White Paper

# Digital Operational Resilience Act (DORA)

## How Thales can help your organization comply with the European Union's DORA Regulation

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

# Introduction

**The digitalization of the financial sector has revolutionized the delivery of financial services providing benefits such as better services, increased efficiency, accessibility, and lower costs. However, this digital transformation has also exposed financial institutions to a myriad of risks, including cyber threats, operational disruptions, and technological vulnerabilities.**

**Traditionally, financial institution risk management regulations in the European Union (EU) focused on core financial operations, for example ensuring that firms had enough capital to cover operational risks and survive an economic crisis. But the financial sector's increasing reliance on technology and technology service providers led to a clear need for information and communication technology (ICT) risk management.**

**In the absence of EU-wide regulations focusing on the risk management of ICT by financial institutions, individual regulatory authorities started issuing rules around the usage of ICT to the organizations under their purview. This led to a patchwork of regulations that has proven difficult for financial entities to navigate.**

**The Digital Operational Resilience Act harmonizes the rules relating to operational resilience for the financial sector applying to 20 different types of financial entities and ICT third-party service providers, covering an estimated 22,000 organizations across the European Union[i].**

# The Digital Operational Resilience Act ("DORA" or the "Act")

Following adoption by the European Parliament, the Council of the European Union announced, on 28 November 2022, the adoption of Regulation (EU 2022/2554) on digital operational resilience for the financial sector. DORA entered into force on 16 January 2023 and will apply to all 27 EU member states as of 17 January 2025.

DORA aims to strengthen the IT security of financial entities such as banks, insurance companies, and investment firms to make sure the financial sector in Europe is resilient in the face of the growing volume and severity of cyber-attacks. The new regulation requires financial entities, and their critical ICT suppliers, to implement contractual, organizational, and technical measures to improve the level of digital operational resilience of the sector.

Enforcement of DORA will be the responsibility of one of the three European Supervisory Authorities (ESAs) that oversee the financial industry, depending on the focus of each specific business. These include the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA), and the European Insurance and Occupational Pension Authority (EIOPA).

# Five Key Pillars of DORA

DORA is structured around five key pillars, each designed to address distinct aspects of financial services digital operational resilience.

**ICT risk management and governance:** DORA makes management and board members responsible for defining, implementing, and maintaining an ICT risk management framework to effectively deliver greater digital operational resilience. DORA mandates that financial entities have in place an internal governance and control framework that ensures an effective and prudent management of ICT risk.

**Incident reporting:** Financial services organizations need to establish systems to monitor, manage, log, classify and report ICT-related incidents to evaluate attacks, mitigate impact on customers and operations, and report to the authorities. In the case of an incident, organizations are required to file three different kinds of reports for critical incidents: an initial notification report to authorities, an intermediate report on progress toward resolving and mitigating the incident, and a final report analyzing the root causes of the incident and its impact.

