CSR Cyber Security Raad

GUIDE TO CYBER SECURITY FOR DIRECTORS AND BUSINESS OWNERS

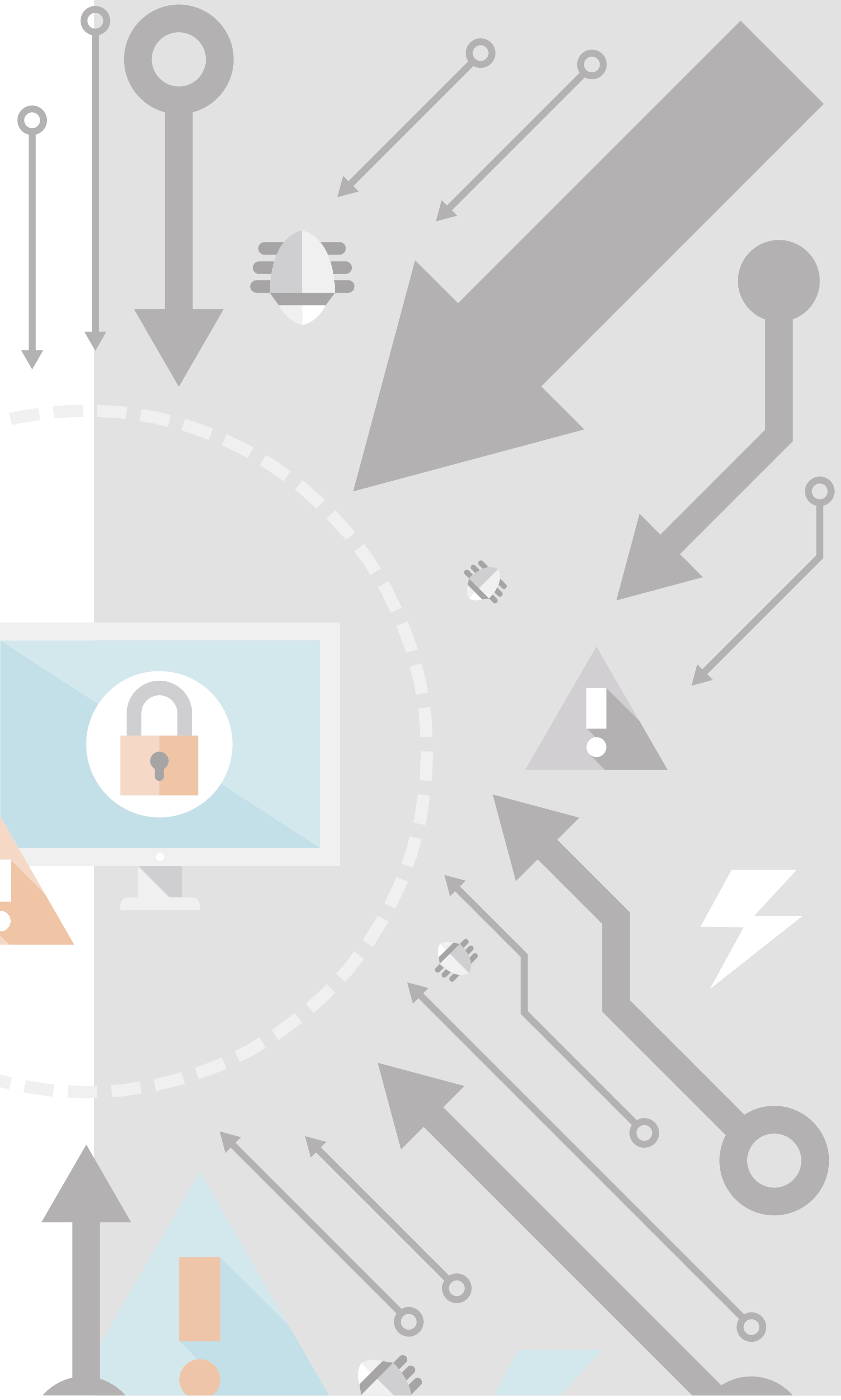


TABLE OF CONTENTS

1. TARGET GROUP OF THIS GUIDE

This guide is intended for directors, business owners and members of supervisory boards across **all** organisations, regardless of size or whether they are public or private. It is also relevant for directors and owners of businesses that are not subject to the cyber security legislation, such as NIS2 or DORA. Throughout this guide, we use the term ‘directors’ to refer to directors, business owners and members of supervisory boards. As this guide is written from a Dutch perspective, it refers to Dutch legislation. However, the insights provided are broadly applicable.

***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).*

2. WHY IS THIS GUIDE IMPORTANT FOR YOU?

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 have a general legal duty to perform their duties properly.[1] This includes ensuring that their organisation has effective risk management and control systems in place. 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 does not suffice to delegate responsibility to the IT department or information security officer, or to restrict involvement to annual budget approvals.

