ZERO. Networks

PLAYBOOK

The Comprehensive DORA Compliance Guide

A Blueprint for Meeting Regulatory Requirements & Boosting Cyber Resilience

Get the 30-day roadmap to achieving DORA compliance by focusing on four key areas: automated microsegmentation, identity segmentation, RPC firewall, and secure remote access. Delve into the importance of DORA, understand the regulatory objectives, and explore how Zero Networks offers a holistic solution for ensuring compliance.

Introduction to DORA and the need for automated microsegmentation

The Digital Operational Resilience Act (DORA) is not just another legislative structure. It's a crucial step in the European Union's mission to protect the financial sector from escalating cyber threats. DORA's main aim is to bolster financial services' operational resilience and cybersecurity, ensuring they can withstand and recover from technological disruptions. The growing complexity of cyber-attacks and financial services' heavy reliance on digital infrastructure underscore the importance of this regulation.

Attackers are progressively capitalising on lateral movement within enterprise networks as cyber threats advance. This technique allows malevolent attackers to traverse a network, transferring from one system to another after exploiting an initial access point. Bad actors want to establish a foothold and access valuable data or systems, which frequently results in significant breaches or disruptions. Lateral movement presents a distinctive obstacle due to its use of valid network functionalities to obscure malicious operations, thereby complicating detection and prevention.

Prevention is paramount in cybersecurity as it blocks threats before they inflict damage, unlike detection and response, which manage breaches postoccurrence. Effective prevention minimises the risk of attacks and reduces the extensive costs and operational disruptions associated with post-breach recovery, maintaining a robust security stance and safeguarding business continuity.

In the complex world of cybersecurity, microsegmentation emerges as a game-changing innovation. It allows organisations to control network traffic and isolate computational resources, significantly reducing the risk of lateral movement by cyber threats. This approach aligns perfectly with the objectives of DORA and offers an advanced solution for protecting the network infrastructure of financial institutions.

