MetaCompliance®

How ISO 27001 Supports DORA Compliance

The EU's Digital Operational Resilience Act comes into force in January 2025. What does it mean for your organisation?

Elevate your **Cybersecurity Training** with **MetaCompliance**

Contents

Introduction:

If you work in IT or cybersecurity at an EU financial organisation—or an ICT vendor that supplies one—you already know the Digital Operational Resilience Act (DORA) is on the way.

Since it's unlikely you're building a compliance program from scratch, you may be wondering which DORA requirements you already have covered... and what you'll need to add or improve ahead of the enforcement date.

If you already have a formal cybersecurity and compliance program in place—as most affected organisations will—you will undoubtedly have many of DORA's requirements covered already. However, since DORA is more stringent in several areas than the widely accepted standards, there will inevitably be some gaps to plug.

This guide gives a brief overview of DORA and then dives into the main additional requirements that will be levied at financial institutions and their ICT providers over and above their existing cybersecurity and compliance programs. We're using ISO 27001 as a basis for this guide because it's the standard that is generally accepted in most EU countries.

What is DORA, and Does Your Organisation Have to Comply?

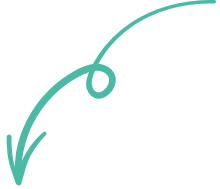
DORA is the new cybersecurity directive for the EU financial sector. It applies to 21 types of financial entities, including traditional financial institutions, FinTech companies, insurance intermediaries, and—critically—ICT providers that supply affected organisations. You can find a full list of affected organisations in Article 2.

The inclusion of third-party providers is a significant component of DORA. Between direct requirements placed on ICT providers and a broader focus on third-party risk management for financial services organisations, DORA aims to close gaps that have enabled significant data breaches from the sector in recent years.

The only exemptions DORA provides are for "very small enterprises," which it defines as financial entities with fewer than 10 employees and an annual turnover and/or balance sheet under €2 million. There's a larger exemption for intermediaries—companies with fewer than 250 employees and a turnover under €50 million or a balance sheet of under €43 million are exempt.

Timeline for DORA Compliance

Originally proposed in 2020, the Council of the European Union and the European Parliament formally adopted DORA in November 2022. Financial entities and their third-party IT providers now have until 17th January 2025 to comply with DORA before enforcement starts. After this, enforcement will be carried out by regulators in each EU member state, called "competent authorities." These authorities will have the power to request that financial entities take specific security measures and remediate vulnerabilities, and they'll be able to impose administrative and criminal penalties on entities that fail to comply. Each member state will decide its own penalties.



The 5 Pillars of DORA

The simplest way to understand DORA is through its five pillars. If you're an ISO 27001 veteran, you'll most likely spot some of the big differences right away—but we'll put them under the microscope in the next section, either way.

1) Risk management and governance

DORA makes a financial entity's leadership responsible for ICT management. Board members and senior leaders will define appropriate risk management strategies, ensure they are executed, and maintain a current understanding of the ICT risk landscape. Critically, leaders can and will be held personally accountable for their entity's DORA compliance.

The main requirements in this pillar are:

- Develop comprehensive ICT risk management frameworks
- Map ICT systems, including critical assets and functions, systems, processes, and providers
- Conduct continuous risk assessments on ICT systems
- Document and classify cyber threats and their steps to mitigate identified risks
- Conduct business impact analyses to assess how scenarios might affect operations
- Set levels of risk tolerance and inform the design of their ICT infrastructure
- Implement suitable cybersecurity protection measures
- Establish business continuity and disaster recovery plans for various cyber risk scenarios

2) Incident response and reporting

Financial entities must have systems to monitor, manage, log, classify and report ICT-related incidents. Depending on their severity, entities may need to report incidents to regulators and affected clients or partners. When critical incidents arise, financial entities will need to file three types of reports.

1. An initial report notifying authorities
2. An intermediate report on progress toward resolving the incident
3. A final report analysing the root causes of the incident.

3) Digital operational resilience testing

Entities will need to test ICT systems regularly to assess security and find vulnerabilities. They will also report on the results of testing and their plans to address any weaknesses to their competent authority.

Basic tests (e.g., vulnerability assessments) are required annually. Financial entities that play a critical role in the EU financial system will also need to complete threat-led penetration testing (TLPT) every three years.

4) ICT third-party risk management

The focus on third-party risk management is one of the things that sets DORA apart from cybersecurity standards that affected entities might already adhere to. DORA's requirements apply not only to financial entities—but also to the ICT providers that supply them.

Financial entities are expected to manage ICT third-party risk. When outsourcing, entities must negotiate contractual arrangements related to exit strategies, audits, and performance targets for accessibility, integrity, and security. **Financial entities cannot contract with ICT providers who don't meet these requirements.** Competent authorities will have the power to suspend or terminate contracts that don't comply with DORA's third-party risk requirements.

Financial entities must also map their third-party ICT dependencies and will be required to diversify their suppliers to ensure critical functions aren't too heavily dependent on a single provider.

5) Information and intelligence sharing

Financial entities must implement processes to learn f rom internal and external ICT incidents.

