Guideline DORA Boardroom training

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 Taskforce are:

Name	Role	Company
Danny Bos	Senior Manager Cyber Security & Privacy	Eraneos
Harry Boersen	Director Tech Advisory	Yaworks
Jesper de Boer	Director IT-audit	Deloitte
René Zendijk	Head of Internal Audit	Scildon
Shankar Sahtie	Consultant Cyber Security	SECURESULT
Sandeep Gangaram Panday	Trust Officer	Schuberg Philis

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

The guideline was reviewed by:

Name	Role	Company
Arno Kroese	Director IT Assurance & Advisory	KPMG
Freddy Dezeure	Independent Advisor	Freddy Dezeure B.V.
Martin van Vessem	CISO	CZ
Steven Debets	Partner	Highberg Digital

Disclaimer

This guideline on Boardroom training is a practical tool designed to support organizations in their journey toward compliance with the Digital Operational Resilience Act (DORA). While this guideline can offer valuable insights, it is important to note that the legal requirements set out in the DORA itself remain leading.

Table of Contents

1. Introduction DORA

The Digital Operational Resilience Act (DORA), officially known as Regulation (EU) 2022/2554, came into force on January, 16th of 2023 and has become into effect per the 17th of January 2025. Now that DORA applies, organizations operating or providing services for the financial sector will be expected to have undergone significant changes and be prepared to abide by new requirements.

In light of the evolving and increasing dependencies on ICT systems, the EU introduced DORA to address multifaceted risks within the financial sector. DORA marks a significant shift in the EU's broader regulatory framework. Now emphasized is the importance of digital operational resilience to safeguard the stability and integrity of the financial market.

DORA is a legislative act intended to ensure that financial entities within the EU can withstand, respond to, and recover from various types of ICT-related disruptions and threats. It consolidates and enhances existing ICT requirements, constructing a unified framework for digital operational resilience across the European financial sector.

DORA specifies numerous requirements to help organizations build and maintain digital operational resilience. These requirements are centered around five pillars:

1. ICT risk management
2. Incident management, classification, and reporting
3. Digital operational resilience testing
4. Managing of ICT third-party risks
5. Information-sharing arrangements

The main text of DORA is supplemented by important technical details in a body of secondary legislation, referred to as level 2 standards. These technical standards consist of two types:

- Regulatory technical standards (RTS), of which there are seven
- Implementation technical standards (ITS), of which there are two

The three European supervisory authorities (ESAs) were jointly appointed to draft these standards. The ESAs consist of the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Markets Authority (ESMA).

Development of the RTS and ITS was separated into work on two sets. The first set was submitted to the European Commission (EC) on 17 January 2024. The three RTS documents in this first set were published in the *Official Journal of the European Union* on 25 June 2024, signaling their official adoption.

The first set consists of the following documents:

- RTS on ICT risk management framework including the simplified ICT risk management framework article 28-41 (part of DORA's first pillar);
- RTS on criteria for the classification of ICT-related incidents (second pillar)
- ITS to establish the templates for the register of information (fourth pillar)
- RTS to specify the policy on ICT services performed by ICT third-party providers (fourth pillar)

The second set, which was submitted to the EC in two parts, on 17 July 2024 and 26 July 2024, consists of the following documents:

