

eBook

THALES
Building a future we can all trust

How Thales Helps Meet Compliance Requirements in EMEA

cpl.thalesgroup.com

Thales helps you meet common compliance and data privacy requirements...



Discover and classify sensitive data and analyze compliance risks



Protect sensitive data with encryption and tokenization



Control access to data with centralized key and policy management



Audit all attempts to access data and encryption keys with logs and reports





...across traditional and next generation platforms



Multicloud data security



Secure sensitive information
in big data analytics



Container data security



Transaction and digital
payment security

Thales Data Protection solutions address key compliance requirements

Discover and Classify Sensitive Data



Discover structured and unstructured data across the entire enterprise



Classify sensitive data based on built-in and customizable templates

Protect Data at Rest and in Motion



Encrypt data at rest anywhere it resides with centralized key management and a secure root of trust



Encrypt data in motion independent of networks

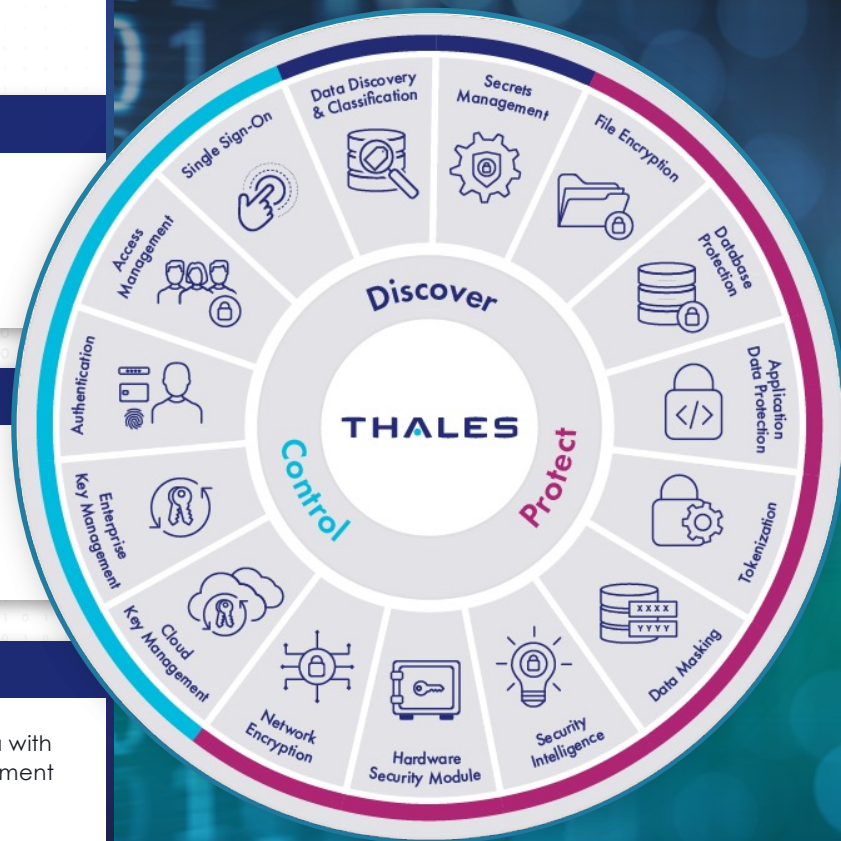
Control Access and Centralized Key Management



Ensure cryptographic keys are always in your control via centralized encryption key and policy management



Control access to sensitive data with privileged user access management and strong authentication



