Comprehensive Guide to the DORA Regulation

Advisera

Table of Contents

1. Overview of DORA EU regulation

1.1. DORA regulation summary

DORA is a European Union regulation that specifies cybersecurity and resilience requirements for financial organizations.

Its full name is “Regulation (EU) 2022/2554 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011,” and it was published on 14 December 2022.

Since DORA is a regulation, this means that it directly applies to practically any financial entity in the European Union — in other words, EU Member States do not need to publish their own regulations on cybersecurity for the financial sector, since financial organizations must comply directly with DORA.

The “DORA” abbreviation stands for “Digital Operational Resilience Act.”

1.2. Why is DORA important?

DORA is important because it introduces the same level of cybersecurity and digital resilience to all financial entities in all EU countries — this way, cybersecurity and continuity of banks, insurance companies, and other financial organizations will be the same across all EU countries.

1.3. Where can I find the full text of DORA?

Here is the official text of DORA: https://eur-lex.europa.eu/eli/reg/2022/2554/oj

You can also find the full text here, arranged by chapters and articles, and with the ability to search by keyword: Full Text of DORA Regulation.

1.4. How is DORA structured?

The DORA regulation has 64 articles structured in the following nine chapters:

- Chapter I - General provisions
- Chapter II - ICT risk management
- Chapter III - ICT-related incident management, classification and reporting
- Chapter IV - Digital operational resilience testing
- Chapter V - Managing of ICT third-party risk
- Chapter VI - Information-sharing arrangements
- Chapter VII - Competent authorities
- Chapter VIII - Delegated acts
- Chapter IX - Transitional and final provisions

1.5. DORA regulation timeline

DORA was published in December 2022, and it applies starting January 17, 2025.

This means that all financial organizations and their IT suppliers must be compliant from January 2025.

2. Who must comply with the DORA regulation?

Since DORA is a regulation focused on financial entities, it is expected that all kinds of financial organizations need to be compliant with it.

But what is interesting is that smaller financial organizations have to comply with different parts of DORA compared to other financial entities, and even more interesting is that IT companies that provide their services to financial organizations need to be compliant as well.

2.1. Which financial organizations must comply with DORA?

In its Article 2, DORA specifies that it applies to almost all financial entities in all EU countries:

- credit institutions
- payment institutions
- account information service providers
- electronic money institutions
- investment firms
- crypto-asset service providers
- central securities depositories
- central counterparties
- trading venues
- trade repositories
- managers of alternative investment funds
- management companies
- data reporting service providers
- insurance and reinsurance undertakings
- insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries
- institutions for occupational retirement provision
- credit rating agencies
- administrators of critical benchmarks
- crowdfunding service providers
- securitisation repositories

However, there are differences between what smaller financial organizations need to comply with when compared to other financial organizations.

2.2. Smaller vs. other financial organizations in DORA

Out of the financial organizations listed above, the following sub-groups have a little bit easier job of complying with DORA:

- small and non-interconnected investment firms
- small payment institutions exempted by the decision of Member States according to Directive (EU) 2015/2366
- specific credit institutions defined in Directive 2013/36/EU (if Member States did not exclude them completely from DORA)

- small electronic money institutions exempted by the decision of Member States according to Directive 2009/110/EC
- small institutions for occupational retirement provision.

These smaller organizations must comply with the "simplified ICT risk management framework" that is specified in DORA's Article 16 and in TITLE III of CDR 2024-1774 Technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework. In other words, these smaller financial entities do not need to comply with the whole Chapter II ICT risk management like the other financial organizations.

However, smaller financial organizations must comply with other parts of DORA in the same way as all the other organizations.

2.3. ICT third-party service providers

IT companies that provide services to financial organizations in the European Union must comply with requirements specified in Chapter V Managing of ICT third-party risk.

In particular, all IT service providers must be compliant with security standards, and follow specific contractual obligations; however, if a service provider is designated as critical, then the requirements are much stricter.

See sections below to find out which IT companies need to comply with DORA, and how.

3. Nine key requirements specified in the DORA regulation

The DORA regulation is quite lengthy: 106 preamble items and 64 articles, altogether 79 pages — it would probably take you a couple of days (if not weeks) to read it through. To save you some reading time, the text below summarizes the most important points from DORA.

Please keep in mind these are requirements from the point of view of financial organizations and their IT suppliers that need to comply with DORA, not from the viewpoint of competent authorities (i.e., government bodies in charge of enforcing this regulation).

3.1. Very detailed requirements for ICT risk management

The requirements for ICT risk management are described in DORA's Chapter II, and in CDR 2024/1774 Regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework; altogether 54 articles in 42 pages — a lot to take in.

DORA has structured the ICT risk management requirements in the following way:

- Governance and organisation
- ICT risk management framework
- ICT systems, protocols and tools
- Identification
- Protection and prevention
- Detection
- Response and recovery
- Backup policies and procedures, restoration and recovery procedures and methods
- Learning and evolving
- Communication

3.2. Simplified ICT risk management framework for smaller financial entities

The ICT risk management requirements specified above would probably be overwhelming for smaller financial organizations, which is why DORA has specified a "lighter" version of ICT risk management for such entities.

This simplified ICT risk management framework is specified in DORA's Article 16 and in Title III of CDR 2024/1774 Regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework.

The simplified framework follows a very similar structure to the "regular" ICT risk management specified in DORA's Chapter II, with the main difference being that the requirements are not as detailed nor as strict.

3.3. Incident & threat classification and reporting

DORA dedicates the whole of chapter Chapter III to management, classification, and reporting of incidents and threats. It requires setting up an incident management process, defines criteria for classifying incidents and threats, and defines how they need to be reported.

Similar to requirements in NIS 2, financial entities need to submit the following incident reports to competent authorities: initial notification, intermediate report, and a final report; further, they need to inform them about significant cyber threats. Financial organizations also need to inform their clients of any major ICT-related incidents or significant cyber threats.

3.4. Testing of digital operational resilience, including penetration testing

In its Chapter IV, DORA requires financial entities to execute a digital operational resilience testing program that includes "a range of assessments, tests, methodologies, practices and tools."

The tests need to be performed at least once a year on all ICT systems supporting critical or important functions. According to Article 25, those tests could include "vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing."

Article 26 introduces the concept of Threat-Led Penetration Testing (TLPT) that needs to be carried out at least once every three years, and provides detailed rules for such testing.

3.5. Managing risks related to ICT third-party providers

DORA specifies very strict rules on how financial entities need to handle their IT providers, in order to reduce third-party risks. Those rules include adopting a strategy on ICT third-party risk and a policy on the use of ICT services, regular review of third-party risks, and preparing an exit strategy (Article 28).

Further, financial entities must perform preliminary assessment of an IT supplier before starting to use their products and services (Article 29) and make sure they comply with information security standards.

Finally, in its article (Article 30), DORA specifies minimum contractual clauses that need to be included in agreements with ICT third-party providers.

3.6. Requirements for ICT service providers and their oversight by the government

ICT third-party providers that provide their services to financial organizations need to comply with security standards, and with specific contractual requirements. If those service providers are designated as critical, then there are a lot more requirements they have to comply with.

European Supervisory Authorities (ESAs) will appoint a Lead Overseer for each ICT third-party provider that is classified as critical. According to Article 33, the purpose of the Lead Overseer is to continually assess whether such an IT provider has in place "comprehensive,

sound and effective rules, procedures, mechanisms and arrangements to manage the ICT risk which it may pose to financial entities."

Lead Overseers have the right of full access to any information from ICT third-party providers, and they can conduct investigations and issue recommendations, as well as enforce fines and other penalties.

3.7. Sharing information on cyber threats

Although Chapter VI is the shortest chapter in DORA, it might introduce quite big changes in how threat intelligence is handled.

It specifies the baseline for exchange of cyber threat information and intelligence, and the role of competent authorities and IT service providers.

3.8. Government bodies (competent authorities) in charge of enforcing DORA

According to regulations referenced in Article 46, for the majority of financial entities that need to be compliant with DORA, EU Member States designate competent authorities that supervise and enforce financial regulations.

There are a couple of exceptions, where EU authorities directly supervise and enforce financial regulations:

- For credit institutions classified as significant - the European Central Bank (ECB)
- For securitisation repositories - the European Securities and Markets Authority (ESMA)

3.9. Penalties for financial organizations and ICT third-party providers

For financial entities, DORA does not specify minimum fines — rather, it gives the freedom to Member States to define their own fines in their countries. It does, however, specify other penalties that can be enacted by competent authorities, including giving orders to stop activities not compliant with DORA, defining any measures to make sure entities are compliant with DORA, and issuing public notices.

For critical ICT third-party service providers, DORA specifies a fine of up to 1% of their worldwide annual turnover. Further, the Lead Overseer (the body that supervises critical service providers) must issue public notice that reveals the name of the service provider that was fined.

Finally, a competent authority overseeing a financial organization using the services of a third-party service provider that is not compliant with DORA can order this financial organization to stop using those services.

4. 18 steps to comply with DORA requirements

If your financial organization needs to comply with the DORA regulation, you need a comprehensive approach to make sure you comply with all the requirements. The steps in the text below present the best practice to cover all of those complex requirements.

From our experience, the following 18 steps will enable you to comply with DORA efficiently. Before reading the steps, a couple of important notes:

- The steps below are designed for financial organizations, whereas for IT companies that need to comply with DORA, see section "Which IT companies need to comply with DORA, and how?"
- In its Article 16, DORA specifies special rules for smaller financial organizations called the "simplified ICT risk management framework" — nevertheless, even for such smaller organizations, the 18 steps listed below are valid, the only difference being that the requirements might be somewhat less strict. See which financial entities qualify for simplified risk management in the section "Who must comply with the DORA regulation?"

4.1. Start with a gap analysis

First, since your financial entity probably already does comply with many DORA requirements, it is useful to find out what are you missing.

Once you know your gap, you can decide which of the following steps are applicable to you.

