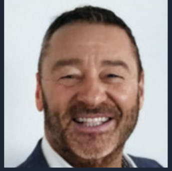
Whitepaper

The Practical Steps to Implementing DORA

QUOD ORBIS

secon.

Contributors



Martin Greenfield, CEO, Quod Orbis

Jason Wilkes, Technical Lead, Quod Orbis

Robert Gupta, CEO, Secon

Contents

Foreword

The European Union's Digital Operational Resilience Act (DORA) marks a critical turning point for financial institutions, ensuring they can not only withstand but thrive in the face of ever-evolving cyber threats and operational disruptions. In today's world, resilience has moved beyond being a regulatory requirement to become a key driver of trust, innovation, and operational excellence. DORA sets the standard for digital resilience across the financial services sector operating within the EU, safeguarding businesses and the ecosystems they serve.

This whitepaper is designed to provide clear, actionable guidance on implementing DORA's five pillars. It goes beyond meeting regulatory requirements to offer practical insights on how to strengthen your organisation's overall security posture and operational resilience. Whether you are in the preparation phase or advancing towards full implementation, this guide will help you prioritise challenges and strategically align your efforts for maximum impact.

We invite our peers, partners and customers to explore the insights shared in this whitepaper. We commit to keep this document updated as more information and guidance is released from the DORA commission, establishing a centralised hub of best practices when it comes to adhering to this regulation.

// Martin Greenfield

CEO, Quod Orbis

"We understand that the urgency to implement DORA is now high, under tight timelines. However, successful implementation doesn't require a linear approach through the five pillars of the regulation. Instead, organisations should focus on identifying and addressing their most significant challenges first."

O Robert Gupta

CEO, Secon

"We view the implementation of DORA not merely as a compliance mandate, but as a strategic opportunity for organisations to enhance their digital infrastructure, safeguard their operations, and reinforce the trust they have built with their stakeholders."

① About DORA

DORA, the Digital Operational Resilience Act, is a comprehensive EU regulation designed to bolster the resilience of the financial sector against digital disruptions. While the UK is no longer an EU member, DORA remains crucial for UK-based organisations engaged in cross-border financial activities or providing payment services to EU customers. Introduced in January 2023 and set to be enforced from January 2025, DORA mandates that financial institutions and related entities implement robust measures to prevent, manage and recover from ICT-related incidents.

The digital revolution has irrevocably transformed the financial landscape since the 2008 crisis. DORA acknowledges the financial industry's existing rigor but places a spotlight on the underlying technology infrastructure. By ensuring operational resilience, the regulation aims to safeguard the stability of the entire financial ecosystem. Given the interconnected nature of modern business, understanding and managing service dependencies will be critical to DORA compliance.

DORA is a regulation not a framework.

The five pillars of DORA – a quick summary:

ICT Risk Management

Incident Reporting

Digital Operational Resilience Testing (DORT)

ICT Third-Party Risk Management

Information Sharing

ICT Risk Management

Financial entities must implement comprehensive and effective ICT risk management frameworks to ensure the security and resilience of their ICT systems. This includes regular risk assessments, the implementation of appropriate security measures, and the establishment of incident response mechanisms.

Incident Reporting

Financial entities must promptly report major ICT-related incidents to the relevant competent authorities. This involves an initial notification, followed by detailed intermediate and final reports. The aim is to provide authorities with sufficient information to assess and manage systemic risks in the financial sector.

Digital Operational Resilience Testing (DORT)

Entities must conduct regular resilience testing of their ICT systems to ensure their ability to withstand and recover from disruptions. It places significant importance on threat-led penetration testing (TLPT), as well as other forms of tests appropriate to the size and complexity of the entity.

ICT Third-Party Risk Management

Entities must manage risks associated with their ICT third-party service providers. This involves assessing the criticality of third-party services, establishing contractual arrangements that include security requirements, and ensuring that third-party providers adhere to the same standards of operational resilience.

Information Sharing

Entities are encouraged to share information on cyber threats and vulnerabilities with each other and with competent authorities. This collaboration aims to enhance the collective understanding of cyber risks and improve the overall resilience of the financial sector.

One of the biggest challenges currently faced by organisations in their preparation for DORA is that the five pillars do not yet have clear technical controls. This lack of clarity in itself is making implementation challenging for organisations, many choosing to delay until more information is released which will inevitably result in a rushed implementation.

As of July 2024, DORA released the final draft regulatory technical standards (RTS), one set of Implementing Technical Standards (ITS) and two guidelines. By comparison, NIST defines six domains, which cover specific controls businesses need to implement. DORA, however, does not follow the same structure. DORA implementation is not a linear process, whereby businesses work through the five pillars in order. This whitepaper identifies the key aspects to focus on.

Not all DORA pillars are equally weighted in terms of the effort required for compliance.

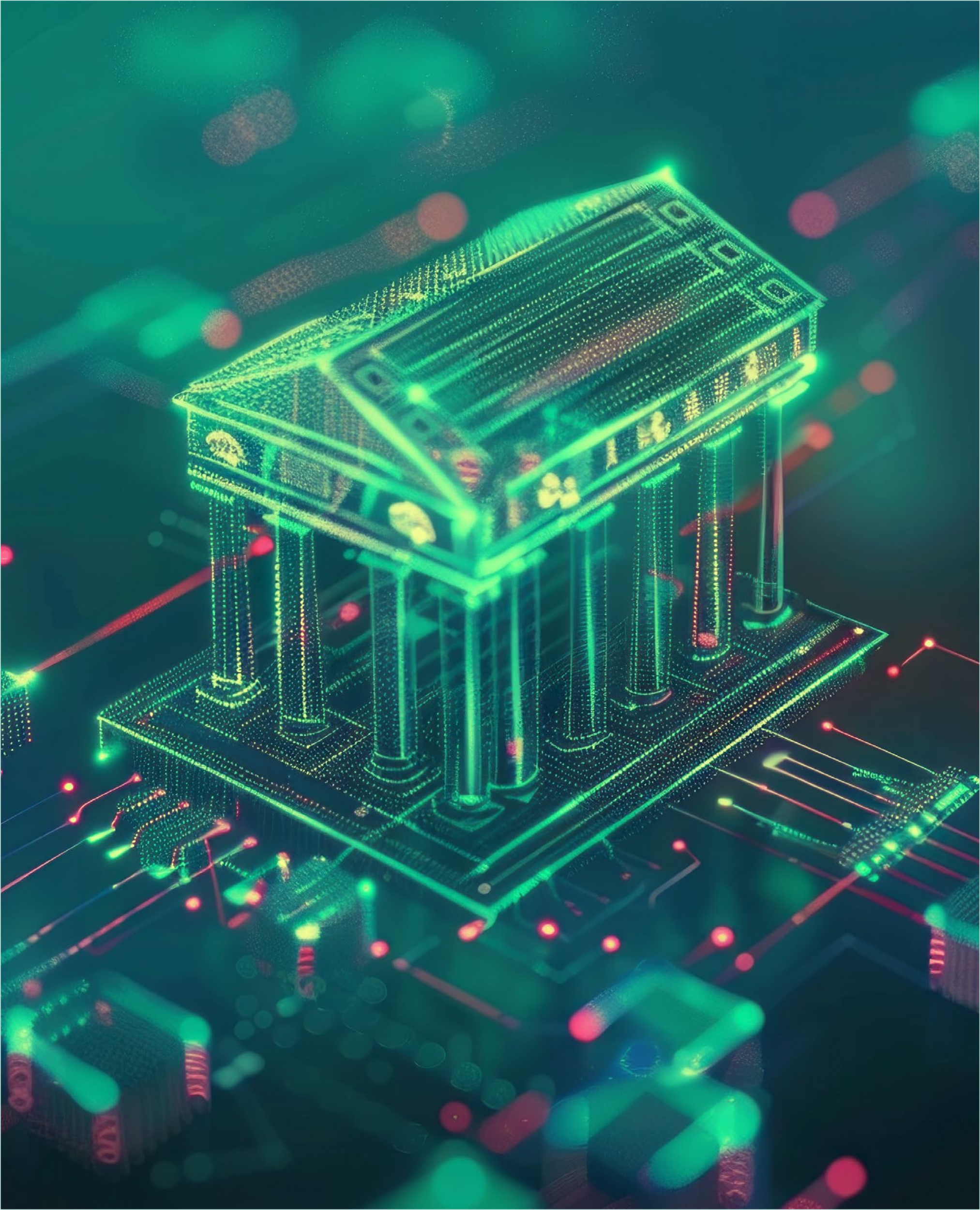
Organisations must pay extra attention to weighting of each pillar. For example, DORA assumes that businesses have an ICT risk management framework in place, rather than providing practical steps for implementation. Whereas the messaging around the need for compliance across extensive third-party networks and subsequent reporting is far more detailed, sitting across multiple pillars.

