FERMA PERSPECTIVES 02

FERMA
Federation of European
Risk Management Associations

AT THE JUNCTION OF CORPORATE GOVERNANCE & CYBERSECURITY

FERMA has made the ongoing digital transformation a priority for our advocacy work for several years now. This is why, in 2017, we launched one of the first European cyber risk governance models jointly with our European colleagues and internal auditors from the ECIIA.

Events since then have only strengthened our view that corporate governance models will quickly become obsolete if they do not embed governance for cyber risks under the leadership of a risk and insurance professional. This new edition of the Cyber Risk Governance Report includes a case study that illustrates how our cyber risk governance model works in practice.

FERMA's ambition is to put forward the risk and insurance management profession as the one that is able to bridge the gaps between the new, key digital functions and the usual business operations. In that way, we work together to enhance our resilience to cyber incidents while we take advantage of the opportunities of digital technologies.

Jo Willaert,
President,
Federation of European Risk Management Associations (FERMA)

For many years, cybersecurity has proved a high-priority and cross-functional risk for all organisations and particularly for internal auditors and risk managers. And it shows no signs of abating, as confirmed in the recent "Risk in focus for 2019: hot topics for internal auditors", published by the ECIIA (eciia.eu).

A major obstacle to mitigating this risk is the piecemeal approach that companies have taken to their IT infrastructure planning and development over past decades.

This guidance is not a magical "one size fits all" solution, but it helps organisations and regulators in defining a strong governance model to align cyber risk and business strategy, to improve coordination and cooperation among the different actors, and eventually to make consistent and understandable decisions about security measures, risk management and the overall cyber security posture.

ECIIA and FERMA want to emphasise the interactions between the three lines of defense to facilitate the communication to the Board which is ultimately responsible for the oversight of the cyber-governance framework.

I would like to thank all members of the ECIIA -FERMA Group for their very valuable input.

Farid Aractingi,
President, European Confederation of Institutes of Internal Auditing (ECIIA)

"As long as companies consider cyber security as a responsibility merely of the IT department, they will not succeed in creating an overall secure environment. Cyber security, as demonstrated in this report, is about the culture in the company. It has to be steered by top management and needs to be supported by all business units. If we are serious about this, a clear governance model is of the utmost importance. I very much welcome the guidance about the model described in this report."

Dirk Lybaert
Chief Corporate Affairs Officer of Proximus

"Cyber risks are like unpredictable storms of ever growing severity; nothing is stronger to weather them sustainably than a proactive alliance between anticipative risk management and farseeing internal audit. "

Carlos Ghosn
Chairman and CEO of RENAULT-NISSAN MITSUBISHI Alliance

The Federation of European Risk Management Associations (FERMA) and the European Confederation of Institutes of Internal Auditing (ECIIA) are taking on an important challenge in this Cyber Risk Governance Report. The World Economic Forum, the international organisation for public-private cooperation, recognises cybersecurity and resilience as vital global public goods as we work in an increasingly connected world.

We are aware that many organisations do not feel that they are equipped with the tools to manage cyber risks with the same level of confidence that they manage other risks. Emerging leading practices have not yet become part of the standard set of board competencies. When we released Advancing Cyber Resilience: Principles and Tools for Boards, we anticipated the creation of further risk management tools at the enterprise, industry, and international level. Such tools will serve the purpose of helping leaders develop the right strategies and processes to ensure cyber resilience.

FERMA and ECIIA's excellent contribution to cyber risk governance is therefore both timely and necessary as the world seeks to reap the benefits of the coming Fourth Industrial Revolution, while working to overcome its challenges, like network threats and vulnerabilities.

In this spirit, we look forward to continuing to work with FERMA and ECIIA partners around the world to ensure that we continue to support and advance our shared cyber resilience.

Derek O'Halloran,
Head of Digital Economy and Society System Initiative, World Economic Forum

"The ability of an organisation to communicate on cyber governance to external stakeholders shows its level of maturity and cannot only rely on compliance with standards and laws. As this report rightfully suggests, a strong cyber-oriented corporate governance is also a necessity. These organisations will be the most able to take on the digitalisation challenge with increased resilience."

Pascal Andrei
Chief Security Officer of AIRBUS

"It's not a matter of IF we get compromised but WHEN! Besides having the right security level of your infrastructure at all times, it is therefore equally important to have a strong risk management governance in place, where a risk-based approach continuously evaluates and raises your security level."

Christian Poulsen
CIO, Vice President for Asset & Technology of Copenhagen Airports

Case Study

By Julie Cain, Sr. Strategic Advisor, Information and Technology Risk Management, Educational Testing Service

Implementing a cyber risk governance scheme is possible and has been done as shown in this example shows. Cybersecurity issues are global and shared across regions, thus a similar approach could be implemented anywhere in the world. Such a cyber risk governance scheme can be perceived only positively in a regulated sector, if it is not already required. If the sector is not regulated, it sends a positive signal to investors, authorities and the general public. Within the organisation, alignment of accountabilities for decision making and resource prioritisation results in process efficiencies and enhanced control effectiveness.

Company snapshot:

Educational Testing Service (ETS) is a US-based not-for-profit organization. Our mission is to advance quality and equity in education by providing fair and valid assessments, research and related services. Our products and services measure knowledge and skills, promote learning and performance, and support education and professional development for all people worldwide.

Together with an extensive network of global partners, we operate and maintain a large number of complex and data intensive IT systems under a variety of global legal and regulatory requirements while facing relentless and increasingly sophisticated cyber threats to confidentiality, integrity and availability of systems and data.

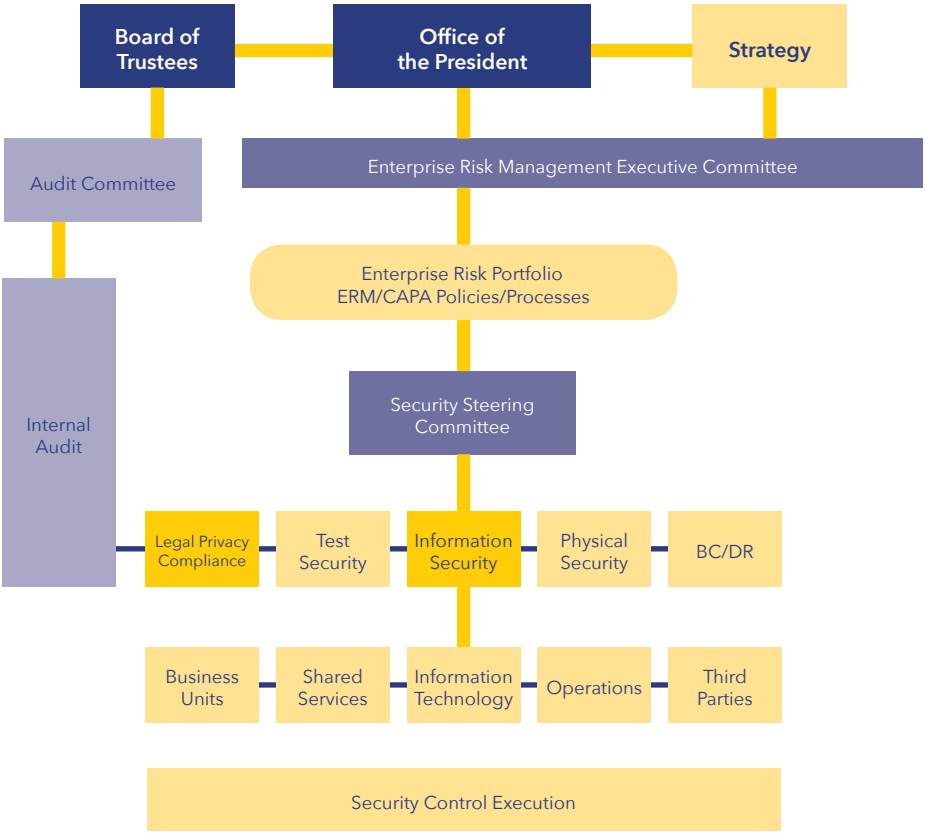
Security ecosystem:

ETS maintains dedicated functions and staff with responsibility for information security, physical security and test security, as well as disaster recovery/business continuity, privacy and internal audit. These organisations communicate and collaborate via a corporate-level security steering committee, led by our Chief Information Security Officer and comprised of the leaders responsible for each function.

The security steering committee defines security policy, determines risk exposures and mitigating controls and proposes, prioritises and provides oversight of significant security initiatives and capital investments, and collaboratively responds to and reports on complex incidents.

Evolution of our approach:

Initially, the functions operated independently and reacted to only their own challenges and opportunities. Overtime, technology innovations necessitated collaborative incident management and joint projects, which lead to more proactive risk identification and mitigating controls, then to true governance and executive decision support as guardrails for business innovation and value creation.