Addressing the key regulatory requirements for Europe

	DORA	NIS 2	GDPR	PCI DSS 4.0	ISO 27001:2022
What is it?	Sets uniform requirements for the security of network and information systems with the objective of enhancing the resilience of financial institutions to cyber-attacks.	Aims to mitigate threats to network and information systems used to provide essential services in key sectors and to ensure the continuity of such services.	Was designed to improve personal data protections and increase accountability for data breaches; governs use, process, and storage of personal data .	Standardizes the security controls that need to be enforced by businesses processing payment card data.	Is the world's best-known standard for information security management systems (ISMS). Provides guidance for establishing, maintaining, and improving an ISMS.
Applies to	Financial institutions and critical third parties (e.g., cloud and data analytics providers).	Critical infrastructure, such as utilities, transport, financial, health, and key service providers	All organizations within the EU, and those foreign organizations capturing personal data from EU citizens.	Organizations handling credit card data.	Organizations across all economic sectors, private, public and non-profit organizations.
Penalties	EUR 10M or 2% of total worldwide turnover.	EUR 10M or 2% of total worldwide turnover.	EUR 10M or 2% of total worldwide turnover.	- Fines up to \$100,000 - Cessation of credit card processing	No penalties, but ISO 27001 certification may provide defense against fines from other regulations.
How Thales Helps?	Thales helps organizations comply with DORA by addressing requirements on chapter II for ICT risk management and chapter V on managing ICT third party risk.	Thales helps organizations comply with NIS 2 by addressing requirements for cybersecurity risk-management measures under chapter 21.	Thales helps organizations comply with GDPR by addressing essential requirements for safeguarding data privacy and data security.	Thales offers comprehensive hardware and software compliance solutions that help organizations address the core principles of PCI DSS.	Thales helps organizations comply with ISO 27001 by addressing essential requirements listed in the Annex A for Information Security Controls.

Digital Operational Resilience Act (DORA) Compliance



Overall objective

The **European Union's Digital Operational Resilience Act** sets uniform requirements for the security of network and information systems of companies and organizations operating in the financial sector as well as critical third parties which provide ICT (Information Communication Technologies)-related services to them, such as cloud platforms or data analytics services. The DORA regulation was adopted on December 14, 2022, and will be enforced starting on January 15, 2025.



Applies to

Financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, payment processing, or insurance, and critical third parties, such as cloud platforms or data analytics services.

















Penalties

Member States are granted discretion on penalties of up to EUR 10M or 2% of total worldwide turnover for the company that violates the law (whichever is higher).











Compliance for Digital Operational Resilience Act (DORA)

Thales helps organizations comply with DORA by addressing requirements on chapter II for risk management and chapter V on managing third party risk.

Requirements	DORA Articles	Thales Supporting Capabilities
Chapter II: ICT Risk Management		
Identify and classify	8.1	 Data Discovery and Classification
Protect data at rest, in use or in transit	9.2	 Transparent Encryption  Tokenization  High Speed Encryptors (HSE)
Access management	9.3,b 9.4,c	 Identity and Access Management  Consent and Preference Management  Transparent Encryption
Implement multi-factor authentication	9.4	 SafeNet Trusted Access
Securely manage cryptographic keys	9.4	 Enterprise Key Management  Hardware Security Modules (HSMs)
Monitor and detect anomalous activities	10.1	 SafeNet Trusted Access  Transparent Encryption
Chapter V: Managing of ICT Third Party Risk		
Mitigate risks of third-party service providers	28.8	 Cloud Key Management  Transparent Encryption

How Thales Solutions Enable DORA Compliance

DORA Requirement	Thales Solution	
<p>8.1: "...<i>identify, classify and adequately document information assets...</i>"</p>	 <p>CipherTrust Data Discovery and Classification</p>	<p>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.</p>
<p>9.2: "...<i>maintain high standards of availability, authenticity, integrity and confidentiality of data, whether at rest, in use or in transit.</i>"</p>	 <p>CipherTrust Transparent Encryption</p>	<p>Delivers data-at-rest encryption for files and folders and privileged user access control. Protects data wherever it resides, on-premises, across clouds, and in big data and container environments.</p>
	 <p>CipherTrust Tokenization</p>	<p>Permits the pseudonymization of sensitive information in databases while maintaining the ability to analyze aggregate data, without exposing sensitive data during analysis or in reports.</p>
	 <p>High Speed Encryptor (HSE)</p>	<p>Provides network-independent, data-in-motion encryption ensuring data, video, voice, and metadata is secure as it moves from site-to-site, or from on-premises to the cloud and back.</p>
<p>9.3,b: "...<i>minimize the risk of... unauthorized access...</i>"</p>	 <p>OneWelcome Identity & Access Management</p>	<p>Limits the access of internal and external users based on their roles and context with granular access and authorization policies that help ensure that the right user is granted access to the right resource at the right time.</p>
<p>9.4,c: <i>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...</i></p>	 <p>OneWelcome Consent and Preference Mgmt.</p>	<p>Enables organizations to gather consent of end consumers such that organizations may have clear visibility of consented data, allowing them to manage access to data that they are allowed to utilize.</p>
	 <p>CipherTrust Transparent Encryption</p>	<p>Provides complete separation of roles where only authorized users and processes can view encrypted data through granular access security policies and key management.</p>
<p>9.4,d: "...<i>strong authentication mechanisms...</i>"</p>	 <p>SafeNet Trusted Access</p>	<p>Enables Multi-factor Authentication with the broadest range of hardware and software methods and form factors, allowing customers to address numerous use cases, assurance levels, and threat vectors with unified policies.</p>

