WHITEPAPER

Digital Operational Resilience Act

Building operational resilience with Sekoia

Prepared by Sekoia

White paper · Compliance · Financial services

CONTENTS

Table of contents

DORA's core areas....3

Who needs to prepare for DORA?....4

From governance to operational resilience....4

Threat led testing with relevant intelligence....5

Turning intelligence into an exercise plan....5

From strategic context to technical data....6

Protecting, tracking and reporting....6

From alert handling to accountable reporting....7

Managing ICT dependencies and supply chain exposure....8

Structured intelligence for coordinated defense....8

A resilient platform for a regulated ecosystem....9

A practical path to digital operational resilience....9

About Sekoia....11

The Digital Operational Resilience Act, known as DORA, establishes a common framework for managing information and communication technology risk across the European financial sector. It applies to financial entities and to relevant ICT third party service providers whose services support them.

DORA is now in its application and enforcement phase. Financial organizations must connect governance, risk management, incident handling, resilience testing, information sharing and third party oversight into one operating model. Compliance is therefore not a documentation exercise. It depends on whether teams can detect, investigate, respond to and learn from disruption across the information system.

This white paper explains the core DORA obligations and shows how the Sekoia SOC platform can support the operational work behind them, from threat informed resilience testing to AI assisted investigation, response automation, evidence management and reporting.

AT A GLANCE

DORA's core areas

DORA core area	What it requires
ICT risk management	Identify and manage ICT risk through governance, controls and continuous oversight.
Incident management and reporting	Classify, investigate, contain and report ICT related incidents with reliable evidence.
Resilience testing	Test whether critical systems, processes and response plans withstand realistic disruption.
Third party ICT risk	Assess and monitor ICT dependencies, including critical service providers and supply chain exposure.
Information sharing	Share relevant threat information and operational lessons with trusted communities and authorities.

SCOPE

Who needs to prepare for DORA?

DORA covers a broad range of financial entities, including banks, payment and electronic money institutions, investment firms, insurance and reinsurance undertakings, trading venues, crypto asset service providers, pension institutions and other regulated organizations. It also creates a framework for oversight of ICT third party service providers that support the financial sector.

The exact obligations depend on the entity, its size, its risk profile and the role it plays in the financial ecosystem. The compliance program should therefore begin with a documented scope assessment and a clear inventory of critical business services, information assets, ICT dependencies and third parties.

THE OPERATING MODEL

From governance to operational resilience

DORA connects board level accountability with day to day security operations. A resilient program needs a clear owner for ICT risk, documented policies, tested response procedures, reliable detection and investigation, and evidence that controls work in practice.

Governance	Operations	Evidence
Management bodies approve and oversee the ICT risk management framework.	Security teams monitor, investigate and respond to threats across the information system.	Organizations retain the records, metrics, reports and test results needed to demonstrate control effectiveness.
Policies should reflect the entity's risk profile and critical services.	Incident processes must be coordinated with business continuity and crisis management.	Findings from incidents and tests should feed continuous improvement.

RESILIENCE TESTING

Threat led testing with relevant intelligence

DORA places resilience testing at the center of operational preparedness. Testing should do more than confirm that a control exists. It should challenge the organization with scenarios that reflect the threat actors, intrusion patterns and dependencies most relevant to its business.

Threat intelligence helps teams move from generic exercises to evidence based scenarios. Sekoia Intelligence provides context on threat actors, intrusion sets, campaigns, infrastructure, malware and indicators of compromise. That context can inform threat led penetration testing, red team exercises, crisis simulations and detection validation.

A practical exercise can follow the path of a real operation: identify the threat actor and intrusion set, reconstruct the campaign, map the infrastructure and malware involved, then test whether the organization can detect, investigate, contain and recover from the activity.

Turning intelligence into an exercise plan

Investigation level	How it informs resilience testing
Threat actor and intrusion set	Select an adversary profile and the techniques associated with it.
Campaign and infrastructure	Build a realistic scenario around the sequence of activity and the services it targets.
Malware and indicators	Define the technical artifacts that should be detected, investigated and shared.
Detection and response	Validate coverage, escalation, playbooks, communications and recovery decisions.

THREAT INTELLIGENCE

From strategic context to technical data

Sekoia Intelligence combines attacker knowledge with operational data that security teams can use in investigations and exercises. It helps organizations understand the risks affecting financial services, connect strategic reporting to technical indicators and improve detection content around relevant tactics, techniques and procedures.

- **Strategic context:** Threat reports help decision makers understand the threats, motivations and trends relevant to their sector.
- **Operational context:** Indicators of compromise, intrusion set information and detection insight help analysts investigate activity in the environment.
- **Exercise design:** Threat intelligence provides the basis for scenarios that are relevant to the organization rather than generic tabletop assumptions.
- **Information sharing:** Standardized formats such as STIX and MITRE ATT&CK help teams exchange structured information with partners and authorities.

DETECTION AND RESPONSE

Protecting, tracking and reporting

DORA requires financial entities to detect, respond to and recover from ICT related incidents on an ongoing basis. That requires continuous monitoring, centralized event collection, correlation, investigation and coordinated response across networks, systems and applications.