Recommendations:

To initiate a dialogue about cyber risk governance in your organisation, consider the following:

- Leverage opportunities to gain bottom up support/cooperation from 1st and 2nd lines of defence.
- A strong champion is critical – it could be the CISO, CSO, CRO or another influential leader.
- It also helps to have top down support/mandate from Board/top management.
- Start small – invite other leaders to existing steering committee/governance/key project meetings and look for ways to help each other meet objectives.

FERMA brings together 22 national risk management associations in 21 European countries. Together we represent the interests of more than 4800 risk and insurance managers in Europe active in a wide range of business sectors.

www.ferma.eu

The European Confederation of Institutes of Internal Auditing (ECIIA) is the professional representative body of 35 national institutes of internal audit in the wider geographic area of Europe and the Mediterranean basin. The mission of ECIIA is to be the consolidated voice for the profession of internal auditing in Europe by dealing with the European Union, its Parliament and Commission and any other appropriate institutions of influence.

www.eciia.eu

TABLE OF CONTENTS

Executive Summary

Beyond the IT domain, cybersecurity is a matter of corporate governance. This aspect of cybersecurity, however, has not been fully explored by European legislation. The European Confederation of Institutes of Internal Auditing (ECIIA) and the Federation of European Risk Management Associations (FERMA), therefore, set up a joint working group of risk managers and internal auditors to provide guidance on the governance of cyber risk.

This document contains recommendations for a cyber governance model that will benefit European organisations – public and private – in managing their exposures to cyber risks. The timing is particularly relevant. We are in the final year before the effective implementation of two major EU laws: the Network and Information Security (NIS) Directive and the General Data Protection Regulation (GDPR).

ECIIA and FERMA advocate that organisations establish a cyber risk governance system, supported by a cyber risk management framework. It must go beyond the implementation of IT measures, in order to efficiently protect their assets and ensure their resilience and continuity. The model is anchored in two strong sets of principles: the eight principles set out in the OECD recommendation on Digital Security Risk Management (2015) and the Three Lines of Defence model, recognised as a standard of Enterprise Risk Management (ERM).

To respond appropriately to cyber risks, FERMA and ECIIA believe that the leadership of an organisation needs to know with accuracy its level of exposure to cyber threats, expressed in financial terms. These exposures, discussed and accepted across functions, are the starting point for decisions on concrete plans to reduce or avoid the most significant cyber risks, in accordance with the organisation's risk appetite.

The proposed cyber risk governance model argues for the creation of a dedicated Cyber Risk Governance Group (the "Group") whose mission is to determine cyber risk exposures in financial terms and design possible mitigation plans. The Group reports to the Risk Committee.

Chaired by the Risk Manager, the Cyber Risk Governance Group brings together operational functions from the first line of defence, including IT, and key functions from the second line of defence, notably the Chief Information Security Officer (CISO) and the Data Protection Officer. (DPO). This cross-disciplinary group has the subject and organisational knowledge to establish what cyber risks would be the most harmful for the organisation and determine suitable responses.

The Group presents senior leadership with possible mitigation plans, including investments in security and risk transfer solutions such as cyber insurance. To ensure continuous improvement of these plans, cooperation between the Group and Internal Audit ensures that they are auditable "by design". Internal Audit will independently review the efficiency of the cyber controls, risks and governance processes implemented.

The Risk Committee, as a board committee, is responsible for enterprise risks and reviews the cyber risk assessments performed by the Group. The Audit Committee indepen.dently reviews the audit of the cyber risk governance system performed by the Internal Audit function.

This proposed cyber risk governance model constitutes an innovative way to approach cyber security. It will allow the Board of Directors to demonstrate that cyber risks management is based on a rational and documented analysis of the risks across the organisation.

Introduction

Digitisation has been an accelerating trend worldwide, representing a key business opportunity for European companies. The proportion and value of intangible assets, including digital assets, will continue to grow strongly in European organisations. As digitisation has become central to the development of many organisations, so has cybersecurity. It is now also a major issue for corporate governance. Having a digital strategy is essential for all organisations.

The data business opens opportunities for European organisations. By contrast, the need for a secure environment is merging with consumer privacy concerns. The European Union's legal framework for data protection is becoming stricter, and companies deploying Big Data projects involving personal data need to meet the requirements of the latest EU Data Protection Regulation.

European organisations have to find the right balance between the desire to develop and innovate by exploiting the value of their increasingly rich data assets and consumer privacy concerns. This situation creates an opportunity to tackle data security and compliance using the same approach. It makes sense for organisations to combine into a single planning process their privacy obligations and the strategic business planning of their data processing requirements, simultaneously improving the quality of project management and reducing costs.

Against this background, the European Confederation of Institutes of Internal Auditors (ECIIA) and the European Federation of Risk Management Associations (FERMA) have worked together to develop a cyber risk management and governance framework. A robust cyber risk governance framework will improve companies' decision-making processes, leading to better product and service development while at the same time providing stronger and more comprehensive assurance that risks are being identified, quantified, managed and mitigated.

Tackling cyber risk effectively will require changing both the processes and the wider culture of organisations. Risk Managers and Internal Auditors, with their organisation-wide remits, have an important and distinctive contribution to make in addressing this challenge, by taking a holistic approach to risks.

The approach proposed in this paper will enable organisations to manage cyber risks more effectively and at lower cost, and react more effectively and rapidly to any cyber incident.

Fundamentally, good cyber risk governance is about protecting value in the organisation. Boards will increasingly need to demonstrate to investors and the public that cyber risks are managed, not only from a technical standpoint but also from a governance and financial perspective. External stakeholders will increasingly seek assurance that organisations have effective cyber risk governance in place. It is already a reality for critical infrastructures under the Network Information Security Directive, which introduces new reporting requirements for security incidents and promotes "a culture of risk management, involving risk assessment and the implementation of security measures appropriate to the risks faced"[1].

ECIIA and FERMA representing the Risk Management and Internal Audit professions at European level, have a key role to play in making a positive contribution to modernising good governance for the cyber age.

[1] See recital 44 of the directive 2016/1148 on Network and Information Security (NIS) http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=FR

1. FUNDAMENTALS OF A CYBER RISK MANAGEMENT FRAMEWORK

1.1. INTRODUCTION

A robust cyber risk management framework is critical for organisations to reduce their exposure yet allow cyber-related opportunities. Cyber risk management is not just an IT issue and the framework should involve all departments and functions across the organisation. As starting points, ECIIA and FERMA recommend that organisations refer to two overarching and internationally recognised models:

- The 2015 OECD principles in OECD Recommendation - Digital Security Risk Management for Economic and Social Prosperity[2] and
- The Three Lines of Defence model promoted in the joint FERMA-ECIIA document Audit and Risk Committees - News from EU Legislation and Best Practices published in 2014[3].

These models are the basis for the analysis and proposals which follow.

1.2. THE OECD PRINCIPLES FOR DIGITAL SECURITY RISK MANAGEMENT

The OECD recommendation sets out eight organising principles to inform the development of a robust cyber risk management framework: awareness, responsibility, rights and obligations, co-operation, risk assessment, security measures, innovation, and preparedness, resilience and continuity.

Although originally designed for public sector entities, FERMA and ECIIA consider that these principles can easily be adapted for use by private sector organisations, as outlined below.

The main objective is to protect the information assets of the organisation, its business, its operations, stakeholders, reputation and brand against internal and external threats.

1.2.1 Awareness, Skills and Empowerment

Building a cyber aware corporate culture

A successful cyber security programme requires full engagement from both the senior management team and all employees. Appropriate culture and "tone at the top" are key, but awareness needs to be driven throughout the entire organisation, since breaches can occur at any level and in any part of the organisation's operations.

Organisations can assess employees to identify the most exposed individuals and groups to help target risk awareness and risk management efforts. As there is "no one size fits all" solution, the function in charge of these assessment may vary among organisations.

The awareness programme for employees can include:

- Training exercises, videos and role playing
- False phishing tests
- E-learning with continuous and measurable evaluation
- Harmonised awareness practices and communication in subsidiaries and supply chains, taking into account their local specific circumstances like the legal constraints.

---

[2] Digital Security Risk Management for Economic and Social Prosperity - OECD Recommendation and Companion Document (2015). It is FERMA and ECIIA's understanding that cyber risks are part of the broader category of digital risks. http://www.oecd.org/sti/ieconomy/digital-security-riskmanagement.pdf

[3] Audit and Risk Committees - News from EU Legislation and Best Practices (2014) http://www.ferma.eu/app/uploads/2014/10/ECIIA_FERMA_Brochure_v8.pdf

1.2.2 Responsibility

Identification and designation of risk owners

Senior management should clearly define and articulate the respective responsibilities of the various risk owners in managing cyber security risks throughout the organisation. All those assigned risk ownership must be capable of effectively contributing to the management of the risks, for example in terms of information, knowledge, skills, resources and tools.

