eBook

Data security compliance with the ISO/IEC 27001:2022 - information security, cybersecurity, and privacy protection standard

How Thales solutions help with ISO/IEC 27001 compliance

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

ISO (International Organization for Standardization) is an independent, non-governmental international organization with a membership of 170 national standards bodies. ISO/IEC 27001 is jointly published by ISO and the International Electrotechnical Commission (IEC) and is the world's best-known standard for information security management systems (ISMS). The ISO/IEC 27001 standard provides all organizations with guidance for establishing, implementing, maintaining, and continually improving information security management systems.

Conformity with ISO/IEC 27001 means that an organization or business has put in place a system to manage risks related to the security of data owned or handled by the organization, and that this system employs all the best practices and principles enshrined in this International Standard.

What are the changes to ISO/IEC 27001?

First published in 2005 ISO/IEC 27001 was revised on September 25, 2013, as ISO/IEC 27001:2013, and again on October 25, 2022, as ISO/IEC 27001:2022. It has been updated to reflect the ever-changing landscape of technology and information security. The biggest change in 2022 is Annex A.

Annex A in ISO/IEC 27001 is a part of the standard that lists a set of classified security controls that organizations use to demonstrate compliance with ISO/IEC 27001 6.1.3 (Information security risk treatment). A total of 24 controls were merged and 58 controls were revised from the ISO/IEC 27002:2013 to align with the current cyber security and information security environment.

	ISO/IEC 27001: 2013	ISO/IEC 27001: 2022
Annex A Control Categories	114 controls 14 sections	93 controls 4 sections • Organizational – 37 controls • People – 8 controls • Physical – 14 controls • Technological – 34 controls

Which companies can be ISO/IEC 27001:2022 certified?

ISO standards are internationally agreed to by cybersecurity experts and are widely recognized globally. ISO certification is available for organizations across all economic sectors (all kinds of services and manufacturing as well as the primary sector; private, public, and non-profit organizations).

What are the penalties for ISO/IEC 27001:2022 non-compliance?

ISO/IEC 27001 is an international standard with no penalties for non-compliance. However, ISO/IEC 27001:2022 certification can provide a layer of defense against fines by regulations such as GDPR in the event of a data breach, by showing an organization's good faith efforts in implementing information security best practices.

How can Thales help with for ISO/IEC 27001:2022 compliance?

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

ISO/IEC 27001:2022 Requirements	Thales Solutions
Classification of Information	
5.12: Classification of Information: 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.
Data Security	
5.3: Segregation of Duties Conflicting duties and conflicting areas of responsibility should be segregated. **5.33: Protection of Records** Records should be protected from loss, destruction, falsification, unauthorized access, and unauthorized release. **5.34: Privacy and Protection of PII** Identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements. **8.7: Protection against Malware** Protection against malware should be implemented and supported by appropriate user awareness. **8.10: Information Deletion** Information stored in information systems, devices or in any other storage media should be deleted when no longer required. **8.11: Data Masking** Should be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies. **8.12: Data Leakage Prevention** Data leakage prevention measures should be applied to systems, networks, and any other devices that process, store, or transmit sensitive information. **8.24: Use of Cryptography** Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.	**CipherTrust Data Security Platform** is an integrated suite of data-centric security products and solutions that unify data discovery, protection, and control in one platform. CipherTrust 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. It provides a complete separation of roles, where only authorized users and processes can view unencrypted data. This ensures privacy and protects sensitive data wherever it resides, on-premises, across multiple clouds, and within big data and container environments. • **CipherTrust Tokenization** with dynamic data masking 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 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. In addition, encrypted information can be effectively deleted by destroying encryption keys. • **CipherTrust Transparent Encryption Ransomware Protection (CTE-RWP)** continuously monitors processes for abnormal I/O activity and alerts or blocks malicious activity before ransomware can take complete hold of your endpoints and servers. It monitors active processes to detect ransomware – identifying activities such as excessive data access, exfiltration, unauthorized encryption, or malicious impersonation of a user, and alerts/blocks when such an activity is detected. **Thales Luna 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. Luna HSMs: • Generate and protect root and certificate authority (CA) keys, providing support for PKIs across a variety of use cases • Sign application code to ensure software remains secure, unaltered, and authentic. • Create digital certificates for credentialing and authenticating proprietary electronic devices for IoT applications and other network deployments. **Thales High Speed Encryptors (HSEs)** 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 limit data leaks and better protect data, video, voice, and metadata from eavesdropping, surveillance, and overt and covert interception— without performance compromise.

