DELL Technologies

How Dell Technologies can help you prepare for the Digital Operational Resilience Act (DORA)

The Digital Operational Resilience Act (DORA) is a regulatory framework that will be legislation in the EU by 17 January 2025. It lists specific requirements for boosting digital operational resilience in the financial sector. It also mandates ICT standards and imposes significant penalties on financial institutions to ensure their readiness and resilience in the face of digital and data-related risks.

Organizations affected by DORA need to begin to look at their critical processes, services, and assets, and perform a gap analysis. Dell can work with you on this and provide technology and services that will strengthen your operational and business resilience and help you to prepare for DORA.

Table of contents

Why DORA?

Cyber incidents in the financial industry have **more than doubled** in the last decade and the rate of increase appears to be accelerating.

Cybercrime is now one of the EU's priorities in the fight against serious and organized crime as part of the European Multidisciplinary Platform (EMPACT) 2022 - 2025. According to the most recent Internet Organized Crime Threat Assessment (IOCTA)[1], Europol's operational analysts are observing new methodologies at play, with threats from increasingly professionalized groups who are exploiting changes in geopolitics and the fragility of global supply chains. With cybercrime activities being pursued with such inventiveness, and conventional service disruptions[2] becoming all too common, the financial sector is under increasing regulatory attention.

There have been a growing number of new regulations coming into play across the globe. From Australia's Operational Risk standard to the Bank of England's Operational Resilience policy, and now with the introduction of the Digital Operational Resilience Act in the EU (DORA), financial organizations are under increasing pressure to strengthen their security posture and exposure to risk.

The DORA regulation marks a distinct shift from the age of best practices and guidance to one of stringent oversight, compliance, and *enforcement*. Organizations falling under the purview of DORA will be required to meet exacting Information and Communication Technology (ICT) standards, with severe financial penalties for non-compliance.

The question is: what does the framework entail and how can your organization prepare? In this guide, we'll outline what DORA is and suggest an approach that will ensure you are prepared.

[1] Source 2023 https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN_0.pdf & spotlight report https://www.europol.europa.eu/publication-events/main-reports/cyber-attacks-apex-of-crime-service-iocta-2023

[2] Conventional risk includes anything from fire, flood, climate change, logistical issues, transport strikes and telco outages.

What is DORA?

The Digital Operational Resilience Act is a regulatory framework that lists specific requirements for boosting digital operational resilience in the financial sector. By harmonizing risk management across the EU, DORA seeks to remove gaps, overlaps, and conflicts that may arise between different EU states. In other words, it will help to standardize and strengthen how institutions prevent, respond to, and recover from ICT and cybersecurity-related incidents. In addition, it mandates stringent ICT standards and imposes significant penalties on financial institutions to ensure their readiness and resilience in the face of digital and data-related risks.

While negotiations began in 2020, DORA came into force on 16 January 2023 and will be effective from 17 January 2025.

Who does it impact?

All financial institutions operating within the European Union will have to abide by the regulation by 2025. This applies not only to banks, investment firms, and credit unions, but also non-traditional entities, such as crypto-asset service providers and crowdfunding platforms. By extension, any organization within the supporting ecosystem — such as consultancies, cloud platforms, and data analysts — will also have to abide by the regulation.

DORA's 5 pillars

The DORA Act consists of 64 articles, grouped together into five overarching pillars:

1. ICT risk management
2. ICT-related incident management, classification, and reporting
3. Digital operational resilience testing
4. The management of third-party ICT risk
5. Information sharing arrangements.

While this regulation is new, with its own specific set of requirements, it aligns with existing best practice frameworks, regulations and standards set by regulatory bodies such as DRII, BCI, DRJ, ISC², ISO, IRM, IEEE et al.

From the guidance shared by the European Commission, it's clear that organizations preparing for DORA will need to:

Facilitate efficient incident reporting

Under article 19 of the DORA Act, you'll have to notify the relevant authorities promptly when faced with a major security incident. DORA enforces strict SLAs for incident reporting. This allows for coordinated responses and threat and risk mitigation.

Ensure supply chain security

Your wider ecosystem may also pose security threats. To protect yourself from further risk, it's important to assess the security of your supply chain and ensure your partners adhere to stringent standards.

Follow a security-and-resilience-by-design approach

To stand a better chance of limiting cybersecurity and resiliency incidents, you'll need to adopt a "security first" mindset. This includes embracing DevSecOps practices, as well as adopting robust authentication methods.

Conduct risk assessments

By assessing your systems, networks, and applications on a regular basis, you'll be better able to identify and prioritize security risks.

Provide employee training

To reduce the risk of insider threats and exposure from conventional disruptions and outages, you should deliver comprehensive training plans to employees across your organization.

Implement continuous monitoring

With round-the-clock monitoring, you can identify and respond to risks and threats as they happen.

How Dell Technologies can help

Your partner in preparing for DORA

Navigating the complexities of new regulations can be challenging, particularly in the face of rapidly evolving cyber threats, operational risk, and ICT talent shortages in the EU. For financial services firms that handle large amounts of sensitive information, this can be especially difficult.

You do not have to work through these challenges alone. With the help of Dell Security and Resiliency Services, you can get ready for DORA.

Now is the time to prepare. Organizations need to look at their critical processes, services, and assets, and perform a gap analysis. Dell can work with you on this and provide technology and services that will strengthen your operational and business resilience. These include:

1. Consulting Services

When building resilience, you need to understand where to begin. Dell can help you identify any weaknesses with advisory and cybersecurity assessment services. This involves a thorough deep dive into your cybersecurity posture, as well as your organization's culture towards cybersecurity and resiliency.