The main areas to be considered are:

- Defining the roles and responsibilities in terms of who owns processes/systems and who is responsible for operating those systems.
- Defining the roles and responsibilities in terms of defining the type and value of data, where data resides, who owns data and who is responsible for the management and security of data.
- Defining the roles and responsibilities for proactive ongoing maintenance and reactive maintenance of systems, including ability to perform when a problem arises and without systematic process in place.

1.2.3 Human Rights and Fundamental Values

Compliance with latest applicable laws, policies and processes

Organisations must be familiar with the detailed requirements that apply to them, and keep up-to-date with changes in the regulatory environment, including national, European and international laws such as the EU Network and Information Security (NIS) Directive and General Data Protection Regulation (GDPR).

The GDPR, which enters into force in May 2018, introduces important new requirements for many companies (see annex 2 on GDPR summary and the section on the Data Protection Officer on page 16). Compliance monitoring includes the management of internal data protection activities, training staff about data processing and conducting internal audits.

In addition to complying with regulations, organisations should also adopt best practice from relevant professional standards and ethical codes[4] to reduce the risk of regulatory or legal action and reputation damage.

1.2.4 Co-operation

Breaking down barriers

Co-operation is essential across boundaries: within organisations and with other organisations and public authorities.

a) Within the organisation and across all business units

All business units in the organisation are involved in the management of cyber risks. One common weak point in cyber security is the lack of coordination between functions, resulting in a siloed approach. Communication processes around cyber security should be formalised to avoid gaps.

Cross-disciplinary teams and dedicated training and awareness workshops can prepare and organise communication channels and launch joint initiatives on cyber security within the organisation.

Incident notification, escalation and communication should follow the processes set out in the relevant business continuity plan. The rapid and automatic exchange of information also relies on the development of regular and structured contacts between different departments and functions.

Effective cyber risk governance also depends on building trust among the various functions, which will drive behaviour within the organisation. Cross-disciplinary teams who have learned to collaborate can be valuable in ensuring a rapid response to incidents.

b) With other organisations and public authorities

Trust is also at the centre of the dialogue between the organisation and third parties, whether suppliers, vendors, partners, other businesses or public authorities. Lack of effective information-sharing among organisations is currently one of the barriers to cyber security and data protection.

[4] E.g.: "FERMA Code of Ethics"; ISO/IEC 27001:2013; ISO/IEC 27002:2013; COBIT Governance network; intercontinental best practice; IPPFs, etc.

All stakeholders should work to develop better and more systematic communication on these issues. Confidence-building measures have a significant part to play in this regard. Working on the basis of similar definitions, references and standards[5] could help mutual understanding and trust, and support better modelling and analysis of cyber risks through agreement on the collection and validation of confidential data.

1.2.5 Risk Assessment and Treatment Cycle
Strategic and operational approaches

The use of an effective Enterprise Risk Management framework is crucial for managing cyber risks. The ERM methodology can be defined as a process "designed to identify potential events that may affect the entity, manage risk to be within its risk appetite and provide reasonable assurance regarding the achievement of entity objectives."[6] The cyber risk dimension must be integrated and managed with other risks.

a) Strategic risk assessment

One of the main drivers for improved cyber risk governance is to enable the Board to take better strategic decisions on cyber risk and to play its full part in setting an appropriate risk appetite[7]. A rigorous risk assessment is crucial to allow the Board to answer such questions as "Do you know the exposure of your company to cyber risk?" or "Can you explain the rationale of the decisions you took on cyber security to preserve the interests and assets of the company?"

b) Three step risk assessment

First is the operational risk assessment, which is mainly technical and typically operational under the authority of the Chief Information Officer (CIO). It consists of securing the organisation against typical attacks, disseminating good practice and developing constant monitoring of the IT networks, regularly tested against the latest known types of cyber attack (see annex 1 on operational risk assessment).

Second, the compliance risk assessment in the context of the latest applicable regulations. The legal function is key to identifying and analysing the severity of this risk, but other roles, such as the Data Protection Officer (DPO), play an important part in helping to determine the cyber security measures that should be taken as a consequence of legal requirements.

Third, a robust enterprise cyber risk management should ensure a thorough assessment of cyber risks across the organisation's operations. Data controllers, processors of essential services and digital service providers should all include a cyber risk assessment within their enterprise risk management system (such as financial, infrastructure, reputational risks, etc.).

c) Scenarios for catastrophic situations to quantify exposure

For a comprehensive risk assessment, the organisation should assess the financial value of its exposure to catastrophic cyber scenarios. The quantification of the impact of these scenarios should include the full potential consequences for the organisation to return to "business as usual". This is a challenging and complex process.

---

[5] For more details on the necessity to work on common categories and agreed definitions for cybersecurity, see Chapter IV.2 of the research report of the IRT SystemX based on a research seminar (November 2015 - July 2016): Mastery of cyber risk throughout the chain of its value and transfer to insurance results of the research seminar http://www.irt-systemx.fr/v2/wp-content/uploads/2016/11/ISX-IC-EIC-transfert-risque-LIV-0401-v10_2016-10-25-ang.pdf

[6] Committee of Sponsoring Organizations of the Treadway Commission (COSO), (2004). Enterprise Risk Management – Integrated Framework Executive Summary (p. 2). http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf
For similar definitions see also: RIMS Strategic and Enterprise Risk Center. RIMS the Risk Management Society. https://www.rims.org/resources/ERM/Pages/WhatisERM.aspx The Institute of Internal Auditors (IIA), (2009). IIA POSITION PAPER: THE ROLE OF INTERNAL AUDITING IN ENTERPRISE-WIDE RISK MANAGEMENT (p.2). https://global.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Role%20of%20Internal%20Auditing%20in%20Enterprise%20 Risk%20Management.pdf

[7] The ISO Guide 73:2009 Risk management - Vocabulary defines risk appetite as the "amount and type of risk that an organization is willing to pursue or retain" https://www.iso.org/standard/44651.html

These scenarios should be coordinated by the risk management function and developed in collaboration with the other relevant business functions and senior management. Attempting to manage cyber risk in isolation endangers early identification of threats and increases the damage of an incident.

Cyber expertise will be necessary to articulate the most plausible scenarios, based not only on their technical feasibility but also on the most likely targets. IT should analyse the potential weaknesses which might render such attacks successful.

Three dimensions will determine the probability and potential severity of an attack: the threat or technical capability available; the exposure or weaknesses that turns the organisation into an identifiable target; and the security level or how well the organisation is equipped to respond to the threat.

Such a risk assessment will give business functions and managers the knowledge to choose and prioritise mitigation measures, technical and financial, and therefore allocate resources effectively to protect value in the organisation.

It is essential that scenarios are rehearsed against the crisis management plans of the organisation and that any lessons learned from these rehearsals are embraced with the plans of the organisation. The Risk Manager is well placed to lead these rehearsals which should include representatives from IT, Human Resources, Finance, Legal and Communications.

1.2.6 Security Measures

Relevant and appropriate

All organisations should take account of the "CIA" paradigm (Confidentiality, Integrity and Availability), meaning that a set of rules limits access to information, the information is trustworthy and accurate, and it is available to authorised individuals. This model forms the basis for well understood concepts of threat, security-dimension and counter-measures such as interception, confidentiality and encryption.

International frameworks and standards set out best practices in security measures.[8] An information security framework or standard is a series of documented processes used to define policies and procedures around the implementation and ongoing management of information security controls. They are a blueprint for building an information security programme to manage risk and reduce vulnerabilities. Frameworks and standards should be tailored to meet the needs of the organisation and continuously evaluated to ensure they remain relevant and appropriate, for example by regular/specific incident monitoring: data analysis, network segmentation, network monitoring, vulnerability management, intrusion detection, etc.

In organisational terms, counter-measures include risk analysis, awareness campaigns, IT education and IT security policies.

1.2.7 Innovation

Technical and organisational

Cyber threats are evolving at an escalating pace and require continuous risk assessment and adaptation of the organisation's control environment. Innovation is, however, also generating tools that can make networks less vulnerable. Different network architecture based on multiple control systems, blockchain technologies for safer transactions or security devices equipped with machine-learning algorithms are some recent examples of ways to increase the level of cyber security.

Innovation can also be organisational. New forms of co-operation between stakeholders and private and public actors sharing knowledge and exchanging information can create more robust cyber defence within and between jurisdictions.

