WHITEPAPER

# DORA Readiness

## From Regulation to Resilience: A Practical Guide to DORA

cybersift

CYBERSIFT COMPLIANCE PLANNER AND EXECUTOR

# Digital Operational Resilience Act (DORA)

This whitepaper delves into the fundamental principles of the Digital Operational Resilience Act (DORA), including its objectives, coverage, and requirements for managing IT risks, reporting incidents, testing resilience, and managing third-party risks. It also explains how Darktrace's Cyber AI can assist organizations in meeting DORA's requirements.

## What is the Digital Operational Resilience Act (DORA)?

The financial services industry has historically been a prime target for threat actors, with stringent regulatory scrutiny. To meet these challenges, the European Union (EU) has introduced the Digital Operational Resilience Act (DORA), a regulation that establishes a binding, comprehensive information and communication technology (ICT) risk manage- ment framework for the EU financial sector. DORA aims to comprehensively address ICT risk management in the financial services sector and harmonize the ICT risk management regulations that already exist in individual EU member states. DORA applies to all financial institutions in the EU, including traditional financial entities such as banks, investment firms, and credit institutions, as well as non-traditional entities such as crypto-asset service providers and crowdfunding platforms. Notably, DORA also applies to third-party service providers that supply financial firms with ICT systems and services, such as cloud service providers and data centers, and firms that provide critical third-party information services, such as credit rating services and data analytics providers.

## DORA Timeline & Specifications

DORA establishes technical standards that financial entities and their critical third-party technology service providers must implement in their ICT systems by 17 January 2025. These standards aim to remove the gaps, overlaps, and conflicts that could arise between disparate regulations in different EU states and create a universal framework for managing and mitigating ICT risk in the financial sector.

# 5 Pillars of DORA

DORA introduces specific requirements for financial entities and ICT providers across fiver pillars: ICT risk management, testing and incident reporting, third-party risk management, Resiliance testing & Information Sharing. These requirements include conducting regular ICT risk assessments, implementing ICT disaster recovery plans, and establishing processes for managing ICT incidents and reporting incidents to competent authorities

## ICT Risk Management

Implementing and maintaining robust ICT systems and technologies is crucial for mitigating ICT risks. This involves continuously identifying all sources of ICT risks and implementing preventive measures to address them. One essential measure is establishing a system for promptly detecting unusual actions, which can help organizations respond quickly to potential threats. In addition to preventive measures, organizations must develop and implement business continuity strategies and disaster recovery plans. These plans should ensure quick recovery from ICT-related incidents, minimizing the impact on business operations and customers. Moreover, organizations should establish mechanisms for learning and evolving from both external events and internal ICT issues. This involves regularly reviewing and updating ICT risk management strategies based on new threats and vulnerabilities, as well as lessons learned from past incidents. By continuously monitoring and improving ICT risk management strategies, organizations can build resilience and ensure the reliability and availability of their ICT systems.

## ICT Incident Reporting

The Digital Operational Resilience Act (DORA) is a comprehensive framework that aims to ensure the operational resilience of financial entities in the European Union (EU). It outlines procedures for managing ICT-related incidents, including record- ing, classification, and reporting. Financial entities are required to establish and implement incident management processes to detect, manage, and report ICT-related incidents, and to put in place early warning indicators as alerts. They must also establish appropriate processes to ensure a consistent and integrated monitoring, handling, and follow-up of ICT-related incidents, to identify and eradicate root causes to prevent the occur- rence of such incidents. DORA also requires financial entities to establish and implement a management process to monitor and log ICT-related incidents, followed by an obligation to classify them based on criteria detailed in the regulation and further developed by the European Supervisory Authorities (ESAs) through regulatory technical standards. The ESAs are required to specify materiality thresholds, and only ICT-related incidents that are deemed major must be reported to the competent authorities using a common template and following a harmonised procedure. Financial entities should submit initial, intermediate, and final reports and inform their users and clients where the incident has or may have an impact on their financial interests.

## Third-Party Risk Management

Financial entities are responsible for managing ICT third-party risk as an integral component of their ICT risk management framework, in accordance with the principles of proportionality and responsibility. They must adopt and regularly review a strategy on ICT third-party risk, taking into account the multi-vendor strategy where applicable. The strategy should include a policy on the use of ICT services supporting critical or important functions on a sub-consolidated and consolidated basis. Financial entities should maintain and update a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers, distinguishing between those that cover ICT services supporting critical or important functions and those that do not. DORA requires financial entities to establish and implement an ICT-related incident management process to detect, manage, and notify ICT-related
incidents. They must put in place early warning indicators as alerts and establish appropriate processes to ensure a consistent and integrated monitoring, handling, and follow-up of ICT-related incidents. The ICT-related incident management process should establish procedures to identify, track, log, categorize, and classify ICT-related incidents according to their priority and the severity and criticality of the services impacted. Roles and responsibilities for different ICT-related incident types and scenarios should be assigned, and dedicated and comprehensive business continuity policies and disaster and recovery plans should be put in place as an integral part of the operational business continuity policy. Harmonizing and streamlining the reporting of ICT-related incidents is achieved via a general requirement for financial entities to establish and implement a management process to monitor and log ICT-related incidents, followed by an obligation to classify them based on criteria detailed in the regulation and further developed by the ESAs.

