adoption of collaborative risk management processes will largely determine the development and the adoption of secure information systems.

As a first objective, the NISP focused on fostering the adoption of effective risk management practices. Businesses and public administrations are often unaware of the actual level of cybersecurity risks they face. Many of them rely solely on deploying basic ICT security solutions, an approach that has been repeatedly proved to be inadequate.

The NISP has addressed a number of questions in relation to the identification and the implementation of risk management practices, including:

- Whether a sector by sector and/or a horizontal approach should be followed when identifying such practices; while some practices may apply across sectors, others may prove relevant only in certain sectors, due to sector specificities or criticality.

- How to ensure a high level of cybersecurity in complex value chains and ecosystems, encompassing many interconnected players and strongly interlinked information systems.

- How to remove the barriers to the adoption of risk management practices and help less advanced stakeholders to progressively increase their level of NIS; whether the use of a Capability Maturity Model, guiding entities to progressively improve their risk management processes, would prove useful in this regard.

- How to raise awareness and obtain C-level engagement.

- Whether minimum security requirements could be identified to help companies and administrations counter basic threats, on which a large part of successful breaches are based, while serving as a basis to progressively implement more sophisticated risk management practices.

- How to build innovation in risk management to be able to cope with the changing nature of threats and permanent technological evolutions.

- Whether cybersecurity risk management should be addressed as a standalone function or as part of business risk management/business continuity and what should be the interplay between the business and cyber risk management frameworks.

The NISP recommendations on risk management aim to help companies and public administrations to increase their preparedness and cooperate more effectively, thereby enhancing cyber resilience in the EU. The outcomes of the NISP will feed into further work led by the Commission with ongoing industry and public sector cooperation to develop recommendations on cybersecurity.

The NISP will complement and underpin the proposed NIS Directive. In particular, it will help companies and public administrations to implement best practices for collaborative risk management and incident notification activities.

The NISP will develop economic, legal and technological incentives at international, EU, national and sectorial levels to adopt risk management practices and adopt secure information systems. Incentives are needed to motivate the decision of businesses and administrations to improve their cybersecurity capabilities beyond immediate enterprise business and operational considerations. This is important for increasing the overall level of cybersecurity in a fully interconnected world. By contributing to creating a stable and harmonised demand for secure ICT solutions and risk mitigating technologies, incentives for end-users will also foster R&D investment and innovation by ICT suppliers.

The Guidelines may be reviewed in light of the practical implementation experience in Member States.

## 2. SCOPE AND OBJECTIVES

### 2.1. Objectives

The Guidelines have the following objectives:

(1) to identify and facilitate the up-take of risk management practices, including standards, to enhance cybersecurity; such practices should be process-related and technology-neutral;

(2) to support organisations to further build up awareness about the strengths and potential weaknesses of their risk management system, to identify good practices, and to initiate a process of improvement;

### 2.2. Scope of the Guidelines

In general, the NISP addresses the following areas:

- Organisational measures: Defining practices, guide or evaluate an organisation's cybersecurity, specifically its capability to identify, assess and mitigate cybersecurity risks, and to deter and handle incidents.

- Secure products and services: practices to demonstrate the ability of products or services to provide a "good" level of cybersecurity performance as part of the ICT value chain.

- Metrics, measurement and language / taxonomy for cyber risk: practices for measuring, describing and evaluating cyber risks, impacts, threats, controls, etc.

- Information exchange: practices for the exchange of cyber incident information, to allow cyber incident reports to be understood and acted upon in the framework of complex cooperation schemes; to facilitate a high level view of all cyber incidents which facilitates spotting trends and directing resources.

- Cybersecurity resources: practices to manage and develop cybersecurity knowledge, skills and resources within an organisation or a sector.

In particular, this Commission notice gives publicity to the first outcomes of the NISP on organisational structures and requirements for risk management.

The guidelines will highlight existing risk management standards and best practices that organisations, depending on their size and needs, can use and tailor to their own approach to risk management. Where possible, it is recommended that international standards are applied. These provide organisations with a structured and proven way to implement and manage risks and security controls, as well as providing the organisation with confidence in the security measures that are in place.

The NISP should continue to develop economic, legal and technological incentives at international, EU, national and sectorial levels to adopt risk management practices and adopt secure information systems. Incentives are needed to motivate the decision of businesses and administrations to improve their cybersecurity capabilities beyond immediate enterprise business and operational considerations. This is important for increasing the overall level of cybersecurity in a fully interconnected world. By contributing to creating a stable and harmonised demand for secure ICT solutions and risk mitigating technologies, incentives for end-users will also foster R&D investment and innovation by ICT suppliers.

### 2.3. The Guidelines

These guidelines enumerate some existing risk management standards and best practices that organisations, depending on their size and needs, can use to tailor their own approach. It addresses the need for each organisation to establish links between cybersecurity risk management and the overall risk management/continuity plan of an organisation, how to identify the level of risk that an organisation is ready to live with. It also looks at maturity frameworks that organisations might want to use in continuously assessing and improving their approaches. It illustrates how national standards relate to international standards.

Today there is a great variety of organisations that are putting in place cybersecurity risk management approaches. One of the challenges is how to come to a common understanding and application of risk management frameworks across the value chain and across sectors.

## 3. METHODOLOGY

### 3.1. Organisation of NISP

The NISP is an inclusive and multi-stakeholder endeavour, aiming to mobilise goodwill and energies to deliver increased cybersecurity in Europe. The NISP is structured between:

- Plenary meetings, composed of senior government and company representatives, held two to three times a year and aimed at steering the work of the Platform and validating the output of the working groups or taskforces

- Thematic working groups or taskforces composed of experts, meeting on a regular basis to conduct technical discussions and produce draft consensus papers.

