CYERA

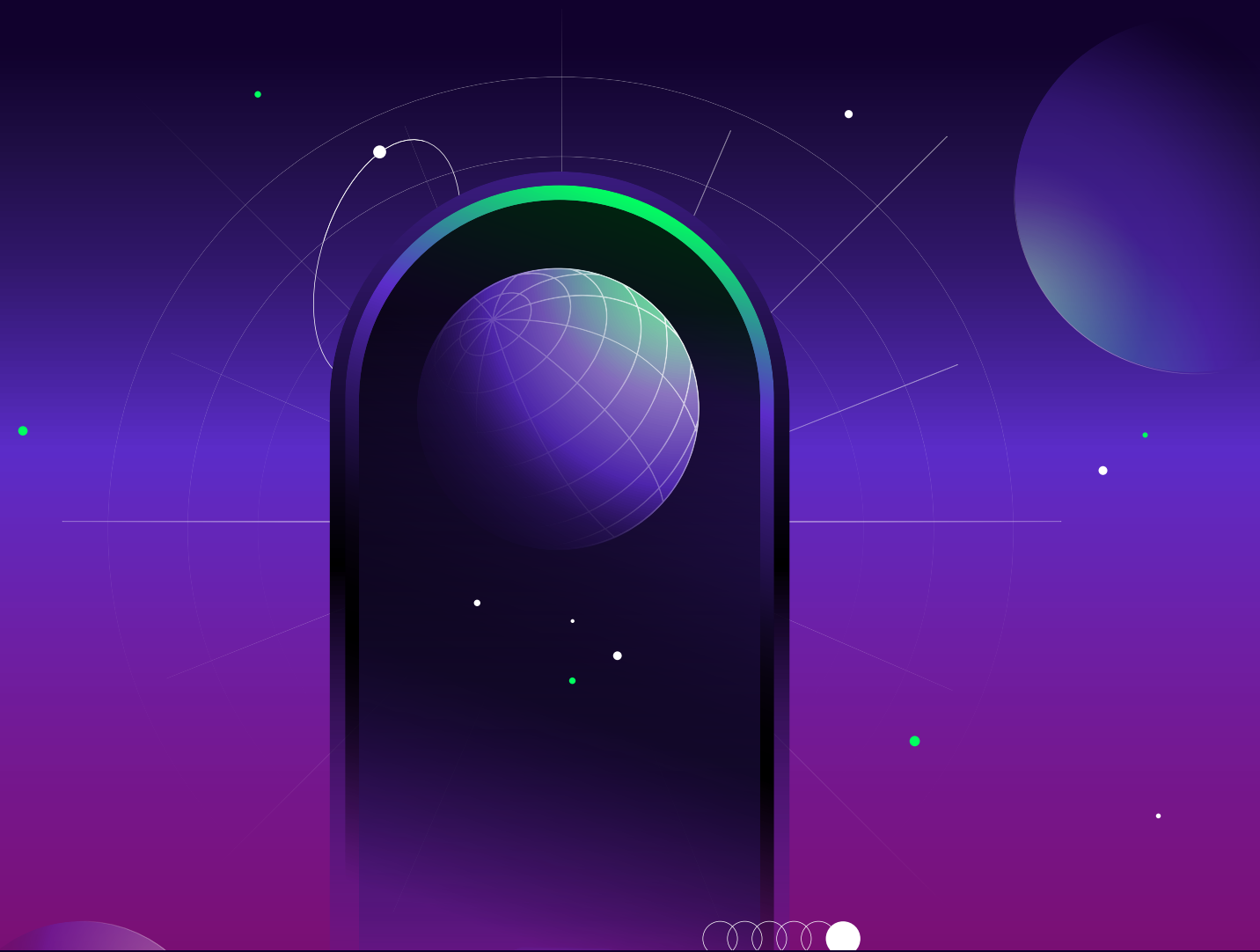
GUIDE

A Data-Centric Approach
to Digital Operational Resilience

How Cyera Supports DORA Compliance

Table of Contents

Introduction	3
ICT Risk Management	4
Incident Management, Classification, and Reporting	8
Digital Operational Resilience Testing	10
Third Party Risk Management	11
Information and Intelligence Sharing	12



Introduction

About DORA

The European Union enacted the Digital Operational Resilience Act (DORA) in response to the 2008 financial crisis. DORA aims to protect the stability and continuity of financial markets even in the face of severe information and communication technology (ICT) related incidents affecting multiple large institutions and/or ICT third-party service providers who support their critical business functions.

