SHIN&KIM
법무법인(유) 세종

South Korea to Overhaul ISMS/ISMS-P Certification Framework

2026.04.29

On April 10, 2026, the Ministry of Science and ICT (MSIT) and the Personal Information Protection Commission (PIPC) jointly announced sweeping reforms to the country's ISMS/ISMS-P (Information Security and Personal Information Protection Management System) certification framework. The overhaul targets a key weakness exposed by recent data breaches at certified organizations: the gap between paper compliance and actual security.

The ISMS-P certification — modeled on ISO/IEC 27001 and 27002 — evaluates whether organizations have adequate data protection management systems in place. While the existing system has produced benefits, a string of high-profile cyber incidents at certified companies have prompted regulators to rethink its foundations.

Four Pillars of the Reform

(1) Broadened Mandatory Scope & Three-Tiered Certification Framework

ISMS-P certification, previously voluntary for most organizations, will become mandatory for:

- Major public system operators;
- Identity verification service providers; and
- Large-scale personal information controllers (based on revenue and volume thresholds).

The scope of mandatory certification is expected to expand in phases beyond these initial categories.

Additionally, a uniform standard will be replaced by three distinct tiers, “enhanced,” “standard,” and “simplified,” calibrated to each organization’s public impact. Telecommunications carriers, data center operators, and similar high-impact entities will face the most stringent “enhanced” requirements. Organizations should assess their tier early, as this will determine audit intensity and compliance obligations.

(2) Site-Based Technical Assessments

The reform moves decisively away from documentation-based reviews. Assessments will now involve:

- A preliminary review to screen out entities with inadequate safeguards before the main audit begins;
  - Key criteria assessed at this stage include: (i) authority of the Chief Information Security Officer (CISO) and Chief Privacy Officer (CPO) over information security policy; (ii) identification of personal information processing assets and external internet-facing assets; (iii) password controls and encryption on personal information processing systems; and (iv) vulnerability and patch management. Entities with deficiencies must remediate before the formal certification process can proceed.
- On-site verification, real-time demonstrations, vulnerability assessments, and penetration testing.

In effect, organizations will need to demonstrate — not just document — their security capabilities.

(3) Strengthened Post-Certification Monitoring

Post-certification obligations will intensify significantly. The reform introduces an ongoing monitoring framework covering the full certification lifecycle, with standardized periodic assessments to verify that security levels are sustained. Importantly, regulators will now have clear grounds to revoke certification where material deficiencies are not remedied within prescribed timeframes.

(4) Enhanced Expertise of Certification Bodies and Auditors

The reform addresses not just what is assessed, but who is doing the assessing. Two measures target the quality and accountability of certification bodies and their auditors: (i) certification bodies will undergo post-cycle reliability assessments, with results factored into future review allocations and re-designation evaluations. Meanwhile, (ii) auditors will receive technical assessment guidelines aimed at raising the standard and consistency of on-site assessments, have their specialist expertise (e.g., AI, cloud) formally tracked, and benefit from improved working conditions, including compensation.

Key Takeaways

Voluntary → Mandatory	ISMS-P certification will become compulsory for major public system operators, identity verification providers, and large-scale personal information controllers — with scope set to expand further.
Three-Tier System	A new enhanced / standard / simplified framework replaces the one-size-fits-all model. Entities with significant public impact (e.g., telecom, data center operators) will face the most rigorous “enhanced” requirements.
Site-Based, Technical Audits	Documentation-only compliance is out. Assessments will now include on-site verification, real-time demonstrations, vulnerability testing, and penetration testing.
Ongoing Monitoring &	Post-certification oversight shifts to a continuous monitoring model. Certification

Revocation	can now be revoked for material deficiencies, meaning that compliance is a permanent obligation, not a one-time hurdle.

Implementation Timeline

H2 2026	Post-certification monitoring enhancements and revocation grounds take effect.
H1 2026 → 2027	Mandatory ISMS-P expansion, three-tier framework, and enhanced certification standards — legislated in H1 2026, targeted for full implementation in 2027

What Organizations Should Do Now

Organizations that will fall under mandatory ISMS-P certification, or that may be classified under the “enhanced” tier, should begin preparations well ahead of 2027. Key steps include:

- Assess whether mandatory certification applies and, if so, which tier;
- Conduct a gap analysis against the new site-based technical assessment criteria;
- Build internal capabilities for continuous compliance, not just audit-readiness; and
- Monitor MSIT and PIPC regulatory developments as enforcement decrees and guidelines are finalized.

About Shin & Kim’s ICT Group

Shin & Kim’s ICT Group provides comprehensive, one-stop legal services by leveraging the firm's distinctive expertise and extensive professional network in the ICT sector, having consistently earned the highest client recognition in recent years. Drawing upon our deep-seated capabilities in broadcasting, telecommunications, personal information protection, and internet IT, we deliver the highest level of legal advisory services encompassing regulatory trend analysis in broadcasting, telecommunications, and ICT; legislative improvement and legislative consulting; regulatory impact assessment; and corporate strategic planning. Furthermore, we possess extensive experience and exceptional expertise in personal information/AI compliance and risk management, providing holistic analysis and strategic responses to legal issues and regulatory risks associated with AI adoption and deployment across diverse industry sectors. Please feel free to contact us with any questions or if you require our assistance on any ICT-related legal matter.

Key Contacts

Sinook Kang
Senior Partner

+82-2-316-4059
sokang@shinkim.com

Kwang-Hee Choi
Senior Advisor

+82-2-316-4651
khchoi@shinkim.com

Jin Hong Noh
Partner

+82-2-316-1639
jhnoh@shinkim.com

Hyein Lee
Senior Foreign Attorney

+82-2-316-1641
hilee@shinkim.com

Ho Sang Yoon
Partner

+82-2-316-2584
hsyoon@shinkim.com

Kyung Min (Kenneth) Kim
Foreign Attorney

+82-2-316-1632
kmikim@shinkim.com