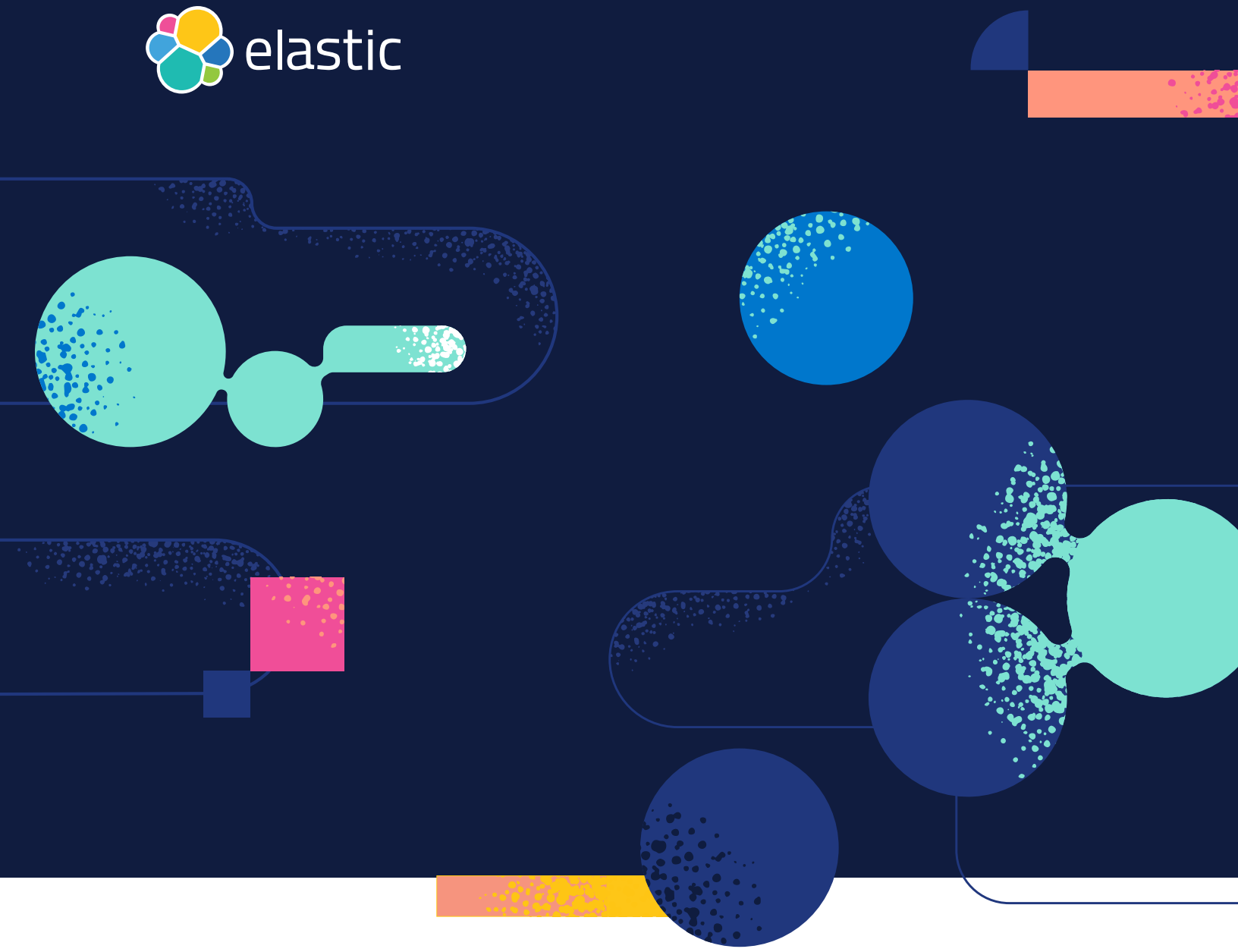


Addressing Operational and Digital Resilience Holistically Under DORA

Understand your interconnected risks at a global, enterprise level with a unified platform

Table of Contents

SECTION 1

How prepared are you for DORA's impact?

DORA calls for a broader understanding – and global view – of digital risks

As financial institutions become more digitally sophisticated and interconnected, regulators are raising concerns about the associated operational risks.

Ransomware attacks on financial institutions globally are up **nearly 10%** from a year ago. The average cost to fully recover:

$2.23 million.

