Audit Procedure: GRC.1 – Information Security Governance

Control Objective

To ensure that cybersecurity responsibilities are clearly assigned within the organization, providing accountability and oversight, and that a defined governance structure exists with authority for security decision-making during incidents.

Related Compliance / Regulatory Requirements

- **SB 626:** Sec. 3(a)(1)
- **NIST CSF:** ID.GV-1, ID.GV-2
- **HIPAA:** §164.308(a)(1)(ii)(A)
- **OIDSA:** §6103(a)(1)
- **OBCA:** §108

Audit Scope

- Review of organizational structure related to information security governance.
- Evaluate roles and responsibilities for security oversight and incident management.
- Assessment of policies, procedures, and documentation supporting accountability.
- Verification of management authority and escalation paths for security decisions.

Audit Procedures

1. Review Governance Structure Documentation

   Objective:

   Confirm the existence of a defined cybersecurity governance framework.

   Procedure:

   i. Obtain the organization chart and information security governance documentation.

   ii. Verify the existence of assigned roles such as:

      a. Chief Information Security Officer (CISO) or equivalent
      b. Security team leads
      c. Incident response team members
      d. Data protection officer (if applicable)

   iii. Confirm that governance responsibilities are formally documented, including authority to make security-related decisions.

Evidence to Collect:

- Organizational chart showing cybersecurity responsibilities.
- Governance policy documents.
- Role descriptions and assignment records.

2. Assess Assignment of Responsibilities

Objective:

Ensure cybersecurity responsibilities are clearly assigned and communicated.

Procedure:

i. Review documentation assigning accountability for:

   a. Security policy enforcement
   b. Security incident response and escalation
   c. Risk management
   d. Compliance monitoring

ii. Conduct interviews with key personnel to validate that they understand their responsibilities.

iii. Verify whether there is a formally documented chain of accountability for security decisions.

Evidence to Collect:

- Responsibility matrices (e.g., RACI charts)
- Job descriptions
- Meeting notes confirming assignment of responsibilities

3. Evaluate Incident Governance and Decision-Making Authority

Objective:

Confirm a defined authority structure exists during cybersecurity incidents.

Procedure:

i. Review the incident response plan for:

   a. Assigned decision-making authorities
   b. Roles and responsibilities during incidents
   c. Escalation procedures

ii. Confirm procedures for authorizing containment, remediation, and communication actions.

iii. Verify that the governance structure allows timely decision-making in critical security situations.

Evidence to Collect:

- Incident response plan or playbooks
- Sample incident logs showing decision-making authority in action
- Minutes from incident response meetings

4. Review Policy and Procedure Compliance

Objective:

Ensure that policies and procedures are aligned with governance requirements.

Procedure:

i. Review policies on:

   a. Information security management
   b. Incident response
   c. Roles and responsibilities

ii. Verify policies are approved by senior management and regularly reviewed.

iii. Check for evidence of communication of policies to relevant staff.

Evidence to Collect:

- Security policies and procedures with approval records
- Training records demonstrating awareness of policies
- Policy review logs

5. Conduct Gap Analysis

Objective:

Identify deficiencies in the governance structure or assignment of responsibilities.

Procedure:

i. Compare current governance practices against regulatory requirements and frameworks.

ii. Document gaps or areas lacking formal accountability.

iii. Provide recommendations for strengthening governance structure.

Evidence to Collect:

- Gap analysis report
- Management action plan for remediation