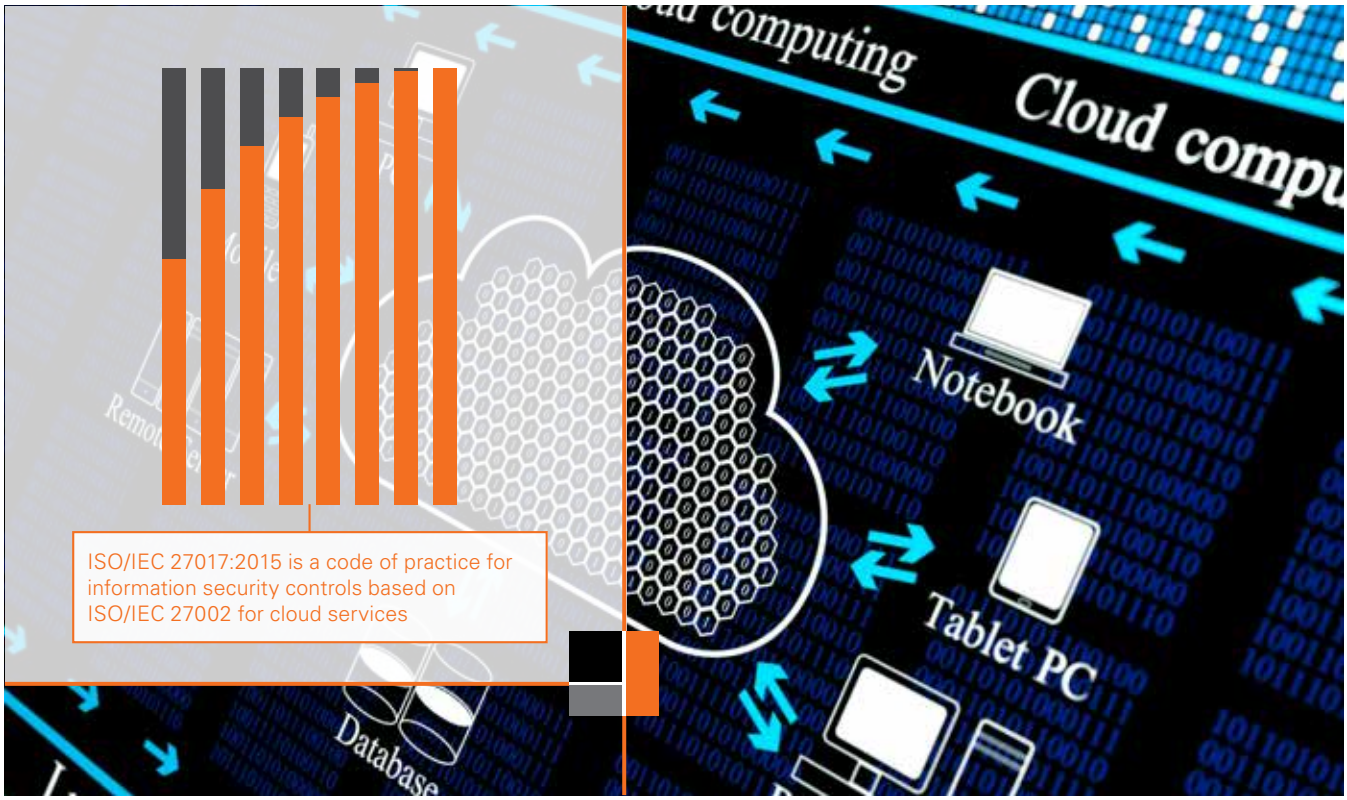

HOW CAN YOU IMPROVE INFORMATION SECURITY CONTROLS FOR DATA STORED USING CLOUD SERVICES?

ENHANCE THE SECURITY OF INFORMATION STORED USING CLOUD SERVICES WITH ISO/IEC 27017:2015 CERTIFICATION FROM SGS

INTRODUCTION

Almost every study one picks up these days forecasts cloud services proliferation. Gartner predicts the marketplace for public cloud services will grow 17.3% to USD 206 billion in 2019 from USD 175 billion in 2018 (1).

Infrastructure-as-a-Service (IaaS) will be the fastest-growing segment of the market, forecasted to grow by 27.6% in 2019 to reach $39.5B, up from $31 billion in 2018. By 2022, Gartner expects that 90% of enterprises purchasing public cloud IaaS will do so from an integrated IaaS and Platform-as-a-Service (PaaS), and will use both the IaaS and PaaS capabilities from that provider.

Applications targeted for personal and consumer level apps are predominated by cloud applications. However, the adoption of cloud services in an enterprise, government and public services environment is still not very high. According to CipherCloud's study, Compliance to Regulations (64%) and Data Security (32%) are the two biggest challenges to cloud adoption.

If a cloud service provider could provide the peace of mind and confidence to its users that its cloud services are reliable, compliant to applicable regulations and contractual requirements, and have adopted the best industrial practices, then this service provider is going to be the cloud service provider of choice. ISO/IEC 27017 and ISO/IEC 27018 are developed with these purposes in mind.

