

ISMS/ISMS-P Reform in Korea: Key Changes and Implications for Compliance

1. Introduction

In April 2026, the Personal Information Protection Commission (PIPC) and the Ministry of Science and ICT (MSIT) announced the “**Measures to Enhance the Effectiveness of the Personal Information and Information Security Management System Certification Scheme**,” thereby formalizing a fundamental structural overhaul of the existing certification regime.

The government has set forth as its core objective the transition from a document-based, one-off inspection regime to a system that continuously monitors actual operational conditions and performs a preventive function against security incidents. In particular, sweeping changes are anticipated across the entire lifecycle of the certification system, including expansion of certification targets, introduction of risk-based differentiated regulation, transition to technology-based audit methods, reinforcement of post-certification management, and practical implementation of certification revocation mechanisms. These changes are expected to have a significant impact on corporate information security and personal data protection compliance strategies as a whole.

2. Overview of ISMS and ISMS-P

The Information Security Management System (ISMS) and Personal Information and Information Security Management System (ISMS-P) certifications are systems designed to evaluate and certify whether a company's information security and personal data protection management systems are established and operated in compliance with applicable laws and international standards.

While ISMS is a certification that focuses on the overall information security management system, ISMS-P is an integrated certification that adds personal data protection requirements to ISMS. It mandates enhanced protective measures for companies that process personal data. Under the current system, ISMS certification is mandatory for certain information and communications service providers exceeding a certain scale, whereas ISMS-P certification has generally been operated on a voluntary basis.

<ISMS vs ISMS-P Comparison Table>

Category	ISMS	ISMS-P
Legal Basis	Article 47 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (Network Act)	Article 32-2 of the Personal Information Protection Act (PIPA)
Purpose	Protection of information assets and establishment of security management systems	Integrated management system for information security and personal data protection
Applicable Entities	Certain information and communications service providers above a specified threshold	Companies and institutions processing personal data (primarily voluntary)
Mandatory Status	Mandatory for certain entities (*) *Includes Information and Communications Service Providers (ISPs) with annual revenue of KRW 10 billion or more, or with an average of at least one million daily users	Principally voluntary
Certification Criteria	80 criteria (management system + safeguards)	101 criteria (ISMS + 21 additional personal data requirements)
Scope of Protection	Information systems and services	Entire lifecycle of personal data processing
Effect	Enhancement of the information security level	Ensuring trust in personal data protection and regulatory compliance
Structure	Single certification	Extended certification based on ISMS

3. Key Aspects of the New Framework

(1) Certification Targets and Standards Framework

Under the current regime, ISMS-P certification has been operated on a voluntary basis, and uniform standards have been applied regardless of a company's size or risk level. However, under the revised framework, mandatory ISMS-P certification will be required for certain entities. Furthermore, the required level of security will be differentiated based on the company's risk profile.

Yulchon Legal Update

In particular, as the certification system is restructured into three tiers, companies above a certain scale will be subject to enhanced certification standards and more stringent audits. This is expected to go beyond mere certification acquisition and drive the comprehensive advancement of corporate security systems.

Category	As-Is	To-Be	Implementation Timeline
Certification obligation	ISMS certification mandatory for certain entities based on revenue and user thresholds; ISMS-P certification voluntary	Mandatory ISMS-P certification for key public and private personal data controllers (*) *Including major public system operators, telecommunications carriers, identity verification agencies, and large-scale personal data processors based on data volume and revenue	Expected to take effect from the second half of 2027 through amendments to the Enforcement Decree of the PIPA and related notices
Application of standards	Single uniform standard regardless of company size or risk level	Three-tiered system (Advanced(*), Standard, Light) with differentiated standards and audit methods *Advanced tier candidates include major ISPs/IDCs with revenue over KRW 1 trillion and service providers with revenue over KRW 3 trillion	Expected from 2027 through amendments to the Network Act Enforcement Decree and notices
Level of standards	Uniform application of ISMS (80) / ISMS-P (101) criteria	Advanced tier subject to additional enhanced criteria (approx. 20 or more additional requirements)	Expected from 2027 through regulatory amendments and guidelines

Category	As-Is	To-Be	Implementation Timeline
Certification scope	Limited to certain systems and services	Expanded to include all digital assets, including external network interfaces and related infrastructure	Expected from 2027 through notice amendments
Risk assessment	Conducted autonomously with limited standards	Introduction of standardized risk acceptance guidelines and strengthened oversight	Expected from 2027 through the guidelines

(2) Certification Audit Methods

Under the current system, audits have largely relied on documents and evidence submitted by companies. However, under the revised framework, direct inspection of actual systems will become central. In particular, technical verification such as vulnerability assessments, penetration testing, and source code analysis will be incorporated, and auditors will directly access systems to verify operational conditions.

In addition, the introduction of a strengthened preliminary audit stage will prevent companies from proceeding to the main audit if they fail to meet the core security requirements of the preliminary audit, thereby preventing companies from obtaining certification through mere procedural formalities.

