Managing New Information Security Boundaries as a Cloud Service Provider

Practical ISMS principles to implement ISO 27001

Author:

Rahul Jayachandran,
Practice Manager- Consulting,
Paladion Networks

PALADION
HIGH SPEED CYBER DEFENSE

Introduction

Cloud service providers now handle massive amounts of data – not only for themselves, but also on behalf of numerous other enterprises and organizations. Information security takes on an extra dimension as logically separate customers share the same physical resources.

This poses a dual challenge for each cloud service provider (CSP). The CSP must define a security boundary that shows which security actions and functions are undertaken by the provider, and which ones are the duty of the customer. It must also manage the additional security aspects of cloud computing multitenancy, because a security risk for one customer can affect another customer in the same cloud.

This white paper gives an overview of these cloud computing security issues, emphasizing those that concern cloud service providers. It outlines in practical steps an approach to achieve certifiable security as a CSP.

> "Cloud computing multitenancy means a security risk for one customer can affect another customer in the same cloud."

How the Cloud is Redefining Data Boundaries and Security Risks

Enterprises and users in general often take the cloud to be a natural extension of their individual computing environments. However, they do not always realize that traditional information boundaries disappear at the same time and that the nature of security precautions must change as a consequence.

At the same time, the convergence of all their data into a single cloud infrastructure also creates an attractive target for criminals. Security risk can affect customer information, personally identifiable information (PII), medical information, credit card information, bank account information, and more.

That risk must be properly managed, whether the confidential information concerned is stored in the cloud, in use, or in transit. An information security management system (ISMS) is a systematic approach designed to manage such risk, keeping confidential information secure, and proactively containing the impact of a possible security breach. The process involves people and processes, as well as IT systems.

"In the cloud, traditional information boundaries disappear and security precautions must therefore change."

Major Security Challenges in the Cloud Environment

Certain dimensions of an information security management system (ISMS) apply to all. The "CIA" formula of information security – confidentiality, integrity, availability – remains a goal, whatever the location or destination of sensitive data:

- Confidentiality. Data considered as confidential is protected against unauthorized exposure or accidental leakage.
- Integrity. Data processed by a system gives a complete, accurate, authorized, complete, timely, and valid result.
- Availability. The data remains available for authorized consultation and processing, possibly according to an agreed service level agreement (SLA).

These fundamental principles of information security already illustrate a key principle: while security must offer adequate protection of data, it must not unduly interfere with operations and productivity.

"Security must protect data, but it must not interfere with operations and productivity."

The extra dimension that a cloud service provider must manage is other people's data. A CSP is in the delicate position of also securing the data of its customers, both with respect to the exterior and between the customers themselves. This gives rise to additional challenges:

- Risk of CSP insider attack on confidential customer data, due to insufficient background checks on CSP employees.
- Lack of proper data isolation and logical storage segregation of multiple customers, leading to data leaks and exfiltration.
- Compromise of virtualization layers and software, through which attackers might modify identities and outputs of virtual machines.
- Inadequate compliance with data privacy regulations, putting entities at risk of fines and reputational damage, whether or not a data breach occurs.

A Continual Management Process

Both the cloud service provider and the customer must handle their part of information security as a continual process. In particular, the establishment and continual updating of an ISMS by a cloud service provider offers an assurance for its customers that CSP security is being managed systematically. Good management is as important as robust technology. Customers benefit from enhanced business continuity, as well as reduction of potential damage or loss. Using a suitable ISMS, a CSP can position these benefits as part of its value proposition to its customers.

A CSP that demonstrably reviews information security and analyzes risk in order to enhance policies, procedures, and contingency planning can not only look good to its customers, but also inspire them to similar behavior for their role in their own security. Conversely, organizations already functioning with strict information security policies, for instance in financial, health, telecoms, and government sectors, will more readily consider a cloud provider that can prove it has implemented a high quality information security management system.

"Organizations more readily consider a cloud provider with a high quality ISMS"

Division of Information Security Responsibilities

While a cloud service provider offers privacy and protection for its customers in its provider's infrastructure, it is not responsible for other customer-initiated actions. For instance, a cloud provider may offer assurances that a customer's application will run as designed (notwithstanding any security aspects concerning other customers). However, the provider is not responsible for the design itself of the customer's application.

A customer remains responsible if it has developed or configured an application with security holes that can be exploited by attackers connecting over the web. Likewise, the customer remains responsible for connections it makes or authorizes to those applications running in the CSP's infrastructure.

