

Achieve Korea Personal Information and Information Security Management System (ISMS-P) Compliance



Korean ISMS-P: The Korean Personal Information and Information Security Management System (ISMS-P) is an information security and personal information management standard created by the Korea Internet & Security Agency (KISA). Compliance with this standard is mandated by the Personal Information Protection Act and “Act on Promotion of Information and Communications Network Utilization and Information Protection” as it is designed to help organizations in Korea protect their information assets.

Overview

In November 2018, the Korean Ministry of Science and ICT (MSIT), Korea Communications Commission, and Ministry of the Interior and Safety merged the **Information Security Management System (ISMS)** and the Korea-Personal Information Management System (**PIMS**) into a new certification system – **Personal Information and Information Security Management System (ISMS-P)**.

The goal of integrating these two systems is to:

- Echo the recent trends in integrating information security and the protection of personal information
- Strengthen the links between these systems
- Reduce the compliance burden on organizations due to the considerable overlap of requirements.

The Korean government introduced the **Information Security Management System (ISMS)** – the certification sponsored by Korea Internet and Security Agency (KISA) and affiliated with the Korean Ministry of Science and ICT (MSIT) under Article 47 in the “Act on Promotion of Information and Communications Network Utilization and Information Protection”.

- The ISMS framework defines a stringent set of control requirements designed to help ensure that organizations consistently and securely protect their information assets, it has a significant overlap with ISO/IEC 27001 control objectives but are not identical.
- The ISMS provides a more detailed investigation against requirements than a general ISO/IEC 27001 assessment.
- KISA is the ISMS certifying authority, certification is valid for three years, and certified entities must pass an annual audit to maintain it.

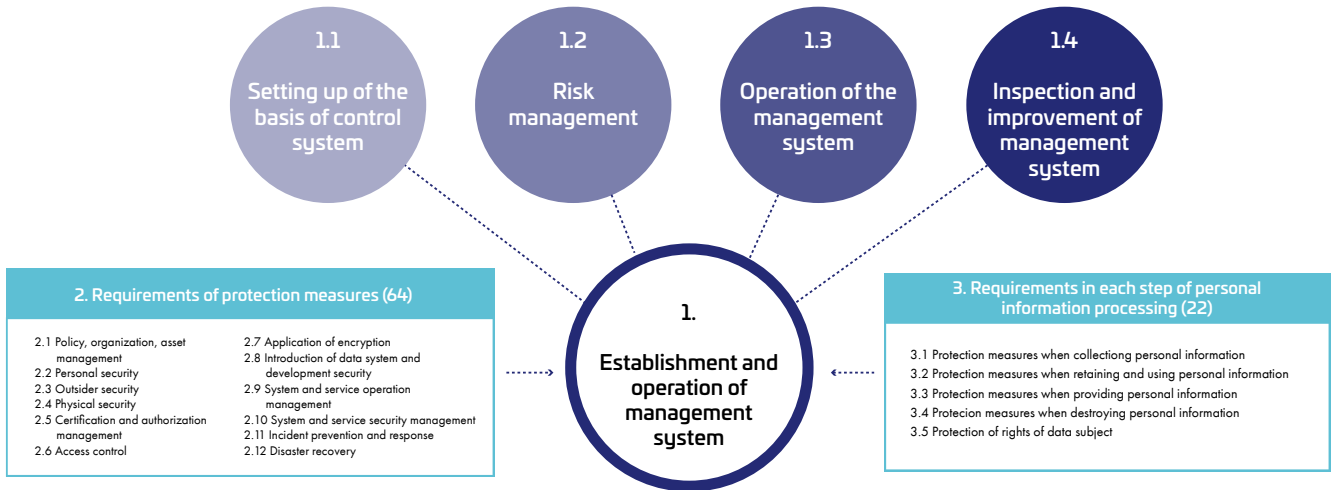
Instead of 104 K-ISMS controls and 82 K-PIMS controls, **ISMS-P** – the new consolidated certification has 80 controls related to information security and 22 controls related to the protection of personal information.

