SOLUTION NOTE

DIGITAL OPERATIONAL RESILIENCY ACT (DORA) AND DNS

How to apply DNS best practices to enable DORA compliance

INTRODUCTION

The Digital Operational Resiliency Act, fondly known as DORA, is a European Union (EU) regulation designed to strengthen the digital resilience of financial institutions. It came into effect on January 17, 2025, and ensures that banks, insurance companies, investment firms and other financial entities can withstand, respond to and recover from ICT (Information and Communication Technology) disruptions, such as cyberattacks or system failures.

DORA is organized into nine chapters with corresponding Regulatory Technical Standards (RTS). Along with banks and other traditional financial services organizations, the act and its standards apply to additional financial sector firms such as crypto asset service providers and third-party ICT providers. According to PWC, mandatory compliance with DORA extends to more than 22,000 entities,[1] as the directive is not limited to companies located in the EU, but also to any financial institution that operates or transacts business within the zone.

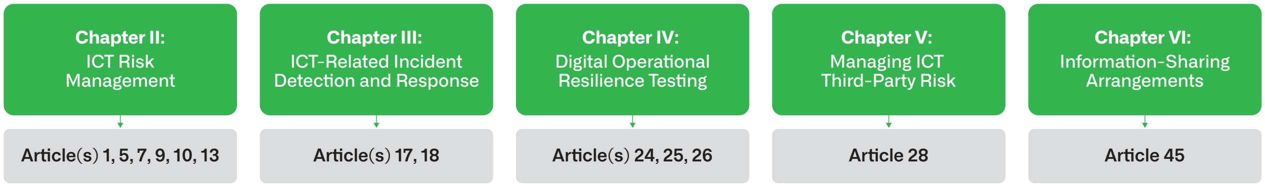
Article 1 of DORA delineates the various regulatory standards that pertain to network and information system security. Topics covered include risk management, incident reporting, resilience testing, the management of ICT third-party risk and the sharing of cyberthreat information and intelligence.[2]

As these standards evolve, specific requirements associated with them will become clearer for financial organizations. As an example, the *Final Report on draft RTS specifying elements related to threat-led penetration tests*[3] provides additional clarity about penetration testing requirements. The report explains that the DORA requirements will interoperate with other security-related regulatory initiatives, such as the Threat Intelligence-Based Ethical Red-Teaming (TIBER-EU) framework associated with the European Central Bank. As the report states, "[the TIBER-EU framework] can also assist competent authorities and financial entities in meeting the requirements for threat-led penetration tests under the Digital Operational Resilience Act (DORA)."[4] The report also references the European Central Bank's document, *Adopting TIBER-EU will help fulfil DORA requirements*.[5]

HOW DNS HELPS WITH DORA COMPLIANCE

The Domain Name System (DNS) plays a central role in all network interactions among devices, applications, internet domains, databases and cloud resources. When managed and deployed strategically, the DNS protocol also serves as a proactive network security enforcement point, a valuable source of digital forensics and an effective facilitator for rapid incident response. As such, DNS is uniquely positioned to assist financial institutions in executing a range of DORA compliance activities, including:

- ICT Risk Management (Chapter II)
- ICT-Related Incident Management, Classification and Reporting (Chapter III)
- Digital Operational Resilience Testing (Chapter IV)
- Managing of ICT Third-Party Risk (Chapter V)
- Information-Sharing Arrangements (Chapter VI)



Chapter II: ICT Risk Management → Article(s) 1, 5, 7, 9, 10, 13

Chapter III: ICT-Related Incident Detection and Response → Article(s) 17, 18

Chapter IV: Digital Operational Resilience Testing → Article(s) 24, 25, 26

Chapter V: Managing ICT Third-Party Risk → Article 28

Chapter VI: Information-Sharing Arrangements → Article 45

Figure 1. Where DNS contributes to DORA compliance activities

It should be noted that in addition to aligning with particular DORA principles, the efficacy of DNS is such that many organizations would benefit from enlisting its capabilities in meeting most of the regulation. Because DNS is already integrated into organizational networks, it offers a more practical and efficient way to enhance resiliency and security than adopting entirely new technologies and controls. When considering where DNS can contribute to DORA activities, entities should apply the proportionality principle in Article 4 of the regulation.