The European legislators have set out specific duties for directors of financial institutions and critical infrastructure providers in DORA[2] en NIS2[3] [4]. 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, while recognising that smaller businesses will naturally need to adapt the guidance to fit the realities of a smaller organisation. For example, we discuss the role of a Chief Information Security Officer (CISO) below[5]. In smaller organisations, appointing a CISO will likely not be feasible, and their tasks can be assigned to other employees.

[1] Article 9(1), Book 2 of the Dutch Civil Code.

[2] Digital Operational Resilience Act (DORA), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554

[3] Network and Information Security Directive (NIS2), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555

[4] For a current overview of all European legislation affecting IT risk management and compliance, including cyber security and cyber resilience, see https://www.norea.nl/nieuws/otc-en-norea-publiceren-nieuwe-editie-van-het-wetgevingsoverzicht

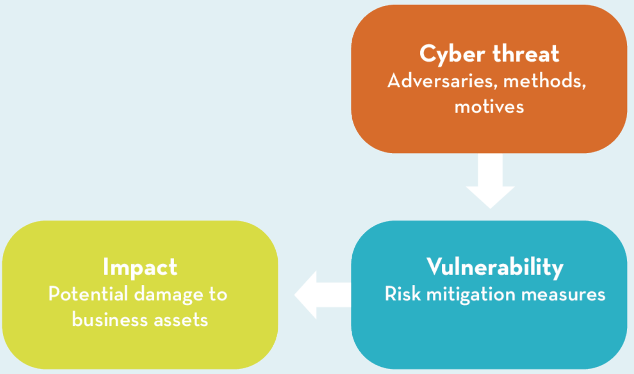
[5] Chief Information Security Officer - Wikipedia https://nl.wikipedia.org/wiki/Chief_information_security_officer

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

Regulatory compliance is important for any organisation. Failure to comply with legislation means your organisation's licence to operate is at risk. 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. Where cyber security risks are critical to achieving your strategy, the **intrinsic motivation** to address these at board level should be paramount. Your organisation cannot function if its ICT does not work properly, and the same applies to your supply chain.

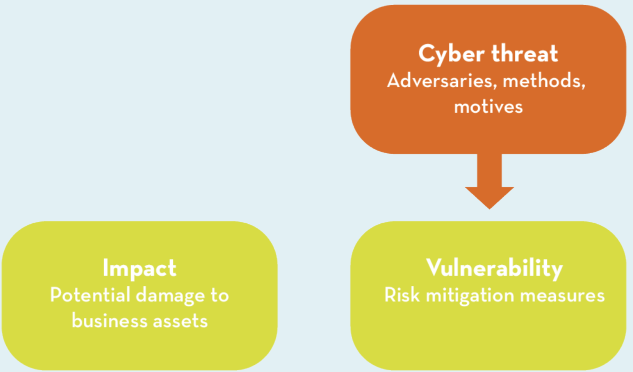
In most cases, your organisation's ICT is not a support function but a primary business process. Although this may seem obvious, it needs mentioning. For example, online banking is a primary business process and largely consists of an ICT platform. If this platform is damaged or disrupted, the primary 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 proper data backups and contingency facilities) must be part of your strategic objectives and activities as a director.

Figure 1: Cyber risk as a combination of factors


Cyber threat
Adversaries, methods, motives
Impact
Potential damage to business assets
Vulnerability
Risk mitigation measures

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 model that includes a third factor: the cyber threat.

Figure 2: Risk reduction through effective risk mitigation measures


Cyber threat
Adversaries, methods, motives
Impact
Potential damage to business assets
Vulnerability
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 or alterations, 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 or a supplier.[6]

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.

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

[6] https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland

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**?[7] 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?[8] How serious would it be if a cyber incident put 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 organisation.

Also 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. A useful guide for this is the NCSC's list of questions for directors to ask their CISO.[9]

Important questions include:

- 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 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 we aware of our key dependencies on ICT suppliers? How do we manage the risks that come with that dependency?
- 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?

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.

[7] https://www.digitaltrustcenter.nl/stappenplan-risicoanalyse

[8] https://www.ncsc.nl/documenten/publicaties/2020/juli/21/factsheet-risicobeheersing

[9] https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/besturen/vragen-voor-bestuurder-aan-ciso

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[10], NIST CSF[11], COBIT[12], and the NOREA DORA Framework[13] 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 alignement between the CIO, CISO, and risk and audit functions. Guidance on selecting a framework is available on the NCSC website.[14]

For smaller businesses where applying a full framework is not feasible, NCSC guidance lists five basic principles of digital resilience, which provide practical tools for developing a cyber security strategy.[15] 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.[16] 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.