The journey to achieving DORA compliance is an evolving process. As the DORA Commission continues to release technical standards aligned with the five pillars, organisations should gain a clearer understanding of how to ensure compliance in the short, medium, and long term.

① Preparing for DORA

DORA implementation is a complex endeavour. While DORA comprises of five pillars, successful implementation will not come from following the model as five steps to address one after the other.

Following a thorough analysis of DORA's stipulations, this whitepaper offers a roadmap to guide preparation, implementation, and ongoing adherence. While each organisation's unique context will influence specific implementation steps, the following structure outlines critical considerations for achieving compliance.



2.1 Taskforce

Effective DORA implementation relies heavily on efficient stakeholder management. DORA's multifaceted nature necessitates forming a dedicated taskforce composed of key representatives across the organisation, whose sole focus is achieving compliance. This group should operate separately from core business activities to maintain objectivity.

The selection of appropriate personnel, whether internal or external, requires careful consideration of roles and responsibilities. A key part of this involves engaging senior leadership, as their buy-in will remain instrumental to long-term strategies. While some organisations may have existing structures in place, similar to regulatory compliance committees, dedicated attention and commitment to DORA is vital.

Open and consistent communication regarding DORA's stipulations and the potential consequences of non-adherence is paramount to keeping stakeholders informed. Depending on business size, cross-functional teams incorporating IT, risk management, compliance and legal functions can significantly benefit DORA implementation.

Stakeholder engagement also extends to third-party service providers, ensuring they meet the same resilience standards and are integrated into the organisation's compliance framework. Aligning these providers is vital, as highlighted by recent cyberattacks attributable to third-party breaches.

Subject: Introduction to the Digital Operational Resilience Act (DORA)

Dear Team,

As part of our commitment to strengthening our resilience against digital risks, it's important to be aware of the new EU regulation, the Digital Operational Resilience Act (DORA), coming into force in January 2025. This regulation is designed to ensure that the financial sector can withstand, respond to, and recover from ICT-related disruptions and threats.

What is DORA? DORA applies to all financial entities and critical third-party service providers in the EU. It sets out requirements for managing ICT risks, reporting incidents, testing operational resilience, and overseeing critical third-party providers.

Key Points:
Risk Management: Organisations must have strong frameworks in place to manage ICT risks, protecting systems and data from cyber threats and disruptions.

Incident Reporting: Major ICT-related incidents must be reported to authorities, with detailed accounts of associated costs and losses.

Resilience Testing: Regular testing of ICT systems is required to assess and improve resilience, including threat-led penetration testing for critical functions.

Oversight of Critical Providers: Critical ICT service providers will be subject to stringent requirements and joint examinations by European and national authorities.

Harmonisation: DORA aims to standardise ICT risk management across the EU, enhancing cooperation between financial entities, regulators, and third-party providers.

Why DORA Matters: DORA is essential for protecting the financial sector from increasing cyber threats and ICT disruptions. Compliance will be mandatory and will help secure our operations and maintain client trust.

Next Steps: We need to align our ICT risk management practices with DORA's requirements, improve our incident reporting, participate in resilience testing, and ensure our third-party providers comply as well.

Please familiarise yourself with DORA, and look out for upcoming training sessions where we'll cover the details and our implementation plan.