The bulk of the work of the platform takes place in the working groups, which meet on a regular basis to conduct technical discussions and provide draft consensus papers on specific topics. Such meetings and the work of the groups is organised essentially in a remote or virtual way (with secure portal and teleconference facilities provided by the Commission and/or ENISA) in order to ensure swift delivery. Work in the NISP is carried out with the following principles in mind:

- Be results-oriented and focused on impact. The objective is to improve the level of cybersecurity in Europe; metrics of success and measures of impact will be defined;

- Be of value to the stakeholders. The main objective of the Platform is to help companies and public administrations to increase their level of preparedness and to cooperate more effectively. For that reason, participants should not only carry out but also steer the work of the Platform;

- Follow a bottom-up approach involving practitioners, in order to make progress on operational issues;

- Adopt a deadline-driven approach, where working groups are asked to deliver specific deliverables in a short timescale;

- Ensure active participation and continuity in the participation, in order to build trust and ensure progress in the work of the Platform;

- Confidentiality rules and supporting tools (e.g. secure platform to share documents) will be implemented as appropriate;

The Commission manages NISP membership with a view to ensuring a balanced and manageable representation of the different stakeholders and to secure participation of the relevant stakeholders in the different working groups. Membership in the working groups is voluntary. The Commission validates on the basis of individual expression of interest from NISP members. Input from non-Platform members will be sought as appropriate. The outputs of the NISP and regular progress reports will be made publicly available to ensure appropriate dissemination of the work of the NISP and allow entities not directly involved in the work of the Platform, including political bodies and the general public, to follow closely its activities.

The NISP comprises three Working Groups (WGs) with membership from governments and industry:

- WG1 – Risk Management;

- WG2 - Incident Notification and Information Sharing;

- WG3 – Research and Innovation.

These guidelines on organisational structures and requirements for risk management are the first outcome of the WG1.

## 4. ORGANISATIONAL STRUCTURES AND GENERAL REQUIREMENTS

All organisations should establish links between cybersecurity risk management and the overall risk management/continuity plan of their business. It is also crucial to identify the level of risk the organisation is ready to live with; within the context of the supply chain in which it operates. In the longer-term, the use of maturity frameworks is recommended that enable all organisations to continuously assess the effectiveness of the practices and standards they apply and identify options for improving their approach.

The chapter addresses all sizes of organisations preferably across all sectors. As a priority the NIS Platform working groups have identified small to medium enterprises (SMEs). 'The category of 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 50 million euro, and/or an annual balance sheet total not exceeding 43 million euro.' (Extract of Article 2 of the Annex of Recommendation 2003/361/EC. These organisations have less resource to apply effective cybersecurity risk management and need the greatest guidance at this time. Therefore SME-specific requirements are also presented.

There are different ways for an organisation to set up its cybersecurity risk management, depending on the degree of direct control the organisation needs to retain. Some organisations have fully-fledged capabilities with specialised personnel, a Chief Information Security Officer (CISO) and in some cases their own Computer Emergency Response Team (CERT). Other organisation may look to outsource functions.

Information and communication technology (ICT) activities and operations are frequently outsourced by large and small organisations and this presents specific challenges when it comes to talking about cybersecurity risk management in the "same language". Many organisations also outsource to entities providing managed security services, rely on trusted cloud platforms, or turn to a national or governmental CERT for assistance with cybersecurity incident management.

Organisations also need to address the awareness and skills of their workforce, spanning from specialised personnel to top management. This chapter builds upon ongoing work to define the skills requirements of general staff (ENISA NIS driving license pilot), specialised personnel (WG3 deliverable on skills) and the awareness of end-users (European Cybersecurity Month).

For the context of this guidance it is important to define the terms "**Cybersecurity**" and "**Cybersecurity Risk Management**" in relation to the terms "**Information Security**" and "**Information Security Risk Management**". These definitions are based on international standards, specifically ISO/IEC 27000:2014 and ISO/IEC 27032:2012.

In ISO/IEC 27000:2014 the term "**Information Security**" is defined as the "preservation of confidentiality, integrity and availability of information".

In ISO/IEC 27032:2012 the term "**Cybersecurity**" based on the definition in ISO/IEC 27000 as "preservation of confidentiality, integrity and availability of information in the Cyberspace.

In ISO/IEC 27000 "**Cyberspace**" is defined as "complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form". Another definition for Cyberspace used in National Cyber Security Strategies is "Cyberspace is the virtual space

of all IT systems linked at data level on a global scale. The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks. IT systems in an isolated virtual space are not part of cyberspace".

Based on these definitions and in the context of this guidance, the term "**Cybersecurity**" is not equivalent to the term "**Information Security**". Cybersecurity addresses only assets that are connected via any type of network to the Internet. Information stored on any other media, such as USB sticks or CD/DVD poses risks and threats of their own. These are not covered within this paper as they do not fall within the scope of the term Cybersecurity.

The three key attributes of the information assets within the scope of cybersecurity risk management are:

- Confidentiality (C);
- Integrity (I);
- Availability (A).

In addition to these attributes (CIA), as stated in ISO/IEC 27000:2014, other properties such as authenticity, accountability, non-repudiation and reliability can also be included within the scope of cybersecurity risk management. Where CIA is considered in this guidance these additional properties should also be considered.

The most common specific technical and procedural controls to mitigate and respond to cybersecurity risks, that were referred to by WG1 members are as follows:

- Management Frameworks (e.g. process and audit):
    - ISO/IEC 27001 - information security management systems. This is the international best practice standard for information security.
    - ISO/IEC 27005 - guidelines for information security risk management.
    - ISO 31000 - risk management and more specifics.
    - ISO/IEC 31010 - risk management and risk assessment techniques.
- Implementing security controls in the supply chain:
    - ISO/IEC 27036 (information technology, security techniques and information security for supplier relationships.