4.2. Obtain senior management support

Even though compliance with DORA is mandatory, you still might have problems with implementing various aspects of it — this is why it is important to have formal approval from the top management for the project, together with enough time, people, and budget to implement it.

This way, you will be able to overcome most of the problems that you will face during the project.

4.3. Set up project management

To make your project run more smoothly, you need to define:

- Responsibilities — who is in charge (project manager), who from the senior management will help you if you get stuck (project sponsor), and with whom from the mid-level management you need to cooperate the most (project team). If you already have a security committee, this might serve as your project team.
- Milestones — define the major steps in your project, and their timing.
- Project outcomes — define exactly what kinds of documents, activities, and other things will be produced during the project.

4.4. Perform initial training

Since DORA and its related Commission Delegated Regulations are quite complex, you should train the project team at the very early stage of the project. In the beginning, it

makes sense to start with introductory topics on DORA, and later on focus on specific DORA requirements.

This way, you will have a knowledgeable team of people that will execute the project in a much more efficient way.

4.5. Define governance and senior management's role

In its Article 5, DORA is quite specific regarding the responsibilities of the senior management, and how to set up the governance of ICT risks. This includes setting up policies, roles, and responsibilities; approving the strategy, audit plans, and budget; setting up reporting channels, etc.

Such governance is the foundation upon which the ICT risk management is built.

4.6. Set up the ICT risk management framework

Article 6 specifies what the risk management framework looks like — according to it, you need to establish appropriate "... strategies, policies, procedures, ICT protocols and tools that are necessary to duly and adequately protect all information assets and ICT assets."

This kind of documented framework will enable you to perform the next steps, starting with risk assessment and treatment.

4.7. Perform asset identification, risk assessment, and treatment

In its Article 8, DORA requires financial organizations to "identify, classify and adequately document all ICT supported business functions, roles and responsibilities, the information assets and ICT assets supporting those functions, and their roles and dependencies," and, on top of this, to identify threats, vulnerabilities, and risks.

Further, it requires classifying those assets that are considered critical, and identifying if ICT third-party service providers support any critical or important functions.

This kind of analysis is important to decide which cybersecurity measures need to be implemented.

4.8. Write and approve the digital operational resilience strategy

Article 8(6) requires a comprehensive document to be written, called the digital operational resilience strategy — it must include several elements, including how the risk management framework supports business strategy and objectives, risk tolerance level, and security objectives, and it needs to explain how the risk management framework needs to be implemented.

This is a crucial step because it sets in motion the implementation of concrete cybersecurity and resilience measures.

4.9. Implement cybersecurity measures

Articles 9 and 10 specify various cybersecurity measures that must be implemented, including network management, access control, authentication, change management, patches and updates, detection of anomalous activities, etc.

These will probably take the longest time to implement, but this is, in fact, the core of cybersecurity.

4.10. Implement resilience measures

Articles 11 and 12 are oriented towards business continuity, and include a top-level ICT business continuity policy, business impact analysis (BIA), response and recovery plans, crisis management and communication, and testing, but also backup and restoration.

These measures are a bit more abstract than the cybersecurity measures from the previous step, but are nevertheless equally important, especially when a financial organization needs to deal with larger incidents.

4.11. Set up risk management for ICT third-party risk

DORA dedicates Articles 28 to 30 to how to handle IT companies that provide their services to financial organizations. This includes assessing the risks related to a particular IT provider, specific contractual obligations, defining the exit strategy, etc.

DORA recognizes that managing supply chain risk is of greatest importance, because it introduces a government oversight of critical IT service providers, although financial organizations are not directly impacted by such oversight.

4.12. Set up regular cybersecurity training

Articles 5, 13, and 16 require financial organizations to set up regular training and awareness for all employees, including the senior management. Articles 13 and 30 go a step further, and require financial entities to "include ICT third-party service providers in their relevant training schemes."

This step is pretty obvious — with all these complex rules and requirements, it would be hard to expect that people would follow them without being trained and aware.

4.13. Set up incident & threat classification and reporting

Articles 17 to 19 require financial organizations to "define, establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents," including their classification and reporting to authorities.

Despite all the (preventive) cybersecurity measures, it will be impossible to avoid every incident — this is why the response to them needs to be effective, and all interested parties need to be informed.

4.14. Set up regular digital operational resilience testing

The whole Chapter IV is dedicated to digital operational resilience testing and requires "the execution of appropriate tests, such as vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing," "for the purpose of assessing preparedness for handling ICT-related incidents, of identifying weaknesses, deficiencies and gaps in digital operational resilience, and of promptly implementing corrective measures." This also includes the "Threat-Led Penetration Testing."

This kind of testing is crucial in order to find out what the real situation is. The internal audit explained in step #16 has a similar purpose, but is done in a different way.

4.15. Set up measurement, monitoring, and reviews

It is impossible to manage anything, let alone cybersecurity and resilience in a financial entity, if you're not informed about its performance. This is why Article 13 requires several types of reports and information to reach appropriate managers, including post-incident reviews, lessons from operational testing, effectiveness of the implementation of the digital operational resilience strategy, technological developments, etc.

This way, the management can react quickly and appropriately to any trend or risk.

4.16. Conduct periodic internal audits

Articles 5 and 6 require financial entities to perform regular internal audits by auditors that have enough independence, and "sufficient knowledge, skills and expertise in ICT risk."

Such audits are crucial to find out what the reality is in a company, because very often policies and procedures define one thing, but in reality employees might be doing something very different.

4.17. Conduct periodic management review

Article 5 specifies several review activities that need to be performed regularly by the senior management — these include reviewing the business continuity policy, response and recovery plans, policy for the use of third-party ICT services, various reports, internal audits, digital resilience budget, etc.

Such reviews are crucial, because this is how the senior management is informed about key risks and activities related to cybersecurity and resilience.

4.18. Execute follow-up actions and corrective measures

Follow-up actions and corrective measures are mentioned in different contexts in DORA — e.g., Article 6 requires a follow-up process after an internal audit, Article 17 requires a follow-up after incidents, Article 24 requires corrective measures after digital operational resilience testing, while Article 30 requires corrective actions to be included in the contracts with IT suppliers.

All of these are crucial for ICT risk management to be continually improved and, consequently, digital operational resilience to be raised to a better level.

5. List of documents required by the DORA regulation

The DORA regulation is pretty specific on what needs to be implemented in order to ensure cybersecurity and resilience of IT systems. The problem is that there are many requirements, and it is hard to conclude what needs to be covered with which documents.

The table below maps each relevant requirement from DORA with documents that are the best suited to cover those requirements.

5.1. DORA requirements and related documents

Before you start reading the list below, a couple of notes:

* "Smaller" financial organizations are the following entities (these are the ones that must go for the simplified ICT risk management framework according to DORA Article 16):

- small and non-interconnected investment firms
- small payment institutions exempted by the decision of Member States according to Directive (EU) 2015/2366
- specific credit institutions defined in Directive 2013/36/EU (if Member States did not exclude them completely from DORA)
- small electronic money institutions exempted by the decision of Member States according to Directive 2009/110/EC
- small institutions for occupational retirement provision.

** "Microenterprises" are those financial entities that employ fewer than 10 persons and have an annual turnover and/or annual balance sheet total that does not exceed 2 million euros.

Requirements	References	Which financial entities	Usually documented through
Set clear roles and responsibilities for all ICT-related functions	DORA Article 5(2)(c) CDR 2024/1774 Title II	All except smaller*	Each document listed in this column must define clear roles and responsibilities for all specified activities
Establish appropriate governance arrangements	DORA Article 5(2)(c) CDR 2024/1774 Title II	All except smaller	ICT Risk Management Policy + all documents listed in this column
Set and approve digital operational resilience strategy; the ICT risk management framework shall include a digital operational resilience strategy setting out how the framework shall be implemented, and shall include methods to address ICT risk and attain specific ICT objectives	DORA Article 5(2)(d); Article 6(8) CDR 2024/1774 Title II	All except smaller	Digital Operational Resilience Strategy

Requirements	References	Which financial entities	Usually documented through
Approve, oversee and periodically review the implementation of ICT business continuity policy	DORA Article 5(2)(e) CDR 2024/1774 Title II	All except smaller	Business Continuity Policy
Approve, oversee and periodically review the implementation of ICT response and recovery plans	DORA Article 5(2)(e) CDR 2024/1774 Title II	All except smaller	Incident Response Plan + Activity Recovery Plan + Disaster Recovery Plan
Approve and periodically review ICT internal audit plan	DORA Article 5(2)(f) CDR 2024/1774 Title II	All except smaller	Internal Audit Program
Allocate and periodically review the appropriate budget	DORA Article 5(2)(g) CDR 2024/1774 Title II	All except smaller	Digital Operational Resilience Strategy
Approve and periodically review policy on arrangements regarding the use of ICT services provided by ICT third-party service providers	DORA Article 5(2)(h) CDR 2024/1774 Title II	All except smaller	Supplier Security Policy
Reporting channels related to ICT third-party service providers: arrangements concluded, planned material changes, and their impact on critical or important functions	DORA Article 5(2)(i) CDR 2024/1774 Title II	All except smaller	Supplier Security Policy
Establish a role in order to monitor the arrangements concluded with ICT third-party service providers on the use of ICT services, or designate a member of senior management as responsible for overseeing the related risk exposure	DORA Article 5(3) CDR 2024/1774 Title II	All except smaller and microenterprises**	ICT Risk Management Policy + Supplier Security Policy
Members of the management body of the financial entity must actively keep up to date with sufficient knowledge and skills to understand and assess ICT risk and its impact on the operations	DORA Article 5(4) CDR 2024/1774 Title II	All except smaller	Security Policy for Human Resources + Training and Awareness Plan