1.2.8 Preparedness, Resilience and Continuity

The importance of culture

Preparedness and resilience capabilities will involve logical protection, embedded training and business continuity and crisis management plans.

[8] Best practices in security measures can be looked up in professional standards such as ISO/IEC 27001:2013; ISO/IEC 27005:2011; ENISA Information Operations – Active Defence and Offensive Countermeasures; ENISA Technical Guideline on Security measures.

Senior leadership must retain oversight of how the organisation is equipped to react to cyber threats, especially when it concerns incidents with the potential to negatively impact the reputation of the organisation; this responsibility cannot be delegated. At the same time, corporate culture that encourages a collaborative approach to managing cyber risk and the rapid detection of any cyber incidents is at the heart of a preparedness strategy designed to minimise the impact of an attack on business continuity. Detection capabilities must include a management component. Key stakeholders involved in cyber risk governance must be sufficiently knowledgeable to identify a potential cyber incident and empowered to "speak up" when he or she becomes aware of a problem.

All business areas should be involved in the drawing up of business continuity and crisis management plans – avoidance of silo working is vital. The plans should be rehearsed at all levels of incident severity, and reviewed and updated on a continuing basis, to reflect lessons learned from rehearsals and from actual and near-miss cyber incidents.

1.3. THE THREE LINES OF DEFENCE

The Three Lines of Defence model is a suitable model for implementing a comprehensive and structured approach to cyber risk management (see Figure 1 in appendix). This model, which is internationally recognised, is consistent with the organisational guidelines already applied in the financial sector.

The Three Lines of Defence model[9] is a useful tool to illustrate the different roles in governance and risk management, the interplay between them and how they fit together to provide stronger corporate governance. Below, the Three Lines of Defence model is adapted to highlight the different functions of particular relevance to cyber security described in this paper. If cyber risk is to be managed effectively in organisations, there must be a "chain of trust" across all the relevant functions.

THE FIRST LINE

The first line of defence is responsible for implementing policy and standards, and has responsibility for day-to-day monitoring of networks and infrastructure. It is responsible for the management of risks and controls. The main identified functions are the IT department, the Human Resources, the Chief Data Officer and the Operations/ Business Units.

THE SECOND LINE

The second line of defence is responsible for performing the majority of the governance functions related to cyber security. Typically the CISO (Chief Information Security Officer) heads this line of defence, defining the policies, standards and technical configuration standards that are implemented by the first line. The second line ensures that the IT function, as part of the operational 1st line of defence is performing appropriate monitoring, reporting and tracking as part of its work programme.

The second line is usually responsible for assessing the risks and exposures related to cyber security against the organisation's risk appetite and ensuring that they are aligned. It monitors current and emerging risks and changes to laws and regulations, and collaborates with the first line functions to ensure appropriate control design.

In line with these responsibilities, common second line activities include designing cyber security policies and procedures; training and testing; conducting cyber risk assessments; monitoring incidents, key risk indicators and remediation; and assessing relationships with third parties and suppliers.

The Risk Management function is part of the second line of defence.

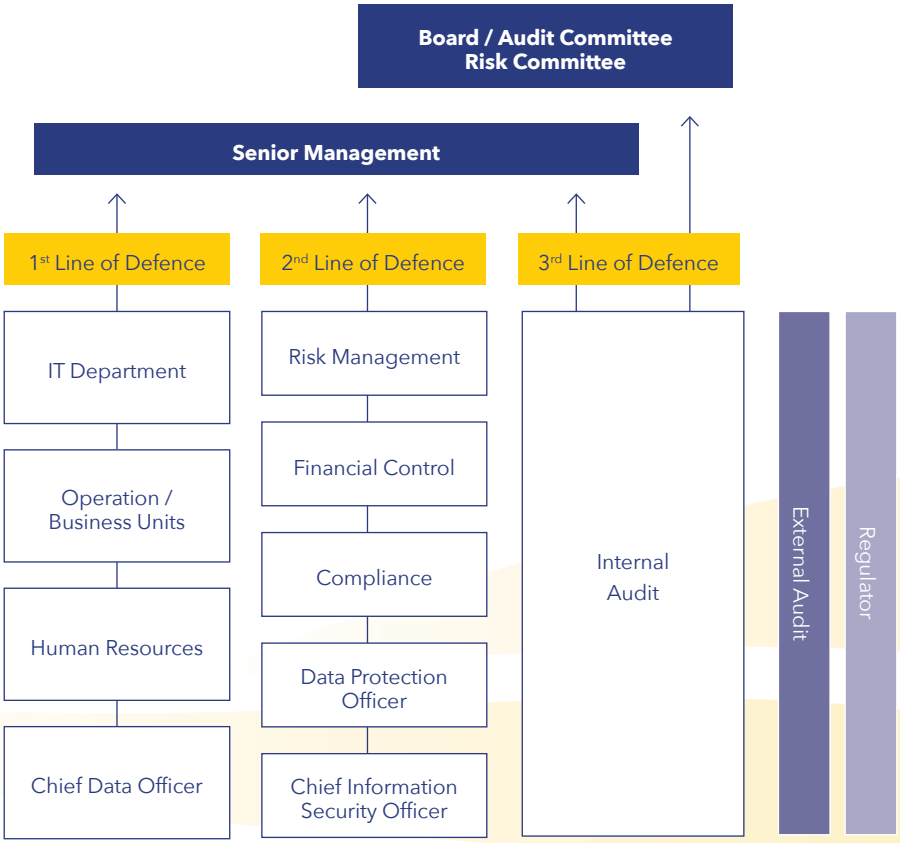
THE THIRD LINE

As the third line of defence, Internal Audit is responsible for providing an objective and independent assurance that the first and second lines of defence are functioning as designed, and looks at the overall coherence and consistency of the information security programme of the organisation. It should provide at least an annual health check to the Board on the state of that programme.

THE BOARD

The Board looks at the organisation's overall approach in relation to cyber risk and the effectiveness with which the different internal functions are collaborating and communicating. The functions in the first, second and third lines of defence need to work closely together, on an ongoing basis, to ensure that the Board has the level of assurance, awareness and understanding necessary to carry out this overarching responsibility.

This collaboration often involves working together to produce an overall assurance map for the organisation and its risks (see annexes: 3. Assurance map example).



2. PROPOSAL FOR A GOVERNANCE MODEL IN THE DIGITAL CONTEXT

Any cyber risk management model can only be efficient if it is implemented within the context of a sound governance model adapted to the needs of the individual organisation. Boards are responsible for the strategy but technical issues might impact the goals. The Board therefore relies on key functions within the organisation to discharge their duties. This is why the design of a governance model is critical.

2.1. THE BOARD

As part of its mandate to ensure the long-term viability and future development of the company, the Board has to take the right decisions in relation to the challenges embedded within digitisation[10].

This need to secure business resilience is not new. What is new is the scale, the complexity of the challenge and the speed of change, for which "traditional approaches" to risk and compliance are inadequate.

The Board, therefore, needs to have the capability within the organisation to respond to this challenge and ensure that it is adequately resourced and supported.

An integrated response across functions is necessary for the Board to increase the resilience of the organisation to cyber risks.

The Board and senior management of each organisation must determine the scale, nature and complexity of the response. They must be sufficiently educated and engaged to make informed decisions.

A Risk Committee and an Audit Committee are well placed to ensure that the same language is spoken across all relevant functions, and to give a unified opinion to the Board.

In some organisations, the Audit Committee has enlarged its remit and changed its name to the Audit and Risk Committee in recognition of the collaboration between the risk management and internal audit functions. Whether there is one committee or two, arrangements to ensure a coherent, comprehensive and high-profile approach to cyber risk are essential. The recommendations below deal with different possible scenarios.