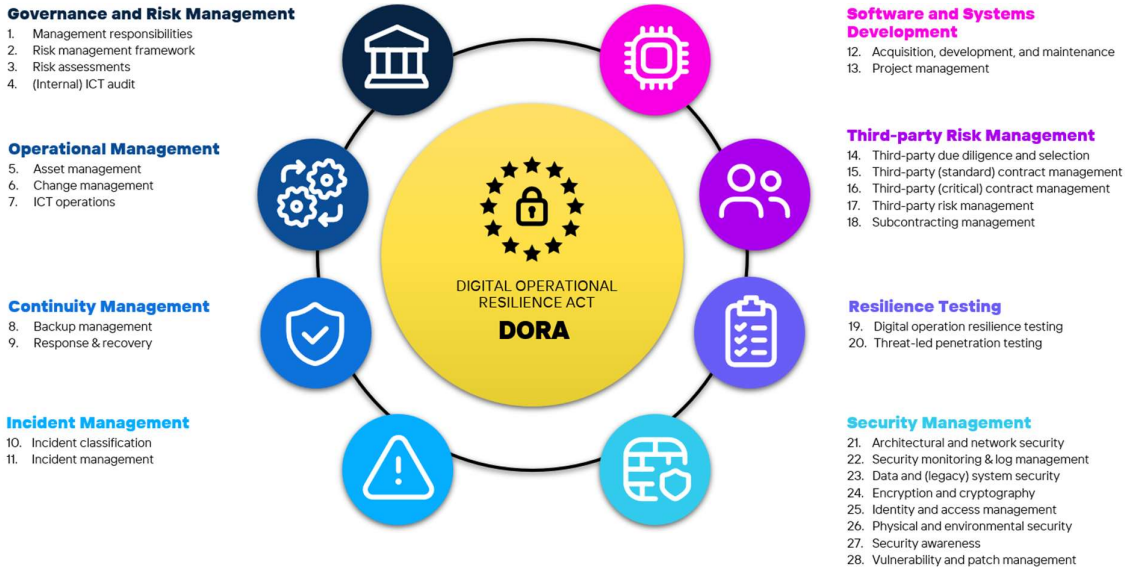
- RTS on content, timelines, and templates on incident reporting (part of DORA's second pillar)
- ITS on content, timelines, and templates on incident reporting (second pillar)
- RTS on subcontracting of critical or important functions (fourth pillar)
- RTS on oversight harmonization (fourth pillar)
- RTS on threat-led penetration testing TLPT (third pillar)

For links to the latest versions of the RTS and ITS, please see https://www.dnb.nl/dora.

2. The DORA Control Framework

In November 2024, NOREA DORA Taskforce published a DORA study report[1], including a DORA control framework[2]. The aim of the study report and framework is to make DORA more accessible to financial institutions. The presented DORA control framework consists of eight control domains, 28 sub-domains, and 95 individual controls. For a visualization, see figure 1. The boardroom training guideline (Appendix A) presented in this publication is aligned with the DORA Control Framework.

[1] https://www.norea.nl/uploads/bfile/52ee1e0f-54ae-4157-9a43-524c746c2ff1
[2] https://www.norea.nl/uploads/bfile/4693bb51-d6c0-4c3d-8e3e-577f74af9d73



3. DORA Training for Board Members

A number of the articles in DORA are elaborated in detail, however some not so much. Combined with the fact that DORA is risk and proportionality based, this means that financial institutions struggle to determine the depth and scope of certain articles. NOREA therefore publishes guidelines and templates for some of these articles and subjects[3]. In this document, we present a guideline for the boardroom training or the management body as called in DORA. The management body is defined in article 3 and includes the management board and the supervisory board.

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: "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.'

And

Article 13.6 " 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).'

[3] https://www.norea.nl/dora

In article 5.4 above, the reference is made to ICT risk. ICT risk is defined in article 3.5 as:

"ICT risk means 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."

Considering the requirements in Article 5.4 and Article 13.6, along with the definition in Article 3.5 of DORA, it is clear that board members must have a thorough and broad understanding of ICT and its specific use in their own organization, **emphasizing the significant knowledge** expectations placed upon them.

4. Why should training be done?

Article 5.4 of DORA requires institutions to ensure that their management body are adequately trained in digital risk and cybersecurity. This enables them to manage risks, make well-informed decisions, and ensure appropriate resilience of the organization in the event of digital incidents.

The training should specifically focus on understanding the digital risks that the organization may encounter. It should also include scenarios and best practices to be prepared for digital disruptions and cyber threats. The training should be regularly repeated and adapted to keep up to date with the rapid evolvement of digital threats and regulations.

The training should also provide insights to steer in the direction of risk prevention and management rather than acting reactively after an incident. This can range from understanding cyber threats to effectively deploying technology solutions for risk management.