How Thales Solutions Enable DORA Compliance

DORA Requirement

Thales Solution

9.4.d: "... protection measures of cryptographic keys whereby data is encrypted."



Luna HSMs

Protect cryptographic keys and provide a FIPS 140-2 Level 3 hardened, tamper-resistant hardware security module for secure cryptographic processing, key generation and protection, encryption, and more.



CipherTrust Enterprise Key Management

Streamlines and strengthens key management in cloud and on-premises environments for home-grown encryption, as well as third-party applications.

10.1: "... detect anomalous activities... monitor user activity..."



CipherTrust Transparent Encryption

Produces security intelligence logs that speed up threat detection using leading security information and SIEMs. Ransomware protection allows administrators to alert/block suspicious activity before ransomware can take hold.



OneWelcome Identity & Access Management

Combines single sign-on and scenario-based access policies in a cloud-based access management solution. Extensive automated reports document all aspects of access/authentication with log streams to SIEM systems

28.8: "For ICT [3rd party] services supporting critical or important functions, financial entities shall put in place exit strategies."



CipherTrust Cloud Key Management

Reduces 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.



CipherTrust Transparent Encryption

Provides complete separation of roles where only authorized users and processes can view encrypted data. This keeps third party cloud provider employees, such as support engineers and DB admins, from seeing the data in the clear.

European Union Network and Information Security Directive (NIS 2)



The image shows the cover page of the Directive (EU) 2022/2555. At the top, it features the European Union flag and the text "EUROPEAN UNION". Below this, it lists "THE EUROPEAN PARLIAMENT" and "THE COUNCIL". The date "Brussels, 17 November 2022 (OR, en)" and the reference "2020/0266(COD) PE-CONS 41/22" are also present. A central graphic depicts a blue padlock on a stack of blue blocks, with the number "9308" and "1" next to it. The main title "Directive (EU) 2022/2555" is followed by "European Parliament and council on measures for a high common level of cybersecurity across the Union". At the bottom, it includes "PE-CONS 41/22", "ECOFIN", "MCA", and "EN".



Overall objective

The **European Union Network and Information Security Directive (NIS 2)** purpose is to build cybersecurity capabilities across the Union. It aims to mitigate threats to network and information systems used to provide essential services in key sectors and ensure the continuity of such services when facing incidents, thus contributing to the Union's security and to the effective functioning of its economy and society. The regulation was adopted 14 December 2022 and is to be transposed by nation states by 17 Oct 2024.



Applies to

Essential Entities: energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, public administration, and space information, and communication technology (cloud, internet, data center and other service providers).

Important Entities: postal and courier services; waste management; manufacture, production, and distribution of chemicals; food supply chain; manufacturing; research; and digital providers (search engines, online marketplaces and social networking).














Penalties

Member States are granted discretion on penalties of up to EUR 10M or 2% of total worldwide turnover for the company that violates the law (whichever is higher).











Compliance for Network and Information Security Directive (NIS 2)

Thales helps organizations comply with NIS 2 by addressing requirements under article 21 for cybersecurity risk-management measures.

