MAZEBOLT

A Comprehensive Guide to DORA Readiness for Financial Services

Table of Contents

Financial Services and the Digital Operational Resilience Act

By 17th January 2025, financial institutions need to comply with the EU's Digital Operational Resilience Act, the DORA. Are you prepared?

The increase in the number of cyber attacks, alongside the interconnected nature of financial services means that digital resilience matters more than ever.

Designed to prevent cyber attacks, limit operational risks, and curb disruptions to financial stability, the EU's Digital Operational Resilience Act[1], more commonly known as DORA, is a financial sector cyber security regulation aimed primarily at financial sector Information Communications Technology (ICT) providers that serve the Banking, Financial Services and Insurance (BFSI) space within the EU. There are limited exemptions in place for companies that qualify as microenterprises or that are subject to a simplified risk management framework [2] Businesses who are found to be non-compliant may incur penalties, fines, and reputational damage in case of an attack.

Through a wide range of requirements, and five key pillars, DORA aims to harmonize digital resilience for ICT in financial services across all EU member states, and to standardize and strengthen ICT risk management across the financial sector and essential third-party providers who operate in this sector.

The Benefits of Regulating ICT Risk Management

1. Enhanced security and resilience: A regulatory framework ensures financial entities and their third party service providers are able to withstand, respond to, and recover from ICT-related disruption and threat.

2. Reduced risk to critical infrastructure: With regulation in place, there is less risk of disruption to financial services and critical infrastructure caused by cyberattacks or ICT failures.

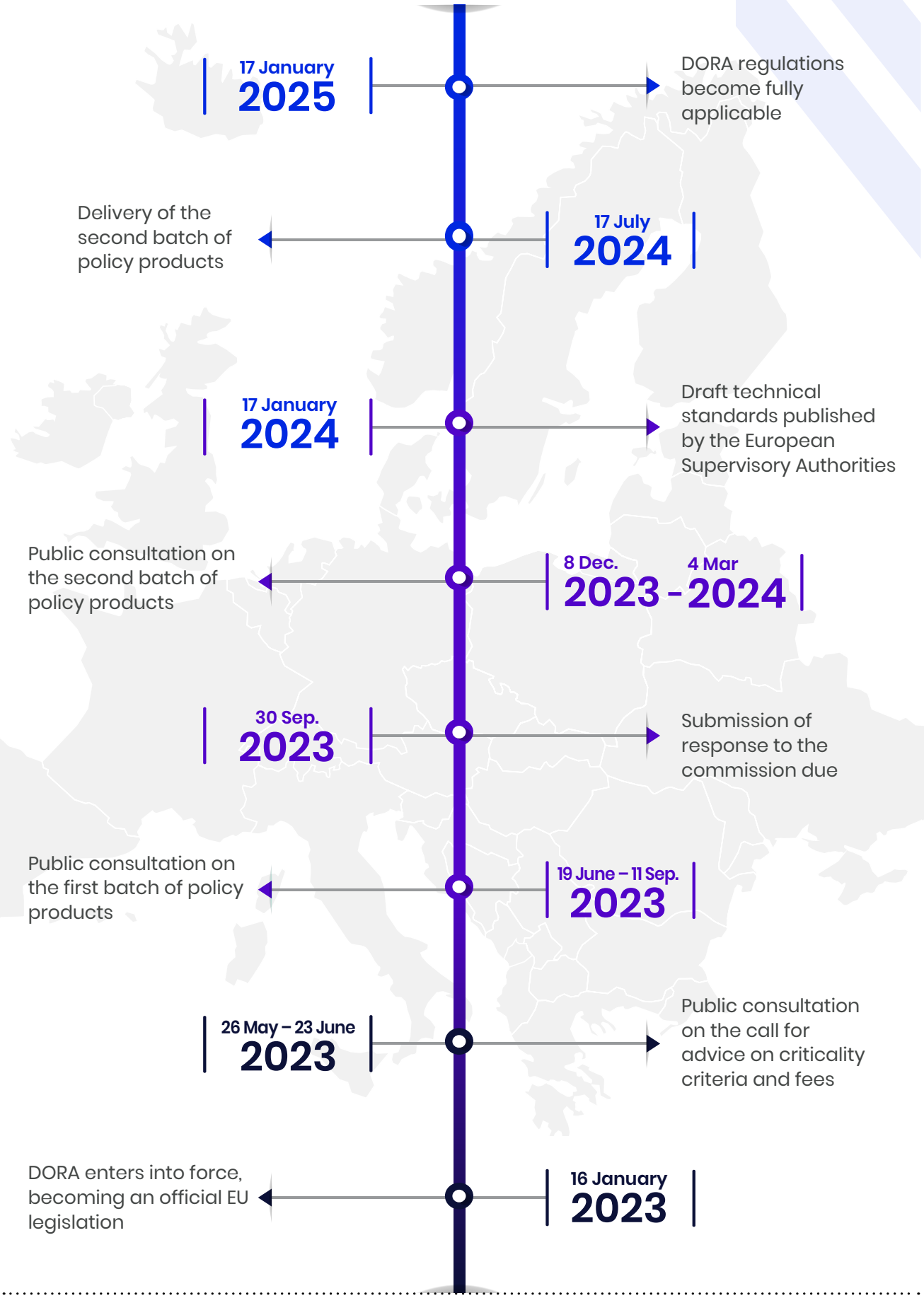
3. Protection of sensitive data: Clearer laws and stronger guidelines around data usage reduces the risk of unauthorized access, data leakage and data loss. This contributes to a more stable and secure financial ecosystem across the EU.