As part of the training the management body must understand 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. In addition, the following subjects are important:

- Digitization and growing dependence on ICT (part 1 of DORA announcement)
- Development and Increasing Threat Landscape (Part 48 of DORA Announcement)
- Increasing legislation and regulations (part 16 of the DORA announcement)
- Digital Operational Strategy and the impact of the important or critical functions on this strategy (art 5.2d and art 13 paragraph 4)
- ICT Risk Management (art 5.2a)
- Budgets & Resources (Article 5(2)(g))

- Continued attention (monitoring) and reporting, including KPIs (Article 6 paragraph 5)
- Creating a risk & security aware culture (Tone at the top) (art 5 paragraph 2 g)

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 internal risks, but also about external threats that can affect the organization. The training courses must be specifically tailored to the situation of the entity and are therefore flexible, depending on the nature and needs of the organization. This means that the content of the training courses can vary periodically.

5. Types of training

Article 5.4 cited in chapter 3 above, mentions that the members of the management body must actively keep themselves up to date with sufficient knowledge. This implies that the training cannot be only an initial and one-time 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 DORA. This training is particularly important during the implementation of DORA and during management changes, when a solid basic knowledge is essential. Also think of this initial training when a new board member or director joins. For this initial training we suggest to cover all 8 domains of the training schedule presented in chapter 9.
- Recurring training, to ensure that knowledge level of the management body remains up-to-date. For recurring trainings, the domains of the training schedule presented in chapter 9 can be selected that have undergone (significant) changes within the institution that justifies training the management body on.

6. 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

We recommend a combination and variation of the above. For example, in Continuity Management, we recommend a crisis simulation exercise based on a cyber-attack, such as ransomware.

Depending on the risk, size of the organization, maturity and threat levels, the frequency of the training courses may differ (article 4), with a minimum frequency of once a year.

Institutions are also free to use Permanent Education sessions in addition or as a substitution for some of the themes.

7. Relation to NIS2

In October 2024 the NIS2 directive (Directive (EU) 2022/2555) came into effect. The NIS2 Directive and DORA are both legislative measures by the European Union aimed at the same objective: enhancing cybersecurity and operational resilience within the region, but they focus on different sectors and have distinct scopes. NIS2 applies broadly to essential and important entities across various sectors, including 3 types of financial institutions[4], whereas DORA is specifically tailored for financial institutions. Together, they contribute to a more cohesive and comprehensive EU cybersecurity strategy.

Like DORA, the NIS2 directive also includes an article (article 20) on training for the members of the management bodies. As such, organizations in scope of NIS2 can benefit from the training schedule presented in chapter 9 as well.

NIS2 only: additional training requirements

In the Netherlands, the NIS2 Directive has been transposed to the Dutch implementation law called the Cyberbeveiligingswet (Cbw). The Cyberbeveiligingswet additionally has been further elaborated in the Cyberbeveiligingsbesluit (Cbb).

The Cbb includes specific requirements regarding:

- The trainer: Article 22 stipulates that the trainer must be independent and qualified. The required independence means that the training cannot be given by a person who is responsible for the security of network and information systems within the relevant essential entity or significant entity. It is possible that a person with such responsibilities, such as a chief information security officer (CISO), is present at a training course to provide clarification on specific context of the essential entity or significant entity.
  Additionally, the trainer will have:
    a) demonstrable experience of best practices in network and information security;
    b) knowledge of national, European and international standards in network and information security;
    c) knowledge of possible measures and solutions to risks as referred to in Article 20; and
    d) knowledge of network and information security issues at strategic and tactical levels
- Certification: The Cbb emphasizes that the training should be concluded with a certificate of participation. The certificate must include at least:

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

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 number of hours the training was attended;
d) the topics covered in the training; and
e) the name of the training provider.

Important to note is that the above 2 requirements are not applicable for institutions in scope of DORA only.

8. Introduction to the Boardroom training objectives

Although it is not new that the boardroom is in the end responsible for everything, the requirement of personal involvement is new. In general the reflex of the boardroom is to delegate tasks and mandate other people. Those become responsible to execute certain tasks and the boardroom stays at a strategic level. With regard to cybersecurity, the boardroom often delegates the responsibility to the CIO and/or CISO. However, with the changed requirements, the board must be more directly involved in steering and making choices regarding cybersecurity.

The exact role of the boardroom depends on many factors however both the DORA and NIS2 have set out certain minimum requirements.