The recommendations below are organized by relevant chapters from the DORA guidelines, along with notations for the specific Articles from the regulation with which they align.

ICT RISK MANAGEMENT

Many financial organizations view DNS as “just part of the network plumbing,” but it is critical to the operational resilience DORA strives to improve. A DNS outage is catastrophic as it impacts nearly all applications and services throughout a financial institution. For this reason, entities complying with DORA should incorporate DNS service availability into risk management planning on par with other core systems.[6] Part of that effort involves using industry best practices in implementing and managing internal DNS infrastructure.

In addition, because financial institutions regularly interact with outside entities and external users, equal attention must be paid to security hygiene around external DNS. For compliance purposes, organizations should ensure that public (authoritative) DNS domains remain resilient and secure. Threat actors actively target misconfigured authoritative domains due to loose security policies and processes. External DNS management may also involve third parties, for which the regulations are still applicable, so those responsible for DORA compliance should take risk management and mitigation of DNS services associated with these parties into consideration.

Recommendations:

- Implement resilient DNS architectures, designed to support service continuity and sized for peak capacity, along with consistent policies and procedures to maintain DNS infrastructure and service availability and security. (Articles 7, 9)
- Ensure one part of the organization is responsible for managing external domain names, acting as an internal registrar/registry, to avoid disparate parts of the organization registering and managing domains via multiple suppliers. (Article 5)
- Implement Protective DNS services to block and log malicious DNS traffic, prevent DNS from being used for data exfiltration, identify anomalous traffic and provide data for forensics and incident response. (Articles 9, 10, 13)

ICT-RELATED INCIDENT MANAGEMENT, CLASSIFICATION AND REPORTING

Security practitioners use DNS during incident response to identify and block further malicious communication and aid in the classification and scope of any compromise. All network communications begin with a DNS query, making the logs, which contain query and response data, along with DHCP logs and asset information, critical to incident management. For instance, ready access to records of which devices on a network may have communicated with a malicious host helps security teams identify the scale and classification of any incident. Similarly, DHCP logs identify which IP addresses have been associated with a given asset. As most security logs identify devices based on transient rather than fixed IP addresses, organizations that wish to ensure accurate and consistent event and threat correlation should ensure that relevant device-level data and context can be shared with security operations tools.

Recommendations:

- Continuously log DNS query and response data, DHCP lease activity and asset data to facilitate accurate event correlation and provide context for forensics as part of incident management. (Articles 17(3), 18(1))
- Implement Protective DNS services as a control point for blocking malicious DNS traffic. This control point should include threat intelligence related to the indicators used in the Protective DNS service, so that the context associated with any blocked traffic can be shared with security ecosystem tools to aid in assessment. (Article 17)

DIGITAL OPERATIONAL RESILIENCE TESTING

Meeting the digital resilience standard for DORA requires additional testing for business continuity and disaster recovery (Article 24), as well as vulnerability and penetration testing within a competent authority framework (Articles 25 and 26). As with risk considerations, those overseeing DORA compliance should consider the foundational role that DNS serves in network availability. For example, organizations can leverage DNS to provide business continuity through global server load balancing. On the disaster recovery front, a DNS outage due to a cyberattack, misconfiguration or natural disaster can cause business operations to cease. Therefore, it is imperative that financial institutions fortify DNS and associated critical network services, such as DHCP, to meet operational resilience requirements.