4. Alignment with cyber insurance guidelines: For businesses looking to obtain comprehensive cyber insurance and receive premium reductions, meeting and exceeding compliance has become table stakes.

1 Digital Operational Resilience Act

2 Recital 43 - exemptions for microenterprises

DORA 24 Month Implementation Timeline



Five Pillars of DORA

1. Digital operational resilience testing

Financial institutions must build a comprehensive program to test and challenge their ICT resilience, proportionate to their size and their risk profile. Any weaknesses or vulnerabilities must be identified and mitigated in a timely manner. DORA specifically cites Threat-led Penetration Testing (TLTP), also known as red team testing, to effectively address exposure.

> DORA places a strong emphasis on testing programs and the need to prepare operationally, beyond what is already being done today. We will have to set up solid crisis simulation exercises.
>
> Karine Pariente, Partner, PwC France [3]

2. ICT risk management

This pillar looks at the set-up, monitoring and maintenance of resilient ICT systems and applications. Continuous identification of risk from a diverse range of sources is highlighted, to ensure quick detection and mitigation of any unusual or anomalous activities. Financial services companies should put processes and incident response policies in place to recover and learn from both their own breaches and others. There are four main elements to DORA's ICT risk management guidelines. Relevant entities must:

1 **Develop and Implement a Framework**
Establish a documented ICT risk management strategy that includes policies, procedures and ICT protocols and tools, as well as how the entity will build, maintain and test resilience.

2 **Protect Information Assets**
Protect software, hardware, servers, physical components, and infrastructure from damage, unauthorized access, and misuse. Entities relying on multiple vendors for ICT services may need a multi-vendor ICT strategy.

3 **Complete Regular Internal Audits**
Undergo regular internal audits by qualified auditors with ICT risk expertise and autonomy. Audit frequency and focus should be proportionate to the entity's ICT risk.

4 **Ensure a Follow Up Process**
Implement a formal follow-up process based on audit findings, including timelines for verifying, addressing and mitigating critical problems.

3 DORA and risk regulation, PWC 2024

3. ICT incident reporting

Each supervisory authority will have their own procedures, but DORA will require incident reporting of all major incidents using a common template, including an initial notification as soon as is practical, intermediate updates as the incident unfolds, and a final report once root-cause analysis is complete. Companies must have a process in place to monitor and log any ICT-related incidents, with DORA-specific classifications and criteria.

Financial services should consider assigning roles for incident response, and creating a method for categorizing and prioritizing risk.

What is classified as a major ICT incident?

A major ICT incident is defined as one that compromises the security of the entity's network and information systems and has an adverse effect on:
Availability: Accessing and using information systems and services.
Authenticity: Ensuring information is genuine and can be trusted.
Integrity: Maintaining the accuracy and completeness of information.
Confidentiality: Protecting information from unauthorized access or disclosure.
Services provided: Delivering its services reliably.

4. Information and intelligence sharing

Enhancing digital resilience on a large scale involves collaborating within trusted communities in the financial sector. DORA encourages the sharing of information that raises awareness of ICT risks, minimizes the chances of an attack spreading, and supports defensive techniques, detection, or mitigation and recovery. Of course, sensitive information should be protected at all times.

5. ICT third party risks

As financial institutions increasingly work with third-party vendors to enhance and scale their operations, DORA mandates the management of third-party risk through monitoring and transparency in service provider contracts. Financial services organizations must maintain a register of third-party arrangements, including data access and SLAs. Thorough risk assessments need to be completed from commencement to termination of a relationship.

Cyber attacks on European financial services firms **more than doubled** between Q2 2022 and Q2 2023, by [4]

119%

4 Akamai State of the Internet Report, 2024

The Looming Financial Risk of Non-compliance

What happens if entities don't comply with DORA? Similar to the General Data Protection Regulations (GDPR), DORA is ready to heavily penalize entities found to be in violation, with fines of up to 2% of their total annual turnover worldwide. For individuals, the penalty can be as much as €1M. Failure to report major ICT incidents or cyber threats may also result in steep fines. Critical third-party ICT service providers may face up to a €5M fine for non-compliance, with individuals being liable for a fine of €500,000.

With this in mind, financial institutions subject to DORA compliance have three courses of action that they could take.