For 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 third-party service providers management policy
- 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

In the table below, which can be used as a library of inspiration for the boardroom, a distinction has been made between knowledge objectives and responsibility objectives. **Knowledge objectives** focus on what board members need to understand, such as the organizations ICT risk management framework, and how cybersecurity

aligns with business strategy. This 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 obligated to fulfil, such as overseeing risk management frameworks, ensuring compliance, and fostering a culture of accountability. By delineating these two categories, organizations can better structure boardroom training and ensure alignment with regulatory demands and best practices for cyber resilience. This distinction also reinforces the board's dual role as both learners and leaders in navigating today's complex digital landscape.

In chapter 9, we present the knowledge training objectives and responsibilities for the management body under DORA 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 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 CSR Cybersecurity Guideline for Directors
- Typically the Responsibility of the Management Body: Clarifies the expected roles of the management body for each domain, reinforcing accountability

9. The DORA Boardroom training objectives

Domain	Knowledge objectives	Responsibility objectives	Mapping to practical questions for improved boardroom dialogue based on the factsheet from the NCSC[5] and CSR[6]	Typically the responsibility of the management body?
1.Governance & Risk Management	• Understand the collective and individual role and accountability of the Management Body members • Being able to contribute to the definition of the organization's risk appetite and risk tolerance level • Understanding the organisation's critical functions and their dependency on ICT services • Understanding the organisation's ICT risk management framework and the risk cycle (plan, do, check and act) • Understand the expectations of the Digital Operational Resilience Strategy (DORA or NIS2 specific) or IT security strategy	• Carry out the management body responsibility for digital resilience and updating the ICT risk framework 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 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 or NIS2 specific) or IT security strategy.	NCSC: • What are the most pressing issues I need to focus on? • What do you 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 it joins 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 the main issues and outcomes of the risk assessments carried out?	Yes

[5] https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/besturen/vragen-voor-bestuurder-aan-ciso
[6] Handreiking cybersecurity voor bestuurders en bedrijfseigenaren of the CSR will be published soon on https://www.cybersecurityraad.nl

Domain	Knowledge objectives	Responsibility objectives	Mapping to practical questions for improved boardroom dialogue based on the factsheet from the NCSC[5] and CSR[6]	Typically the responsibility of the management body?
	• Being able to understand and approve the most important controls and policies • Understand the need for transparent cyber reporting to and active oversight by the Management Body	• Implement appropriate CISO reporting line, autonomy, reporting frequency, in person attendance etc. • Decide on proper governance documentation regarding reporting and decision making.	• What are our biggest risks and threats and do we have sufficient control over them? • Which of these risks are incidental and/or structural? • How do we identify and calculate the probability and impact and distinguish between the different types of risks and what role do I play in them? • What residual risks are there? Are these acceptable? • Have the residual risks been discussed with the supervisory authorities?	
2.Operational management	• Understanding the importance of asset inventory • Understanding key principles of resilient systems • Understanding key controls and the possible impact of gaps	• Assess business risk of critical IT applications, underlying components and key dependencies • Assess impact of threats, gaps in controls and fallback options. • Provide direction on improvement actions, priorities and timelines	NCSC: • What are our key assets and processes? CSR: • Do we have an actual inventory of our ICT systems? Do we have shadow ICT systems or legacy systems?	Yes
3.Continuity management	• Understanding the business continuity policy and the response & recovery plans • Understanding the media management, crisis organization and communication plan • Understanding the quick decision making role of the management body during severe attacks or disruptions	• Knowing, and periodically challenging the measures for the resilience of critical functions under duress or disruptions • Stewardship in NO-IT scenario's and capacity to carry out agreed measures and responsibilities. • Practicing 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, what do these look like?	Yes

Domain	Knowledge objectives	Responsibility objectives	Mapping to practical questions for improved boardroom dialogue based on the factsheet from the NCSC[5] and CSR[6]	Typically the responsibility of the management body?
	• Understanding the different types of back-up and recovery strategies			
4.Incident management	• Understanding the key aspects of the incident management policy and escalation paths. • Understanding classification and reporting of incidents • Knowing the most important stakeholders and their roles in the event of a major incident.	• Knowing the DORA and NIS2 specific major incident reporting timelines (if relevant also SEC) • Knowing how to report major incidents to the supervisory authorities in the different regions • Capacity to lead the technical incident response and participate in the strategic response to major incidents	CSR: • Do we have an incident response plan? • Are we, as a company and as the board, (sufficiently) insured against cyber risks?	No
5.Software and systems development	• Understanding the key aspects of the software and systems development policy	• Understanding most critical aspects regarding testing systems • Understanding how well the required tests are performing	N/A	No
6.Third-party Risk management	• Understanding 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 • Understanding 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	• Knowing the critical third-party providers of the institution and oversee their periodic evaluation whether the strategy still fits • Knowing the impact of changes in the chain of critical subcontractors • Knowing the level of compliance to the required security and contractual requirements of the critical third-party providers of the institution • Having insight in involvement of the critical third-party providers of	NCSC: • Which third parties do we use? CSR: • Do we know the dependencies of ICT suppliers and do we control the involved risks?	Yes

