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

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.

What about ISO 27002?

While ISO/IEC 27001 specifies the requirements for establishing an ISMS, ISO/IEC 27002 provides the detailed best practices and controls that can be applied within the ISMS. The main difference is that the ISO/IEC 27001 is a standard that organizations can get certified for, while ISO/IEC 27002 is not. The requirements in the tables below are listed on both ISO 27001 and ISO 27002.

How Thales Helps with 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.

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

ISO 27001 Annex A Requirements	Application Security	Data Security	Identity & Access Management
5 Organisational controls **5.3, 5.5, 5.9, 5.10, 5.12, 5.15, 5.17, 5.18, 5.19, 5.21, 5.23, 5.25, 5.28, 5.33, 5.34**		√	√
6 People controls **6.7**			√
7 Physical controls **7.1, 7.2**			√
8 Technological controls **8.3, 8.5, 8.7, 8.8, 8.10, 8.11, 8.12, 8.15, 8.16, 8.20, 8.24, 8.26, 8.33**	√	√	√

- **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 behaviour 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.

How our Application Security Solutions help with ISO 27001 compliance

ISO 27001:2022	Thales Capabilities	Thales Solutions
8.7 Protection against malware	• Use signature, behavioral and reputational analysis to block all malware injection attacks.	**Web Application Firewall**
8.8 Management of technical vulnerabilities	• Discover, inventory, and remediate vulnerabilities in APIs that process, receive, transmit, and store sensitive data.	**API Security**
8.16 Monitoring activities **8.20 Networks security**	• Inspect all traffic, detect and prevent web-based attacks with WAF. • Prevent DDoS attacks with scalable DDoS attack traffic absorption provided by edge servers. • Prevent malicious Bot attacks with automated protection.	**Web Application Firewall** DDoS **DDoS Protection** **Bot Protection**
8.26 Application security	• Protect apps from runtime exploitation, while integrating with tools in the CI/CD pipeline. • Detect and prevent cyber threats with web application firewall. • Monitor API activity, track usage, detect anomalies, and identify potential unauthorized access attempts.	**Runtime Protection** **Web Application Firewall** **API Security**

How our Data Security Solutions help with ISO 27001 compliance

ISO 27001:2022	Thales Capabilities	Thales Solutions
GOVERNANCE & REPORTING **5.5 Contact with authorities** **5.7 Threat intelligence** **5.9 Inventory of information** **5.10 Acceptable use of information** **5.12 Classification of Information** **5.25 Assessment on security events** **5.28 Collection of evidence** **8.7: Protection against Malware** **8.8 Management of vulnerabilities** **8.15 Logging**	• Identify structured and unstructured sensitive data at risk across Hybrid IT. • Identify vulnerabilities and document current state of compliance. • Monitor data access and activity and identify threats to sensitive data. • Collect evidence of security events through automated reporting, dashboards, and secure audit trail. • Log sensitive data access and stream to SIEM systems. • Maintain a year's worth of records for audit reporting • Automatically notify relevant authorities. • Monitor for abnormal I/O activity and block malware	**Data Security Fabric** • Data Discovery & Classification • Data Activity Monitoring • Data Risk Analytics • Vulnerability Management • Data Governance • Reports and Portals **CipherTrust Platform** • Data Discovery & Classification • Transparent Encryption • Ransomware Protection
DATA PROTECTION **5.33 Protection of records** **5.34 Privacy and protection of PII** **8.10 Information deletion** **8.11 Data masking** **8.12 Data leakage prevention** **8.24 Use of cryptography** **8.26 Application security** **8.33 Test information**	• Protect data-at-rest, in use, and secrets across hybrid IT. • Protect data in motion with high-speed encryption. • Pseudonymize and mask sensitive information for production or tests. • Protect cryptographic keys in a FIPS 140-2 Level 3 environment. • Streamline key management in cloud and on-premises environments. • Manage and protect all secrets and sensitive credentials. • Maintain crypto-agility with products designed for post-quantum upgrade. • Secure execution with Confidential Computing.	**CipherTrust Platform** • Transparent Encryption • Tokenization & Masking • Key & Secrets Management • Confidential Computing • Community Edition • Application Data Protection **Hardware Security Modules** **High Speed Encryption**
INFORMATION ACCESS CONTROL **5.3 Segregation of duties** **5.18 Access rights** **8.3 Information access restriction**	• Enforce granular user access policies to sensitive data and secrets. • Enable complete separation of roles where only authorized users and processes can view unencrypted data.	**CipherTrust Platform** • Transparent Encryption **Data Security Fabric** • Data Risk Analytics
CLOUD RISK **5.23 Information security for use of cloud services** **5.19 Information security in supplier relationships**	• Reduce third party risk by controlling cloud encryption keys and conserving cloud portability of data. • Ensure complete separation of roles. • Monitor & alert anomalies before disrupting supply chain.	**CipherTrust Platform** • Cloud Key Management • Transparent Encryption **Data Security Fabric** • Data Activity Monitoring • User Rights Managements

How our Identity & Access Management Solutions help with ISO 27001 compliance

ISO 27001:2022	Thales Capabilities	Thales Solutions
5.15 Access control **5.18 Access rights** **8.3 Information access restriction** **8.15 Logging**	• Limit the access of internal and external users to systems and data based on roles and context with policies. • Centralize access control over multiple hybrid environments in a single pane of glass, log all events and stream logs to external SIEM systems. • Prevent password fatigue with Smart Single Sign-On with conditional access. • Create frictionless, secure and privacy protected access for customers.	**Workforce Access Management** **Customer Identity & Access Management** • Policy control • Centralized access • Contextual access • SSO, Passwordless • Logging
5.17 Authentication information **8.5 Secure authentication**	• Enable Multi-Factor Authentication (MFA) with the broadest range of hardware and software methods. • Build and deploy adaptive authentication policies. • Protect against phishing and man-in-the-middle attacks. • Risk-Based Authentication and PKI and FIDO Authenticators.	**Workforce Access Management** **Customer Identity & Access Management** **Broad Range of Authenticators**
5.23 Information security for use of cloud services **5.21 Managing information security in ICT supply chain** **5.19 Information security in supplier relationships**	• Enable relationship management with suppliers, partners or any third-party user. • Minimize privileges by using relationship-based fine-grained authorization.	**Workforce Access Management** • Third-party Access Control • Delegated User Management • Externalized Authorization
6.7 Remote working	• Secure and convenient remote access to cloud services and enterprise apps for thousands of employees. • Separate remote access for contractors and gig workers.	**Workforce Access Management** **Customer Identity & Access Management**
7.1 Physical security perimeters **7.2 Physical entry**	• Simplify the management of physical and logical access by consolidating all corporate security applications in a single user's badge. • Enable secure physical access to buildings and restricted areas, visual identification of the cardholder, secure access to sensitive resources.	**Smart cards**

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.

Disclaimer: The information contained herein is believed to be accurate on the date of publishing. Thales provides this material for your information only. Its content is not legal advice nor does it amount to a certification or guarantee of compliance in respect of any applicable law. Third parties shall be solely responsible for their own interpretation of any applicable law. The information should not be construed as a commitment to deliver any specific upgrade, feature or functionality. You should not rely on the anticipated timelines or potential upgrades, features or functionality described in the presentation when making a decision to purchase products from Thales. Thales does not accept any liability howsoever arising from any use of this material.

cpl.thalesgroup.com

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