A VIEW ON SECURE SOFTWARE FOR DORA COMPLIANCE

Software Resilience in the Era of DORA_

VERACODE

Contents

Introduction

This whitepaper provides an in-depth exploration of the Digital Operational Resilience Act (DORA), in effect as of January 2025, focusing on its implications for the financial sector. It outlines the key requirements of DORA and discusses the role of software security best practices in achieving DORA compliance. It also examines how Application Risk Management can assist organizations in meeting DORA's stringent requirements, thereby ensuring robust digital operational resilience.

What is DORA?

Regulatory frameworks are essential for ensuring the resilience and security of organisations, especially in the financial sector. The Digital Operational Resilience Act (DORA) is a comprehensive regulatory framework that encompasses various regulations aimed at enhancing digital operational resilience within the financial sector.

DORA, governed by three European authorities - the banking authority, the insurance and pension authority, and the securities and markets authority - went into force on 17 January 2025. This act establishes security requirements for companies within the financial sector and their third-party service providers.

One driving force behind why you need to pay attention to DORA is that it's a regulation and not a directive. A regulation means that since January 2025, it's in effect without anything else needing to happen as far as being translated into laws; a directive would mean it needs another round of lawmaking to follow the directive's direction.

What are the key requirements of DORA?

The key pillars of DORA include information and communication technology (ICT) risk management, incident reporting, digital operational resilience testing, risk management, and third-party risk management. Each pillar focuses on specific aspects of digital resilience, ensuring that financial entities have effective measures in place to address potential threats and disruptions. By understanding the DORA framework and its key pillars, organisations can implement strategies to achieve digital operational resilience and safeguard their operations.

1. Risk Management_

The risk management pillar focuses on the identification, assessment, and mitigation of risks associated with operational resilience. Entities must have internal governance and control frameworks that ensure the effective and prudent management of all Information and Communications Technology (ICT) risks to bring about a high level of operational resilience.

2. Third-Party Risk Management_

This pillar emphasizes the need for organisations to assess and manage the risks posed by their third-party service providers. DORA defines a set of key principles for entities to achieve sound management of ICT third-party risks and engage in a robust contractual relationship with ICT third-party service providers.

3. Incident Reporting_

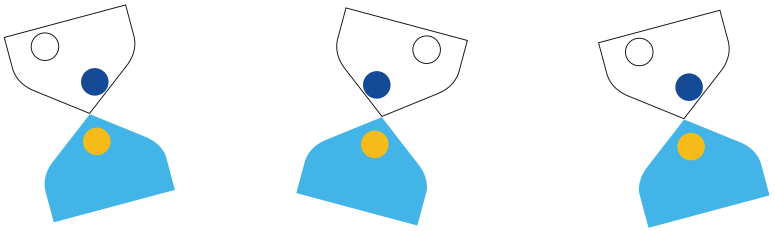
Incident reporting is a critical aspect of DORA, requiring organisations to promptly report any significant operational disruptions or cyber incidents. As part of their ICT-related incidents management process, entities must define, establish, and implement a management process to detect, manage, and notify them.

4. Information Sharing_

The information sharing pillar encourages collaboration and the exchange of cyber threat intelligence among organisations. DORA promotes information-sharing arrangements among financial entities with a view to enhancing digital operational resilience, by raising awareness of cyber threat information and intelligence, including indicators of compromise, tactics, and cybersecurity alerts.

5. Digital Operational Resilience Testing_

The final pillar of DORA emphasizes the importance of a programmatic approach of regular testing to ensure the operational resilience of organizations. As part of the ICT risk management framework, entities have to establish, maintain, and regularly review a sound and comprehensive digital operational resilience programme.



How can software security best practices help with DORA compliance?

This regulation doesn't introduce anything new in explaining best practices for digital resilience; it just adds the "or else" to what has already been found to be beneficial. Here are the practices and which articles they're cited in.

