illumio

EBOOK

Strategies for DORA Compliance: The Key Role of Microsegmentation

Table of Contents

Introduction: Meet DORA

A stable financial system is vital to a healthy global economy. As the financial markets rely more than ever on digital systems, managing threats and reducing disruptions has never been more critical. At the same time, financial firms — and the complex digital supply chain that supports them — face a growing array of cyberattacks.

It's a challenge European leaders know all too well. In November 2022, the EU parliament passed the Digital Operational Resilience Act (DORA). The act, which applies to financial firms and their critical service providers, creates a regulatory framework for managing and recovering from digital threats. The goal: keep finance running smoothly amid a rising tide of risk.

DORA applies not just to banks, but to a wide range of financial firms in the EU. (See Figure 1 on Page 3 for a full list.) Also on the hook are critical service providers such as cloud providers, data centers, and managed service providers (MSPs). (See Figure 2 on Page 4.) Picture a major cloud service provider under threat of outage or cyberattack. Under the new rules, an EU bank using that platform for critical applications must have a plan to manage the incident with as little disruption as possible.

This e-book explores DORA, why it matters, and the role of microsegmentation in compliance efforts.

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.

Figure 1: Types of businesses that must comply with DORA

Service providers play vital roles in the finance sector. Under DORA, they must maintain operational resilience so that their critical services always function. Here are those named in the DORA rules:

- **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**

Figure 2: Financial service providers that are subject to DORA

DORA's five pillars

DORA is based on five key areas, as shown in Figure 3.

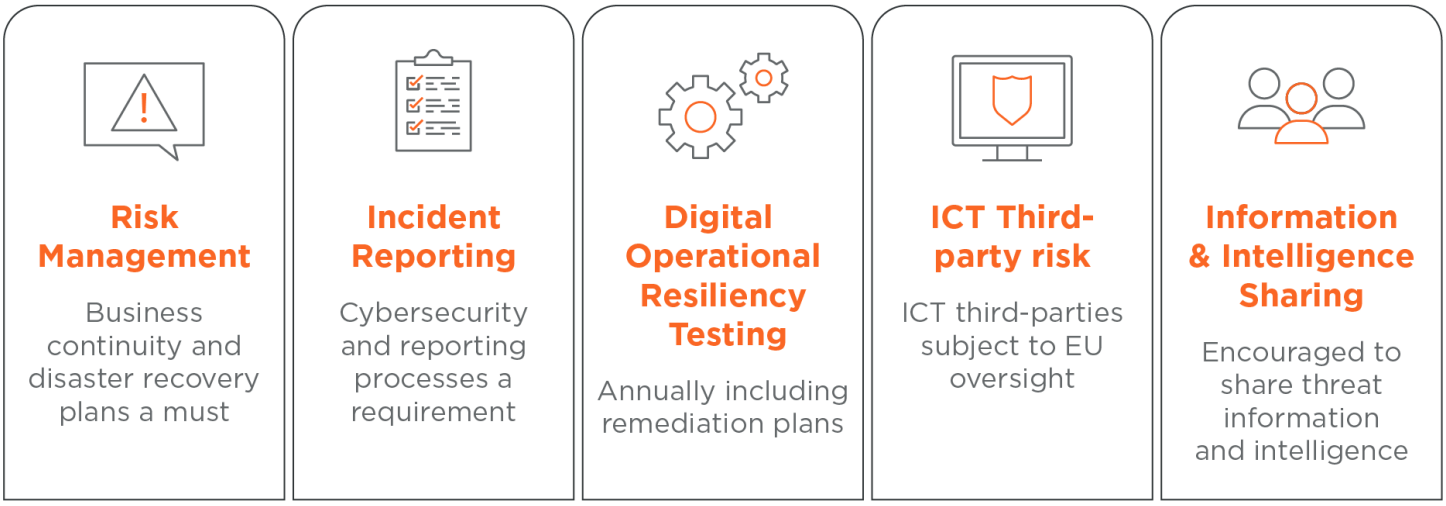


Figure 3: DORA's five pillars and requirements

Our interconnected global financial system

Banks rely on connected digital systems to handle transactions, manage accounts, and provide online banking. If even one bank is attacked, the entire global financial system could suffer the effects.

That's why DORA is a big step towards a safer, more resilient global financial system. Its goals are threefold:

- Help the EU's financial sector lead in digital technology
- Support innovative European companies
- Boost security and trust in the global financial system

Vulnerabilities and risks

In an April 2024 report, the International Monetary Fund (IMF) warned of the growing threat that cyberattacks pose for global financial systems. For one, these attacks are becoming more advanced. And all too often, they are aimed squarely at key parts of the financial world. These include not just banks, but payment systems, financial markets, and others.

