Cybersecurity POAM *(Sample)*

Prepared for

State Government Client

((

1.0 Overview

1.1 Executive Summary

The Plan of Action and Milestones (POAM), also referred to as a corrective action plan, is the authoritative agency management tool for documenting the remediation actions of system risk. The POAM is a management process that.

A GRC Auditing Resource was selected to perform a comprehensive review and compliance assessment of a state government agency's policies, procedures, and processes based on its established Information Security Management System policy, and identify potential gaps in compliance and associated recommendations for improvement with respect to that policy. This preliminary release provides a summary of recommended actions only for the first segment of the client's ISMS, with a comprehensive POAM review to be provided on or before March 22, 2024.

Although, by its own declaration in the preliminary assessment, the client has not had any internal or external breach, a summary of the recommendations made during this initial stage of the client's ISMS audit is provided in Section 2 of this document, which highlight potential discrepancies that may become indicators of compromise, should a security event occur.

1.2 Conventions & Purpose

Guidacent follows POAM conventions based on US General Services Administration guidelines, with the intent of this POAM engagement being to outline potential risks to the client that may occur as a result from gaps or discrepancies within its stated the client's ISMS security policy, and delineates the tasks necessary to mitigate those discrepancies and provide a means for:

1. Planning and monitoring corrective actions;
2. Defining roles and responsibilities for weakness resolution;
3. Assisting in identifying the security funding requirements necessary to mitigate weaknesses;
4. Tracking and prioritizing resources Informing decision makers within the client.

1.3 The Client's Security Program Maturity & POAM Process

Effective remediation of security discrepancies is essential to building a mature and sound Infrastructure Security program. Evidence of the proper implementation and use of the POAM process is a critical element in the assessment of the client's program performance by the State 's designated Chief Information Security Officer.

1.4 Identification of Policy Discrepancies

Policy discrepancies identified by this engagement can be classified proactively or reactively. Proactive discrepancies occur when regular program and system reviews are conducted by the organization responsible, and vulnerabilities are identified and/or documented. Reactive discrepancies indicate that a particular gap or discrepancy has been identified using audits or external reviews, as in the case of this engagement.

1.5 Risk-based Exceptions

While this POAM identifies those gaps to be considered to be Indicators of Risk (while all other assessment references should be considered as "Acceptable"), in some situations, a discrepancy may not be included because a determination was made that the continued existence of the discrepancy is an *acceptable risk*. Such a determination must be certified by the Chief Information Security Officer.

2.0 the client's ISMS Assessment Summary & Recommendations *(Segment)*

2.1 Locus of Influence of 141.10 Policies *(Specify a "Zero-trust" Environment)*

- **STATED:**
  "INTRODUCTION
  (2) Assumes mutual distrust until proven friendly, including relationships within government, with trading partners, and with anonymous users in a least-privilege approach to access control."

- **ASSESSMENT:** Zero-trust Security Architecture (ZTSA) is a security model that implements the principle of least privilege (PoLP) to correlate user access within an operating environment. The objective of ZTSA is to ensure that each user is only assigned the privileges necessary to complete their tasks.

- **REPORTED: "**Information Technology Office (ITO) has procedures to address user type set up based on job classification, program need, (Local admin, Contractor, employee) - then ITO Security audit annually."

- **RECOMMENDATION:** Establish a baseline security policy for ZTSA as a mandate, which include the parameters for the following components:
  — ***Protect Surface***
  … A protect surface is a component of operations within the client's operations, which requires safeguarding from a potential threat or compromise. It should include the data, applications, assets, and services that are most critical for your enterprise to protect.
  — ***Review contextual parameters***
  … Identify & implement mandatory user access and review contextual parameters (i.e., time of access, location, device type).
  — ***Ensure multi-factor authentication is 100% mandatory***
  … While the client/ the client's ISMS stipulates MFA is deployed, the client must ensure this feature is a mandatory requirement before any access is given.
  — ***Implement Principle of Least Privilege***
  … Users are allowed access only when that access is required to accomplish their respective responsibilities and tasks.