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

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

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

[13] https://www.norea.nl/uploads/bfile/4693bb51-d6c0-4c3d-8e3e-577f74af9d73

[14] Find the risk management framework that suits your organisation | What can you do yourself? | National Cyber Security Centre

[15] Five basic principles of digital resilience | What can you do yourself? | National Cyber Security Centre; on Digital Trust Centre's website, you will also find the Cyber Security Check for self employed professionals and SMEs, as well as the five basic principles for secure digital enterprise | Digital Trust Centre (Ministry of Economic Affairs)

[16] https://www.digitaltrustcenter.nl/maak-je-mkb-bedrijf-cyberweerbaar

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 organisation.[17] The first KCI on the list is by far the most important: establishing an 'Inventory of ICT systems'. 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 critical 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	% kroonjuwelen gedekt door beveiligingsmonitoring
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

[17] 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.

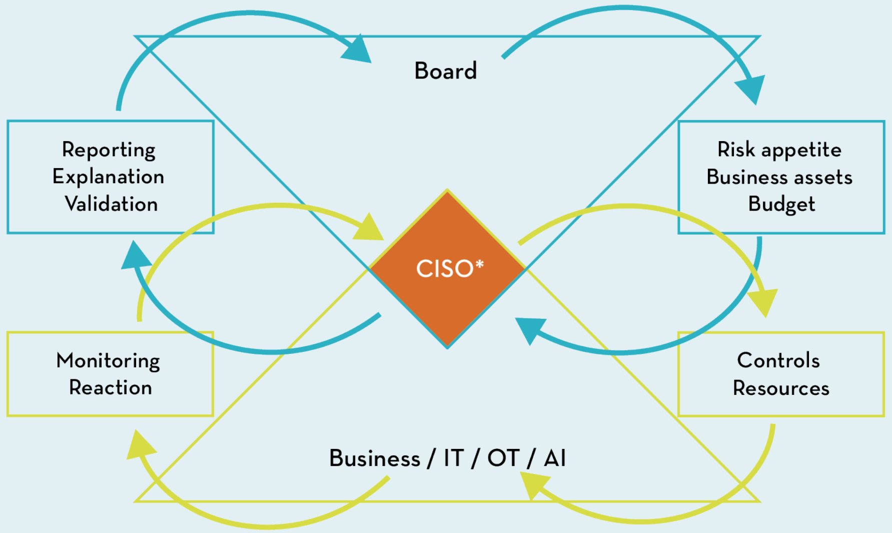
Also be cautious when using averages as they can conceal serious risks. For example, if a KCI calculates the percentage of resolved cyber incidents based on **all** cyber incident types (low, medium and high risk), it might report that 95% were resolved **without** business impact. However, a single 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, TIBER, and ART.[18]

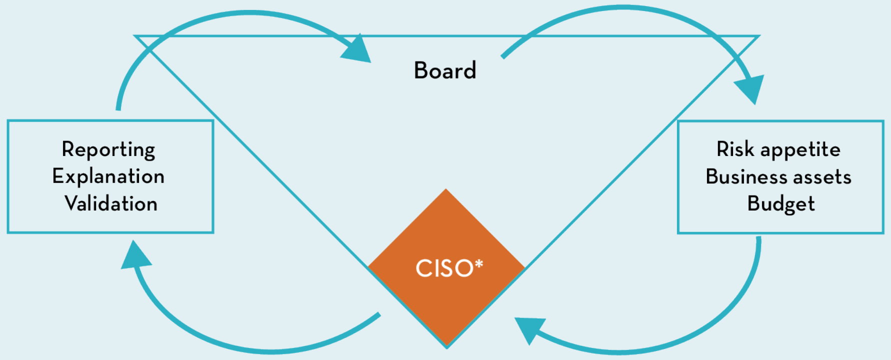
[18] https://www.dnb.nl/voor-de-sector/betalingsverkeer/begeleiding-cyberweerbaarheidstesten-door-dnb/

6. CONTINUOUS OVERSIGHT – GOVERNANCE

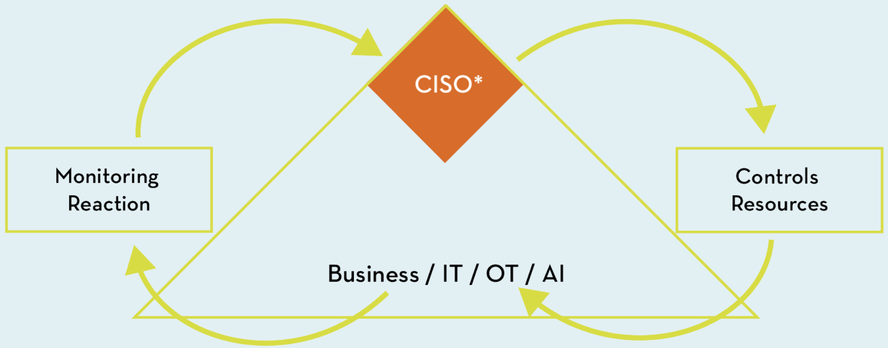
Established practices exist for reporting and assigning responsibilities around traditional business risks. However, for managing cyber security risks, such practices are often still lacking. For example, it is difficult to measure the effectiveness of cyber security programmes and to obtain reasonable 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 that organisations appoint 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. Also 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 have a general statutory duty to perform their duties properly.[19] This includes ensuring that the organisation has effective risk management and control systems in place.