## Digital operations Resiliance Testing

The Digital Operational Resilience Act (DORA) requires financial entities to establish a robust ICT risk management framework, which includes the detection and management of risks related to the usage of ICT. This framework should be propor- tionate to the entity's size, business, and risk profile. The European Supervisory Authorities (ESAs) will develop draft regulatory technical standards (RTS) to specify the elements of the ICT risk management systems, protocols, and tools to minimize ICT risk and the components of the ICT business continuity plans. Regular checks of the ICT risk management framework are necessary to promptly identify and eliminate weaknesses, deficiencies, or gaps. Financial entities should implement counteractive measures as needed to ensure digital operational resilience. DORA's testing requirements are proportionate to the entity's size, business, and risk profile. Threat Led Penetration Testing (TLTP) or Red/Purple Team Assessment should be conducted to address higher levels of risk exposure. DORA also emphasizes the importance of manag- ing ICT third-party risks by establishing a struc- tured approach to assess, monitor, and mitigate risks associated with third-party ICT service providers. Financial entities should conduct comprehensive due diligence on potential service providers, maintain detailed registers of all contractual arrangements, and perform regular audits to ensure ongoing compliance with DORA standards and contractual obligations. DORA's provisions for third-party ICT risk man- agement are designed to safeguard the financial sector from the vulnerabilities that arise from external dependencies. By adopting a holistic approach to DORA compliance, financial entities can ensure that their operations are not only resilient but also contribute to the stability and security of the broader financial ecosystem.

# Information sharing

The Digital Operational Resilience Act (DORA) emphasizes the importance of information sharing and collaboration among financial entities to enhance digital operational resilience. DORA encourages financial entities to share cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cybersecurity alerts, and configuration tools. This sharing is intended to raise awareness of cyber threats, limit or impede the ability of cyber threats to spread, support financial entities' defensive capabilities, threat detection techniques, mitigation strategies, or response and recovery stages. The information sharing arrangements must protect the potentially sensitive nature of the information shared and be governed by rules of conduct that respect business confidentiality, personal data protection, and guidelines on competition policy. These arrangements should define the conditions for participation, operational elements such as the use of dedicated IT platforms, and the involvement of public authorities where appropriate. Financial entities are required to notify competent authorities of their participation in these information-sharing arrangements.

# How CyberSift, helps with DORA

The financial services industry has historically been a prime target for threat actors, with stringent regulatory scrutiny. To meet these challenges, the adoption of the Digital Operational Resilience Act (DORA) introduces added compliance requirements for European financial organizations and CyberSift with a variety of Solutions & Services will assist you in keeping your business protected and compliant with DORA regulations.

## Maturity Assessment

Conducting a thorough maturity assessment is vital to evaluate alignment with DORA requirements for financial institutions, encompassing banks, payment institutions, investment firms, crypto asset service providers, and critical third-party ICT providers. Our in-house personel will be able to actively assess your systems to identify strengths and weaknesses in cybersecurity, operational resilience, and regulatory compliance. Subsequently, a gap analysis reveals disparities between the current state and DORA mandates.

CyberSift can support an entity's information by identifying misconfigurations and/or gaps in existing security controls, and can manage all incident reports and logs. Furthermore, our suite offers solutions that can be used to support a security testing and vulnerabilities by providing visibility to traffic patterns. CyberSift can support monitoring of third-party risks by detecting suspicious or anomalous activity (which may originate from a compromised/malicious third-party) Additionally, CyberSift has the ability of leveraging threat intelligence from industry powerhouses like IBM X-Force. Meticulously analyzing information from the community, we detect threats that slip past conventional barriers. With CyberSift SIEM, a versatile solutions delivered as a virtual or physical appliance or provisioned as a cloud service, we can assist your business to analyze popular Firewall and Windows events for anomalies out of the box. This will allow you to be provided with a foundation for security administrators and thus promptly respond to incidents and conduct in-depth investigations. To bridge these gaps and achieve compliance, a targeted mitigation plan is developed via our CyberSift DORA Tracker to plan and execute effectively. This plan includes implementing enhanced cybersecurity measures, strengthening operational resilience frameworks, updating regulatory compliance practices, conducting training programs, fostering collaboration with third-party providers, and establishing continuous monitoring mechanisms.