Domain	Knowledge objectives	Responsibility objectives	Mapping to practical questions for improved boardroom dialogue based on the factsheet from the NCSC[5] and CSR[6]	Typically the responsibility of the management body?
	• Expectations of the Register of Information (DORA specific) • Understanding 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, avoidance of vendor lock-in, strategic autonomy	the institution in continuity tests, resilience tests (TLPT in DORA), security awareness campaigns etc.		
7.Resilience testing	• Understanding the purpose of the different types of digital operational resilience testing, such as Red Teaming and TLPT (DORA specific)	• Understanding 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, knowing the results and improvements identified in the test	CSR: • Do we perform resilience tests?	No
8.Security management	• Understanding the most important risk mitigation measures[7] • Having insight in most relevant attack vectors in the domain of the institution. Knowledge of the different types of risks involved in network and information	• Understanding how security is organized in the institution and how reporting occurs • Oversee the implementation status and coverage of the most critical security measures of the institutions	NCSC: • As an organization, do we have a cybersecurity strategy? If so, what does it look like? • To what extent is there a positive security culture within the organization? • What level of knowledge is required within the rest of the organization?	Yes

[7] See also chapter 5 with key controls in Handreiking cybersecurity voor bestuurders en bedrijfseigenaren of the CSR (published soon) on https://www.cybersecurityraad.nl

Domain	Knowledge objectives	Responsibility objectives	Mapping to practical questions for improved boardroom dialogue based on the factsheet from the NCSC[5] and CSR[6]	Typically the responsibility of the management body?
	systems, such as the threat of malware, insider threat and DDoS attacks that pose a risk to integrity and availability (specifically for NIS2) • Understanding the monitoring of the most critical cyber security risks • Insight into the cyber threat profile of the institution and possible impact of cyber-attacks on the organization • Insight in important social engineering measures, such as Spoofing, Phishing, Inserting subversive individuals into organizations and interpersonal manipulations, Quishing (QR phishing).	• Implement cyber hygiene for yourself, give the good example by complying with the organisation's policies and convey cybersecure tone at the top	• 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? • Do we have a plan for the situation that ICT does not work anymore? (fallback) • Do we know the dependencies of ICT-suppliers and do we control the involved risks? CSR: • 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?	

10. Conclusion

In essence, the Digital Operational Resilience Act (DORA) mandates not only a robust risk management framework but also fosters a culture of continuous learning and awareness among the management body and all employees of financial institutions. This continuous education is pivotal in equipping them with the necessary skills and knowledge to manage digital risks effectively and fortify the organization against the ever-evolving landscape of cyber threats.

To meet DORA's requirements, the management body must transcend traditional oversight roles and engage actively in the digital resilience process. Their involvement goes beyond participation, it demands a commitment to regularly update and expand their digital competencies, enabling them to effectively identify, evaluate, and mitigate potential threats. Moreover, this proactivity ensures they remain well-prepared to tackle future incidents and emerging digital challenges with agility and confidence.

Furthermore, the call for continuous learning within DORA underscores the importance of embedding digital resilience into the organizational ethos. By prioritizing ongoing training programs, financial institutions can create an environment where preparedness against cyber threats is ingrained in their operational strategy, driving both individual and collective accountability across all levels. This holistic approach not only enhances the institution’s resilience but also solidifies its reputation in the financial sector as a leader in managing digital risks responsibly.

Ultimately, DORA acts as both a catalyst and a framework for the management body to lead the charge towards a resilient future, ensuring their organizations not only comply with regulatory expectations but also thrive in an increasingly digital world.