Deontae Carter, Ethan Brock, Emiliano Ceja, Jordan Marshall, Sierra Maldonado

Table of Contents

Compliance Documentation SOP

Purpose:

The purpose of this Compliance Documentation Standard Operating Procedure (SOP) is to provide guidelines for documenting security controls, configurations, and monitoring solutions in a hardened AWS system. This SOP ensures compliance with relevant standards and frameworks, such as PCI DSS, GDPR, HIPAA, etc.

Scope:

This SOP applies to all employees, contractors, and stakeholders responsible for the compliance documentation of the AWS environment, including the Linux server for PCI and PII, Windows server with a DC, private subnet, VPN tunneling, CloudWatch Log Aggregation System, Lambda detection system, and VPC flow logs.

Responsibilities:

- Compliance Officer: Oversee the compliance documentation process and ensure adherence to standards.
- IT Department: Provide necessary information, configurations, and evidence for compliance controls.
- Security Department: Conduct regular assessments, vulnerability scanning, and support compliance efforts.

Prerequisites:

- Understanding of relevant compliance standards and control requirements.
- Access to necessary documentation, configurations, and compliance guidelines.

Compliance Documentation Requirements:

1. 2.1 Identify Compliance Standards:

Identify relevant compliance standards and frameworks applicable to the AWS environment.

- 2.2 Understand Compliance Controls:

Familiarize yourself with specific control requirements mandated by the applicable standards.

- 2.3 Determine Documentation Format:
- Determine the format and structure for documenting compliance controls and their implementation details.

Security Controls Documentation:

2. 3.1 Identify Security Controls:

Identify the implemented security controls in the AWS environment.

- 3.2 Document Control Implementation:
- Document control objectives, descriptions, and implementation details.
- Include configurations, settings, and evidence to support compliance.

Compliance Monitoring and Review:

3. 4.1 Regular Compliance Assessments:

Conduct periodic assessments to ensure ongoing compliance with standards.

- 4.2 Documentation Review

Review and update compliance documentation as needed to reflect any changes or updates.

- 4.3 Remediation and Action Plan

Address any identified compliance gaps or issues promptly and develop an action plan for remediation.

- 4.4 Compliance Reporting:
- Generate compliance reports as required for internal or external stakeholders.

References:

- Ethan Denny's SOP Template
- Chat GPT Assistance
- NIST Cybersecurity Framework
- ISO 27001

Definitions:

- Policy: Broad, overarching guidance explaining the "why" behind actions.
- SOP: Detailed documentation explaining the "what, when, why" for specific procedures.
- Work Instructions: Step-by-step directions explaining the "how" for a particular task.

Revision History:

5/15/2023 -- "Compliance Documentation SOP" created by Emilio Ceja