Requirements	References	Which financial entities	Usually documented through
The ICT risk management framework shall include at least strategies, policies, procedures, ICT protocols and tools that are necessary to duly and adequately protect all information assets and ICT assets	DORA Article 6(2) CDR 2024/1774 Title II	All except smaller	ICT Risk Management Policy + all documents listed in this column
Minimise the impact of ICT risk by deploying appropriate strategies, policies, procedures, ICT protocols and tools	DORA Article 6(3) CDR 2024/1774 Title II	All except smaller	ICT Risk Management Policy + all documents listed in this column
Assign the responsibility for managing and overseeing ICT risk to a control function	DORA Article 6(4) CDR 2024/1774 Title II	All except smaller and microenterprises	ICT Risk Management Policy
Ensure appropriate segregation and independence of ICT risk management functions, control functions, and internal audit functions	DORA Article 6(4) CDR 2024/1774 Title II	All except smaller	ICT Risk Management Policy
The ICT risk management framework shall be documented and reviewed	DORA Article 6(5) CDR 2024/1774 Title II	All except smaller	ICT Risk Management Policy
The ICT risk management framework shall be subject to internal audit by auditors on a regular basis	DORA Article 6(6) CDR 2024/1774 Title II	All except smaller and microenterprises	ICT Risk Management Policy + Internal Audit Procedure
Internal auditors shall possess sufficient knowledge, skills and expertise in ICT risk, as well as appropriate independence	DORA Article 6(6) CDR 2024/1774 Title II	All except smaller and microenterprises	Internal Audit Procedure
Establish a formal follow-up process, including rules for the timely verification and remediation of critical ICT audit findings	DORA Article 6(7) CDR 2024/1774 Title II	All except smaller	Internal Audit Procedure + Procedure for Corrective Actions

Requirements	References	Which financial entities	Usually documented through
Identify, classify and adequately document all ICT supported business functions, roles and responsibilities, the information assets and ICT assets supporting those functions, and their roles and dependencies in relation to ICT risk	DORA Article 8(1) CDR 2024/1774 Title II	All except smaller	Asset Management Procedure + IT Asset Register
On a continuous basis, identify all sources of ICT risk, in particular the risk exposure to and from other financial entities, and assess cyber threats and ICT vulnerabilities relevant to their ICT supported business functions, information assets and ICT assets	DORA Article 8(2) CDR 2024/1774 Title II	All except smaller	Risk Management Methodology + Risk Assessment Table / Risk Register
Review on a regular basis, and at least yearly, the risk scenarios impacting them.	DORA Article 8(2) CDR 2024/1774 Title II	All except smaller	Risk Management Methodology + Risk Assessment Table / Risk Register
Perform a risk assessment upon each major change in the network and information system infrastructure, in the processes or procedures affecting their ICT supported business functions, information assets or ICT assets	DORA Article 8(3) CDR 2024/1774 Title II	All except smaller and microenterprises	Risk Management Methodology + Risk Assessment Table / Risk Register
Identify all information assets and ICT assets, including those on remote sites, network resources and hardware equipment, and map those considered critical	DORA Article 8(4) CDR 2024/1774 Title II	All except smaller	Asset Management Procedure + IT Asset Register
Map the configuration of the information assets and ICT assets and the links and interdependencies between the different information assets and ICT assets	DORA Article 8(4) CDR 2024/1774 Title II	All except smaller	Asset Management Procedure + IT Asset Register
Identify and document all processes that are dependent on ICT third-party service providers, and identify interconnections with ICT third-party service providers that provide services that support critical or important functions	DORA Article 8(5) CDR 2024/1774 Title II	All except smaller	Asset Management Procedure + IT Asset Register

Requirements	References	Which financial entities	Usually documented through
For the purposes of paragraphs 1, 4 and 5 of Article 8, maintain relevant inventories and update them periodically and every time any major change as referred to in paragraph 3 occurs	DORA Article 8(6) CDR 2024/1774 Title II	All except smaller	Asset Management Procedure + IT Asset Register
On a regular basis, and at least yearly, conduct a specific ICT risk assessment on all legacy ICT systems and, in any case before and after connecting technologies, applications or systems	DORA Article 8(7) CDR 2024/1774 Title II	All except smaller and microenterprises	Risk Management Methodology + Risk Assessment Table / Risk Register
Continuously monitor and control the security and functioning of ICT systems and tools	DORA Article 9(1) CDR 2024/1774 Title II	All except smaller	Monitoring Procedure
Design, procure and implement ICT security policies, procedures, protocols and tools that aim to ensure the resilience, continuity and availability of ICT systems, in particular for those supporting critical or important functions	DORA Article 9(2) CDR 2024/1774 Title II	All except smaller	ICT Risk Management Policy + all documents listed in this column
Develop and document an information security policy defining rules to protect the availability, authenticity, integrity and confidentiality of data, information assets and ICT assets, including those of their customers	DORA Article 9(4)(a) CDR 2024/1774 Title II	All except smaller	ICT Risk Management Policy
Establish a sound network and infrastructure management structure using appropriate techniques, methods and protocols; design the network connection infrastructure in a way that allows it to be instantaneously severed or segmented in order to minimise and prevent contagion, especially for interconnected financial processes	DORA Article 9(4)(b) CDR 2024/1774 Title II	All except smaller	Network Security Policy
Implement policies that limit the physical or logical access to information assets and ICT assets, and establish to that end a set of policies, procedures and controls that address access rights and ensure a sound administration thereof	DORA Article 9(4)(c) CDR 2024/1774 Title II	All except smaller	Access Control Policy

Requirements	References	Which financial entities	Usually documented through
Implement policies and protocols for strong authentication mechanisms	DORA Article 9(4)(d) CDR 2024/1774 Title II	All except smaller	Authentication Policy
Implement documented policies, procedures and controls for ICT change management; the ICT change management process shall be approved by appropriate lines of management and shall have specific protocols in place	DORA Article 9(4)(e) CDR 2024/1774 Title II	All except smaller	Change Management Policy
Have appropriate and comprehensive documented policies for patches and updates	DORA Article 9(4)(f) CDR 2024/1774 Title II	All except smaller	Patch Management Policy
Have in place mechanisms to promptly detect anomalous activities, including ICT network performance issues and ICT-related incidents, and to identify potential material single points of failure; all detection mechanisms must be regularly tested	DORA Article 10(1) CDR 2024/1774 Title II	All except smaller	Monitoring Procedure
Detection mechanisms must enable multiple layers of control, define alert thresholds and criteria to trigger and initiate ICT-related incident response processes, including automatic alert mechanisms for relevant staff in charge of ICT-related incident response	DORA Article 10(2) CDR 2024/1774 Title II	All except smaller	Monitoring Procedure
Devote sufficient resources and capabilities to monitor user activity, the occurrence of ICT anomalies and ICT-related incidents, in particular cyber-attacks	DORA Article 10(3) CDR 2024/1774 Title II	All except smaller	Monitoring Procedure
Put in place a comprehensive ICT business continuity policy, which may be adopted as a dedicated specific policy, forming an integral part of the overall business continuity policy	DORA Article 11(1) CDR 2024/1774 Title II	All except smaller	Business Continuity Policy

Requirements	References	Which financial entities	Usually documented through
Implement the ICT business continuity policy through dedicated, appropriate and documented arrangements, plans, procedures and mechanisms aiming to ensure the continuity, quickly, appropriately and effectively respond to, and resolve, all ICT-related incidents	DORA Article 11(2) CDR 2024/1774 Title II	All except smaller	Business Impact Analysis Methodology + Business Continuity Strategy + Crisis Management Plan + Business Continuity Plan + Incident Response Plan + Disaster Recovery Plan + Activity Recovery Plan
Activate, without delay, dedicated plans that enable containment measures, processes and technologies suited to each type of ICT-related incident and prevent further damage, as well as tailored response and recovery procedures	DORA Article 11(2)(c) CDR 2024/1774 Title II	All except smaller	Incident Response Plan
Estimate preliminary impacts, damages and losses	DORA Article 11(2)(d) CDR 2024/1774 Title II	All except smaller	Business Continuity Plan
Set out communication and crisis management actions that ensure that updated information is transmitted to all relevant internal staff and external stakeholders	DORA Article 11(2)(e) CDR 2024/1774 Title II	All except smaller	Crisis Management Plan
Implement ICT response and recovery plans	DORA Article 11(3) CDR 2024/1774 Title II	All except smaller	Incident Response Plan + Disaster Recovery Plan + Activity Recovery Plan
Maintain and periodically test appropriate ICT business continuity plans, notably with regard to critical or important functions outsourced or contracted through arrangements with ICT third-party service providers	DORA Article 11(4) CDR 2024/1774 Title II	All except smaller	Maintenance and Review Plan + Business Continuity Testing and Exercising Plan
Conduct a business impact analysis (BIA) of exposure to severe business disruptions	DORA Article 11(5) CDR 2024/1774 Title II	All except smaller	Business Impact Analysis Methodology + Business Impact Analysis Questionnaire

Requirements	References	Which financial entities	Usually documented through
Test the ICT business continuity plans and the ICT response and recovery plans in relation to ICT systems supporting all functions at least yearly; test the crisis communication plans	DORA Article 11(6) CDR 2024/1774 Title II	All except smaller	Business Continuity Testing and Exercising Plan
Include in the testing plans scenarios of cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity, backups and redundant facilities	DORA Article 11(6) CDR 2024/1774 Title II	All except smaller and microenterprises	Business Continuity Testing and Exercising Plan
Regularly review ICT business continuity policy and ICT response and recovery plans	DORA Article 11(6) CDR 2024/1774 Title II	All except smaller	Maintenance and Review Plan
Have a crisis management function, which, in the event of activation of their ICT business continuity plans or ICT response and recovery plans, must set out clear procedures to manage internal and external crisis communications	DORA Article 11(7) CDR 2024/1774 Title II	All except smaller and microenterprises	Crisis Management Plan
Keep readily accessible records of activities before and during disruption events when their ICT business continuity plans and ICT response and recovery plans are activated	DORA Article 11(8) CDR 2024/1774 Title II	All except smaller	Disaster Recovery Plan + Activity Recovery Plan
Report to the competent authorities an estimation of aggregated annual costs and losses caused by major ICT-related incidents	DORA Article 11(10) CDR 2024/1774 Title II	All except smaller and microenterprises	Incident Management Procedure
Develop and document backup policies and procedures, and restoration and recovery procedures and methods	DORA Article 12(1) CDR 2024/1774 Title II	All except smaller	Backup Policy + Backup and Restoration Procedure
Testing of the backup procedures and restoration and recovery procedures and methods must be undertaken periodically	DORA Article 12(2) CDR 2024/1774 Title II	All except smaller	Backup and Restoration Procedure