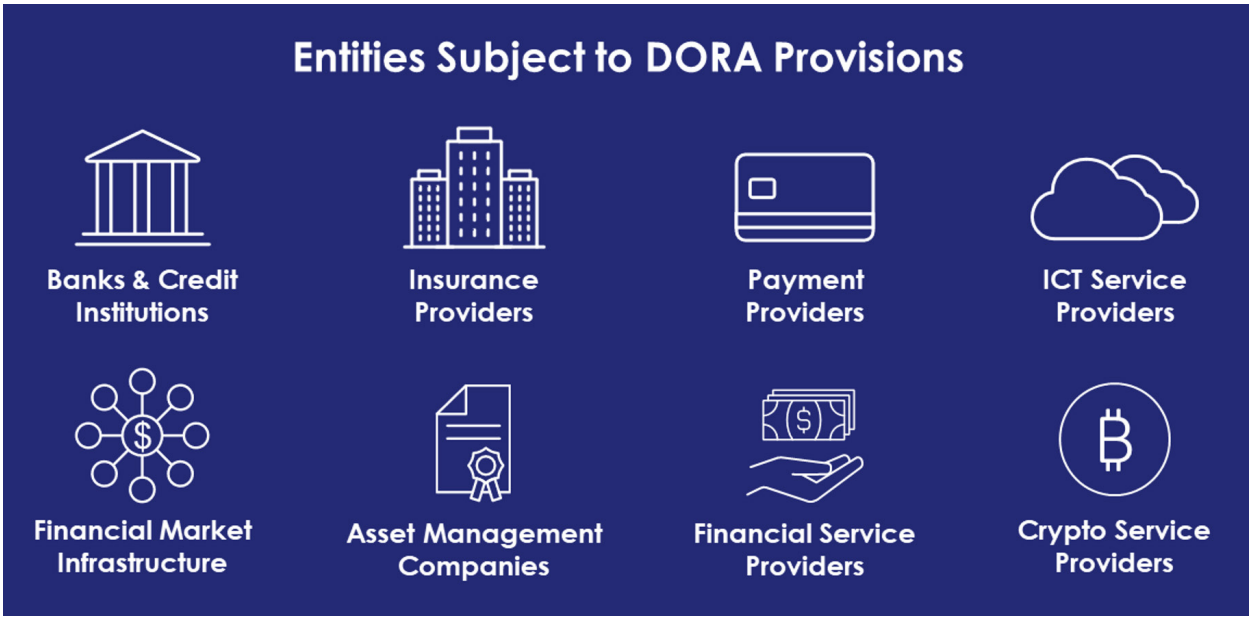
**Digital operational resilience testing:** Financial entities need to implement and perform a comprehensive digital operational resilience testing program annually. DORA also outlines that financial entities need to ensure the involvement of ICT third-party providers in their digital operational resilience testing if applicable. Threat-led penetration testing, to be undertaken by financial entities at least every three years, should also be done with the direct participation of the relevant ICT third-party service providers.

**ICT third-party risk:** One of DORA'S key emphases is ICT third-party risk and its role in risk mitigation. Financial institutions rely heavily on external ICT providers who may be outside of the EU, such as several cloud providers. Consequently, financial entities need to include ICT third-party risk as an integral component of their ICT risk management framework. DORA brings critical ICT third-party providers under the direct supervision of one of the three European Supervisory Authorities (ESAs) overseeing the financial industry and enforcing the Act.

**Information sharing:** DORA also encourages voluntary information sharing about cyberthreat information and intelligence to enhance the industry's digital operational resilience. DORA regulators acknowledge the importance of exploiting the data-rich ecosystem to strengthen the financial industry's incident prevention and response capabilities. This overcomes existing, hindering regulatory barriers.

# Covered Entities

DORA applies to a broad range of financial service providers, including banks, credit institutions, payment institutions, e-money institutions, investment firms, and crypto-asset service providers, among others. Importantly, DORA defines critical ICT services provided to financial institutions. If an organization is a provider of critical ICT services to a financial institution, it will be subject to direct regulatory oversight under the DORA framework. That includes, for example, cloud platforms and data analytics services, even if they are based outside the EU.




# Penalties

DORA is an EU Regulation, which means that it is the law in the EU as of 17 January 2025. Unlike an EU Directive, DORA does not have to be translated into each EU member state's national legislation. Failure to comply with DORA comes with strict penalties:

- Financial entities that violate DORA may face fines of up to two percent of their total annual worldwide turnover or, in the case of an individual, a maximum fine of EUR 1,000,000. The amount of the fine will depend on the severity of the violation and the financial entity's cooperation with authorities.
- Third-party ICT service providers designated as "critical" by the European Supervisory Authorities may face fines of up to EUR 5,000,000 or, in the case of an individual, a maximum fine of EUR 500,000 for non-compliance with DORA. The ESAs will have the authority to impose these fines.

# How Thales Helps with DORA Compliance

Thales' solutions can help Financial Institutions and third-party ICT providers comply with DORA by simplifying compliance and automating security reducing the burden on security and compliance teams. We help address essential cybersecurity risk-management requirements under articles 8, 9, 10, 11, 19 and 28 of the regulation, covering ICT Risk Management and Governance, Incident Reporting, and ICT Third Party Risk Management.

We provide comprehensive cyber security solutions in three key areas of cybersecurity: Application Security, Data Security, and Identity & Access Management.

