illumio

EBOOK

# Faster Attacks, Higher Stakes

## Microsegmentation and DORA Compliance in the Age of Frontier AI

# Table of Contents

# Introduction: DORA in force with more challenges than ever

The Digital Operational Resilience Act (DORA) has been in force for EU financial firms since January 17, 2025. The European Commission first proposed it in September 2020 to strengthen the EU financial sector against growing digital risk, and it was adopted in December 2022.

A lot has changed since then. Cloud adoption accelerated, and financial firms became far more dependent on connected technology providers. At the same time, cyberattacks grew faster and more automated.

Now frontier AI is raising the stakes again. The European Central Bank has warned that these models can find software vulnerabilities and generate working exploits at unprecedented speed, compressing the time between discovery and exploitation. At the same time, financial firms face more European Union (EU) rules, including the AI Act and new demands tied to data, technology, and third-party risk.

DORA is no longer a future deadline. It's an active requirement for financial entities across the EU and for the information and communication technology (ICT) providers that support them. And it applies in a technology and threat landscape that keeps shifting.

The question has changed. It's no longer "What is DORA?" It's "Can you prove it?" And the proof regulators want is operational, not paperwork.

Financial firms must now show that they understand ICT risk, manage third-party dependencies, report major incidents, and keep critical services running during disruption.

This matters in a financial system built on shared infrastructure. Firms rely on cloud services, payment platforms, data centers, software providers, and managed service providers.

DORA raises the bar from planning for recovery to proving resilience in practice. Policies and reports still matter. B ut firms also need clear visibility, tested controls, strong segmentation, and fast containment when disruption begins.

This ebook explores what DORA demands in practice — and how microsegmentation can help you reduce risk, protect critical services, and prove operational resilience when regulators ask.

# Who must comply with DORA

DORA applies to a wide range of financial entities in the EU, not just banks. It covers firms across payments, trading, securities, investment services, and crypto-asset services.

That broad scope reflects how finance works today. One firm's ICT risk rarely stays with that firm — it travels through the payment, trading, and settlement links that tie institutions together. Resilience depends on knowing where those links run and managing them deliberately. The figure below shows the entity types DORA covers.

## DORA applies to a wide range of financial sector businesses within the EU:

- **Credit institutions (banks).** All types of banks, including retail, commercial, and investment banks.
- **Payment service providers.** Entities providing services like credit transfers, direct debits, and payment cards.
- **Electronic money institutions.** Companies issuing electronic money and handling e-wallets.
- **Investment firms.** Firms providing investment services and activities.
- **Crypto asset service providers.** Entities involved in the issuance, offering, and exchange of crypto assets.
- **Central securities depositories (CSDs).** Institutions that hold securities and facilitate their transfer.
- **Trading venues.** Including regulated markets, multilateral trading facilities (MTFs), and organized trading facilities (OTFs).
- **Central counterparties (CCPs).** Entities that enable trading in derivatives and other financial instruments.

# The third parties that keep finance running

Service providers play a critical role in financial resilience. Under DORA, firms must know which third-party ICT providers support critical or important functions. They must also know how those providers connect to internal systems.

The next question is impact. What happens if a provider fails, is attacked, or becomes unavailable?

Third-party risk is no longer just a vendor-management issue. It's an operational resilience challenge. Firms need clear visibility into where dependencies exist and how providers connect to critical services. They also need to know how fast access can be limited if disruption begins.

- **Cloud service providers**
- **Data center services**
- **Managed service providers (MSPs)**
- **Software providers**
- **Telecom services**
- **Payment processing services**
- **IT support services**
- **Infrastructure as a service (IaaS) firms**
- **Platform as a service (PaaS) firms**

# DORA's five pillars are still central

DORA is built around five core pillars:

- ICT risk management
- ICT-related incident reporting
- Digital operational resilience testing
- ICT third-party risk management
- Information and intelligence sharing

Together, the pillars cover how firms manage ICT risk day to day, how they report major incidents, how they test their defenses, how they oversee the providers they depend on, and how they share threat intelligence with peers.

The pillars still define the regulation. But the focus has shifted. Financial firms now have to put them into practice.