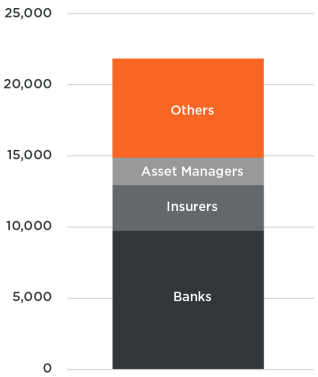
Over the last 20 years, the financial sector has faced more than 20,000 cyberattacks, the report found. All told, that has added up to more than $12 billion in global losses. During that time, the risk of an attack has steadily increased and losses have soared.

IMF Warns: Global Financial Stability Under Thread from Cyber Risks[1]

Attractive target

The financial sector has suffered more than 20,000 cyberattacks, causing $12 billion in losses, over the past 20 years.

Financial sector cyber incidents
(number, 2004-23)



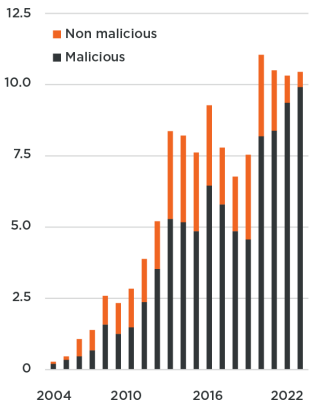
Financial sector losses
(billions of US dollars, 2004-23)

Source: Advisen cyber loss data and IMF staff calculations.

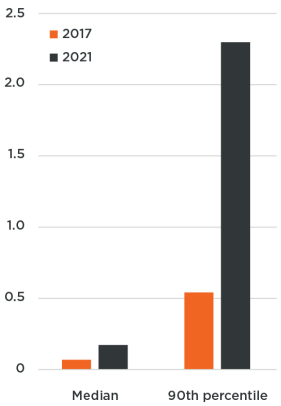
Greater threat

The risk of suffering a cyberattack and extreme losses from it has increased.

Cyber incidents
(thousands)



Estimated maximum firm loss
(billions of US dollars)



Sources: Advisen Cyber Loss Data; Capital IQ; and IMF staff calculations.
Note: Panel 1 cyber events are classified according to Advisen. Delayed reporting may lead to the underestimation of cyber events in more recent periods. Panel 2 is based on the estimated posterior density function of the highest loss of all firms within a year.

IMF

The report pointed to a number of factors behind the increase. Among them:

- **Increased digitization.** More digital services. More online transactions. Heavier reliance on cloud computing.
- **Improved attacker techniques:** Highly sophisticated methods from advanced persistent threat (APT) actors. Automated attacks that use AI.
- **Exploits.** Zero-day vulnerabilities and targeting software supply chains.

[1] https://www.weforum.org/agenda/2024/05/financial-sector-cyber-attack-threat-imf-cybersecurity/

- **Ransomware advances:** Rise of ransomware-as-a-service (RaaS). Higher ransom demands. More frequent attacks.
- **Greater connectivity:** More IoT devices and interconnected networks creating new points of attack.
- **Weak security posture:** Poor security in small and medium businesses. Slow adoption of best practices.
- **Economic and political conflicts:** Cyberattacks fueled by geopolitics and financial gain.
- **The human factor:** More phishing and social engineering. Low security awareness.
- **Regulatory challenges:** Outdated rules. Clashing security standards.
- **Advanced tools:** State-of-the-art hacking tools available on the dark web. Better collaboration among cybercriminals.

What it's costing us

The average cost of a data breach stands at $6.08 million. But the most severe breaches can cost far more. And the worst of them can ripple throughout the global financial system.

That was the case in two major attacks on the financial sector, one in 2016 and the other in 2023. While each was unique, they both served as vivid reminders that an attack can have profound, wide-ranging impacts.

Ransomware attack on ICBC: Disruption of the $26 trillion U.S. Treasury market

On November 9, 2023, the Industrial and Commercial Bank of China (ICBC), one of the world's largest banks by total assets, faced a major ransomware attack.

The attack, believed to be the work the Lockbit group, [2] went after ICBC systems used to process U.S. Treasury trades and repurchase agreement financing (also known as repo financing).[3] It blocked ICBC from core systems, bringing trading and payments to a standstill.

The shock echoed through the $26 trillion U.S. Treasury market. It also raised widespread concerns about the financial sector's frailty. Above all, ICBC is a stark example of how the breach of a single bank can ripple throughout the broader financial ecosystem.

How the Bangladesh financial breach redefined cybersecurity in global finance

The 2016 Bangladesh Bank breach is a pivotal event in global finance. In that attack, thieves stole $81 million from the bank's account at the Federal Reserve in New York.

