Module 02 Course Project – Trust Service Principles and Security Controls

John Doe, Student

Rasmussen College

Author Note

This assignment is being submitted on July 12, 2019, for Clifton Krahenbill’s CIS3240C Section 01 Security Controls.

# Security Control Compliance

Security and compliance require the proper balance, to provide an organization with effective safeguards, against threats. These dangers can come from internal or external sources. Reliable security focuses on the attributes of protecting a company. Audits or risk assessments are methods for enforcing compliance (Armor Defense, 2019). The concept of security control compliance incorporates countermeasures, which mitigate risks and demonstrate a company’s ability to abide by regulatory policies.

# SANS Compliance vs. SOC Compliance

SANS and SOC (System and Organization Controls) are two well-known security control compliance standards, but each contains distinct features. The SANS Institute is an organization with collective security research, policies, and educational security programs (SANS, 2019). While the AICPA (American Institute of CPAs) organization offers SOC compliance reports (Association of International Certified Professional Accountants, 2019). Furthermore, CPAs (Certified Public Accountants) can conduct these SOC reports, improving the security controls of a company. This section of the proposal addresses the various functions of SANS compliance and SOC compliance.

*SANS Features*

More than 165,000 individuals received SANS training, improving their approaches to effective security (Tittel & Kyle, 2019). One of these SANS courses includes the GIAC (Global Information Assurance Certification) program, teaching individuals the standards of IT security. Another popular feature of SANS is CIS (Critical Security Controls), which are a set of cyber defense actions for preventing current cyber threats (Gerberding, 2017). CIS contains twenty recommendable controls, covering various concepts such as malware defense, data recovery, and penetration testing. Moreover, the US military, NSA, DHS, and other organizations selected and defined CIS. For the sake of productivity, SANS also offers free information security policy templates (SANS, 2019). General, network security, server security, application security, and old/retired, are the available policies.

*SOC Features*

SOC reports are resourceful for organizations trying to meet certain user needs. There is three common SOC security report (SOC 1, SOC 2, and SOC 3) versions, with ***SOC 1 and SOC 2 containing two different types***. SOC 1 reports address internal service organization controls concerning the auditing of financial statements (Hemmer, 2018). Those reading a SOC 1 report can include financial executives, compliance officers, and financial auditors. SOC 2 reports discuss a company’s controls applicable to security, availability, processing integrity, confidentiality, and privacy. Those reading a SOC 2 report can include the same readers of a SOC 1 report, in addition to IT executives and business partners. A SOC 3 report addresses trust service criteria for general use, containing minimal detail on a company’s security controls (Bantz, 2016). For example, SOC 3 reports can be viewable on company websites. When conducting a Type I evaluation, the SOC report will consider the design of controls at a specific date. While conducting a Type II evaluation, involves the design and testing of security controls to determine their effectiveness over a lengthy time frame.

# Why Use SOC 2 Type II for XYZ Technologies Services

Security compliance became an important factor for XYZ Technology Services, due to the recent cyber-attack on the financial department. As a result, protecting user data is now a top priority. SOC 2 Type II compliance is the selection of choice by majority rule. Although SANS provides effective procedures, it’s not the best choice for XYZ Technology Services. The board members realize SOC 2 can specifically apply to technology organizations (Wilkins, 2018). For example, companies that ***store customer data*** in the cloud. Migrating to the cloud is a feasible future for XYZ Technology Services. One of the main reasons to incorporate SOC 2 compliance is to validate that systems enforce solid trust principles (Security, availability, processing integrity, confidentiality, and privacy of customer data). Complying with SOC 2 requires proper monitoring for any unauthorized or suspicious activity to a company. Thus, improving how XYZ Technology Services will deal with hazardous emails and secure contractor information. SOC 2 Type I, would only focus on the design of security controls at a specific moment. This does not address the effectiveness of such controls. SOC 2 Type II is ideal for the company because this report evaluates the operational effectiveness of security controls (Imperva, 2019). Therefore, XYZ Technology Services can determine how impactful their countermeasures are.

# Project Timeline

Implementing SOC 2 Type II should begin immediately, but will require time to become sufficient. Six weeks to three months is the average timeline for a SOC 2 reporting process (Risk3sixty LLC, 2017). However, notable goals for many organizations is to have Type II reporting cover twelve months of security controls. Then annual Type II reports should occur, enforcing continuous security control monitoring. SOC 2 reporting requires this abundance of time for numerous reasons such as planning/strategy, readiness assessments (Pre-audit stage), remediation procedures, auditing, and maintenance. The initial stage of planning/strategy is where the organization decides which SOC 2 features to adopt. Readiness assessments are the next stage, which compares a company’s current environment to SOC 2 requirements. Remediation procedures could be a necessity, depending on the results from readiness assessments. During the remediation procedures stage, the company must fix any identifiable issues preventing them from incorporating SOC 2. After the above stages, audit procedures can begin to evaluate the security of company systems. Lastly, Maintaining SOC 2 compliance is mandatory, which typically requires consistent auditing and adjusting of any vulnerabilities.

# Conclusion

Adopting SOC 2 Type II security compliance is a reasonable proposition. XYZ Technology Services needs effective safeguards to mitigate risks. Not only are these security measures necessary, but the company also needs to validate that these security controls are effective. Using SOC 2 Type II offers the company a reliable reporting system to evaluate security controls and enforce compliance.

References

Armor Defense, Inc. (2019). Security vs. compliance. Retrieved from <https://www.armor.com/security-compliance/>

Association of International Certified Professional Accountants. (2019). SOC for service organizations: Information for service organizations. Retrieved from <https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/serviceorganization-smanagement.html>

Bantz, J. (2016). SOC 2 and SOC 3: What’s the difference? Retrieved from <https://www.macpas.com/soc-2-and-soc-3-whats-the-difference/>

Gerberding, K. (2017). NIST, CIS/SANS 20, ISO 27001 – Simplifying security control assessments. Retrieved from <https://www.hitachi-systems-security.com/blog/nist-cissans-20-iso-27001-simplifying-security-control-assessments/>

Hemmer, N. (2018). SOC 1 vs. SOC 2. Retrieved from <https://linfordco.com/blog/soc-1-vs-soc-2-audit-reports/>

Imperva. (2019). SOC 2 compliance. Retrieved from <https://www.imperva.com/learn/data-security/soc-2-compliance/>

Risk3sixty LLC. (2017). How long does it take to get a SOC 2 report? Retrieved from <https://www.risk3sixty.com/2017/12/05/how-long-does-it-take-to-get-a-soc-2-report/>

SANS. (2019). Information security policy templates. Retrieved from <https://www.sans.org/security-resources/policies>

SANS. (2019). About. Retrieved from <https://www.sans.org/about/>

Tittel, E. & Kyle, M. (2019). SANS GIAC certification guide: Overview and career paths. Retrieved from <https://www.businessnewsdaily.com/10786-sans-giac-certification-guide-overview-and-career-paths.html>

Wilkins, T. (2018). Nine common questions about SOC 2 compliance. Retrieved from <https://www.threatstack.com/blog/9-common-questions-about-soc-2-compliance>