At EU level, the responsibilities of directors of financial institu-tions and critical infrastructure have been tightened under new directives and regulations – including NIS2,[20] CER,[21] en DORA.[22] These instruments require regulated entities to take measures to manage cyber security risks and specify that it is the respon-sibility of directors to approve those 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.

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 speci-fication of cyber governance: roles, responsibilities, authori-ties 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 forthcoming CRA.[23]

→ **Click to read more about: NIS2, CER, DORA and CRA**

[19] Article 9(1), Book 2 of the Dutch Civil Code

[20] Network and Information Security Directive (NIS2), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555

[21] Critical Entities Resilience Directive (CER), 2022/2557 - EN - CER - EUR-Lex

[22] Digital Operational Resilience Act (DORA), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554

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

Directors' responsibilities under NIS2 and DORA

Both NIS2 and DORA require regulated 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 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.

First insight for directors is that ultimate responsibility for managing and overseeing cyber risks cannot be delegated to specialist executives or to a specialised audit or other committee.

Responsibility lies with the board as a whole **(collective responsibility)**. Individual directors may be held jointly and severally liable for the board's collective responsibilities, even if certain tasks have been delegated to specific members of the management body.

The second point is that the Dutch General Administrative Law Act (*Algemene wet bestuursrecht*) is relevant to enforcing the implementation and other requirements under NIS2 and DORA. This means that if a legal entity commits a breach, the person who ordered **the act (*opdracht heeft gegeven tot het feit*)** or was the **de facto manager (*feitelijk leidinggever*)** may also be subject to corrective measures, such as an administrative fine, or order subject to administrative coercion or a penalty sum.

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 legislator 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 – as well as the Dutch Cyber Security Strategy[24] – 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 legislator 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.

[24] See the underlying strategic choices on p. 18–19, Nederlandse+Cybersecuritystrategie+2022-2028 (1).pdf

9. EXTERNAL REPORTING OBLIGATIONS

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

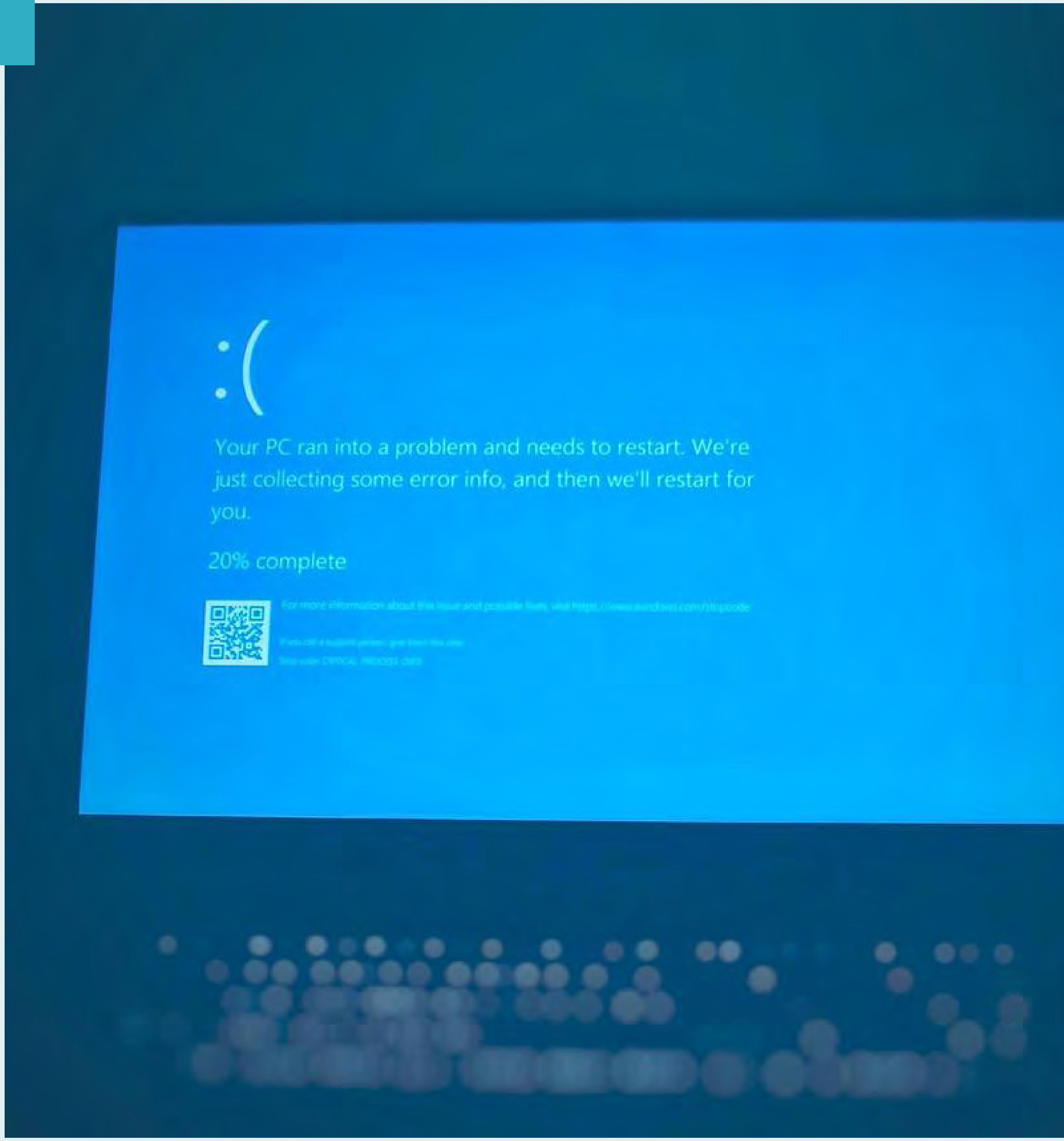
- Supervisory authorities responsible for the legislation applicable to your organisation;
- Auditors auditing your financial statements, shareholders and the financial market;
- Customers;
- Insurers.

