NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Boardroom Training guideline

With a focus on DORA and NIS2

A guideline by NOREA

PO box 242, 2130 AE Hoofddorp

Phone: +31 (0) 88 4960 380

The Netherlands

e-mail: norea@norea.nl

Taskforce participants

The authors of this guideline from the Regulatory Taskforce are:

Name	Role	Company
Danny Bos	Senior Manager Cyber Security & Privacy	Eraneos
Harry Boersen	CTO	ANVA
Iliass el Attoti	Manager Technology Risk	EY
Jesper de Boer	Director IT-audit	Deloitte
René Zendijk	Head of Internal Audit	Scildon
Shankar Sahtie	Consultant Cyber Security	SVJ Consultancy
Sandeep Gangaram Panday	Consultant Cyber Security	Brightlyn

For the full member list and more content created by the Taskforce, please see https://www.norea.nl/regulatory

The guideline was reviewed by:

Name	Role	Company
Arno Kroese	Partner Business & Digital Risk	Grant Thornton
Bart Pieters	Adviseur Informatiebeveiliging & Privacy	CIO Rijk van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Freddy Dezeure	Independent Advisor	Freddy Dezeure B.V.
Martin van Vessem	CISO	CZ
Steven Debets	Partner	Highberg Digital

Supervisory authorities

This guideline has been shared with several supervisory authorities (DNB, AFM, Cbw-supervisory authorities) and the CIO Rijk, part of the Ministry of Interior and Kingdom Relations. The supervisory authorities and CIO Rijk provided the following joint response:

"These knowledge objectives have been prepared by NOREA to provide guidance to the industry on practical implementation of boardroom training. DNB, AFM and the Cbw-supervisory authorities did not contribute to its development. The development of these knowledge objectives is in accordance with previous initiatives from DNB, AFM, the Cbw-supervisory authorities and CIO Rijk to work together within the sector to increase the overall cyber resilience. DNB, AFM, the Cbw-supervisory authorities and CIO Rijk appreciate these sectoral initiatives which support overall awareness of cyber resilience.
DNB, AFM, the Cbw-supervisory authorities and CIO Rijk stress that complying with applicable laws and regulations is at all times a responsibility of the institution. No confidence can be derived from the use of this guidance that parties thereby act in accordance with laws and regulations."

Disclaimer: This guideline on Boardroom training is a practical tool designed to support organizations in their journey to ensure compliance with the applicable regulation. While this guideline can offer valuable insights, it is important to note that the legal requirements itself remain leading. Additionally, as NIS2 is implemented through national legislation, the relevant national legislation may contain additional requirements.

Feedback can be shared through norea@norea.nl

Table of Contents

1. Introduction

As dependency on ICT systems increases throughout all sectors of society, the European Union (EU) has introduced two key legislations to better manage the multifaceted risks that critical industries face: Regulation (EU) 2022/2554, more commonly referred to as The Digital Operational Resilience Act (DORA) and Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity across the Union (The NIS2 Directive/NIS2). These two laws entailed a significant shift in the EU's approach to cybersecurity; taken together they contribute significantly to a more cohesive and comprehensive EU cybersecurity strategy.

The NIS2 Directive applies broadly to essential and important entities across various sectors, including three types of financial institutions[1]. In the Netherlands, the NIS2 Directive has already been adapted via the Dutch implementation law called the Cyberbeveiligingswet (Cbw), which has been further elaborated in the Cyberbeveiligingsbesluit (Cbb). DORA is specifically tailored for financial institutions, as it applies to organizations operating or providing services for the financial sector. For more background information on DORA, refer to the NOREA publication on DORA[2].

While their scope and focus differs, the two legislations have the same objective: enhancing cybersecurity and operational resilience to ensure the stability and integrity of critical industries within the EU. Most importantly, both legislations mandate that the management body take an active, personal role in cybersecurity, which means that managers are now required to have a foundational understanding of cybersecurity principles and best practices.