This incident exposed glaring flaws in the global banking system. It also raised alarms about whether current safeguards are enough to combat a wave of new threats.

The breach prompted urgent calls for reforms. This led to new laws governing the Society for Worldwide Interbank Financial Telecommunications' (SWIFT) secure payment messaging system.

More broadly, the incident served as a wake-up call heard around the globe. A flurry of new rules aimed at preventing similar breaches forced banks to beef up their security controls and do business in a more transparent manner.[4]

[2] (Trend Micro) (Cyber.gov.au).

[3] U.S. Securities and Exchange Commission (SEC): SEC Glossary

[4] The Bangladesh Bank Heist and Its Global Ramifications" published in the Journal of Financial Crime (Emerald Publishing)

Shifting from business continuity to operational resilience

Business continuity planning has long been a cornerstone of the financial services sector. This discipline focuses on recovering *after* outages and other failures. DORA is all about being prepared *before* anything happens. Instead of just planning for recovery, DORA shifts the focus to resilience.

How DORA evolved from PCI-DSS, SWIFT, and NIS2

The financial sector is already one of the most regulated. PCI-DSS, SWIFT, and the Network and Information Security Directive 2 (NIS2) are just a few of the standards they must follow.

DORA expands the scope beyond data protection and access controls. It enhances resilience by addressing a wider range of areas, such as:

- Risk management
- Incident response
- Business operations
- Third-party risk
- Service supply chain dependencies

Which has precedence, DORA or NIS2?

NIS2 is an EU directive that aims to strengthen cybersecurity. It updates and expands the original NIS mandates[5] to cover more sectors and improve resilience against cyber threats. Focus areas include risk management, incident reporting, and cooperation among member states.

NIS2 and DORA serve different purposes. NIS2 sets cybersecurity rules for critical sectors such as energy, transport, health, and banking. It offers a broad framework for almost any industry. DORA, on the other hand, is designed to boost digital resilience within the financial sector.

For financial firms in the EU and key service providers (see Figure 2 on Page 4), DORA takes priority.

Member states must implement NIS2 by January 1, 2025. DORA requires member states to integrate its rules into national laws and begin enforcing them by January 17, 2025.

Dora, PCI-DSS, and NIS2: key differences

	SWIFT Customer Security Programme	PCI-DSS	NIS2	DORA
Purpose	Secure transactions between banks around the world.	Secure payment card transactions around the world.	Strengthen cybersecurity risk management, incident reporting, and cooperation among EU member states and beyond.	Manage and recover from digital threats to minimize disruptions to the EU financial system.
Scope	Narrow: protect SWIFT payments infrastructure	Narrow: rules center on protecting customer data and payment card information	Broad: targets network and information security across multiple critical sectors	Mid: Focuses on financial institutions and related service providers
Enforcement	None	PCI Security Standards Council	National authorities across industry sectors in member states	European regulatory bodies
Enforcement deadline	n/a	October 18, 2024	January 1, 2025	Jan. 17, 2025

[5] European Commission - NIS Directive

DORA foundations: NIST cybersecurity framework and ISO 27001

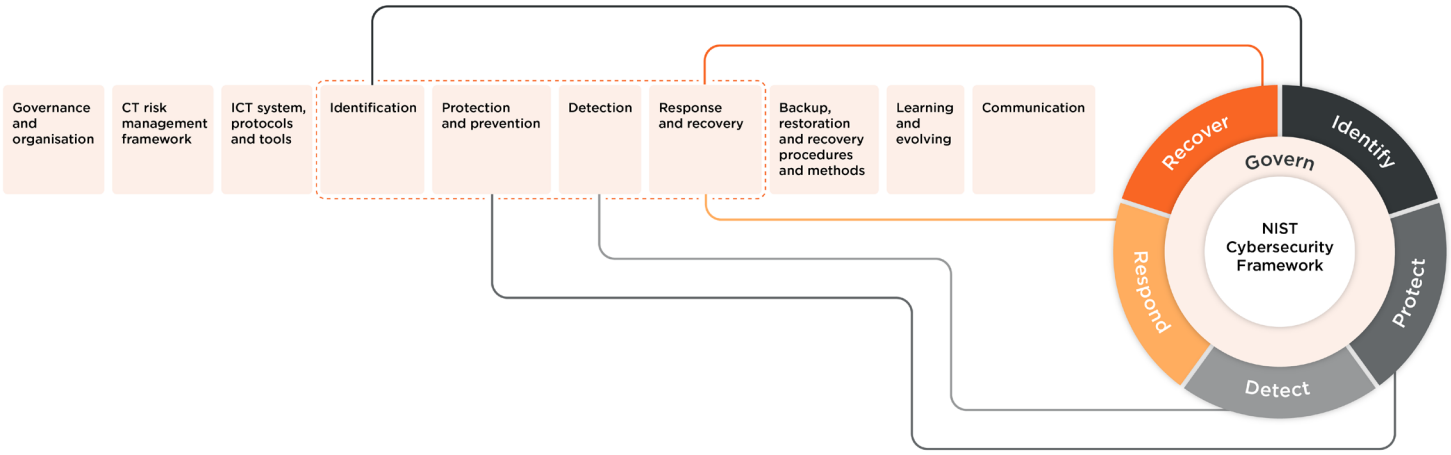
ISO 27001 inspired the information and communication technology (ICT) risk management portion of DORA. The earlier framework is flexible, pragmatic, and risk-based; DORA mirrors this detailed approach.

