AUTOMATED COMPLIANCE SYSTEM FOR SERVICE ORGANIZATIONS

Meiran Galis[1]*,
Tomislav Unkašević[2],
Zoran Banjac[2],
Milan Milosavljević[2]

[1]Singidunum University,
Belgrade, Serbia

[2]Vlatacom Institute,
Belgrade, Serbia

Abstract:

Cloud-based applications are becoming an increasingly important component for many enterprises. For customers' data to remain confidential and secure, service organizations must adhere to security and privacy best practices, applicable laws, and regulations. There has been some effort to develop uniform standards for cloud security, but most service organizations need to apply with a combination of security and privacy regulations and standards. For early-stage technology companies, this mission can be even more challenging since they are oriented towards product development and have limited resources to invest in the compliance of security, availability, confidentiality, integrity, and privacy.

These risks have led to uncertainty among Software-as-a-Service ('SaaS' customers about what measures they should require from their IT vendors and whether those measures will be in line with their policies and commitments to their customers. The rapidly evolving cloud utilization of corporations migrated to the cloud, or new technology companies (start-ups) has led to a security audit examination report. The report developed from the accounting audit, based on global accounting audit methodology and the COSO framework examined by technology auditors.

This paper integrated a study case of a Service Organization's security audit in the field of financial payment.

An automated compliance system has been proposed that could assist both Service Organizations and Service Auditors to ease the audit process and make it more efficient and effective, compromise lack of expertise, save employees' time, decrease human errors, and eliminate non-compliance issues by automation, integrations, machine learning, and pre-designed workflows.

Keywords:

Cloud computing, information security, IT audit, compliance, ISMS.

INTRODUCTION

1.1. CLOUD STRUCTURE AND SERVICES THAT CLOUD PROVIDES

Cloud computing is an application-based software infrastructure that stores, process and manage data on a remote server (data centre), which can be accessed through the Internet to the backend by the Cloud Provider or the application by the end-user client that uses the results.

Correspondence:
Meiran Galis

e-mail:
meiran.galis@gmail.com

DOI: 10.15308/Sinteza-2021-21-27

Cloud providers offer a broad set of global cloud-based products, including computing power, databases, storage, networking, analytics, management tools, and more.

In a cloud computing architecture, objects are organized into the components and subcomponents that form cloud computing. These include a client-side platform, a server-side platform, a cloud-based delivery mechanism, and a network.

Consequently, the cloud computing architecture consists of these components.

1.2. SERVICES THAT THE SERVICE ORGANIZATIONS OFFERS TO END-USERS

The software-as-a-service model allows applications to be delivered via the Internet. The software can be accessed via the Internet instead of being installed and maintained, freeing organizations from complex software and hardware management. Almost every industry can benefit from SaaS implementation. Service Organizations provide a variety of services, including:

- Managed Security: Security Information and Event Management (SIEM), anti-malware, network configuration scanning, source code vulnerability analysis, Identity, access management, and incident management.
- Organizational Systems: recruitment human resource management, change management system, vendor risk management, customer relationship management, and sales analysis.
- Financial services: transaction processing, payment processing, purchasing, peer lending, payroll management, financial compliance, VAT reclaim, Tax refund, and Insurance on-demand.
- Healthcare: remote diagnosis, medical surgery video analysis, visual aid, blood diagnostics, and more.

1.3. DEFINED SECURITY REQUIREMENTS

Management remains responsible for risk arising from Service Organizations to regulators, boards of directors, shareholders, and customers. A service organization's internal environment is controlled by its management, responsible for setting the controls.

For assessment, prioritization, administration, and mitigation of the risks associated with service organization systems and processes, enterprises request information periodically on the design, operation, and effectiveness of controls across the platform.

To strengthen their risk assessment procedure, companies may request Service Organization to comply with specific standards based on their geographic location, industry, technology, and internal policy.

For example, while European enterprises request compliance with ISO/IEC 27001 framework, United States enterprises request compliance with the AICPA SOC 2 framework. Therefore, the security requirements are subjected to the framework the company has been asked to comply with by their customers.

1.4. DEFINED SYSTEM MODEL CLOUD PROVIDER – END-USER

Companies of all sizes, types, geographies and industries use cloud services for various use cases, including customer-centric web applications, disaster recovery, backups, virtual desktops, software development, testing, and big data analytics. Service locations, data centers, or hardware platforms and the operating systems on which applications do not matter much to end-users.