DORA is composed of five “pillars” - ICT Risk Management; Incident Management, Classification, and Reporting; Digital Operational Resilience Testing; Third Party Risk Management; and Information and Intelligence Sharing. Together, these pillars prescribe controls to protect financial entities’ information systems and assets, and prevent systemic risks that might arise from overreliance on certain ICT third party service providers.

About Cyera

Cyera is a unified, AI-native data security platform that empowers businesses to discover, classify and protect data. It allows security leaders to manage sensitive data across highly permissive and widely distributed environments with high precision and efficiency.

The platform’s agentless, fully automated data discovery provides a comprehensive inventory of sensitive data across structured and unstructured sources, and across IaaS, SaaS, DBaaS and on-premises environments. This capability enables organizations to address critical data challenges like data proliferation and drift. Powered by AI-native classification, Cyera goes beyond traditional methods by also understanding context, intent, and nuance - decoding data down to the DNA level. This deep insight helps uncover ghost data, reveal sensitive data risks, reduce false positives, and mitigate threats like data breaches and ransomware — areas where conventional data loss prevention and data governance tools fall short.

By combining advanced technology with ease of use, and scale from its cloud-delivered backbone, Cyera empowers organizations to confidently secure their data, maintain compliance, and unlock the full potential of their data to drive innovation.

ICT Risk Management

DORA requirements

Governance and organization
"Financial entities shall have in place an internal governance and control framework that ensures an effective and prudent management of ICT risk."

This requirement calls for the creation of a management body responsible for establishing cybersecurity controls, assessing and managing risk to ICT assets, and establishing business continuity policies, among other things.

ICT risk management framework
"Financial entities shall have a sound, comprehensive and well-documented ICT risk management framework as part of their overall risk management system, which enables them to address ICT risk quickly, efficiently and comprehensively and to ensure a high level of digital operational resilience."

The ICT risk management framework is responsible for developing strategies to protect information and ICT assets, minimizing risks to those assets, and promoting operational resilience.

ICT systems, protocols, and tools
Financial institutions must use updated ICT systems, protocols, and tools that are reliable, resilient, and adequate to the task of accurately processing all data necessary to support business activities.

Cyera capabilities

DORA's ICT Risk Management pillar encourages organizations to identify and prioritize their most mission-critical assets and processes, in order to build resilience into their operations in the most cost-effective manner possible. Cyera is a key component in that process.

With respect to risk analysis, Cyera discovers and classifies organizational data across your entire ICT ecosystem, including web and cloud-based services and storage buckets, with 95 percent precision. Crucially, this includes discovering and classifying exposed business critical data, much of which is often duplicate, stale or ghost data that had previously gone undetected.

Cyera continuously monitors your entire data estate, and can be configured to alert on policy violations or the occurrence of anomalous or suspicious activity. It also integrates with third party tools, including identity providers and SIEM tools, to help enforce your organization's data governance policies and support automated handling of processes like incident response or the remediation of access misconfigurations. Event logs can be leveraged to provide deeper analysis of data risks.

Cyera also offers a Data Risk Assessment service that provides your security officials with a virtual, CISO-led evaluation of your organization's data security posture relative to more than 30 control frameworks such as ISO 27001 and NIST CSF.

This service provides actionable intelligence that can help you immediately shrink your attack surface, gain greater visibility into potential threats, and develop a plan for improving your security posture going forward, including timelines and milestones.