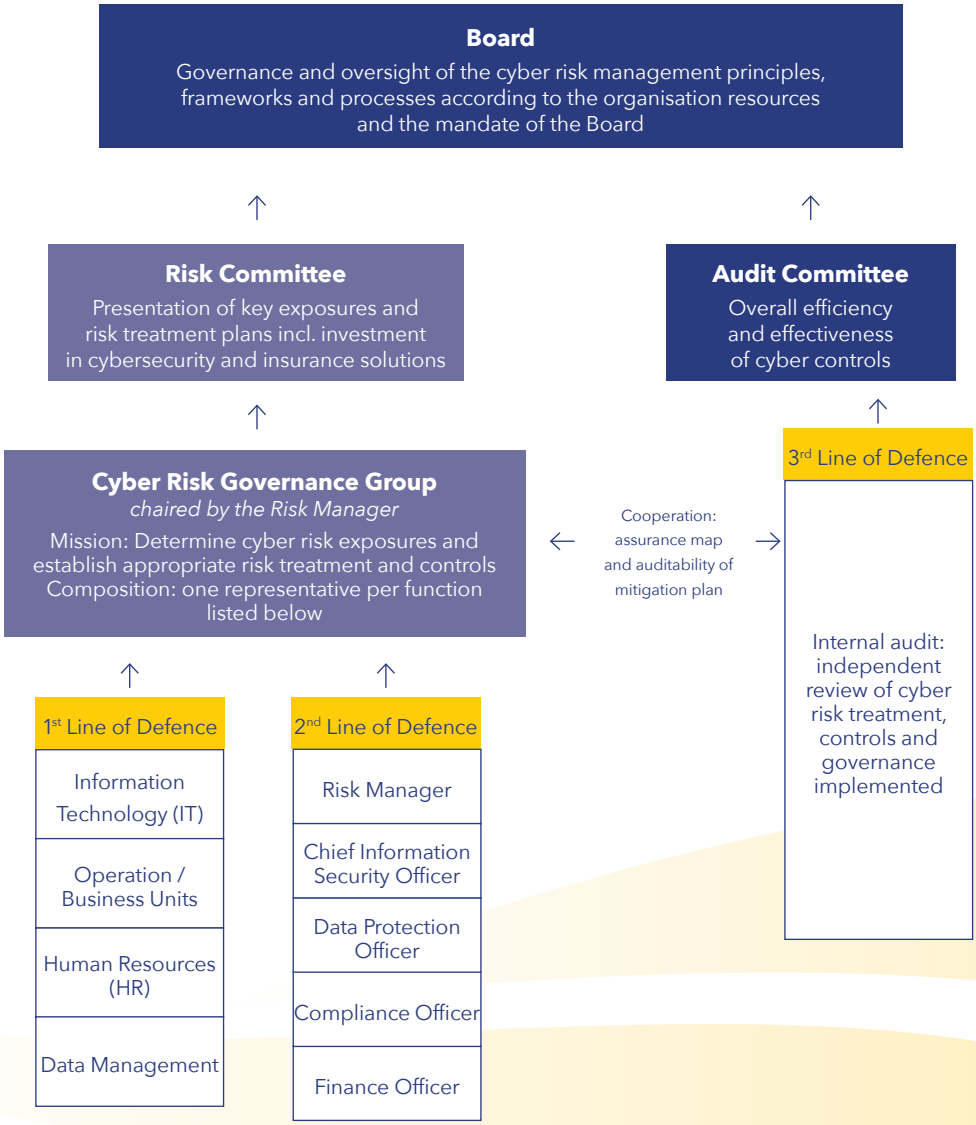
2.2. THE RISK COMMITTEE AND THE CYBER RISK GOVERNANCE GROUP

Because cyber risks affect strategic aspects of the Board's mandate (such as valuation, reputation and trust), and the complexity of assessing cyber risks, an organisation should establish a designated Cyber Risk Governance Group. This should be an executive body and not be seen as a new committee of the Board as it would typically report to the Risk Committee, which will operate across functions at an enterprise level addressing all risks.

The Cyber Risk Governance Group should be co-ordinated by the Risk Manager, who is best positioned with expertise to lead the identification, assessment, quantification and mitigation of cyber risks in line with the organisation's overall Enterprise Risk Management (ERM).

The Cyber Risk Governance Group is composed of representatives of key functions involved in cyber including IT, HR, Communications, Finance and Legal as well as the Data Protection Officer (DPO) which is a mandatory function and the Chief Information Security Officer (CISO). The Risk Manager will also assist the other functions in terms of procedures, systems, processes and training.

[10] For more details, see the World Economic Forum publication Advancing Cyber Resilience Principles and Tools for Boards published on 18 January 2017 http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf


Board
Governance and oversight of the cyber risk management principles, frameworks and processes according to the organisation resources and the mandate of the Board
Risk Committee
Presentation of key exposures and risk treatment plans incl. investment in cybersecurity and insurance solutions
Audit Committee
Overall efficiency and effectiveness of cyber controls
Cyber Risk Governance Group
chaired by the Risk Manager
Mission: Determine cyber risk exposures and establish appropriate risk treatment and controls
Composition: one representative per function listed below
Cooperation: assurance map and auditability of mitigation plan
3rd Line of Defence
Internal audit: independent review of cyber risk treatment, controls and governance implemented
1st Line of Defence
Information Technology (IT)
Operation / Business Units
Human Resources (HR)
Data Management
2nd Line of Defence
Risk Manager
Chief Information Security Officer
Data Protection Officer
Compliance Officer
Finance Officer

The mandate of the Cyber Risk Governance Group is to act as the interface with each key function to determine their cyber risk exposure and establish possible mitigation plans. The Cyber Governance Group will present to the Risk Committee and the Board cyber risk mitigation plans including investment in cybersecurity and insurance solutions and a set of key performance indicators including cyber benchmarks appropriate to the organisation.

The decision to create a Cyber Risk Governance Group for overseeing the management of cyber risks would send a strong positive message to external stakeholders about the cyber risk governance of the organisation.

The Cyber Risk Governance Group works with the Internal Auditors to exchange information on the ERM system and ensure that mitigation plans are auditable. The plans should be documented with clearly defined roles and responsibilities in the event of a disruptive cybersecurity exploit. The auditability "by design" of all mitigation plans is indeed crucial in order to evaluate their impact and review the alignment with the strategy.

The Internal Auditors share with the Cyber Risk Governance Group the assurance map[11] for the cyber risks. The mapping is done across the organisation to understand where the overall risk and assurance roles and accountabilities reside. The aim is to ensure that there is a comprehensive risk and assurance process in place with no duplicated effort or potential gaps.

2.3. ROLE OF THE THREE LINES OF DEFENCE IN THE DIGITAL CONTEXT

3.1 First Line of Defence

The functions described below play a role in cyber risk management and the establishment of mitigation plans. They typically have ownership, responsibility and accountability for assessing, controlling and mitigating risks.

a) Information Technology

The Information Technology (IT) function is typically active in administering security procedures, training and testing, maintaining secure device configurations, and ensuring that software and security patches are up-to-date. Sometimes IT is also in charge of information security in the organisation, although the trend is to operate an information security function independent from IT which reports directly to the to senior management and the Board.

Risk Managers support IT in defining risk management procedures and ensuring integration with other business functions. Internal Auditors review the activities and assess the risks and the quality of the internal controls (IT audit). They can and should seek the assistance of specialists in specific IT domains.

b) Data Management

Within the Data Management function, the Chief Data Officer (CDO) is a senior executive who is responsible for the organisation's enterprise-wide data and information strategy, for governance, control and policy development, and for effective implementation. The CDO's role combines accountability and responsibility for information protection and privacy, information governance, data quality and data life cycle management, along with the exploitation of data assets to create business value.

When the CISO function exists, it often takes the role and tasks of the CDO.

CDOs are increasingly tasked with driving innovation and optimising the use of data by:

- Finding ways to use existing data as a competitive advantage;
- Increasing data valuation by combining internal and external sources;
- Data monetising: exploring new sources of revenue tied to data;
- Ensuring data privacy and security;
- Maintaining data quality and integrity.

[11] International Professional Practices Framework, IIA Global, Practice Advisory Guide 2050-2, Assurance Map

The CDO assists the Risk Manager defining procedures for data protection and for the assessment of data management. Internal Audit will consult the CDO as a "data" specialist and make recommendations on the review of data controls.

c) Human Resources

As cyber security problems can result from action from within the company's own workforce, the human resources (HR) function is an important participant. We recommend the following key "basic precautions" for HR teams:

- Ensure that newly hired employees have not brought any external data or information with them;
- Remove access rights of any former employees from the date/hour of exit. This is crucial because many incidents have been reported of former employees stealing confidential company data upon departure;
- Ensure effective disciplinary procedures and actions for employees who do not comply with security guidelines;
- Play a leading communications role in addressing the concerns of employees in the event of a disruptive cyber incident (denial of access of locations and systems);
- Provide clear security guidelines for mobile devices granted to personnel;
- Establish a clear "whistleblowing" policy and procedure[12]. Internal Audit could have a prominent role in investigating any allegations of wrongdoing;

HR personnel should focus on their own security processes and in all circumstances should preserve their right of audit.

Risk Managers work with HR to identify the key actors, the new risks and the ways to reduce them. Internal Audit reviews the new processes set up by HR, gives an independent view on assurance and makes recommendations to improve internal controls.

3.2 Second Line of Defence

The actors in the second line of defence monitor and facilitate the implementation of effective risk management practices by the first line, and assist risk owners in reporting adequate risk-related information throughout the organisation.

a) Risk Managers

Responsible for the oversight of cyber risk management, the Risk Manager must ensure that the organisation can continue to perform its activities, based on criteria accepted by the organisation's executive leadership and validated by key functional peers in the second line.