Requirements	References	Which financial entities	Usually documented through
When restoring backup data using own systems, use ICT systems that are physically and logically segregated from the source ICT system	DORA Article 12(3) CDR 2024/1774 Title II	All except smaller	Backup and Restoration Procedure
Maintain redundant ICT capacities equipped with resources, capabilities and functions that are adequate to ensure business needs	DORA Article 12(4) CDR 2024/1774 Title II	All except smaller	Business Continuity Strategy
In determining the recovery time and recovery point objectives for each function, take into account whether it is a critical or important function and the potential overall impact on market efficiency	DORA Article 12(6) CDR 2024/1774 Title II	All except smaller	Business Impact Analysis Methodology + Business Continuity Strategy
When recovering from an ICT-related incident, perform necessary checks, including any multiple checks and reconciliations	DORA Article 12(7) CDR 2024/1774 Title II	All except smaller	Incident Management Procedure
Have in place capabilities and staff to gather information on vulnerabilities and cyber threats, ICT-related incidents, in particular cyber-attacks, and analyse the impact they are likely to have	DORA Article 13(1) CDR 2024/1774 Title II	All except smaller	Monitoring Procedure
Put in place post ICT-related incident reviews after a major ICT-related incident disrupts their core activities, analysing the causes of disruption and identifying required improvements to the ICT operations or within the ICT business continuity policy	DORA Article 13(2) CDR 2024/1774 Title II	All except smaller	Incident Management Procedure + Post Incident Review Form + Procedure for Corrective Actions
On a continuous basis incorporate into the ICT risk assessment process lessons derived from the digital operational resilience testing and from real life ICT-related incidents, along with challenges faced upon the activation of ICT business continuity plans and ICT response and recovery plans; senior ICT staff shall report at least yearly to the management body on the findings	DORA Article 13(3); Article 13(5) CDR 2024/1774 Title II	All except smaller	Risk Assessment Methodology + Incident Management Procedure

Requirements	References	Which financial entities	Usually documented through
Monitor the effectiveness of the implementation of their digital operational resilience strategy, map the evolution of ICT risk over time, analyse the frequency, types, magnitude and evolution of ICT-related incidents, in particular cyber-attacks and their patterns, with a view to understanding the level of ICT risk exposure, in particular in relation to critical or important functions, and enhance the cyber maturity and preparedness	DORA Article 13(4) CDR 2024/1774 Title II	All except smaller	Digital Operational Resilience Strategy + Risk Assessment Methodology + ICT Risk Management Policy
Develop ICT security awareness programmes and digital operational resilience training as compulsory modules in their staff training schemes; those programmes and training must be applicable to all employees and to senior management staff, and must have a level of complexity commensurate to the remit of their functions; where appropriate, financial entities must also include ICT third-party service providers in their relevant training schemes	DORA Article 13(6) CDR 2024/1774 Title II	All except smaller	Security Policy for Human Resources + Training and Awareness Plan
Monitor relevant technological developments on a continuous basis, also with a view to understanding the possible impact of the deployment of such new technologies on ICT security requirements and digital operational resilience	DORA Article 13(7) CDR 2024/1774 Title II	All except smaller and microenterprises	ICT Risk Management Policy
Have in place crisis communication plans enabling a responsible disclosure of, at least, major ICT-related incidents or vulnerabilities to clients and counterparts as well as to the public	DORA Article 14(1) CDR 2024/1774 Title II	All except smaller	Crisis Management Plan
Implement communication policies for internal staff and for external stakeholders	DORA Article 14(2) CDR 2024/1774 Title II	All except smaller	Crisis Management Plan
At least one person must be tasked with implementing the communication strategy for ICT-related incidents and fulfil the public and media function for that purpose	DORA Article 14(3) CDR 2024/1774 Title I	All except smaller	Crisis Management Plan

Requirements	References	Which financial entities	Usually documented through
Put in place and maintain a sound and documented ICT risk management framework that details the mechanisms and measures aimed at a quick, efficient and comprehensive management of ICT risk	DORA Article 16(1)(a) CDR 2024/1774 Title III	Only smaller	ICT Risk Management Policy + all documents listed below in this column
Continuously monitor the security and functioning of all ICT systems	DORA Article 16(1)(b) CDR 2024/1774 Title III	Only smaller	Monitoring Procedure
Minimise the impact of ICT risk through the use of sound, resilient and updated ICT systems, protocols and tools	DORA Article 16(1)(c) CDR 2024/1774 Title III	Only smaller	All documents specified for smaller financial organizations
Allow sources of ICT risk and anomalies in the network and information systems to be promptly identified and detected and ICT-related incidents to be swiftly handled	DORA Article 16(1)(d) CDR 2024/1774 Title III	Only smaller	Monitoring Procedure
Identify key dependencies on ICT third-party service providers	DORA Article 16(1)(e) CDR 2024/1774 Title III	Only smaller	Supplier Security Policy + Strategy on ICT third-party risk
Ensure the continuity of critical or important functions, through business continuity plans and response and recovery measures, which include, at least, back-up and restoration measures	DORA Article 16(1)(f) CDR 2024/1774 Title III	Only smaller	Business Continuity Plan + Incident Response Plan + Activity Recovery Plan + Disaster Recovery Plan + Backup and Restoration Procedure
Test, on a regular basis, the plans and measures, as well as the effectiveness of the controls implemented	DORA Article 16(1)(g) CDR 2024/1774 Title III	Only smaller	Business Continuity Testing and Exercising Plan
Implement relevant operational conclusions resulting from the tests and from post-incident analysis into the ICT risk assessment process	DORA Article 16(1)(h) CDR 2024/1774 Title III	Only smaller	Exercising and Testing Report + Corrective Actions

Requirements	References	Which financial entities	Usually documented through
Develop, according to needs and ICT risk profile, ICT security awareness programmes and digital operational resilience training for staff and management	DORA Article 16(1)(h) CDR 2024/1774 Title III	Only smaller	Security Policy for Human Resources + Training and Awareness Plan
The ICT risk management framework must be documented and reviewed periodically and upon the occurrence of major ICT-related incidents, and continuously improved on the basis of lessons derived from implementation and monitoring	DORA Article 16(2) CDR 2024/1774 Title III	Only smaller	Maintenance and Review Plan + Monitoring Procedure + Procedure for Corrective Actions
Define, establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents, including: early warning indicators; procedures to identify, track, log, categorise and classify ICT-related incidents; assign roles and responsibilities; set out plans for communication to staff, external stakeholders and media and for notification to clients, and for internal escalation procedures; ensure that at least major ICT-related incidents are reported to relevant senior management; and establish ICT-related incident response procedures	DORA Article 17(1) and (3)	All	Incident Management Procedure
Record all ICT-related incidents and significant cyber threats	DORA Article 17(2)	All	Incident Management Procedure + Incident & Threat Log
Establish appropriate procedures and processes to ensure a consistent and integrated monitoring, handling and follow-up of ICT-related incidents, to ensure that root causes are identified, documented and addressed in order to prevent the occurrence of such incidents	DORA Article 17(2)	All	Incident Management Procedure + Procedure for Corrective Actions
Classify ICT-related incidents and determine their impact	DORA Article 18(1) CDR 2024/1772	All	Incident Management Procedure
Classify cyber threats as significant based on the criticality of the services at risk	DORA Article 18(2) CDR 2024/1772	All	Incident Management Procedure

Requirements	References	Which financial entities	Usually documented through
Report major ICT-related incidents to the relevant competent authority	DORA Article 19(1)	All	Incident Management Procedure
On a voluntary basis, notify significant cyber threats to the relevant competent authority when the threat is of relevance to the financial system, service users or clients	DORA Article 19(2)	All	Incident Management Procedure
Inform clients about the major ICT-related incident and about the measures that have been taken if a major ICT-related incident occurs and has an impact on the financial interests of clients, financial entities	DORA Article 19(3)	All	Incident Management Procedure
Inform clients that are potentially affected of any appropriate protection measures in the case of a significant cyber threat	DORA Article 19(3)	All	Incident Management Procedure
Submit the following to the relevant competent authority: (a) an initial notification; (b) an intermediate report, followed, as appropriate, by updated notifications every time a relevant status update is available, and (c) a final report	DORA Article 19(4)	All	Incident Initial Notification + Incident Intermediate Report + Incident Final Report
Establish, maintain and review a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk-management framework for the purpose of assessing preparedness for handling ICT-related incidents, of identifying weaknesses, deficiencies and gaps in digital operational resilience, and of promptly implementing corrective measures	DORA Article 24(1)	All except microenterprises	Resilience Testing Program

Requirements	References	Which financial entities	Usually documented through
The digital operational resilience testing programme shall include a range of assessments, tests, methodologies, practices and tools, such as vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing	DORA Article 24(2); Article 25(1)	All	Resilience Testing Program
Ensure that digital operational resilience tests are undertaken by independent parties, whether internal or external	DORA Article 24(4)	All except microenterprises	Resilience Testing Program
Establish procedures and policies to prioritise, classify and remedy all issues revealed throughout the performance of the tests and shall establish internal validation methodologies to ascertain that all identified weaknesses, deficiencies or gaps are fully addressed	DORA Article 24(5)	All except microenterprises	Procedure for Corrective Actions
Ensure that appropriate tests are conducted on all ICT systems and applications supporting critical or important functions, at least yearly	DORA Article 24(6)	All except microenterprises	Resilience Testing Program
Perform the tests by combining a risk-based approach with a strategic planning of ICT testing, by duly considering the need to maintain a balanced approach between the scale of resources and the time to be allocated to the ICT testing and the urgency, type of risk, criticality of information assets and of services provided, as well as any other relevant factor, including the financial entity's ability to take calculated risks	DORA Article 25(3)	Only microenterprises	Resilience Testing Program
Carry out at least every 3 years advanced testing by means of Threat-Led Penetration Testing (TLPT) - cover several or all critical or important functions of a financial entity, and perform on live production systems supporting such functions	DORA Article 26(1) and (2)	All except smaller and microenterprises	Resilience Testing Program