- Application Security: Protect applications and APIs at scale in the cloud, on-premises, or in a hybrid model. Our market leading product suite includes Web Application Firewall (WAF) protection against Distributed Denial of Service (DDoS) and malicious BOT attacks, security for APIs, a secure Content Delivery Network (CDN), and Runtime Application Self-Protection (RASP).
- Data Security: Discover and classify sensitive data across hybrid IT and automatically protect it anywhere, whether at rest, in motion, or in use, using encryption, tokenization, and key management. Thales solutions also identify, evaluate, and prioritize potential risks for accurate risk assessment. They also identify anomalous behavior and monitor activity to identify potential threats and verify compliance, allowing organizations to prioritize where to allocate their efforts.
- Identity & Access Management: Provide seamless, secure, and trusted access to applications and digital services for customers, employees, and partners. Our solutions limit the access of internal and external users based on their roles and context with granular access policies and multi-factor authentication that help ensure that the right user is granted access to the right resource at the right time.

**Mapping Thales Capabilities to DORA Requirements**

| Requirement | How Thales helps | Solution Areas |
|---|---|---|
| **ICT Risk Management and Governance** | | |
| Article 8.1:<br><br>"...**identify, classify** and adequately document information assets..." | • Discover and classify potential risk for all public, private, and shadow APIs.<br>• Identify structured and unstructured sensitive data at risk on-premises and in the cloud.<br>• Identify current state of compliance, documenting gaps, and providing a path to full compliance. | **Application Security**<br>API Security<br>**Data Security**<br>Data Discovery & Classification<br>Data Risk Analytics<br>Vulnerability Management |
| Article 9.2:<br><br>"...**maintain** high standards of availability, authenticity, integrity and **confidentiality of data, whether at rest, in use or in transit.**" | • Encrypt data-at-rest on-premises, across clouds, and in big data or container environments.<br>• Pseudonymize sensitive information in databases.<br>• Protect data in motion with high-speed encryption.<br>• Gain full sensitive data activity visibility, track who has access, audit what they are doing and document. | **Data Security**<br>Transparent Encryption<br>Tokenization<br>Key Management<br>High Speed Encryption<br>Data Governance<br>Data Activity Monitoring |
| Article 9.4, b:<br><br>"...implementing automated mechanisms **to isolate affected information assets in the event of cyber-attacks;**" | • Detect and prevent cyber threats with web application firewall, ensuring seamless operations and peace of mind.<br>• Safeguard critical network assets from DDoS attacks and Bad Bots while continuing to allow legitimate traffic.<br>• Data activity monitoring for structured and unstructured data across cloud and on premises systems. | **Application Security**<br>Web Application Firewall<br>DDoS Protection<br>Bot Protection<br>API Protection<br>**Data Security**<br>Data Activity Monitoring Data Risk Analytics |

| | | |
|---|---|---|
| Article 9.4, c:<br><br>"...**implement policies that limit the physical and virtual access** to ICT system resources and data to what is required only for legitimate and approved functions and activities..." | • Limit the access of internal and external users to systems and data based on roles and context with policies.<br>• Apply contextual security measures based on risk scoring.<br>• Leverage smart cards for implementing physical access to sensitive facilities. | **Identity & Access Management**<br>Workforce Access Management<br>**Data Security**<br>Transparent Encryption<br>Data Risk Analytics |
| Article 9.4, d:<br><br>"...implement policies and protocols for **strong authentication** mechanisms..." | • Enable multi-factor authentication (MFA) with the broadest range of hardware and software methods and form factors.<br>• Build and deploy adaptive authentication policies based on the sensitivity of the data/application. | **Identity & Access Management**<br>Multi-Factor Authentication<br>Risk-Based Authentication |
| Article 9.4, d:<br><br>"...**protection measures of cryptographic keys** whereby data is encrypted." | • Protect cryptographic keys in a FIPS 140-2 Level 3 environment.<br>• Streamline key management in cloud and on-premises environments. | **Data Security**<br>Hardware Security Modules<br>Key Management |
| Article 9.4 e:<br><br>"Implement documented policies, procedures and controls for **ICT change management** including changes to software, hardware, firmware components, systems or security parameters..." | • Automatic reconciliation of production changes.<br>• Vulnerability assessment and risk mitigation.<br>• Detect changes in data layer schemas.<br>• Approval process for production level changes. | **Data Security**<br>Data Security Fabric<br>Vulnerability Management<br>Orchestration, Workflows and Playbooks |
| Article 10.1:<br><br>"...have in place mechanisms to promptly **detect anomalous activities, including ICT network performance issues and ICT-related incidents**..." and | • Detect and prevent cyber threats with web application firewall, ensuring seamless operations and peace of mind.<br>• Safeguard ICT network performance and integrity from DDoS attacks and Bad Bots while continuing to allow legitimate traffic. | **Application Security**<br>Web Application Firewall<br>DDoS Protection<br>Bot Protection |
| Article 10.3:<br><br>"...**monitor user activity**.." | • Data activity monitoring for structured and unstructured data across cloud and on-prem systems.<br>• Produce audit trail and reports of all access events to all systems, stream logs to external SIEM systems. | **Data Security**<br>Data Activity Monitoring<br>**Identity & Access Management**<br>Workforce Access Management |
| Article 11:<br><br>"...comprehensive ICT **business continuity** policy..." | • Mitigate of DDoS attacks in as little as three seconds.<br>• Implement preventive measures to predict and avoid crisis situations. | **Application Security**<br>DDoS Protection<br>**Data Security**<br>Professional Services<br>Artificial intelligence |

