GUIDE TO CYBER SECURITY FOR DIRECTORS OF COMPANIES

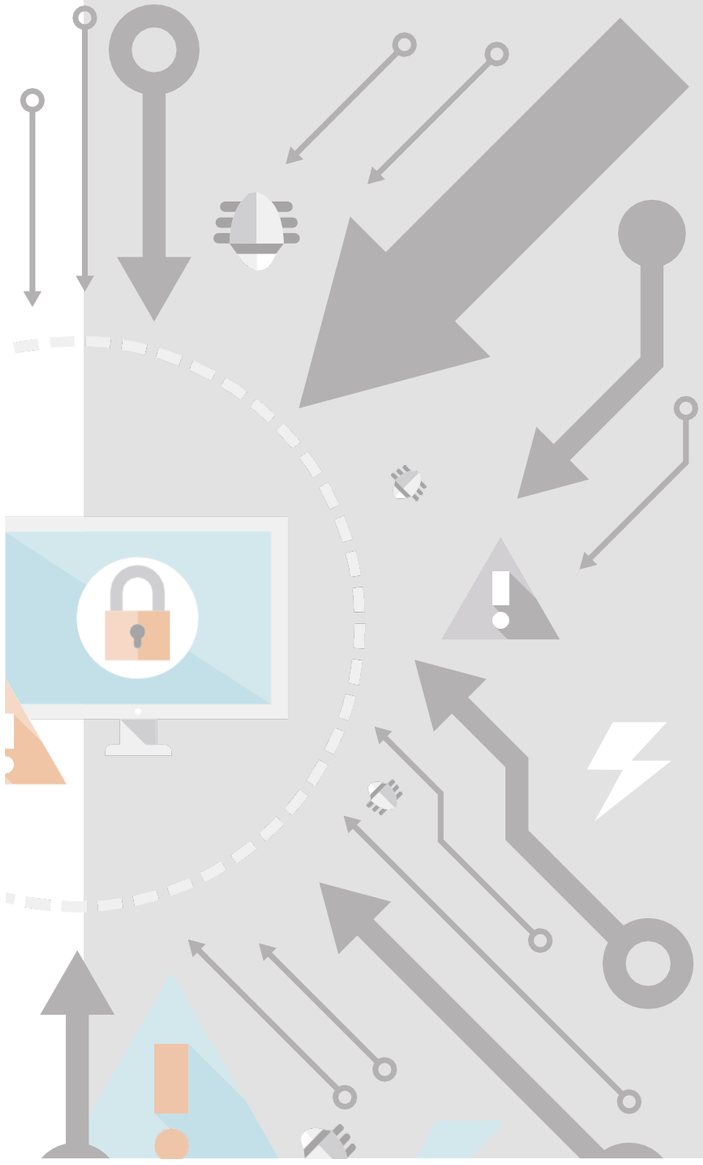


TABLE OF CONTENTS

1. TARGET AUDIENCE OF THIS GUIDE

This guide is intended for Directors across **all** organisations, regardless of size or whether they are public or private. Throughout this guide, we use the term 'Directors' to refer to members of the board of directors, business owners and members of supervisory boards (if any). The document is intended as a general guide for Directors to manage and oversee the cyber risk and resilience of their organization and, where relevant, to comply with obligations under European cybersecurity laws, like the Second Network and Information Systems Directive ("**NIS2**"), the Digital Operational Resilience Act ("**DORA**") and the Cyber Resilience Act (the "**CRA**"). This document is intended as a guide and should not be consulted as constituting legal advice.

2. WHY IS THIS GUIDE IMPORTANT FOR YOU?

Cyber threats are usually external in nature. They come from adversaries – such as cyber criminals or hostile states – intending and able to cause harm to your organisation (or a supplier).

Our society, economy and national security are heavily dependent on information and communication technology (ICT). Increasingly, machines in production lines and businesses' logistical infrastructure are also connected to the internet. We are vulnerable if something goes wrong, and many organisations are not well prepared for a 'no-ICT' situation. In times of geopolitical tension, organisations are more vulnerable to digital disruption. Cyber security is no longer just an ICT issue – it is a strategic priority for Directors. Directors are subject to a range of statutory and common law duties under national law as part of their role in managing the business of a company.[1] These include ensuring that their organisation has effective risk management and control systems in place. Directors may be held personally liable for breach of these duties under national law, including potential restriction and disqualification as Directors, or civil or criminal liability in certain circumstances.

As cyber security risks consistently rank among the top three risks facing any organisation, it is essential that Directors have sufficient cyber expertise, and that cyber risks are fully integrated into regular risk management and control systems. Cyber security risks are a **strategic** risk. It is not sufficient to delegate responsibility to the Company's IT department or information security officer, or to restrict involvement to annual budget approvals.

The EU legislators have set out specific duties for Directors of financial institutions and critical infrastructure providers in DORA[2] and NIS2[3] . The impact of these obligations is far-reaching. They require organisations to take adequate measures to manage cyber security risks, establish that it is the Directors' duty to approve these measures and supervise their implementation, stating that Directors can also be held liable in that regard. They also set requirements for Directors' training, knowledge and expertise.

These requirements are not only relevant to organisations directly subject to the new legislation. Given the growing cyber threat, Directors of all organisations are required to take responsibility. In short, managing cyber risks is an integral part of your role as a Director. This guide aims to assist you.

[1] The formulation and the level of detail with which such duties are expressed vary in the different Member States of the EU and UK. See for EU: Civil liability of company directors: which obligations apply - Your Europe; See for UK: Your duties, responsibilities and obligations as a director - GOV.UK

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554

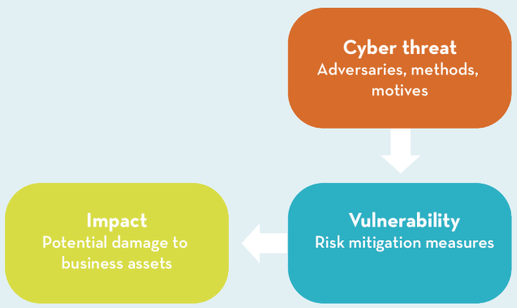
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555

3. THE GOAL IS CYBER SECURITY AND RESILIENCE OF YOUR ORGANISATION

Regulatory compliance is important for any organisation. Failure to comply with regulation can jeopardise business operations, including the ability to offer products and services in the marketplace.. However, compliance is not an end in itself; it is a means to an end – namely, ensuring the success and continuity of your organisation's business processes and protecting the data of customers or the public. Furthermore, compliance allows organisations to demonstrate their investments in security, building trust with customers and regulators. Where cyber security risks are critical to achieving your strategy, Where cyber security risks are critical to achieving your strategy, the **intrinsic motivation** to address these at the board level should be paramount.. Your organisation cannot function if its ICT does not work properly, and the same applies to your supply chain and any ICT products and services you sell.