The main advantages of cloud computing are (1) agility, (2) resilience, (3) reliability, and (4) fault tolerance. There are three methods of cloud computing [1]:

1. Infrastructure as a Service (IaaS) - virtual hardware resources which provide access to computers (physically or virtual machines), network capabilities, and storage space. This is managed by the Cloud Provider, including secure design, physical access, surveillance and detection, monitoring and logging, infrastructure maintenance, device management, business continuity, and disaster recovery;
2. Platform as a Service (PaaS) – Procurement of IT resources, software maintenance, capacity planning, OS patch management. It allows Service Organization not to have to manage basic infrastructure and focus on application management. They provide customers with services built on their infrastructure;
3. Software as a Service (SaaS) – A complete cloud-based product or platform maintained, managed, and operated by a Service Organization, also called 'end-user application.' It allows the end-user (customer) to focus on its core services and outsource supportive or internal IT applications.

Compliance and security are the joint responsibility of the Cloud Provider and the Service Organization. The Cloud Provider manages the elements and addresses

them from the Physical Security of the objects (i.e., data center) to the host operating system and virtualization layer in which the service operates. The nature of the shared responsibility also gives Service Organizations increased control and flexibility over their assets. This division of duties can be considered the security of the cloud (Cloud Provider) instead of the security in the cloud (Service Organization).

2. SECURITY OF THE MODEL

The risks and threats for the global IT enterprise environment are dynamically and constantly evolving, as threat actors discover new vulnerabilities and advanced methods of exploiting them. There is no need to set up a large office, expensive equipment, and qualified staff. All required is a computer, Internet connection, and time devoted to learning cyber hacking techniques. The threat actor can act from any country globally and can compromise any enterprise in any country. State-sponsored actors are highly knowledgeable, have access to sophisticated resources, and are heavily funded. Other threat actors are activist groups that generally do not want to steal money or trade secrets but want to expose the observed "wrongdoings" of large enterprises or promote their reputation. The internal threat actor is another threat that needs to be considered; these are disloyal, frustrated, or negligent employees that can use their access privileges and position for fraud, scams, or stealing of confidential information. As risk is defined as a vulnerability meeting threat [2], enterprises should identify risks and reduce them to an acceptable level.

Service Organizations have to deal with these threats by defining the organization and regulations they need to comply with, performing baseline assessments based on a chosen security framework, identifying gaps, assigning organizational responsibilities and timelines to monitor and remediate internal control, and leveraging external audits incorporate change management triggers.

2.1. INFORMATION SECURITY STRATEGY

Information security strategy requires a top-down approach, management commitment, and a direct link to the business goals [3]. For protection to be adequate, it must deal with complete administrative, operational, and technical controls related to people, procedures, technology, and data. To ensure proper governance, a set of organizational standards should be developed to provide accepted defined limits for the minimum-security baseline required for different aspects.

Strategy implementation must be implemented through an Information Security program that includes approved policies and standards by stakeholders. In short, the information protection program must consist of elements such as:

- Assignment of roles and responsibilities;
- Periodic risk assessments and impact analysis;
- Information assets must be identified and classified; controls must be appropriate, efficient, and adequate;
- Integrate security into all processes in the organization;
- Monitor security elements;
- Access management methods that ensure proper authentication of identities and access permissions for information users;
- Meaningful metrics;
- Instructions on information security obligations for all employees, including management and board members;
- Training for the functioning of security processes, as needed;
- Develop and test business continuity plans for outages or disasters.

The basic information security program will utilize a combination of technological, procedural, and administrative controls (e.g., Physical Security, Environmental Security) to protect information assets, background checks, onboarding / offboarding employee, identity access management, IDS / IPS, firewall, cryptography, anti-virus, penetration test, vulnerability scan) as well as automated and manual controls. In addition, these controls should specify a reduction of potential consequences to an acceptable level set and approved by senior management that addresses both vulnerabilities and threats.

2.2. MUTUAL RESPONSIBILITY

Traditionally, enterprises were responsible for all aspects of security, including applications, physical servers, user controls, and physical perimeter security. The Cloud Service Provider (CSP) offers relief to Service Organizations by taking on a portion of many operational duties, including security. The shared responsibility model [4] clearly defines ownership of protection

between the Cloud Provider and Service Organization; each retains complete ownership over assets, processes, and functions. Service Organizations can secure their environments more easily by collaborating with a CSP and sharing security responsibilities. The responsibility for cloud security, data protection, and privacy lies with both customers and cloud service providers.

Responsibility	On-Premises	SaaS	PaaS	IaaS
Data Governance	C	C	C	C
Endpoint Protection	C	C	C	C
User Access Management	C	C	C	C
Identity Infrastructure	C	C	CSP C	C
Application	C	CSP	C	C
Network Control	C	CSP	C	C
OS Security	C	CSP	CSP	C
Host	C	CSP	CSP	CSP
Network	C	CSP	CSP	CSP
Data Centre	C	CSP	CSP	CSP

Table 1 - Mapping responsibility for data security requirements to cloud service models
C= Client; CSP = Cloud Service Provider

2.3. SECURITY STANDARDS

Defines requirements for the formulation, implementation, management, and improvement of the information security management system (ISMS) [5]. The objective of a standard is to assist companies in Securing their information resources and keeping risk low. Enterprises that meet the requirements of a standard may decide to be certified by a certification body (depending on the standard and industry) upon completing an audit performed by a certified auditor of an approved certification body.