- Article 25
- Article 26
- Article 5 & Article 13

Article 25

> The digital operational resilience testing programme referred to in Article 24 shall provide, in accordance with the criteria set out in Article 4(2), for the execution of appropriate tests, such as vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing.
>
> **-Article 25, Testing of ICT tools and systems**

The beginning of Article 25 mentions several software security best practices that should be included in the digital operational resilience testing programme. These practices aim to ensure the security and resilience of digital operations.

Firstly, vulnerability assessments and scans are mentioned as appropriate tests. These involve identifying and assessing vulnerabilities in software systems, which is a fundamental step in maintaining software security. By regularly conducting vulnerability assessments and scans, organisations can identify and address potential weaknesses before they are exploited by malicious actors.

Open source analyses are also mentioned as part of the testing programme. Open source software is widely used in various applications, and it is crucial to assess its security. Open source analyses involve reviewing the security and license risks of open source components used in software systems, ensuring that they are free from known vulnerabilities and adhering to best practices.

Adopting and utilizing scanning software solutions is important for the business, as this allows them to determine and assess the security posture of software systems. These tools can help organisations identify potential vulnerabilities and weaknesses in their software, allowing them to take appropriate actions to mitigate risks.

Source code reviews are mentioned as a best practice where feasible. The feasibility of this only comes into question if this is a manual review process; having appropriate tools as part of your development lifecycle enables you to automate and scale out code reviews across your business applications.

This involves reviewing the source code of software systems to identify any security vulnerabilities or weaknesses. Source code reviews can help identify coding errors, insecure coding practices, and potential backdoors that could be exploited by attackers.

Scenario-based tests, compatibility testing, performance testing, end-to-end testing, and penetration testing are also mentioned as part of the testing programme. These tests aim to assess the resilience and security of software systems under various scenarios and conditions. By conducting these tests, organisations can identify any vulnerabilities or weaknesses in their software and take appropriate actions to address them.

Overall, this part of the article emphasizes the importance of incorporating various software security best practices into the digital operational resilience testing programme.

Article 26

> Each threat-led penetration test shall cover several or all critical or important functions of a financial entity, and shall be performed on live production systems supporting such functions.
> Financial entities shall identify all relevant underlying ICT systems, processes and technologies supporting critical or important functions and ICT services, including those supporting the critical or important functions which have been outsourced or contracted to ICT third-party service providers.
>
> **-Article 26, Advanced testing of ICT tools, systems and processes based on TLPT**

This article discusses software security best practices in the context of threat-led penetration testing (TLPT) for financial entities. TLPT is a method used to assess the security of live production systems supporting critical or important functions of a financial entity.

One of the key software security best practices highlighted in the article is the need for financial entities to identify all relevant underlying ICT systems, processes, and technologies supporting critical or important functions. This includes systems and services that may have been outsourced or contracted to third-party service providers. By identifying these systems, entities can ensure that they are included in the TLPT scope and subjected to security testing.

Another best practice mentioned is the assessment of which critical or important functions need to be covered by the TLPT. This assessment helps determine the precise scope of the penetration testing and ensures that all necessary functions are included. It is important for financial entities to validate this assessment with competent authorities to ensure that the scope is appropriate and comprehensive.

By emphasizing the need to cover critical or important functions and validate the scope with competent authorities, the article highlights the importance of prioritizing security testing for software systems that are crucial to the financial entity's operations. This aligns with the best practice of focusing security efforts on the most critical components of a system.