Our goal is to provide clear guidance on what these requirements for managers entail, enabling organizations to implement these laws effectively and to carry out their responsibilities with a unified perspective.

2. Scope of training for Board Members

While some of the articles of DORA and NIS2 are highly detailed, others remain vague. Combined with the fact that both regulations are risk and proportionality based, means that institutions struggle to determine the depth and scope of certain requirements. In this document, we present a guideline for the boardroom training, or the training of the "management body" (as per DORA) or "management bodies of the essential or important entities" (as per NIS2).

DORA, through auxiliary legislation and directives, defines management body as the board and the supervisory board. NIS2 does not give an in-text definition of what it considers as management bodies of the essential or important entities (this was done to accommodate for the diverse organizational structures across the EU), but it is largely

[1] Credit institutions and Financial market infrastructures, Operators of trading venues and Central counterparties (CCPs)

[2] https://www.norea.nl/uploads/bfile/52ee1e0f-54ae-4157-9a43-524c746c2ff1

understood that this definition refers to the governing and leadership team of the organization.

The basis for the training for board members, including their responsibility for the education of staff, of organizations has its origin in Articles 5.4 and 13.6 of DORA. Article 5.4 requires that *"Members of the management body of the financial entity shall 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."* In addition, Article 13.6 further requires that *"Financial entities shall develop ICT security awareness programmes and digital operational resilience training as compulsory modules in their staff training schemes. Those programmes and training shall be applicable to all employees and to senior management staff, and shall have a level of complexity commensurate to the remit of their functions. Where appropriate, financial entities shall also include ICT third-party service providers in their relevant training schemes in accordance with Article 30(2), point (i)."*

In Article 5.4 above, the reference is made to ICT risk. ICT risk is defined in Article 3(5) as: "*any reasonably identifiable circumstance in relation to the use of network and information systems which, if materialised, may compromise the security of the network and information systems, of any technology dependent tool or process, of operations and processes, or of the provision of services by producing adverse effects in the digital or physical environment.*"

In NIS2 the reference to training for the management bodies is in Article 20.2: "*Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.*"

The requirements that derive from the Articles described above are clear. DORA and NIS2 require organizations to ensure that their management body is adequately trained in cybersecurity generally, and well aware of the ICT environment of their organization specifically. This entails a significant knowledge expectation, the responsibility for which rests directly with the board members themselves.

3. Why should training be done?

Training should be done to enable board members to manage risks, to make well-informed decisions, and to ensure appropriate resilience of the organization in the event of ICT incidents.

The training should focus on and be tailored towards understanding the specific ICT risks that the organization may encounter. It should be regularly repeated and adapted to keep up to date with the rapid evolvement of digital threats and regulations. The training courses must therefore be flexible (depending on the nature and needs of the

organization), which means that the content of the training courses could also periodically vary. This can range from understanding cyber threats to effectively deploying technology solutions for risk management and response. Training should also include scenarios and best practices to be prepared for events such as digital disruptions or cyber threats.

As part of the training the management body must also understand the key elements of digital operational resilience. The focus should be on the organization's ability to withstand disruptions and continue critical operations during and after a major ICT incident. The training should also steer in the direction of risk prevention and management rather than post-incident reactivity.

An additional objective of the training for the management body is to ensure that the ICT Risk Management framework and the associated risks are understood. This is not only about understanding internal risks, but also about external threats that can affect the organization.

4. Types of training

The Articles cited in chapter 2 above, mention that the members of the management body must actively keep themselves up to date with sufficient knowledge. This implies that the training cannot be one-time only/only initial training. Therefore, a distinction can be made between two types of training:

- Initial training: aimed at transferring knowledge and increasing insight into the most important parts of digital resilience. This training is particularly important during the implementation phases of DORA and NIS2 and during management changes, when a solid basic knowledge is essential. For this initial training we suggest to cover all 8 domains of the training schedule presented in chapter 8.
- Recurring training: aimed at ensuring that knowledge level of the management body remains up-to-date. For recurring trainings, we recommend to select the domains of the training schedule presented in chapter 8, that have undergone (significant) changes within the institution, are linked to the greatest risks and/or may have a negative impact on the organization.