Requirements	NIS 2 Articles	Thales Supporting Capabilities
Article 21: Cybersecurity risk-management measures		
Risk Analysis	21.2.a	 Data Discovery and Classification
Supply chain security	21.2.d	 Cloud Key Management  Transparent Encryption
Cryptography and policies	21.2.h	 Hardware Security Modules (HSMs)  Tokenization  Enterprise Key Management  Transparent Encryption  High Speed Encryptions (HSE)
Access control and multi-factor authentication	21.2.i.j	 SafeNet Trusted Access  Identity and Access Management  Transparent Encryption

How Thales Solutions Enable NIS 2 Compliance

NIS 2 Article	Thales Solution
21.2. a: "...policies on risk analysis and information system security;"	 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.
21. 2. d: supply chain security , ... concerning the relationships between each entity and its; direct suppliers or service providers	 CipherTrust Cloud Key Management Reduces 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.
	 CipherTrust Transparent Encryption Provides complete separation of roles where only authorized users and processes can view encrypted data. This keeps third party cloud provider employees, such as support engineers and DB admins from seeing the data in the clear.
21. 2. h: "...policies and procedures regarding the use of cryptography and, where appropriate, encryption"	 CipherTrust Transparent Encryption Delivers data-at-rest encryption for files and folders and privileged user access control with granular policies. Protects data wherever it resides, on-premises, across clouds, and in 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.
	 CipherTrust Enterprise Key Management Streamlines and strengthens key management in cloud and on-premises environments for home-grown encryption, as well as third-party applications.
	 High Speed Encryptor (HSE) Provides network-independent, data-in-motion encryption ensuring data, video, voice, and metadata is secure as it moves from site-to-site, or from on-premises to the cloud and back.
	 Luna 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.

How Thales Solutions Enable NIS 2 Compliance

NIS 2 Article

Thales Solution

21. 2. i: "...access control policies and asset management;

21. 2. j: the use of **multi-factor authentication or continuous authentication solutions...**"



OneWelcome Identity & Access Management

Limits the access of internal and external users based on their roles and context with granular access and authorization policies that help ensure that the right user is granted access to the right resource at the right time.



SafeNet Trusted Access

Enables Multi-factor Authentication with the broadest range of hardware and software methods and form factors, allowing customers to address numerous use cases, assurance levels, and threat vectors with unified policies.



CipherTrust Transparent Encryption

Provides complete separation of roles where only authorized users and processes can view encrypted data through granular access security policies and key management.

General Data Protection Regulation (GDPR)



Overall objective

The **European Union General Data Protection Regulation (GDPR)** is designed to improve personal data protection and increase organizational accountability for data breaches. GDPR governs the way in which we can use, process, and store personal data (information about an identifiable, living person).

GDPR requirements apply to all member states of the European Union, aiming to create more consistent protection of consumer and personal data across EU nations. Some of the key privacy and data protection requirements of the GDPR include: consent of subjects for data processing, anonymizing collected data to protect privacy, providing data breach notifications, and safely handling the transfer of data across borders.



Applies to

The GDPR applies to all organizations within the EU, as well as those supplying goods or services to the EU or monitoring EU citizens, no matter where they are based.
















Penalties

Member states are granted discretion on penalties of up to EUR 10M or 2% of total worldwide turnover (whichever is higher) for the company that violates the law.








Compliance for General Data Protection Regulation (GDPR)









Thales helps organizations comply with GDPR by addressing essential requirements for safeguarding data privacy and data security throughout multiple articles of the legislation.

Requirements	GDPR Articles	Thales Supporting Capabilities
Consent for Processing	Article 7	 Consent and Preference Management
Right to erasure	Article 17	 CipherTrust Data Security Platform
Data protection by design and by default	Article 25	 CipherTrust Data Security Platform
Data processing by third parties	Article 28	 Cloud Key Management  Transparent Encryption
Pseudonymization and encryption	Article 32	 Hardware Security Modules (HSMs)  Tokenization  Enterprise Key Management  Transparent Encryption  High Speed Encryptions (HSE)
Notification of data breach	Article 33	
Access to personal data	Article 32	 Identity and Access Management  Transparent Encryption  High Speed Encryptions (HSE)
Safeguard data transfers	Article 46	