### 4.1. Cybersecurity risk management organisational structures

This section gives an overview of good practices regarding organisational structures (namely 'functions') that have emerged to ensure effective cybersecurity risk management. Some examples of practical and pragmatic cases are highlighted. Where possible the benefits of practices and losses that could have been avoided are qualified and quantified.

This chapter specifies high-level recommendations that detail activities that should be performed by individual functions within an organisation.

Note: required roles are covered in the next section. The listed activities in this section describe what the organisation should address and perform, but does not outline how this should be implemented. This distinction is important to understand as it enables any organisation; independent of size, business, local jurisdiction, working environment and culture, to implement the necessary controls to the extent necessary and appropriate.

First of all, as an initial and clear recommendation, risk management must be **an ongoing, continual process** performed by either one person, or several people with different roles/functions within an organisation. It is essential for the effectiveness of this process that **top management is committed** to these activities by showing support, giving direction and proving input and feedback.

For an organisation looking to apply cybersecurity risk management, regardless of the size and business sector, the implementation of the following functions/roles should be considered:

- Business (e.g. security, legal, regulatory, procurement, commercial and communications);
- Risk;
- Technical (ICT);
- Governance; and
- Audit.

Despite collaboration between these different roles, current trends tend to define a clear segregation in the management of risk between them. This segregation should adopt the "3-lines of defence":

- First line: Business functions line management and supporting technology functions
- Second line: Risk function and compliance/governance functions
- Third line: Internal audit

The "Risk function" performs the risk identification and risk analysis. It develops the appropriate risk assessment process, risk treatment process, risk assessment methodology, risk criteria and the risk acceptance criteria. It presents them to the "Governance function" that officially approves them.

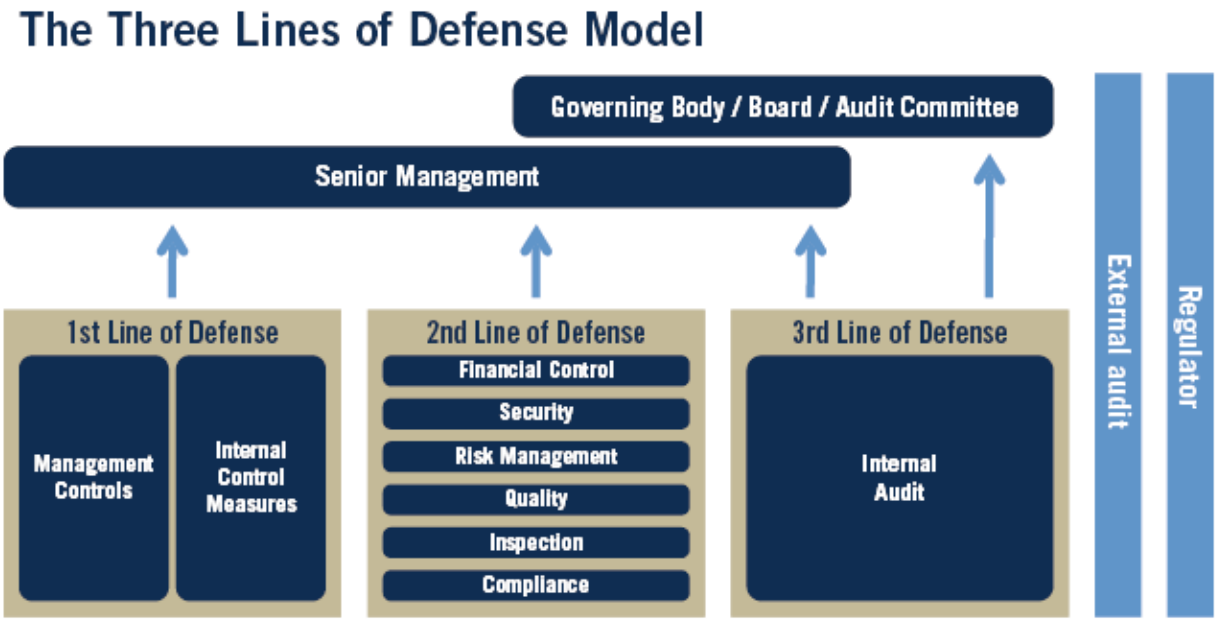
The "Governance function" has the accountability for defining policies and guidelines on risk.

The "Business function" is the official "risk owner". It is accountable for the risk treatment plan, performing risk assessments according to the specified frequency and is supported by the "Risk function". The accountability of the business function guarantees the proper buy-in of business process owners. This also emphasises that cybersecurity risks are not IT risks but business risks!

After a risk assessment has been performed, the "Risk function" will act as an intermediary between the risk owner (Business function) and the "Technical function", who are tasked to provide concepts and controls to address the identified risks. These concepts and controls are then presented to the risk owners who have the accountability and competence to select the most appropriate specific controls.

The "Audit function" frequently assesses the compliance of the defined processes, methodologies and control selection etc. and reports back to the "Governance function".

Finally, the "Governance function" reviews existing processes, procedures and methodologies regarding their effectiveness and adequacy.




Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

It is essential that the above roles apply equally to large corporates and SMEs with a focus on business and organisational issues; not just technical or IT issues. This model ensures responsibilities are clear, with increasing accountability and risk culture through the internal challenge from the second line of defence. To make it easier for SMEs to implement this model, it is possible to merge the first and second line of defence together, while keeping Internal Audit segregated and independent.

In some cases, because of the constraints on internal audit resources; usually due to downsizing and budget tightening, a control self-assessment approach can be followed. The objective of a control self-assessment is to shift some of the control monitoring responsibilities (especially for areas of high risks) from the internal audit function to the business functional areas, in order to enhance audit's responsibilities. The purpose of this is to help to develop a sense of control-ownership with the risk owner (Business functions), along with reducing their resistance to control improvement initiatives as described in the ISACA CISA framework/certification.

