cpl.thalesgroup.com

THALES
Building a future we can all trust

Data Security Compliance with the Digital Operational Resilience Act (DORA)

How Thales solutions help with DORA Compliance

What is DORA?

The European Council adopted the Digital Operational Resilience Act (DORA) in November of 2022 to enhance the resilience of financial institutions to cyber-attacks. DORA does this by streamlining and harmonizing requirements in the European Union for the security of information systems and networks of organizations operating in the financial sector as well as critical third party providers of ICT (Information Communication Technologies)-related services.

The main pillars of DORA legislation are:

- ICT risk management
- ICT related incident management, classification and reporting
- Digital operational resilience testing
- Management of ICT third-party risk
- Information sharing arrangements

Which companies are subject to DORA?

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. But 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.

When will DORA be enforced?

DORA entered into force on January 16, 2023, with an implementation period of two years. Financial entities and their ICT suppliers and service providers are expected to be compliant with the regulation by January 17, 2025.

What are the penalties for DORA non-compliance?

Entities found in violation of the Act's requirements 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.

How can Thales help with DORA compliance?

Thales helps organizations comply with DORA by addressing essential requirements for risk management and managing third party risk.

Chapter II: ICT Risk Management

DORA lays out frameworks and guidelines for risk management intended to help build mature risk management programs and improve operational resiliency.

Thales helps organizations by:

- Identifying and classifying sensitive data for risk assessment
- Protecting data at rest, in use, and in motion
- Protecting access to sensitive data, systems, and applications.
- Protecting cryptographic keys and implementing strong multi-factor authentication
- Detecting anomalous activities and monitoring user activity

DORA	Requirement	Thales Solutions
Article 8.1	**"...identify, classify** and adequately document information assets..."	**CipherTrust Data Discovery and Classification** identifies structured and unstructured sensitive data on-premises and in the cloud. Built-in templates enable rapid identification of regulated data, highlight security risks, and help uncover compliance gaps.
Article 9.2	"...maintain high standards of availability, authenticity, integrity and **confidentiality of data, whether at rest, in use or in transit."**	**Protect Data at Rest:** **CipherTrust Data Security Platform** provides multiple capabilities for protecting data at rest in files, volumes, and databases. Among them: • **CipherTrust Transparent Encryption** delivers data-at-rest encryption with centralized key management and privileged user access control. This protects data wherever it resides, on-premises, across multiple clouds, and within big data and container environments. • **CipherTrust Tokenization** permits the pseudonymization of sensitive information in databases while maintaining the ability to analyze aggregate data, without exposing sensitive data during the analysis or in reports. **Protect Data in Motion:** **Thales High Speed Encryptors (HSE)** provide 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. Our network encryption solutions allow customers to better protect data, video, voice, and metadata from eavesdropping, surveillance, and overt and covert interception— without performance compromise. Thales HSEs are available as both physical and virtual appliances, supporting a wide spectrum of network speeds from 10 Mbps to 100 Gbps. Rigorously tested and certified to exacting standards such as FIPS 140-2 L3 and Common Criteria, Thales HSE network encryption solutions have been vetted by such organizations as the USA Department of Defense Information Network (DoDIN) and NATO.
Article 9.3, b	**"...minimize the risk of corruption or loss of data;** unauthorized access **and of the technical flaws..."**	**Thales OneWelcome identity & access management** products and solutions limit the access of internal and external users based on their roles and context. Backed by strong authentication (MFA), granular access policies and fine-grained authorization policies help ensuring that the right user is granted access to the right resource at the right time; whereby minimizing the risk of unauthorized access.

How can Thales help with DORA compliance?