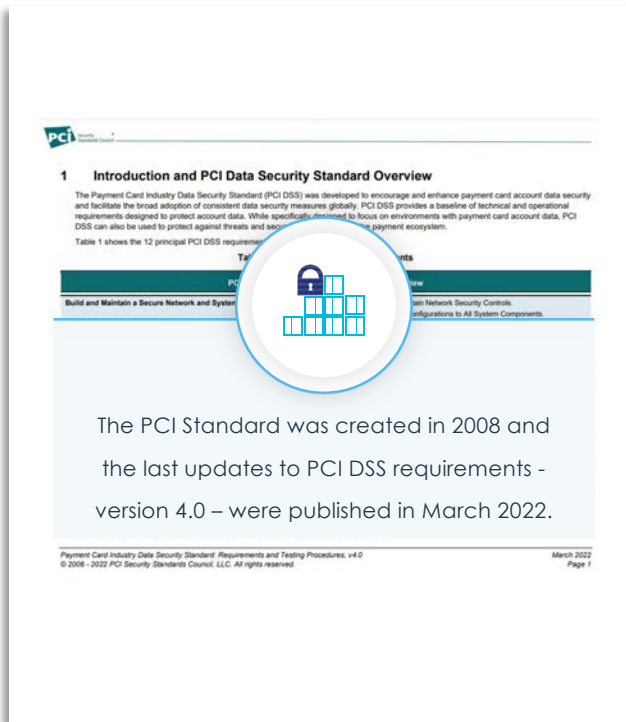
How Thales Solutions Enable GDPR Compliance

GDPR Article	Thales Solution
7: "...the controller shall ... demonstrate that the data subject has consented to processing of his or her personal data.;"	 OneWelcome Consent and Preference Mgmt. Enables organizations to gather consent of end consumers such that organizations may have clear visibility of consented data, allowing them to manage access to data that they are allowed to utilize.
17: "...data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her..."	 CipherTrust Data Security Platform Includes data discovery and classification which identifies structured and unstructured sensitive data on-premises and in the cloud. Once the desired personal data is identified, CipherTrust Data Security Platform can selectively "destroy" data simply by destroying the encryption keys for the desired dataset.
25: "Data protection by design and by default"	 CipherTrust Data Security Platform Implement data protection by design and by default by: Discovering and classifying sensitive data across hybrid IT, setting centralized data security policies and enforcing them on any environment, securing sensitive data with encryption and tokenization, and protecting access to sensitive data with granular security policies.
28: "Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures"	 CipherTrust Cloud Key Management Reduces third party risks by maintaining on-premises under the full control of the organization the keys that protect sensitive data hosted by third party cloud providers.
	 CipherTrust Transparent Encryption Provides complete separation of roles where only authorized users and processes can view encrypted data. This keeps third party cloud provider employees, such as support engineers and DB admins from seeing the data in the clear.

How Thales Solutions Enable GDPR Compliance

GDPR Article	Thales Solution	
<p>32: "controller and the processor shall implement...the pseudonymization and encryption of personal data."</p>	 <p>CipherTrust Tokenization</p>	<p>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.</p>
<p>33: "notify the personal data breach to the supervisory authority... unless it is unlikely to result in a risk to the rights and freedoms of natural persons."</p>	 <p>CipherTrust Transparent Encryption</p>	<p>Delivers data-at-rest encryption for files and folders and privileged user access control with granular policies. Protects data wherever it resides, on-premises, across clouds, and in big data and container environments.</p>
<p>32: "notify the personal data breach to the supervisory authority... unless it is unlikely to result in a risk to the rights and freedoms of natural persons."</p>	 <p>CipherTrust Enterprise Key Management</p>	<p>Streamlines and strengthens key management in cloud and on-premises environments for home-grown encryption, as well as third-party applications.</p>
	 <p>High Speed Encryptor (HSE)</p>	<p>Provides network-independent, data-in-motion encryption ensuring data, video, voice, and metadata is secure as it moves from site-to-site, or from on-premises to the cloud and back.</p>
	 <p>Luna HSMs</p>	<p>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.</p>
<p>32: "unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed"</p>	 <p>OneWelcome Identity & Access Management</p>	<p>Limits the access of internal and external users based on their roles and context with granular access and authorization policies that help ensure that the right user is granted access to the right resource at the right time.</p>
<p>46: "controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards..."</p>	 <p>CipherTrust Transparent Encryption</p>	<p>Provides complete separation of roles where only authorized users and processes in the correct geographies can view encrypted data through granular access security policies and key management.</p>
	 <p>High Speed Encryptor (HSE)</p>	<p>Provides network-independent, data-in-motion encryption ensuring data, video, voice, and metadata is secure as it moves from site-to-site, or from on-premises to the cloud and back.</p>