For Clarity a RACI (R: responsible, A: accountable, C: consulted, I: informed) matrix is depicted below which maps functions and roles.

| | *FUNCTIONS* | | | | |
|---|---|---|---|---|---|
| *ROLES* | Audit | Governance | Risk | Business | Technical (ICT) |
| Define policies and guideline on cyber-security risk management | | A/R | | C | |
| Define methods for risk management | | A | R | C | C |
| Perform risk Identification and Risk Analysis | | I | R | A | C |
| Define Risk, Impact/Consequence and Likelihood Criteria | | A | C | R | |
| Evaluate Risk (in coherence with criteria) | | I | C | A/R | |
| Define Risk Treatment | | C | | A/R | C |
| Provide Controls | | | C | A | R |
| Audit | A/R | I | I | C | C |

Finally, listed below are some examples of losses that could have been avoided or reduced by applying good risk management:

- Anti-malware is one of the mitigation measures and controls recommended in the NISP WG1 Final recommendations back in April 2014. Ineffective anti-virus and malware software disinfection can be the door to threats. Recovery efforts and costs from an infection can be significant.
- In today's world, email is a fundamental tool for day a day work and so are the possible threats that can be introduced through it. For that reason, it has to be controlled and anti-spam policies have to be applied where possible.
- Ineffective anti-spam can result in more than 75% of incoming emails being spam which leads to a waste of computing resources, people's time and opens up the potential for phishing attacks.
- Cyber-attacks are becoming more frequent, more sophisticated more widespread and, as a consequence, so are the impacts of these attacks. For this reason, cybersecurity is becoming more and more important in order to reduce the likelihood and impact of these attacks, along with reducing the vulnerabilities of assets in the Cyberspace. The recommendations included in all documents from NIS Platform are intended to help organisations to apply cybersecurity essentials to tackle with this problem.

### 4.2. Key roles to cultivate a risk management culture

This section gives an overview of typical key roles required within an organisation to cultivate a risk management culture. They can be incorporated by an organisation as appropriate, depending on factors such as requirements, size or business sector. The responsibilities of each of the key roles are highlighted. It also highlights who in the organisation is best placed to engage with external entities to ensure there is a consistent approach to cybersecurity risk management. In case of outsourcing (ICT) operations, specific

questions that should be asked to ensure a consistent approach to cybersecurity risk management are detailed.

According to law the board is legally liable for risk, therefore, an organisation should define who owns collaborative risk management on the board and what that means for the organisation.

The Chief Executive Officer's (CEO) leadership is crucial and the General Counsel or similar position should be responsible for setting the main policies for compliance. The Chief Information Security Officer's (CISO) advice, governance and assurance activities should also be involved.

Risk Managers should drive the process. Non-Executive Directors (NED) are key in challenging risk management practices, data ownership, retention and protection policies. There also needs to be strong engagement between audit function, IT security, CISO and NEDs.

The corporate risk officer (CRO) is responsible for overseeing the identification and management of risks. Some of these risks may become the responsibility of the CISO, Chief Information Officer (CIO) and/or Head of Human Resources (HR).

Fraud risk management should come under the Head of Fraud in the organisation and cybersecurity risk management should come under the CISO.

A CISO should be appointed by the group board members and beneath the CISO each business unit (BU) should appoint a CISO BU. Continuous audits by internal or external auditors are essential. The BU CIO is responsible for ensuring external ICT providers are compliant with the ICT security management.

The CISO and CIO also have the responsibility for clearly translating security and technical imperatives into the board language of business need.

ICT's roles and responsibilities should be well defined and it is recommended that the following roles are part of the ICT division:

- ICT Users;
- process owners;
- ICT resource owners;
- ICT service providers and operations.

Collaboration across the organisation is important to ensure cyber risk management is effectively implemented and the organisation should aim to avoid silos. If the organisation certifies a supplier's processes, it is forced to guaranty that its suppliers (which may be SMEs) have implemented the appropriate controls, either by auditing them or by requesting an external certification such as ISO/IEC 27001. It is also important that an organisation establishes and understands its risk appetite. Risk appetite is covered in a subsequent section of this chapter.

It is recommended that for ICT purchases, supply chain risks are managed in the same way and to the same degree as internal risk; ISO/IEC 27036 provides specification and guidelines on how this can be achieved.

For employees it is absolutely critical that all staff understand they have personal responsibility for cybersecurity, regardless of their role in the organisation, however, it is the organisation's responsibility to ensure staff understand how their role specifically relates to the cyber component. Cybersecurity risk management is addressed if individual responsibility is clear. **The tasks may be outsourced, but responsibility and accountability remains with the organisation.**

Risk management culture in an organisation can be differentiated between leadership, ownership and responsibility. It can be achieved by incorporating the following principles:

- don't lead from ICT or CSO. ICT can provide expertise but will not be taken seriously if it is trying to lead on business issues;
- risk management is not a program; it needs to be part of the organisation's culture;
- internal and external business codes of conduct should include a cybersecurity component;
- general risk management is essential and shouldn't be taken for granted;
- where risk management exists then it needs to explicitly include cybersecurity;
- cybersecurity risk management won't function if genera risk management is lacking;
- the exact risk management methodology selected isn't important, but it should link operational risk to strategic business risk;
- there should be robust management information to underpin risk management; decisions/discussions. A risk register that includes cyber security helps to achieve this.

Risk portfolios for organisations can often be broken down into four areas:

- strategic;
- operations;
- legal/compliance; and
- financial/reporting.

Enterprise risk management (ERM) within each area should be sponsored by an executive from the organisation's top management. They should ensure that a regular and effective risk management rhythm is followed and accountability for enterprise risks exists. An appropriate mission for an organisation's ERM team may include:

- facilitating a programmatic and global approach to enterprise risk management;
- establishing broad accountability for the most critical organisational risks; along with
- enabling and enhancing business objectives through value creation and protection.