## Incident Reporting

| | | |
|---|---|---|
| Article 19:<br><br>"**Reporting of major ICT-related incidents**..." | • A year's worth of retained records are instantly accessible for detailed search and investigation. Audit data is archived automatically but remains accessible in seconds for queries and reporting. | **Data Security**<br>Reports and Portals |

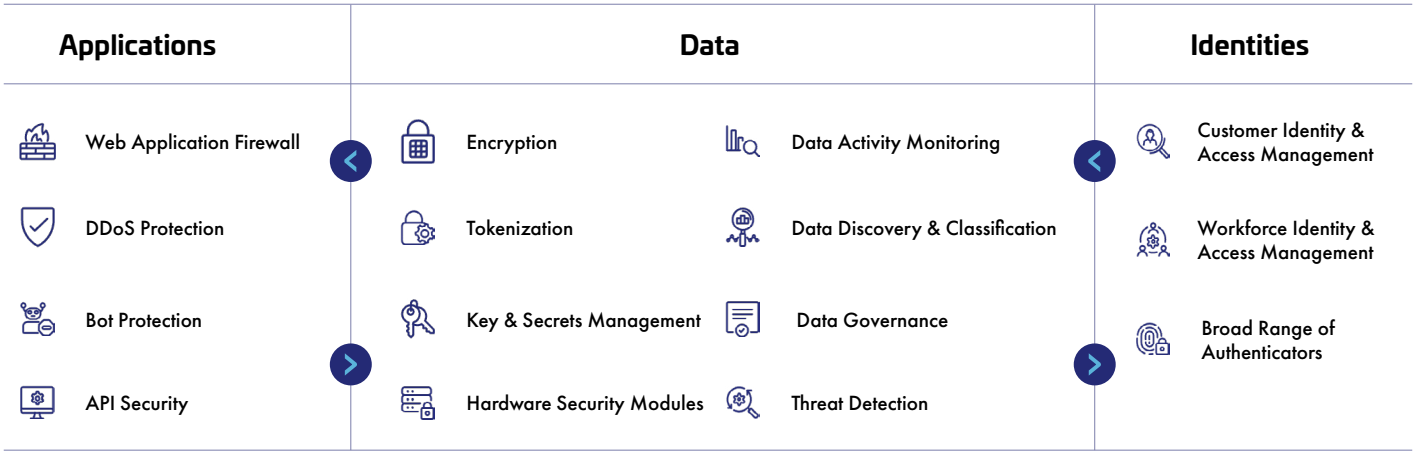
## Managing of ICT third-party risk

| | | |
|---|---|---|
| Article 28:<br><br>"**manage ICT third-party risk**..." | • Reduce third party risk by maintaining on-premises control over encryption keys protecting data hosted by in the cloud.<br>• Ensure complete separation of roles between cloud provider admins and your organization, restrict access to sensitive data.<br>• Monitor and alert anomalies to detect and prevent unwanted activities from disrupting supply chain activities.<br>• Enable relationship management with suppliers, partners or any third-party user; with clear delegation of access rights.<br>• Minimize privileges by using relationship-based fine-grained authorization. | **Data Security**<br>Cloud Key Management<br>Transparent Encryption<br>Data Activity Monitoring<br>User Rights Management<br>Discovery and Classification<br>**Identity & Access Management**<br>Third-party Access Control<br>Delegated User Management<br>Externalized Authorization |