Payment Card Industry Data Security Standard (PCI DSS) Compliance



Overall objective

The **Payment Card Industry Data Security Standard (PCI DSS)** was jointly developed by American Express, Discover, JCB, MasterCard, and Visa, to **standardize the security controls** that need to be enforced by businesses processing payment card data. The goal of the PCI Data Security Standard (PCI DSS) is to **protect cardholder data and sensitive authentication data** wherever it is stored, processed, or transmitted.



Applies to

All entities involved in payment card processing including **merchants, processors, acquirers, issuers, and service providers**. It also applies to all entities that store, process, or transmit **cardholder data and/or sensitive authentication data**.



Penalties












Fines for non-compliance with PCI can vary from **\$5,000 to \$100,000 per month** as well as **increased audit requirements and potential shut down** of credit card activity by a merchant bank or credit card brand.

However, these fines will still be less than costs from **lawsuits**, actions by the federal government, **compensation fees** to customers affected, and other financial penalties related to non-compliance.



Compliance for PCI DSS 4.0

Thales offers comprehensive hardware and software solutions that help organizations comply with the core principles of the Payment Card Industry Data Security Standard (PCI DSS) .

Requirements	PCI DSS 4.0	Thales Data Protection Supporting Capabilities
Secure Systems and Software	2, 6	 Hardware Security Modules (HSMs)
Protect cardholder data	3.4, 3.5, 3.6, 3.7	 Hardware Security Modules (HSMs)  Tokenization  Transparent Encryption  Enterprise Key Management  CipherTrust Manager
Encrypt data transmissions	4.2	 Network Encryption
Restrict access to cardholder data	7.1, 7.2	
Identify and authenticate access to system	8.2, 8.3, 8.4, 8.5	 Transparent Encryption  Identity & Access Management  SafeNet Trusted Access
Track access to cardholder data	10.1, 10.3, 10.5	
Identify cardholder data across Hybrid IT	12.5, 12.10.7	 Data Discovery and Classification

How Thales Solutions Enable PCI DSS 4.0 Compliance

PCI DSS 4.0 Requirement	Thales Solution
2, 6: Secure Systems and Software	 Luna HSMs Enable multi-tenancy and separation of duties to ensure that only authorized users can access the secure data. Also protects electronic integrity and authenticity of code and identities, whether it is a physical or virtual server or the user, in a tamper-proof hardware device.
3.4, 3.5, 3.6: Protect cardholder data	 CipherTrust Transparent Encryption Delivers data-at-rest encryption for files and folders and privileged user access control. Protects cardholder data wherever it resides, on-premises, across clouds, and in big data and container environments.
	 CipherTrust Tokenization The CipherTrust Tokenization solution includes several dynamic data masking options, enabling the display of just the first six or last four digits of the PAN or the full 16-digit PAN, depending on the role of the user.
	 Enterprise Key Management Streamlines and strengthens key management in cloud and enterprise environments over a diverse set of use cases. Enables centrally managing the key lifecycle and access policies in a FIPS certified hardware.
	 CipherTrust Manager CipherTrust Manager centralizes the management and storage of encryption keys in a high-availability cluster of appliances that is centrally managed. CipherTrust Manager can function as central key manager for multiple external encryption platforms including third party platforms.
	 Luna 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.
4.1: Encrypt data transmissions	 High Speed Encryptors (HSE) Provide network-independent, data-in-motion encryption ensuring cardholder and other sensitive data is secure as it moves from site-to-site, or from on-premises to the cloud and back.