That means knowing which systems support critical services. It means seeing how applications, workloads, users, and third parties connect. It also means testing whether controls work under pressure.

When something goes wrong, firms must respond fast enough to limit disruption. The five pillars are not just compliance categories. They are the basis for proving that critical services can withstand failures, cyberattacks, and supply-chain disruption.

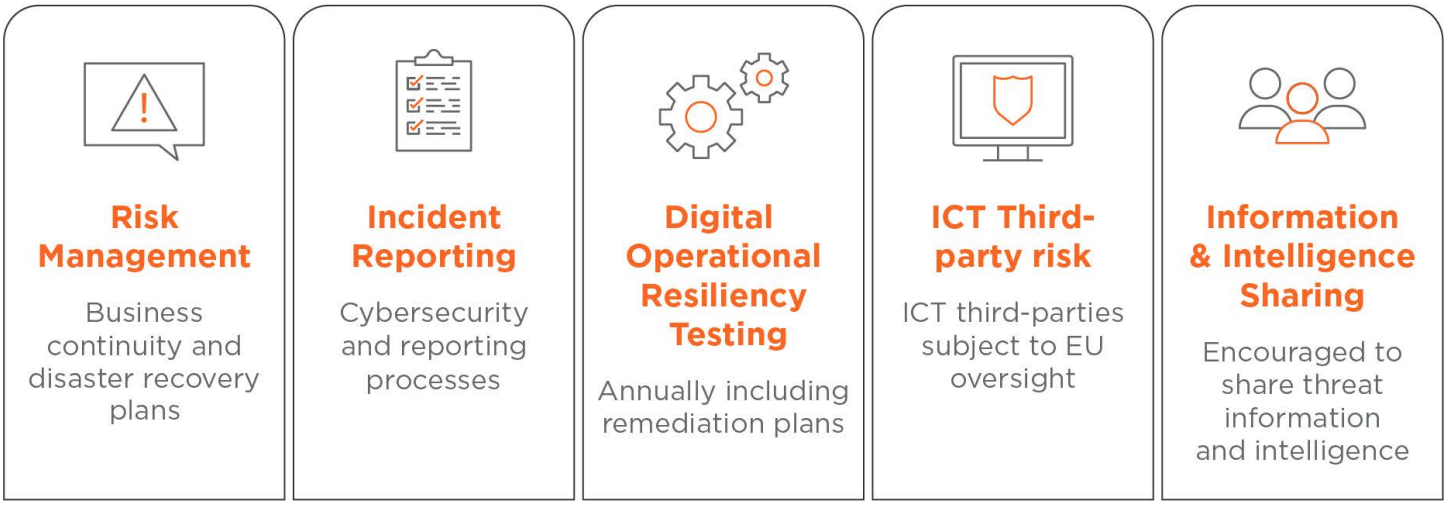



Figure 1: DORA's five pillars and requirements

## DORA is being tested in practice

The first phase of DORA enforcement made one point clear: resilience depends on connected systems, shared services, and third-party providers.

In 2025, EU financial entities reported 3,383 major ICT-related incidents under DORA. One-third had a cross-border impact, and one-third came from failures linked to third parties. System failures and external events caused most incidents; cybersecurity accounted for about 10%.

The findings reinforce a core point of DORA. Resilience does not depend on preventing every incident. It depends on finding disruption quickly, containing the impact, and keeping critical services running.

They also show how quickly disruption moves across borders and through the financial system, which is why operational resilience can't be treated as an internal-only problem.

Financial firms rely on cloud platforms, software vendors, data centers, payment processors, managed service providers, and other ICT partners. These providers are essential to daily operations. They can also create concentration risk when many firms rely on the same systems or services.

The cyberthreat landscape is changing too. AI and automation are helping attackers find vulnerabilities faster, scale attacks, and exploit weaknesses with less effort.

DORA responds to this reality. It pushes firms to map their dependencies, test resilience, and prepare for disruption across the ICT ecosystem.

## Vulnerabilities and risks

Risk in the financial sector rarely stays in one place. It moves between systems, providers, and firms.