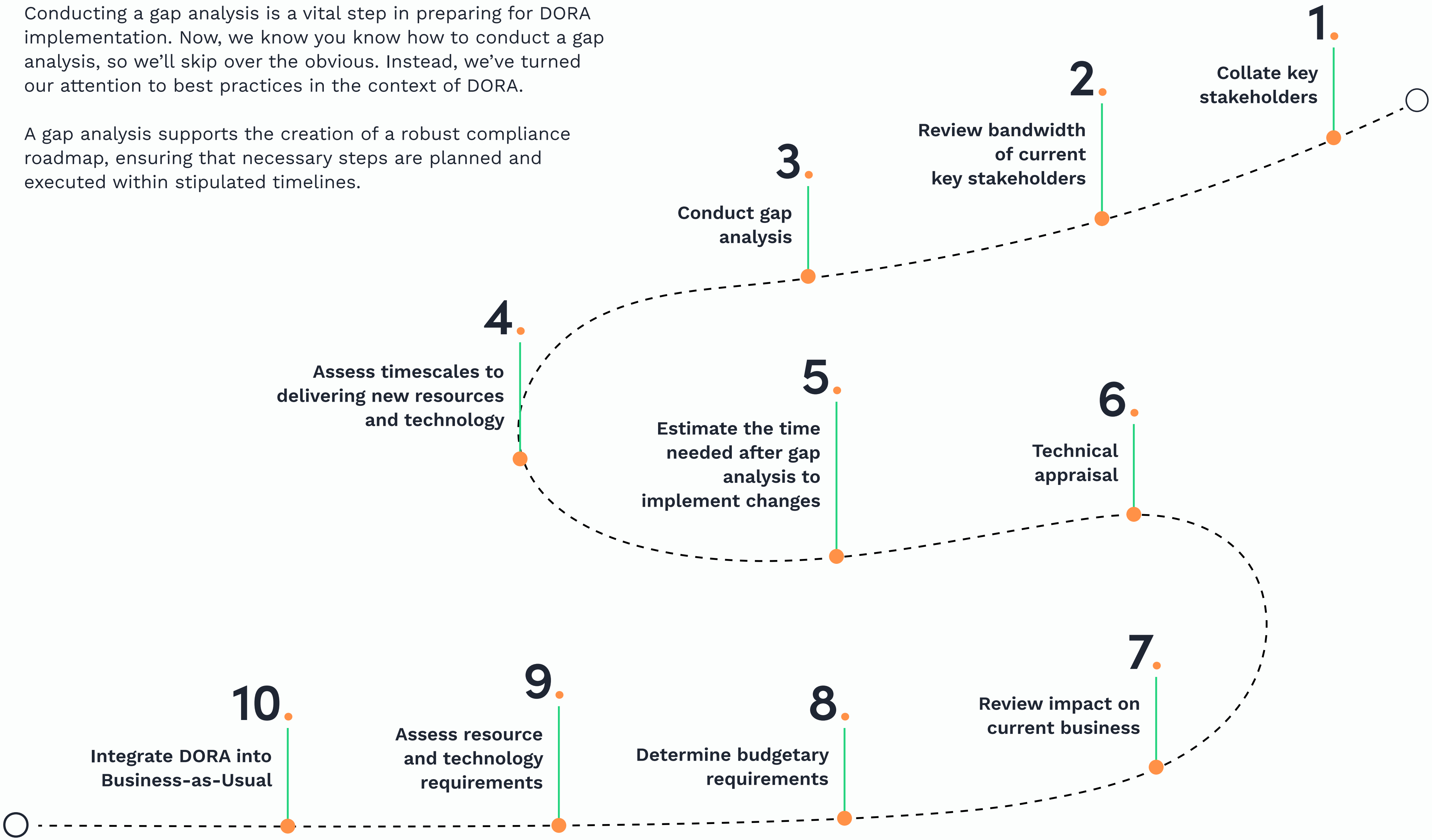
Best regards,

[Your Name]

2.2 Gap Analysis

Conducting a gap analysis is a vital step in preparing for DORA implementation. Now, we know you know how to conduct a gap analysis, so we'll skip over the obvious. Instead, we've turned our attention to best practices in the context of DORA.

A gap analysis supports the creation of a robust compliance roadmap, ensuring that necessary steps are planned and executed within stipulated timelines.



1. Collate key stakeholders
2. Review bandwidth of current key stakeholders
3. Conduct gap analysis
4. Assess timescales to delivering new resources and technology
5. Estimate the time needed after gap analysis to implement changes
6. Technical appraisal
7. Review impact on current business
8. Determine budgetary requirements
9. Assess resource and technology requirements
10. Integrate DORA into Business-as-Usual

What does a good Gap Analysis look like?

There are five key features that define an optimal DORA gap analysis.

1. Comprehensive
Covers all relevant aspects of the regulation, including ICT risk management, incident reporting, resilience testing, third-party risk management and information sharing.

2. Prioritised
Categorises gaps based on their severity and potential impact on the organisation's operations and compliance status. Critical issues are addressed first to minimise the risk of significant disruptions.

3. Actionable
Outlines specific actions, timelines, and responsibilities for addressing identified gaps. It is crucial to assign ownership for each task to ensure accountability and track progress effectively.

4. Focused
Includes a detailed estimation of the resources and costs required to address compliance gaps. This helps in budget planning and ensures that the organisation can allocate the necessary resources to achieve full compliance.

5. Tailored
Is customised to align with the specific regulatory requirements and business objectives of the organisation.

What should your organisations review as part of a DORA Gap Analysis?

First, don't overlook areas that you already cover, risk management being a critical example. It's too easy for businesses to bypass the risk management element of DORA, thinking that being ISO27001 compliant covers them. That's not the case.

Instead, ask yourself: does your existing framework cover all DORA controls? If not, is a remediation plan in place? Are you confident in the existing reporting structure on that framework? Have you considered the technical/cyber responsibilities, such as detection, response and recovery?

Beyond that, as the whitepaper comes onto later in Section 3.1, third party networks play a huge role in DORA compliance – do not underestimate the extent of preparation and ongoing maintenance required here.

If you are a multifaceted business sitting across multiple sites, there are some considerations to take into account:

- **Regulatory scope:** Identify which parts of your business fall under DORA, including any local regulatory differences that might apply across different regions.
- **Current compliance assessment:** Review your existing digital infrastructure and operational resilience policies to see how they align with DORA requirements.
- **Third-party management:** Evaluate the compliance of all third-party ICT providers with DORA standards, ensuring contracts and SLAs include necessary provisions for managing ICT risks.
- **Governance and oversight:** Ensure senior management is actively involved in ICT risk management, and that governance structures are in place for digital resilience.
- **Cross-site consistency:** Apply policies and procedures uniformly across all sites, while allowing for local regulatory nuances.
- **Continuous improvement:** Set up monitoring systems and feedback loops to continuously enhance your digital resilience.

Equally, if you are a parent company, you need full visibility across the businesses that sit below you. For example, do all entities fall under your compliance banner or are they separate legal entities that will review DORA compliance separately?

2.3 Budgets

The next critical step in DORA preparation is to budget effectively for compliance. Following a structured approach like the example outline below ensures nothing is overlooked.

① **Prioritise gaps**
Start by categorising the identified gaps based on their criticality and impact on operations. This prioritisation helps allocate resources to the most crucial areas first, ensuring that critical functions are promptly addressed.

↓

② **Leverage existing resources**
Review your current ICT systems and processes to identify areas that can be optimised or adapted to meet DORA requirements. This can significantly reduce the need for new investments and make the compliance process more cost-effective.

↓

③ **Ascertain the additional resource costs for remediation**
Determine the cost of necessary technology upgrades or new acquisitions to meet DORA standards. This includes ICT risk management tools, incident reporting systems and resilience testing programs.

Engage external consultants and partners if needed to provide expertise and guidance on implementing compliance measures effectively. Partners can help streamline processes and ensure that all regulatory requirements are met efficiently.

Allocate funds for comprehensive training programs for all employees, including board members and C-level executives. Training is essential for ensuring that everyone understands their roles and responsibilities under DORA.

Follow a phased approach to compliance, breaking down the implementation into short, medium, and long-term goals. This allows for focused and manageable budget allocation across different periods.