Ultimately, this will give you a better understanding of:

- Your critical applications, processes, and data sets and where ownership should lie with each.
- The risk level of your systems and the cost of potential interruption.
- Which applications, systems, or processes require review.
- Cybersecurity, data security and resiliency knowledge gaps within your organization, that may require training.

As an output of our consultation and assessments, we'll provide you with a list of tailored recommendations. We'll also design a roadmap that will help to ensure your security strategy aligns with DORA's regulatory requirements, as well as industry best practices.

2. Incident Response (IR)

DORA requires that financial entities must report any major ICT-related event to the relevant competent authority. Timeframes will be determined within the coming months. For now, it's important to stay agile. When impacted, it's critical to act as quickly as possible.

By partnering with Dell Technologies, you can respond swiftly to threats and minimize your downtime. We provide both proactive and reactive Incident Response services:

- **Incident Recovery Retainer Service (IRRS)**. This is our proactive service. It begins with an evaluation of your organization's recovery readiness and coverage, including a report to guide you in strengthening your ability to recover devices and infrastructure.

  In the event of an attack, the retainer-based service includes incident recovery hours to help you recover fast and get back to business with minimal interruption. Our team of industry-certified experts in cybersecurity and infrastructure are by your side throughout the process.

- **Incident Response & Recovery (IRR)**. This is our reactive service in the event of a cyberattack. Our experts will eliminate threats, recover your data, and rebuild your targeted infrastructure either onsite or remotely. We'll also help you provide reporting to the relevant regulatory authorities.

3. Managed Detection and Response (MDR)

To prepare for DORA, you must conduct regular threat detection. This consists of monitoring your network as well as testing the resilience of your systems.

Our MDR service combines the expertise of our certified security analysts with advanced threat intelligence to monitor current and emerging threats across your network on a 24/7 basis. We use leading XDR technology to detect these threats in real time, allowing our MDR analysts to quickly initiate an appropriate response. Thus, limiting the chance of a security incident and the resulting regulatory fines.

More than this, with Pen Testing and Attack Simulation Management, we can find and address misconfigured or out-of-date security controls through regular breach attack simulations (BAS) and an annual penetration test. BAS detects faulty security controls on devices and software in your IT environment. Pen testing complements BAS by attempting to reach a specific goal, such as a high-value system. Skilled pen testers emulate threat actor techniques, including pivoting and adapting techniques to reach the target.

4. Cyber Recovery

In the event of a cyberattack or other ICT-related event, the quicker you can recover your systems and data, the faster you can resume business operations. Being prepared means creating thorough backup and retention policies for your systems, as well as developing a robust cyber recovery plan.

If you need assistance creating these plans, you can leverage Dell Technologies Cyber Recovery Advisory services to operationalize a cyber recovery vault capability. Together, we'll ensure your backup and cyber recovery environments and procedures are well-defined and align with DORA's incident response recommendations. So, if a cyberattack does occur, you'll have data protected and ready for recovery after incident response and remediation processes.

5. Resiliency Program Management (RPM)

Resiliency Program Management is a strategic, programmatic approach to Resiliency and Security program management through a set of robust capabilities which drives the definition, strategy, implementation, and ongoing management of your resiliency program. Whether you require strategy and definition around a resiliency program, management of your resiliency program, skills augmentation or a trusted resiliency partner, Dell's Resiliency Program Management services will deliver results.

6. Education

According to a 2022 Ponemon Institute study, insider threats – both malicious and accidental – have increased by 44% over the past two years. This has resulted in organizations spending $15.38 million, annually, to deal with the fallout.

Cybersecurity awareness training is essential to provide employees with the knowledge and skills needed to recognize, report, and prevent security incidents. It is a clear requirement from the Digital Operational Resilience Act (DORA) that your Board of Directors and CEO have the knowledge and skills necessary to assess cybersecurity risks, challenge security plans, discuss activities, formulate opinions, and evaluate policies and solutions that protect the assets of their organization. Failure to maintain adequate risk oversight can expose companies, officers, and directors to liability.

To increase your security and resiliency maturity, and prepare for DORA, your organization should deploy briefings for executive management, as well as regular training for employees.

Dell offers Managed Security Awareness Training and Cybersecurity Courses for both employees and security professionals, with monthly reporting on your employees' training progress available in a centralized customer portal. Reporting on training is a requirement for DORA, and industry recognized world class security and resiliency training partners are highly recommended. With the right cyber awareness training, your employees will be well equipped to deal with potential issues.

Embark on your journey to operational resilience

January 2025 will be here soon. In the coming months, financial organizations and supporting third parties will need to bolster their infrastructures, systems, and policies to prepare for DORA.

Like many businesses in a similar position, you may feel concerned about this deadline and the work involved. Expert advice and practical support can help you face the challenge with confidence.

By partnering with Dell Technologies, you can develop stronger security and resiliency strategies, keep on top of emerging threats, and become better equipped to meet DORA's requirements.

We're here to help. To begin your journey with us, we'd recommend booking a 60-minute DORA discovery meeting with our experts or an Accelerator Workshop. Together with your IT security and resiliency leadership and their teams, we'll deep dive into your business and uncover areas that require further support. With our industry leading technology, proven frameworks, and experience of helping organizations strengthen their resiliency, we can discuss what is needed to create a tailored roadmap that will help to keep your operations secure and compliant with regulations.

If you experience a cyberattack and need help, call our global Emergency Incident Response & Recovery Team 24/7

or email incident.recovery@dell.com for immediate assistance.

DELL Technologies