Digital Operational Resilience Act (DORA) for Financial Firms

Power Up Your Jakarta EE

Contents

Guide Updated: **May 2025**

Digital Operational Resilience Act (DORA) for Financial Firms

The Digital Operational Resilience Act (DORA) Application assists application developers working in highly regulated environments, such as financial institutions server providers, to implement enhanced application and data security.

Are you a Chief Information Security Officer or Compliance Officer working for a financial institution such as a corporate bank or insurance company with operations and customers living in the countries that belong to the European Union (EU)? Then one part of the development environment that you'll be focused on is runtime security, to help mitigate the risks to cardholder and other customer data. You must balance priorities between ensuring any application server platform adopted by your organisation aligns with internal security policies and complies with strict regulatory standards. However, mere compliance and avoidance of fines is insufficient. You can simultaneously carve out a competitive advantage while fortifying your resilience against security vulnerabilities. Also, you can monitor for security incidents while reinforcing your customers' trust.

In this guide, we'll focus on the Digital Operational Resilience Act (DORA), with a brief mention of both the Payment Card Industry Data Security Standard (PCI-DSS) and the Cyber Resilience Act (CRA). We'll also help you understand how deploying modern application server software can harden the security of both legacy and modern containerized application infrastructure against a costly data breach.

Note: The information provided does not, and is not intended to, constitute legal advice; instead, all information, content, and materials available are for general informational purposes.

Why Financial Institutions' Website Applications Offer an Attractive Attack Surface

Financial institutions invest heavily in providing services through user interfaces such as web applications. This is supported with infrastructure such as on-premises data centres and private clouds, as well as dynamic, hybrid, and multi-cloud runtime environments.

This poses a complex security challenge for CISOs – not least because the expanding attack surface is so attractive to malicious hackers who are intent on stealing customers' personal details and lucrative cardholder data (CHD).

The financial sector alone fights off a staggering 141% more high-severity vulnerabilities per app compared with other industries. The top two most common types of attacks are local file inclusions (LFI) at 58% and cross-site scripting (XSS) at 24% of all vulnerabilities.

Financial institutions must make sure their chosen application server software can:

- Provide resilience against the latest security vulnerabilities
- Offer custom authentication and authorization configuration
- Establish working backup and recovery measures, including considerations around data formats and transitions – even for legacy systems
- Maintain logs that help them trace back when things go wrong
- Monitor their systems to and identify and patch security holes

Steve Millidge, CEO at Payara Services, comments: "As financial institutions adapt to DORA's stringent resilience standards, it's critical to recognize that middleware represents a key element to build robust, compliance cybersecurity measures. Securing the application runtime layer ensures that the applications and systems organizations depend on are simultaneously performant and trustworthy. By partnering with a customer-centric vendor that is at the forefront of middleware security, such as Payara Services, IT teams can confidently align with evolving regulatory requirements while strengthening the resilience of their infrastructures."

What Types of Data Are at Risk?

All sorts of data are collected, stored, processed, transferred, shared and otherwise managed by financial apps and the middleware, such as the application server, on which they depend:

- Personal and family information such as names, addresses, contact details, and next of kin
- Cardholder data (CHD) as defined under the PCI DSS regulations: Primary Account Number (PAN), Cardholder Name, Expiration Data, Service Code, Full track data (magnetic stripe data or equivalent on a chip), Card verification code, and PINs/PIN blocks
- Account balances, as well as details of purchases, sales, or other transactions
- Acquisition, ownership, and disposal of properties, vehicles, shares, or other assets
- Health information
- Travel plans

Data Protection Legislation & Standards Affecting Financial Institutions & Payara Support

Let's look at a few, respected compliance measures for organisations operating in the countries (and with the data of customers) belonging to the EU.

Digital Operational Resilience Act EU (DORA)

Designed to reinforce the resilience of the financial sector in the countries in the European Union, the DORA has been in effect since 17 January 2025.

It's important to note the emphasis on third parties in the Act. IOPA's ESAs report on the landscape of ICT third-party providers in the EU found 15,000 such "third- party service providers" that "directly support many critical or important functions", most of which are "non-substitutable" (see Executive Summary).

How Does Payara Server Enterprise Help?

Before we get into a DORA regulation summary, here are several ways in which our runtime security is a non-negotiable priority for CISOs:

- Support for reinforcing the security of containerized development with Payara Server Enterprise and Docker images as well as necessary dependencies and configuration – even externalized configuration through environments variables with the MicroProfile Configuration API (for Data Sources, Connection Poll definitions, and Activation Config properties)
- Thin WAR files meaning:
- A single small artifact that can be adapted rapidly as your application evolves
- The underlying Payara Server Enterprise layer can be standardized and versioned across the organization for consistency, offering a known deployment platform for security compliance
- Security guidelines delivering rapid provision of unified, end-to-end security and resilience across every cluster and cloud in your entire infrastructure

How Financial Institutions Can Comply With DORA

Payara Server Enterprise can be configured to help you establish mandated data security measures like impenetrable security controls, real-time auditing, and information-rich logs.