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.[25] There are also initiatives that enable integrated reporting on ICT controls, such as the International Digital Reporting Standard (IDRS).[26]

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.

[25] https://cyberriskinstitute.org/

[26] International Digital Reporting Standards, Governance of IT, version 2.1, May 2025



:(

Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

20% complete

For more information about this issue and possible fixes, visit https://www.windows.com/stopcode

If you call a support person, give them this info:

Stop code: CRITICAL PROCESS DIED

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 supervisory board members 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:

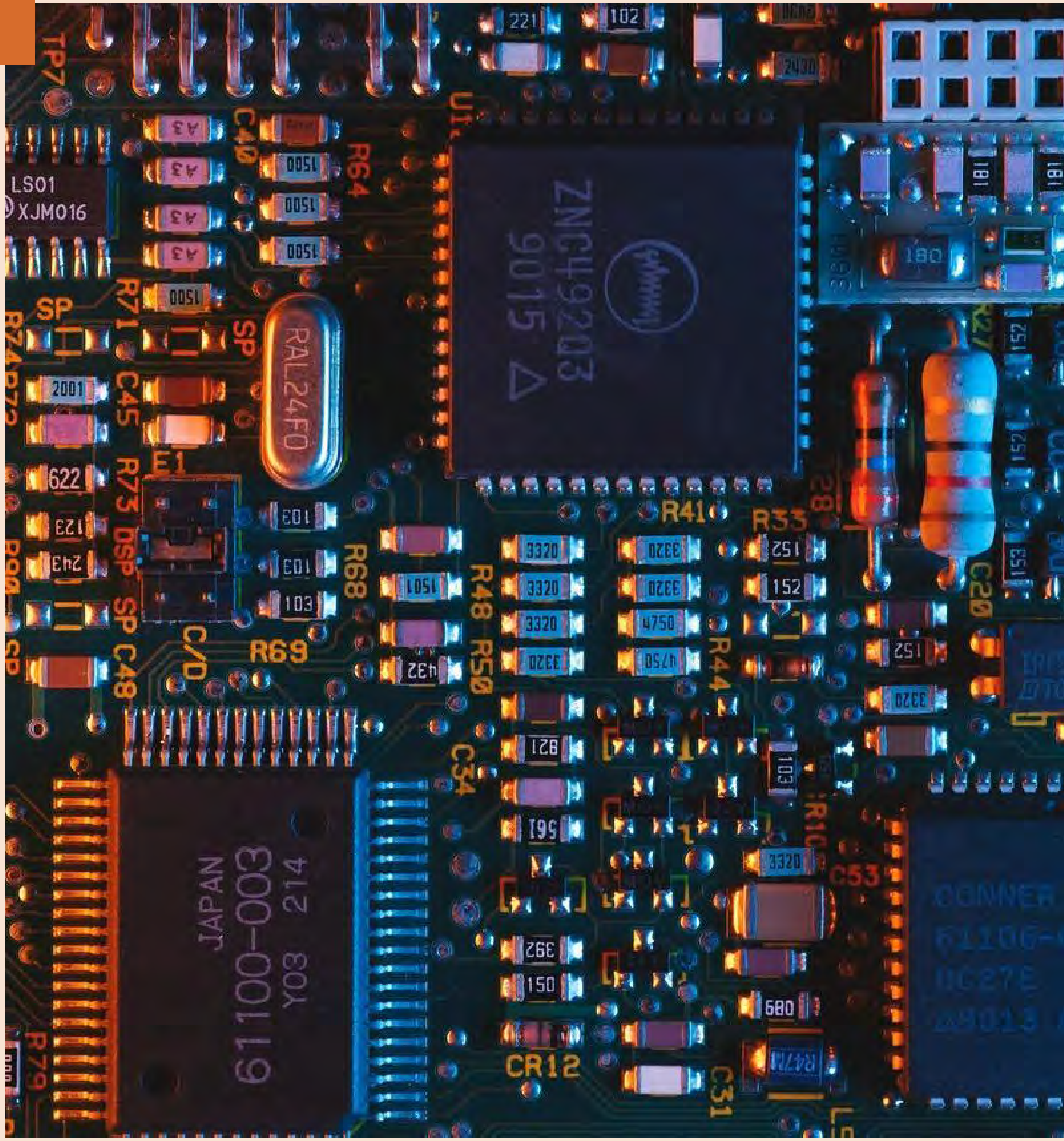
- Relevant elements of cyber regulation, both within the EU and beyond;
- The role and responsibility of directors;
- The value and limitations of frameworks;
- How best to set up an international cyber risk management programme that allows efforts to be leveraged elsewhere;
- Good cyber governance (role 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 take action and implement the necessary changes to governance and reporting to enable you to have oversight.