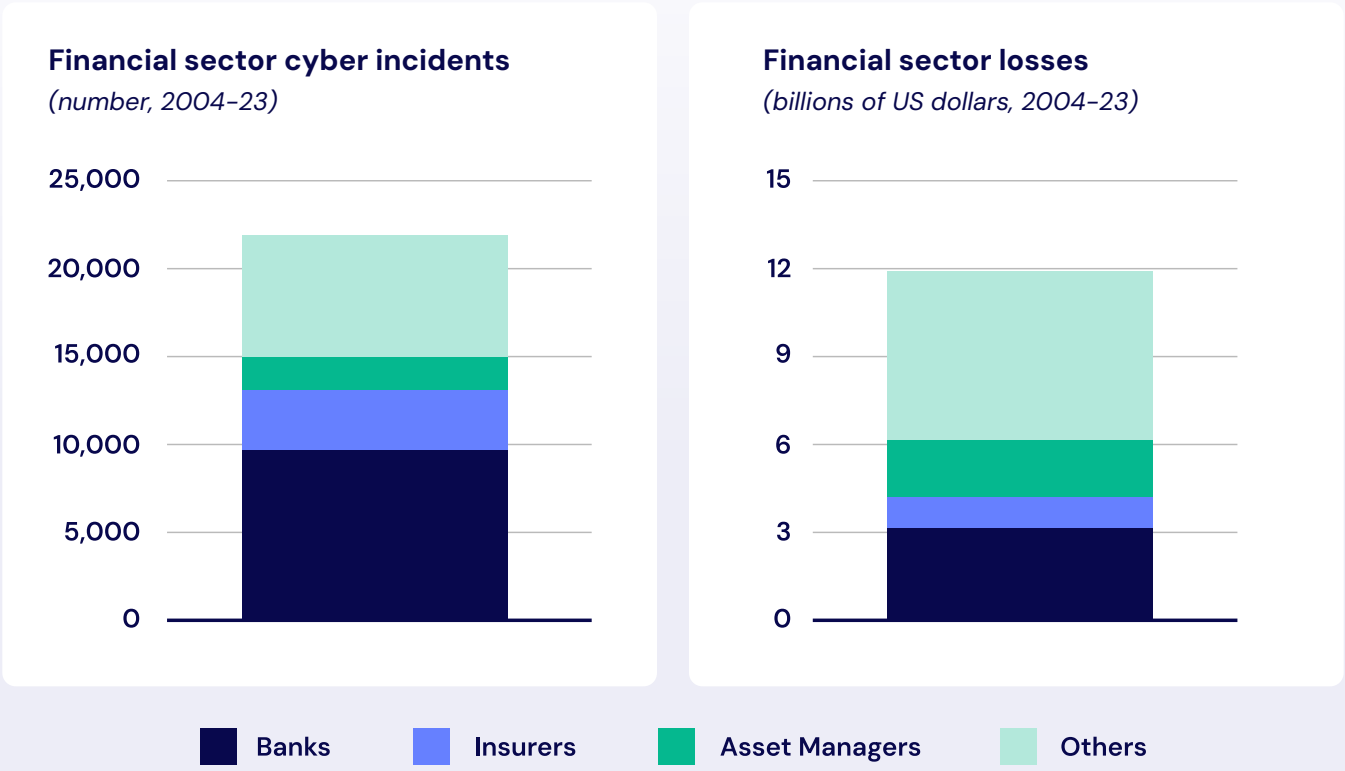


Why is DORA being implemented?

DORA's implementation directly reacts to the increasing variety of cyber threats targeting the financial industry. According to the International Monetary Fund (IMF.org), the financial sector is an attractive target to hackers and has suffered over 20,000 cyberattacks over the past 20 years, resulting in over $12 billion in losses.

Attractive Target

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



These perils jeopardise the protection of confidential financial information and present substantial hazards to financial systems' overall stability and integrity. Acknowledging the critical interdependencies between financial stability and digital operational resilience, the European Union has implemented proactive measures to establish uniformity in resilience protocols throughout its member nations.

The implementation of DORA is a testament to the European Union's proactive approach to enhancing financial institutions' cybersecurity preparedness. This strategic endeavour is not a reaction to past incidents but a forward-looking initiative to cultivate a secure digital environment. It aims to ensure the prosperity of financial services in the face of imminent cyber disruptions and boost faith in the sector's prospects, instilling a sense of confidence in the audience.

The outcome regulators are trying to achieve with DORA

Regulators aim to strengthen the financial sector's overall cybersecurity posture to reduce the frequency and severity of cyber-related incidents. This involves enhancing incident response mechanisms to ensure that financial institutions have the necessary capabilities to detect cyber threats and implement prompt and effective countermeasures.

An additional crucial outcome is improving risk management for third parties. DORA mandates rigorous supervision of the extensive network of financial sector service providers. This guarantees that external entities uphold cybersecurity protocols based on the industry's stringent criteria.

The regulation's overarching goal is cultivating an environment that consistently conducts assessments and evaluations of digital resilience. This would allow financial institutions to proactively identify vulnerabilities and risks and adapt to the constantly evolving cyber threat landscape. This proactive posture is required to preserve the confidence and trust of investors, business partners, and consumers in the financial system.

Excessively open networks

Despite significant advancements in cybersecurity technology, the susceptibility of organisational networks to attacks remains an immense obstacle. Many financial institutions face the complexity of their digital environments, which often comprise vast, interconnected networks that provide cyber adversaries ample opportunities to exploit weaknesses. The constant development of cyber threats, which discover methods to bypass traditional security protocols, further exacerbates this concern. Given the increasing intricacy of attacks and these networks' vulnerable, open state, it is imperative to devise innovative security solutions that can effectively accommodate these ever-evolving threats.

Role of microsegmentation in addressing DORA and cybersecurity challenges

Microsegmentation presents a strategic resolution to the difficulties emphasised by DORA. By allowing financial institutions to partition their devices and networks into secure and manageable segments, this technology effectively diminishes the attack surface by restricting adversaries' lateral movement across the network and, more specifically, business-critical platforms.

Microsegmentation is an exceptionally effective instrument for DORA compliance. It improves ICT risk management by implementing a robust incident response capability and a precise network and device access control mechanism. Financial institutions can improve their cybersecurity by enabling the expeditious detection and segregation of compromised assets by reacting promptly and efficiently to cyber threats.