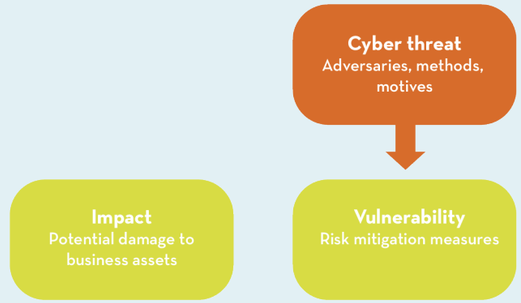
In most cases, your organisation's ICT is not a support function but a primary business process. Although this may seem obvious, it needs mentioning. For example, online banking is a primary business process and largely consists of an ICT platform. If this platform is damaged or disrupted, the primary process is no longer viable. The same applies to manufacturing companies where, for example, machines are remotely controlled and monitored. Managing cyber risks and improving cyber resilience (for instance, through backups and contingency measures) must be part of your strategic objectives and activities as a Director.

Figure 1: Cyber risk as a combination of factors



Cyber risks are business risks. Concepts such as risk mitigation, risk appetite and residual risk are not new. Risk is a combination of 'impact' and 'likelihood'. Cyber risks may arise from human error (for example, where software settings are not properly configured) or from ICT failures in the supply chain. Unlike most business risks, however, cyber risks are largely shaped by intentional threats from external actors. For this reason, we use a risk model that includes a third factor: the cyber threat.

Figure 2: Risk reduction through effective risk mitigation measures



Impact relates to your business assets and the potential consequences for your organisation's operations. This could include service disruption, theft of intellectual property or confidential information, personal data breaches, harm to individuals or reputational damage. These are the potential consequences in relation to the three factors of ICT security: ensuring the **confidentiality**, **integrity** and **availability** of information.

Cyber threats are usually external in nature. They come from adversaries – such as cyber criminals or hostile states –intending and able to cause harm to your organisation, a client or a supplier.

The last factor is **vulnerability**. This is the factor you can influence by applying risk mitigation measures – referred to in specialist jargon as 'controls' – to your ICT systems. ICT systems include servers, databases, operational technology (OT), and network and cloud infrastructure. Examples of controls include the use of multi-factor authentication (MFA) for login processes, the management of privileged access rights, and continuity measures in case of failure, such as reliable data backups and contingency plans.

When risk mitigation measures are properly aligned with the cyber threat, the impact on your business assets should remain within your risk appetite.

4. WHAT QUESTIONS SHOULD YOU BE ASKING AS A DIRECTOR?

Start by asking yourself and your co-Directors the following: How much risk are we willing to take? What is our **risk appetite**? How much disruption to our organisation is acceptable? How damaging would it be if our know-how or intellectual property were lost to a competitor through corporate espionage? How serious would it be if a cyber incident puts us on the front pages?

What are the consequences of a personal data breach? What budget are we willing to allocate for handling cyber incidents? How do we deal with cyber extortion (ransomware)? The appendix includes a non-exhaustive list of risks that may be recognisable for your organization.

Consider the strength of your organisation's security culture. Can employees raise their concerns? Are roles and responsibilities for managing cyber risks clearly assigned?

As a Director, you should also ask your Chief Information Security Officer (CISO) specific questions, these could include:

- Do we clearly document roles and responsibilities, including direct and indirect reporting, for cybersecurity functions?
- What are our ICT systems, and do we have an up-to-date inventory? How much undocumented ICT (shadow ICT) do we have?
- What are the main threats to our organisation, and why? Consider threat actors, their tactics and methods, as well as the risk of unintentional disruption.
- Do we have legacy systems that are no longer supported by the supplier? Do we have a phasing-out plan, and how are we mitigating the risk in the meantime?
- How important is the cyber security of our products and services to our customers, or even to society at large?
- What are our key controls, and what is their current status?
- What are the consequences of missing or ineffective controls? How will we improve them?
- Are our key ICT systems tested for security and resilience (red teaming)?
- Do we have an incident response and recovery plan? Do we test it?
- Do we have a plan B in case our ICT fails? What contingency options are in place?
- How large is our residual risk? Does it fall within our risk appetite?
- Are there cybersecurity functions, tooling, or other matters that are misaligned with the organization's risk appetite or risk management framework? If so, what resources are needed for remediation?
- Are we aware of our key dependencies on ICT suppliers? How do we manage the risks that come with that dependency?
- What do we do to identify, evaluate, monitor, and mitigate risk from third parties?
- Do we have contractual terms to manage third-party risk?
- Do we also have active risk-management programs for third parties in addition to protective contractual programs? What do such programs involve, and how effective are they ?
- Are the resources we allocate to cyber security sufficient and effective?
- Which systems are so critical that we strictly limit access, or even allow access only at physical locations?
- As a company and as Directors, are we adequately insured against cyber risks?
- Under what circumstances would we consider complying with extortion demands?
- How well trained is our personnel in cyber security?
- How does our cyber security compare to others in our sector?

If your organisation develops and sells ICT products and service, you may also want to ask the following questions:

- Have we implemented security-by-design and security-by-default principles in the development and delivery of our digital products and services? How do we ensure that cyber security is integrated throughout the entire product lifecycle, from design to deployment and maintenance?
- What tools and indicators exist to measure adherence to secure software development requirements? And what do they show?
- What cyber security risks do our products and services pose to our customers and end-users? Do we have processes in place to identify, assess and mitigate vulnerabilities in our products before they reach the market, and how do we respond to security issues discovered after deployment?
- For the ICT product and services offered to customers, have they been developed according to secure software development principles?
- What measures are used to ensure the security of ICT products or services that that are acquired for use in the organization or for integration with our products and services?
- What measures exist to manage cybersecurity risk from any merger or acquisition of corporate entities? Or from divesting or selling part of the organization?
- What measures exist to ensure use of appropriate cryptography and other technical controls to ensure security?

