Compliance Brief

Data Security Compliance with the Information and Cyber Security Guidelines 2023 for Indian Insurance Industry

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

What are the Information and Cyber Security Guidelines 2023?

The digitalization initiated by the Indian government in 2017 and the remote working arrangements during COVID-19 marked a change in the manner of data handling and processing by the Indian insurance industry. The insurance industry started to streamline its operations to enhance business efficiencies and customer experience, which also exposed the insurance sector to greater vulnerabilities of cyber threats and data leaks.

With the evolving cybersecurity landscape, the Insurance Regulatory and Development Authority of India (IRDAI) introduced the Information and Cyber Security (ICS) Guidelines 2023 on April 24, 2023, which superseded the 2017 Guidelines.

What are the changes to ICS Guidelines 2023?

The primary emphasis of the ICS Guidelines 2023 is on a data-centric security approach – securing the data itself rather than just the network or system it is stored in. The ICS Guidelines 2023 also mandates Regulated Entities (RE) to adopt a risk-based approach, take necessary measures to secure data management, and mitigate cyber threats against loss, misuse, or leak of sensitive customer information in any form.

Vision: To provide a user-centric trusted and secure set of resources and environment for employees to conduct business while ensuring the protection of the organization's information assets including customer data.

Mission: Ensuring the security of all Organization's information assets through implementing up-to-date security mechanisms for prevention and monitoring of threats; governance of information security-related activities and awareness of all employees.

Which companies are subject to ICS Guidelines?

ICS Guidelines 2023 applies to all insurance intermediaries, including brokers, foreign reinsurance businesses (FRBs), corporate agents, web aggregators, third-party administrators (TPAs), insurance marketing firms (IMFs), insurance repositories, insurance self-network platforms (ISNPs), corporate surveyors, motor insurance service providers (MISPs), common service centers (CSCs), and the Insurance Information Bureau of India (IIB) (collectively with insurers, the "Regulated Entities").

How can Thales help with the Information and Cyber Security Guidelines 2023?

Thales helps organizations comply with Information and Cyber Security Guidelines 2023 by addressing 6 security domain policies.

Security Domain Policies & Description	Thales Solution
2.1 Data Classification	
3.3 Data Classification Process "ensure that the information assets for which they are responsible are **assigned a classification** rating (Confidential, Restricted, Internal, and Public) that properly indicates its business value and criticality to the organization."	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.

Security Domain Policies & Description	Thales Solution
Confidential Information **3.4.1.2 Storage Requirements** "require **user authentication** that can uniquely identify each user or administrator." "Storage environments shall be periodically reviewed and audited to help ensure that information is sufficiently secured." **3.4.1.3 Transfer Requirements** "When CONFIDENTIAL information is transmitted outside of the Organization network,... it shall be sent in **encrypted** form or via a secured channel. **Encryption keys** shall be managed and protected by authorized resources ..." **Restricted Information** **3.4.2.3 Transfer Requirements** "... it shall be sent over a secured channel or **in encrypted form**. **Encryption keys shall be managed and protected** by authorized resources as defined in the Cryptographic Security policy." **3.5.3 Storage, Transfer & Destruction of PII** "SPI will be accorded the **same level of security as confidential information** irrespective of the classification of such information..."	**Data Security Fabric** monitors data from a unified viewpoint for auditing across diverse on-premises and cloud platforms, providing oversight for relational databases, NoSQL databases, mainframes, big data platforms, and data warehouses. Detailed structured an unstructured data activity is captured automatically, making it easier to fulfill audit requests. **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.
2.2 Asset Management	
3.1 Information Asset Profiling "Data will be classified as per data classification policy." "Other information assets will be classified to reflect business needs, legal-regulatory-certificatory requirements and confidentiality-integrity-availability concerns..." **3.2.2.1 Asset Labeling** "Every asset shall be marked for **identification and inventory control**..." **3.2.2.2 Asset Inventory and Documentation** "...asset shall be clearly identified individually and (if appropriate) collectively in combination with other assets to form an identifiable information asset..."	**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.

Security Domain Policies & Description	Thales Solution
3.2.2.3 Authorization Inventory "The asset inventory shall contain details of **authorization mechanism** for all information assets" "For Organization-owned assets, the authorization record shall consist of the owner and the features of the asset used to authorize the asset to the Organization's network ..." 3. "For non Organization-owned assets, the authorization record shall consist of parameters used for **two factor authentication**..." **3.2.3 Asset Use** "... use client certificates to **authenticate hardware assets** connecting to the organization's trusted network..." "Assets shall not be taken out of Organization's premises without appropriate authorizations. In scenarios where the asset may need to be taken out of Organization's premises for repairs / replacement appropriate authorizations shall be taken after ensuring that the data contained in the assets has been securely erased."	**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. Combining secrets management with **key management** is like having a fortified vault for all your valuable assets in one place for inventory control.
3.2.6 Asset Disposal "... critical and sensitive information shall be **disposed in a secure manner** by incineration or shredding, or erasure of data for use by another application within the organization;" "Any information that resides in the asset shall be **removed from the equipment before disposal** using secure erase / disposal techniques..." "In case of confidential data, **cryptographic techniques shall be used** to protect data on removable media...	**CipherTrust Enterprise Key Management** ensures secure asset disposal, it streamlines and strengthens key management in cloud and enterprise environments over a diverse set of use cases, encrypted information can be effectively deleted by destroying encryption keys. 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.
2.3 Access control	
3.3 User-ID Creation and Maintenance "Levels of access granted to all Users shall enforce **segregation of duties** and adhere to the "need to know" principle." **3.5 Privileged User Accounts** "Privileged user accounts shall be limited to individuals with specific business justification for this level of access. **Audit logging of system** activities performed by privileged users, shall be maintained." **3.8 Compliance and audit** "All evidence for granting, revoking, or changing remote access privileges shall be **maintained in a repository** such as Change Management System."	**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 (STA)** 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. It 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. STA also offers an up-to-date audit trail of all access events to all systems. Extensive automated reports document all aspects of access enforcement and authentication.