How Thales Solutions Enable PCI DSS 4.0 Compliance

PCI DSS 4.0 Requirement

Thales Solution

7.1, 7.2: Restrict access to cardholder data

8.1, 8.3, 8.7: Track access to cardholder data

10.1, 10.2, 10.3: Identify and authenticate access to system



OneWelcome Identity & Access Management

The OneWelcome Identity Platform enables you to centrally manage unique user identities, risk-based authentication policies, and add/revoke access to systems in your cardholder data environment (CDE). OneWelcome offers powerful and expansive modern authentication capabilities that meet the needs of diverse users.



SafeNet Trusted Access

Offers the broadest range of authentication methods and form factors, and allows customers to address numerous use cases, assurance levels, and threat vectors. It provides a full audit trail of access events as well as automated log export and seamless integration with SIEM systems.



CipherTrust Transparent Encryption

Provides separation of roles where only authorized users and processes can view encrypted data. Any read, write, or other access request for sensitive data is audited. Security intelligence logs capture access records and connect with leading security information and SIEM systems.

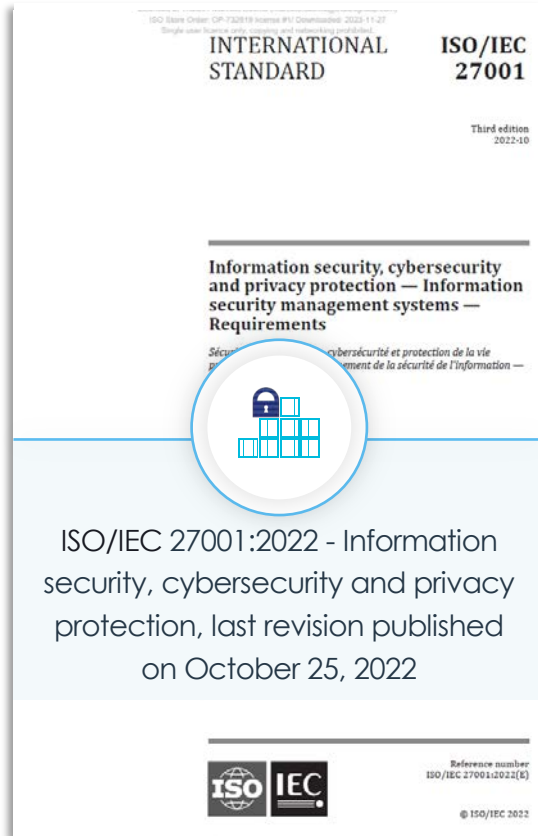
12.5; 12.10.7: Detection of stored PAN anywhere



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, such as PANS, and help uncover compliance gaps.

ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection



ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection, last revision published on October 25, 2022



Overall objective

ISO/IEC 27001 is the world's best-known standard for information security management systems (ISMS). The ISO/IEC 27001 standard provides organizations of any size and from all sectors with guidance for establishing, implementing, maintaining, and continually improving an information security management system.

Conformity with ISO/IEC 27001 means that an organization has put in place a system to manage risks related to the security of data owned or handled by the organization. ISO/IEC 27001 was first published in 2005 and updated on October 25, 2022, as ISO/IEC 27001:2022 reflecting the ever-changing landscape of technology and information security.



Applies to

ISO certification is available for companies across all economic sectors (all kinds of services and manufacturing as well as the primary sector; private, public and non-profit organizations).



Penalties

ISO/IEC 27001 is an international standard with no penalties for non-compliance. However, ISO/IEC 27001 certification can provide a layer of defense against fines by regulations such as GDPR by showing good faith efforts of an organization in information security.



Compliance for ISO 27001:2022 Information security, cybersecurity and privacy protection

Thales helps organizations comply with ISO/IEC 27001:2022 by addressing essential requirements listed in the Annex A for Information Security Controls.