DORA	Requirement	Thales Solutions
Article 9.4, c	**"...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, and..."**	**Thales OneWelcome Identity Platform** allows organizations to virtually (or logically) limit the access to confidential resources through use of MFA (including phishing-resistant authentication) and granular access policies. SafeNet IDPrime smart cards can be leveraged for implementing physical access to sensitive facilities. These smart cards can also augment Passwordless authentication initiatives relying on PKI and FIDO technology. **Thales OneWelcome Consent & Preference Management** module enables organizations to gather consent of end consumers such that financial institutions may have clear visibility of consented data, thereby allowing them to manage access to data that they are allowed to utilize.
Article 9. 4, d	**"...strong authentication mechanisms..."**	**SafeNet Trusted Access** is a cloud-based access management solution that makes it easy to manage access to both cloud services and enterprise applications with an integrated platform combining single sign-on, **multi-factor authentication (MFA)** and scenario-based access policies. SafeNet Trusted Access provides a single pane view of access events across your app estate to ensure that the right user has access to the right application at the right level of trust.
	"... protection measures of cryptographic keys whereby data is encrypted."	**Thales Key Management** offerings streamline and strengthen key management in cloud and enterprise environments over a diverse set of use cases. Leveraging FIPS 140-2-compliant virtual or hardware appliances, Thales key management tools and solutions deliver high security to sensitive environments and centralize key management for home-grown encryption, as well as third-party applications. **Hardware Security Modules (HSMs)** 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. Luna HSMs are available on-premises, in the cloud as-a-service, and across hybrid environments. • Generates and protects root and certificate authority (CA) keys, providing support for PKIs across a variety of use cases • Signs application code to ensure software remains secure, unaltered, and authentic • Creates digital certificates for credentialing and authenticating proprietary electronic devices for IoT applications and other network deployments
Article 10. 1	**"...detect anomalous activities... monitor user activity..."**	**CipherTrust Transparent Encryption** security intelligence logs and reports streamline compliance reporting and speed up threat detection using leading security information and external SIEM systems. **CipherTrust Transparent Encryption Ransomware Protection** extension detects ransomware identifying activities (excessive data access, exfiltration, unauthorized encryption, or impersonation with malicious actions). It alerts or blocks malicious activity upon detection of on all file system input and output at guard points. **SafeNet Trusted Access** allows organizations to respond and mitigate the risk of data breach by providing an immediate, up to date audit trail of all access events to all systems. Extensive automated reports document all aspects of access enforcement and authentication. In addition, the service automatically streams logs to external SIEM systems.

Chapter V: Managing of ICT Third Party Risk

DORA emphasizes the need for managing ICT third-party service providers risk and the need for financial entities to have "Exit strategies."

- **Thales helps organizations reduce third party risks by leveraging key management and encryption to enforce strict separation of duties between financial institutions and 3rd party providers and maintain portability of workloads to other providers when necessary.**

DORA	Requirement	Thales Solutions
Article 28.8	"For ICT **[3rd party] services supporting critical or important functions,** financial entities shall **put in place exit strategies."**	**CipherTrust Cloud Key Manager** can reduce third party risks by maintaining on-premises under the full control of the financial institution the keys that protect sensitive data hosted by third party cloud providers under "bring your own keys" (BYOK) systems. This increases operational efficiency through harmonization and automation. It reduces operational costs, risk of errors, and data breaches, thereby improving your security posture. **CipherTrust Transparent Encryption** provides complete separation of administrative roles where only authorized users and processes can view unencrypted data. Unless a valid reason to access the data is provided, sensitive data stored in a third-party cloud provider will not be accessible in clear text to unauthorized users. These could include third party cloud provider employees, such as support engineers; privileged users, such as DB admins or Sys admins; or potentially malicious processes. By enabling enterprises to "bring their own encryption (BYOE)" to the cloud, CipherTrust Transparent Encryption increases operational sovereignty and portability of workloads between third-party ICT providers. In addition, **Thales Data Security solutions** offer the most comprehensive range of data protection, such as **Thales Data Protection on Demand (DPoD)** that provides built in high availability and backup to its cloud-based **Luna Cloud HSM** and **CipherTrust Key Management** services, to the HSE network encryption appliances that provides options to zeroize.

About Thales

Thales is a global leader in data security, trusted by governments and the most recognized companies around the world to help them protect their most sensitive data. The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

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