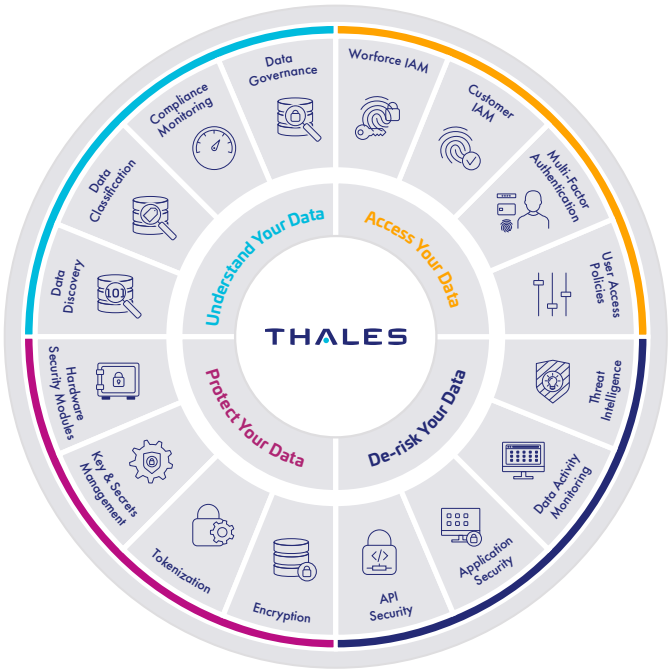
Security Domain Policies & Description	Thales Solution
2.16 Monitoring, Logging and Assessment	
3.3 Information systems logging and monitoring All information systems will be configured to log system activities and generate alerts for any unusual activity to system administrators. The activities of privileged users such as system administrators and system operators shall be logged and independently reviewed on a regular basis.	CipherTrust Transparent Encryption Ransomware Protection (CTE-RWP) continuously monitors processes for abnormal activity and alerts or blocks malicious activity. It monitors active processes to identify activities such as excessive data access, exfiltration, unauthorized encryption, or malicious impersonation of a user, and alerts/blocks when such an activity is detected.
2.12 Cryptographic Controls	
3.1 Use of Cryptograph Controls **"Cryptographic controls** shall be used for securing information that is confidential and restricted and transported by mobile or removable media devices or across communication lines... Information used to verify the identification of remote terminals shall be appropriately protected. Static or reusable authentication information shall be **encrypted** during storage and while passing through the network **using encryption software or hardware**."	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.
3.2 Key Management "A policy on the use, protection and lifetime of **cryptographic keys** shall be developed and implemented through their whole lifecycle."	CipherTrust Manager enables organizations to centrally manage encryption keys, provide granular access control and configure security policies. CipherTrust Manager is the central management point for the CipherTrust Data Security Platform and manages key lifecycle tasks including generation, rotation, destruction, import and export, provides role-based access control to keys and policies, supports robust auditing and reporting, and offers developer friendly REST API. 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.

Security Domain Policies & Description	Thales Solution
2.19 Cloud Security	
3.4.7 Encryption "... ensure that the cloud service provider support **Key Management Interoperability Protocol (KMIP)**. KMIP provides a standardized way to manage encryption keys across diverse infrastructures. Organization shall prefer **Hardware encryption keys**, in compliance with the Federated Information Processing Standard (FIPS) 140 2-3 and above," "Organization shall **devise encryption, key management** procedures..."	**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, and support KMIP as well as third-party applications. **CipherTrust Cloud Key Management** allows organizations to separate the keys from the data stored in the cloud, preventing unauthorized data access by the Cloud Service Provider by using the Hold-Your-Own-Key (HYOK) technology, organizations retain full control and ownership of their data by controlling encryption key access.
3.4.8 Application Security "Organization shall ensure Application Security for applications hosted over the Cloud in accordance with the existing "Information and Cyber Security Policy, Security Domain Policy, Section 2.5 – 'Information Systems acquisition and development', subsection –'Application Security'."	**CipherTrust Data Security Platform** provides multiple capabilities for application security. Among them: • **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.

Organizations can leverage Thales' suite of identity and data security solutions available on a single unified platform to become compliant today and stay compliant in the future. Contact us now!

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.



cpl.thalesgroup.com

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