Requirements	References	Which financial entities	Usually documented through
Identify all relevant underlying ICT systems, processes and technologies supporting critical or important functions and ICT services, including those supporting the critical or important functions which have been outsourced or contracted to ICT third-party service providers, and assess which critical or important functions need to be covered by the TLPT	DORA Article 26(2)	All except smaller and microenterprises	Asset Management Procedure + IT Asset Register + Resilience Testing Program
Take the necessary measures and safeguards to ensure the participation of ICT third-party service providers in the TLPT	DORA Article 26(3)	All except smaller and microenterprises	Supplier Security Policy
Apply effective risk management controls to mitigate the risks of testing of any potential impact on data, damage to assets, and disruption to critical or important functions, services or operations	DORA Article 26(5)	All	Resilience Testing Program
Provide to the authority a summary of the relevant findings, the remediation plans and the documentation demonstrating that the TLPT has been conducted in accordance with the requirements	DORA Article 26(6)	All	Resilience Testing Program
Only use testers for the carrying out of TLPT, that: (a) are of the highest suitability and reputability; (b) possess technical and organisational capabilities; (c) are certified by an accreditation body; (d) provide an independent assurance, or an audit report, in relation to the sound management of risks associated with the carrying out of TLPT; (e) are duly and fully covered by relevant professional indemnity insurances	DORA Article 27(1)	All	Supplier Security Policy + Resilience Testing Program

Requirements	References	Which financial entities	Usually documented through
Management of ICT third-party risk must be implemented in light of the principle of proportionality, taking into account: (i) the nature, scale, complexity and importance of ICT-related dependencies, and (ii) the risks arising from contractual arrangements on the use of ICT services concluded with ICT third-party service providers, taking into account the criticality or importance of the respective service, process or function, and the potential impact on the continuity and availability	DORA Article 28(1)(b) CDR 2024/1773	All	Supplier Security Policy
Adopt and regularly review a strategy on ICT third-party risk, taking into account the multi-vendor strategy, where applicable; the strategy must include a policy on the use of ICT services	DORA Article 28(2) CDR 2024/1773	All except smaller and microenterprises	Strategy on ICT third-party risk + Supplier Security Policy
The management body must regularly review the risks identified in respect to contractual arrangements on the use of ICT services supporting critical or important functions	DORA Article 28(2) CDR 2024/1773	All except smaller and microenterprises	Supplier Security Policy + Strategy on ICT third-party risk
Maintain and update a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers	DORA Article 28(3) CDR 2024/1773	All	Register of Contractual Arrangements + Supplier Security Policy
Report at least yearly to the competent authorities on the number of new arrangements on the use of ICT services, the categories of ICT third-party service providers, the type of contractual arrangements and the ICT services and functions which are being provided; inform the competent authority in a timely manner about any planned contractual arrangement on the use of ICT services supporting critical or important functions	DORA Article 28(3) CDR 2024/1773	All	Supplier Security Policy

Requirements	References	Which financial entities	Usually documented through
Before entering into a contractual arrangement on the use of ICT services, financial entities must: (a) assess whether the contractual arrangement covers the use of ICT services supporting a critical or important function; (b) assess if supervisory conditions for contracting are met; (c) identify and assess all relevant risks in relation to the contractual arrangement; (d) undertake all due diligence on prospective ICT third-party service providers; (e) identify and assess conflicts of interest	DORA Article 28(4) CDR 2024/1773	All	Supplier Security Policy
Only enter into contractual arrangements with ICT third-party service providers that comply with appropriate information security standards	DORA Article 28(5) CDR 2024/1773	All	Supplier Security Policy
Pre-determine the frequency of audits and inspections of ICT service providers, as well as the areas to be audited through adhering to commonly accepted audit standards in line with any supervisory instruction and on the basis of a risk-based approach	DORA Article 28(6) CDR 2024/1773	All	Supplier Security Policy
Verify that auditors, whether internal or external, or a pool of auditors, possess appropriate skills and knowledge where contractual arrangements concluded with ICT third-party service providers entail high technical complexity	DORA Article 28(6) CDR 2024/1773	All	Supplier Security Policy
Ensure that contractual arrangements on the use of ICT services may be terminated in any of the following circumstances: (a) significant breach by the ICT third-party service provider; (b) circumstances altering the performance of the functions provided through the contractual arrangement; (c) ICT service provider's evidenced weaknesses pertaining to its overall ICT risk management; (d) where the competent authority can no longer effectively supervise the financial entity	DORA Article 28(7) CDR 2024/1773	All	Supplier Security Policy

Requirements	References	Which financial entities	Usually documented through
For ICT services supporting critical or important functions, put in place exit strategies; exit plans must be comprehensive, documented and sufficiently tested and reviewed periodically; identify alternative solutions and develop transition plans enabling to remove the contracted ICT services and the relevant data from the IT service provider	DORA Article 28(8) CDR 2024/1773	All	Supplier Security Policy + ICT Service Exit Strategy
Take into account whether the envisaged conclusion of a contractual arrangement in relation to ICT services supporting critical or important functions would lead to any of the following: (a) contracting an ICT third-party service provider that is not easily substitutable; or (b) having in place multiple contractual arrangements in relation to the provision of ICT services supporting critical or important functions with the same ICT service provider or with closely connected ICT service providers	DORA Article 29(1)	All	Supplier Security Policy
Weigh benefits and risks that may arise where the contractual arrangements on the use of ICT services supporting critical or important functions include the possibility that an ICT third-party service provider further subcontracts ICT services supporting a critical or important function to other ICT third-party service providers; also consider the insolvency law provisions	DORA Article 29(2)	All	Supplier Security Policy
Consider the compliance with EU data protection rules (GDPR and others) where contractual arrangements on the use of ICT services supporting critical or important functions are concluded with an ICT third-party service provider established in a non-EU country	DORA Article 29(2)	All	Supplier Security Policy

Requirements	References	Which financial entities	Usually documented through
Assess whether and how potentially long or complex chains of subcontracting may impact their ability to fully monitor the contracted functions and the ability of the competent authority to effectively supervise the financial entity where the contractual arrangements on the use of ICT services supporting critical or important functions provide for subcontracting	DORA Article 29(2)	All	Supplier Security Policy
The contractual arrangements on the use of ICT services must include at least the following elements: (a) a clear and complete description of all functions and ICT services; (b) the locations, namely the regions or countries, where the contracted or subcontracted functions and ICT services are to be provided and where data is to be processed; (c) provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data, including personal data; (d) provisions on ensuring access, recovery and return in an easily accessible format; (e) service level descriptions, including updates and revisions thereof; (f) the obligation of the ICT third-party service provider to provide assistance to the financial entity when an ICT incident occurs; (g) the obligation of the ICT third-party service provider to fully cooperate with the competent authorities; (h) termination rights and related minimum notice periods; (i) the conditions for the participation of ICT third-party service providers in the financial entities' ICT security awareness programmes and digital operational resilience training	DORA Article 30(2)	All	Supplier Security Policy

Requirements	References	Which financial entities	Usually documented through
The contractual arrangements on the use of ICT services supporting critical or important functions must include, in addition to the elements referred to in paragraph 2, at least the following: (a) full service level descriptions; (b) notice periods and reporting obligations; (c) requirements for the ICT third-party service provider to implement and test business contingency plans and to have in place ICT security measures, tools and policies; (d) the obligation of the ICT third-party service provider to participate and fully cooperate in the financial entity's TLPT; (e) the right to monitor, on an ongoing basis, the ICT third-party service provider's performance; (f) exit strategies	DORA Article 30(3)	All	Supplier Security Policy
When negotiating contractual arrangements, financial entities and ICT third-party service providers shall consider the use of standard contractual clauses developed by public authorities for specific services	DORA Article 30(4)	All	Supplier Security Policy

5.2. Common cybersecurity documents not required by DORA

I'm aware that the list above is very extensive; however, DORA did not mention some documents that are quite common when managing cybersecurity:

- Information Classification Policy — provides clear rules on how to classify documents and other information, and how to protect those assets according to classification level.
- Mobile Device, Teleworking and Work from Home Policy — specifies the rules for using laptops, smartphones, and other devices outside of company premises.
- Bring Your Own Device (BYOD) Policy — specifies security aspects if employees are using their private devices for work.
- Disposal and Destruction Policy — specifies how to dispose of devices and media, in order to delete all sensitive data and avoid breaking intellectual property rights.
- Procedures for Working in Secure Areas — defines security rules for data centers, archives, and other areas that need special protection.
- Clear Desk and Clear Screen Policy — defines rules for each employee on how to protect his/her workspace.

6. Which IT companies need to comply with DORA, and how?

DORA is a regulation that is focused on cybersecurity and resilience of financial organizations in the European Union — however, for these organizations to be safe, DORA pays special attention to supply chain security, in particular to the IT companies that provide services to financial organizations.

In effect, such IT companies must comply with certain elements of DORA — the text below explains which IT companies fall under the scope of DORA, and what exactly is required of them.

6.1. Which IT companies must comply with DORA?

In its Article 3, DORA specifies the following terms and definitions:

- **ICT** — "information and communication technology"
- **ICT services** — "digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services"
- **ICT third-party service provider** — any company (whether independent or part of a financial group) providing ICT services to financial entities

Therefore, all IT and telecom companies that provide their services to financial entities on an ongoing basis (with the exception of analogue telephone services) must be compliant with DORA.

6.2. What must ICT service providers comply with?

All ICT third-party service providers that provide services for financial organizations must comply with the following:

Compliance with security standards. According to Article 28, financial organizations can use services only from companies complying with appropriate information security standards — even through DORA does not say which standards, this will probably go in the direction of ISO 27001 and the European Cybersecurity Certification Scheme.