2.2 Industry Standards Supported *(Remove the Ambiguity)*

- **STATED:**
  "INTRODUCTION
  (3) "Supports industry standards where applicable" Please describe which industry standards are supported and how they are implemented."

- **ASSESSMENT:** Because GRC guidelines and policies can assist the client in remaining aligned with government and industry regulations, ensuring a consistent message regarding *which* GRC "industry standard" plays a critical and quantifiable role in cybersecurity by ensuring measurable governance is in place and cybersecurity risks are managed against defined parameters.

- **REPORTED: "***DES ITO depending on group has their own industry standards. ITO Security uses 141.10 as the standard for which security requirements*

are made from while NIST 800.53 v5 as our control standard which we use to address the ambiguous items within 14.10."

- **RECOMMENDATION:** Remove all ambiguous references to "appropriate," and generic terms such as "industry standards," and provide accurate references to policies and frameworks implemented throughout DES. This also provides an authorized foundation through which all departments (regardless of understanding of Cybersecurity), may use as a point of reference.

2.3 Specify which IT Security Standards are considered for "adherence"

- **STATED:**
  "Departments are responsible for adherence to these IT security standards to protect IT systems and applications..."

- **ASSESSMENT:** The client has implied through conversation that it comports with NIST 800 framework guidelines, but that assumption is implied loosely in the 141.10 policy.

- **REPORTED: "***ITO Security conducts internal audits based on our IT security standards, NIST 800.53 controls, the client policies for our IT systems and applications.*"

- **RECOMMENDATION:** Consider rewriting the ISMS (this particular section), based on specific details to how the policy defines operational standards:
  - *"Departments within the client are responsible for adherence to NIST 800.53 IT security standards, which provide guidance for how to secure and manage IT systems and applications."*

2.4 Define "A Shared and Trusted Environment"

- **STATED:**
  "(1) Ensure(s) secure communications between governmental agencies take place within a shared and trusted environment."

- **ASSESSMENT:** An application security policy (ASP) includes best practices and operational guidelines for maintaining the client's application security parameters. the client should ensure it defines the objectives that security controls should achieve when developing, deploying, and managing software applications, and declare those secure design requirements as an ASP, with additional security consideration as outlined by the Open Web Application Security Project (OWASP).

- **REPORTED: "***ITO Security conducts Security Design Reviews with Office of Internal Affairs for new project and large changes to applications. Small changes are put through internal review."*

- **RECOMMENDATION:** the client/ should articulate what is defined as "large changes" and "small changes" and explain what assessment parameters are followed during the SDLC.

2.5 Identify SPLUNK as the security control deployed for SIEM

- **STATED:**
  "STANDARDS
  1.1 The department IT Security policy documentation must: … (7) Contain results, logs, and records from risk and security assessments to demonstrate that the assessments performed met the intended security objectives of the department."

- **ASSESSMENT:** A log collection / SIEM tool has been implemented but has not been identified. Identifying and specifying the SIEM tool's operational parameters provides quantifiable evidence of what and how audit trails may be required for review and analyzed, should an event take place.

- **REPORTED: "***Our source of truth is our logging tool Splunk - this is maintained and monitored by our Network team. ITO Security uses this if/when incidents occur."*

- **RECOMMENDATION:** To understand the purpose relating to a particular activity or event, or for later use as accountability or compliance SPLUNK should be identified as the source of information, with associated guidelines for how this tool is deployed and which department is responsible for its outputs (with respect to "IT Security Program documentation).

3.0 The Client's ISMS *(sample review)* General Conclusion

The client, as a state agency, acknowledges cyber threats as a category of risks to operational security. To enable the mission of state agencies and the state enterprise to reduce business risk and cost and protect the state's reputation, the Office of the Chief Information Officer (the client), has engaged an independent consulting firm to review the client's stated policies and procedures as defined in the client's ISMS.