Financial firms face both digital and operational risk. Ransomware, zero-day exploits, and supply-chain attacks can disrupt critical services. So can system outages and failures at technology providers.

Cloud services and connected infrastructure can spread the impact of an incident. A problem in one system can affect other systems that depend on it.

Attackers are also moving faster. Automation and AI can help them find weak points and scale attacks. Greater connectivity can give them more lateral paths from a vulnerable or compromised system.

These risks are harder to contain. A disruption at a shared provider can affect many firms. Complex cloud, hybrid, and third-party environments can also hide critical dependencies.

This is what DORA asks firms to plan for: know your connections, manage the risk inside them, and be ready to limit disruption the moment something goes wrong.

## How frontier AI raises the stakes

Frontier AI is changing the speed of cyber risk. Models like Mythos show how quickly AI can find vulnerabilities and map weaknesses. They can compress work that once took specialist teams much longer.

For banks, that creates a new problem. The vulnerability backlog may grow faster than teams can patch it.

That matters under DORA because resilience is not built on perfect prevention. EU banks must keep critical services running when systems fail or vendors are disrupted. They must also prepare for attackers that can move faster than normal remediation cycles.

The question is no longer just, "How fast can we patch?" It's, "If this weakness is exploited, how far could the disruption spread?"

This is where AI risk becomes an operational resilience issue. An AI-enabled attacker could move across a connected banking environment before normal processes catch up.

Payment systems, core banking applications, customer-facing channels, cloud services, and third-party ICT providers may all sit on the same risk path.

DORA pushes banks to prove they can manage that risk. They need to know which systems support critical functions and how those systems connect. They also need to limit unneeded access and test whether controls can contain disruption.

AI makes this work more urgent. Banks can't count on a clean vulnerability backlog, so they need a clear view of their blast radius — how far an attacker could travel from a single compromised system — and the ability to shrink it quickly.

## When one firm's disruption becomes everyone's problem

The financial sector is a prime target because disruption can reach far beyond one firm.

The 2023 ransomware attack on the Industrial and Commercial Bank of China (ICBC) is one example. The attack disrupted systems used to process U.S. Treasury trades and repo financing.

The impact reached one of the world's most important financial markets. It showed how one incident can ripple across the financial system.

That is the type of risk DORA is designed to reduce.

Operational resilience is not just about stopping attacks. It's also about limiting the impact when attacks, outages, or third-party failures occur. Firms need to keep critical services running, contain disruption quickly, and recover with confidence.

## From compliance to proof of resilience

DORA is pushing firms beyond written compliance. Policies still matter. Documentation still matters. But regulators now expect firms to show that controls work.

Threat-led penetration testing is one way to prove that. It tests whether firms can withstand realistic attacks and recover from them.

That creates a practical challenge. Firms need to show that they understand their environment. They need to know which assets support critical services. They also need to contain an incident before it spreads.

Firms must also show that access controls, segmentation policies, incident response, and recovery plans work under real conditions.

This is where resilience becomes measurable.

- Can you see how critical systems connect?
- Can you identify risky or unneeded communication?
- Can you isolate an affected workload without taking down the business?
- Can you show regulators that your controls reduce real risk?

DORA turns these questions into operational requirements.

## Where firms are struggling

For many financial firms, the hardest part of DORA is not understanding the regulation. It's understanding the environment.

Modern finance depends on a web of applications, workloads, cloud platforms, data centers, vendors, and third-party ICT providers. Some connections are well documented. Many are not.

That creates several challenges:

- Firms may not have a complete view of how critical services depend on third parties.
- Core banking systems may connect to more vendors, applications, and services than security teams realize.
- Legacy systems may still support critical processes but lack modern controls.
- Cloud and hybrid environments can make dependencies harder to map.
- Incident response teams may not know what can be safely isolated during an active event.

Third-party risk is one of the biggest DORA implementation challenges. Firms can assess vendors, review contracts, and request proof of controls. But they can't fully control a third party's environment.

They can control how their own environment connects to those providers.

That makes visibility and segmentation essential. Firms need to know what is connected, what should be connected, and what can be cut off if risk rises.