It is recognised that it is not always practical for SMEs to implement an organisational structure exactly as described above. In order to be applicable to organisations of all size, the roles described could be undertaken by a number of people, or as it often is within SMEs one person can take various roles. However, distinctions must be maintained between roles and responsibilities.

### 4.3. Organisational controls to ensure effective risk management

This section gives an overview on the key risk management activities that can be implemented within an organisational structure to ensure effective cybersecurity risk management. Key cybersecurity risk management measures, i.e. those having greater impact than others, are discussed, together with the support available to organisations in order to enhance their capabilities for managing cybersecurity risks. Note that in terms of technical and procedural controls, the reader is referred to the standards listed above.

It is very important to make cybersecurity vulnerabilities, threats and risks a subject of interest at every level of the organisation, and, specifically, not limited to the ICT department. C-level management commitment is essential to get the needed resources and also to raise awareness among non-technical people (and all personnel) in the organisation. In particular, SMEs should include cybersecurity risks in their Strategic and Operational Plans.

Cyber risk management should be included in organisational vision statements and the fact made clear that all personnel are responsible for inputting to risk management activities and implementing and maintaining controls. Clear roles and responsibilities need to be reflected in job descriptions, personal goals and remuneration.

Cyber risk education, awareness and responsibilities need to be driven at varying levels:

- organisation-specific and industry-sector-specific requirements;
- national and international perspectives;
- cyber awareness compliance tracking;
- role-specific training;
- frequent awareness campaigns ("drip feeding" messages).

The nature of interrelations between the leaders of the organisation and the 'troops' at ground level will vary depending on the maturity and size of the organisation. In line with this, clearly defined roles and responsibilities should be implemented across the organisation.

Determining an acceptable level of risk (see risk appetites, below) can only be achieved once the risks are identified, analysed and evaluated: this means that some form of appropriate and effective risk analysis is required and this must feed into the organisations risk management and governance framework.

Information sharing can be a good means of assisting organisations less mature in cybersecurity. Large organisations could share information, methods and tools with smaller organisations, particularly with SMEs in their supply chain. This would contribute to raising the overall level of cyber protection within supply chains. In parallel with this, the publication of examples of cybersecurity incidents and cost-effective means of dealing with vulnerabilities and threats will help smaller organisations. There are also voluntary schemes available such as national CERTs (Computer Emergency Response Teams) which offer organisations access to shared knowledge in a trusted environment in order to improve cooperation and coordination.

Reducing the complexity involved in cyber risk management would also assist organisations and SMEs in particular. Volumes of current information may appear, or actually be, overwhelming to some, especially when specific knowledge, processes and resources (and therefore costs) are required to process it. A means of addressing this is to attempt simplification through segmenting organisations according to relevant characteristics (size, type, industry, supply chain, etc.). This could help to filter and pre-process information that is relevant to each segment and result in more specific and practical information and actions.

Cybersecurity risks should not only be seen as an operational issue but rather as an enterprise-wide risk. Organisation need to conduct cost/benefit analysis (i.e. who can afford what in which time line) and measuring capability strength is important.

Industry standard approaches to risk management should be considered, e.g. the "Identify, Protect, Detect, Respond, Recover" model.

*Identify*: key assets, vulnerabilities and impacts from cyber compromises. Threats and the likelihood of attack, overall risk, and the prioritisation of assets key to the survival of the organisations and its customers, plus risks that must be addressed.

*Protect*: After risks have been assessed and prioritised, it is important to manage them. A large part of risk management is focused on preventing events from happening (i.e., decreasing their likelihood), containing events from expanding, and/or preventing events from causing damage if they occur (i.e., decreasing their impact). Doing a combination of both mitigates the risk. The prevention element of the risk management program should enable enterprise risks to be tracked and reported to the right level in the organisation, with the most significant risks being made known to those leading the organisation. As a part of the prevention process, it is important to include the following elements in any analysis:

- changes in the risk drivers or scenarios within an enterprise risk area;
- progress since the last update (e.g., risk mitigation or improvements in controls);
- changes in direction or timing for reduction or mitigation (e.g., milestone changes);
- risk ownership and support from the responsible organisations (e.g., changes due to reorganisations);
- related high risk audit issues that are open or pending.

*Detect*: detection may be the most difficult but critical part of risk management. Talented and patient adversaries will delete logs, change data, and take whatever actions are necessary to gain and retain access to a network. Detecting when an attacker has gained access to a network, system, or asset requires incredibly skilled forensic investigators equipped with cutting-edge tools and resources. Several competencies should be considered:

- dedicated threat intelligence - for the organisation to be able to defend against targeted attacks, it is critical that they have internal teams in place that have the skill sets to develop and consume threat intelligence;
- continuous monitoring - continuous monitoring should be a part of any organisation's approach to detection. With the appropriate monitoring capabilities in place, adequate data will be available to determine whether a compromise has occurred. Monitoring services should be divided into three high-level categories:
    - baseline security monitoring for broad detection of malicious or anomalous network activity;

- specialized security monitoring for critical assets and critical processes; and
- data analysis and reporting to provide telemetry to other key internal security detection and response partners across the enterprise.

*Respond*: incident response is a priority for all organisations, given the ways in which attackers attempt to use vulnerabilities in software or compromise features in a product or service to commit some harm.

*Recover*: An organisation's ability to recover from a cybersecurity incident is largely dependent on its overall capabilities for reliability and resiliency. Traditionally, organisations are managed with a focus on avoiding failures. However, the scale and complexity of the larger originations, interconnection between organisations and lengthy supply chains brings inherently different challenges than were faced in the past. Despite the best plans and detailed risk management efforts, hardware will fail, people will make mistakes, and software will contain vulnerabilities. Accordingly, strategies and plans are recommended for recovery of key assets and resources are developed.