80 controls related to information security

- Establishment and operation of management system [16]
- Requirements for protection measures [64]

22 controls related to the protection of personal information

- Requirements of each step of personal information processing [22]



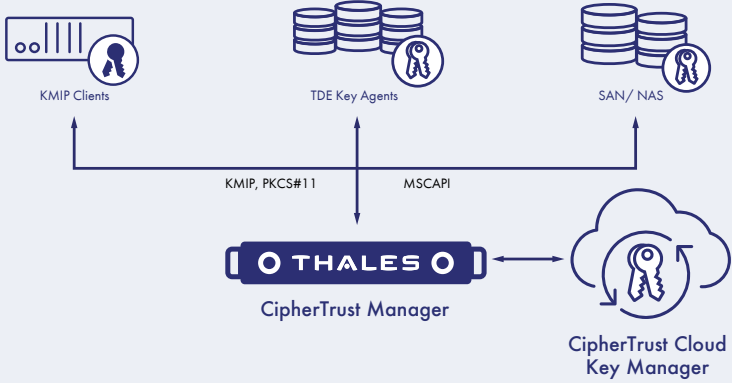
Who must obtain the ISMS-P certification?

KISA mandates certification for compulsory subjects that include:

Internet service providers	Internet datacenter	Any organization that meets these conditions:
<ul style="list-style-type: none"> • that are authorized by Article 6, Section 1 of the Telecommunication Business Act 	<ul style="list-style-type: none"> • designated as an “integrated information and communication facilities” by Article 46 in the Act on Promotion of Information and Communications Network Utilization and Information Protection. 	<ul style="list-style-type: none"> • Hospitals categorized as a “higher general hospital” in Article 3, Section 4 of the Medical Service Act whose annual sales or tax revenue is at least \$150 million (USD). • Schools, per Article 2 in the Higher Education Act, where the number of enrolled students is at least 10,000 as of December 31 of the immediately preceding year. • Information network service providers whose sales of information and communication services are at least \$10 million (USD) or an average of at least 1 million users per day in the previous three months; excluding, however, a financial company under subparagraph 3 of Article 2 of the Electronic Financial Transactions Act.

How Thales can help?

With extensive experience helping organizations comply with compliance mandates, Thales offers integrated solutions that enable your organizations to address the Personal Information and Information Security Management System **(ISMS-P)**.

ISMS-P requirements	Recommendations
<p>2.7 Application of encryption</p> <p>2.7.2 Encryption key management</p> <ul style="list-style-type: none"> • Management procedures for the safe generation, use, storage, distribution, and destruction of encryption keys should be established and implemented, and recovery measures should be prepared if necessary. • For encryption key generation, use, storage, distribution, and destruction, policies and procedures including the following should be established. • Encryption must be performed when storing, transmitting, and delivering personal and important information according to the encryption policy. 	<p>Protection of cryptographic keys</p> <p>Luna HSMs from Thales provide a hardened, tamper-resistant environment for secure cryptographic processing, key generation and protection, encryption, and more. Available in three FIPS 140-2 certified form factors, Luna HSMs support a variety of deployment scenarios.</p> <p>In addition, Luna HSMs:</p> <ul style="list-style-type: none"> • Generate and protect root and certificate authority (CA) keys, providing support for PKIs across a variety of use cases • Sign your application code so you can ensure that your software remains secure, unaltered, and authentic • Create digital certificates for credentialing and authenticating proprietary electronic devices for IoT applications and other network deployments <p>Key Management</p> <p>CipherTrust Manager enables you to centrally manage keys for all CipherTrust Data Security Platform products, and securely store and inventory keys and certificates for third-party devices—including IBM Security Guardium Data Encryption, Microsoft SQL TDE, Oracle TDE, and KMIP-compliant encryption products. By consolidating key management, CipherTrust Manager fosters consistent policy implementation across multiple systems and reduces training and maintenance costs. Or, use standards-based APIs, to simplify the deployment of applications integrated with key management capabilities and automate testing and development of administrative operations. CipherTrust Key Management solutions support a variety of use cases including:</p> <ul style="list-style-type: none"> • CipherTrust Cloud Key Manager streamlines bring your own key (BYOK) management for Amazon Web Services, Microsoft Azure, Salesforce and IBM Cloud. The solution provides comprehensive cloud key lifecycle management and automation to enhance security team efficiency and simplify cloud key management. • CipherTrust Transparent Database Encryption Key Management supports a broad range of databases solutions such as Oracle, Microsoft SQL, and Microsoft Always Encrypted. • CipherTrust KMIP Server centralizes management of KMIP clients, such as full disk encryption (FDE), big data, IBM DB2, tape archives, VMware vSphere and vSAN encryption, etc. 