Contractual obligations. According to Article 30, financial organizations need to include the following clauses in contracts with ICT service providers:

- provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data, including personal data
- provisions on ensuring access, recovery and return in an easily accessible format of personal and non-personal data processed by the financial entity
- the obligation of the ICT third-party service provider to provide assistance to the financial entity
- the participation of ICT third-party service providers in the financial entities' ICT security awareness programmes and digital operational resilience training

6.3. What are critical ICT service providers?

According to Article 31, a *critical* ICT third-party service provider is designated as such according to the following criteria:

- the systemic impact on the stability, continuity or quality of the provision of financial services
- the systemic character or importance of the financial entities that rely on the relevant ICT third-party service provider
- the degree of substitutability of the ICT third-party service provider, and
- the reliance of financial entities on the services provided by the relevant ICT third-party service provider in relation to critical or important functions of financial entities.

According to Article 3 of DORA, a *critical or important function* is "a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law."

European Supervisory Authorities (ESAs) — meaning the European Banking Authority (EBA), European Securities and Markets Authority (ESMA), and European Insurance and Occupational Pensions Authority (EIOPA) — are the ones that determine for each ICT third-party service provider whether it is critical or not.

They decide who is critical based on the criteria listed above, and based on a document that describes these criteria in more detail: CDR 2024/1502 - The criteria for the designation of ICT third-party service providers as critical for financial entities.

6.4. What additional DORA requirements exist for critical ICT service providers?

On top of the requirements specified above, DORA requires critical ICT service providers to comply with a lot more:

Oversight by government bodies. Article 31 specifies that critical service providers are subject to oversight activities by a Lead Overseer, which is appointed by European Supervisory Authorities (ESAs).

According to Article 33, the purpose of the Lead Overseer is to continually assess whether such an IT provider has in place "comprehensive, sound and effective rules, procedures, mechanisms and arrangements to manage the ICT risk which it may pose to financial entities."

Paying for the supervision. Article 43 specifies that the supervision comes with a cost, and that the Lead Overseer calculates this cost every year. According to CDR 2024/1505 The amount of the oversight fees to be charged by the Lead Overseer to critical ICT third-party service providers and the way in which those fees are to be paid, the minimum annual fee is 50,000 euros.

Supervision access. According to Article 39, the IT service provider needs to allow the Lead Overseer to "enter in, and conduct all necessary onsite inspections on, any business premises, land or property of the ICT third-party service providers, such as head offices, operation centres, secondary premises, as well as to conduct off-site inspections."

Supervision elements. According to Article 33, the Lead Overseer must check the following:

- ICT requirements to ensure the security, availability, continuity, scalability and quality of services
- ability to maintain at all times high standards of availability, authenticity, integrity or confidentiality of data
- the physical security contributing to ensuring the ICT security, including the security of premises, facilities, data centres
- the risk management processes, including ICT risk management policies, ICT business continuity policy and ICT response and recovery plans
- the governance arrangements, including an organisational structure with clear, transparent and consistent lines of responsibility and accountability rules enabling effective ICT risk management
- the identification, monitoring and prompt reporting of material ICT-related incidents, the management and resolution of those incidents, in particular cyber-attacks
- the mechanisms for data portability, application portability and interoperability
- the testing of ICT systems, infrastructure and controls
- the ICT audits
- the use of relevant national and international standards applicable to the provision of its ICT services to the financial entities

Documentation and evidence. According to Article 37, the Lead Overseer may require the following documentation and evidence: "all relevant business or operational documents, contracts, policies, documentation, ICT security audit reports, ICT-related incident reports, as well as any information relating to parties to whom the critical ICT third-party service provider has outsourced operational functions or activities."

Additional contractual obligations. Article 30 specifies that financial entities must sign agreements with specific clauses for critical service providers, including:

- precise quantitative and qualitative performance targets within the agreed service levels
- notice periods and reporting obligations
- implementing and testing business contingency plans

- have in place ICT security measures, tools, and policies that provide an appropriate level of security for the provision of services by the financial entity
- participate and fully cooperate in the threat-led penetration testing of a financial entity
- unrestricted rights of access, inspection, and audit by the financial entity
- obligation to fully cooperate during the onsite inspections and audits
- continuing to provide the ICT services during a period of cancellation of the agreement
- allowing the financial entity to migrate to another ICT third-party service provider

Treatment of non-EU suppliers. Article 31 says that if the critical service provider is based in a non-EU country, then it must establish a subsidiary within the EU.

Article 36 specifies that the Lead Overseer may exercise the powers "on any premises located in a third-country which is owned, or used in any way, for the purposes of providing services to Union financial entities, by a critical ICT third-party service provider."

Fines and penalties. In its Article 35, DORA is quite specific on fines that critical ICT third-party service providers need to pay if they are not compliant: This is up to 1% of their worldwide annual turnover, and the amount of the fine depends on the number of days that the service provider was not compliant. Further, the Lead Overseer must issue a public notice that reveals the name of the service provider that was fined.

Article 42 specifies perhaps the worst penalty — a competent authority can require a financial organization that is a client of an IT service provider that is not compliant with DORA to stop using their services.

See also: ISO 27001 Implementation Guide: Checklist of Steps, Timing, and Costs Involved.

7. How to organize DORA training and awareness

The DORA regulation is very specific when it comes to training and awareness requirements — and this is not only for financial organizations, but also for the IT companies that supply their services to financial entities.

The text below specifies what those DORA requirements are, and suggests how to organize effective training and awareness according to this EU regulation.

7.1. Training and awareness requirements for financial organizations

To start, what exactly does DORA require? There are several articles in DORA that prescribe training and awareness for financial organizations:

- Article 5(2) g) requires organization-wide training and awareness: management bodies of financial entities must "allocate and periodically review the appropriate budget to fulfil the financial entity's digital operational resilience needs in respect of all types of resources, including relevant ICT security awareness programmes and digital operational resilience training referred to in Article 13(6), and ICT skills for all staff."
- Article 5(4) requires training and awareness for senior management: "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."
- Article 13(6) requires training and awareness for both senior management, and all the employees — financial entities must "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."
- Article 16(1) point (h) requires training and awareness as a consequence of testing and incidents: "implement, as appropriate, relevant operational conclusions resulting from the tests referred to in point (g) and from post-incident analysis into the ICT risk assessment process and develop, according to needs and ICT risk profile, ICT security awareness programmes and digital operational resilience training for staff and management."
- Article 19 (b) in "CDR 2024-1774 Technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework" requires the whole staff of financial organizations to be informed about security documentation, reporting channels for anomalous behavior, and returning all the assets upon termination of employment.
- Article 28 in "CDR 2024-1774 Technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework" requires the organization, as part of simplified ICT risk management, to allocate and review "at least once a year the budget necessary to fulfil the financial entity's digital operational resilience needs in respect of all types of resources, including relevant ICT security awareness programmes and digital operational resilience training and ICT skills for all staff."

7.2. Training and awareness requirements for IT suppliers

As mentioned earlier, DORA specifies that ICT suppliers of financial organizations also need to go for training and awareness — basically, this training needs to be arranged by the financial organization:

- Article 13(6) says that "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)."
- Article 30(2) point (i) goes a step further and says that "the contractual arrangements on the use of ICT services shall include at least the following elements: … the conditions for the participation of ICT third-party service providers in the financial entities' ICT security awareness programmes and digital operational resilience training in accordance with Article 13(6)."
- Article 19 (b), in "CDR 2024-1774 Technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework" similarly to the requirement listed for financial organizations, requires the whole staff of ICT third-party service providers to be informed about security documentation, reporting channels for anomalous behavior, and returning all the assets upon termination of employment.

7.3. Which topics should be covered in DORA training & awareness?

When defining topics for training and awareness, the best approach is to go through each DORA article and determine which of them need to be covered with training or awareness.

However, since different DORA requirements are relevant to different employees, the best approach is to group employees and define which articles, i.e., topics, are the best suited for them.

In general, you could go with the following groups:

- Topics for senior management
- Topics for security managers
- Topics for mid-level management
- Topics for IT employees
- Topics for all other employees
- Topics for IT service providers

In the table below, you can see how to map DORA requirements (and requirements of some Commission Delegated Regulations) to particular target groups.

Training topics	Senior management	Security managers	Mid-level management	IT employees	All other employees	IT service providers
What is the DORA regulation? (all relevant DORA articles)	✓	✓	✓	✓	✓	✓
What are the main requirements specified in DORA? (all relevant DORA articles)	✓	✓	✓			
What are DORA Commission Delegated Regulations? (all published CDRs)	✓	✓	✓			
DORA implementation steps (all relevant DORA articles)		✓	✓			
Which IT providers need to comply with DORA?		✓	✓	✓		✓
What must ICT service providers comply with? (Articles 28, 30, 31, 33, 35, 37, 39, 42, and 43)		✓	✓			✓
Why should ICT suppliers go for ISO 27001 and ISO 22301 because of DORA?		✓				✓
Relationship between ISO 27001, ISO 22301, and DORA		✓				✓
DORA vs. NIS 2 vs. GDPR vs. CER	✓	✓	✓			✓
Governance responsibilities for senior management (Article 5)	✓	✓	✓			

Training topics	Senior management	Security managers	Mid-level management	IT employees	All other employees	IT service providers
Key elements of an ICT risk management framework (Article 6; CDR 2024/1774 Articles 2 and 3)	✓	✓	✓			
Basic concepts of risk assessment and treatment (Article 8; CDR 2024/1774 Articles 3 and 31)		✓	✓			
Review of the ICT risk management framework (Article 6 paragraph 5; CDR 2024/1774 Article 27)	✓	✓	✓			
Internal audit of the ICT risk management framework (Article 6 paragraph 6)	✓	✓	✓			
Follow-up and corrective actions (Article 6 paragraph 7; Article 13 paragraph 3 and 5; Article 17 paragraph 2)	✓	✓	✓			
Defining the digital operational resilience strategy (Article 6 paragraph 8)	✓	✓	✓			
Encryption and cryptography (Article 7; CDR 2024/1774 Articles 6 and 7)		✓		✓		✓
Identifying ICT-supported business functions, roles and responsibilities, and assets (Article 8; CDR 2024/1774 Articles 4 and 5)		✓	✓	✓		