From a business continuity management perspective, the following standards (and associated controls): ISO/IEC 27031, ISO/IEC 22301, ISO/IEC 22399, and NFPA1600 could be considered. These standards collectively help ensure timely, relevant, and accurate operational information by specifying processes, systems of work, data capture, and management. From an operational standpoint, there are certain specific principles and practices that should be kept in mind when thinking about recovery. For example:

- Design for recoverability. When the unforeseen happens, a service must be capable of being recovered, preferably quickly and automatically. Teams should be able to restore a service quickly and completely if a service interruption occurs, e.g. the organisation should design the service for component redundancy and data failover so when failure is detected, whether it's one component, a group of servers or an entire physical location or data center, the service automatically uses another component, server(s), or physical location to keep the service running.
- Testing for recoverability. Testing verifies the accuracy of the recovery procedures and highlights any discrepancies or areas that were unintentionally overlooked during the plans creation. Also, testing familiarises personnel with the plans objectives and provides the necessary preparation for quick, decisive response.
- Diagnostic aids. Diagnostic aids for root cause analysis of failures can be used. These aids must be suitable for use in non-production and production environments, and should rapidly detect the presence of failures and identify their root causes using automated techniques.
- Automated rollback. Automated rollback for most aspects of operations, from system configuration to application management to hardware and software upgrades is desirable. This functionality does not prevent human error but can help mitigate the impact of mistakes and make the service more dependable.
- Defence–in-depth. A defence-in-depth approach should ensure that a failure remains contained if the first layer of protection and does not isolate it. In other words, organisations should not rely on a single protective measure, but rather, factor multiple protective measures into their service design. Business continuity processes should also be implemented with procedural controls (not only with technical countermeasures).
- Forensics. In addition to threat intelligence and continuous monitoring, in today's threat environment strong forensic capabilities need to be considered as an important element of

detection. After an incident is detected it has to be contained and eradicated efficiently and effectively in order to minimise damage.

The topics covered in this section are expanded on further in the WG1 Initial Recommendations, where a comprehensive list of organisational cybersecurity controls and metrics can be found.

### 4.4. Determination of risk appetite

This section gives an overview how an organisation can determine its risk appetite, how an organisation should agree its risk exposure and decide on the level of risk it is ready to live with, as well as how often an organisation should evaluate its risk appetite.

It is important that all types of cybersecurity risks are identified and managed by an organisation. Ownership should be assigned for the management of each risk type, or risk. There should be a high degree of coordination, collaboration and communication across the organisation to ensure collaborative cybersecurity situational awareness. There should be no silos in an organisation and typically, governance, risk and compliance (GRC) and ERM functions and systems should be linked.

There should be a matrix of capabilities vs. the business sector requirements vs. the size of the organisation. Most large organisations will usually have all the functions in-house but smaller SMEs may have outsourced providers. The organisation should implement the capabilities and an organisational structure to support these capabilities. This includes the internal governance structure that supports the board for each of the five stages in risk mitigation, describe in the previous section:

1. Identify;
2. Protect;
3. Detect;
4. Respond;
5. Recover.

The mapping of each capability should meet each operational risk and the objective of each capability should be clear. The assurance of each capability should be defined, including red teaming, serious gaming and also independent external audit. Continuous improvement in response to dynamic change should also be implemented.

An organisation should define what it means by "risk appetite". For example, ENISA's definition is "Willingness of an organisation to accept a defined level of risk". There are several differences between public and private sector organisations starting with the understanding of cost-benefit. Private sector organisations may have more economic drivers whereas public sector organisation may have more political drivers. Cybersecurity risks should be aligned with business processes as there could be different drivers to agreeing risk appetite. An SME's approach to determining risk appetite is usually as subset of these drivers.

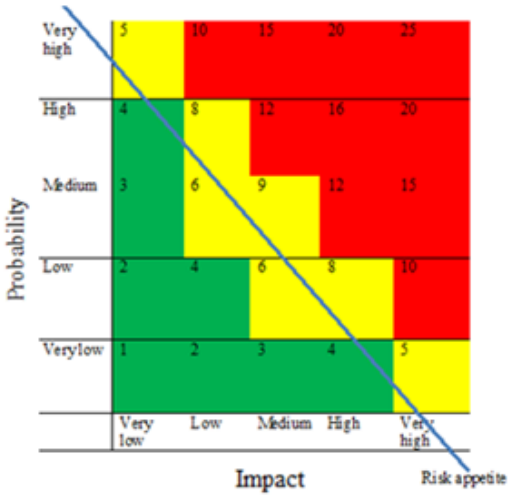
Risk management as wider approach with the determination of risk appetite as sub-activity should be continuous process. Determination of cybersecurity risk appetite has to be

connected with enterprise risk management (ERM). The starting point should be to understand what is important to the organisation (e.g. critical information assets) and what causes risk (e.g. driven by vulnerabilities and threats). In some cases the organisation is driven by external factors when deciding what is important e.g. if organisation is serving critical infrastructure services. In analysing criticality the three main cybersecurity features of the assets that should be considered:

- Confidentiality;
- Integrity;
- Availability.

Risk categorisation may facilitate decisions. For bigger organisations, the categorisation may be at the level of market risk or operational risk. For SMEs, risk categorisation may be at the level of malware risk or attack risk.

Common understanding and decisions on acceptable levels of risk can be facilitated via the use of a generic risk matrix. There are numerous simple ways to determine relative risks such as the use of a "matrix of probability of compromise/attack vs. impact of CIA compromise" as shown in the 5x5 matrix below.




This matrix uses a scoring mechanism of 1-25 to highlight relative risks. The absolute score is not important. The red-amber-green (or high-medium-low) categories are what an organisation should focus on, as these are mapped onto the scores to give an indication of relative priorities for action (i.e. spending money on mitigation and management activities). This type of matrix can also be used to determine whether the risks are vulnerability driven (impact) or threat driven (probability).
Risk strategies, can also be overlaid onto matrices such as this. Very often risk 'calculations' can be facilitated by simple tools such as in-house spreadsheets that follow best practice frameworks such as IEC/ISO 31000:2009. The use of tools provides greater flexibility for conducting 'what-is' and sensitivity analysis on the results.