## Planning & Executing

The CyberSift DORA Tracker allows you to strategically map out a DORA compliance plan with ease. Allowing businesses to track and monitor progress of all the thourough requirments requested by Digital Operational Resilience (DORA) introduces that introduces a set of key obligations and broad ICT Risk Management Framework for Finance Sector. Throughout the process, adherence to DORA requirements will be paramount. This will be facilitated by the use of our DORA TRACKER. which will enable seamless tracking of progress, task completion, and alignment with regulatory mandates. Compliance with DORA is crucial for enhancing the operational resilience and security of the financial sector. Failure to comply with any of the DORA obligations may result in corrective actions and/or sanctions. To ensure effective implementation of all the obligations set out in DORA, it is essential that all affected institutions start preparing for DORA compliance. Our specialized tool, provides a detailed overview of an organization's digital resilience and help identify gaps that need to be addressed to achieve compliance. By integrating these strategies and technologies, we'll not only enhance the client's cybersecurity posture but also streamline the path to achieving compliance with DORA regulations.

## CyberSift DORA Tracker

The CyberSift Dora Tracker represents a cutting-edge assessment tool, conceived internally by our CTO, David Vassallo, with the precise aim of aiding businesses in comprehen- sively navigating the path to DORA compliance. This innovative solution facilitates a meticulous understanding of DORA's requirements, enabling businesses to effectively map their solutions to the core requisites outlined in the act. With 45 main articles and over 100 sub-articles to adhere to, tracking progress can be daunting. However, our tool simplifies this process, provid- ing clear insights into each regulation and guiding businesses through every step towards compliance. With our support every step of the way, achieving and maintaining DORA compli- ance becomes streamlined and achievable.

# Log Management

In order to meet the rigorous compliance demands of DORA, the implementation of central log management, fortified by robust security analytics, stands as an indispensable tool. This integrated system facilitates uninterrupted monitoring while also empowering organizations to generate high-fidelity alerts, significantly expediting the response, investigation, and recovery processes in the event of security incidents. It not only aids in fulfilling regulatory requirements but also strengthens the overall security posture of financial institutions, ensuring their operational resilience.

Cybersift SIEM offers Centralized log management that supports various DORA compliance aspects, including:

## Access Monitoring

It allows the user to have an outline of all the central log management that ingests access logs from various resources, aiding in detecting and investigating anomalous behavior.

## General System Monitoring

Give the user and overview of capacity utilization, Event Per Second (EPS) rates, an overview of alert statuses, with historical timelines. This multifaceted approach ensures a thorough understanding of the system's performance and its ability to respond effectively to any anomalies.

## Network Monitoring

Network security monitoring often entails the intricate task of correlating and analyzing data from a multitude of diverse tools, creating a comprehensive surveillance system to detect and respond to potential threats. Firewalls are central to network security, controlling incoming and outgoing traffic, including the detection of suspicious activities targeting potentially malicious servers. Complementing this, intrusion detection systems (IDS) and intrusion prevention systems (IPS) provide an added layer of defense, revealing potential evasion tactics used by cyber threats. This integration enhances network visibility and understanding.

## O365 Monitoring

Monitoring of Office 365 events, especially those related to phishing attempts, is a proactive approach to strengthening email security. By allowing users to keep a vigilant eye on these events, organizations can foster a sense of ownership and enhance their collective cybersecurity defenses.

## Web Attack

Our SIEM solution strengthens your defenses against web attacks by providing real-time monitoring, rapid threat detection, and centralized log management. It facilitates proactive incident response, ensuring swift actions to counter threats and streamline compliance reporting. With advanced analytics and user-friendly features, it's your key ally in defending against web attacks and fortifying your cybersecurity.

cybersift

# Custom Dashboards

CyberSift Siem offers fully searchable audit logging, threat detection, and detailed reports spanning every corner of your environment, ensuring not threat goes unnoticed. Built on Elasticsearch and supported by AWS and GCP, CyberSift SIEM is easily scalable, offering agility and customization. Its hybrid approach integrates anomaly- and signature-based systems, reducing false positives for a balanced and effective cybersecurity solution. CyberSift's in-house solutions are customizable and adaptable, enabling organizations to meet industry standards and regulations while maintaining a vigilant defense against security risks. With its advanced, AI-driven tools and state-of-the-art machine learning algorithms, CyberSift empowers organizations to stay ahead of potential threats and protect their digital assets effectively.
Via CyberSift SIEM you will be able to collect and analyze data from network endpoints and nodes, providing real-time threat intelligence and aiding in the detection of indicators of attack (IoA). These tools can identify patterns of anomalous behavior, assisting organizations in gaining insights into potential threats within their networks.



## Contact us

info@cybersift.io

+356 7949 8471 (MT)

+44 20 8638 0550 (UK)