The Cyber Risk Governance Group should meet regularly to identify critical resources, including information, which are needed for the effective and efficient operation of the organisation and achievement of short- and long-term business objectives.

The Risk Manager is responsible for defining the cyber risk exposure of the organisation and acts as facilitator between the Board and relevant business functions, such as IT, finance, compliance and human resources.

The Risk Manager coordinates the Risk Committee and the Cyber Risk Governance Group, ensuring that they are integrated and deliver their objectives and responsibilities. As chairman of the Group, the Risk Manager works with each key function described in this document to understand the business impacts of cyber risks and proposes the appropriate mitigation plans for the organisation to the Risk Committee.

The Risk Manager adds a unique value in identifying and quantifying the risk exposure with a financial analysis. He/she organises quantification aspects of cyber security, and must arbitrate between operating requirements and security constraints. For example, it may be desirable to have open access to information for business development purposes, although specific customer requirements mean that some data need to be behind secure information barriers with strict access control.

[12] In some organisations, this role is also played by the Chief Compliance

The Risk Manager decides about insurance programmes to obtain the most effective level of insurance cover at the best achievable cost. This is based on an analysis of the policies already in place and additional cover which may be purchased. Cyber-specific policies should provide external assistance support including access to, and fees for, data breach experts, media advisors and legal advisors required in the case of an insured event coming to pass.

In the implementation of a cyber risk management framework, the Internal Audit function needs to be kept informed during the development of the cyber risk management framework, and may offer advice in its consulting role. A deep understanding both of the organisation and of the technical issues is necessary to assess the execution and the performance of such processes[13].

b) Data Protection Officer

The Data Protection Officer (DPO) is responsible for all matters related to data protection. The role covers everything from providing information and advice to the organisation, to monitoring compliance and acting as the first point of contact for data protection authorities. The DPO function will be mandatory in the European Union as from May 2018 when the core activities of an organisation require a regular and systematic monitoring of data subjects on a large scale (see annex 2 on NIS and GDPR provisions).[14]

The main responsibility of the DPO is to ensure compliance with the applicable privacy and data protection regulations. He/she advises on and monitors the execution of Data Privacy Impact Assessments, performed when process and/or marketing activities pose a high risk to data protection.

The DPO is fully independent and should neither seek nor receive any instruction regarding the exercise of these duties. He/she reports directly to the highest level of executive management. The role of DPO does not necessarily need to be a new appointment. It could be exercised by other existing positions in the organisation, notably the risk manager, with some adjustments, thus avoiding an extra cost. In some organisations, the DPO sits within the legal function.

Co-ordination with Internal Audit is recommended in order to avoid duplication of work. Results of the audits of both functions should be exchanged and discussed, and, vitally, will be used to provide information on the level of assurance to the Audit Committee and the Board.

To understand where the DPO should sit in the organisation, it is important to note that this function requires a certain level of neutrality and independence from personal data-processing activities. Therefore, we are convinced that sufficient separation of the DPO from IT is necessary to ensure that cyber risk management strategies remain aligned with the business strategy and objectives.

The DPO should be part of the Risk Committee and Cyber Risk Governance Group as this is a mandatory function under the EU GDPR and will ensure that the protection of personal data is taken into account in the mitigation plans chosen by the Risk Committee for proposal to the Board. Another justification for the presence of the DPO at this Risk Committee is also the requirement for the DPO to report to the highest management level[15].

---

[13] This is part of the auditability by design of all mitigation plans as mentioned in page 13 at section 2) The Risk Committee and the Cyber Risk Governance Group

[14] For more information on the concepts of core activities, large scale, regular and systematic monitoring, see the DPO Guidelines released by the Article 29 Working Party on 5 April 2017, available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

[15] According to Guidelines on Data Protection Officers (DPOs) adopted on 13 December 2016 by the ARTICLE 29 DATA PROTECTION WORKING PARTY, such direct reporting should ensure that senior management (e.g. board of directors) is aware of the DPO's advice and recommendations as part of the DPO's mission to inform and advise the controller or the processor. This direct reporting is also valid when the highest management level is provided with an annual report of the DPO's activities. http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

c) Chief Information Security Officer

The Chief Information Security Officer (CISO) or equivalent coordinates and manages information security across the organisation, including IT, human resources, communications, legal, facilities management, risk management and other functions. The most successful CISOs balance security, productivity and innovation. The CISO is an advocate for security as well as a business enabler, while being mindful of the need to protect the organisation from the unexpected.

There is currently a debate about the reporting line for the CISO and the positioning of the function (in the IT function or not). In smaller organisations, this function is often vested in the non-executive position of Information Security Officer (ISO) or Chief Information Officer (CIO).

The CISO plays a key role managing cyber risks efficiently and effectively by selecting the mitigation plans proposed by the different functions in accordance with IT, to ensure they are in line with the information security policy applicable in the organisation. The CISO should be a member of the Cyber Risk Governance Group.

d) Finance Officer

In a digital context, Finance Officers provide the financial support for the investment in cyber security to manage the risks internally, and validate the budget for the cost of risk transfer, including insurance. They are also responsible for reporting the financial situation of the organisation to external stakeholders, ensuring compliance with relevant legislation and managing investor affairs.

Although the position of Risk Manager in the organisation will vary, the Risk Manager is often formally part of the Finance team[16]. Risk Managers work with the Financial Controller, where that role exists, to obtain the key financial inputs for quantification of the exposure of the organisation to risk. The Risk Manager also provides the CFO with recommendations on risk financing, and as part of this, the insurance strategy, to validate financing options and budget.

As an independent function, Internal Audit is never part of Finance, but it interacts with Finance by validating that identified processes are effectively applied. In the event of deficiencies, Internal Audit provides Finance with its recommendations for corrective measures. In particular, Internal Audit reviews the fraud and ethics processes and compliance with legislation.

e) Compliance Officer

Legal teams are not only concerned with compliance risks, cyber incidents can also create liabilities.

Contractual obligations with customers and suppliers can increase the potential impact of a cyber incident in the organisation if their activities and assets are affected. Suitably qualified experts must scrutinise contracts before they are agreed.

The scope of liabilities for cyber incidents is especially complex in organisations with large supply chains or business ecosystems, notably where information flows across geographic borders and between business functions and stakeholders. These liabilities will sometimes also include increasingly heavy fines for breaching the provisions of the new legislation on data protection in the European Union.

The compliance function plays a role in the cyber risk assessment process coordinated by the Risk Manager. Internal Audit works closely with the compliance function assessing the risks of non-compliance with regulations. As digitisation is now "business as usual" and an increasing source of opportunity, any legal changes concerning data and cyber security need to be risk assessed.

3.3 Third Line of Defence: Internal Audit

Under the Institute of Internal Auditors (IIA) International Professional Practice Framework, the mission of Internal Audit is "to enhance and protect organisational value by providing risk-based and objective assurance, advice and insight."[17] This mission can apply equally in the

[16] According to the latest FERMA European Risk and Insurance Report 2016, CFOs remain the primary reporting line for risk and insurance managers. See slides 25 and 26 at https://www.slideshare.net/FermaForum/ferma-risk-and-insurance-report-2016-full-report-with-questions-67394892

[17] IIA, 'International Professional Practices Framework', https://global.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx

specific area of organisations' exposure to cyber security risk.

Internal Audit[18] plays an important role in the development, implementation and ongoing assessment of organisations' cyber risk management plans, in coordination with the Cyber Risk Governance Group.

The main method through which Internal Audit can fulfil this role is the provision of independent assurance to the Board (via the Audit Committee) on the functioning of cyber security processes, including the overall effectiveness of the activities performed by the first and second lines of defence in managing and mitigating cybersecurity risks and threats.

This assurance is provided through Internal Audit's work plan based on key risks assessed and how these risks are managed, by testing the controls, policies and procedures put in place.

Common activities of the third line of defence include:

- Providing independent, ongoing evaluations of preventive and detection measures;
- Evaluating IT assets of users with privileged access for standard security configurations, problematic websites, malicious software and data exfiltration;
- Tracking diligence of remediation;
- Conducting risk-based and objective assurance of third parties and suppliers, in line with the work of the second line of defence in this area.

Furthermore, as set out in the IIA Global Technology Audit Guide, as the third line of defence, the Internal Audit function can be consulted about the establishment of cyber risk management arrangements[19].

2.4. EXTERNAL STAKEHOLDERS

a) Insurers

The first condition for opening a dialogue with the insurance market is for the organisation to understand its exposure to cyber risks. Once the cyber risk exposure has been identified, managed and controlled, the organisation can decide whether to invest in increasing its cyber protection level, based on the data provided by the Risk Manager (i.e. exposure, impact and financial implications) and its risk appetite. The Risk Manager should determine which cyber risks may already be insured under existing insurance policies to determine the residual risk.