In deciding the level of risk an organisation is ready to live with, an understanding of the consequences is essential. In many cases, not only the loss of money has to be considered but also, for example loss of reputation, or even external factors such as compliance to local laws

and regulations. Decisions should be clearly informed and made at board level, with correspondence with the risk department (if it exists). Decisions should be taken from a business perspective and not just from an ICT perspective (decision should not be made by technical people but with them).

An organisation should consider the next steps as there are different options (risk strategies) to mitigate the risk to an acceptable level e.g. avoiding risk, removing risk source, changing the likelihood, changing the consequence, takin/increasing risk or retaining the risk.

Good practice dictates that that risk appetites (along with all risks) should be evaluated at least annually and preferably should be a continuous process to address the many changes to environmental variables that may occur. Typical examples are:

- High impact changes in ICT – for example launch a new system;
- significant changes in business – for example entrance to new markets;
- new interconnections (especially via the Internet) – for example launching a web-based portal;
- incidents with great impact – for example system disruptions or attacks;
- events affecting future risk – for example regulatory or legislative changes.

In order to have comparable risk appetite over time, risk analysis should be repeatable, i.e. similar initial conditions should result in (as much as possible) similar risk analysis outputs. Risk analysis and risk acceptance should be a continuous process.

Risk appetites and levels of acceptance should also be communicated up and down supply chains and/or with key partners to ensure harmony in risk assessment and risk management and to ensure nothing slips "between the gaps". KRIs (Key Risk Indicators) are useful tools that help to achieve this.

# 5. SPECIFIC REQUIREMENTS FOR SMALL AND MEDIUM ENTERPRISES

## 5.1. The goals of cybersecurity for Small and Medium Enterprises (SMEs)

This section gives overview of why SMEs should address cybersecurity risks and what incentives are available to encourage SMEs to address cybersecurity risks.

With the threat of cyber-attacks showing no signs of abating SMEs need to demonstrate their cybersecurity capability to investors, customers, partners and stakeholders alike. The process to secure assurance can be arduous and resource-intensive for SMEs, who must demonstrate their capability to manage cybersecurity risks to a range of third parties, of which include:

- customers (e.g. to gain trust around data security and enhance reputation);
- business partners (e.g. as part of logistics, mobility, services, or supply chain/procurement processes);
- financial institutions (e.g. to demonstrate accountability, increase financial standing).

The main driver for SMEs to address cybersecurity risk is typically contractual requirements, where SMEs are mandated to deliver a secure service as part of the supply chain of their customers (who are usually larger organisations). A collaborative approach to risk management is vital for successful cyber risk management. To ensure SMEs deliver secure services contractual terms should define the following:

- policies;
- procedures;
- mandatory and legislative requirements.

SMEs should look to review and consider complying with appropriate industry cybersecurity standards or requirements such as those highlighted in the risk management frameworks for SMEs section below. This not only ensures SMEs are not vulnerable to attack, but also gives SMEs a competitive advantage in an environment where large organisations and national states are increasingly looking for compliance to specific standards when they go out to tender.

It is in the business interest of SMEs to address cybersecurity risks. If SMEs don't manage cybersecurity risks effectively the potential impacts are extensive but may include:

- financial losses from theft of information, financial and bank details or money;
- financial losses from disruption to trading and doing business;
- costs from cleaning up affected systems and getting them up and running;
- costs of fines if personal data is lost or compromised;
- costs of losing business through damage to reputation and customer base;
- damage to other organisations they supply or are connected to.

Some examples of current incentives to encourage SMEs to adopt good cyber risk management are highlighted below:

- Governments have mandated the compliance to cyber minimum requirements into public procurement for contracts in certain areas. This means that SMEs must be compliant to them to deliver services to Government.
- The insurance industry has started to recognise the role of these cyber minimum requirements, specifically its targeting of the basics all organisations should have in place. Some insurers have already partnered up with some stakeholders to offer insurance products (in some cases free) alongside these cyber minimum requirements.
- Liability reduction and/or safe harbor protection in cases where an adequate level of cybersecurity performance is demonstrated, for example based on (certified) implementation of best practices; conversely increased liability could be the consequences of poor cybersecurity risk management.
- Tax incentives in cases where an adequate level of cybersecurity performance is demonstrated.

- The use of public funding to foster risk management and the adoption of secure ICT solutions, for example by making certain public grants or loans conditional on the adoption of adequate cybersecurity measures by beneficiaries.
- participation in information sharing platforms, where participants are able to share up-to-date information on threats and vulnerabilities.

### 5.2. The ways to manage SMEs cybersecurity risks

This section gives an overview on how should SMEs manage cybersecurity risks. Different approaches are needed depending on whether a SME is managing cybersecurity risks internally or outsourcing them. Along with the implications of outsourcing the management of cybersecurity risks in terms of resources, costs and keeping up with technological developments.

Although SMEs can manage cybersecurity risks in-house they often will not have the resources and/or knowledge to do this effectively. SMEs should consider working with their clients to adopt their solutions for managing cybersecurity risks, or should look to implement appropriate security standards which provide a good baseline for managing cybersecurity risks.

An effective alternative for SMEs to manage cybersecurity risks is through outsourcing to a specialised provider for managed Security Services. SMEs should look to professional support to mitigate against vulnerabilities or threats to their business or to the business of their customers.

It is important that SMEs are diligent and use trustworthy outsourcing partners when outsourcing the management of cybersecurity risks. To ensure they outsource to the right partner, SMEs should understand the different cybersecurity certifications (and level of certification) outsourcing partners hold. It is also important that SMEs have the capability in their organisation to manage the contract with suppliers and assess performance of it. Otherwise they risk receiving a poor quality service which could have significant cost implications.