DORA requirements	Cyera capabilities
Identification Financial entities must identify and classify: • All ICT supported business functions, roles and responsibilities, and ICT assets supporting those functions; • All sources of ICT risk, including cyber threats and vulnerabilities; • All information and ICT assets, wherever located, as well as network and hardware assets, and map their configurations; • All processes dependent on ICT third-party providers.	Cyera's AI-native DSPM identifies and classifies all of your organization's data, whether in the cloud or on-prem, with 95 percent precision. It can also identify who has access to your data, what kind of access they have, and what they're doing with it. No other DSPM solution provides such an accurate and complete picture of your entire data estate. Moreover, Cyera's Omni DLP can track when your data is sent to third-party applications and services. Cyera provides seamless visibility and control over the data that moves through your organization, helping you better understand the nature of your attack surface, and which processes are dependent on third-party providers.
Protection and prevention Financial entities must put in place an information security policy and security tools to protect the confidentiality, integrity, and availability of data at rest, in transit, and in use. This includes policies limiting physical and logical access to ICT assets, requiring strong authentication for users, and implementing risk-based change management procedures and controls.	Cyera's intuitive administrative dashboard allows your security team to implement controls aligned with most major frameworks, as well as customized policies unique to your organization. Cyera's Identity Access catalogues all entities that have access to your organization's data, whether human or non-human, internal or external. Cyera also discovers stale identities that still have access to sensitive data, and supports the implementation of multifactor authentication by determining whether entities with access to your data have enabled MFA or not. Cyera detects when sensitive data is accessible by users with insecure passwords or passphrases, and can trigger alerts for remediation.

DORA requirements	Cyera capabilities
Detection Deploy a defense-in-depth strategy that uses multiple layers of controls to detect and alert on anomalous activity. Ensure resources devoted to detection are adequate to the volume of traffic encountered by the system, and that alert thresholds and criteria are appropriately defined.	Cyera continuously monitors your entire data estate, logs data events, and engages in audit logging to track data movement across your organization, who's using it, and what they're using it for. Cyera's intuitive user interface makes it easy for administrators to detect anomalies and suspicious events, and engage in forensic analysis of events. Cyera integrates with a range of logging and monitoring tools, and alerts on the detection of anomalous or suspicious activity such as the sharing of large numbers of sensitive records.
Response and recovery Financial entities must put in place a business continuity plan that includes implementing, auditing, and testing a response and recovery plan for ICT related incidents. The response and recovery plan should ensure the continuity of critical functions, effectively respond to incidents to minimize damage, estimate losses, and manage communication with internal and external stakeholders.	Cyera supports the implementation of your response and recovery plan in several ways. For one thing, Cyera generates alerts on policy violations, and can classify them by criticality. It can determine the data blast radius from an incident, and also integrates with SIEM tools to support automated remediation workflows. More broadly, Cyera's AI-native DSPM understands your data at a very granular level, making it much easier to discover and prioritize the most critical dependencies and issues, as well as essential remediation actions necessary to ensure continuity of service and reduce loss exposure. Cyera's unmatched data visibility cuts operating expenses throughout response and recovery, reducing the time spent on remediation, data forensics, and crisis management communication.

DORA requirements	Cyera capabilities
Backup policies and procedures, restoration and recovery procedures and methods Financial entities must establish backup policies and restoration and recovery procedures. ICT systems that support backups should be physically and logically separated from source systems. Financial entities must also maintain redundant ICT capacities adequate to fulfill business needs. Recovery time and recovery point objectives for each function should be based on criticality of the function for market efficiency.	Cyera supports the implementation of your organization's data backup plan through unparalleled data discovery and classification capabilities. This capability helps define the scope of the backups that will be necessary to maintain service continuity in the face of serious incidents. Partnering with backup technology provider Cohesity, Cyera helps your organization manage its backups and verify their completeness.
Learning and evolving Financial entities should have in place the capability to ingest and analyze information about ICT-related threats and vulnerabilities, and to conduct incident reviews after major ICT-related incidents. Incident reviews should catalog lessons learned and suggest changes to improve the speed and effectiveness of incident response.	Cyera's Data Risk Assessment service provides your security officials and information technology teams with a virtual, CISO-led evaluation of your organization's data security posture relative to more than 30 control frameworks such as ISO 27001 and NIST CSF. The service provides actionable intelligence that can help you immediately shrink your attack surface, gain greater visibility into potential threats, and develop a plan for improving your security posture going forward, including timelines and milestones.
Communication Financial entities must put in place a crisis communication plan to facilitate communication of information about ICT-related threats, vulnerabilities, and incidents with internal and external stakeholders.	Cyera's Breach Readiness service helps your organization develop a meaningful and actionable crisis communication plan. This service leverages Cyera's data security platform in conjunction with virtual CISO-led tabletop exercises and OSINT and dark web intelligence to deliver actionable insights with respect to your specific operating environment. Breach Readiness will show you which data are at risk, the potential materiality of a breach, how your organization would respond, and most importantly, which issues can be proactively fixed to prevent a material data breach in the first place.