1. Sit tight until DORA comes into effect, and manage required changes on the fly
2. Implement tactical changes proactively where there are known gaps
3. Build resilience by design by deploying a complete solution

Where Does DDoS Attack and Vulnerability Testing Come in?

As DORA puts an emphasis on continual risk assessment, operational resilience, and timely detection and mitigation, the current approach for red teaming testing against DDoS attacks is insufficient for DORA readiness.

Companies deploy DDoS protection solutions both on premises, and in the cloud. These solutions are intended to block DDoS attacks in real time, but in reality — complete protection is impossible. The sheer volume of DDoS attacks, the varied attack vectors, and the sophistication of new and emerging tools that utilize AI technologies mean that, like your network itself, the threat landscape is dynamic and ever-changing. MazeBolt research shows that even organizations that deploy DDoS protection solutions still experience between 40-75% vulnerability exposure of their online services[5]. The most common reasons include misconfigurations, lack of software patching and insufficient protections deployed.

Financial services organizations need compliance certification so that they can operate. The legacy approach to prove compliance was to run manual red team testing, and obtain a certificate that claimed they could withstand an attack. This would involve intentionally attacking their networks once or twice a year to test resilience, which resulted in downtime to online services.

The main problem with this approach is the limited time frame that red teams have to do their job. Once or twice each year, the business gets the approvals necessary to allow for potential business disruption, and red teams spend no more than 3-4 hours attacking with intensity. During that window, there's

5 https://mazebolt.com/radar-testing/

no way to attack all online services, as many enterprises will have hundreds in place. There's also no time to try all attack vectors on all targets. On average, red team tests may cover between 10-15 methods of attack on a singular domain. To compare, there are over 150 attack vectors in the wild, meaning that thousands of simulations need to be run to ensure full coverage. — because any one of them could be your next attack.

In addition, the rise in AI tools is introducing endless "mutating" variants of malware code[7], evading detection from red teams who only have time to look for what they know during a single "snapshot" in time.

Compliance is not a checkbox item that can be solved in a couple of hours each year. Financial institutions that still have this mindset are facing great risk.

While your certificate may claim that your business, data and customers are secure, in reality all you can say is you had point-in-time protection against a small number of specific DDoS variants. That's certainly not good enough for DORA compliance.
Is it good enough for you?

DDoS attacks rose
40%
in 2023 [8]

The True Risk of Sporadic Red Team Testing

A large bank in Europe implemented annual red teaming to simulate DDoS attacks in their environment. Despite a limited amount of time and resources given to the task, this financial institution was given a certificate, the green light that their network was secure.

The following day, a different kind of DDoS attack compromised the entire organization, bringing down everything from the firewall and load balancers to the labs and physical ATM machines. The operational downtime and loss of online services cost the enterprise millions of dollars. The bank's DDoS mitigation vendor gave them a guarantee that the vulnerability was fixed, but the following year — the same test brought the organization down again.

The fear of business disruption, and the need to obtain a wide range of approvals means that financial organizations can rarely perform red teaming more than once or twice each year. As this enterprise learned the hard way, with this cadence of testing, there's no way to be sure your network is secure.

7 CSO Online, ChatGPT and Mutating Malware

8 Based on data from Qrator Labs, 2023

MazeBolt: Business Continuity and DORA Readiness

With DORA regulations impending, it's time for financial institutions to shift their strategy from reactive to proactive.

The main reason why enterprises can't run more frequent or expansive red team testing is the fear of disruption to business continuity. MazeBolt has removed that limitation with a non-disruptive, always-on technology that protects against DDoS attacks — RADAR™.

This one-of-a-kind approach gives organizations the freedom to test continuously, across all online services, and against all known attack vectors — with no downtime to online services.

If a vulnerability is detected, your company can implement our recommended mitigation steps and then test immediately to validate that the issue has been resolved.

Compliance with DORA across all five pillars

1. **Resilience testing:** Simulations of tens of thousands of distinct DDoS attacks, with no disruption to business continuity.
2. **Risk management:** Continuous attack and vulnerability simulations that run 24/7 to find the gaps in current mitigation tools.
3. **Reporting:** A direct view into the impact of an incident on availability and services provided, as well as a complete reporting history and logs in case of an audit
4. **Third-party risk:** Challenging the efficacy of third-party DDoS mitigation products to ensure service availability, and documenting and reviewing vulnerabilities.
5. **Information sharing**: Partnerships with mitigation vendors offer the community a proactive approach to fixing issues once identified.

DORA will impact all financial services ICT providers and businesses in the financial services industry across Europe, as well as organizations outside the EU that target people living in the EU. Without the right testing procedures and reporting capabilities in place — your organization will be directly in the line of fire.

Running manual red team testing once or twice a year over 0.5% of your attack surface doesn't mean your online services are resilient. MazeBolt's RADAR™ a year to cover only 0.5% of your attack.

Assess your DDoS vulnerability rating with our free DDoS Threat Rating Tool

Learn more