Source: InvenioIT (Sophos report); average cost is for 2023 and does not include actual ransom payments

Regulations aimed at strengthening the digital resilience and operational resilience of financial entities are nothing new; however, they've historically been addressed as siloed issues. The EU's **Digital Operational Resilience Act (DORA)** is the first to merge the two issues together under a single regulation.

Acknowledging the business reality that operational and IT risks are inextricably linked, DORA requires institutions to develop a deeper understanding of how the information and communication technology (ICT) across their ecosystem impacts operations. For example, how might a natural disaster affect the ability of critical third-party ICT vendors in that region to deliver continuous service? What business processes would that affect and how would it impact customers?

Critical aspects of DORA

Compliance deadline	January 17, 2025
Organizations impacted	A broad range of financial institutions in the EU, as well as their ICT providers (regardless of their location).
Primary concern	"ICT incidents and a lack of operational resilience have the possibility of jeopardizing the soundness of the entire financial system, even if there is "adequate" capital for the traditional risk categories."
Key areas of focus	Explicitly addresses ICT risk and sets rules on: • ICT risk management • Incident reporting • Digital operational resilience testing • Third-party risk monitoring

Source: https://www.digital-operational-resilience-act.com/

DORA compliance is mandatory; violators face serious penalties.

Fines can reach as high as 10 million euros or 5% of the entity's total global annual revenue, whichever is higher.

Criminal penalties are on the table as well for responsible individuals within the institution, depending on the severity and nature of the non-compliance.

Sources: SealPath and F5

Adopting a more unified approach

While different teams within a financial institution will address the technical requirements of DORA, leaders must think holistically about the key driving force behind this regulation: *How can you develop an integrated view of your ICT and operational risks in order to strengthen your operational resilience?*

Four fundamental areas need to be addressed:

Improve visibility into the ICT risks across your entire ecosystem

Empower teams to find the information they need faster

Strengthen accountability at every level

Tighten control over third-party ICT risks

DORA presents a valuable opportunity. Institutions have a chance to revisit critical challenges around digital resilience, bring diverse parts of the organization together, and transform fundamental capabilities that will maintain the resilience of the financial ecosystem. Given the systemic reach of digital technologies, financial institutions and ICT providers can work together to increase trust in the industry and create value for the long term.

McKinsey, "Europe's new resilience regime: The race to get ready for DORA" (June 2024)

SECTION 2

Strengthen your digital operational resilience

Improve visibility into the ICT risks across your entire ecosystem

What DORA requires

A comprehensive, well-documented ICT risk management framework that addresses multiple dimensions of risk, including dependencies on third-party service providers.*

The challenge you face

There's a sea of different tools and systems that keep critical business processes and functions running. When something goes wrong, it can be challenging to pinpoint the source of the problem or mitigate a ripple effect.

To address the challenge, you need to:

- ☑ Develop a more holistic view of ICT risks across internal systems, business processes, and third-party vendors.
- ☑ Adopt a common business process taxonomy to support a "common language" across functional stakeholders.
- ☑ Map internal systems, business processes, and third-party vendors to the taxonomy to support end-to-end understanding of potential risks.

> *Elastic Observability allows us to integrate data from the entire application chain, monitor that data, spot latencies, and alert the specific trading desk to the exact trades that could be affected.…We not only immediately know when something is wrong, but we can also understand why and quickly apply a fix.*
>
> **Observability Manager at a leading French-based international bank**

Read more about how the bank improved performance and operational efficiency with Elastic.

* Article 6, Digital Operational Resilience Act

Empower teams to find and detect potential issues faster

What DORA requires

Establish clear mechanisms, policies, and procedures to detect anomalies and report incidents quickly.*

The challenge you face

Siloed teams and data limit the speed at which you can identify, mitigate, and resolve potential ICT risks. The potential impact at the enterprise level isn't always clear, impeding decision-making.

To address the challenge, you need to:

- Create more transparency between systems to make it easier to analyze and access relevant information about ICT risks.
- Give teams a single source of truth for information, so they can collaborate more efficiently to resolve issues.
- Use automation and AI to find anomalies and provide real-time intelligence about the threat environment.

> *We have reduced the time to find the customer impact during incidents by 90% by having all the logging and telemetry data in Elastic and correlating events.*
>
> **Kartik Deshpande, Staff Software Engineer, WePay**

Dive into more detail about how Elastic helps WePay cut issue detection time and improve application performance.