Incident Management, Classification, and Reporting

DORA requirements	Cyera capabilities
ICT-related incident management process Financial entities must put in place an ICT-related incident management process to detect, manage, and notify about ICT-related incidents. All incidents should be recorded to ensure consistent monitoring, handling, and follow-up of ICT incidents, as well as the identification, documentation, and mitigation of the incidents' root causes. Incidents should be classified and prioritized based on the severity of the threat to critical systems.	Cyera continuously monitors your entire data estate, logs data events, and engages in audit logging to track data movement across your organization, who's using it, and what they're using it for. Cyera also generates alerts upon violations of organizational policies, or on the occurrence of anomalous or suspicious events, and can classify events by criticality. When a data issue/alert is generated, Cyera has the ability to send a message via email, Slack, or other workflow channels directly to the data owner, notifying them of the issue and providing instructions and guidance for remediation. Cyera also integrates with SIEM tools to support automated remediation workflows.

DORA requirements	Cyera capabilities
Classification of ICT-related incidents and cyber threats The severity of an ICT-related incident should be assessed based on the number and/or size of the clients affected, the duration of the incident, the amount of data impacted, the criticality of the services affected, and the direct and indirect economic costs of the incident. Cyber threats should be classified based on the criticality of the services at risk.	Cyera is integral to the classification of ICT-related incidents and threats. Cyera's AI-native DSPM scans your organization's entire ICT ecosystem, including SaaS, IaaS, PaaS, and DBaaS services, as well as on-prem systems. It can identify and classify data according to category and sensitivity with 95 percent precision. This gives your organization greater visibility into stores of business critical data that you may not have been aware of, and helps you understand where that data resides and who is using it, making it easier to inventory business critical applications and services, and enforce zero trust access controls for all users. Cyera then continuously monitors and logs all data events. Alerts generated by Cyera inform administrators of the number and nature of records affected, which helps your organization understand the materiality of any breach and its blast radius. Furthermore, Cyera's DSPM, Identity Access, and Omni DLP can help your organization understand which users and services were involved in or affected by an incident.
Reporting of major ICT-related incidents and voluntary notification of significant cyber threats Financial entities must report major ICT-related incidents to the relevant authorities, and may report other incidents that they deem a threat to the financial system, users, or clients.	Cyera's unmatched data discovery and classification capability will help your organization rapidly determine the blast radius and materiality of any breach. No other DSPM solution makes it possible to fulfill your reporting requirements as promptly and accurately as Cyera can.

Digital Operational Resilience Testing

DORA requirements

General requirements for the performance of digital operational resilience testing
Financial entities must put in place a process of operational resilience testing to identify weaknesses, deficiencies, or gaps in their operational resilience.

Testing should be done by an independent party (internal or external), and should involve a range of assessments, methodologies, and tools.

Processes must be put in place to classify, prioritize, and mitigate any issues discovered through the testing process.

Testing of ICT tools and systems
Operational resilience testing should include a range of appropriate tests, including:

"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."

Advanced testing of ICT tools, systems, and processes based on threat-led penetration testing
Some large financial entities such as credit institutions and payment institutions must undergo threat-led penetration testing every three years, covering all relevant ICT services that support critical business functions.

Cyera capabilities

Cyera offers several services that can help your organization prepare for vulnerability and penetration testing.

Cyera's Data Risk Assessment service provides your security officials with a virtual, CISO-led evaluation of your organization's data security posture relative to more than 30 control frameworks such as ISO 27001 and NIST CSF. The service provides actionable intelligence that can help you immediately shrink your attack surface, gain greater visibility into potential threats, and develop a plan for improving your security posture going forward, including timelines and milestones.

Cyera also offers a service called Breach Readiness. This service leverages Cyera's data security platform in conjunction with virtual CISO-led tabletop exercises and OSINT and dark web intelligence to deliver actionable insights with respect to your specific operating environment.

