Strengthen your cloud security

An introduction to ISO/IEC 27017 and ISO/IEC 27018 for organizations certified to ISO/IEC 27001

An Introduction

Organizations are increasingly adopting cloud services to meet the demands for enhanced security and to establish a scalable foundation that can support the anticipated surge in AI innovation.[1]

But no matter where data is stored, it can be vulnerable to a breach. IBM's 2024 'Cost of a Data Breach Report' highlighted that cloud environments are particularly vulnerable and costly when breaches occur.

Specifically, around 40% of all breaches in 2024 involved data spread across public clouds, private clouds, and on-premises systems. Public clouds, in particular, were noted for having the highest breach costs, costing USD 5.17 million on average.[2]

As an organization already certified to ISO/IEC 27001, you are well aware of the importance of maintaining a robust Information Security Management System (ISMS).

To further enhance your security posture, organizations with high dependency on cloud services should consider enhanced cloud-specific security controls beyond those listed in ISO/IEC 27001 and detailed in ISO/IEC 27002.

ISO/IEC 27017 (Information security for cloud services) and ISO/IEC 27018 (PII in public clouds) provide additional guidance and controls specifically tailored for cloud environments.

1. Foundry : Cloud Computing Study
2. Cost of a Data Breach Report 2024

Why consider ISO/IEC 27017 and/or ISO/IEC 27018?

Adopting cloud services standards can significantly strengthen your cloud security measures, ensuring that your organization remains resilient against emerging threats and compliant with stringent data protection regulations. By integrating these standards into your existing ISMS, you can achieve a higher level of security and trust in cloud services, either provided or used by your organization.

Extending your ISMS to include ISO/IEC 27017 and ISO/IEC 27018 can provide several advantages:

- Mitigate cloud-specific security risks and bolster overall information security.
- Showcase advanced security practices to clients and stakeholders, gaining a competitive edge.
- Stay ahead of evolving regulatory requirements and industry standards.
- Optimize security processes for greater efficiency.

ISO/IEC 27017 – Information Security for Cloud Services

ISO/IEC 27017 is a security standard that provides guidelines for information security controls specifically designed for cloud services, based on controls listed in ISO/IEC 27001 Annex A and detailed in ISO/IEC 27002. It aims to reduce the risk of security issues for both cloud service providers and users.

Key areas include:

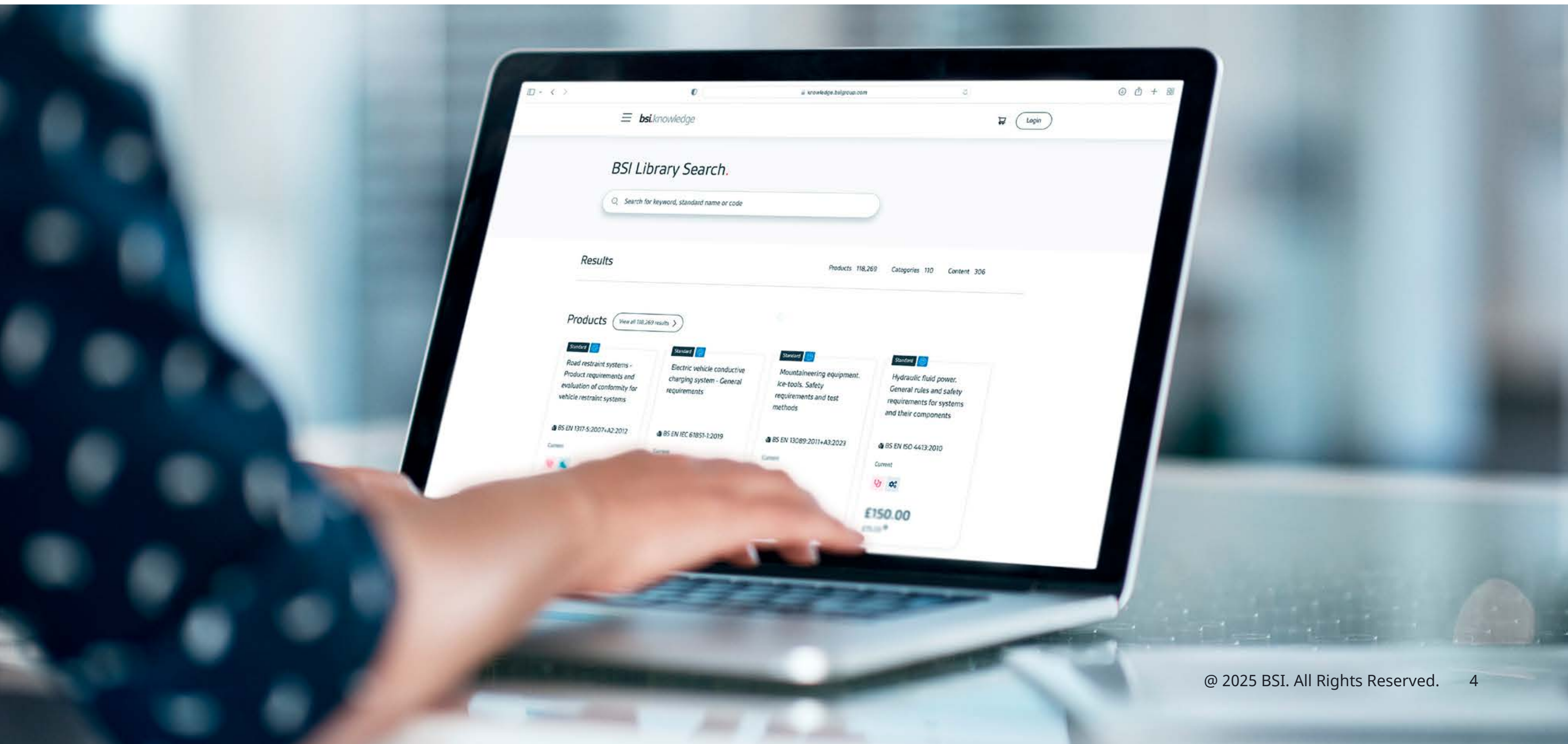
- Addresses security responsibilities between cloud service providers and customers.
- Covers risks such as data breaches, data loss, and service disruptions.
- Includes controls for data encryption, access management, and incident response.