You should receive regular (quarterly) reports with the answers to these questions, along with context on major cyber incidents inside and outside the organisation, emerging threats and regulatory developments. At the same time, the CISO should highlight any developments that significantly alter the risk landscape – for better or worse – and propose relevant actions and resources.

5. PRIORITISE TO EFFECTIVELY MITIGATE YOUR CYBER RISKS

As a Director, you are expected to approve your organisation's cyber risk strategy and oversee its implementation. Zero risk is impossible, and resources are limited. Fortunately, it is possible to prioritise aspects of cyber risk and maintain strategic oversight without needing to know every detail.

Frameworks such as ISO/IEC 27001[4] , NIST CSF[5] , and COBIT[6] , and Cyber Fundamentals[7] are useful tools for managing cyber security risks. They comprehensively outline the organisational measures and processes your organisation can implement to ensure cyber security and resilience. It does not matter which framework your organisation chooses, provided that only one framework is used internally, in alignment between the CIO, CISO, and risk and audit functions.

A word of caution: frameworks primarily focus on ensuring processes are in place (for example, whether there exists a contingency process) but do not themselves guarantee that the risks are sufficiently mitigated. In other words, frameworks do not assess the effectiveness of controls. They furthermore typically include processes for accepting deviations from prescribed controls. While this meets the process requirement; it does not equate to actual risk mitigation. Certification under a framework provides only a limited degree of assurance.

Frameworks include hundreds of controls to cover all aspects of security risk management. Not all controls are equally important. Experience shows that a very limited subset of key controls covers the most significant security risks. Measuring the proper functioning and effectiveness of these key controls enables your organisation to set up a strategic dashboard with Key Control Indicators (KCIs), allowing you to exercise well-informed oversight.

[4] https://www.iso.org/isoiec-27001-information-security.html

[5] https://www.nist.gov/cyberframework

[6] https://www.isaca.org/resources/cobit

[7] https://www.researchgate.net/publication/374061802_Ten_Key_Insights_for_Informed_Cyber_Oversight

Below is a list of KCIs drawn up by a working group of CISOs from major multinationals. It can serve as a starting point for determining KCIs in your own organization.[8] The first KCI on the list is by far the most important: establishing an 'Inventory of ICT assets'. After all, an organisation cannot protect what it doesn't know exists. Most of the other KCIs relate directly to the ICT systems in the inventory. For example, the KCIs that cover making backups or installing security updates apply only to ICT systems that are accounted for in the inventory. The effectiveness of these KCIs diminishes if that inventory is incomplete.

Table 1: Examples of Key Control Indicators

	Description	Measurement
KCI 1	Inventory of ICT assets	% of ICT assets included in inventory, in accordance with policy
KCI 2	Privileged accounts	% of privileged accounts managed within policy; number of privileged accounts
KCI 3	Addressing vulnerabilities	% of high-risk security updates applied within N hours
KCI 4	Reliable backups of data and applications	Maximum time to recover critical resources (% of critical resources recoverable in N hours)
KCI 5	Secured workstations	% of workstations configured in line with policy
KCI 6	Log collection	% of critical systems onboarded for log collection
KCI 7	Network security	% of compliant network security settings
KCI 8	Third-party compliance	% of compliant key connections with third parties
KCI 9	Identity management	% of systems and users covered by multi-factor authentication (MFA) – % of privileged accounts using phishing-resistant MFA
KCI 10	Major incidents	% of major cyber incidents with no business impact
KCI 11	Risk acceptance	Number of risk accepted policy deviations
KCI 12	Security of internet-exposed ICT systems	% of internet-exposed assets that are adequately protected and monitored
KCI 13	Crown jewels monitoring	% of crown jewels covered by security monitoring
KCI 14	Origin of cyber incidents	% of security incidents linked to deficiencies in at least one key control
KCI 15	Resilience testing	Results of resilience testing (red teaming)
KCI 16	Cryptography	% of resources with post-quantum security % of resources with compliant key management

[8] https://www.researchgate.net/publication/374061802_Ten_Key_Insights_for_Informed_Cyber_Oversight

KCIs reflect your organisation's priorities. The way you select and report on them will shape its direction. These choices are thus crucial and require thorough discussion and decisions at board level.

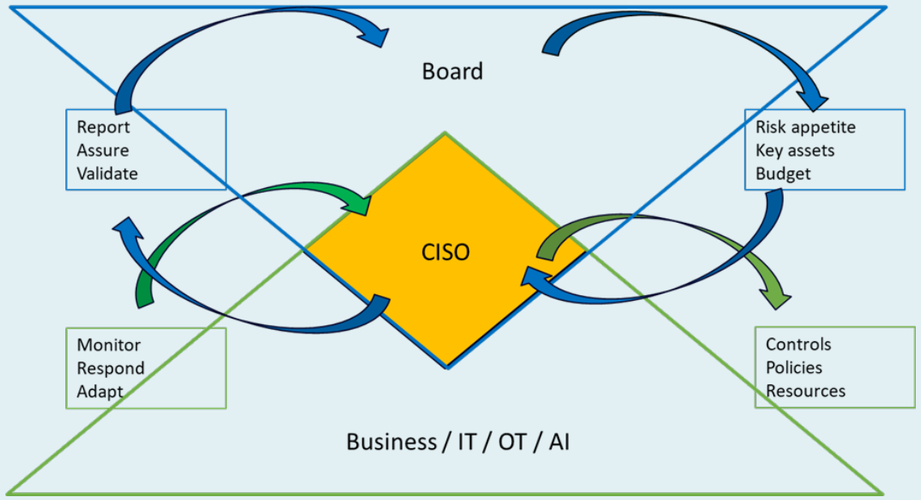
In industrial environments, do not overlook the situation around operational technology and process automation (OT). OT often involves outdated software that is no longer maintained, and security updates for control software are difficult to install during production. In such cases, alternative protective measures (such as isolation) must be taken. These measures require separate reporting.