Requirements	ISO 27001 controls	Thales Supporting Capabilities
Annex A: Information Security Controls		
Classification of Information	5.12	 Data Discovery and Classification
Data Security	5.3, 5.33, 5.34 8.7, 8.10, 8.11, 8.12, 8.24	 CipherTrust Data Security Platform  Hardware Security Modules (HSMs)  High Speed Encryptions (HSE)
Access Control and Authentication	5.15, 5.17, 5.18 6.7 8.3, 8.4, 8.5	 Identity and Access Management  SafeNet Trusted Access  Transparent Encryption
Cloud Security	5.23, 5.30	 Cloud Key Management  Transparent Encryption
Application Security	8.25, 8.26	 CipherTrust Platform Community Edition  CipherTrust Secrets Management

How Thales Solutions Enable ISO/IEC 27001:2022 Compliance

ISO 27001 Controls

Thales Solution

5.12: "...Information should be classified according to the information security needs..."



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.

5.3: Segregation of Duties



CipherTrust Data Security Platform

The CipherTrust Data Security Platform is an integrated suite of data-centric security products and solutions that unify sensitive data discovery, protection, and control in one platform. Its extensive features include encryption, tokenization, key-management, and granular access controls.

5.33: Protection of Records



CipherTrust Tokenization

Permits the pseudonymization/masking of sensitive information in databases while maintaining the ability to analyse aggregate data, without exposing sensitive data during the analysis or in reports.

5.34: Privacy and Protection of PII



CipherTrust Enterprise Key Management

Streamlines and strengthens key management in cloud and on-premises environments for home-grown encryption, as well as third-party applications.

8.7: Protection against Malware

8.10: Information Deletion



CipherTrust Transparent Encryption (CTE)

Delivers data-at-rest encryption for files and folders and privileged user access control with granular policies. Protects data wherever it resides on hybrid IT with complete separation of duties.

8.11: Data Masking



CTE Ransomware Protection

Watches for abnormal I/O activity on files hosting business critical data on a per process basis. It allows administrators to alert/block suspicious activity before ransomware can take hold of your endpoints/servers.

8.12: Data Leakage Prevention

8.24: Use of Cryptography



Luna 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.



High Speed Encryptor (HSE)

Provides network-independent, data-in-motion encryption ensuring data, video, voice, and metadata is secure as it moves from site-to-site, or from on-premises to the cloud and back, reducing risk of data leakage.

How Thales Solutions Enable ISO/IEC 27001:2022 Compliance

ISO 27001 Controls

Thales Solution

5.15: Access Control

5.17: Authentication information

5.18: Access Rights

6.7: Remote Working

8.3: Information Access Restriction

8.4: Access to Source Code

8.5: Secure Authentication



OneWelcome Identity & Access Management

Limits the access of internal and external users based on their roles and context with granular access and authorization policies that help ensure that the right user is granted access to the right resource at the right time.



SafeNet Trusted Access

Enables Multi-factor Authentication with the broadest range of hardware and software methods and form factors, allowing customers to address numerous use cases, assurance levels, and threat vectors with unified policies.



CipherTrust Transparent Encryption

Delivers data-at-rest encryption for files and folders and privileged user access control with granular policies. Provides complete separation of roles where only authorized users and processes can view encrypted data.

5.23: Information security for use of cloud services

5.30: ICT readiness for business continuity



CipherTrust Cloud Key Management

Reduces third party risks by maintaining on-premises under the full control of the organization the keys that protect sensitive data hosted by third party cloud providers.



CipherTrust Transparent Encryption

Provides complete separation of roles where only authorized users and processes can view encrypted data. This keeps third party cloud provider employees, such as support engineers and DB admins from seeing the data in the clear.

8.25: Secure development lifecycle

8.26: Application security requirements



CipherTrust Platform Community Edition

Makes it easy for DevSecOps to deploy data protection controls in hybrid and multi-cloud applications, providing key management, transparent encryption for Kubernetes, and tokenization.



CipherTrust Secrets Management

Protects and automates access to secrets across DevOps tools and cloud workloads including secrets, credentials, certificates, API keys, and tokens as part of a state-of-the-art secrets management solution.

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