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 just goes to show 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.



Mapping ISO 27001 and the NIST Cybersecurity Framework are useful for DORA compliance; they follow similar patterns.

Leading with threats, not compliance

For effective DORA compliance, take a threat-led approach rather than going through compliance checklists. In other words, focus on protecting your most critical assets. This approach can simplify your security efforts by targeting specific, actionable risks. With continuous testing and strong leadership support, the threat-led approach can provide clear, measurable results to keep you ahead in a fast-changing threat landscape.

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 for securing 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 helps 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: I**dentify 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 asset

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.

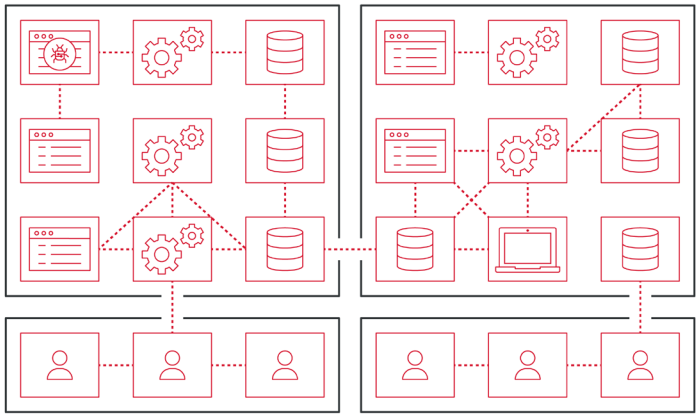
Next steps

DORA is a big step toward securing the financial sector in a fast-changing threat landscape. The global financial system is more interconnected than ever — and will always be a prime target for attackers. That makes DORA more than a regulatory directive. It's a strategic imperative.

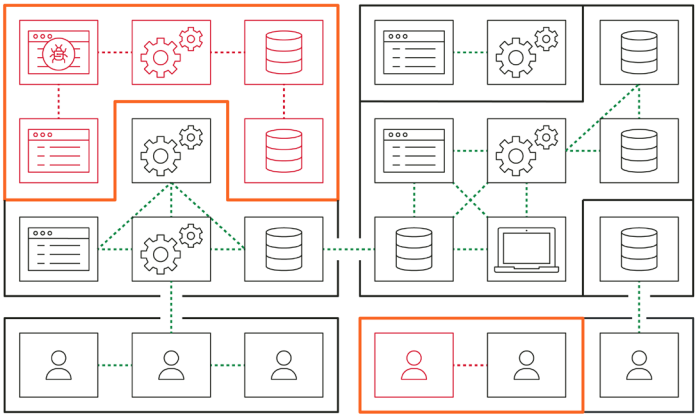
Microsegmentation, as outlined in this guide, offers a potent solution to meet DORA mandates. As part of a broader zero-trust approach, it can enhance visibility, safeguard access, and contain breaches. Taking this approach, financial firms can build resilience, reduce risk, and maintain trust in the global financial system.

Microsegmentation can help you comply with DORA in three key ways:

- **Understand risk.** Visualize all communication and traffic, both known and unknown, between workflows, devices, and the internet.
- **Define security tools.** With every change, automatically set granular segmentation policies to control unneeded and unwanted communications.
- **Contain attacks.** Proactively isolate high-value assets. Reactively isolate compromised systems during an active attack to stop the spread.



WITHOUT SEGMENTATION



WITH SEGMENTATION

To learn more about Illumio Zero Trust Segmentation and how it can help you comply with DORA, visit **illumio.com/dora**

About Illumio

Illumio, the Zero Trust Segmentation Company, stops breaches from spreading across the hybrid attack surface. The Illumio ZTS Platform visualizes all traffic flows between workloads, devices, and the internet, automatically sets granular segmentation policies to control communications, and isolates high-value assets and compromised systems proactively or in response to active attacks. Illumio protects organizations of all sizes, from Fortune 100 to small business, by stopping breaches and ransomware in minutes, saving millions of dollars in application downtime, and accelerating cloud and digital transformation projects.