# Why microsegmentation matters for DORA

Microsegmentation helps firms turn DORA requirements into working controls.

Microsegmentation divides an environment into small, isolated zones and controls what is allowed to pass between them. Rather than trusting everything inside the network perimeter, each workload, application, and service can reach only what it genuinely needs. When something is compromised, the damage stops at the segment boundary instead of moving freely across the environment.

It gives teams a clearer view of how workloads, applications, users, devices, and third-party services communicate. That view helps them map dependencies, spot risky connections, and find the systems that support critical business services.

Teams can then limit unneeded access. They can separate critical systems from less trusted parts of the environment. They can also restrict third-party connections to only what is needed.

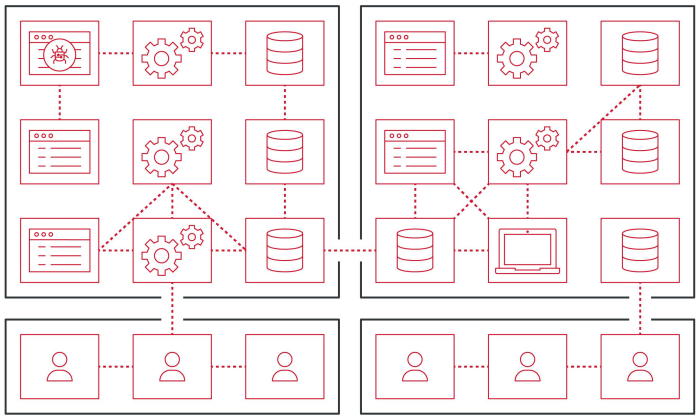
Most importantly, microsegmentation helps contain disruption.

If a workload is compromised, teams can isolate it quickly. If a third-party connection becomes risky, they can limit access. If ransomware starts to spread, segmentation can shrink the blast radius and help keep critical services running.

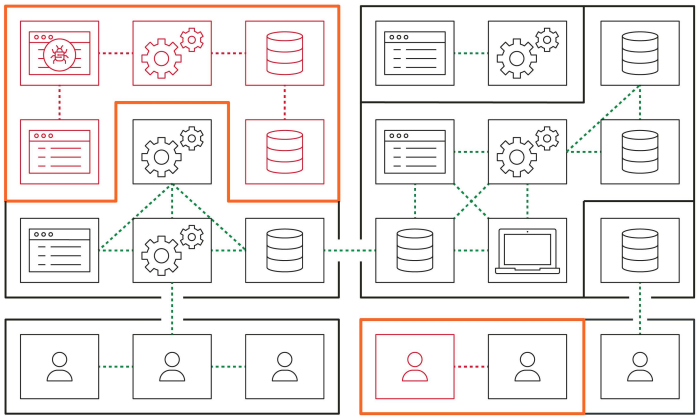
This directly supports several DORA goals:

- Identify and monitor ICT assets, connections, and dependencies
- Document network connections and data flows
- Restrict access based on criticality and risk
- Segment ICT systems and networks
- Log traffic activity for better detection and investigation
- Temporarily isolate affected ICT assets during incidents

DORA asks for resilience you can demonstrate. Microsegmentation helps resilience show up in daily operations — in the connections you allow, the access you remove, and the systems you can isolate on short notice.



WITHOUT SEGMENTATION



WITH SEGMENTATION

## DORA foundation: NIST Cybersecurity Framework and ISO 27001

The diagram below shows how the NIST Cybersecurity Framework and ISO 27001 align with DORA, so you can see where controls you already run support DORA requirements.

ISO 27001 inspired the information and communication technology (ICT) risk management portion of DORA. The earlier framework is flexible, pragmatic, and risk-based; DORA mirrors this detailed approach.

DORA also aligns closely with the National Institute of Standards and Technology (NIST) cybersecurity framework functions. The NIST framework covers the complete security lifecycle:

- **Identify:** Assets, systems, dependencies, and risks.
- **Protect:** Implement controls to safeguard assets and mitigate risks.
- **Detect:** Identify events that impact assets.
- **Respond and recover:** Build capabilities to mitigate, isolate, analyze, and recover from incidents.