ISMS-P requirements

3.2 Protection measures when retaining and using personal information

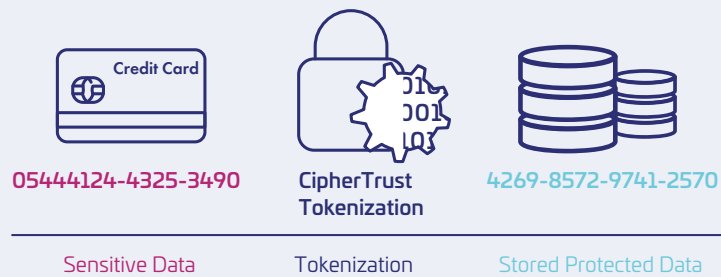
3.2.3 Limited display of personal information

- When inquiring and outputting personal information (printing, screen display, file creation, etc.), the purpose shall be specified, and according to the purpose, the minimization of output items, restrictions on the display of personal information, protection measures for output, etc. shall be carried out.
- In addition, in order to prevent excessive use of personal information in the data processing process such as big data analysis and testing, personal information that is not essential for business must be deleted or taken measures to prevent identification.

Recommendations

CipherTrust Tokenization with Dynamic Data Masking

- CipherTrust Tokenization offers application-level tokenization services in two convenient solutions that deliver complete customer flexibility: Vaultless Tokenization with Dynamic Data Masking and Vaulted Tokenization. Both solutions secure and anonymize sensitive assets—whether they reside in the data center, big data environments or the cloud.
- CipherTrust Vaultless Tokenization protects data at rest while its policy-based Dynamic Data Masking capability protects data in use. A RESTful API in combination with centralized management and services enables tokenization implementation with a single line of code per field. Vaultless Tokenization is provided by dedicated, distributed-cluster-capable Tokenization Servers, offering full separation of duties. Tokenization management and configuration including an operational dashboard with convenient tokenization configuration workflows occurs in a graphical user interface.
- CipherTrust Vaulted Tokenization offers non-disruptive format preserving tokenization with a wide range of existing formats and the ability to define custom tokenization formats. Vaulted Tokenization provides a high level of security for highly sensitive data, and instances of it may be installed on a per-server basis or installed as a web service supporting multiple clients.



Key Takeaways:

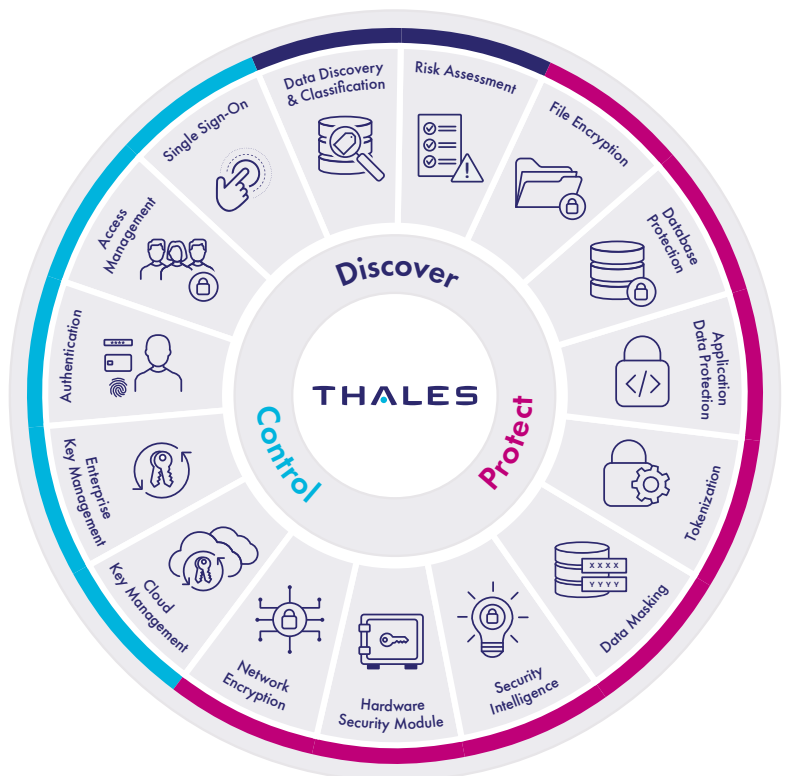
Enhance Data Security and address the ISMS-P requirements





- Simplify data security, and accelerate time to compliance
- Protect sensitive data with encryption or tokenization
- Control access to the data and centralize key management

About Thales

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.

Decisive technology for decisive moments.



> cpl.thalesgroup.com <    

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