* Article 9, 10, 17, Digital Operational Resilience Act

Strengthen accountability at every level

What DORA requires

Management is ultimately accountable for the organization's digital operational resilience. Effective oversight requires greater visibility and accountability across the entire organization.*

The challenge you face

Most leaders lack a timely, complete view of the ICT risks facing the organization. The information inside reports is stale by the time it reaches their inbox.

To address the challenge, you need to:

- ☑ Make it easier to share real-time data and information across security, compliance, operations, and IT teams to give everyone a shared understanding of current risks.
- ☑ Ensure your people consistently follow specific protocols for managing and reporting anomalies and incidents.

> *Elastic Security delivers value, including more freedom to do things such as automating processes, enriching data, and filtering false positives. The impact of that value can be multiplied across the organization.…We now have a unified approach to our security data and can detect issues quickly, as well as meet the data conservation requirements of financial regulators.*
>
> **Maxime Rousseau, Chief Information Security Officer, Personal Capital**

Learn how Personal Capital strengthened its security processes with Elastic.

* Article 5, Digital Operational Resilience Act

Tighten control over third-party ICT risks

What DORA requires

Manage and regularly review ICT risks related to third parties that support critical functions.*

The challenge you face

End-to-end delivery often involves a complex set of third-party and internal interactions. Managing and mitigating related risks requires the integration of dependencies and the understanding of this interconnectedness, as well as clear processes for handling them.

To address the challenge, you need to:

- ☑ Create more transparency between systems to make it easier to analyze and access relevant information about third-party ICT risks.
- ☑ Tighten controls with third parties to ensure contracts include the necessary provisions to be compliant with DORA.

Key questions every financial institution should ask critical third-party providers in light of DORA

1. *How do you support audits and audit rights for the services you provide?*
2. *How do you disclose security vulnerabilities in your products and services?*

* Articles 28-30, Digital Operational Resilience Act

SECTION 3

One solution to close the gaps

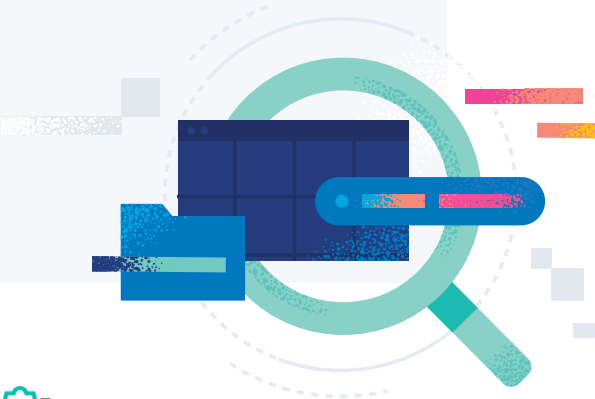
Elastic helps you close DORA compliance gaps

The good news is you're likely already collecting and documenting much of the information that DORA requires. You just need a more efficient way to find, analyze, and report relevant data. This is where Elastic excels: We help you connect the dots faster.

You don't have to change the tools you're already using or disrupt the flow of business. The Elastic Search AI Platform can work together with your current systems, data, and tools to bring together information in one place, creating greater transparency and efficiency. The Elastic Search AI Platform not only helps you fulfill DORA requirements but also can improve your digital operational resilience long-term.

The ideal state for DORA

- Comprehensive monitoring and alerts for anomalous behavior
- Rapid response and reporting to incidents
- Evidence of process and policy compliance across the enterprise
- A common product and service taxonomy across functions and system



How Elastic helps

Improve visibility

- Provides visibility, monitoring, and observability across your entire IT ecosystem via a single platform
- Aligns data to business processes by enriching logs, metrics, app data, business data, and third-party assessments, so you can better understand impact

Accelerate response times

- Automates anomaly detection, alerts, and investigation
- Shortens issue recovery time with automated workflows

Make reporting and governance easier

- Embeds your policies and procedures in automated workflows by ingesting relevant playbooks
- Enables flexibility in reporting, with real-time dashboards and time-stamped data that help you track trends over time
- Ingests vendor management data and assessment documents to help you quickly identify relevant information on mitigating and managing risks

Transform the way you manage ICT risks

Over the next decade, we'll see a wave of regulation around technology-related risks. DORA is a warning bell for what lies ahead.