# Visibility and Control: Thales and Imperva

**Thales and Imperva, a Thales company, deliver a broad portfolio of complementary application security, data security, and identity & access management products to provide a comprehensive solution that helps address DORA requirements. The portfolio delivers comprehensive data-centric security that protects data and all paths to it with platforms that reduce the complexity and risks of managing applications, data, and identities in the cloud.**

THALES Building a future we can all trust + imperva a Thales company




## Application Security Solutions

### Web Application Firewall (WAF)

Modern web applications are mission-critical for most organizations in all business sectors, and protecting these apps is key for business continuity and resilience. The **Imperva Web Application Firewall** provides out-of-the-box security for web applications, detecting and preventing cyber threats, ensuring seamless operations and peace of mind. Our WAF solution protects against Open Worldwide Application Security Project (OWASP) Top 10 security threats, such as cross-site scripting, illegal resource access, and remote file inclusion, blocking attacks in real time. Our threat research team updates rules that are automatically pushed out daily to ensure our solution protects customers from the latest threats.

### Distributed Denial of Service (DDoS) Protection

DDoS attacks are cybercrimes that attempt to force a website, computer, or online service offline. **Imperva DDoS Protection** provides comprehensive DDoS protection for websites, networks, DNS servers and individual IPs. Our solutions have mitigated the largest attacks in history, immediately and without incurring latency or interfering with legitimate users. Our high-capacity global network holds more than six Terabits per second (6 Tbps) of scrubbing capacity and can process more than 65 billion attack packets per second. This global network of 44+ points of presence (PoPs), each outfitted with a DDoS scrubbing center powered by proprietary Behemoth custom technology, cloud-based WAF, advanced bot mitigation services and more, acts as a software-defined mesh network for optimal performance.

### Bot Protection

The volume of automated threats on the internet is continuously rising, as bad bots account for over thirty percent of all internet traffic. **Imperva Advanced Bot Protection** safeguards mission-critical websites, mobile apps, and APIs from automated threats and online fraud without affecting the flow of business-critical traffic. It defends customers against web scraping, account takeover, scalping, transaction fraud, gift card fraud, denial of service, competitive data mining, unauthorized vulnerability scans, spam, click fraud, and web and mobile API abuse.

### API Security

Whether developing applications in new cloud-native microservice and serverless architectures, automating business-to-business processes, or providing a back-end for mobile applications, APIs are essential to the modern enterprise. Through automatic discovery and continuous monitoring of API endpoints, **Imperva API Security** enables comprehensive API visibility for security teams – without requiring development to publish APIs via OpenAPI or by adding resource-intensive workflow to their CI/CD processes. Moreover, every time an API is updated, security teams can stay on top of the change, understand any new risks, and incorporate changes, which leads to faster, more-secure software

release cycles. Imperva API Security enables security teams to keep pace with innovation without impacting development velocity.

## Data Security Solutions

### Data Discovery and Classification

A crucial first step to aligning with the NIS2 framework is understanding what constitutes sensitive data, where and how it is stored, and who can access it. **CipherTrust Data Discovery & Classification** discovers and classifies data in all the data stores in an organization's data estate, from structured to semi-structured to unstructured across on-premises, hybrid, cloud, and multi-cloud environments. This visibility enables organizations to build a strong data privacy and security foundation.

### Data Activity Monitoring

Continuous monitoring captures and analyzes all data store activity, in the cloud or on-premises, for both application and privileged user accounts, providing detailed audit trails that show who accessed what data, when, and what was done to the data. **Imperva Data Security Fabric Data Activity Monitoring (DAM)** unifies auditing across diverse on-premises platforms, providing oversight for relational databases, NoSQL databases, mainframes, big data platforms, and data warehouses. It also supports databases hosted in Microsoft Azure and Amazon Web Services (AWS), including PaaS offerings such as Azure SQL and Amazon Relational Database Services (RDS). Detailed data activity is captured automatically, making it easier to fulfill audit requests.