5. Form and frequency of training

Training may be given in different forms and shapes, such as:

- In house, preferably during a regular Board meeting,
- Classroom,
- Discussion (e.g., dilemma discussions),
- E-learning,
- Crisis exercise (simulation and/or tabletop),
- Evaluations of major incidents.

Depending on the risk, size of the organization, maturity and threat levels, the frequency of the training courses may differ (see also chapter 4). Institutions are also free to use Permanent Education sessions in addition or as a substitution for some of the themes.

6. Specific NIS2 requirements for the Netherlands

In the Netherlands, NIS2 has been implemented through the Cyberbeveiligingswet (Cbw) and the Cyberbeveiligingsbesluit (Cbb), which have some additional requirements encoded on top of the ones already prescribed by NIS2.

The Cbb includes specific requirements regarding:

- The goal: Article 21 states that purpose of the training is to equip board members of essential and important entities with the knowledge and skills to identify risks to the security of network and information systems, assess their impact on the services provided, and evaluate cybersecurity risk management measures and their consequences for those services.
- Requirements of the training: Article 22 states that the training must enable board members to identify and assess risks to network and information systems, covering:
    - types of risks,
    - risk management processes, and
    - risk assessment methods.

  Additionally understand and evaluate cybersecurity risk management measures, addressing the topics listed in Article 21(3)(a–j) of the Act (such as policies, incident handling, business continuity, supply chain security, and use of cryptography).
- Certification: Article 23 emphasizes that the training should be concluded with a certificate of participation. The certificate must include at least:
    a) the name of the board member of the essential entity or significant entity;
    b) the date(s) on which the training was attended;
    c) the topics covered in the training; and
    d) the name of the training provider.

7. Introduction to the knowledge objectives for the management body

Although it is not new that the boardroom is in the end responsible and accountable for all security operations, personal liability is new. In general, the reflex of the boardroom is to delegate tasks and mandate other people. They become responsible to execute specific tasks, while the boardroom mainly remains focused on strategic oversight. Regarding cybersecurity, the boardroom often delegates the responsibility to the CIO and CISO. However, due to the changed requirements, now the board must be directly involved in guiding and making decisions regarding cybersecurity.

The specific responsibilities of the boardroom depends on many factors, but both DORA and NIS2 have set out certain minimum requirements.

For the NIS2 the requirements are as follows:

- The management bodies approve the cybersecurity risk-management measures,

- The management bodies oversee the implementation of the cybersecurity risk-management measures.

Under DORA the requirements are:

- The Management body shall take ultimate responsibility for effectively managing all ICT risks of the financial entity,
- The Management body shall set and approve the digital operational resilience strategy and periodically update when needed,
- The Management body reviews and approves periodically (e.g. annually) the ICT business continuity policy and the ICT response and recovery plans,
- The Management body reviews and approves periodically (e.g. annually) internal ICT audit plans, ICT audits, and material modifications to the audits,
- The Management body reviews and approves periodically (e.g. annually) the ICT third-party service providers management policy.

The personal involvement of the boardroom is critical in fostering and demonstrating a strong security culture. Based on experience and inspired by the Dutch Corporate Governance Code[3], typical cyber activities for the boardroom include:

- Establishing clear governance and reporting for cybersecurity,
- Identifying and defining critical functions and assets that require protection,
- Setting the organization's cybersecurity risk appetite,
- Allocating adequate budgets and resources to address identified risks and ensure compliance with regulatory requirements,
- Aligning cybersecurity priorities with overall business objectives and regulatory obligations,
- Fostering a culture of accountability and resilience.