While some organizations may see an overall improvement in their security posture through using a cloud service provider with good infrastructure security, a part of information security management will always remain the responsibility of the customer. An effective approach to an information security management system must take account of this duality.

The Paladion Approach to Cloud Security

Paladion helps organizations and cloud service providers in particular to address cloud information security, through the architecture and functionality of Paladion's ISMS solution. The solution provides a solid platform for a CSP to plan, implement, and evolve a consistent set of policies, processes, and systems to minimize risk in its CSP infrastructure. This in turn allows it to fulfill its responsibilities to its customers in their use of that infrastructure.

The Paladion ISMS solution is designed to remain effective and efficient for all time horizons, whether near or far, through:

- Clear thinking and continuing evaluation of the information security needs of cloud service providers and their customers.
- Update mechanisms for CSPs to keep up with changes, however rapid, in infrastructure technology, allowing CSPs to manage threats of which they may not even have been previously aware.
- Continual security evaluation as CSP internal organization and customer requirements change.
- Mutual information security benefits for CSPs and the individual customers they serve. Care is taken to avoid information security enhancements made in one area or for one customer adversely affecting another.

Paladion's methodology to ensure security in the cloud environment is also based on relevant international standards and best practices:

- ISO / IEC 27001:2013. The ISO 27001 standard applies to all organizations (CSPs and their customers) seeking to protect their information. It provides the framework for managing security and is certifiable by independent, recognized certifying bodies.
- ISO / IEC 27017:2015. Also applicable to cloud service providers and their customers, ISO 27017 defines security in cloud computing.
- ISO / IEC 27018:2014. Applicable only to cloud providers, ISO 27018 defines the protection of personal data handled by a cloud service provider on behalf of others.
- CSA Cloud Control Matrix. A set of controls for assessing cloud-centric information security risks, drawing from industry reference sources such as ISO 27001/2, ENISA (European Union Agency for Network and Information Security), ISACA (previously known as the Information Systems Audit and Control Association), AICPA (American Institute of Certified Public Accountants), and FedRAMP (see below).

- FedRAMP. The Federal Risk and Authorization Management Program is a US government-wide mandated program offering a standardized approach to security evaluation, authorization, and monitoring for cloud products and services.

Via Paladion's services, a cloud service provider can achieve certification against the ISO 27001:2013 standard, leading to automatic compliance with other international standards such as ISO 27017 and ISO 27018.

"Paladion's cloud security methodology is based on international standards and best practices."

Acceleration of the Information Security Implementation Process

An effective approach to accelerating the implementation of information security includes the following:

- A single, collaborative web-based solution to establish and federate the entire information security management system for ISO 27001 / ISO 27018 certification, and to demonstrate compliance to management and auditors.

- A ready-to-use knowledge repository for the possible threats, vulnerabilities, and security controls for the cloud environment, simplifying risk assessment and risk treatment.

- Automation of the implementation process to bring together information asset, security, and compliance representatives, while avoiding the errors of manual approaches.

- Automation of ISO 27001 compliance activities such as asset management, risk management, internal audit, management review, document management, effectiveness metrics management, reports and analysis.

- Customizability for different information security awareness needs for cloud providers compared to cloud consumers, for instance, through built-in security awareness contents for both providers and consumers.

- The means (audit checklist, tool) for cloud service providers and consumers to regularly monitor the compliance in regards to standard or best practice

- Real time monitoring of information security management activities with centralized dashboard, reporting and trending features.

- End-to-end IS audit management with ready-to-use audit checklists, evidence management and non-compliance tracking.

Paladion's solution RisqVu GRC offers these features, speeding and simplifying the demonstration of information security compliance by CSPs to customers, auditors, and management. Paladion helps CSPs gain and maintain the requisite knowledge and expertise to keep an effective, dynamic ISMS operational.

Paladion's Step by Step ISMS Implementation Guide

- Customizability for different information security awareness needs for cloud providers compared to cloud consumers, for instance, through built-in security awareness contents for both providers and consumers.

Coverage: All requirements of ISO 27001, ISO 27017, ISO 27018 and CSA CCM

- The means (audit checklist, tool) for cloud service providers and consumers to regularly monitor the compliance in regards to standard or best practice

Coverage: ISO 27001, ISO 27017 and ISO 27018

- Real time monitoring of information security management activities with centralized dashboard, reporting and trending features.