Recommendations:

- Review internal and external DNS architecture and services for "identifying weaknesses, deficiencies and gaps in digital operational resilience, and of promptly implementing corrective measures." Technical standards such as NIST 800-81 may be useful in this regard. (Article 24(1))
- When developing a comprehensive digital operational resilience testing program, ensure it specifically covers DNS services, infrastructure and protocols. Restoring DNS services is an essential prerequisite to the recovery of an organization's applications and services, and DNS itself may facilitate continuity of service and disaster recovery. (Article 24(1))
- Given a network's reliance on DNS, ensure that specific testing procedures for DNS services and infrastructure are part of the overall resilience testing plan. (Article 24(2))
- When testing operational resilience and working with external threat-led penetration testing (TLPT) providers, ensure specific DNS-related tests are carried out for availability and security. (Articles 25, 26)
- Key areas to include:
    - » Verify DNS resiliency is working as designed, especially that there are multiple redundant paths for name resolution.
    - » Ensure that outbound DNS traffic from an organization's networks routes through controlled DNS resolvers (that should log query and response data).
    - » Query for domain names associated with the current malicious activity.
    - » Test if it is possible to exfiltrate data via DNS queries and to infiltrate malware via DNS responses.
    - » Put in place procedures and automated tools that take DNS security hygiene into account, such as ensuring that dangling domain names and incorrect delegation of subdomains are rectified.

MANAGING ICT THIRD-PARTY RISK

DNS services, such as external DNS, are within the DORA scope because third parties may manage them. Additionally, they may also manage DNS subdomains that have been delegated to them for specific services.

Recommendations:

- Review agreements with any third parties managing DNS services or infrastructure, such as external domains, to ensure they conform to your organization's regulations and policies and provide the same operational resiliency and security levels. (Article 28)

INFORMATION-SHARING ARRANGEMENTS

Financial institutions regularly share indicators of compromise (IoCs) and tactics, techniques, procedures (TTPs) with trusted financial services communities, including appropriate protections to safeguard sensitive information. Within these trusted groups, financial entities can use DNS query and response logs, as well as information from blocked malicious domains, as part of the information they share.

Recommendations:

- Prepare for information sharing by implementing a policy to provide DNS-related IoCs. Agreeing on data formats with a sharing group in advance would help operationally, especially where indicators will be ingested into operational tools such as a security information event management (SIEM) system. In particular, information from malicious activity captured and shared through Protective DNS services often helps other financial entities elevate network defense. (Article 45)

SIMPLIFY DORA COMPLIANCE WITH INFOBLOX

To more easily achieve DORA compliance, financial organizations should align their DNS services with DORA principles by focusing on resilience and security to manage ICT risks effectively. This alignment includes enhancing protections against threats like phishing and data exfiltration and adhering to frameworks like TIBER-EU and MITRE ATT&CK for threat intelligence. Infoblox offers solutions tailored to mitigate these risks and support compliance with ICT risk management regulations.

Additionally, Infoblox's robust DNS infrastructure and security solutions are uniquely positioned to support financial entities in achieving compliance with DORA's principles. By focusing on secure and resilient DNS services, Infoblox helps those under DORA mitigate risks associated with unmanaged DNS communication, such as phishing, malware command and control and data exfiltration. Leveraging industry-leading frameworks like MITRE ATT&CK, Infoblox provides actionable intelligence and tailored mitigations that align with ICT risk management requirements. Furthermore, Infoblox's expertise in integrating guidelines from ENISA and NIST ensures that financial entities fulfill availability and security obligations while navigating complex regulatory landscapes effectively.

[1] How the digital operational resilience act helps your continuity, PwC.
[2] DORA Chapter 1 General Provisions, Article 1(1) Subject Matter
[3] Final Report on draft RTS specifying elements related to threat led penetration tests (reference JC 2024 29), European Securities and Markets Authority (ESMA), July 07, 2024.
[4] What is TIBER-EU?, European Central Bank.
[5] Adopting TIBER-EU will help fulfil DORA requirements, European Central Bank, September 2024.
[6] DORA Regulation "(22) 'critical or important function' means a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law."

infoblox

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20250625v1