The Sekoia SOC platform brings detection, investigation, response automation and cyber threat intelligence into one operating environment. Sekoia Defend provides the detection, triage, case management and response engine. Sekoia Elevate adds AI agents that investigate, correlate, explain and recommend action. Together, they help security teams move from an alert to a documented decision with less manual work.

- **AI assisted investigation:** Sekoia Elevate investigates and triages alerts automatically. What used to take hours now takes minutes, roughly 5x faster, helping teams establish severity and impact sooner.
- **Response automation:** Sekoia Defend uses playbooks to coordinate containment, enrichment, escalation and follow up actions across connected tools.

- **Contextual detection:** Sekoia Intelligence provides attacker knowledge and detection insight that help teams prioritize relevant activity.
- **Exposure context:** Sekoia Reveal adds asset, identity, exposure and vulnerability context to help analysts understand what is at risk and prioritize action.
- **Operational evidence:** The Sekoia SOC platform keeps alerts, cases, events and investigation context together so teams can support reporting, reviews and post incident learning.

INCIDENT MANAGEMENT

From alert handling to accountable reporting

A DORA incident process should define how events are detected, classified, escalated, investigated, contained and reported. It should also make clear who owns each decision and what evidence is required at every stage.

Operational question	Sekoia capability
What happened?	Correlated events, detection content, CTI and investigation context provide a common view of the incident.
How serious is it?	Sekoia Elevate accelerates first level investigation, while analysts retain control over the verdict and escalation path.
What should happen next?	Sekoia Defend playbooks coordinate response actions, enrichment, notifications and handoffs.
What can we prove?	Cases, alerts, events and response history provide a traceable record for reporting and review.
What should change?	Threat intelligence, detection coverage and incident findings feed exercises and control improvement.

THIRD PARTY RISK

Managing ICT dependencies and supply chain exposure

DORA treats ICT third party risk as part of operational resilience. Financial entities need a clear view of the services they depend on, the information those services process, the risks they introduce and the response arrangements that apply when a provider is disrupted.

Sekoia supports this work by bringing third party signals into the same detection and investigation workflow as internal activity. Sekoia Reveal can add exposure, asset and identity context. Sekoia Defend can correlate signals across connected systems and coordinate response. Sekoia Intelligence can provide threat context for suppliers, technologies and attack patterns that affect the financial sector.

- **Dependency visibility:** Connect relevant logs and security signals so teams can monitor the services and environments that matter to critical operations.
- **Prioritized remediation:** Use exposure and vulnerability context to focus attention on assets, identities and dependencies with the greatest operational relevance.
- **Coordinated response:** Use playbooks to define actions across internal teams, providers and other stakeholders.

INFORMATION SHARING

Structured intelligence for coordinated defense

DORA encourages financial entities to share cyber threat information and lessons learned through trusted channels. The value of sharing depends on the quality, structure and context of the information exchanged.

Sekoia Intelligence and the Sekoia SOC platform support structured information through formats and frameworks such as STIX and MITRE ATT&CK. This makes it easier to move from a raw indicator to a useful picture of the threat, the affected assets, the techniques involved and the actions already taken.

SECURITY ASSURANCE

A resilient platform for a regulated ecosystem

As a technology provider serving security teams, Sekoia treats platform security, vulnerability management, monitoring and transparency as part of its responsibility to customers and partners. The current security program, hosting model and certification claims should be confirmed against the latest Trust Center information before publication.

- **Security assurance:** Sekoia is certified according to ISO/IEC 27001, PCI DSS, the Spanish ENS and SOC 2 Type 1 report.
- **Vulnerability management:** Our product is pentested annually by leading auditors and continuously tested for vulnerabilities.
- **Internal monitoring:** Our SOC platform is used to monitor all company activities, and the Sekoia CERT is a recognized member of InterCERT.
- **Transparency:** Do you want to know more about our security program? Discover the Sekoia transparency hub: https://trust.sekoia.com

CONCLUSION

A practical path to digital operational resilience

DORA turns operational resilience into a continuous management responsibility. Financial entities need more than policies. They need a working system that connects threat intelligence, detection, investigation, response, testing, reporting and improvement.

Sekoia helps security teams build that operating model on an open SOC platform. Sekoia Intelligence brings attacker knowledge. Sekoia Defend brings detection and response. Sekoia Elevate accelerates investigation with AI agents. Sekoia Reveal adds context on assets, identities and exposure. Together, these capabilities help organizations make better security decisions, support their reporting obligations and prepare for realistic disruption.

The objective is clear: make resilience measurable in daily operations, not only during an audit.

ABOUT

About Sekoia

Sekoia is the European agentic cybersecurity company building the Cyber Operations Platform for the AI era. Unifying cyber threat intelligence, detection and response, exposure management, and agentic AI, Sekoia is rebuilding cybersecurity from the ground up. Through the Autonomous SOC, machines investigate at scale while security teams govern operations with clarity and control. Fully open and agnostic by design, the platform helps organizations achieve strategic and tech autonomy. From SMEs supported by MSSPs to Fortune 2000 enterprises, Sekoia makes advanced defense accessible to all.

Read more on www.sekoia.com

GET IN TOUCH

Act from clarity

Talk to our team about where you stand on DORA — and what to build next.

sekoia.com

trust.sekoia.com · Security & compliance portal