ISO/IEC 27001:2013 is an excellent standard for cloud operations, but cloud service providers wanted more sector-specific controls, to help them to pinpoint the issues specific to cloud operations. ISO/IEC 27017 and ISO/IEC 27018 were published to address these requests from the industry.

Traditional Service Level Agreements (SLA) provided by a cloud service provider focus mainly on the performance of the data centres such as servers and network availability, environmental and physical security issues, and traditional operational services such as back-up and monitoring. Cloud services have their specific concerns that are not usually addressed in service level and contractual agreements.

Typical examples of these concerns are:

1. Location of the data. Because of the cloud architecture, the data, and even the servers, are not necessarily located in a local data center
2. Ownership of data. Would the cloud service provider use the data stored in the cloud for analytics or other purposes by the service providers?
3. Removal of data. Once a cloud service is terminated, would the data stored in the cloud service be retrievable, or completely removed?
4. Service Level Agreement. Would the SLA address these issues, in addition to concerns related to availability?

The above are just some of the issues not always addressed in their contractual and service agreements. Some of these issues may even lead to breaches of local and international data privacy laws and regulations. Examples include the UK Data Protection Act (2018), the EU General Data Protection Regulation, the Hong Kong Privacy Data Protection Ordinance and the Taiwan Personal Information Protection Act.

Reference: (1) Gartner

SGS

ISO/IEC 27017 AND ISO/IEC 27018

ISO/IEC 27017 Code of practice for information security controls based on ISO/IEC 27002 for cloud services and ISO/IEC 27018 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors were developed by Joint Technical Committee ISO/IEC JTC 1 Subcommittee SC 27 – the same committee that developed the ISO 27001 standard.

ISO/IEC 27017:2015 gives guidelines for information security controls applicable to the provision and use of cloud services by providing:

- additional implementation guidance for relevant controls specified in ISO/IEC 27002;
- additional controls with implementation guidance that specifically relate to cloud services

The standard provides guidelines supporting the implementation of information security controls for cloud service customers and cloud service providers. Furthermore, a cloud service provider itself could also be a cloud service customer (for selecting downstream cloud service providers such as IaaS provider). In this case the organization would need to implement all the controls as a cloud service provider and as a cloud service customer.

ISO/IEC 27018:2019 provides commonly accepted control objectives, controls and guidelines for implementing measures to protect personally identifiable information (PII) in line with the privacy principles of ISO/IEC 29100 and the principles of personal data privacy regulations around the world. Typically, when an organization is implementing ISO/IEC 27001, it is protecting its own information. In a SaaS environment, the data belong to that of the SaaS service provider's customers, or even the customers of the service providers' customers. This increase in data protection responsibility warrants additional controls over the data. This standard provides additional controls on PII in two ways:

- Providing guidance on how certain ISO/IEC 27001 controls are implemented in a PII protection context
- Providing additional controls and associated guidance intended to address PII protection requirements not currently addressed by existing ISO/IEC 27001 controls

The second edition (ISO/IEC 27018:2019) has recently replaced the first edition (ISO/IEC 27018:2014), which constituted a minor revision. The main changes compared to the first edition included the following:

- Use of the expression "can", instead of "may" and "might"
- Adding "It is the responsibility of" under clauses 9.2.1 and 12.3.1; and
- Changes to the numbering in Annex A, to correct an earlier mistake

THE ROAD TO CERTIFICATION

ISO/IEC 27017 and ISO/IEC 27018 are not standalone management system standards and need to be assessed along with an ISO 27001 management system audit. All applicable controls in ISO/IEC 27001, ISO/IEC 27017 and/or ISO/IEC 27018 would need to be effectively implemented in order to attain successful certification.

BENEFITS OF CERTIFICATION

The benefits of implementing and certification towards ISO/IEC 27017 and ISO/IEC 27018 include:

1. Improved customer confidence. The additional controls provided by the two standards provide the extra assurance that cloud-specific technical and contractual issues are addressed and clearly stipulated
2. Enhanced governance and risk management. Certification demonstrates the organization's commitment, technical capability and confidence that applicable regulations and additional risks inherited in the cloud architecture are addressed
3. Reduced customer audits. Many customers would assert their governance to their suppliers through frequent customer audits. The certification provides proof by an independent third party that the organization's cloud operations are not only controlled but are controlled according to an internationally best practice benchmark standard

WHY SGS?

SGS is the world's largest leading inspection, verification, testing and certification company. SGS is recognized as the global benchmark for quality and integrity. With more than 94,000 employees, SGS operates a network of over 2,600 offices and laboratories around the world.

SGS has the largest pool of auditors, and the majority of them are qualified to multiple standards. This large pool of multi-skill auditors means we are capable of handling multi-standards audits simultaneously at different locations in the world, expediting the compliance assurance process and enabling worry-free project management on your side.

CONTACT US

To download your free copy of the booklet, go to www.sgs.co.uk/iso27001pitfallsbooklet.

www.sgs.co.uk/iso27001
uk.nowisthetime@sgs.com
+44 (0)1276 697715
www.sgs.com/facebook
www.sgs.com/twitter
www.sgs.com/linkedin

WHEN YOU NEED TO BE SURE

SGS