bsi.

...making excellence a habit.™

ISO/IEC 27017

Extending ISO/IEC 27001 into the Cloud

A Whitepaper

Cloud customers are concerned about security—it remains a key reason why organizations hesitate to adopt cloud services despite the flexibility and scalability the cloud can offer. A key concern focuses around the ability of cloud service providers (CSPs) to treat customer data with sufficient care and attention.

The main elements of this are the worries that data could end up in the wrong hands and what control does a customer have over careless operators. But there are other concerns too: issues such as customer identity, segregation of assets on virtual servers and what happens to assets in the event of a CSP going out of business are also issues that play on potential cloud users' minds.

The ISO 27001 series addresses some of these concerns but a new standard, ISO/IEC 27017 Information technology — Security techniques, goes further and offers more peace of mind for potential cloud customers. Typical cloud standards and technical standards that address the cloud provider controls and guidance aimed at the cloud service provider. What's unique and extremely helpful about ISO/IEC 27017 is that it provides both the CSP and cloud service customer with guidance and advice. In addition to ensuring services are safe, ISO/IEC 27017 also aims to educate customers on what they should want from their host in the cloud.

The standard provides cloud-based guidance on 37 of the controls in ISO/IEC 27002 but also features seven new controls.

- **CLD.6.3.1:** Agreement on shared or divided responsibilities between the customer and provider around information security roles associated with cloud services have to be clearly laid out, recorded and communicated.
- **CLD.8.1.5:** Addresses how assets are returned or removed from the cloud when the contract/ agreement between the customer and provider is terminated.
- **CLD.9.5.1:** The provider has to protect and separate the customer's virtual environment from other customers and external parties.
- **CLD.9.5.2:** The customer and provider must ensure virtual machines are configured and hardened to meet the needs of the organization.
- **CLD.12.1.5:** The customer's responsibility to define, document and monitor the administrative operations and procedures associated with the cloud environment and the CSP's requirement to share documentation about critical operations and procedures as and when customers require it.
- **CLD.12.4.5:** How the capabilities of the provider enable the customer to monitor activity within a cloud computing environment.
- **CLD.13.1.4:** Consistent configurations should be made so that the virtual network environment is in line with the information security policy of the physical network.

Roles and responsibilities

Ambiguity in roles and in the definition and allocation of responsibilities related to issues such as data ownership, access control, and infrastructure maintenance can give rise to business or legal disputes; especially when dealing with third parties. As the standard states:

> "Data and files on the cloud service provider's systems created or modified during the use of the cloud service, can be critical to the secure operation, recovery and continuity of the service. The ownership of all assets, and the parties who have responsibilities for operations associated with these assets, such as backup and recovery operations, should be defined and documented. Otherwise, there is a risk that the cloud service provider assumes that the cloud service customer performs these vital tasks (or vice versa), and a loss of data can occur."

Essentially, the standard requires that it's clearly laid out which party is responsible for what from the outset.

Security controls

It's not only the separation of responsibilities that the standard helps define: ISO/IEC 27017 also goes into much more detail about the type of security controls that service providers should be implementing – helping reduce the barriers to cloud adoption.

ISO/IEC 27017 offers a way for cloud service providers to indicate the level of controls that have been implemented. This means documented evidence—backed up by independent sources like certification to certain standards—show that appropriate policies have been implemented and, most importantly, what types of controls have been introduced. This information should be shared with the cloud customer before any contract is signed to help alleviate any potential issues in the future.

In cases where independent audits aren't practical or would pose a greater risk to information security , the standard does provide an option for CSPs to self-assess. When this is the case, the CSP must tell customers that they have self-assessed.

Cryptography

There's also guidance about any cryptography being used. This applies to the customer and the provider as both have responsibilities in this area. The provider should tell the customer how it's using cryptography and help customers apply protection of their own. It should also consider special cases, such as health data, where they may be some additional regulatory guidelines.

Customers should also be upfront about the type of cryptography that they're using – and they ought be using cryptography if the risk analysis suggests that it's needed. In fact, this is the sort of dispute, or misunderstanding that underpins the need for the standard. Not only should both parties assure each other that the network is being protected, they should also be able to assure each other that there's compatibility between the two systems. And, crucially, it should be determined whether these controls apply to data at rest, in transit or both, as this has caused misunderstandings before.

Customer relationship

The standard extends requirements beyond technology and also lays out guidelines for training. Many customers are happy about cloud providers' infrastructure but are wary about the level of support.

There is, after all, plenty of evidence to suggest employees are often the weak point in any organization's security measures. It's not just faulty security devices that customers need to be wary of, but rather whether staff are following all of the appropriate measures. The new standard not only sets out that providers should be supplying awareness and training for employees and contractors, but also stipulates that the training should cover regulatory requirements, customer access and specific requests.

Asset ownership

Who owns what in the cloud can be a point of confusion. The standard suggests that there be an inventory made of assets that are stored in the cloud and also refers back to the guidance information specified in ISO/IEC 27002 on the ownership, acceptable use of and return of assets. The new standard also lays out parameters for the safe disposal of customer assets so that sensitive data isn't simply dumped in virtual dustbins

Who benefits?

The simple answer is: everyone. Well everyone associated with the cloud.

The road to cloud can be paved with misunderstandings and apprehension. Any organization entrusting sensitive customer data to a third party has come to know there are grey areas where rights and responsibilities have not been clearly defined. There's a lot that's been taken on trust and that's not necessarily the best recipe for success.

CIOs and IT managers will be encouraged by the changes to their relationships with CSPs supported by the standard as they introduce a real degree of assurance to cloud computing security. Overview and implementation training around ISO/IEC 27017 may prove to be very helpful as an organization makes decisions about adopting cloud and which partners are suited to their needs.

CSPs that choose to implement ISO/IEC 27017 will also benefit by knowing they're offering a secure solution that their customers can trust, which goes a long way in building a cloud-based relationship. And, of course, by working with their customers through their adoption process ISO/IEC 27017 protects themselves from harmful accusations or law suits that may disrupt their business and damage their brand.

bsi.

Find out more
Call: 1300 730 134
Visit: bsigroup.com/en-au