Any work you've done toward ISO27001 and NIST compliance sets a good base for DORA. It also shows how well-grounded practices can lead into resilient frameworks.

If you are already working toward ISO 27001 compliance, you can boost your DORA efforts by adding the required controls. Auditors can check ISO 27001 compliance and, at the same time, whether your information security management system (ISMS) meets your security needs and aligns with DORA mandates.

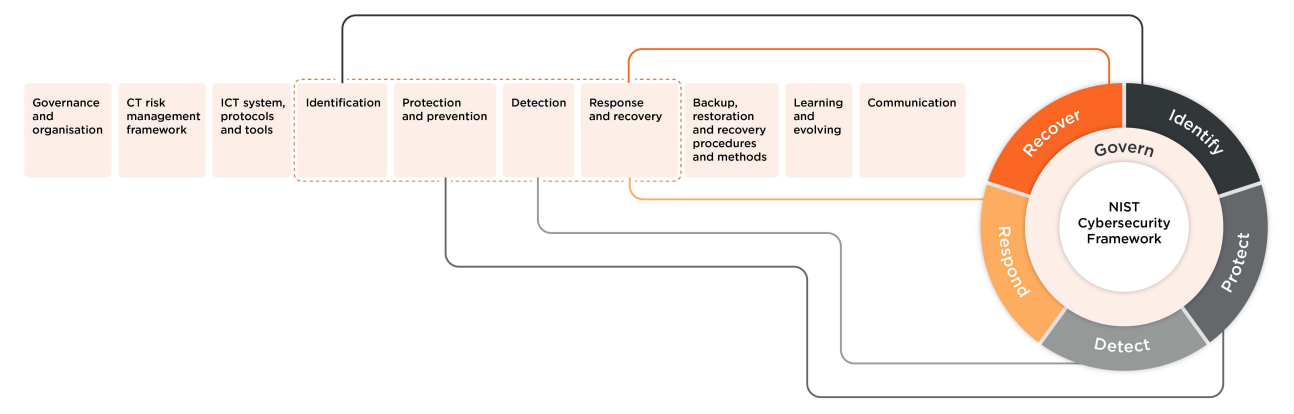



Figure 2: NIST Cybersecurity Framework and ISO 27001 alignment with DORA

# Network segmentation under DORA

DORA's network segmentation rules are meant to boost ICT security by isolating parts of your network. This approach limits unsanctioned access, contains breaches, and reduces risk.

DORA compliance starts with three key elements:

- Clear visibility
- Well-mapped dependencies
- Effective segmentation practices

These proactive measures help contain breaches, boost operational resilience, and align with DORA's main objectives.

In the past, segmentation was often costly and burdensome. But more modern approaches, especially those that incorporate Zero Trust principles, can simplify the process. By focusing on workload management and using metadata-based policies, you can segment your networks and hybrid clouds without changing architectures. These proactive measures help contain breaches, boost operational resilience, and align with DORA's main objectives.

DORA doesn't call out Zero Trust by name. The EU left it out by design to give firms some flexibility when choosing a compliance strategy. That said, DORA mandates are closely aligned with a Zero Trust approach. That's because they focus on blocking unsanctioned access and containing breaches — key goals of Zero Trust.

## DORA objectives, requirements, implementation strategies, and benefits

### Objective:

Enhance ICT security by minimizing unauthorized access risks and containing potential breaches within isolated network segments.

### Key requirements:

- **Segregation and segmentation:** Implement network segregation and segmentation based on the criticality, classification, and risk profile of ICT systems and networks.
- **Dedicated networks:** Establish separate and dedicated networks for critical ICT asset administration to prevent unauthorized access.
- **Access controls:** Apply robust network access controls to ensure that only authorized personnel can access sensitive or critical network segments.
- **Encryption:** Use encryption to secure network connections, especially those involving critical or sensitive data, to maintain confidentiality and integrity in transit.

### Implementation:

- **Mapping and visualization:** Effectively manage and identify potential vulnerabilities by mapping and visualizing network segments.
- **Risk-based approach:** Segregate networks by assessing the risk profile and criticality of systems and data to apply appropriate security measures.