↓

④ **Cost-benefit analysis**
Conduct a thorough cost-benefit analysis for any new investments required. This ensures that each expenditure provides a strong return on investment and aligns with the strategic goals of the organisation. Consider cost-effective solutions like open-source tools and collaborative efforts with external partners.

↓

⑤ **Implement automated solutions**
Invest in automated compliance and monitoring tools to provide real-time insights and alerts, which help maintain continuous compliance (as expressed within the regulation). Automation improves team efficiency by removing time-intensive, manual workload and also ensures timely detection and remediation of any compliance issues.

↓

⑥ **Conduct regular reviews and updates**
Methods like continuous monitoring allow you to regularly review and update your compliance strategy based on the results of operational resilience tests and past incidents. Allocate budget for periodic reviews and necessary updates to keep up with evolving regulatory requirements and ensure sustained compliance.

↓

⑦ **Produce comprehensive documentation**
Ensure thorough documentation of all compliance efforts, including risk assessments, remediation actions and training programs. This documentation is crucial for regulatory reporting and audits.

③ DORA in Practice

Once your organisation has established a solid foundation for DORA implementation, the next step is to operationalise it and establish best practices to make ongoing compliance sustainable.

3.1 The third-party priorities

Attention! The requirements around third-party networks are extensive.

DORA mandates a risk-based approach across all areas, including business and cyber security. Central to DORA is the rigorous management of third-party risks to ensure the digital resilience of financial institutions.

The first step in managing third-party risk under DORA is to identify all third parties involved in the provision of ICT services. This includes maintaining a comprehensive register documenting all contracts with each provider, distinguishing between critical and non-critical services. The register must be regularly updated and accessible to competent authorities as needed.

Within the context of your organisation, assess the services provided by third parties. Evaluate the potential impact on operations if a service were to fail and identify key business services crucial to your financial offerings. For instance, in a pension portfolio, a service provider's authentication failure could disrupt operations.

Calculate the downstream impact of third-party failures, including their own suppliers, and review upstream to assess how their service disruptions would affect your business.

Note: DORA is yet to define how far along a third-party network is applicable to regulation compliance.

While financial entities may believe they fully understand their operational resilience and have a good idea of how long they can survive if something goes wrong, today’s environment demands a deeper understanding of how third-party risks impact operational resilience. You only have to look at the CrowdStrike outage back in July 2024 to truly measure the detrimental impact that gaps in third party operations can have.

1.

Reviewing contracts and ensuring oversight

Ensuring DORA compliance involves rigorous pre-contract due diligence and continuous oversight throughout the contractual relationship. The key steps can be broken down as follows:

Pre-contract due diligence:

- Assess all relevant risks associated with the contract, including the potential for subcontracting and the implications of using overseas providers.
- Evaluate the ICT third-party service providers’ adherence to high-quality information security standards.
- Consider the insolvency laws and the ability to recover data quickly if the provider faces bankruptcy.

Contractual provisions:

- Contracts must be in writing and include detailed service level agreements; some will need to be rewritten.
- Contracts should stipulate the conditions under which the financial institution can audit, inspect and terminate the contract, especially for critical functions.

Ongoing oversight:

- Establish a risk-based approach to determine the frequency and scope of audits and inspections of third-party providers.
- Implement continuous monitoring and reporting mechanisms to track the performance and compliance of third-party services.
- Maintain a detailed and updated register of all third-party contracts, which should be readily available for regulatory review.

2.

Handling third-party risk management

Businesses can handle third-party risk management effectively by adopting a structured and strategic approach:

Develop a comprehensive strategy:

- Integrate third-party risk into the overall ICT risk management framework.
- Regularly evaluate and update the third-party risk management strategy to adapt to new threats and regulatory updates.

Leverage automated tools and platforms:

- Utilise automated platforms for vendor profiling, due diligence assessments and contract lifecycle management. These tools can streamline the process, reduce manual errors and ensure continuous compliance monitoring.

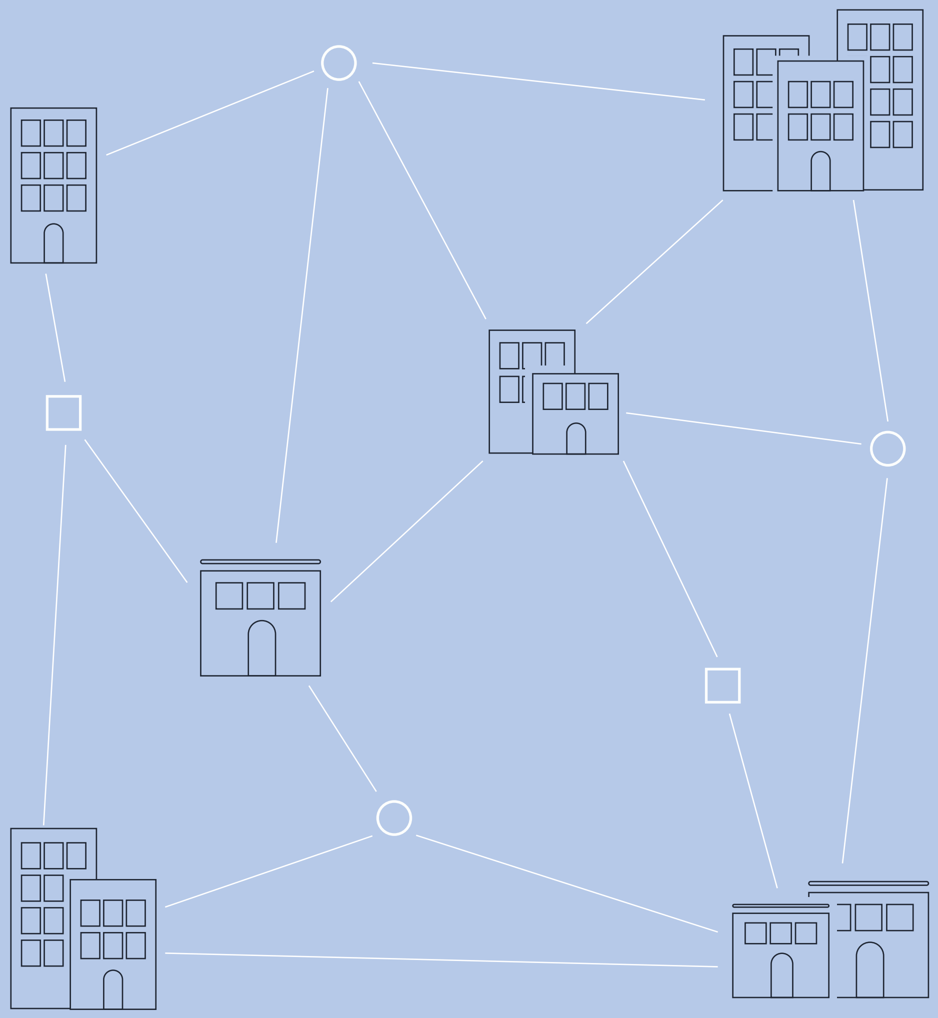
Instil a culture of continuous improvement:

- Engage in periodic reviews and updates of third-party risk management policies and procedures.
- Foster a culture of continuous improvement and resilience by regularly training staff and updating compliance practices based on the latest regulatory and industry guidance.