Breach Readiness will show you which data are at risk, the potential materiality of a breach, how your organization would respond, and most importantly, which issues can be proactively fixed to prevent a material data breach in the first place.

By helping your organization identify and prioritize its areas of greatest data risk, Cyera can assist you in creating effective threat-led penetration testing programs that are demonstrably focused on building resilience.

Third Party Risk Management

DORA requirements

General principles
Financial entities must have in place a plan for managing the risk of relying on ICT third-party service providers.

Entities should employ a multi-vendor strategy to prevent the concentration of ICT risk.

Before onboarding an ICT third-party service, entities should assess the criticality of the functions the service would support, the suitability of the service provider to provide that support, any risks or potential conflicts of interests that the service provider would present, and an exit strategy for offboarding the service provider without disrupting business activities.

Assessment of ICT concentration risk
Whether onboarding a critical ICT third-party service would result in excessive concentration of ICT risk depends on:

1. Whether the service provided is not easily substitutable; and
2. Whether the financial entity would have in place multiple contracts with the same service provider for the provision of services supporting critical ICT functions.

Key contractual provisions
Article 30 of DORA sets out many required provisions that financial entities must include in service level agreements with their ICT third-party providers, to ensure adequate mitigation of ICT-related risks associated with the provision of those services.

Cyera capabilities

Cyera can help your organization assess its ICT concentration risk. First, Cyera's AI-native DSPM can discover all your organization's data and classify it by sensitivity. Then it can trace data through users and applications, giving the organization a better picture of which applications are the most heavily used, and by which users, including unsanctioned "Shadow IT" applications.

Cyera leverages data intelligence to show you where your critical dependencies lie, helping your organization better understand which applications and data are most critical to your day-to-day operations. In particular, by shining a light on Shadow IT, your organization can finally get a clear picture of its supply chain landscape, allowing you to determine whether your organization is over-reliant on a single vendor for multiple critical ICT functions.

Cyera's Omni DLP and Identity Access can also assist your organization in verifying that ICT third-party providers are adhering to some of the key contractual provisions required by DORA. That includes provisions concerning the location of data processing and storage, and the implementation of adequate access controls such as strong passphrases and multi-factor authentication.

Information and Intelligence Sharing

DORA requirements

Information sharing arrangements on cyber threat information and intelligence
To promote digital operational resilience, DORA encourages financial entities to participate in voluntary information sharing arrangements with other financial entities.

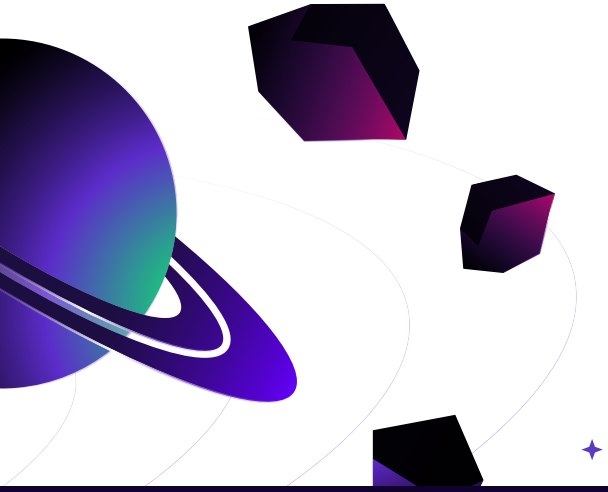
Participants should share intelligence on things like indicators of compromise, tactics, techniques, and procedures, security alerts, and configuration tools.

Participants in information sharing arrangements must ensure that sensitive data of their clients or customers is not inadvertently shared with unauthorized parties.

Cyera capabilities

With Cyera in place, your organization can confidently participate in information sharing arrangements to promote threat intelligence in the financial community.

Cyera's AI-native DSPM scans and classifies all your organization's data across IaaS, PaaS, SaaS, and DBaaS services, as well as on-prem systems. The comprehensive picture of your data estate that Cyera provides enables you to identify the most meaningful data to be shared with other organizations. Cyera helps you ensure the data you share is accurate and credible, without the risk of a lot of false positives.



CYERA.IO