Some practical tips for organising cyber training for directors[27]:

- Deliver the training in person, at the office, as a scheduled agenda item during a regular board meeting;
- Invite your CIO, CISO, head of risk, auditor and head of legal affairs, so that all responsible parties receive the same message;
- 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.

[27] For example, use NOREA's boardroom training guideline

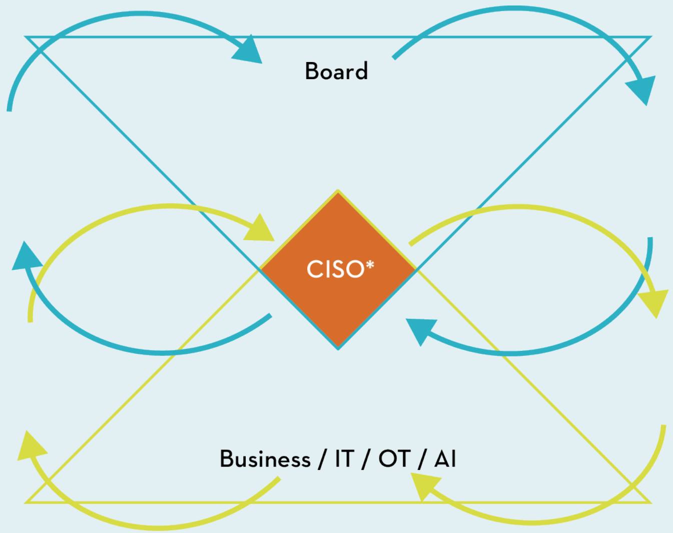


11. KEEP YOUR FINGER ON THE PULSE AND IMPROVE WHERE NECESSARY

Don't assume that cyber risks are static. Your organisation, your infrastructure and the threat landscape are constantly evolving. Technological developments such as AI, quantum computing and the Internet of Things 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 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 yourself 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.

This guide is a product of the Cyber Security Council of the Netherlands.

13. ACKNOWLEDGEMENTS

This guide is a product of the Cyber Security Council. Our thanks go to the authors of this guide and the contributing organisations.

Authors:

- Lokke Moerel (Professor of Global ICT Law, Tilburg University and CSR member representing the academic sector)
- Freddy Dezeure (independent consultant)

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)

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
Raamwerk	A document that sets out guidelines, standards and best practices to help mitigate cyber security risks
Awb	General Administrative Law Act (*Algemene wet bestuursrecht*)
DNB	De Nederlandsche Bank (Dutch central bank)
AFM	Dutch Authority for the Financial Markets
MFA	Multi-factor authentication, requires multiple verification factors to log in
Phishing resistant MFA	MFA with additional security to prevent phishing of verification factors

References

Tien belangrijke inzichten voor geïnformeerd cybertoezicht (Ten key insights for informed cyber oversight)
Cyberrisico's rapporteren aan raden van bestuur, bestuursuitgave (Reporting cyber risks to management boards, executive edition)
Cyberrisico's rapporteren aan Raden van Bestuur, CISO-uitgave (Reporting cyber risks to management boards, CISO edition)

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 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.

APPENDIX 4:
MORE INFORMATION ON SPECIFIC DUTCH STATUTORY REQUIREMENTS

Read more about NIS2 – Cyber Security Act

The NIS2 Directive applies to entities in sectors already covered by the original NIS Directive, as well as entities in newly added sectors. Organisations that fall within the scope of the Directive (and therefore the Dutch Cyber Security Act referred to below) are classified based on its specific criteria as either an 'essential' or an 'important' entity. The Dutch Authority for Digital Infrastructure (RDI) has developed a self-assessment tool[28] that organisations can use to determine whether they fall under the Cyber Security Act and whether they are considered 'essential' or 'important'.