Benefits of ISO/IEC 27017 certification:

- Protect your information assets within the cloud computing environment from cyberattacks.
- Support progress towards legal and regulatory requirements.
- Lower the risk of information security incidents.
- Save costs by reducing the need for duplicate controls.
- Strengthen your information security management system with cloud-specific security controls.
- Align your global cloud security strategy and controls with an international code of practice.

Purchase your copy of the ISO/IEC 27017 standard >

Learn more about ISO/IEC 27017 certification >



ISO/IEC 27018 – Information Technology – PII in Public Clouds

ISO/IEC 27018 is a privacy standard that provides guidelines for protecting personally identifiable information (PII) in public clouds acting as PII processors. This standard helps Cloud Service Providers to demonstrate to their users that data they hold is protected and only used for purposes explicitly consented to, while also assessing risk and implementing controls to safeguard PII.

Key areas include:

- Emphasizes consent, transparency, data minimization, and accountability in handling personal data.
- Provides guidelines for data retention, deletion, and disclosure.
- Helps meet data protection regulations, such as UK GDPR.

Benefits of ISO/IEC 27018 certification:

- Establish objectives, controls and guidelines for implementing measures to protect PII.
- Create competitive differentiation by inspiring customer trust through reliability and consistency.
- Applies to all types and sizes of organizations: public, private, government, and not-for-profit.
- Show existing and potential customers your management system is certified to the standard.
- Demonstrate that your customer data is secure in the cloud environment and will only be used with their consent.
- Give customers peace of mind and confidence in your organization.

Purchase your copy of the ISO/IEC 27018 standard >

Learn more about ISO/IEC 27018 certification >

Cloud Security Training Courses

Manage cloud security risk, from cloud control implementation and auditing techniques to defining roles and responsibilities for data. Browse our cloud security courses below:

Certificate of Cloud Security Knowledge (CCSK)

Gain the skills to identify security threats and best practices for securing the cloud. Learn how to assess, build, and secure a cloud infrastructure.

Certified Cloud Security Professional (CCSP)

Learn more about cloud computing, mobile security, application development security, risk management, cyber, and more. Gain an understanding of how to apply the 6 Domains covered in the Common Body of Knowledge in practice.

CSA Star Lead Auditor

Learn how to effectively prepare a cloud service provider for a CSA STAR audit and have sufficient knowledge and skills to conduct 1st and 2nd party audits.

Browse our full range of courses here >

Get support – Let's shape your organization's future together.

As your partner in progress, we'll help you become future ready and drive progress towards a sustainable world.

For support and more information, please contact us.

Visit **bsigroup.com**

Call **0345 086 9000**

Email **certification.sales@bsigroup.com**