Only then should a dialogue with the insurance market start, with a view to transferring the residual risk to the insurer and considering what additional solutions might be valuable as part of a specific cyber insurance programme.

From an insurance perspective, insurers without in-house expertise on cyber security may need to partner with third parties to assess the level of management of cyber risks. Unfortunately, the results of these investigations can differ between insurers as a consequence of different methods and approaches. To organise a dialogue on cyber risk based on trust and confidentiality, Risk Managers and insurers must work towards similar conclusions about the cyber risk exposure of the organisation.

The conditions for a fruitful dialogue between insured and insurers must establish how interested parties communicate about underwriting information; how confidentiality is managed; how claims are lodged; and how to address the involvement of external experts to assess and respond to cyber incidents. A confidential dialogue on cyber risk exposure is necessary to ensure that the cover is tailored to the needs of the organisation. A confidential dialogue will also enable better exchanges when an event occurs. The insurance market must understand the circumstances of the insured better; the insured must in turn get better at explaining its cyber exposure and protection needs.

[18] The opinion shared in the section is an extract from Chartered IIA (UK & Ireland) on Cybersecurity, 2017

[19] IIA, 'Assessing Cyber security Risk: Roles of the Three Lines of Defence', 2016, p. 13-14, https://global.theiia.org/standards-guidance/recommendedguidance/ practice-guides/Pages/GTAG-Assessing-Cyber security-Risk-Roles-of-the-Three-Lines-of-Defence.aspx : Internal audit can assist for the prioritising response and control activities; validated cyber risk security provisions.

To support the development of a better-functioning cyber insurance market, it seems essential to share the same language to foster a qualitative dialogue between the Risk Manager and the insurer. This necessity for a common language on cyber risk also applies to the other stakeholders in the management of cyber risks (operational, IT, insurers, lawyers, etc) who tackle the subject using their own individual definitions, sometimes without sharing them, or at least without understanding the interpretation of other parties.

b) Co-operation with public authorities

Public authorities consider cyber security as a societal and geopolitical issue, affecting vital infrastructure as well as the rights and freedom of citizens, and the economy. Because major and disruptive cyber incidents would have systemic impacts across borders, collaboration between governments, security organisations, companies and insurers is needed to protect critical infrastructure and increase resilience. In case of catastrophic cyber losses, it is unlikely that the private sector on its own could indemnify the liabilities that could arise.

At state level, organisations have increasingly close relationships with information security and data protection authorities. These interactions are necessary to understand not only the expectations of the regulators to ensure compliance, but also to help authorities increase the overall resilience of the community towards cyber-attacks.

The level of cyber resilience could be increased by a greater cooperation between public authorities and organisations, notably in the following two areas:

1. Establishing a common framework that clearly defines liabilities right along the supply chain to end customers, describing who carries which type of cyber risk and to what extent.

2. Developing a framework for a cyber security risk assessment supported by a database of cyber insurance claims in order to have up-to-date status on cyber threats and the costs of known losses and near misses.

c) Vendors

The Cyber Risk Governance Group should identify the critical vendors that should be subject to a specific risk assessment. Organisations face significant risks if their vendor relationships are not carefully managed and monitored. Therefore, management should establish processes to review vendor risks on an ongoing basis.

The level of screening should be tailored to the risks posed by each vendor. Security, privacy and business requirements should be addressed in the Request for Proposals (RFP) or tender process. It is also recommended that relevant security and privacy questionnaires should be sent to potential vendors.

Effective vendor risk management is essential to ensure that the use of service and goods from providers and/or suppliers do not generate potential adverse events (business disruption, security and/or privacy breach…) which could negatively impact the company's business performance.

The risks associated with vendor relationships, however, will vary depending on the vendor's position along the supply chain, and its criticality in terms of service or process provided and/or outsourced. As with any contractual activities, it is important to discuss with the legal function the selection of the most appropriate requirements and wording for the company's specific circumstances.

2.5. INTERACTIONS BETWEEN RISK MANAGERS AND INTERNAL AUDITORS

Each function has its own specific role, responsibilities and activities, but there are some areas of overlap. We have shown throughout this paper, close co-operation, based on a sound understanding of the complementary functions, is absolutely essential not only to manage cyber risks in an efficient manner but also to ensure that the management has a strategy and plan in place to notify the Board, the authorities, the customers and the public in the event of a major cyber incidents. In the next page is summarised some of the key areas of complementary activity and collaboration[20].

[20] IIA Position Paper (2009) : The Role of Internal Auditing in enterprise wide risk management (the original fan has been adapted to the Cyber Risk Management context): https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Role%20of%20Internal%20Auditing%20in%20Enterprise%20Risk%20Management.pdf

Internal Audit alone	Independently review cyber controls and cyber risk program and report control weaknesses to the Audit Committee
	Independently review cyber security culture in the organisation
	Independently review compliance with legislation
	Independently review the process for the crisis management plan
	Make recommendations for improving the cyber control environment
Internal Audit or Risk Managers	Exchange on cyber risk exposure and on cyber risk management effectiveness
	Ensure auditability of control mechanisms
	Inform and guide the Audit Committee on cyber security issues
	Establish the cyber risk assurance map
Risk Managers alone	Coordinate the risk committee reporting to the Board on cyber risk exposure and mitigation plans including insurance
	Chair the Cyber Risk Governance Group
	Identify and quantify cyber risk exposure (with stress tests and scenarios)
	Establish with the first and second lines of defence controls for cyber risk management implementation
	Establish oversight for cyber risk management implementation

3. CONCLUSION

- There is a trend toward more transparency and regulation over cyber security. The implementation of the two new European Union laws impacting cybersecurity, the Network and Information Security Directive and General Data Protection Regulation, will reinforce the obligations for organisations.

- Beyond IT, cybersecurity is also becoming a matter of corporate governance, and the right governance framework is crucial to an efficient management of cyber risks.

- With a strong cyber risk management framework in place, organisations will manage the challenges and opportunities of digitisation in a holistic way and ensure effective management of cyber risk across the organisation.

- The eight principles developed by the OECD for a digital security risk management are applicable to the private sector and describe all the aspects to be considered to manage cyber risks effectively.

- A cyber risk governance framework should be based on the Three Lines of Defence model to define the role of each function, including that of the Risk Committee and the Audit Committee.

- Risk Managers should coordinate the Risk Committee which will present selected mitigation plans, including investments in cyber security and insurance coverage solutions, to the Board of Directors.

- Organisations should create a "Cyber Risk Governance Group", reporting to the Risk Committee and chaired by the Risk Manager, to determine with other functions the cyber risk exposure, expressed financially, and establish the possible mitigation plans. The Group should cooperate with Internal Auditors to avoid silos.

- Internal Auditors review the controls implemented and give an independent assurance to the Audit Committee about the cyber risk, the efficiency of the controls and the mitigation plans.

- The Risk Committees and the Audit Committees must collaborate to present a common view to the Board about cyber risk management.

- The collaboration starts with Internal Auditors working together with Risk Managers:

  - They ensure that all the mitigation measures put in place for cyber risks can be audited and that duplication of work is avoided in terms of assessments. They agree on the assurance coverage of each function by establishing an assurance map.

  - They also work together on recommendations for constant improvements in the controls and processes in place for cyber security

  - Although the definitions in the guidance are based on large organisations, the same principles of cyber risk management are valid for private and public organisations, large or small. The identification, quantification and mitigation of cyber risks are key for all organisations.

  - The proposed cyber governance framework is applicable in all organisations. Some functions may be shared but the general principles of controls in layers and close co-operation are recommended.

  - The proposed cyber governance framework will demonstrate to the external stakeholders how cyber risks are managed, not only from a pure IT perspective but also from an enterprise perspective.

  - The proposed cyber governance framework will increase the resilience of organisations to cyber risks and promote a greater competitiveness for European organisations globally.