Coverage: ISO 27001and ISO 27017

PALADION

- Develop the asset inventory to document all the information assets in the cloud with correct stakeholder / customer information.

  Coverage: ISO 27001, ISO 27017 and ISO 27018

- Develop a risk management framework for the cloud service provider to ensure security of the cloud assets and the PII information on the cloud.

  Coverage: ISO 27001, ISO 27017 and ISO 27018

- Identify high risk environments and data flows from the cloud network architecture to ensure they have the required mitigation controls and also identify the applicable legal compliance impacts.

  Coverage: ISO 27001and CSA CCM

- Develop or update the ISMS framework for the cloud environment with required set of policies and procedures to be followed by both the service provider and service customer.

  Coverage: ISO 27001and ISO 27017

- Define the required set of policies to ensure the protection of personal information stored and processed in the cloud environment.

  Coverage: ISO 27001 and ISO 27018

- Provide a separate information security awareness session for the cloud service provider personnel and the cloud service customer to educate on the do's and don'ts of security while accessing the information from and to the cloud environment

  Coverage: ISO 27001, ISO 27017 and ISO 27018

- Implement security best practices in the cloud environment which includes segregation of virtual computing environment, virtual machine hardening, aligning the security management for virtual and physical network, and monitoring of the cloud services.

  Coverage: ISO 27001, ISO 27017, ISO 27018, CSA CCM

- Implement PII security controls in the cloud environment for access to and authorization of PII data, disclosure of PII data and erasure of temporary files, security of PII data logs, etc.

  Coverage: ISO 27001, ISO 27018

- Conduct a pre-certification audit to ensure the completeness and effectiveness of the security implementation and to verify whether the implementation complies with standard recommendations.

Coverage: ISO 27001, ISO 27017 and ISO 27018

- Readiness for the certification should be ensured as an output of the pre-certification audit.

Coverage: ISO 27001 and ISO 27018

- Paladion will assist in the external certification by providing the required documents and evidences for the auditor and thereby successful completion of the certification audit.

Coverage: ISO 27001, ISO 27017 and ISO 27018

- Paladion's ISMS service will ensure that the organization is certified against the international standard and also receives the statement of confirmation of the security best practices followed for cloud security.

Coverage: ISO 27001, ISO 27017 and ISO 27018

"Paladion helps CSPs gain and maintain an effective, dynamic ISMS."

Conclusion

To manage information security effectively, cloud service providers must understand how the cloud and multitenancy change the information security landscape. The extra dimension of customers' data brings additional challenges. However, a CSP with the right information security management system can not only meet these challenges, but also increase the perceived value of its services to its customers. Paladion's ISMS solution offers a robust, affordable, high-quality, standards-based platform to help both CSPs and their customers simplify and optimize information security, with a clear roadmap to implementation, certification to international standards, and continuing compliance and protection.

"Paladion's ISMS solution helps CSPs and their customers simplify and optimize information security for continuing compliance and protection."

PALADION
HIGH SPEED CYBER DEFENSE

ABOUT PALADION

Paladion is a global cyber defense company that provides Managed Detection and Response Services, DevOps Security, Cyber Forensics, Incident Response, and more by tightly bundling its semi-autonomous cyber platform and managed services with leading security technologies. Paladion is consistently rated and recognized by independent analyst firms and awarded by CRN, Asian Banker, Red Herring, amongst others.

For 17 years, Paladion has been actively managing cyber risk for over 700 customers from its six cyber operations centers placed across the globe. It houses 900+ cyber security professionals including security researchers, threat hunters, ethical hackers, incident responders, solution architects, consultants and more. Paladion is also actively involved in several information security research forums such as OWASP, and has authored several books on security monitoring, application security, and more.

WW Headquarters: 11480 Commerce Park Drive, Suite 210, Reston, VA 20191 USA. Ph: +1-844-507-7668

Bangalore: +91-80-42543444, Mumbai: +91-2233655151, Delhi: +91-9910301180, London: +44(0)2071487475, Dubai: +971-4-2595526, Sharjah: +971-50-8344863, Doha: +97433559018, Riyadh: +966(0)114725163, Muscat: +968 99383575, Kuala Lumpur: +60-3-7660-4988, Bangkok: +66 23093650-51, Jalan Kedoya Raya: +62-8111664399.

sales@paladion.net | www.paladion.net