As a European directive, NIS2 must be transposed into Dutch law before it takes effect. In the Netherlands, the NIS2 Directive is being implemented through a new law – the Cybersecurity Act – whose bill was published on 11 December 2024.[29]

The Cybersecurity Act will be further detailed in an order in council – the Cybersecurity Decree – for which the internet consultation closes on 30 March 2025,[30] as well as in ministerial regulations based on the Act or the Decree. The Decree elaborates on several aspects of the Cyber Security Act, including the duty of care, the registration obligation and the training obligation for directors.

This guide will be updated, if necessary, once the Cyber Security Act and Cyber Security Decree are finalised. This is not expected before the end of 2025.

NIS2 Cyber Security Act – Responsibilities of directors

Article 21 (duty of care) of the Cyber Security Act states that regulated entities 'must implement appropriate and proportionate technical, operational and organisational measures to manage risks to the security of the network and information systems used in their operations or to provide their services. They must also implement these measures to prevent incidents or minimise their impact on the customers of their services and on other services.'

[28] https://regelhulpenvoorbedrijven.nl/NIS-2-NL/
[29] Cyberbeveiligingswet | Overheid.nl | Wetgevingskalender
[30] Overheid.nl | Consultatie Cyberbeveiligingsbesluit

Under **Article 26 of the Cyber Security Act** the management board must:

- Approve the measures referred to in Article 23.
- Oversee these measures and how they are implemented.
- Have and maintain the necessary knowledge and skills.

Article 21 does not list the measures included in Article 21 NIS2. The Cyber Security Act states that these measures will be specified in an order in council, which has been done in Chapter 4 (duty of care) of the Cyber Security Decree. This covers all of the requirements set out in Article 21 NIS2, and in some areas provides additional detail.

NIS2 Cyber Security Act – Supply chain requirements

With regard to supply chain measures, Article 10 of the Cyber Security Decree states that organisations must establish policies addressing dependencies on products and services from direct suppliers, insofar as these may affect the security of their own network and information systems.[31]

NIS2 Cyber Security Act – Liabilities of directors

NIS2 outlines two types of personal liability for individuals in the organisation.

Collective liability. *De bestuursorganen kunnen aansprakelijk worden gesteld voor het niet treffen van de maatregelen door de entiteit voor het beheer van cyberbeveiligingsrisico's.*

Liability is attributed to the 'management bodies' as a whole, which implies collective responsibility. This means that individual members can be held jointly and severally liable for responsibilities within the management board as a whole, even if certain duties have been delegated to specific members of the management body.

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.[32]

'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.

NIS2 does not specify the nature or scope of the liability (civil, administrative or criminal). This will need to be addressed in national law. The Cyber Security Bill does **not** include provisions to implement the NIS2 liability provisions.[33]

According to the Explanatory Memorandum[34] to the bill, existing Dutch administrative law provisions on director liability, as set out in the General Administrative Law Act (Awb), already provide an adequate legal basis. This means that if a legal entity commits a breach, the person who instructed the action or had de facto control may also be subject to corrective measures, such as an administrative fine, an administrative enforcement order or a penalty payment.

The Explanatory Memorandum does not address civil liability of directors under the Dutch Civil Code, suggesting that the general rules for internal and external liability of directors under Dutch private law remain unchanged.

Although not a liability provision, NIS2 does state that in exceptional circumstances, a managing director or other person with executive responsibility at the level of legal representative may be temporarily suspended from performing management duties.[35] Such a suspension must be imposed by a court, at the request of a supervisory authority.

NIS2 Cyberbeveiligingswet - Trainingsvereisten

The Cyber Security Act requires that each director acquire the following knowledge and skills within two years after the Act enters into force:

- the ability to identify risks to the security of network and information systems;
- the ability to assess risk control measures in the area of cyber security;
- the ability to evaluate the impact of such risks and risk control measures on the services provided by the entity.

[31] See p. 10 of the Explanatory Memorandum to the consultation version of the Cyber Security Decree.
[32] Article 32(6), in conjunction with Article 33(5) NIS2.

[33] Articles 20, 32(6) and 33(5) NIS22.
[34] *9248e519-467c-4323-873a-2dcdd47d3948_1.pdf, see section 5.6.6.
[35] However, Article 32(5) applies only to essential *entities*, not to *important entities*.

Directors must demonstrably keep these skills up to date and be able to provide certificates of participation for training completed. The Cyber Security Decree further specifies that the training must cover at least the following topics:

- the types of risks to network and information systems;
- the risk management processes;
- risk assessment methodology;
- the risk control measures (see Article 21 of the Cyber Security Act) that the management board is expected to approve and oversee their implementation.

No requirements are set regarding the duration of the training.