Exit strategies:

- Develop comprehensive exit strategies for critical third-party services to ensure that the termination of any contract does not disrupt business operations or compromise regulatory compliance. These strategies should include alternative solutions and transition plans.

Third-party networks can be several layers deep, and DORA is yet to define where the original financial entity's compliance responsibilities end.



3.2 Reporting

DORA emphasises the importance of easy access to information for the greater good. This aligns with the second pillar of the regulation but will also contribute to the information-sharing aspect within pillar 5.

Financial entities must establish robust processes to detect, manage and report significant ICT-related incidents to the relevant authorities. This transparency ensures that swift action can be taken to mitigate risks.

Financial institutions should shift their perspective from viewing each other as competitors to collaborating and sharing best practices. By exchanging information on attack types and remediation strategies, they can collectively strengthen their defences. While local competent authorities must be notified of any breaches, reporting and sharing best practices is crucial for ensuring that financial institutions are committed to incident reporting and collaborative efforts.

To streamline reporting, automated processes should be implemented to generate reports without manual intervention.*

While specific timeframes may be required, these will likely be determined by technical standards – some of which are yet to be approved by the commission. To effectively manage ICT-related incidents, procedures should be established to identify, track, log, categorise and classify them based on priority, severity and the criticality of impacted services. These procedures should adhere to the criteria outlined in Article 18.

*How CCM can help

- **Provides continuous and accurate monitoring of operational resilience controls.**
- **Automates monitoring to reduce the risk of human error, leading to more accurate and consistent data.**
- **Delivers detailed insights into the effectiveness of controls across various systems and processes.**
- **Enables proactive incident reporting to allow organisations to report incidents to regulators promptly.**
- **Facilitates transparency which will support financial institutions in clear and accurate information sharing.**
- **Gives assurance of the information accuracy they receive.**
- **Creates DORA specific dashbaords which demonstrate necessary compliance.**
- **Achieves enhanced risk management with near-real-time monitoring and proactive risk identification.**

3.3 Penetration Testing

One of the critical components of DORA is the emphasis on Threat-Led Penetration Testing (TLPT), a rigorous form of testing designed to identify and mitigate vulnerabilities in financial entities' digital infrastructure. Where organisations have previously shown reluctance around testing out of fear of operational disruption, this leniency will end with DORA.

TLPT goes beyond conventional penetration testing. It involves simulating real-world cyber threats, often orchestrated by threat intelligence providers and penetration testers, to assess the full spectrum of an organisation's people, processes and technologies. The goal is to mimic the tactics, techniques and procedures (TTPs) of attackers to uncover vulnerabilities that standard tests might miss.

DORA's requirements for TLPT

Under DORA, financial entities deemed critical will be urged to conduct TLPT far more regularly. This frequency ensures that their defences remain robust against evolving cyber threats. Such a change requires a cultural shift within the organisation. There will be no excuse – fears of operational disruption will be wildly overruled by the need to test each required system.

The regulatory technical standards (RTS) developed by the European Supervisory Authorities (ESAs) provide detailed criteria for these tests, ensuring consistency and effectiveness across the financial sector.

Following a TLPT, financial entities must develop remediation plans addressing identified vulnerabilities. These plans should include a root cause analysis, proposed measures, and a timeline for implementation.

Key components of TLPT under DORA

1. Providers and testers

Threat intelligence providers must have at least five years of experience, relevant professional knowledge and a proven track record in threat intelligence and red team testing. External testers should have significant experience in penetration testing and red team exercises, with specific requirements on their professional background and prior engagements.

2. Risk management

Before and during the TLPT, a comprehensive risk assessment is mandatory. It should consider potential impacts on the financial sector and the stability at both union and national levels. Measures must be in place to manage risks, including certifications and insurance for providers, and clear separation of duties to avoid conflicts of interest.

3. Testing phases

The TLPT process is divided into three phases:

Preparation: Formation of the control team, scoping, and selection of providers and testers.

Testing: Active testing involving a range of TTPs to simulate attacks on live production systems.

Closure: Review and analysis of the testing outcomes, including replay and purple teaming* exercises to maximise learning.

***Purple teaming exercises involve collaboration between the red team (attackers) and the blue team (defenders) to improve detection and response strategies. DORA only mandates these exercises in the closure phase of TLPT (Article 26.51).**

3.4 Tools

Choosing tools that align with DORA requires a strategic approach to meet regulatory requirements and bolster cyber security. Financial entities must select tools that address DORA's mandates for incident detection, risk management and regulatory reporting.

The criteria to consider are:

- ↓↑ Integration with Existing ICT Infrastructure
- Scalability
- Data Protection Features
- Continuous Monitoring
- Alignment with Other Compliance Frameworks
- Understanding the Relationship Between DORA and Other Frameworks

Selecting tools that align with DORA

Selecting the right tools to comply with DORA is crucial for financial institutions to strengthen cyber security and meet regulatory requirements. These tools should not only address current mandates but also prepare for future challenges and align with other frameworks like GDPR, PSD2, and ISO/IEC 27001. When deciding on the tools for your organisation, consider the following:

↓↑ 1. Integration with Existing ICT Infrastructure

A key consideration when selecting cyber security tools under DORA is their ability to integrate seamlessly with the organisation's existing ICT. Poor integration can lead to operational disruptions, potentially increasing vulnerabilities.

- **Unified Management Platforms:** Tools should support integration with existing Security Information and Event Management (SIEM) systems, Identity and Access Management (IAM) solutions, and other critical cyber security infrastructure, such as firewalls and intrusion detection systems. This ensures comprehensive monitoring and centralised control.
- **API Compatibility:** The tools must offer robust API support to enable integration with other security solutions, facilitating data exchange and operational efficiency.
- **Vendor Collaboration:** Selecting vendors that provide strong integration support, including detailed documentation, APIs, and professional services, can significantly reduce implementation risks and ensure smooth deployment.

2. Scalability

Given that DORA is designed to evolve alongside the digital threat landscape, the tools selected must be scalable to accommodate both current and future regulatory demands.

- **Modular Architecture:** Tools should be designed with a modular architecture, allowing for the addition of new functionalities without necessitating a complete system overhaul. This is particularly important for adapting to new DORA requirements or integrating additional compliance needs from frameworks like PSD2, which mandates strong customer authentication and secure communication protocols.
- **Cloud Readiness:** As cloud services become more prevalent, it's vital that tools are compatible with cloud environments, offering scalability in terms of user load, data storage, and processing power. This is crucial for managing increased data volumes or expanding operations across multiple jurisdictions.
- **Futureproofing:** Tools should be capable of integrating updates or patches provided by vendors in response to regulatory changes, ensuring ongoing compliance without significant reconfiguration.