Article 5 and Article 13

> The management body shall allocate and periodically review the appropriate budget to fulfil the financial entity's digital operational resilience needs in respect of all types of resources, including relevant ICT security awareness programmes and digital operational resilience training referred to in Article 13(6), and ICT skills for all staff;"
> Financial entities shall assess which critical or important functions need to be covered by the TLPT. The result of this assessment shall determine the precise scope of TLPT and shall be validated by the competent authorities.
>
> **-Article 5, Governance and organisation**

> Financial entities shall develop ICT security awareness programmes and digital operational resilience training as compulsory modules in their staff training schemes. Those programmes and training shall be applicable to all employees and to senior management staff, and shall have a level of complexity commensurate to the remit of their functions. Where appropriate, financial entities shall also include ICT third-party service providers in their relevant training schemes in accordance with Article 30(2), point (i).
>
> **-Article 13, Learning and evolving**

Education and building awareness are fundamental software security best practices. These articles emphasize the importance of ICT security awareness and digital operational resilience training for staff in financial entities. They require financial entities to develop ICT security awareness programmes and digital operational resilience training as compulsory modules in their staff training schemes.

In terms of secure code education and awareness, these articles indirectly address the need for financial entities to include software security best practices in their training programmes. By requiring the development of ICT security awareness programmes, the articles imply that staff should be educated about secure coding practices and the importance of writing secure code.

Overall, while these articles do not explicitly mention secure code education and awareness, they indirectly address the need for financial entities to include software security best practices in their training programmes by emphasizing the importance of ICT

How can Application Risk Management help with DORA compliance?

To help achieve digital operational resilience and ensure compliance with DORA, organisations can leverage the expertise of an industry pioneer like Veracode. As a trusted Application Risk Management provider, Veracode can play a significant role in helping you navigate DORA regulations.

Veracode's expertise in application security testing aligns with the risk management and digital operational resilience testing pillars of DORA. Our comprehensive testing capabilities, including Static Analysis (SAST), Dynamic Analysis (DAST), Penetration Testing (PTaaS), and Software Composition Analysis (SCA), can assist organizations in fulfilling the security requirements for risk assessment processes outlined in DORA.

Risk management needs data, and this data comes from a programmatic approach to application and cloud security in a platform with robust analytics. Our platform can give you quick access to information about when an app was scanned last, what the results of the scan were, how many open and closed findings you have, benchmarks against peers in your industry, and more.

Our ASPM tool aggregates findings from across tools, which include vulnerabilities, misconfigurations, over-permissioned accounts, data sensitivity issues, and indicators of compromise, are normalized, pre-investigated, and prioritized based on business, asset, and environment context. It's also tool agnostic and operates in an open ecosystem way that allows correlation across many tools.

Furthermore, Veracode's vulnerability intelligence and threat research can contribute to the information sharing pillar of DORA. By staying ahead of emerging vulnerabilities and sharing this knowledge with our customers, we can help them enhance their threat intelligence capabilities and strengthen their overall security posture.

Finally, our secure code education is a best-in-class choice. Security Labs is immersive and hands-on secure code training that can even be gamified. The State of **Software Security 2025 report** found that among organizations that use Security Labs, teams boast flaw half-lives that are 7.5 months shorter than the time-to-fix of teams that aren't using the Labs.

Additional Considerations_

One final comment about risk management and vulnerability testing: testing alone is insufficient for reducing risk. Testing must be accompanied by addressing the results of the tests. This means fixing the findings from the scan that pose risk. Manual vulnerability fixing is a tedious task, but you can read more about AI-assisted remediation at **www.veracode.com/fix.**

Veracode is a global leader in Application Risk Management for the AI era. Powered by trillions of lines of code scans and a proprietary AI-assisted remediation engine, the Veracode platform is trusted by organizations worldwide to build and maintain secure software from code creation to cloud deployment. Thousands of the world's leading development and security teams use Veracode every second of every day to get accurate, actionable visibility of exploitable risk, achieve real-time vulnerability remediation, and reduce their security debt at scale. Veracode is a multi-award-winning company offering capabilities to secure the entire software development life cycle, including Veracode Fix, Static Analysis, Dynamic Analysis, Software Composition Analysis, Container Security, Application Security Posture Management, and Penetration Testing.

Learn more at **www.veracode.com**, on the **Veracode blog**, and on **LinkedIn** and **Twitter**.

Learn More | Request Demo