A Standard for Managing Cloud Security

Using the ISO 27017 Standard

By Thomas M. Smith, CD, CISSP

December, 2017

ABSTRACT

Cloud services can pose significant risks to both a cloud service provider as well as a cloud customer. Unlike the traditional risks, each participant could isolate, contain and manage their security risks usually independent of each other. The cloud environment present challenges and often requires coordination between the customer and the provider. Once the risks are identified, controls can be established and implement that are suitable to both parties in the cloud service arrangement.

This paper sets out the enhanced security controls that are provided in the International Organization for Standardization (ISO) I 27017 Information Security Code of Practice. It is important to note that this Standard is predicated on the assumption that the customer and service provider are using or intend to use the controls as set out in ISO/IEC 27002 Standard.

Introduction

Any business should recognize that there are both risks and rewards in developing business opportunities and delivering services to clients. Certain risks are considered acceptable as long as they are adequately managed. Selecting and implement an industry recognized set of security controls is a sound approach to managing security risks, especially in the cloud environment.

Information security means the preservation of confidentiality integrity and availability of information and therefore the controls selected can be implemented as a baseline set of protective measures as well as mitigating specific or general risks.

The ISO 27017 Standard provides implementation guidance for 37 of the existing ISO 27002 controls cloud-based services. It also provides an additional 7 controls that are unique to the cloud environment.

Controls to be Changed to Satisfy the Cloud Requirements

Using the ISO/IEC 27017:2015 Standard as the guide, then following controls have unique implementation requirements for the cloud environment and would require changes from the initial 27002 control implementation to address the cloud environment:

It should be noted that some of these controls are now segregated into cloud service provider requirements and/or cloud service customer requirements which makes it easier to determine if the changes apply depending on your organization's role as being either a service provider or a customer.

Control Category	*Controls Affected*
• *Information Security Policies*	• *Policies for information security*
• *Organization of Information Security*	• *Information security roles and responsibilities* • *Contact with authorities*
• *Human Resources Security*	• *Information security awareness, education and training*
• *Asset Management*	• *Inventory of assets* • *Labelling of information*
• *Access Control*	• *Access to networks and network services* • *User registration and de-registration* • *User access provisioning* • *Management of privileged access rights* • *Management of secret authentication information of users*

- *Cryptography*
- *Physical and Environmental Security*
- *Operations Security*
- *Communications Security*
- *System Acquisition Development and Maintenance*
- *Supplier Relationships*
- *Information Security Incident Management*
- *Information Security Aspects of Business Continuity Management*
- *Compliance*

- *Information access restriction*
- *Secure log-on procedures*
- *Use of privileged utility programs*
- *Policy on the use of cryptographic controls*
- *Secure disposal or re-use of equipment*
- *Change management*
- *Capacity management*
- *Separation of development, testing and operational environments*
- *Information backup*
- *Event logging*
- *Protection of log information*
- *Clock synchronization*
- *Management of technical vulnerabilities*
- *Segregation in networks*
- *Information transfer policies and procedures*
- *Information security requirements analysis and specification*
- *Secure development policy*
- *Addressing security within supplier agreements*
- *Information and communication technology supply chain*
- *Responsibilities and procedures*
- *Reporting information security events*
- *Collection of evidence*
- *No changes*
- *Identification of applicable legislation and contractual requirements*
- *Intellectual property rights*
- *Protection of records*
- *Regulation of cryptographic controls*
- *Independent review of information security*

New Cloud Controls to be Implemented

There are seven new controls incorporated into an extended control set that must be implemented to satisfy the requirements of ISO 27017, depending on whether you are are the cloud customer or the cloud service provider:

New Control		*Applies To*
CLD 6.3.1	*Shared roles and responsibilities within a cloud computing environment*	*Cloud service customer; and the Cloud service provider*
CLD 8.1.5	*Removal of cloud service customer assets*	*Cloud service customer; and the Cloud service provider*
CLD 9.5.1	*Segregation in virtual computing environments*	*Cloud service provider only*
CLD 9.5.2	*Virtual machine hardening*	*Cloud service customer; and the Cloud service provider*
CLD 12.1.5	*Administrator's operational security*	*Cloud service customer; and the Cloud service provider*
CLD 12.4.5	*Monitoring of Cloud Services*	*Cloud service customer; and the Cloud service provider*
CLD 13.1.4	*Alignment of security management for virtual and physical networks*	*Cloud service provider only*

It is very important to bring additional attention to the roles and responsibilities that are allocated to the service provider and the service customer.

Summary

The division of responsibilities and the implementation of the additional controls are an excellent approach to resolving security controls management and expectations. Organizations would do well to document its own roles and responsibilities. A cloud service provider would be well served by also documented its roles and responsibilities as well as informing customers of their responsibilities.

From a cloud service provider perspective, implementing the controls as provided in the Standard can improve adoption of cloud services and mitigate legal and other issues that traditionally may arise between the parties involved in the service.

Bibliography

BSI, Extending ISO/IEC 27001 into the Cloud

ISO, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services, ISO/IEC 27017:2015

ISO, Information technology — Security techniques — Information security management systems — Requirements

NIST, The NIST Definition of Cloud Computing, Special Publication 800-145

NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February 12, 2014.