3. Data Protection Features

DORA places significant emphasis on the protection of data integrity, confidentiality, and availability. Therefore, tools must incorporate robust data protection features to comply with these stringent requirements.

- **Encryption Capabilities:** Ensure that tools offer strong encryption for data at rest and in transit. This is critical for protecting sensitive financial information from breaches and unauthorised access, aligning with both DORA and other data protection frameworks such as GDPR.
- **Data Anonymisation and Masking:** Tools should include features for data anonymisation and masking, particularly when handling personally identifiable information (PII). This is essential for complying with GDPR and other data privacy regulations.
- **Granular Access Controls:** Implement advanced access control mechanisms such as multi-factor authentication (MFA) and role-based access control (RBAC). These features are crucial for ensuring that only authorised personnel have access to sensitive data, thus maintaining compliance across multiple frameworks, including ISO/IEC 27001, which sets out best practices for information security management.
- **Audit Trails and Monitoring:** Tools should be capable of generating comprehensive audit trails, documenting data access and processing activities. This feature is essential for compliance with DORA's reporting requirements and can be equally beneficial for fulfilling the audit and logging requirements under frameworks like PSD2 and ISO/IEC 27001.

4. Continuous Monitoring

DORA places huge emphasis on the need to continuously monitor business systems in order to maintain a clear understanding of any gaps that need to be addressed. (Article 6, Article 7, Article 10, Article 14, Article 16 & Article 19). Continuous Controls Monitoring (CCM) is the orchestration layer that pulls every tool together into a single source of truth, monitoring an organisation's entire ecosystem.

- **Enhanced Accuracy and Reduced Errors:** Automated, continuous monitoring minimises human errors that can occur in periodic manual assessments. This leads to more accurate and reliable data, ensuring that the organisation's controls are functioning as intended at all times.
- **Operational Efficiency:** Automating the monitoring process reduces the need for manual checks and audits, freeing up resources and allowing employees to focus on higher-value tasks. This leads to greater operational efficiency and cost savings.
- **Proactive Issue Resolution:** Continuous monitoring allows for the early detection of potential issues, enabling a proactive approach to resolving them before they escalate into significant problems.

5. Alignment with Other Compliance Frameworks

While DORA specifically addresses the financial sector, many of its requirements align closely with other compliance frameworks that govern cyber security and operational resilience across industries.

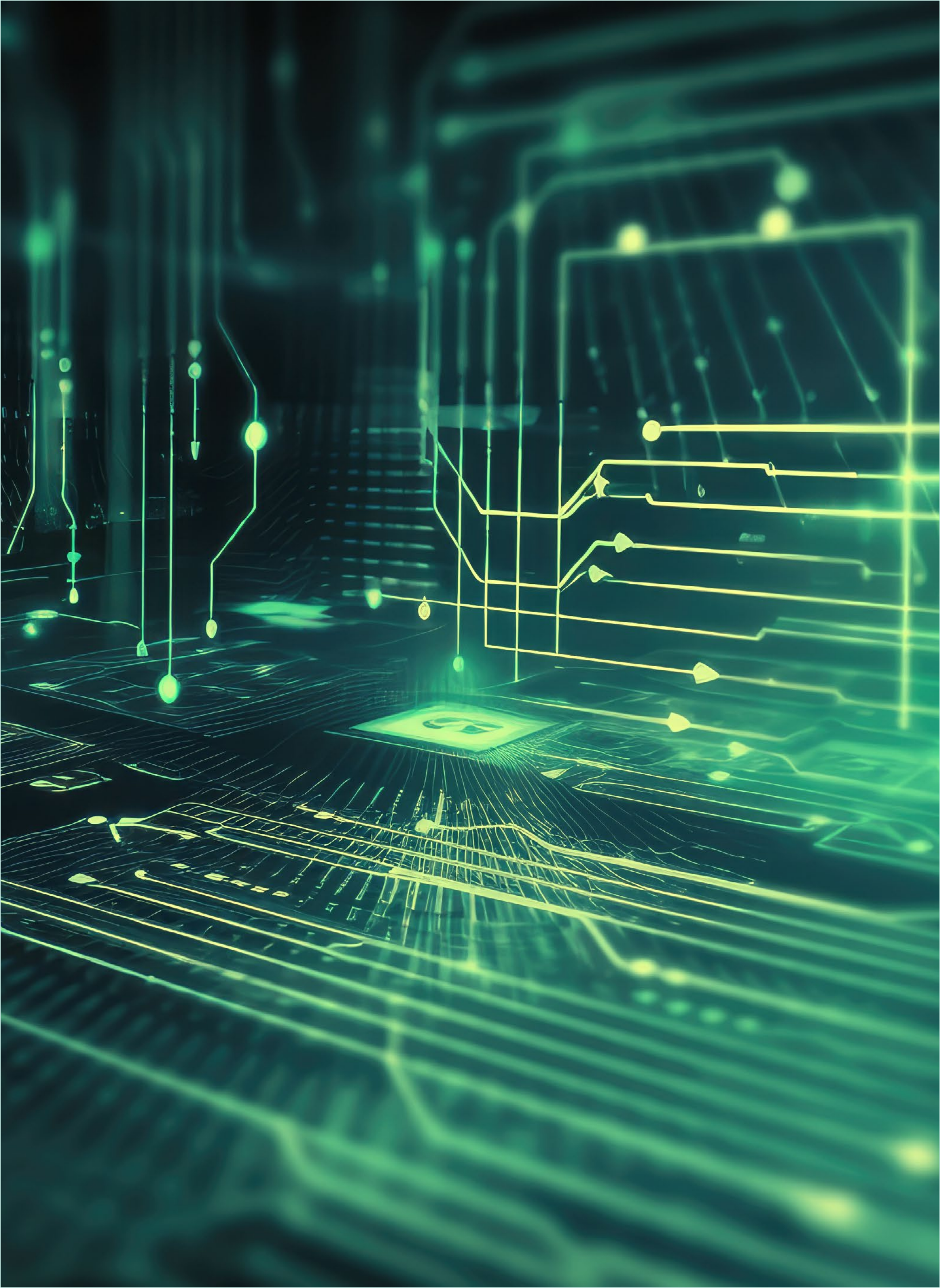
- **Incident Detection and Response:** Tools designed to meet DORA's mandates for incident detection and response can also help fulfil requirements under frameworks such as GDPR, which mandates timely notification of personal data breaches, and ISO/IEC 27001, which requires an established incident management process.
- **Risk Management Solutions:** Risk management tools that facilitate continuous monitoring, assessment, and mitigation of cyber security risks under DORA can be leveraged to meet similar obligations under frameworks like the Basel III regulations, which emphasize the importance of risk management in the banking sector.
- **Regulatory Reporting:** Tools that streamline the regulatory reporting process under DORA, such as automated reporting systems that track and report on ICT-related incidents, can also support compliance with other frameworks that require comprehensive reporting, such as GDPR's data breach notification requirements and the reporting standards set by PSD2.