DORA encourages—but doesn't require—entities to participate in voluntary threat intelligence sharing. Any information shared must still be protected according to any relevant regulations. For example, personally identifiable information (PII) is still covered by General Data Protection Regulation (GDPR) requirements.

ISO 27001: A Solid Foundation for DORA Compliance

So, how do all of these DORA requirements compare to the more established (and well-understood) ISO 27001 standard?

First, there is a fundamental difference between DORA and ISO 27001:

ISO 27001 is an information security standard, while DORA focuses on operational resilience.

At its core, ISO 27001 helps organisations "*manage risks related to the security of data owned or handled by the company,*" while DORA aims to "*strengthen the IT security of financial entities*" with the ultimate goal of "*making sure that the financial sector in Europe is able to stay resilient in the event of a severe operational disruption*".

While similar, the two standards aren't identical and don't have identical objectives. If your organisation currently bases its cybersecurity practices on ISO 27001, you will need to account for DORA's additional requirements in your Information Security Management System (ISMS). For example, you'll need to consider DORA while identifying relevant legal and contractual requirements, interested parties, etc.

In other words, ISO 27001 provides a solid foundation for DORA compliance... but it doesn't take care of everything.

The "Good": How ISO 27001 Supports DORA Compliance

If your organisation already maintains compliance with ISO 27001, you'll have substantially less work ahead of you to reach DORA compliance ahead of the January 2025 enforcement date.

The main benefits of ISO 27001 for DORA compliance are:

An existing focus on risk management.

Both ISO 27001 and DORA place a significant emphasis on establishing and maintaining a risk management framework. If you're already following the ISO 27001 methodology, you'll have processes in place to identify and address information security risks. This will provide a strong foundation for compliance with DORA's risk management requirements, although keep in mind that because DORA focuses on operational resilience, you will be required to manage a broader range of risks.

Many security controls are already covered

Plenty of DORA requirements are addressed directly by ISO 27001 controls, and a brief mapping exercise should confirm your organisation's compliance in these areas. In particular, a formalised ISMS will cover typical controls and processes such as incident response plans, user access controls and management, common security policies, etc.

Cost and time savings.

As a consequence of the above, organisations that are already leveraging ISO 27001 will find the process of determining gaps and reaching DORA compliance considerably easier, faster, and less costly. Adapting an existing system—in this case, your ISMS—is inevitably faster and more efficient than building a new compliance program from scratch.

Evidence of compliance *and* security.

One of the greatest benefits of adopting an internationally recognised standard like ISO 27001 is that it makes it much easier to evidence compliance with new regulations whenever they arise. Auditors and regulatory authorities are already accustomed to reviewing programs based on ISO standards and are far more likely to accept them with a minimum of fuss... so long as they are properly implemented. DORA will be no exception—if you have a clearly defined and professionally implemented ISMS based on ISO 27001 that includes the new requirements, regulators and stakeholders will be far more confident in your organisation's digital resilience.

What About ISO 27002?

ISO 27002 is a set of best practices and control objectives that cover "key cybersecurity aspects" like user access controls, cryptography, human resource security, and incident response. There are several areas of DORA which, while not directly covered by ISO 27001, can be addressed using supplementary controls from ISO 27002.

Perhaps the most notable examples relate to business continuity and disaster recovery:

- ISO 27002 Control 5.29: Information Security During Disruption
- ISO 27002 Control 5.30: ICT Readiness for Business Continuity

While ISO 27002 controls are not required for ISO 27001 certification—and there's no certification available for ISO 27002—identifying aspects of ISO 27002 that contribute to DORA compliance is a sensible strategy. The two ISO standards are designed and intended to be used together, and ISO 27002 controls will be relatively easier to build into your existing ISMS compared to completely bespoke controls or controls recommended by other frameworks.

Full implementation of ISO 27002 is not mandatory for DORA compliance, but most of the controls recommended by ISO 27002 *are* relevant. Obviously, make your best judgement according to your organisation's needs, but we'd recommend at least considering ISO 27002 and implementing its controls as appropriate.

The "Not So Good": 4 Major Gaps in ISO 27001

As effective as ISO 27001 and 27002 undoubtedly are for managing information security risk, there are some clear gaps compared to what's required for DORA compliance. To ensure your organisation is fully DORA compliant ahead of the 17th January 2025 enforcement date, you'll need to:

- Map DORA-specific requirements to your existing ISMS.
- Conduct a gap analysis and assessment to determine your current DORA compliance status and identify areas where additional controls and practices are required.
- Update and extend your ISMS to incorporate these additional controls and processes.
- Develop additional documentation and evidence mechanisms for new controls and practices.

Since your ISMS is unlikely to precisely reflect the content of ISO 27001 and 27002, it's difficult to provide exact guidance on where you'll find gaps. Your controls and practices may be more extensive in some areas compared to the ISO standards—and potentially less extensive in others—based on your organisation's specific needs and circumstances.