### Threat Detection

Threat detection is one of the most important capabilities to prevent or identify and respond to a cyberattack. **Imperva Data Security Fabric Data Risk Analytics** monitors data access and activity for all databases and provides the visibility needed to pinpoint risky data access activity for all users, including privileged users. Organizations can uncover hidden risks and vulnerabilities while creating reports to effectively communicate risk and ongoing activities. It delivers real-time alerting and user access blocking of policy violations and cost-effectively retains years of data for audits

Combining deep domain security expertise with machine learning (ML) allows organizations to identify suspicious user and computer system behaviors that violate security policies, practices, and peer group norms. Purpose-built detection algorithms instantly recognize active attack exploits and immediately send incident alerts.

### Encryption

Encryption plays an important role in protecting data's confidentiality, integrity, and availability across its lifecycle: at rest, in-motion, and in use.

- **Data at Rest**
  Depending on your security requirements and infrastructure, different approaches can be used to protect data-at-rest in files, volumes, and databases. **CipherTrust Data Security Platform** provides multiple capabilities for protecting data at rest in files, volumes, and databases. Transparent Encryption operates at the file system layer, delivering data-at-rest encryption with centralized key management, granular access controls, and data access logging to meet best practice requirements for protecting data. To protect data-at-rest from zero-day and privileged escalation attacks, ransomware protection uses real-time behavior monitoring to alert or block malicious activity before ransomware can take hold of data. Database protection at the database layer supports key management for native TDE use cases or the ability to do field or column-level encryption on databases. At the application layer, libraries for C and Java can be deployed, or solutions at the network layer can be used as a gateway to apply encryption without modifying the application code.

- **Data in Motion**
  Protecting data in-motion is essential to prevent from eavesdropping, surveillance, and overt and covert interception of sensitive data. **Thales High Speed Encryption** provides certified, network-independent, data-in-motion encryption (layers 2, 3, and 4), ensuring data is secure as it moves from site to site or from on-premises to the cloud and back, allowing customers to better protect data, video, voice, and metadata flowing between repositories. The network encryption solution has been proven to deliver maximum uptime in the most demanding, performance-intensive environments. It has near-zero latency and can operate in full-duplex mode at full-line speed while offering flexible and vendor-agnostic interoperability, meaning it's compatible with all the leading network vendors throughout your network.

### Tokenization

Tokenizing or masking data reduces the cost and effort required to comply with internal security policies, industry frameworks, and regulatory mandates, such as NIS2, the European Union's Global Data Protection Regulation (GDPR), and the Payment Card Industry Data Security Standard (PCI-DSS). **CipherTrust Tokenization** permits the pseudonymization of sensitive information in databases so you can analyze aggregate data without exposing sensitive data during analysis. It offers application-level tokenization services in two convenient solutions that deliver complete customer flexibility: Vaultless Tokenization with Dynamic Data Masking and Vaulted Tokenization. Both solutions secure and anonymize sensitive assets, whether they reside in the data center, big data environments, or the cloud.

### Key & Secrets Management

Centralized key management consolidates on-prem and cloud encryption keys, so you can apply consistent security policies across multiple file servers, databases, applications, virtual machines, and cloud platforms. **CipherTrust Key Management** provides a greater command over your keys and simplifies key lifecycle management tasks while enhancing data security through consistent enforcement of key policies, fine-grained access control, and robust auditing and reporting of all key management and encryption operations.

Modern development trends such as containerization, cloud transformation, DevOps, and automation have contributed to a massive increase in the use of secrets (credentials, certificates, keys) for authentication, which can be vulnerable to cyber-attacks when not securely managed. **CipherTrust Secrets Management** protects and automates access to mission-critical secrets across DevOps tools and cloud workloads, including secrets, credentials, certificates, API keys, and tokens, to help security and governance teams reduce risk by streamlining security processes.

### Data Governance

Organizations need to monitor files and databases across hybrid IT to help ensure data is secure, private, accurate, available, and usable. **Imperva Data Security Fabric** includes discovering and mapping file and database servers and identifying sensitive data such as social security numbers, credit card data, etc. It allows organizations to understand current data usage, enabling role and workflow management of data to grant access to data stewards and creating reports around data to measure effective alignment to NIS2 and other regulation requirements.