6. Understanding the Relationship Between DORA and Other Frameworks

DORA can be seen as a cornerstone regulation for the financial sector, setting stringent standards for digital operational resilience. However, its requirements often overlap with those of other regulatory frameworks, offering financial institutions an opportunity to streamline compliance efforts.

- **Complementary Frameworks:** DORA's focus on ICT risk management, incident reporting, and operational resilience is complemented by other frameworks like GDPR, which governs data protection, and PSD2, which focuses on secure payment services. Compliance tools designed for DORA will often align with these frameworks, providing a unified approach to regulatory adherence.
- **Harmonisation Efforts:** As the regulatory environment becomes more complex, there is a growing trend towards harmonising requirements across different frameworks. Tools that are flexible and adaptable can help financial institutions navigate these overlapping regulations more efficiently.
- **Dual Compliance:** Achieving compliance with DORA will often contribute towards meeting the obligations of other frameworks, reducing the overall burden of adhering to multiple regulatory requirements.

By considering these detailed criteria and understanding the interconnectedness of DORA with other regulatory frameworks, financial institutions can select tools that not only ensure compliance but also enhance their overall cyber security posture. This strategic approach will help institutions navigate the complexities of the digital regulatory environment while safeguarding critical assets and maintaining operational continuity.



The Importance of a Security Operations Centre (SOC)

Achieving compliance with DORA is not just about meeting regulatory requirements—it's about fundamentally enhancing your organisation's security posture. For financial institutions, the Security Operations Centre (SOC) is at the heart of this transformation. To ensure your SOC not only meets but exceeds DORA standards, it's essential to dive deeper into the specific capabilities and best practices that will set your organisation apart.

1. Advanced Monitoring and Detection Capabilities

While the basic requirement of continuous monitoring is clear under DORA, truly advanced monitoring goes beyond just having eyes on your systems 24/7. It's about leveraging the latest technologies and methodologies to predict, detect, and respond to threats with precision and speed.

- **Continuous Controls Monitoring:** Tools like CCM provides continuous visibility into the state of controls and compliance. This transparency helps stakeholders understand the organisation's risk posture and the effectiveness of its compliance efforts. As organisations grow, their risk and compliance needs become more complex. CCM scales more effectively than periodic manual monitoring, ensuring that controls remain robust and effective across larger and more distributed environments.

- **Real-Time Threat Intelligence Integration:** Instead of relying solely on internal data, your SOC should integrate external threat intelligence feeds that offer insights into the latest global threat landscapes. This integration allows your team to anticipate potential attacks and adjust your defences accordingly. Under DORA, especially Articles 10 and 11, proactive defence mechanisms are key to maintaining operational resilience.

- **Behavioural Analytics and Anomaly Detection:** Employing machine learning algorithms that learn and adapt to the normal behaviour patterns of your systems can dramatically enhance your SOC's detection capabilities. Anomaly detection tools that flag deviations from the norm can identify zero-day attacks or insider threats that traditional signature-based detection methods might miss.

- **Automated Response Orchestration:** Automation is not just a tool for efficiency—it's a necessity for meeting DORA's stringent response time requirements. By orchestrating automated responses to common threats, such as isolating affected systems or initiating failover procedures, your SOC can mitigate risks almost instantaneously, reducing the window of vulnerability.

2. Sophisticated Incident Response and Management

DORA's emphasis on structured and effective incident response plans requires more than just having a plan on paper. Your SOC must be capable of executing these plans with military precision, ensuring that every team member knows their role and every action is tracked and documented.

- **Incident Response Playbooks:** Develop detailed playbooks that cover a range of scenarios, from phishing attacks to ransomware. These playbooks should include step-by-step instructions, decision trees, and communication templates. Ensure that these playbooks are regularly tested and updated based on the latest threat intelligence and lessons learned from past incidents.

- **Cross-Functional Incident Drills:** Regularly conduct cross-functional incident response drills that involve not only your SOC team but also other departments like legal, compliance, and communications. This ensures that everyone is prepared to respond effectively under pressure, as required by Article 12 of DORA.

- **Post-Incident Forensics and Root Cause Analysis:** After an incident, a thorough forensic analysis is crucial to understand what happened, how it happened, and how similar incidents can be prevented in the future. Implement a continuous feedback loop where findings from post-incident analyses are used to refine your incident response plans, aligning with DORA's focus on continuous improvement and resilience (Article 14).

3. Robust Compliance and Reporting Mechanisms

Meeting DORA's reporting requirements involves more than just sending incident reports to regulators. It requires a comprehensive approach to documentation, audit trails, and communication with stakeholders.

- **Automated Compliance Dashboards:** Implement dashboards that provide real-time visibility into your SOC's compliance status. These dashboards should track key metrics such as incident response times, system uptime, and compliance with regulatory reporting timelines. They can also automate the generation of compliance reports, ensuring that your organisation stays ahead of DORA's requirements.

- **Granular Audit Trails:** Ensure that your SOC systems maintain detailed audit logs that document every action taken during an incident. These logs are not only essential for compliance but also provide valuable insights during post-incident analyses. Article 16 of DORA emphasises the importance of accountability, and maintaining comprehensive audit trails supports this requirement.

- **Proactive Regulator Engagement:** Build relationships with your regulators before incidents occur. Regularly update them on your SOC's capabilities, and ensure that your incident reports are clear, comprehensive, and submitted within the required timelines. This proactive approach can help build trust and may provide some leeway in times of crisis.

4. Comprehensive Risk Management and Resilience Testing

DORA's focus on resilience testing is a call to action for financial institutions to go beyond traditional risk assessments and engage in rigorous, scenario-based testing.

- **Scenario-Based Resilience Testing:** Move beyond standard penetration testing to conduct scenario-based resilience tests that simulate real-world attacks. These tests should involve red teaming exercises where attackers and defenders simulate advanced persistent threats (APTs) to test your SOC's ability to detect and respond to sophisticated attacks. Article 9 of DORA mandates such proactive measures to ensure resilience.
- **Supply Chain Risk Management:** DORA requires that financial institutions also consider risks from their third-party suppliers. Implement a supply chain risk management programme that evaluates the security posture of all vendors and integrates their monitoring into your SOC. Regularly test your response to incidents that could arise from vulnerabilities within your supply chain.
- **Dynamic Risk Assessment Tools:** Use tools that not only assess risk at a single point in time but continuously monitor and update your organisation's risk profile. These tools should factor in both internal and external data, including geopolitical events, emerging threats, and changes in the regulatory landscape.