Also be cautious when using averages as they can conceal serious risks. For example, if a KCI calculates the percentage of resolved cyber incidents based on all cyber incident types (low, medium and high risk), it might report that 95% were resolved without business impact. However, a single high-risk incident with serious consequences could go unnoticed.

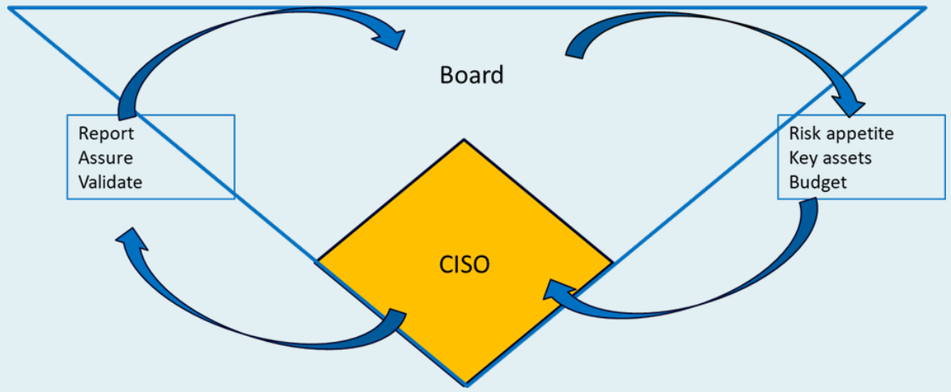
Finally, your organisation needs to be prepared for extreme scenarios (no ICT, loss of a supplier, etc.). It is recommended that you test your organisation's resilience and robustness regularly by holding table-top exercises and conducting external cyber resilience tests such as TLPT (Threat Level Penetration Testing) and TIBER (Threat Intelligence- based Ethical Red Teaming).

6. CONTINUOUS OVERSIGHT – GOVERNANCE

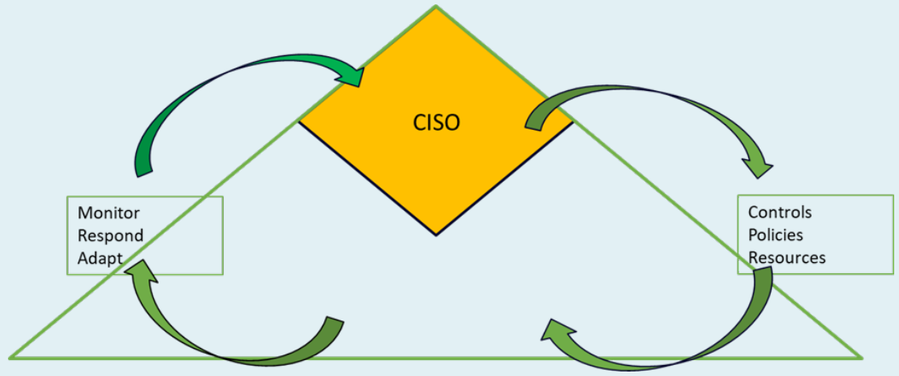
Established practices exist for reporting and assigning responsibilities around traditional business risks. However, for managing cyber security risks, such practices are often still lacking. For example, it is difficult to measure the effectiveness of cyber security programmes and to obtain reasonable assurance that residual risk remains within the organisation's risk appetite. As a result, cyber risk reports to Directors vary widely. They often focus on progress in implementing processes, measuring effort rather than effectiveness.



The figure above illustrates an ideal situation for cyber governance – the organisation of decision-making, monitoring, reporting, and oversight of cyber security risk management. The starting point is the appointment of a CISO (or similar officer). The CISO holds a central role in cyber governance and is responsible for developing and implementing measures to control cyber security risks. The CISO works closely with the internal operational services (business, ICT and OT operations, innovation) as well as risk management and audit functions.



In the upper part of the figure, you see that the CISO coordinates cyber risk mitigation measures with the board, especially regarding risk appetite, business priorities, and budget. The board receives regular updates from the CISO on the status of KCIs, the threat landscape, significant incidents and regulatory developments.



In the lower part of the figure, you see that the CISO implements the board's strategy through cyber controls, working together with the internal operational services. The CISO monitors the effectiveness of cyber controls, responds to deviations and incidents, and makes any necessary adjustments. Many activities take place in the lower pyramid, i.e. 'under the hood' for the board.

As a Director, you must ensure your CISO has the skills, resources and autonomy to develop and implement the organisation's cyber security policy and to support you in exercising duly informed oversight. In doing so, you should ensure that your internal processes, responsibilities and reporting lines are clearly documented in your governance framework.

It is important that the CISO is supported by a clear mandate, the authority to act decisively and active cooperation from all business units.

Encourage coordination between the CISO's reporting and the reports from risk management and audit. Also request regular reporting, not only in the event of an incident. Ensure that reporting does not focus solely on progress in process implementation, measuring effort rather than effectiveness. Ideally, the CISO should report in person to the management board each quarter, and additionally whenever necessary. Give the CISO sufficient 'airtime'.

7. LEGAL ASPECTS OF YOUR MANAGEMENT RESPONSIBILITY

Directors are subject to a range of statutory and common law duties under national law as part of their role in managing the business of a company. These include ensuring that the organisation has effective risk management and control systems in place.

At EU level, the responsibilities of Directors of financial institutions and critical infrastructure have been tightened under new directives and regulations – including NIS2[9], CER[10], and DORA[11]. These instruments require in-scope entities to take measures to manage cyber security risks and specify that it is the responsibility of Directors to approve those measures and supervise their implementation, and in certain circumstances stating that Directors can also be held liable in that regard. They also set requirements for Directors' training, knowledge and expertise in certain instances.

The impact of the new statutory provisions is far-reaching. In most organisations, the new statutory obligations require a review of existing risk management and control systems – including those across the supply chain – and a clearer specification of cyber governance: roles, responsibilities, authorities and reporting lines.