Training topics	Senior management	Security managers	Mid-level management	IT employees	All other employees	IT service providers
Measurement, monitoring, and controlling the ICT systems (Article 9 paragraph 1; Article 13 paragraph 4; Article 16 paragraph 1; CDR 2024/1774 Articles 2, 3, 8, 31)	✓	✓	✓			
Policies and procedures for ICT operations security (Article 9 paragraph 2; CDR 2024/1774 Article 8)		✓		✓		✓
Capacity and performance management (Article 9 paragraph 2; CDR 2024/1774 Article 9)		✓		✓		✓
Data and system security (Article 9 paragraph 2; CDR 2024/1774 Article 11)		✓		✓		✓
Logging procedures, protocols, and tools (Article 9 paragraph 2; CDR 2024/1774 Article 12)		✓		✓		✓
Physical and environmental security (Article 9 paragraph 2; CDR 2024/1774 Article 18)		✓	✓			✓
Organizing human resources security (Article 9 paragraph 2)		✓	✓			✓
Human resources policy (Article 9 paragraph 2; CDR 2024/1774 Article 19)	✓	✓	✓	✓	✓	✓

Training topics	Senior management	Security managers	Mid-level management	IT employees	All other employees	IT service providers
Secure communications - secure transfer/transit of data (Article 9 paragraph 3 point a; CDR 2024/1774 Article 14)		✓		✓		✓
Handling the risk of data corruption (Article 9 paragraph 3 point b)		✓		✓		✓
Handling risks arising from data management (Article 9 paragraph 3 point d)		✓	✓	✓		✓
Developing a top-level information security policy (Article 9 paragraph 4 point a)	✓	✓	✓	✓	✓	
Establishing network and infrastructure management structure (Article 9 paragraph 4 point b; CDR 2024/1774 Article 13)		✓		✓		✓
Policies for limiting physical and logical access (Article 9 paragraph 4 point c; CDR 2024/1774 Article 21)		✓	✓	✓		✓
Identity management and strong authentication mechanisms (Article 9 paragraph 4 point d; CDR 2024/1774 Article 20)		✓		✓		✓
ICT project management (CDR 2024/1774 Article 15)		✓	✓	✓		✓

Training topics	Senior management	Security managers	Mid-level management	IT employees	All other employees	IT service providers
ICT change management (Article 9 paragraph 4 point e; CDR 2024/1774 Article 17)		✓	✓	✓		✓
Vulnerability, patch management, and updates (Article 9 paragraph 4 point f; CDR 2024/1774 Article 10)		✓		✓		✓
ICT systems acquisition, development, and maintenance (CDR 2024/1774 Article 16)		✓	✓	✓		✓
Mechanisms to promptly detect anomalous activities (Article 10; CDR 2024/1774 Article 23)		✓	✓	✓		✓
Implementing an ICT business continuity policy (Article 11 paragraphs 1, 2, and 4; Article 9 paragraph 2; CDR 2024/1774 Article 24)	✓	✓	✓	✓	✓	✓
Implementing ICT response and recovery plans (Article 11 paragraph 3; CDR 2024/1774 Article 26)		✓	✓	✓		✓
Business impact analysis, RTO, and RPO (Article 11 paragraph 5; Article 12 paragraph 6)		✓	✓			
Testing business continuity and recovery plans (Article 11 paragraph 6; CDR 2024/1774 Article 25)		✓	✓	✓	✓	✓

Training topics	Senior management	Security managers	Mid-level management	IT employees	All other employees	IT service providers
Crisis management and crisis communication plans (Article 11 paragraph 7; Article 14)	✓	✓	✓			
Emergency communications (Article 11 paragraph 7; Article 14)	✓	✓	✓	✓		
Managing backup and restoration (Article 12 paragraphs 1, 2, 3, and 7)		✓		✓		✓
Secondary processing site (Article 12 paragraphs 4 and 5)		✓	✓	✓		
Threat intelligence (Article 13 paragraph 1)		✓		✓		✓
Post-incident reviews (Article 13 paragraph 2)		✓	✓	✓		
Organizing security training and awareness (Article 13 paragraph 6)		✓	✓	✓		✓
Monitoring technological developments (Article 13 paragraph 7)		✓		✓		
Main elements of the simplified ICT risk management framework (Article 16; CDR 2024/1774 Title III)	✓	✓	✓	✓		

Training topics	Senior management	Security managers	Mid-level management	IT employees	All other employees	IT service providers
Main elements of the incident management process (Article 17; CDR 2024/1774 Article 22)	✓	✓	✓	✓		
Classification of ICT incidents and threats (Article 18; CDR 2024/1772 Articles 1 to 10)		✓	✓	✓		
Reporting of major incidents and cyber threats (Article 19)		✓		✓		
Main elements of digital operational resilience testing (Article 24)	✓	✓	✓			
Resilience testing of ICT tools and systems (Article 25)		✓		✓		✓
Key elements of Threat-Led Penetration Testing - TLPT (Articles 26 and 27)		✓		✓		✓
Main elements of management of ICT third-party risk (Article 28; CDR 2024/1773 Articles 1 to 4)	✓	✓	✓			✓
Monitoring, inspection, and audit of the ICT third-party service provider (Article 28 paragraph 6; Article 30 paragraph 3 points a and e; CDR 2024/1773 Article 9)		✓	✓			✓
Exit strategies for ICT services (Article 28 paragraph 8; CDR 2024/1773 Article 10)		✓	✓	✓		✓

Training topics	Senior management	Security managers	Mid-level management	IT employees	All other employees	IT service providers
Assessment of risks of ICT service providers (Article 29; CDR 2024/1773 Articles 5, 6, and 7)		✓	✓	✓		✓
Clauses to be included in contracts with ICT service providers (Article 30; CDR 2024/1773 Article 8)		✓	✓			✓
Who are critical ICT service providers? (Article 31; CDR 2024/1502 Articles 2, 3, 4, 5, and 6)		✓	✓			✓
The roles of Lead Overseer and competent authorities for critical ICT service providers (Articles 33, 35, 36, 37, 38, 39, 42, and 43)		✓				✓
Penalties and fines (Articles 50, 51, and 54)	✓	✓	✓			✓

7.4. Security awareness topics for all employees

When it comes to awareness, DORA's articles 5, 13, 16, and 30 require ICT security awareness programs for all employees — not only for financial entities, but also for ICT service providers.

Since DORA did not specify what the content of such awareness programs should be, below you will find a list of suggested topics that could be suitable for a company-wide cybersecurity awareness program:

- Basic cyber hygiene practices
- Backup basics
- Basics of authentication
- Basics of network security
- Insider threats
- Cloud security basics
- Computer malware
- Email security
- Human error

- Identity theft
- The mind of a hacker
- Passwords
- Device physical security
- Privacy
- Intellectual property
- Protecting paperwork
- Security of mobile devices
- Social engineering
- Social media
- Remote work

7.5. Options for delivering NIS 2 training

Essentially, you have three potential options for delivering training to a group of people:

1) Instructor-led in-classroom training. This is the traditional way of delivering training — you place everyone in a room, and the instructor presents all the relevant topics face to face. This enables attendees to ask questions and allows for some interactivity through shorter workshops, but organizing such training is difficult.

Pros:

- Training can be adapted according to the needs of the company
- Higher engagement

Cons:

- Probably the most expensive
- Cannot be delivered very often
- Hard to deliver separate training for different target groups

2) Instructor-led online training. This is similar to instructor-led in-classroom training; however, the main difference is that there is no physical classroom — the training is delivered through online tools like MS Teams, Zoom, or similar. This still enables attendees to ask questions and organize short workshops; while organizing such training is easier, there are still challenges because all attendees must be present at the same time.

Pros:

- Training can be adapted according to the needs of the company
- Easier to organize than in-classroom training

Cons:

- Lower engagement, because attendees tend to ask fewer questions through online tools
- All attendees must be present at the same time

3) Pre-recorded online training delivered via learning management system (LMS). This approach is different from the first two options — here, all the videos are pre-recorded and

uploaded to LMS software that distributes the videos to attendees and tracks their attendance (and test results, if needed). This disables direct engagement with the instructor (although some AI solutions are now addressing this problem), but organizing such training is far easier.

Pros

- Easy tracking of attendance and test results
- Employees can watch videos at their convenience
- The most budget-friendly option

Cons

- Attendees cannot ask questions, at least not directly to the instructor

7.6. Which training delivery option to choose?

The choice really depends on the type of training:

Regular vs. one-time training. If the training happens only once, then instructor-led classroom training or instructor-led online training is something that can be organized, as opposed to training that needs to be delivered regularly (e.g., monthly, quarterly, annually). For such regular training, pre-recorded online training via LMS is a more appropriate solution.

Required engagement. If the training covers some very in-depth topics that require high engagement with the instructor, then instructor-led classroom training or instructor-led online training is probably a better solution. If the training covers some more general topics that do not require high engagement, then pre-recorded online training via LMS will be a more practical solution.

Number of attendees. If the training involves a smaller group of people, then instructor-led classroom training or instructor-led online training will be manageable. If the training involves a larger number of people, then pre-recorded online training via LMS will be easier.

Time zones. If all attendees are in the same time zone, then instructor-led classroom training or instructor-led online training will be feasible; however, if the attendees are scattered across different time zones, pre-recorded online training via LMS is a more viable solution.

7.7. A mixed approach might work the best

Ultimately, you might end up with a mix of the approaches described above — for selected employees that require one-time training with in-depth knowledge, you might go with instructor-led training, whereas for regular training that has to be delivered to a larger number of employees and that does not go into too much depth, pre-recorded online training via LMS will probably do a good job.

8. Penalties and enforcement

8.1. Penalties for financial entities

Unlike NIS 2, DORA does not specify minimum fines for financial entities — rather, it gives the freedom to Member States to define their own fines in their countries.