Furthermore, microsegmentation's significance in enabling digital operational resilience testing cannot be emphasised enough. This functionality permits the replication of cyber assaults on isolated networks, thereby allowing the organisations to evaluate their susceptibilities and capacity for resilience while avoiding compromise to the overall network and its services.

Financial institutions can adopt microsegmentation to address the dual challenge of complying with DORA's rigorous standards and bolstering cyber defences. This technology is not just a compliance instrument; it represents a progressive strategy towards cybersecurity. It empowers institutions to confront contemporary risks while establishing the groundwork for a more protected and secure digital future, making the audience feel informed and empowered.

It is critical for financial institutions to strategically integrate microsegmentation into their cybersecurity frameworks to comply with DORA regulations and progress towards a zero-network model. Built upon the foundational tenets of least privilege and stringent access control, this model embodies the highest level of cybersecurity strategy implemented within the financial industry. By ensuring that microsegmentation practices are rigorously executed and continuously improved, financial institutions can effectively manoeuvre through the intricacies of the digital era and reinforce themselves against present and future cyber threats.

Why Zero Networks is best placed to solve this critical business challenge

Senior executives working in the financial sector must ensure compliance with DORA and many other regulations. This highlights the criticality of implementing sophisticated cybersecurity protocols to protect operational resilience in the face of ever-changing cyber threats. Microsegmentation restricts the lateral movement of threats and localizes vulnerabilities, making it a critical piece of a DORA-compliant security architecture—but organizations can't afford a long-term, profoundly complex implementation to meet DORA requirements and fend off hefty fines.

The Zero Networks platform provides a full suite of capabilities that check DORA's boxes in four easy steps and can be implemented within 30 days.

1 Microsegmentation

Microsegmentation has historically been reserved for large and/or mature organizations due to its complex, labour-intensive, and costly implementations, thereby impeding adherence to the stringent standards set forth by DORA. Implementing automated, agentless microsegmentation offers a viable resolution by simplifying, deploying, and managing policies. This novel methodology enables swift adjustment to emerging cyber risks and effortlessly complies with the compliance requirements set forth by DORA. In this context, eliminating agent-based systems substantially decreases operational overheads, enhancing efficiency and minimising expenditures.

By deconstructing the complexities inherent in conventional IT security duties, Zero Networks microsegmentation automation increases the efficacy of cybersecurity measures. Financial institutions can surmount common implementation obstacles by utilising automation and userfriendly interfaces and guarantee regulatory compliance with increased effectiveness and convenience.

2 Identity Segmentation

Identity segmentation is crucial for establishing a secure architecture via role-based access controls for DORA compliance. By rigorously using the least privilege principles to regulate network access, this approach guarantees that solely authorised users and devices are granted access to applications, services, or platforms, thereby reducing the potential for unauthorised access.

3 RPC Firewall

Incorporating Zero Networks' exclusive RPC (Remote Procedure Call) firewall is crucial, especially in Microsoft environments where RPC is widely employed. Facilitating meticulous management of RPC traffic reduces the likelihood of cyber intrusion originating from services critical to Microsoft services functioning, such as those present in domain controllers. By implementing this strategy, the DORA's rigorous emphasis on cybersecurity substantially diminishes the network's attack surface.

4 Secure Remote Access

Identity segmentation is crucial for establishing a secure architecture via role-based access controls for DORA compliance. By rigorously using the least privilege principles to regulate network access, this approach guarantees that solely authorised users and devices are granted access to applications, services, or platforms, thereby reducing the potential for unauthorised access.

Zero Networks provides comprehensive access control solutions for various entities, including third-party business partners, devices, individuals, and remote workers. This allows financial institutions to enhance their operational resilience, reduce their attack surface, and attain rigorous adherence to the cybersecurity requirements set forth by DORA. This enables them to protect their reputation and maintain ongoing confidence in their operational capabilities.

Segment Smarter, Not Harder.

Zero Networks is a unified zero trust platform for network segmentation, identity segmentation, and remote access.

Book a demo

ZERO. Networks