If your organisation sells products with a digital component (hardware, software, IoT devices or apps used to operate such products), these will also have to meet strict cyber security requirements under the CRA.[12]

[9] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555

[10] https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en

[11] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32022R2554

Directors' responsibilities under NIS2 and DORA

Both NIS2 and DORA require in-scope entities to have proper cyber risk management in place. They also specify the minimum risk control measures that must be implemented. Directors have a duty to:

- Approve the cyber risk-management measures;
- Oversee the implementation of these measures;
- Acquire sufficient knowledge and skills through training to be able to identify cyber risks, assess the effectiveness and impact of cyber risk management and evaluate cyber risk reporting.

Directors' liability under NIS2 and DORA

Both NIS2 and DORA contain provisions under which boards and individuals in the organisation may be held personally liable. The publicity around NIS2 and DORA has focused heavily on the issue of personal liability. In practice, however, the real expansion of liability under the new legislation stems mainly from the fact that Directors' duties and responsibilities are now specifically described.

If these duties are not properly discharged, Directors will find it difficult to demonstrate that they have fulfilled their statutory obligation to ensure proper governance. As Directors' responsibilities are now more precisely set out, this also applies to the oversight duties of supervisory boards (in a 2-tier board system). Both NIS2 and DORA provide for additional provisions on potential personal liability.

NIS2– Liabilities of directors

NIS2 outlines two types of personal liability for individuals in the organisation. Note that under NIS2, the type or scope of liability (civil, administrative, or criminal) is not specified, and such specification must therefore be set out in the national NIS2 implementation law.

Collective liability. Management bodies can be held liable for the entity's failure to implement measures to manage cyber security risks. Liability is attributed to the board as a whole, which implies collective responsibility. This means that individual members can be held jointly and severally liable for responsibilities within the board as a whole, even if certain duties have been delegated to specific members thereof.

Individual liability. Any natural person who is responsible for or acts as the legal representative of a regulated entity can be held liable for failing to meet their obligations to ensure NIS2 compliance.[33]
'Legal representation' is interpreted based on whether the individual has:
- the authority to represent the entity;
- the authority to make decisions on behalf of the entity;
- the authority to exercise control over the entity.

Individual liability is therefore not limited to directors. The provision also applies to individuals below the highest management level (i.e. employees, such as a CISO), provided that the individual concerned has been assigned the relevant responsibilities and powers. This could, for example, apply to a CISO who is authorised to make decisions relevant to NIS2 compliance, such as taking the network offline in the event of a security incident or reporting such an incident to the competent authority.

[12] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847

The above does not apply in full to the liability of government bodies, civil servants, and elected or appointed public officials, whose liability may differ in certain respects. NIS2 explicitly leaves room for such distinctions.

Although not a liability provision, NIS2 stipulates that in very exceptional circumstances, the general director or another person with managerial responsibilities at the level of the legal representative may be temporarily suspended from performing managerial functions. Such suspension must be imposed by a court at the request of a supervisory authority. The possibility of temporary suspension does not apply to directors of government bodies

DORA – Liabilities of directors

Under DORA, national competent authorities may impose certain administrative penalties and corrective measures on the financial entity. DORA also grants national competent authorities the power to impose administrative penalties or corrective measures on members of the financial entity's management body and other persons who are responsible for the breach under national law.[44]

8. RESPONSIBILITY FOR CYBER EXTENDS BEYOND YOUR OWN ORGANISATION

Your organisation is part of a supply chain. The cyber security of your ICT depends on that of your suppliers. In turn, your customers depend on the cyber security of your products and services. Your cyber risk management is therefore not limited to your own organisation.

Extend your oversight to your supply chain, prioritising suppliers or service providers that are critical to your organisation and mitigate their cyber risks. They may also be targets for cybercriminals, which could cause your organisation to become an unintended victim. It is advisable to assess suppliers based on technical dependency (replaceability) and undesirable geopolitical dependencies. However, avoid excessive control requirements if suppliers or service providers are not critical to your organisation and processes.

The European legislation has included the security of cyber risks in your direct suppliers and service providers as part of the duty of care under NIS2 and DORA. The underlying strategic rationale of this legislation is that 'large' organisations support 'small' ones in managing their cyber risks.

Ensure that the design, configuration and use of your own digital products are secure (security-by-design and security-by-default), preferably supported by certification.

If your organisation sells products with a digital component (such as hardware, software, IoT products or apps used to operate products), extend your oversight to cover these products and reduce the cyber risk for your customers by ensuring that the design, configuration and use are secure (security-by-design and security-by-default). When exercising oversight, also consider any potential social impact that an incident in your organisation might cause.