SMEs should look to use simple (generic and tailored) solutions when outsourcing the management of cyber risks and look to standardised obligatory procurement checklists by large account customers or industry segments alike (e.g. HIPAA or PCI).

Not all cybersecurity risks can be outsourced. It is worth noting that although the management of a cybersecurity risk can be outsourced, the impact and the legal responsibility will usually remain with the SME.

SMEs should also take the cybersecurity of disruptive technologies they utilise into account. Disruptive technologies provide new opportunities for SMEs but also new challenges, particularly with regard to the protection of sensitive information and regulatory compliance. Such technologies include:

- mobile;
- smart metering;
- big data;
- internet of things;
- and cloud.

Considering cloud services specifically, SMEs should look to outsource to trusted cloud providers. Several international best practice standards for assessing cloud security exist together with good resources that are freely available to SMEs such as:

- ISO27018 (http://www.iso.org/iso/catalogue_detail?csnumber=61498)
- Cloud Security Alliance's Cloud Controls Matrix (CCM) based on US FEDRAMP (https://cloudsecurityalliance.org/research/ccm/)
- ENISA's Cloud Certification Schemes List (CCSL) and Meta-framework (CCSM) (https://resilience.enisa.europa.eu/cloud-computing-certification);

### 5.3. Risk management frameworks for SMEs

This section gives an overview of the specific frameworks or requirements to enable SMEs to implement (and measure the effectiveness of) an organisational structure that ensures effective cybersecurity risk management.

As SMEs need simple, flexible, efficient and cost-effective security solutions, there are risk management frameworks or guidance schemes focused on SMEs because of their adaptable scope and simplicity. Some of them are promoted by national governments, others are developed through private initiatives. There are also SME-centric frameworks developed by ENISA. Nevertheless, the goal is the same, to raise the bar regarding cybersecurity.

A well-known government promoted frameworks aimed at SMEs is the UK's Cyber Essentials (CES) (https://www.cyberstreetwise.com/cyberessentials/) which provides SMEs with mitigations to the majority of common internet based attacks. It is recognised that some organisations may have particular additional services (e.g. web applications, payments systems etc.) that require additional and specific controls beyond those provided by CES, however, the CES framework covers essential aspects for an organisation IT systems and is complementary to other standards such as PCI-DSS or ISO/IEC 27001 amongst others.

Another example is the Belgian cybersecurity guide (http://iccbelgium.be/becybersecure/), which is a 10 actions guide that goes through the risk management process. Providing a self-assessment with guidance for follow up steps that organisations can follow to assess cybersecurity maturity and implement improvements. Besides these 10 actions, there is also a list of globally recognised good practices, standards and frameworks for organisations to consult in order to improve their information security and cybersecurity.

Finally, there is also a simplified SME- risk management framework developed by ENISA (https://www.enisa.europa.eu/activities/risk-management/current-risk/infosec-smes). It is a 'one-size-fits-all' solution created for small organisations and non-expert users with relatively simple IT-components. Because this framework is aimed at non-expert users, it is recommended that SMEs have at least some initial support from experts.

Any framework that is implemented by an SME should be simple enough to be managed by personnel with limited expertise and knowledge. The framework should also provide multi-quality level certification and have a roadmap towards evolving maturity built in.

Within risk management and cyber awareness there are two key areas that organisation must address:

- network security; and
- information security.

This is also true for SMEs. To enable SMEs to break from the status quo as the weakest link it is acknowledged that specific knowledge transfer and training is required. As stated in the section above (ways to manage SMEs cybersecurity risks) outsourcing can be an option for SMEs to acquire this knowledge. In addition to this if SMEs' managers engage with risk management processes it could provide them with additional knowledge to better understand Cybersecurity issues. This could be further enhanced through the implementation of various awareness programs.

There are a number of resources that are already available for SMEs, some of which are referenced below:

http://cert.org/information-for/managers/
http://www.sans.org/security-resources/
https://www.cyberstreetwise.com/cyberessentials/
http://iccbelgium.be/becybersecure/
https://www.enisa.europa.eu/activities/risk-management/current-risk/infosec-smes

# 6. LIST OF REFERENCES AND RELEVANT DOCUMENTS

## 6.1. List of Standards and Frameworks

The complete list of standards and frameworks highlighted in this chapter by the members, that complements the more detailed one sorted at the beginning of the document is as follows:

- ISO/IEC 22301;
- ISO/IEC 22399;
- ISO/IEC 27000:2014;
- ISO/IEC 27001 - Information Security Management Systems;
- ISO/IEC 27002;
- ISO/IEC 27018:2014 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27031;
- ISO/IEC 27005 - guidelines for information security risk management;
- ISO/IEC 27032:2012;
- ISO/IEC 27036 (Information technology, security techniques and information security for supplier relationships);
- ISO 31000 - risk management;
- ISO/IEC 31010 risk management and risk assessment techniques
- SANS Top 20 Critical Security Controls
- HM Government 10 Steps
- Guide d'hygiène informatique (FR)
- NIST 800-53 Rev 4
- Cyber Essentials Scheme (UK)
- CESG's Cloud Principles Summary (UK)
- The Cloud Security Alliance's Cloud Security Matrix (CSM)
- The Australian Signals Directorate (ASD),
- ISACA CISA framework/certification
- NFPA1600
- ICAEW's Cybersecurity in Corporate Finance
- Cyber Streetwise
- Belgian Cybersecurity guide
- ENISA simplified RM/RA approach for SMEs
- Information Security Doctrine of the Russian Federation
- IS 7799 – Israel Information Security Standard
- ENISA's Cloud Certification Schemes List (CCSL) and Meta-framework (CCSM)