However, if your ISMS is reasonably faithful to the letter of the ISO standards, you're likely to find gaps in four primary areas:

1. Business continuity
2. Security testing
3. Supply Chain Risk Management (SCRM)
4. Incident reporting

Gap 1: Business Continuity Management

DORA requires financial entities to protect operational continuity at all times, including during an incident. Note that DORA defines incidents more broadly than simply those caused by cyberattacks, so your organisation must be prepared to remain operational regardless of what happens.

To achieve this, you'll need to implement a comprehensive resilience framework that covers business continuity, disaster recovery, and crisis management. This goes beyond the scope of the ISO standards, *even if* you've implemented the additional ISO 27002 controls mentioned earlier.

While some of ISO 27001's controls and practices touch on Business Continuity Management (BCM), the standard doesn't provide a process for implementing or maintaining BCM. Of course, you're free to develop custom controls and standards to address these gaps in your organisation.

However, if you prefer to stay within the ISO family of standards, you may want to consider using ISO 22301, which governs Business Continuity Management Systems (BCMS). ISO 22301 can help you implement, maintain, and continuously improve business continuity processes across your organisation and/or for specific business functions.

Gap 2: Enhanced Security testing

This is one area where DORA is unambiguously stricter than the ISO family of standards. Regardless of how diligently you've implemented ISO 27001/2—or any other ISO standard—you may need to add some additional controls to supplement your existing ISMS in order to comply with DORA.

Most notably, DORA requires financial entities to undergo penetration testing. By comparison, ISO 27001 requires vulnerability management but doesn't explicitly require penetration testing.

Specifically, DORA requires financial entities to undergo:

- Resilience testing of ICT tools and systems at least annually
- Threat-led penetration testing at least every 3 years

Note that DORA specifies a wide range of testing mechanisms for the resilience testing requirement:

"...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."

Meanwhile, the threat-led penetration testing requirement is left more open to interpretation and future clarification. The current DORA text states that *"The precise scope of threat led penetration testing, based on the assessment of critical functions and services, shall be determined by financial entities and shall be validated by the competent authorities."*

While the exact testing requirements for DORA are not completely clear at this point, they are considerably more stringent than any ISO standard—and, in all likelihood, more stringent than the controls and practices most financial entities have in place.

Gap 3: (SCRM) Supply Chain Risk Management

SCRM has become a hot topic in recent years following a spate of high-profile cybersecurity breaches of large organisations. ISO 27001 and 27002 don't define a process for implementing third-party risk, so if your ISMS is limited to these standards, you've got some work ahead of you.

Again, it is possible to develop your own solution to the problem of supply chain risk. However, this is unlikely to be the best solution—regulators will increasingly expect organisations to adopt best practice solutions to widespread risks, so identifying a relevant and appropriate standard is more likely to be your best choice.

ISO 27036 covers information security for supplier relationships and: *"specifies fundamental information security requirements for defining, implementing, operating, monitoring, reviewing, maintaining and improving supplier and acquirer relationships."*

Alternatively, if you prefer to look outside the ISO family of standards, you could consider an alternative such as ComplianceForge's C-SCRM framework. This framework is explicitly designed with operational resilience (in addition to information security) in mind, making it clearly aligned with DORA's underlying principles.

Note that you don't have to use a specific framework to implement SCRM, but you do have to be able to prove that you have the necessary controls in place. This is often easier when using an established framework or standard because the justification for your process is inherent to it.

Gap 4: Incident Reporting

Implementing DORA compliance incident notification and communication practices is going to be a significant body of work for most financial entities.

Specifically, financial entities must report incidents classified as "major ICT-related incidents" to their competent authority. The reporting requirements are split into three "levels," each with its own timescale requirement:

1. An **initial notification** within 4 hours after classification (max 24 hours after discovery)
2. An **intermediate report** within 72 hours (and updates as needed to track the incident status)
3. A **final report** within a month specifying the root cause of the incident

While ISO 27001 does specify notification procedures, they are nowhere near rigorous enough to comply with DORA. Financial entities will need to ensure their detection, analysis, digital forensics, and incident response processes are sufficient to meet these new requirements. These processes will also need to be tested frequently to ensure they are sufficient in the event of a serious incident.

Summing Up (and Looking to the Future)

The good news for affected organisations that already use ISO 27001 as the basis of their ISMS is that DORA's requirements can be addressed without significantly altering your overall approach. If you're willing to adopt further standards from the ISO family, you can reach almost full compliance without concerning yourself with alternative standards organisations or developing your own.

That said, many financial entities and ICT providers will find the new SCRM and incident reporting requirements challenging, particularly if they haven't already begun designing and implementing the necessary controls and practices.

Looking further afield, following widely accepted standards like those issued by ISO is likely to be a good strategy going forward. With DORA and NIS2 coming into full force in the next 12 months—not to mention regulatory changes in the U.S.—it's clear that regulators globally are increasingly determined to levy strict cybersecurity and resilience requirements across a range of industries.

Building your organisation's cybersecurity and compliance programs on top of an established standard will position it to adapt to tightening regulations as needed and dramatically reduce the risk of serious cybersecurity incidents and breaches.