Read more about DORA

The Digital Operational Resilience Act (DORA) is European legislation aimed at enhancing the digital resilience of the financial sector. DORA includes a *regulation* and a *directive*.[36] The regulation, which applies directly in the Dutch legal system, entered into force on 17 January 2025. However, implementation and enforcement arrangements were required. This was done through an amendment to the EU Financial Markets Regulations (Implementation) Decree (*Besluit uitvoering EU-verordeningen financiële markten*), which designated DNB and the AFM as the competent authorities responsible for implementing and enforcing DORA.[37]

On 17 January 2025, the implementing Act for the DORA directive, including amendments to the Financial Supervision Act (*Wet op het financiële toezicht*) to align with the DORA regulation[38], and the Implementing Decree for digital operational resilience in the financial sector (*Implementatiebesluit digitale operationele weerbaarheid financiële sector*) also came into force. The three European Supervisory Authorities (ESAs) have been jointly appointed to lead the development of technical standards for DORA, some of which have already been published.[39]

DORA – Responsibilities of directors

Article 5 DORA imposes the following obligations on financial entities:

- Financial entities must have an internal governance and control framework that ensures an effective and prudent management of ICT risk.
- The 'management body' must define, approve, oversee and be responsible for the implementation of all arrangements related to the ICT risk management framework. Article 5(2)(a) then expressly provides that the management body bears 'the ultimate responsibility for managing the financial entity's ICT risk'. 'Management body' means both the management board and the supervisory board.[40]
- Members of the management body must actively keep up to date with sufficient knowledge and skills to understand and assess ICT risk and its impact on the operations of the financial entity, including by following specific training on a regular basis, commensurate to the ICT risk being managed.

Knowledge of DORA is now a topic that usually comes up in suitability interviews for directors and supervisory board members.

DORA – Liabilities of directors

The competent authorities may impose certain administrative penalties and corrective measures on the financial entity.[41]The DORA regulation also grants 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.[42]

As competent authorities, DNB and AFM are tasked with implementing and enforcing DORA.[43] They may impose an order subject to a penalty or a fine in case of violations of DORA rules and also exercise powers granted under the Financial Supervision Act (Wft). The AFM's and DNB's enforcement policy have not changed with the introduction of DORA.[44]

[36] Directive (EU) 2022/2556 on a framework for digital operational resilience in the financial sector.

[37] More specifically, by amending Annex 35 to the EU Financial Markets Regulations (Implementation) Decree.

[38] DORA Implementation Act, amending the Financial Supervision Act to implement Directive (EU) 2022/2556 on a framework for digital operational resilience in the financial sector

[39] For a list of technical standards, see: DORA | De Nederlandsche Bank

[40] See footnote 9.

[41] Article 50(2)(c), read together with 50(4) and 50(5) DORA.

[42] Article 50(5) DORA.

[43] By amending Annex 35 to the EU Financial Markets Regulations (Implementation) Decreen.

[44] For DNB and AFM's enforcement policy and sanctions, see: wetten.nl - Regeling - The enforcement policy of the AFM and DNB - BWBR0044284

Read more about CER

The CER Directive targets ‘critical entities’ that provide essential services in sectors such as energy, drinking water, transport, digital infrastructure, food, healthcare, financial market infrastructure, wastewater, government, banking and aerospace. In addition to the cyber security requirements under NIS2, ‘critical entities ‘are also subject to requirements to ensure their **physical resilience**, for example against sabotage.

The CER Directive is implemented in the Critical Entities Resilience Act (*Wet weerbaarheid kritieke entiteiten*).[45] The ministries responsible for the critical sectors determine which organisations they designate as critical entities. Organisations therefore do not have to make this determination themselves. The Critical Entities Resilience Act will be elaborated in an order in council – the Critical Entities Resilience Decree (*Besluit weerbaarheid kritieke entiteiten*) – the internet consultation for which closes on 30 March 2025.[46] The requirements under the CER Directive/ Critical Entities Resilience Act are not discussed further here.

Read more about CRA

The Cyber Resilience Act (CRA)[47] is a European Regulation that sets binding requirements for the cyber security of ‘all products with digital elements’ (including all hardware, software and IoT devices). This ensures that consumers and businesses can safely use digital products, such as webcams and smart TVs that form part of the Internet of Things (IoT).

The law requires companies to treat cyber security not as an afterthought but as a core part of their product development. A transition period has been introduced, ending on 11 December 2027, allowing products and processes to be adjusted to meet the new requirements. The transition period for the mandatory reporting of cyber security incidents ends earlier, on 11 September 2026. The requirements under the CRA are not discussed further here.

[45] Wet weerbaarheid kritieke entiteiten | Overheid.nl | Wetgevingskalender
[46] Overheid.nl | Consultatie Besluit weerbaarheid kritieke entiteiten
[47] https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202402847

CSR Cyber Security Raad