ICT Risk Management

DORA states that firms must provide ICT Risk Management – including for third parties on which their systems rely.

You can use Payara Server Enterprise's configuration mechanisms to provide a secure environment for your web app:

- Configure Admin Data Connectivity to establish robust data storage, organization, and recovery with the Java Database Connectivity (JDBC) API
- Use Secure Admin to secure the communication between the DAS and any remote clients
- Configure the Basic Authentication Schedule (as well as Form, Client-cert, and Digest) or the Jakarta Security API to ensure strong access control mechanisms are in place to restrict access to specific system components and cardholder data
- Define and configure Jakarta Security compatible security realms and authentication mechanisms that allow users to access application resources dynamically
- Define and configure customized PKI-compatible digital certificates and keys to enable secure transport across multiple communication protocols.

ICT-Related Incident Reporting

When ICT-related incidents do occur, you must report major incidents to competent authorities.

As a starter, you can rely on our robust development processes:

- Alignment with the Federal Information Processing Standards (FIPS) of the National Institute of Standards and Technology (NIST)
- Adherence to guidelines set by the Open Web Application Security Project (OWASP)
- Rapid resolution of any security issues detected in our own software, along with monthly releases to deliver bug and security fixes
- Reporting of CVEs to the CVE Program – meaning that security vulnerabilities are quickly identified, resolved, and disclosed publicly

Exchange of Information and Intelligence on Cyber Threats

In addition to specific reporting of incidents, you must share general information and intelligence on cyber threats.

In our case, we:

- Operate as an official CVE Numbering Authority (CNA)
- Run webinars and attend events to share information on the industry-specific risks, implications, and best practice

Oversight Framework With Documentation Including Dependencies

You must create and maintain an Oversight Framework to manage ICT risks – including documenting all ICT-supported business functions, assets, and (third-party) dependencies.

- Run a customized Eclipse MicroProfile Health Check to configure automated verification of your application's computing nodes
- Use OpenTelemetry to trace the flow of requests in microservices environments across service boundaries

Other Important AppSec Measures for Financial Institutions

Let's look briefly at the two other data security compliance measures that are designed to help your engineering and security teams build a secure IT environment for your banking or insurance application infrastructure – PCI-DSS and CRA. You should also consider CCPS, NIST, and PSD2.

Payment Card Industry Data Security Standard (PCI-DSS) Compliance

While the PCI-DSS is not legislation, it is regarded as an essential, respected information security standard.

This includes all **“components, people, and processes”** in the cardholder data environment (CDE), including organisations that are involved in payment card processing (merchants, processors, acquirers, issuers and service providers), even if some of this activity is outsourced – as well as **“requirements for developers and solution providers to build and securely manage payment devices, software, and solutions for the payment industry”** (Overview of PCI SSC Standards, PCI DSS v4.x Quick Reference Guide).

For further information, see PCI DSS Quick Reference Guide.

The Cyber Resilience Act (CRA) Europe

The CRA 2024 is designed to address the cybersecurity of “products with digital elements” (PDE) – including software, hardware, and remote data processing solutions – that are on the market for commercial activity, and that connect to a device or network.

For further information, see EU Cyber Resilience Act and EU Cyber Resilience Act: What are its Essential Requirements for Software Products?.

Financial Institutions Like Hyperwallet and Rakuten Trust Payara Server Enterprise

Hyperwallet is a payout platform and PayPal service offering currency choice to payees. Following our configuration review including 70+ deployment, integration, and performance checks, the company witnessed an improvement across 25% of their configurations for a stable and highly secure deployment.

For further information, see Hyperwallet Increases Efficiency with Payara Server Enterprise.

Japanese international bank Rakuten Card migrated from former application server software with CVE bugs, patches that introduced new security issues, and slow support. With Payara Server Enterprise, the company now enjoys modern, stable, cloud-native application server middleware; expert mentoring from our Japanese-speaking engineers within the Java EE community; and integration with Docker in order to build secure, signed container images.

For further information, see Rakuten Card Smoothly Transitions to Cloud-Nature Architecture with Payara Server Enterprise.

Explore Payara Server Enterprise’s Enhanced Security Features for Containerized Jakarta EE Applications

Read our Tech Blog, to keep up to date with the latest data security legislation including DORA, PCI-DSS, and CRA, as well as other regulations and standards. Visit Payara Server Enterprise for a free trial of our application server technologies to see how you can use our dedicated security features.

Interested in Payara?

sales@payara.fish

UK: +44 800 538 5490
Intl: +1 888 239 8941

www.payara.fish

Registered Office: Malvern Hills Science Park, Geraldine Road, Malvern, United Kingdom, WR14 3SZ