One constant across these regulatory changes will be the need to better understand and observe what's happening across your ICT ecosystem.

Elastic's platform is well-positioned to help you prepare for what's next. We help you:

Balance the need for greater transparency and tight security.

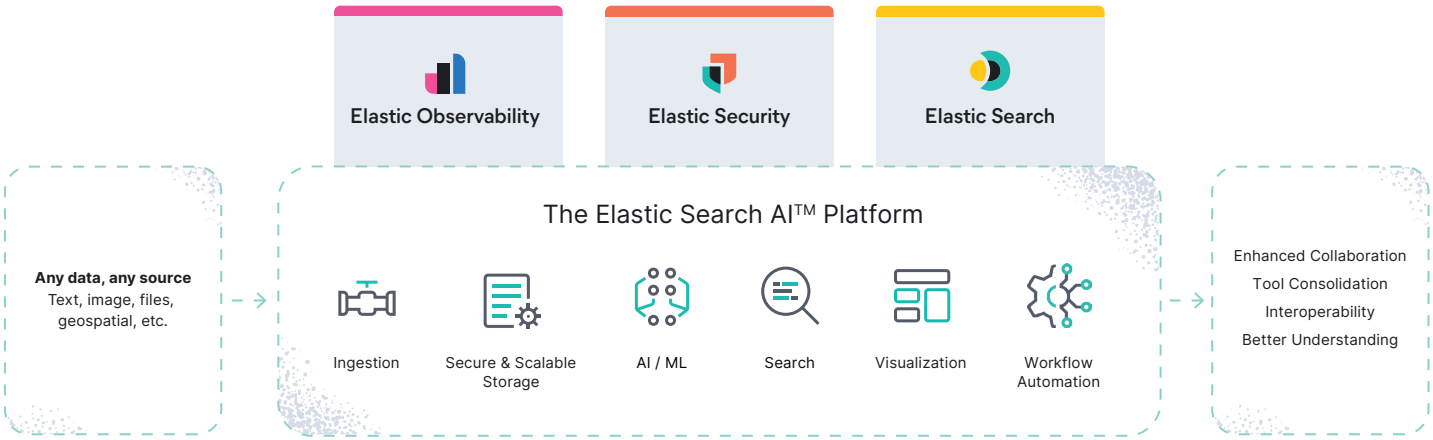
- Enable teams to access the right information at the right time, while keeping data security a top priority.
- Make it easier for management to understand what's happening in real time.

Improve productivity and efficiency.

- Scale work without straining resources with the assistance of AI and automation.
- Digest, analyze, and extract relevant information for reporting faster.
- Make it easier for teams to collaborate and work in parallel.

How Elastic works

The Elastic Search AI Platform leverages the speed, scale, and relevance of Search AI to power search, observability, and security solutions.



Elastic Observability

Quickly get to the root cause of why your systems aren't working as expected by:

- Surfacing the indicators that really matter
- Custom-building workflows for accelerated root cause and response
- Improving visibility across your entire ecosystem, across public and private clouds, as well as on-prem deployments

Elastic Security

Detect and respond to threats at speed and scale and make threat intelligence actionable by:

- Pulling in unstructured data from across your organization to search and correlate it all to identify patterns
- Automating threat detection
- Activating AI-powered security analytics
- Triaging alerts

Elastic Search

Help employees and customers quickly find what they need by:

- Providing visibility and real-time reporting for analysis across massive datasets
- Leveraging machine learning to determine what search results are most relevant
- Building generative AI experiences

How Elastic is addressing DORA

We're intimately familiar with the financial sector regulatory landscape.

Our deep bench of legal and compliance experts continuously monitor the global financial regulatory landscape. We regularly adjust our controls to keep customers compliant with changing requirements.

We work with institutions across every financial vertical.

wepay Emirates NBD DISCOVER ZURICH WELLS FARGO

Transparency and security are embedded in our product.

We have a team of security engineers, practitioners, and researchers who eat and breathe security: Elastic Security Labs provides our customers with the latest security intelligence research from across the globe. Our Trust Center provides real-time information about Elastic's compliance with various regulatory frameworks.

elastic

Elastic connects your digital resilience strategy

How we help financial services customers:
https://www.elastic.co/industries/financial-services

To learn more about how we can help you, contact:
https://www.elastic.co/contact?baymax=rtp&rogue=eswt-1165-b#sales