### Hardware Security Modules

A hardware security module (HSM) is a dedicated crypto processor that protects the crypto key lifecycle. It acts as a trust anchor that protects the cryptographic infrastructure of some of the world's most security-conscious organizations by securely managing, processing, and storing cryptographic keys inside a hardened, tamper-resistant device. **Thales Luna Hardware Security Modules** protect cryptographic keys and provide a FIPS 140-2 Level 3 hardened, tamper-resistant environment for secure cryptographic processing, key generation and protection, encryption, and more. They are available on-premises, in the cloud as-a-service, and across hybrid environments.

Luna HSMs generate and protect root and certificate authority (CA) keys, supporting PKIs across various use cases. They sign the application code to ensure the software remains secure, unaltered, and authentic. They create digital certificates for credentialing and authenticating proprietary electronic devices for IoT applications and other deployments.

## Identity & Access Management Solutions

### Customer Identity & Access Management

Customer Identity & Access Management (CIAM) manages access for identities external to an organization such as the identities of customers, gig workers, suppliers, or partners. **Thales OneWelcome Identity Platform** provides a consistent identity experience across all customer touchpoints, allowing organizations to balance security and usability to enable a frictionless experience at scale for customers–regardless of their location, device, or application. The Platform enables organizations to thrive in a regulated market, helping them meet requirements of local, national and international data regulations with a CIAM solution that can handle the most complex data privacy and protection regulations.

### Workforce Identity & Access Management

A disproportionate number of data breaches start with unauthorized access of data and sensitive resources, credential compromise, and privilege abuse. **Thales SafeNet Trusted Access** is a cloud-based access management solution that makes it easy to manage access both to cloud services and to enterprise applications with an integrated platform combining single sign-on (SSO), multi-factor authentication (MFA), and scenario-based access policies. SafeNet Trusted Access provides a single pane view of access events across an organization's app estate to ensure that the right user has access to the right application at the right level of trust. SafeNet Trusted Access allows organizations to virtually (or logically) limit the access to confidential resources through use of MFA (including phishing-resistant authentication) and granular access policies.

### Broadest Range of Authentication Solutions

Multi-factor authentication is a requirement of NIS2 and most other regulations and standards. **Thales OneWelcome Authenticators** include a broad range of hardware and software authentication methods and form factors for workforce and external users. These include phishing-resistant authentication capabilities, such as CBA and FIDO, in addition to a user-friendly smartphone-based authenticator app called MobilePASS+. External users, including customers or partners, also have nuanced authentication needs. With the OneWelcome Identity Platform, organizations can enable both low-assurance and high-assurance authentication mechanisms, including SCA (Strong Customer Authentication) or use of FIDO Passkeys.

# Conclusion

DORA represents a pivotal step towards fortifying the operational resilience of the European Union's financial sector in an increasingly digitalized landscape. By delineating comprehensive requirements for operational resilience, ICT risk management, and third-party oversight, DORA aims to bolster financial stability, enhance consumer protection, and foster trust in digital financial services. However, the successful implementation of DORA will hinge upon addressing various challenges and ensuring effective coordination among stakeholders.

Drawing on decades of experience helping corporate entities and public enterprises adhere to compliance mandates, Thales offers a broad range of products and services that enable organizations to strengthen cyber resilience, address the security of supply chains, streamline reporting obligations, and comply with the more stringent supervisory measures and stricter enforcement requirements of DORA.

Moreover, the combined Thales and Imperva portfolios help simplify compliance across multiple overlapping regulatory regimes in addition to DORA, such as GDPR and NIS2, or standards such as ISO 27001, PCI, or the NIST Cybersecurity Framework 2.0. Our portfolio delivers unparalleled centralized visibility and control over data, application, and access control security, helping automate security and compliance processes and reducing the burden on security and compliance teams.

# About Thales

As the global leader in data security, Thales helps the most trusted brands and organizations around the world protect their most sensitive data and software, secure the cloud, provide seamless digital experiences, and achieve compliance through our industry-leading application security, data security & governance, identity and access management, and software licensing solutions. Thales completed its acquisition of Imperva on December 4, 2023.

Price Waterhouse Coopers: DORA and its impact on UK financial entities and ICT service provider[i]

THALES

Building a future we can all trust

## Contact us

For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com

© Thales - April 2024 • HP V03