4. ANNEXES

1. Operational risk assessment: example of a stress test/business impact analysis based on a cyber risk register

	STRESS TEST => Business Impact Analysis (BIA)	1 not significant (less € XXX) up to 5 critical (Excess € XXXX)			
N°	Cyber Risk Threats/perils register	Confidentiality	Integrity	Availability	Privacy
1	**Data privacy breach (personal info)**				
	Third party (customer information theft / access)				
	Customer Privacy information breach (IT or SW failure)				
2	**Copyright/trademark infringement**				
	IPR infringement/IP theft				
	Trade secrets stolen				
3	**Mobile Equipment/devices/smartphone lost or stolen**				
	Theft or loss of hardware (smartphone, laptop,...) => «Improper disposal»				
	Improper use or disposal of equipment whereby it gets lost/stolen/looked into				
4	**Internet portals hacking**				
	Information/data hacking				
	E-commerce site fraud				
5	**Unauthorised access/use**				
	Misuse of access right and privileges (internal & external)				
	Unauthorised info acquisition/espionage				
6	**Law infringement**				
	Illegal tapping telephone conversion &:or customer data flows (ex PABX hacking)				
	Customer Location insights information abuse				
7	**Information systems attacks**				
	Malware/Spam's & malicious code				
	Denial of service				
8	**Human error**				
	Employee security error & omission (ex.) data base containing sensitive data to be Internet-facing and searchable through Google				
	Target employees with carefully crafted corrupted phishing emails				
9	**Social engineering**				
	E-mail scams, Phishing attack				
	Cyber Extortion				
10	**Insecure network transmissions**				
	Internet failures (IP connections breach)				
	Own outsourced cloud services (incl CRM) hacking				
11	**Impaired access to customer systems**				
	Customer DB/application intrusion (incl. in the cloud):				
	Access rights abused/misused internally (incl exit employees)				
12	**Supply chain/outsourcing/offshoring Fraud & infidelity**				
	(Non) authorised access/disclosure caused by outsourcing/contractors				
	Unauthorised/uncontrolled copies of sensitive/confidential information's				
13	**Code of conduct internal policies violation**				
	Financial privileged info abuse or protected data disclosure				
	Employee confidential info theft (USB, ...)/rogue employee/Employee fraudulent act				
14	**Unauthorised payment transactions**				
	Fraud on payment processing/fund transfer				
	Abuse of customer credit cards information				
15	**Branded exploits against customer & public**				
	Registration of domains that exploit company brand without approval				
	Creation or usage of social media accounts using company brands				

2. Summary and comparison of Network & Information Security (NIS) Directive and General Data Protection Regulation (GDPR)

	NIS DIRECTIVE	GDPR
Entities covered	Nationally designated providers of essential services; digital service providers - (micro and small enterprises are excluded if they have annual turnover - less than 10mio Euro)	Data controllers and processors of "Personal data"
Competent national supervisory authority/regulator	A member state's "competent authority" or its 'computer security incident response team' (CSIRT)	The data protection authorities
Risk mitigation measures required	(1) To adopt "appropriate and proportionate technical and organisational measures" (2) Digital service providers are further required to ensure the level of security, taking into account the following elements: - security system and facilities - incident management - business continuity management - monitoring, audition and testing - compliance with international standards	(1) Pseudonymisation and/or encryption of personal data (2) Ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data (3) Ensure ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident (4) Establish a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing (5) Appointment of Data Protection Officer (DPO) when the core activities of an organisation require a regular and systematic monitoring of data subjects on a large scale (6) Data Protection Impact Assessment
Fines	EU countries are responsible for determining their own "effective, proportionate and dissuasive" penalties for infringement of the NIS rules	(1) Regulators have authority to issue penalties equal to the greater of €€10million or 2% of the entity's global gross revenue for violations of record-keeping, security, breach notification, and privacy impact assessment obligations (2) Violations of obligations related to legal justification for processing (including consent…), data subject rights, and cross-border data transfers may result in penalties of the greater of €20 million or 4% of the entity's global gross revenue
Must be implemented into national law by member states.	Yes, member states must implement the Directive into national laws by 9 May 2018	It is an EU regulation and will apply directly to all member states after implementation period until 25 May 2018
Harm threshold for duty to notify	(1) Actual, adverse and significant impact on continuity of essential services; or (2) actual, adverse and substantial impact on provision of enumerated digital services	Accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed
Duty to notify Supervisory Authority (SA)	Yes, a member state's "competent authority" or its 'computer security incident response team' (CSIRT) "without undue delay" – unless (1) another EU legal act with "at least equivalent" notification requirements already requires breach notification; or (2) the affected entity a communications company subject to Art. 13a of Directive 2002/21/EC	Yes, unless the breach is "unlikely to result in a risk to the rights and freedoms of individuals"
Deadlines for notification to SA	Without undue delay (but national law can shorten to "immediately")	Generally within 72h of becoming aware of a breach; any longer period may not be undue and must be justified
Content of notice to SA	Set by national law	"At least" the nature of the breach, categories and approximate number of data records, DPO contact details or information contact points, likely consequences of the breach and measures taken or proposed to address/ mitigate the breach
Duty to notify the data subject	Not required under NIS Directive; possible under national legislation	Yes, if (1) a breach is likely to result in high risk to rights and freedoms of individuals; and (2) none of the Art 32., 3. exceptions apply (ex ante encryption, ex post mitigation or disproportionate burden)
Deadline to notify the data subject	N/A	Without undue delay
Data subjects required to be notified	N/A	Company must communicate the personal data breach to the data subject
Content of report to data subject	N/A	Describe in plain language the nature of the breach and provide "At least" DPO contact details or information contact points, likely consequences of the breach and measures taken or proposed to address/mitigate the breach

3. Assurance map example

	1st line: Control Self Assessment				2d line: Monitoring					3d line:	Current Overall Assurance
	IT Depart-ment	Opera-tions/ Business Units	Human Re-sources	CDO	CISO	DPO	Financial Control	Com-pliance	Risk	Internal Audit	
Process1											
Process2											
Process3											
...											

- High Assurance : Satisfactory
- Medium Assurance : Improvement needed
- No Assurance : Not satisfactory
- Not applicable

4. Interesting Readings and Sources

1. Fireeye / Marsh & McLennan Companies, "Cyber risk report 2017 – Cyber threats: a perfect storm about to hit Europe" (2017)
2. Marsh & McLennan Companies, "MMC CYBER HANDBOOK – Increasing resilience in the digital economy" (2016)
3. World Economic Forum, "Advancing Cyber Resilience Principles and Tools for Boards" (2017)
4. Slovak Presidency in the Council of the EU, "Conference on Cyber Issues under the Slovak Presidency in the Council of the EU" (2016)
5. Marsh & McLennan Companies, "Continental European Cyber Risk Survey: 2016 Report" (2016)
6. Palo Alto Networks - Duncan Brown, "the State of the Art" Paradox White Paper" (2016)
7. OECD, Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document (2015)
8. Georgia Tech Information Security Center, "Governance of Cybersecurity: 2015 Report" (2015)
9. ISACA, The Institute of Internal Auditors Research Foundation, "Cybersecurity – What the Board of Directors needs to ask" (2014)
10. National Association of Corporate Directors, "Cyber-Risk Oversight" (2014)

5. ECIIA/FERMA JOINT EXPERT GROUP

NAME		ORGANISATION	TITLE	ASSOCIATION
Roland	Bittner	Deutsche Bank	Corporate Insurance Manager Marine & Specialty / Property	GVNW
Philippe	Cotelle	Airbus Defence & Space	Head of Insurance and Risk Management	AMRAE
Kristine	Esper Raffel	Copenhagen Airport	Group Risk Manager	DARIM
Julia	Graham	AIRMIC	Deputy CEO & Technical Director	AIRMIC
Chiara	Guizzetti	IIA Italy	Technical Management Manager	IIA Italy
Raúl	Mateos Martín	BBVA	Internal Auditor	IIA Spain
Alisdair	McIntosh	Chartered IIA (UK & Ireland)	Policy and External Relations Director	Chartered IIA (UK & Ireland)
David	Metivier	Sodexo	Group IS&T Audit Director	IFACI
Ivo	Miltchanski	Risk Consult Bulgaria Ltd	Risk Manager & Loss Adjuster	BRIMA
Olivier	Moumal	Proximus	Director Audit Risk & Compliance GCA-ARC	BELRIM
Alfredo	Zorzo	One eSecurity	Risk & Insurance Director/ Business Development Director	AGERS
Pascale	Vanden-bussche	ECIIA	Secretary General	ECIIA
Typhaine	Beaupérin	FERMA	Chief Executive Officer	FERMA
Julien	Bedhouche	FERMA	European Affairs Adviser	FERMA

Federation of European Risk Management Associations (FERMA)

Avenue de Tervuren 273 Tervurenlaan B12
1150 Brussels, Belgium
T. +32 2 761 94 32 - F. +32 2 771 87 20
Email: enquiries@ferma.eu
Transparency Register N°018778010447-60
www.ferma.eu

European Confederation of Institutes of Internal Auditing (ECIIA)

Koningsstraat 109-111 B5
1000 Brussels, Belgium
T.+32 2 217 33 20 - F. +32 2 217 33 20
Email: info@eciia.eu
Transparency Register N°849170014736-52
www.eciia.eu