There are dozens of comprehensive security standards available, and enterprises choose those that work for their business needs based on customers' requests, laws, and regulations, creating a competitive edge or the strategic security decision of the management. A few well-known security standards are the following:

- ISO/IEC 27001 - an international standard that deals with the management of information security management systems. A joint effort by ISO and IEC was responsible for the publication of the standard [6];
- NIST - The National Institute of Standards and Technology [7] in the USA formed several frameworks, including SP 800-53 and the Cybersecurity framework. Despite being a federal law, it is also widely applied in state and local governments and private organizations. Federal and state government agencies must follow it. Many private organizations, too, use NIST SP 800-53 as their security controls framework.
- Cloud Security Alliance (CSA)- The CSA [8] is a global organization working to identify and improve cloud security standards. Through its educational programs, research, events, and products, the CSA leverage the subject matter expertise of industry professionals, associations, governments, companies, and individual members to deliver cloud security-specific information. A cloud control framework was developed by the CSA, known as the Cloud Controls Matrix.
- SOC 2 Type II - Formed by the American Institute for Certified Public Accountants (AICPA) and utilizing the COSO framework [9], a Service Organization Control (SOC) 2 is an internal control examination of the outsourcing of services performed by an organization. SOC 2 provides valuable information that can be used to assess the risks associated with outsourced services. This audit function inspects the system regarding security, availability, confidentiality, processing integrity, and privacy.

3. IMPLEMENTATION

The SOC 2 Type II examination is used to assess the effectiveness of controls in a service organization. The controls are designed and mapped based on the AICPA COSO framework by the Service Organization. The Trust Service Principles (TSP) is divided into five principles: Security, availability, confidentiality, processing integrity, and privacy. When assessing the design and operational effectiveness by at least one of the principals, the TSP Service Organization may be used.

An organization's internal control system may be at risk for failure because of the following factors:

1. Identify the nature of the enterprise's activities;
2. A company's operating environment;
3. Information that the enterprise generates uses, and stores;

4. Contracts signed between an organization and its customers and third parties;
5. Responsibilities related to the management and maintenance of enterprise systems and processes;
6. Technology, connection methods, and delivery channels used to serve customers;
7. Service Organizations can utilize third-party resources that have access to the Service Network and data to provide elements to the Service Network;
8. Changes from the following: system operations, data processing, management governance, supported by the functions, regulatory and legal requirements that Service Organizations should adhere to;
9. Introduction of new services, products, or technologies.

Service Organizations address these risks by implementing control mechanisms that, if effective, give reasonable assurance of the attainment of the objectives. For each TSC, the framework also presents areas of focus based on experience and judgment to be utilized in real-world situations.

A key component of COSO's Internal Control-Integrated Framework is the emphasis placed on the points of focus that are intended to represent important aspects of the criteria.

A Service Organization's management can use these focus areas to design, implement, and operate controls for security, availability, confidentiality, processing integrity, and privacy.

Additionally, management and auditors can use the focus points to determine whether the controls are adequate in design and operation to achieve the Service Organization's control objectives.

3.1. DESCRIPTION

The Case study focuses on SOC 2 Type II examinations. A Service Organization's effectiveness of the design and operating of controls contained in its management's system description document relative to security, availability, and confidentiality during a given period for achieving its goals based on the criteria in a SOC 2 Type II. A SOC 2 Type II engagement includes an auditor's opinion about the design and operating effectiveness of controls implemented in Service Organizations. These documents also provide detailed information on the audited systems and controls and the results of those tests. An organization's software, procedures, and data are created, implemented, and managed by employees to achieve company goals and meeting management's specific needs.

System segments can be classified into five categories:

1. Infrastructure - IT environment that consists of physical and virtual resources managed by Service Organization to provide services. The physical environment, related structures, information technology, and hardware are all considered.
2. Software - Applications supporting the operating systems, middleware, and utilities of the infrastructure; Databases used, external-facing web-based applications, and proprietary applications;
3. People - Personnel who organize, provide guidance, develop, operate, secure, and use a system;
4. Data - The data types used by the system, including transaction streams, files, databases, tables, and anything else the system produced or processed;
5. Procedures - Procedures for providing services, including appropriate procedures for initiating, authorizing, performing, delivering, and preparing reports and other information.

3.2. CASE STUDY

The case study is based on an insurance platform that provides rating, quoting, binding, policy issuance, premium billing, and reporting. Since the industry in which the company operates is heavily regulated. Since the company offers insurance and fixed insurance platforms for insurance agencies in the US, some customers require them to show substantial compliance with global security standards.