As mentioned above, the exact role of the boardroom depends on many factors, and it can deviate per the needs of the organization. In the table below the full set of knowledge and responsibility objectives for an organisation are listed, which can be used as a library of inspiration to tailor cybersecurity based on the organizations risk profile and risk proportionality.

In the table a distinction has been made between knowledge objectives and responsibility objectives. **Knowledge objectives** focus on what board members need to understand, such as being able to contribute to the definition of the risk appetite or understanding the importance of an asset inventory. This knowledge equips them with the foundational awareness needed to make informed decisions. On the other hand, **responsibility objectives** outline the legal and strategic duties that board members are obliged to fulfil, such as overseeing risk management frameworks, monitoring compliance, and ensuring a proper and tested business continuity strategy. By delineating these two categories, organizations can better structure boardroom training and ensure alignment with regulatory demands and best practices for cyber resilience.

[3] https://www.mccg.nl/documenten/2025/03/corporate-governance-code-2025

This distinction also reinforces the board's dual role as both learners and leaders in navigating today's complex digital landscape.

In chapter 8, we present the knowledge training objectives and responsibilities for the management body by using the following structure:

- Domain: Identifies specific focus areas within the DORA framework that require attention,
- Knowledge Objectives: Outlines essential knowledge board members need to understand[4] regarding their digital risk management responsibilities,
- Responsibility Objectives: Delineates the legal and strategic duties board members must fulfil for compliance and resilience,
- Mapping to Practical Questions for improved boardroom dialogue: Provides practical questions to enhance discussions within the boardroom based on the NCSC factsheet and the CSC Cybersecurity Guideline for Directors.

[4] The word "understand" is based on Bloom's taxonomy; https://wij-leren.nl/taxonomie-van-bloom.php

8. The Knowledge objectives for the management body

Domain	Knowledge objectives	Responsibility objectives	Mapping to practical questions for improved boardroom dialogue based on the factsheet from the NCSC[5] and CSC[6]
1.Governance & Risk Management	• Understand the roles, responsibilities and accountability of the Management Body members, including the 3LoD. • Understand the organisation's ICT risk management framework and the risk cycle (plan, do, check and act). • Be able to contribute to the definition of the organization's risk appetite and risk tolerance level. • Understand the organisation's critical functions and their degree of dependency on ICT services. • Understand the expectations of the Digital Operational Resilience Strategy (DORA specific) or IT security strategy. • Be able to understand and approve the most important security policies. • Understand the need for transparent cyber reporting to and active oversight by the Management Body.	• Carry out the management body responsibility for digital resilience and update the ICT risk framework by taking into account the organization's environment (e.g. increased threats or geopolitical developments). • Oversee the resilience of most critical ICT and the mitigation of the cyber security risks of the organization within the risk appetite. • Understand and approve the Internal Audit year plan and specifically, the prioritization and added value of the audits in relation to the key IT risks. • Oversee compliance with regulatory cyber requirements (DORA and NIS2 specific) or IT security strategy.	NCSC: • What are the most pressing issues I need to focus on? • What do I need to ensure that management allocates sufficient people and resources to achieve the objectives? • What mechanism is in place within the organization to secure the cybersecurity strategy and approval of policies around risk management by management? • With what frequency is cybersecurity on the agenda to ensure that there is sufficient progress on this topic? • What is the role and task of the CISO when they join board meetings? • As a board member, what do I need to know to gain sufficient insight into this organization's cybersecurity risks? • Are risk assessments carried out, if so, what are their main issues and outcomes? • What are our biggest risks and threats and do we have sufficient control over them? • Are our risks incidental or structural? • How do we identify and calculate the probability and impact and how do we distinguish between the different types of risks? What role do I play in them? • What residual risks are there? Are these acceptable?