However, DORA does specify other penalties for financial entities that can be enacted by competent authorities:

- Ordering a financial entity to stop activities that are not compliant with DORA.
- Defining any measure (including fines) to make sure financial entities are compliant with DORA.
- Issuing public notices that can reveal the names of non-complying financial entities, as well as persons in charge.

8.2. Penalties for critical ICT third-party service providers

DORA is quite specific on fines that critical ICT third-party service providers need to pay if they are not compliant: This is up to 1% of their worldwide annual turnover, and the amount of the fine depends on the number of days that the service provider was not compliant.

The Lead Overseer (the body that supervises critical service providers) must issue public notice that reveals the name of the service provider that was fined. The competent authority can require a financial organization that is a client of a non-compliant service provider to stop using their services.

8.3. Which government bodies enforce DORA?

DORA does not bring any novelties when it comes to enforcement — in its Article 46 it refers to existing regulations that specify which competent authorities are in charge of supervising particular types of financial organizations.

According to regulations referenced in Article 46, for the majority of financial entities that need to be compliant with DORA, EU Member States designate competent authorities that supervise and enforce financial regulations.

There are a couple of exceptions, where EU authorities directly supervise and enforce financial regulations:

- For credit institutions classified as significant - the European Central Bank (ECB)
- For securitisation repositories - the European Securities and Markets Authority (ESMA)

8.4. The role of European Supervisory Authorities (ESAs)

The European Banking Authority (EBA), European Securities and Markets Authority (ESMA), and European Insurance and Occupational Pensions Authority (EIOPA) have several tasks according to DORA, including defining guidelines and regulatory technical standards (which will be published as Commission Delegated Regulations), defining which ICT third-party service providers are critical, appointing Lead Overseers for critical service providers, etc.

ESAs publish various materials related to DORA and other activities on their websites; you can find them here:

- European Banking Authority (EBA)
- European Securities and Markets Authority (ESMA)
- European Insurance and Occupational Pensions Authority (EIOPA)

9. Relationship to other standards and regulations

9.1. How is DORA related to ISO 27001 and ISO 22301?

DORA does not mention cybersecurity standards like ISO 27001 (nor any other standard from the ISO27k series), or business continuity standards like ISO 22301.

However, when reading DORA's Chapter II ICT risk management and CDR 2024-1774 Technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework, it becomes obvious that many concepts were taken from ISO 27001, ISO 27002, ISO 27005, and ISO 22301. Therefore, financial entities will find it useful to use those standards to comply with DORA's risk management requirements.

For IT suppliers, DORA Article 28 specifies that "Financial entities may only enter into contractual arrangements with ICT third-party service providers that comply with appropriate information security standards." Since ISO 27001 is the most popular information security standard worldwide, the certification against this standard will most probably become even more popular.

9.2. How is DORA related to NIS 2?

The full title of NIS 2 is "Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union."

Although NIS 2 and DORA were both published on the same day (December 27, 2022), there are big differences between them:

	DORA	NIS 2
Type	Regulation (directly applicable to financial institutions)	Directive (companies comply with local legislation that is published)
Applies to	Financial institutions	Organizations that are considered essential and important entities
Protection	Besides cybersecurity measures, the emphasis is also on overall resilience of financial institutions.	Emphasis on cybersecurity measures
Effective from	January 17, 2025	October 18, 2024

9.3. Must financial organizations comply with NIS 2?

NIS 2 lists "banking" and "financial market infrastructures" as sectors that need to be compliant with NIS 2 — however, according to NIS 2 Article 4, DORA and other sector-specific regulations have priority over NIS 2.

In effect, any financial entities that are in the scope of DORA do not need to comply with NIS 2.

The reason why banking and financial market infrastructures are listed in NIS 2 is that this allows competent authorities in charge of NIS 2 to more easily exchange information about such financial entities.

9.4. What is the difference between DORA and the EU GDPR?

The full title of the EU GDPR is "Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)."

Even though both DORA and the GDPR focus on protection of data, each has a different angle:

	DORA	EU GDPR
Type	Regulation (directly applicable to financial institutions)	Regulation (directly applicable to all companies)
Applies to	Financial institutions	Any organization that processes personal data, including financial institutions
Protection	The focus is on protecting any data in ICT systems and achieving digital resilience.	Cybersecurity measures apply to personal data only; there is also a legal aspect of protection of personal data.
Effective from	January 17, 2025	May 25, 2018

9.5. What is the difference between DORA and the Critical Entities Resilience Directive (CER)

The full title of CER is "Directive (EU) 2022/2557 on the resilience of critical entities."

Although DORA and CER (as well as NIS 2) were published on the same day (December 27, 2022), they each have a different scope:

	DORA	CER
Type	Regulation (directly applicable to financial institutions)	Directive (companies comply with local legislation that is published)
Applies to	Financial institutions	Organizations that are considered critical according to Member State decision
Protection	Besides resilience, the emphasis is also on cybersecurity measures.	Emphasis on resilience and business continuity
Effective from	January 17, 2025	October 18, 2024; however, critical entities need to become compliant within 10 months from the day they are designated as critical.

10. What are DORA Commission Delegated Regulations?

The text of the DORA regulation is pretty lengthy, but nevertheless it doesn't specify all the requirements — it has prescribed that certain details will be further specified in Commission Delegated Regulations (CDRs).

Commission Delegated Regulations are regulatory technical standards published by the EU Commission that further specify certain rules for DORA — they can be considered as appendices to DORA. Such CDRs are proposed by European Supervisory Authorities, and then published by the EU Commission.

10.1. Which DORA CDRs have been published?

At the time this white paper was written, the following CDRs were published:

- CDR 2024/1502 - The criteria for the designation of ICT third-party service providers as critical for financial entities — related to DORA Article 31
- CDR 2024/1505 - The amount of the oversight fees to be charged by the Lead Overseer to critical ICT third-party service providers and the way in which those fees are to be paid — related to DORA Article 43
- CDR 2024/1772 - The criteria for the classification of ICT-related incidents and cyber threats, setting out materiality thresholds and specifying the details of reports of major incidents — related to DORA Article 18
- CDR 2024/1773 - Regulatory technical standards specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers — related to DORA Article 28
- CDR 2024/1774 - Regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework — related to DORA Article 15 and Article 16

10.2. Explanation of DORA CDRs

Let's analyze each of these CDRs in more detail:

CDR 2024/1502 - The criteria for the designation of ICT third-party service providers as critical for financial entities specifies:

- European Supervisory Authorities must use a set of criteria to decide whether an ICT third-party service provider is critical.
- Those criteria include: systemic impact, systemic character and importance, criticality or importance of the functions, and degree of sustainability.

CDR 2024/1505 - The amount of the oversight fees to be charged by the Lead Overseer to critical ICT third-party service providers and the way in which those fees are to be paid specifies:

- Lead Overseers must calculate the oversight fees based on their overall cost of supervision.
- The minimum annual oversight fee is €50,000 per critical ICT third-party service provider.
- Oversight fees are paid once a year.

CDR 2024/1772 - The criteria for the classification of ICT-related incidents and cyber threats, setting out materiality thresholds and specifying the details of reports of major incidents specifies:

- Financial entities need to take into account various aspects of an incident when deciding if it is a major incident.
- Those aspects include: number of clients affected, number of financial counterparts affected, amount of transactions affected, reputational impact, duration and service downtime, geographical spread, data losses, criticality of services affected, and economic impact.
- Financial entities must classify threats, and decide if threats are significant based on several criteria.

CDR 2024/1773 - Regulatory technical standards specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers specifies:

- When creating the policy for contractual arrangements on the use of ICT services, financial entities must take into account overall risk profile and complexity, and include several elements in the policy.
- Elements that must be included in the policy are: governance arrangements, life cycle for the adoption and use of contractual arrangements, risk assessment, due diligence, conflicts of interest, contractual clauses, monitoring of the contractual arrangements, and exit from and termination of the contractual arrangements.

CDR 2024/1774 - Regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework specifies:

- A very detailed list of ICT security policies, procedures, protocols, and tools that financial entities need to establish.
- These must cover several areas, including ICT risk management, ICT asset management, encryption and cryptography, ICT operations security, network security, ICT project and change management, physical and environmental security, human resources policy, identity management, access control, ICT-related incident detection and response, ICT business continuity management, and report on the ICT risk management framework review.
- The CDR specifies separate rules for a simplified ICT risk management framework.

10.3. Upcoming CDRs

Here are some of the CDRs that are in the process of being published:

- Technical standards on major incident reporting
- Guidelines on oversight cooperation
- Guidelines on the estimation of aggregated costs/losses caused by major ICT-related incidents
- Regulatory technical standards on the harmonization of conditions enabling the execution of the oversight activities
- Regulatory technical standards specifying elements related to threat-led penetration tests

- Regulatory technical standards on the criteria for determining the composition of the joint examination team
- Regulatory technical standards on subcontracting ICT services supporting critical or important functions under DORA

So, as you can see, DORA in itself is already pretty specific when it comes to cybersecurity rules, but together with these CDRs it becomes very demanding with regard to how cybersecurity needs to be implemented.

Sources:

- DORA regulation
- Series of DORA articles on Advisera.com

Author:

Dejan Kosutic

Leading expert on cybersecurity & information security and the author of several books, articles, webinars, and courses. As a premier expert, Dejan founded Advisera to help small and medium businesses obtain the resources they need to become compliant with EU regulations and ISO standards. He believes that making complex frameworks easy to understand and simple to use creates a competitive advantage for Advisera's clients, and that AI technology is crucial for achieving this.

As an ISO 27001, NIS 2, and DORA expert, Dejan helps companies find the best path to compliance by eliminating overhead and adapting the implementation to their size and industry specifics.

Advisera Expert Solutions Ltd
for electronic business and business consulting
www.advisera.com

Our offices

US Office
1178 Broadway, 3rd Floor #3829
New York NY 10001
United States

EU Office
Zavizanska 12
10000 Zagreb
Croatia, European Union

EMAIL:
support@advisera.com