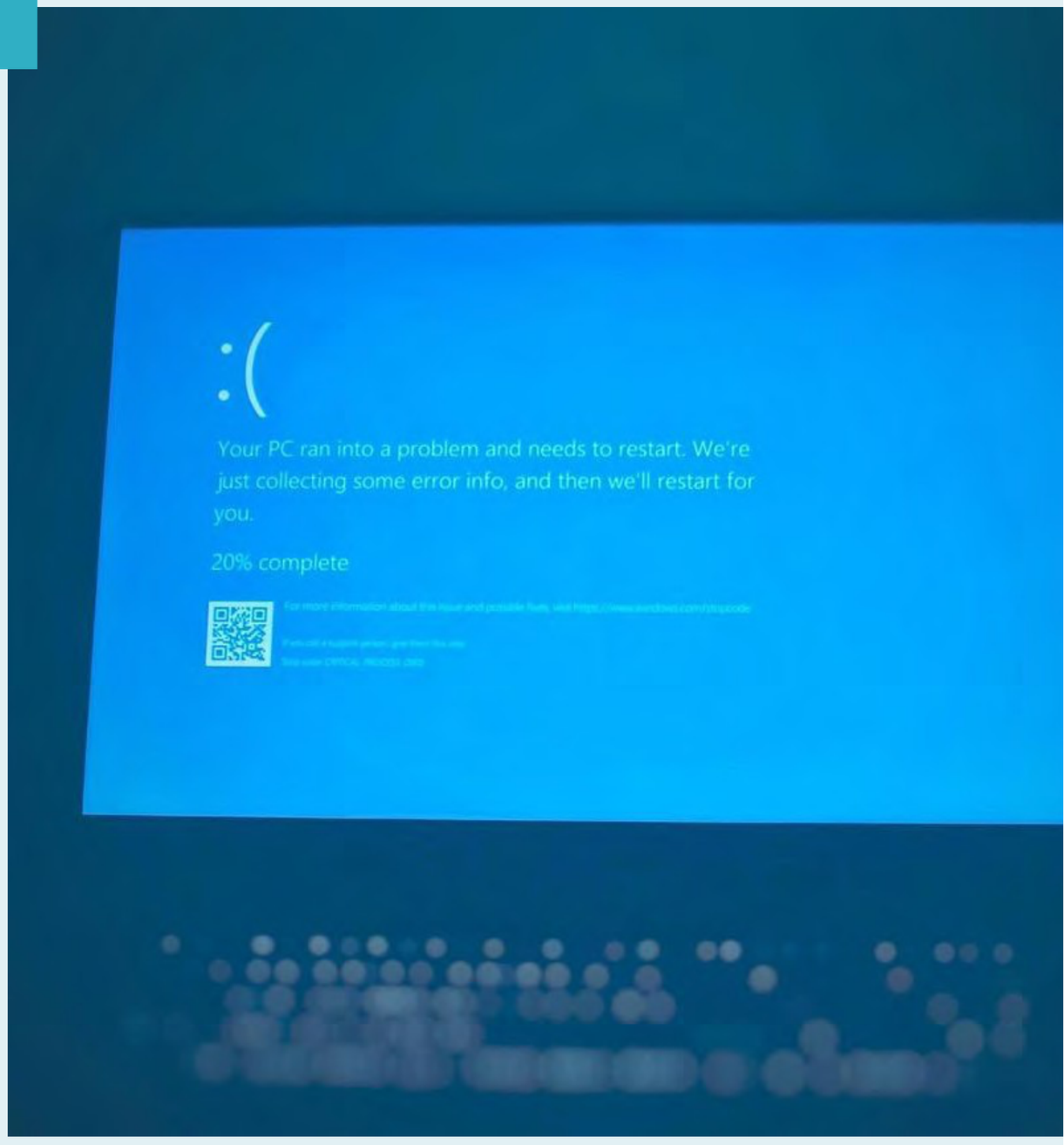
The European legislation has included the security of cyber risk in your own products with a digital component as part of the duty of care under the CRA. This will help strengthen the digital resilience of both businesses and consumers.

9. EXTERNAL REPORTING OBLIGATIONS

Your organisation also has external cybersecurity reporting obligations, including to:

- Supervisory authorities responsible for the legislation applicable to your organisation;
- Auditors auditing your financial statements, shareholders and the financial market;
- Customers;
- Insurers.

The building blocks of these external reporting obligations are similar to those of the internal framework applied by your organisation. To bridge the gap between your internal framework and those used by your external stakeholders, 'mappings' are available, such as the CRI Profile.[13] When applying a mapping, you must ensure that your organisation provides sufficient context in the external reporting and coherently reports the elements that the external party expects.



[13] https://cyberriskinstitute.org/

10. DIRECTOR TRAINING WITH IMPACT

Practice shows that training of Directors can have a significant impact on an organisation. The training must then go beyond delivering theoretical content. Directors and members of board committees do not need to become technical experts. The purpose of the training is not to turn you into a 'CISO-light', but to enable you to engage in an informed strategic discussion and to exercise effective oversight.

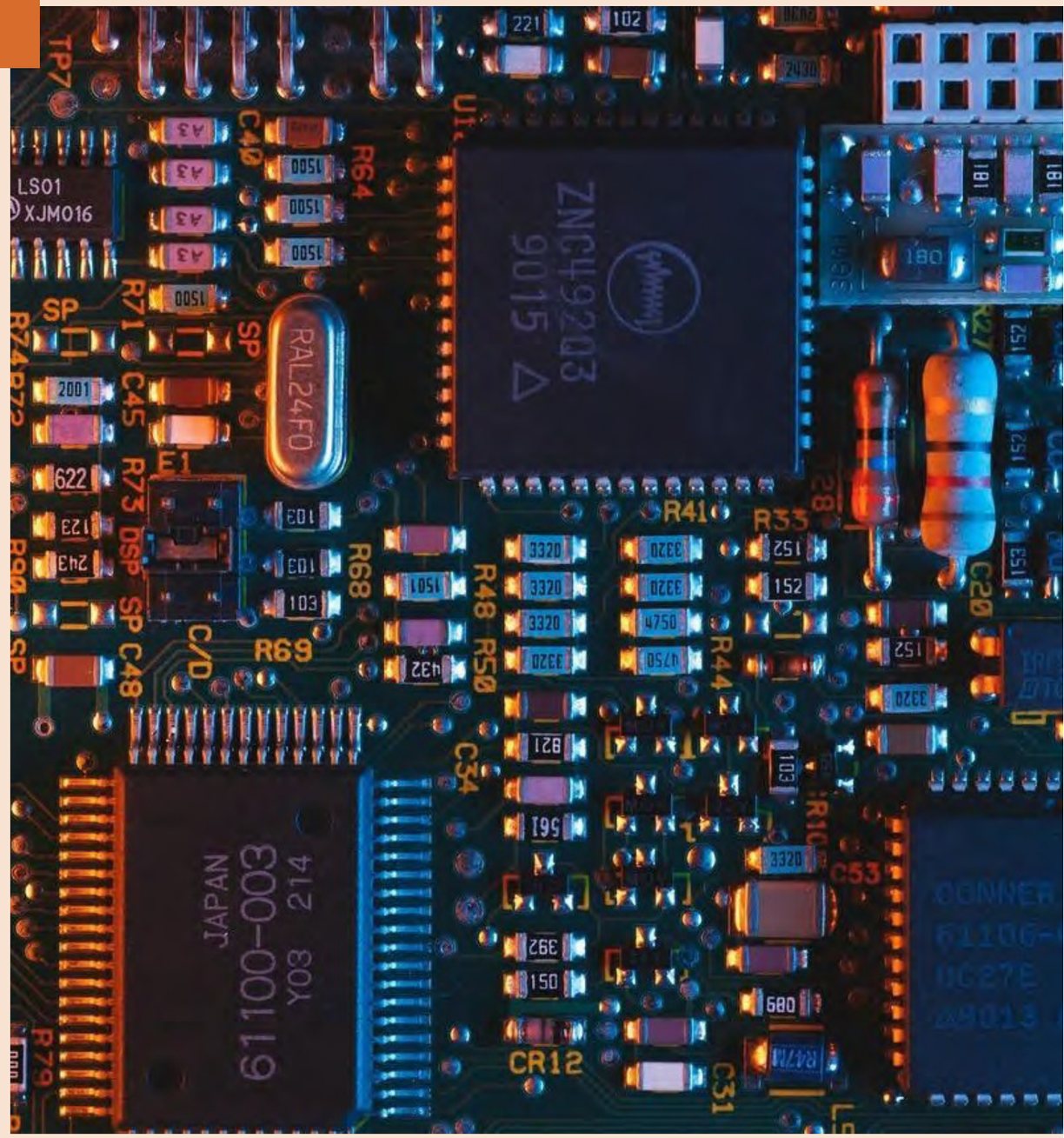
Key topics to be addressed include:

- Relevant elements of cyber regulation, both within the EU and beyond;
- The role and responsibility of Directors;
- The value and limitations of frameworks;
- How best to set up an international cyber risk management programme that allows efforts to be leveraged elsewhere;
- Good cyber governance (role of CISO, who reports what to whom and how often?);
- What is our risk appetite?
- What are the key controls and how do we measure them?
- Gap analysis between current cyber risk management and the desired situation;
- Establishing a continuous improvement process (*Plan-Do-Check-Act*).

Once these strategic elements have been properly addressed, the board will be in position to act and implement the necessary changes to governance and reporting to enable you to have oversight.

Some practical tips for organising cyber training for Directors:

- Deliver the training in person, at the office, as a scheduled agenda item during a regular board meeting;
- In many cases, current cyber governance and reporting to Directors will not yet meet the ideal situation. Use the preparation phase to discuss and resolve any internal friction or disagreements between departments;
- Tailor the content of the training to your organisation, your infrastructure, your sector and your existing governance and reporting structures;
- Allow sufficient time (2–3 hours) to hold a meaningful discussion on risk appetite, key controls, reporting processes and governance;
- Use the training as a continuous improvement tool for your organisation.

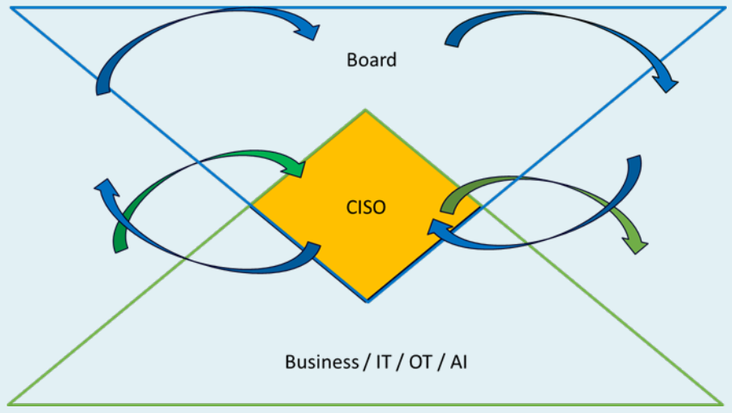


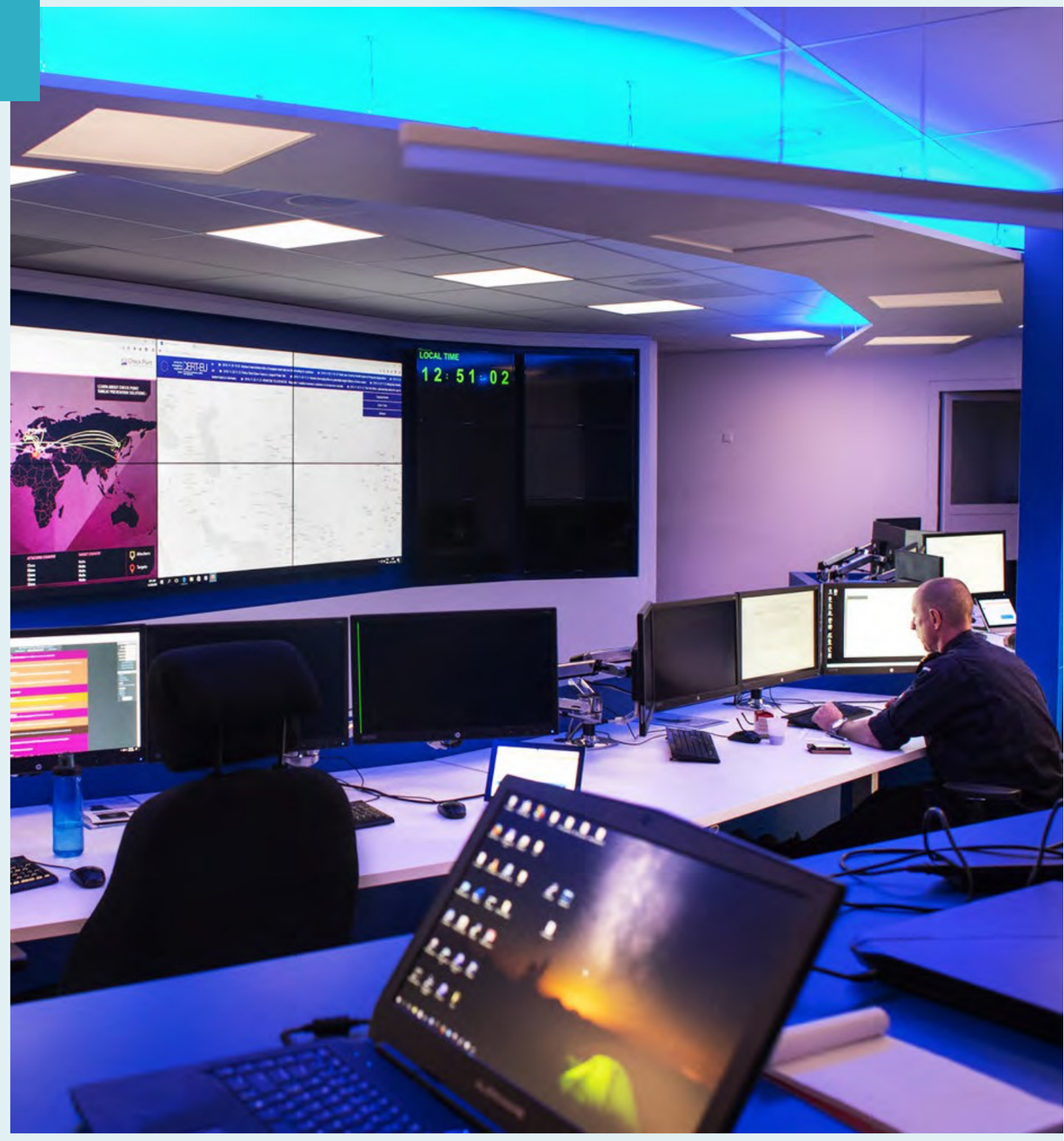
11. KEEP YOUR FINGER ON THE PULSE AND IMPROVE WHERE NECESSARY

Don't assume that cyber risks are static. Your organisation, your infrastructure, your ICT products and services, and the threat landscape are constantly evolving. Technological developments such as AI, quantum computing and the Internet of Things (IoT) introduce new risks and require prompt adjustment of your security strategy.

It is therefore important to ensure that your processes and security measures are periodically reviewed and adapted to all developments to ensure that the risks remain within your risk appetite. Cyber risk management should be part of a continuous improvement process. The aim is to ensure business continuity for your business and that of the entire supply chain.

Figure 3: Continuous improvement





12. SET THE RIGHT TONE AT THE TOP – LEAD BY EXAMPLE

Be aware that you are a potential target of cybercriminals. You have access to valuable business assets. Cyber security should therefore be second nature to you, such as strictly separating work and private use of laptops and mobile phones, applying MFA and using an application to manage your passwords. While this is necessary to reduce the risk you may pose to your organisation, your attitude will also positively influence how your employees behave. Good cyber security starts at the top.

13. ACKNOWLEDGEMENTS

This guide is a product of the Dutch Cyber Security Council (CSR). It is based on the Guide to cybersecurity for Directors and business owners[14] and on white papers published by the community[15], authored by Freddy Dezeure, Lokke Moerel et all.

Authors:
- Lokke Moerel (Professor of Global ICT Law, Tilburg University and CSR member)
- Freddy Dezeure (Microsoft Deputy CISO for Europe)

With contributions from the following individuals and organisations:

- Sabine Gielens (on behalf of VNO-NCW and MKB-Nederland)
- Michiel Steltman (on behalf of ECP)
- Liesbeth Holterman (on behalf of Cyber Veilig Nederland)