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

[6] https://www.cybersecuritycouncil.nl/documents/2025/08/14/guide-to-cyber-security-for-directors-and-business-owners

Domain	Knowledge objectives	Responsibility objectives	Mapping to practical questions for improved boardroom dialogue based on the factsheet from the NCSC[5] and CSC[6]
			• Have the residual risks been discussed with the supervisory authorities? • As an organization, do we have a cybersecurity strategy? If so, what does it look like?
2.Operational management	• Understand the importance of asset classification and inventory management. • Understand key principles of resilient systems.	• Provide direction on improvement actions, priorities and timelines for key assets and processes.	NCSC: • What are our key assets and processes? CSC: • Do we have an actual inventory of our ICT systems? Do we have shadow ICT systems or legacy systems? Suggested additional question: • How do we identify gaps in key controls?
3.Continuity management	• Understand the business continuity policy and the response & recovery plans. • Understand the media management, crisis organization and communication plan. • Understand the quick decision-making role of the management body during severe attacks or disruptions • Understand the different types of back-up and recovery strategies.	• Know, and periodically challenge the measures for the resilience of critical functions under duress or disruptions. • Stewardship in NO-IT scenarios and capacity to carry out agreed measures and responsibilities. • Practice various crisis scenarios or cyber drills (tabletop, walkthroughs, simulation games).	NCSC: • Suppose things go wrong unexpectedly, do we have a contingency plan (backup/redundancy systems) and an Incident response plan? If so, how do these look like?
4.Incident management	• Understand the key aspects of the incident management policy and escalation paths. • Understand classification and reporting of incidents. • Know the most important stakeholders and their roles in the event of a major incident.	• Monitor the DORA and NIS2 specific major incident reporting timelines (if relevant also SEC – Securities and Exchange Commission). • Know how to report major incidents to the supervisory authorities in the different regions.	CSC: • Do we have an incident response plan? • Are we, as a company and as the board, (sufficiently) insured against cyber risks? Suggested additional question:

Domain	Knowledge objectives	Responsibility objectives	Mapping to practical questions for improved boardroom dialogue based on the factsheet from the NCSC[5] and CSC[6]
			Do we have an overview of our reported major incidents and the current status of the required improvements?
5.Software and systems development	• Understand the key aspects of the software and systems acquisition, development and maintenance policy.	• Understand the most critical aspects of software and systems acquisition, development and maintenance. • Understand most critical aspects regarding testing systems • Understand how well the required tests are performing.	N/A
6.Third-party Risk management	• Understand the third-party risk management process incl. supplier management and understand that third party risk must be managed as an integral component of ICT risk and ICT risk management framework. • Understand key contractual agreements such as e.g. exit strategy, unrestricted rights of access, inspection and audit and notice periods and reporting obligations of the TPP (third-party provider). • Expectations of the Register of Information (DORA specific). • Understand the risk management aspects in the context of critical outsourcing, such as, due diligence, supplier assessments, impact of changes and monitoring of the internal control and performance of the chain of ICT service providers,	• Know the critical third-party providers of the institution and oversee their periodic evaluation whether the strategy still fits. • Understand the impact of changes in the chain of critical subcontractors. • Understand the level of compliance to the required security and contractual requirements (e.g. exit plan) of the critical third-party providers of the institution. • Have insight in involvement of the critical third-party providers of the institution in continuity tests, resilience tests (TLPT in DORA), security awareness campaigns etc.	NCSC: • Which third parties do we use? CSC: • Do we know the dependencies of ICT suppliers and do we control the involved risks? Suggested additional question: • Which ICT service providers do we rely on for our critical processes/functions? • What are alternatives for our most critical ICT service providers?