ISO/IEC 27001:2022 Requirements	Thales Solutions
Access Control & Authentication	
5.15: Access Control Rules to control physical and logical access to information and other associated assets should be established and implemented. **5.17: Authentication information** Allocation and management of authentication information should be controlled by a management process. **5.18: Access Rights** Access rights to information should be provisioned, reviewed, modified, and removed according to policy. **6.7: Remote Working** Security measures should be implemented when personnel are working remotely. **8.3: Information Access Restriction** Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control. **8.4: Access to Source Code** Read and write access to source code, development tools, and software libraries should be managed. **8.5: Secure Authentication** Secure authentication technologies and procedures should be implemented.	**Thales OneWelcome** identity and access management 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 ensure the right user is granted access to the right resource at the right time. This minimizes the risk of unauthorized access. • **SafeNet Trusted Access** is a cloud-based access management solution that provides commercial, off-the-shelf multi-factor authentication with the broadest range of hardware and software authentication methods and form factors. • **Thales converged badge solutions** simplify the management of physical and logical access by consolidating all corporate security applications in a single user's badge: physical access to buildings and restricted areas, visual identification of the cardholder, secure access to sensitive digital resources thanks to PKI-certificate based and/ or FIDO authentication. • The broad list of **supported authentication methods** meets the needs of a large variety of users and enables organizations to protect all their users and sensitive digital resources with strong multifactor authentication. **Thales OneWelcome Consent & Preference Management** module enables organizations to gather the consent of end consumers, so, for example, financial institutions have clear visibility of consented data allowing them to manage access to data they are allowed to utilize. **CipherTrust Transparent Encryption** encrypts sensitive data and enforces granular privileged-user-access management policies that can be applied by user, process, file type, time of day, and other parameters. It provides complete separation of roles, where only authorized users and processes can view unencrypted data.
Cloud Security	
5.23: Information security for use of cloud services Processes for acquisition, use, management, and exit from cloud services should be established. **5.30: ICT readiness for business continuity** ICT readiness should be planned, implemented, maintained, and tested based on business continuity objectives.	**CipherTrust Cloud Key Manager** can reduce third cloud security risks by maintaining on-premises under the full control of the organization the keys that protect sensitive data hosted by third party cloud providers under "bring your own keys" (BYOK) systems. **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 will not be accessible in cleartext to unauthorized users. **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.

ISO/IEC 27001:2022 Requirements	Thales Solutions
Application Security	
8.25: Secure development lifecycle Rules for the secure development of software and systems should be established and applied. **8.26: Application security requirements** Information security requirements should be identified, specified, and approved when developing or acquiring applications.	**CipherTrust Platform Community Edition** makes it easy for DevSecOps to deploy data protection controls in hybrid and multi-cloud applications. The solution includes licenses for CipherTrust Manager Community Edition, Data Protection Gateway, and CipherTrust Transparent Encryption for Kubernetes. **CipherTrust Secrets Management** is a state-of-the-art secrets management solution, which protects and automates access to secrets across DevOps tools and cloud workloads including secrets, credentials, certificates, API keys, and tokens. **CipherTrust Application Data Protection** offers developer-friendly software tools for encryption key management as well as application-level encryption of sensitive data. It can take place immediately upon data creation or first processing and can remain encrypted regardless of its data life cycle state – during transfer, use, backup or copy, to provide the highest level of security at the application layer. **Thales Data Protection on Demand (DPoD)** is a cloud-based marketplace that offers Luna HSMs and CipherTrust solutions as a service. This enables in-house teams to leverage these proven and certified data security solutions easily and securely in their own offerings.

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.