5. Enhanced Collaboration and Communication Strategies

Effective incident response often requires collaboration beyond the walls of your SOC. DORA recognises this, stressing the importance of both internal and external communication.

- **Internal Communication Protocols:** Establish and regularly update communication protocols that ensure all relevant stakeholders are informed during an incident. This includes setting up secure communication channels that remain operational even if your primary systems are compromised.
- **Information Sharing with External Entities:** Participate in industry-wide information-sharing initiatives. DORA encourages collaboration to bolster collective security resilience. Sharing anonymised data about incidents with peers, regulators, and industry bodies can provide early warnings about emerging threats and help you stay ahead of potential attacks.
- **Crisis Management Communication Plans:** Develop comprehensive crisis management plans that detail how your organisation will communicate with external stakeholders during a cyber incident. These plans should include predefined messages for different scenarios, ensuring that your organisation maintains transparency and trust with clients, partners, and regulators throughout the crisis.

6. Continuous Staff Training and Development

DORA places significant emphasis on the human element of cyber security, recognising that even the most advanced technologies are ineffective without a skilled and informed workforce.

- **Specialised Training Programmes:** Beyond basic cyber security training, your SOC staff should undergo specialised training in areas such as threat hunting, digital forensics, and incident response automation. This training should be tailored to the specific tools and technologies used within your SOC.

- **Tabletop Exercises and War Games:** Regularly conduct tabletop exercises and cyber war games that challenge your SOC team to respond to complex, multi-stage attacks. These exercises help identify gaps in your response capabilities and provide valuable hands-on experience that's crucial for real-world incident handling.

- **Certification and Professional Development:** Encourage continuous professional development by supporting your SOC team in obtaining advanced certifications such as the Certified Information Security Manager (CISM) or Certified Ethical Hacker (CEH). These certifications not only enhance your team's skills but also demonstrate your organisation's commitment to maintaining a highly qualified cyber security workforce.

Elevating your SOC to meet and exceed DORA standards is not just about compliance—it's about building a resilient, proactive, and adaptive cyber security infrastructure that can protect your organisation from the evolving threat landscape.

④ An Evolving Conversation

This whitepaper serves as a practical guide for short and long-term DORA objectives. As the conversation evolves and new guidance is released, this document will be regularly updated to ensure its continued relevance and value.

For now, we've summarised some of the key questions currently left unanswered by DORA. Each one will be updated with newly released information and additional guidance.

Questions that are still unanswered

1. Implementation and Compliance

How will smaller financial institutions manage the resource demands of DORA compliance?

What will the audit and enforcement process look like in practice?

How will organisations manage the ongoing reporting requirements?

2. On going Operational Challenges

How will firms effectively manage third-party risks, especially with critical service providers?

What are the best practices for conducting resilience testing and simulation exercises?

3. Technology and Innovation

How will the adoption of new technologies impact DORA compliance?

What role will cyber security play in the broader context of digital operational resilience?

4. Regulatory and Legal Considerations

How will DORA interact with other existing and upcoming regulations?

Will there be updates or amendments to DORA based on early feedback and challenges?

5. Global Coordination & The UK Digital Operational Resilience Act

How will DORA's requirements align with global standards for operational resilience?

How will cross-border operations be managed under DORA?

6. Long-Term Impact

What will be the long-term impact of DORA on the financial services industry?

How will organisations balance compliance with DORA against the need for innovation and agility?

Do you have any burning questions about DORA that you need answered as a priority? Join the discussion by signing up to The Financial Compliance & Digital Resilience Circle

Sources

- An overview of the Digital Operational Resilience Act (DORA)
- ESAs published second batch of policy products under DORA
- Regulatory Technical Standards on ICT risk management framework and on simplified ICT risk management framework
- Digital Operational Resilience Act - EBA
- ESAs published joint final Report on the draft technical standards on subcontracting under DORA
- Regulation (EU) 2022/2554 of the European Parliament and of the Council - 14 December 2022
- Draft Regulatory Technical Standards on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents
- Draft Regulatory Technical Standards specifying elements related to threat led penetration tests under Article 26(11) of Regulation (EU) 2022/2554

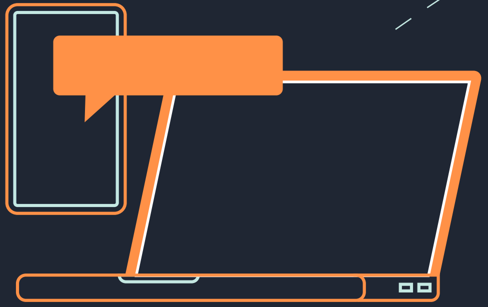
DORA Articles

- The final text of the Digital Operational Resilience Act (DORA) - Article 6, ICT risk management framework
- The final text of the Digital Operational Resilience Act (DORA) - Article 7, ICT systems, protocols and tools
- The final text of the Digital Operational Resilience Act (DORA) - Article 9, Protection and prevention
- The final text of the Digital Operational Resilience Act (DORA) - Article 10, Detection
- The final text of the Digital Operational Resilience Act (DORA) - Article 11, Response and recovery
- The final text of the Digital Operational Resilience Act (DORA) - Article 12, Backup policies and procedures, restoration and recovery procedures and methods
- The Articles (Proposal) of the Digital Operational Resilience Act - Article 14, Further harmonisation of ICT risk management tools, methods, processes and policies
- The final text of the Digital Operational Resilience Act (DORA) - Article 16, Simplified ICT risk management framework
The final text of the Digital Operational Resilience Act (DORA) - Article 18, Classification of ICT-related incidents and cyber threats
- The final text of the Digital Operational Resilience Act (DORA) - Article 19, Reporting of major ICT-related incidents and voluntary notification of significant cyber threats
- The final text of the Digital Operational Resilience Act (DORA) - Article 26, Advanced testing of ICT tools, systems and processes based on TLPT

Sources

Additional sources

- What Is the Digital Operational Resilience Act (DORA)? | IBM
- Publications Office (europa.eu)
- Implementing DORA - Achieving enhanced digital operational resilience in European financial services - Remarks by Director Gerry Cross (centralbank.ie)



Resources

Check out some other resources from Quod Orbis and Secon on DORA:

- From branches to bytes: The digital evolution of banking and its cybersecurity challenges
- The impact of the digital operations resilience act (DORA) on financial institutions
- Cutting through the confusion: The key provisions and requirements of the digital operational resilience act (DORA)
- DORA Regulation UK - Secon Cyber
- Navigating DORA: Essential Insights for Financial and Payment Institutions - Secon Cyber
- The Role of Threat-Led Penetration Testing in DORA - Secon Cyber
- DORA on Autopilot: Automate the Digital Operational Resilience Act with Continuous Controls Monitoring
- DORA Compliance with CCM data sheet