Companies are required to comply with different regulations, laws, and standards. This requirement is based on several factors, including geographical location, industry-oriented standard (i.e., healthcare, payments, Etc.), data stored & processed, service commitments to customers, and management decisions. First, a company will need to identify with which regulations and laws it needs to comply. For example, if a company controls or processes the personally identifiable information ('PII') of EU citizens, the company needs to comply with the GDPR. On another example, if a company wishes to have business activities in the United States, there is a high probability that its prospective customer will condition their contract according to the SOC2

Type II examination. Some countries' regulations refer to security goals, while others specify detailed implementations in their regulations. Some nations simply establish security goals, while others require risk management [10]—the combination of all the above supporting the decisions with the compliance strategy.

Therefore, compliance with the regulatory framework is based on the sole judge on the board of directors and based on local and international regulations, global standards requested from customers, including industry-oriented certifications/audits and contractual commitments.

The selected Service Auditor was EY, who examined the accompanying description of the assurance Service Organization's platform according to the COSO criteria for describing the service organization system for Security, Availability, and Confidentiality and by the EY Audit methodology [11].

Under this requirement, the Auditor's plan and audit must achieve reasonable assurance about whether (1) the description was presented according to the criteria to describe the official organization, and (2) the controls described effectively met the applicable TSCs during the audit period. This technical judgment is based upon several factors, such as the likelihood of material misstatements or fraud and the quality, timing, and extent of the methods selected. The Auditor believed the evidence he collected was sufficient and appropriate to make a positive conclusion on the attestation.

In the Readiness Assessment process, system components were categorized into five categories: Hardware, Software, People, Procedure, and Data.

In the audit attestation process, the entity provided information to determine whether its controls were adequate. Auditors developed controls testing plans, timing, and scope based on the characteristics of control environments and sufficient tests.

4. CONCLUSION

The thesis suggests a novel approach that supports the development of automated, utilizing artificial intelligence, robotic process automation, and integrations.

A holistic methodology will oversee a range of administrative, procedural, and technical controls and provide continuous monitoring of the effectiveness of the controls.

Further developments in the context of information security and compliance audits will be seen soon. The current state of information security audits is managed periodically and population-based on samples, while it will transform for extensive data analysis of all tested cases.

The automated compliance solution will generate policies and procedures based on several gap analysis questionnaires assign to the relevant business unit owner to build a customized control list based on the COSO framework used by the AICPA. Integrations with suitable organizational systems will scan the environment to validate if gaps were remediated.

Once the controls were designed and implemented in the organization, the automated compliance system will continuously monitor those controls and trigger alerts, tasks, and user reports on issues that arise in non-compliance. These issues will be seen and addressed promptly, supporting governance information security management, laws and regulations, and audit programs of the organization.

The system will automatically aggregate the appropriate evidence to a dedicated dashboard mapped to the relevant control objectives, test procedure, and framework. Alerts will be sent directly to the organization's alerting tool upon system identification. This functionality will reduce the time spent gathering evidence for external audits and is used as a communication tool for cooperation between the Service Organization's internal stakeholders and the Service Organization and external Service Auditor.

REFERENCES

[1] Communications of the ACM, "A vire of Cloud Computing," *The ACM Digital Library*, vol. 53, no. 4, pp. 50-58, 2010.

[2] McGraw-Hill Education, "CISSP," vol. 8, pp. 41-60, 2019.

[3] ISACA, "CISM Review Manual," vol. 15th Edition, 2016.

[4] A. S. O. A. Michael Lane, "Managing the Risks of Data Security and Privacy in the Cloud: A Shared Responsibility between the Cloud Service Provider and the Client Organisation," *The Bright Internet Global Summit,* 2017.

[5] ISACA, "An Introduction to the Business Model for Information Security," 2009.

[6] "Information technology — Security techniques — Information security management systems — Requirements," *ISO/IEC 27001:2013*, vol. II, pp. 4-22, 2013.

[7] National Institute of Standards and Technology, "Security and Privacy Controls for Federal Information Systems and Organizations," *NIST Special Publication 800-53*, vol. 5, 2020.

[8] Cloud Security Alliance, "The Notorious Nine Cloud Computing Top Threats," *CSA*, vol. 1, pp. 6-21, 2013.

[9] AICPA, "TSP Section 100," *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, pp. 4-12, 2020.

[10] Joseph Johnson, Susan J. Lincke, Ralf Imhof and Charles Lim, "A Comparison of International Information Security Regulations," *Interdisciplinary Journal of Information, Knowledge, and Management*, vol. 9, pp. 89-116, 2014.

[11] EY, "Audit Quality: A Globally Sustainable Approach," vol. I, pp. 10-31, 2017.