- Marlou Snelders (on behalf of FME)
- Ronald Verbeek (on behalf of the CIO Platform)
- Eelco Stofbergen (on behalf of NLdigital)
- Pieter van den Berg (on behalf of the National Coordinator for Counterterrorism and Security)
- Tim Puts (on behalf of the Ministry of Defence)

Front page picture: credit https://gmilo.com/en

[14] Guide to cyber security for directors and business owners | Cyber Security Council
[15] Ten Key Insights for Informed Oversight

APPENDICES

APPENDIX 1:
LIST OF ABBREVIATIONS AND TERMINOLOGY

CISO	Chief Information Security Officer or equivalent officer
CIO	Chief Information Officer
ICT	Information and Communication Technology. In this guide, ICT is used in the broadest sense to refer to all forms of information technology.
OT	Operational Technology
IoT	Internet of Things
NIS2	Network and Information Security Directive (EU)
CER	Critical Entities Resilience Directive (EU)
DORA	Digital Operational Resilience Act (EU)
CRA	Cyber Resilience Act (EU)
Control	Risk mitigation measure
KCI	Key Control Indicator
MFA	Multi-factor authentication, requires multiple verification factors to log in

APPENDIX 2:
NON-EXHAUSTIVE LIST OF CYBER RISKS

- √ Disruption of continuity in business processes, such as goods production, administration, access to buildings, logistics, external communication, or website availability.
- √ Unauthorised access to personal data (privacy) of employees, customers, the general public, patients, etc..
- √ Extortion following a ransomware attack or threats to publicly release confidential data.
- √ Direct financial loss due to deception of employees with access to funds, misuse of financial processes or forgery in the invoicing chain.
- √ Reputational damage and loss of trust from customers or the public due to a cyber attack becoming public knowledge.
- √ Reputational damage due to unauthorised takeover of official communication channels.
- √ Reputational damage and product liability issues caused by compromised products or services.
- √ Strategic harm caused by the loss of confidential data to geopolitical adversaries, business secrets to competitors or confidential legal or financial information
- √ Accidents involving injury or material damage due to compromised products or services in sectors such as healthcare or transport.
- √ Financial loss due to the cost of incident response and repair of infrastructure.
- √ Financial consequences from the legal impact of an incident, such as disputes with customers, regulators or insurers.

APPENDIX 3:
CHECKLIST FOR DIRECTORS

- √ Organise an all-hands training session for Directors to enable informed decision-making and oversight of implementing cyber risk management. Ask your CISO to map the threat landscape for your organisation.
- √ Determine your risk appetite
- √ Ask for a cyber risk strategy and a set of measures to manage cyber security risks to be drawn up, submitted and then formally approved.
- √ Ask for the top KCIs to be proposed, with targets set, measured and reported on a quarterly basis. Organise and test the incident response and recovery plan.
- √ Adapt your cyber governance to include clear mandates and reporting lines for setting, monitoring and reporting on the cyber risk strategy. Ensure the CISO has sufficient resources, autonomy and support.
- √ Ask for the relevant regulatory requirements for your organisation to be identified and a plan drawn up to ensure compliance.
- √ Determine which individuals or roles could be held liable under applicable regulation and arrange appropriate liability insurance.
- √ Check whether you have asked your CISO all relevant questions.