Korea-Information Security Management System (K-ISMS)

Microsoft Azure has achieved certification for the Korea-Information Security Management System (K-ISMS).

Microsoft and K-ISMS

Based on a rigorous evaluation by the Korea Internet & Security Agency (KISA), Microsoft Azure achieved the Korea-Information Security Management System (K-ISMS) certification to host data. The certification covers Azure services that encompass compute, storage, networking, databases, and security, and the datacenter infrastructure of the Microsoft Korea Central and Korea South regions. The specifications for K-ISMS certification are based on ISO/IEC 27001, ISO/IEC 27018, and other international standards that govern the hosting of data.

Achieving this certification means Azure customers in Korea can more easily demonstrate adherence to local legal requirements to protect key digital information assets and meet KISA compliance standards more easily. In addition, Korean organizations that have a legislated mandate to obtain their own K-ISMS certification—certain internet and information network service providers, large hospitals and schools, and so on—can more efficiently meet their own K-ISMS compliance requirements by building on the Azure certification.

The audit covered the measures Microsoft takes to secure data and protect its confidentiality including the:

- Certification of Microsoft business cloud services (with annual audits for compliance) to ISO/IEC 27001:2013 Information Security Management Standards.
- High level of privacy protection based on Microsoft compliance with the ISO/IEC 27018 Code of Practice for Protecting Personal Data in the Cloud.
- Layered approach in how Microsoft datacenters are designed, built, and operated to strictly control physical access to the areas where customer data is stored.

Microsoft in-scope cloud services

- Azure
  Learn more
- Intune

Audits, reports, and certificates

Azure certification is effective for three years from the certification date (19 November 2018) with an annual reassessment by KISA, the certifying body.

- Azure K-ISMS certification (Korean)

About K-ISMS

Under Article 47 in the "Act on Promotion of Information and Communications Network Utilization and Information Protection" (Korean and English), the Korean government introduced the Korea-Information Security Management System (K-ISMS). A country-specific ISMS framework, it defines a stringent set of control requirements designed to help ensure that organizations in Korea consistently and securely protect their information assets.

To obtain the certification, a company must undergo an assessment by an independent auditor that covers both information security management and security countermeasures. It covers 104 criteria including 12 control items in 5 sectors for information security management, and 92 control items in 13 sectors for information security countermeasures. Some of these include examination of the organization's security management responsibilities, security policies, security training, incident response, risk management, and more. A special committee examines the results of the audit and grants the certification.

March 2019

The K-ISMS framework is built on successful information security strategies and policies, as well as security counter measures and threat response procedures to minimize the impact of any security breaches. These have a significant overlap with ISO/IEC 27001 control objectives but are not identical; K-ISMS is more a detailed investigation against requirements than it is a general ISO/IEC 27001 assessment.

Under the supervision of the Korean Ministry of Science and Information Technology (MSIT) (Korean and English), the Korea Internet & Security Agency (KISA) (Korean and English) is the certifying authority of the K-ISMS. Certification is valid for three years, and certified entities must pass an annual audit to maintain it.

Frequently asked questions

Who must obtain the K-ISMS certification?

There are voluntary and compulsory subjects. Voluntary subjects, like Microsoft, apply for K-ISMS certification if they wish. However, KISA mandates certification for compulsory subjects that include:

- Internet service providers that are authorized by Article 6, Section 1 of the Telecommunication Business Act and provide information network services in Seoul and all metropolitan cities.
- Internet datacenters 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.
- Any organization that meets these conditions:
    - 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 USD$ 150 million.
    - 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 USD$ 10 million or an average of at least 1 million users per day in the previous 3 months; excluding, however, a financial company under subparagraph 3 of Article 2 of the Electronic Financial Transactions Act.

How does the integration of the K-ISMS and K-PIMS impact the Microsoft certification?

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

The integration of these two systems reflects the recent trends in the integration of information security and the protection of personal information. The goal was both to strengthen the links between these systems and to reduce the compliance burden on organizations due to the considerable overlap of requirements. Instead of 104 K-ISMS controls and 82 K-PIMS controls, the new consolidated certification will have 80 items related to information security and 22 items related to the protection of personal information.

Organizations can apply for the K-ISMS certification based on the 80 controls for information security, or they can apply for the ISMS-P by complying with the 22 additional requirements for personal information protection. Microsoft can apply for an audit under the new ISMS-P certification system; however, we will wait until our current K-ISMS certification expires in 2021, at which point we will apply for an ISMS-P audit.

Additional resources

K-ISMS-certified organizations (Korean)

K-ISMS documents and guidelines (Korean)

Azure Regions