Category	As-Is	To-Be	Implementation Timeline
Audit method	Document-based, sampling inspection	On-site verification and validation of actual operations	Expected from 2027 through amendments to relevant laws and notices
Audit workforce & duration	Limited personnel and duration	Additional auditors for the Standard tier, specialized vulnerability assessors for the Advanced tier; extended audit duration	

Category	As-Is	To-Be	Implementation Timeline
Vulnerability assessment	Based on company-submitted materials	Conducted by specialized personnel, including penetration testing	Expected from 2027 through amendments to relevant laws and notices
Audit procedure	Single-stage main audit	Multi-stage process starting from preliminary audit and main audit to post audit	
Preliminary audit	Formal review	(1) Core requirement verification, (2) technical audits for high-risk and incident-prone entities, determining eligibility for the main audit	
Core audit items	Lack of a clearly defined focus	Focus on key items such as CISO/CPO authority, asset identification, encryption, and patch management	
Technical audit	Limited	Full-scale implementation (vulnerability scanning, code analysis, penetration testing)	
Scope of inspection	Sampling of selected systems	Comprehensive inventory of all assets with a focus on critical systems	

(3) Post-Certification Management and Revocation

Previously, post-certification management was relatively lax, and there were virtually no cases of certification revocation. Under the revised framework, however, requirements for maintaining certification will be significantly strengthened. In particular, in the event of a major security incident, certification audits will be immediately suspended, and certification status will be re-evaluated following a government investigation.

Furthermore, with the introduction of clearly defined criteria for “material deficiencies,” certification may be revoked if such deficiencies are not remedied within a specified period, thereby making certification maintenance risk a tangible reality.

Yulchon Legal Update

Category	As-Is	To-Be	Implementation Timeline
Management Approach	Snapshot-based inspection	Continuous monitoring system (with standardized periodic checklists)	To be implemented from the second half of 2026 through the guidelines
Scope of Monitoring	Focused on certification point-in-time	Continuous monitoring throughout the certification lifecycle	
Impact of a major security incident	Limited impact on certification status	Suspension of audit and re-evaluation of certification after government investigation	
Revocation of certification	Abstract legal basis	Explicit criteria for revocation (*) and actively enforced revocations *Examples include failure to comply with post-management obligations, failure to submit required materials, failure to remedy critical deficiencies, and occurrence of serious legal violations	
Management of incident history	Limited	Managed by KISA and used to intensify audits	
Management of companies that experienced security incidents	Same as general companies	Enhanced audits with increased personnel and duration (approx. double), focusing on root cause and remediation	Expected from 2027 through regulatory amendments

(4) Audit Quality and Oversight

Management of certification bodies and auditors will also be strengthened, bringing audit quality under direct regulatory supervision. This is designed to ensure more reliable certification outcomes, consequently increasing the accountability and liability of audit institutions.

Category	As-Is	To-Be	Implementation Timeline
Oversight of certification body	Limited evaluation and sanctions	Assessment of auditor's reliability conducted and reflected in the allocation of audit slots	Expected from 2027 through notice amendments
Audit quality management	Limited ex-post control	Annual inspections and possible revocation of designation	
Auditor expertise	Insufficient technical capability	Introduction of specialized audits (AI, cloud) and enhanced technical training	
Consistency of standards	Variability across auditors	Standardization through technical audit guidelines	Expected from 2027 through regulatory amendments

4. Implications for Compliance

With the expansion of mandatory ISMS-P certification, companies once pursuing certification on a voluntary basis are now falling under regulatory oversight. For companies subject to advanced certification, significantly higher levels of technical and administrative safeguards will be required. This is expected to necessitate not only increased investment in information security but also comprehensive restructuring of organizational frameworks, internal controls, and governance systems.

Furthermore, as audit methods become more technology-driven and shift toward on-site verification, operational security capabilities—such as vulnerability management, access control, logging, and patch management—will be directly evaluated. This marks a departure from the traditional document-based compliance approach, which may no longer be sufficient. Moreover, since security incidents can jeopardize certification status, cybersecurity risks now transcend technical issues to impact certification maintenance and overall business continuity.

Yulchon Legal Update

Ultimately, companies will need to establish continuous security management systems throughout the entire lifecycle of certification, enhance incident response capabilities, and strengthen governance structures at the executive level. In particular, given the emphasis on the substantive authority and role of CISO and CPO, information security is likely to evolve into a core component of enterprise-wide risk management, rather than remaining confined to the IT function.

Yulchon, drawing on extensive experience in advising on governance improvements, *ex-ante* regulatory compliance, ISMS-P certification, and responses to cybersecurity incidents and personal data breaches, will provide strategic support to help companies respond proactively in the evolving regulatory environment.

Related Areas

Data & Technology

Privacy & Cybersecurity

IP & Technology

Contact

Doil SON

+82-2-528-5836
dison@yulchon.com

Sun Hee KIM

+82-2-528-5838
kimsh@yulchon.com

Dayeon AHN

+82-2-528-5254
dyahn@yulchon.com

Wonseon Kiersten CHOI

+82-2-528-6758
wschoi@yulchon.com

Sanghyun PARK

+82-2-528-5578
sanghyunpark@yulchon.com



Attorneys at Law
YULCHON

Material included in our newsletter has been prepared for informational purposes only and is not offered as legal advice on any particular matter. Yulchon and contributing authors disclaim all liability for the newsletter's content and are not responsible for any third-party content which can be accessed through this newsletter.