Domain	Knowledge objectives	Responsibility objectives	Mapping to practical questions for improved boardroom dialogue based on the factsheet from the NCSC[5] and CSC[6]
	avoidance of vendor lock-in, strategic autonomy.		
7.Resilience testing	• Understand the purpose of the different types of digital operational resilience testing, such as Red Teaming and TLPT (DORA specific).	• Understand the Digital Operations Resilience Test Program of the institution and knowing that the program must cover the entire critical (ICT) environment • If TLPT is applicable, monitoring the results and improvements identified in the test.	CSC: • Do we perform resilience tests? Suggested additional question: • How are we involved in the preparation and evaluation of resilience testing?
8.Security management	• Understand the most important controls (see an example list in the guideline from the Cyber Security Council chapter 5[7]). • Have insight in most relevant attack vectors in the domain of the institution. • Knowledge of the different types of risks involved in network and information systems, such as the threat of malware, insider threat and DDoS attacks that pose a risk to integrity and availability (specifically for NIS2). • Have insight into the cyber threat profile of the institution and possible impact of cyber-attacks on the organization. • Have insight in important social engineering measures, such as	• Ensure security roles and responsibilities are clear and implemented, including proper reporting lines. • Oversee the implementation status and coverage of the most critical security measures of the institutions. • Implement cyber hygiene for yourself, give the good example by complying with the organisation's policies and convey cybersecure tone at the top.	NCSC: • To what extent is there a positive security culture within the organization? • What level of knowledge is required within the rest of the organization? • To what extent is education and training required for the organization? • What measures have we taken to protect our key assets? • What is the status of these measures and which ones still need to be taken to reach an acceptable resilience level? • Which measures are we not taking and why are we not taking these measures? • Who is responsible for the measures taken? • Is there an overview of the measures implemented to protect the systems (including their physical environment) and data of the organization? • How do we monitor implementation/compliance with the agreed measures? • What needs to be done to address the current deficiencies and what do you as CISO need from me?

[7] https://www.cybersecuritycouncil.nl/documents/2025/08/14/guide-to-cyber-security-for-directors-and-business-owners

Domain	Knowledge objectives	Responsibility objectives	Mapping to practical questions for improved boardroom dialogue based on the factsheet from the NCSC[5] and CSC[6]
	Spoofing, Phishing, Inserting subversive individuals into organizations and interpersonal manipulations, Qishing.		CSC: • Which systems are so important that we need restricted access? • How important is cybersecurity for our products and our clients? Or even for society? • How does our cybersecurity compare to our peers?

9. Conclusion

In essence, the Digital Operational Resilience Act (DORA) and the Network and Information Security Directive (NIS2) collectively mandate not only the implementation of robust risk management frameworks but also the promotion of a culture of continuous learning and awareness across all levels of an organization. While DORA focuses on strengthening digital resilience in financial institutions, NIS2 extends this imperative to organizations across critical sectors, emphasizing a unified approach to cybersecurity. Both frameworks highlight the dual role of the management body, requiring both knowledge objectives and responsibility objectives to be addressed. Knowledge objectives focus on equipping leaders with the necessary understanding of cyber risks, threat landscapes, and regulatory requirements, while responsibility objectives ensure they are accountable for implementing governance frameworks, fostering resilience, and aligning cybersecurity initiatives with organizational strategy.

To meet these regulatory requirements, the management body must transcend traditional oversight roles and take an active approach to resilience. This involves continuously expanding and updating their competencies to effectively identify, assess, and mitigate threats, fulfilling their obligations. Simultaneously, they are responsible for driving the governance processes and fostering a culture of digital resilience, ensuring their organizations remain prepared for future challenges. Proactively addressing these objectives ensures not only compliance but also sustained agility and confidence in navigating an increasingly dynamic digital landscape.

Furthermore, the shared emphasis on continuous learning within both DORA and NIS2 underscores the importance of embedding cyber resilience into the organizational ethos. By prioritizing structured training programs, institutions can create an environment where preparedness against cyber threats becomes integral to operations, driving both individual awareness and collective accountability. This dual focus on comprehension and action strengthens the institution’s resilience and enhances its reputation as a leader in managing digital risks responsibly.

Ultimately, DORA and NIS2 serve as complementary frameworks, providing both the guidance and the legal imperative for management bodies to lead the charge in building a more resilient future. By addressing both knowledge and responsibility objectives, organizations can not only comply with expectations but also position themselves as proactive leaders in today’s increasingly interconnected and high-risk digital landscape.