### Benefits:

- **Enhanced security:** Limit the spread of breaches and protect sensitive data.
- **Improved cyber resilience:** Isolate critical systems for continuous operations during security incidents.

# DORA and the essential role of microsegmentation

When looking into how segmentation helps meet DORA rules, focus on the benefits. Start by mapping your technology dependencies and documenting data flows.

These first steps are vital to understanding the functions, needs, and dependencies of your environment. They help you identify risks, manage them, and keep things running smoothly.

Here's a summary of DORA guidelines and how microsegmentation applies.

## Identification

**DORA Regulatory Technical Standards**

**Section III, Article 4:** Identify and monitor the links and interdependencies among ICT assets.

**Section VI, Article 13:** Document all the network connections and data flows.

**Microsegmentation use cases**
- Asset mapping and visibility

You must be able to see all interactions across your environment. To this end, you should map your assets and spot potential risks. Asset mapping and visibility provide the insight you need to build cyber resilience and meet DORA mandates.

## Protection and prevention

**DORA Regulatory Technical Standards**

**Section V, Article 11:** Implement access restrictions, supporting the protection requirements for each level of classification.

**Section VI, Article 13:** Segregate and segment ICT systems and networks based on criticality, importance, and classification.

**Section V, Article 10:** Deploy mitigation measures to address vulnerabilities.

**Microsegmentation use cases**
- Critical asset protection
- Ransomware containment
- Environmental separation
- Vulnerability risk reduction

You must protect your most valuable assets and limit access to workloads based on a few key factors. These may include how critical or important those assets are or how they're classified. Limiting access is essential. It keeps people and systems productive while boosting cyber resilience.

But you can't discern what should and shouldn't have access if you don't know where your critical applications are running. In today's dynamic, hybrid, multi-cloud environments, that's easier said than done; modern workloads can run almost anywhere — in the cloud, data centers, or endpoints.

Once you have mapped out your workloads, you can:
- Set policies
- Validate them
- Quickly deploy to segment key workloads

Protecting critical assets lets you segment and separate ICT systems for DORA compliance.

## Detection

**DORA Regulatory Technical Standards**

**Section V, Article 12:** Log events related to network traffic activities.

**Microsegmentation use cases**
- Asset mapping and visibility

You must be able to see all interactions across your environment. To this end, you should map your assets and spot potential risks. Asset mapping and visibility give you the insight you need to build cyber resilience and meet DORA mandates.

## Response and recovery

**DORA Regulatory Technical Standards**

**Section VI, Article 13:** Temporarily isolate ICT assets

**Microsegmentation use cases**
- Incident response and recovery

You must contain attacks by quarantining compromised network workloads. Isolating infected assets stops attacks from spreading across the network and hybrid cloud. After the attack, you can secure compromised assets and safely restore them to prevent reinfection. Microsegmentation can ease the incident response and recovery process, helping to isolate ICT assets, boost cyber resilience, and achieve DORA compliance.

# Next steps: operationalize resilience

DORA is a practical test of resilience, and it's one your teams have to be able to pass on any given day.

That test has a practical starting point. Map which systems support each critical service and how third-party providers connect to them. Remove the access that those services don't need. Then rehearse containment, so teams know what can be safely isolated during a live incident. A compliance checklist can't answer those questions; only controls that work in real environments can.

Microsegmentation helps firms take that next step. It gives teams visibility into risk. It also helps them limit unneeded access and isolate systems during an incident.

In a connected financial system, resilience depends on speed and control. The faster you can see risk, limit access, and stop disruption from spreading, the better prepared you are to meet DORA's expectations — and to protect the services your customers depend on.

Illumio helps financial firms turn these expectations into controls that work every day. Illumio Segmentation maps how your workloads, applications, and third-party services communicate, then enforces policies that limit access to only what a critical service needs — across data centers, cloud, and endpoints. Illumio Insights adds AI-driven detection, so your teams can spot lateral movement and isolate an affected system quickly, and it captures the traffic records you can use as evidence for regulators.

To see how Illumio supports DORA compliance, visit **illumio.com/dora**