Scenario 2 (Incident Response)

Governance Charter Update Recommendations

Prepared by: Michael Jordan

Date: 6/18/2025

Recommendation Overview

A recent internal audit showed that SecureTech's data‑breach response times were slow because team members were unsure who owned which tasks during an incident. Clarifying roles, creating explicit escalation routes, and institutionalizing training will reduce delays and improve overall incident‑response maturity.

Recommended Changes to the Governance Charter

New Role or Responsibility

- **Title:** Incident Response Lead
- **Purpose:** Provide single‑threaded leadership and coordination for every security incident.
- **Responsibilities:**
  - Serve as primary incident commander and point of contact.
  - Coordinate IT, GRC, Legal, Communications, and SOC resources.
  - Maintain and update the incident‑response playbook.
  - Lead incident drills and ensure lessons learned are captured.
- **Reporting Structure:** Reports to the GRC Team Lead; dotted‑line collaboration with the Security Operations Center (SOC).

Process Enhancements

- **Purpose:** Eliminate ambiguity and accelerate decision‑making during incidents.
- **Specific Changes:**
  1. **Tiered Escalation Matrix** – Define severity levels (Low, Medium, High, Critical) with clear notification paths, timelines, and backup contacts.
  2. **RACI Matrix** – Map Responsible, Accountable, Consulted, and Informed parties for each incident phase (Identification, Containment, Eradication, Recovery, Communication).

Policy or Procedure Additions

- **Purpose:** Embed continuous improvement and accountability into incident management.
- **Details:**
  - **Post-Incident Review (PIR):** Conduct within two weeks of any High or Critical incident to analyze root cause, team performance, and control gaps; update procedures accordingly.
  - **Playbook Versioning:** Require formal version control and sign-off for any updates to incident-response documentation.

Training Requirements

- **Description:**
  - Onboarding module for all new personnel with incident-response duties.
  - Quarterly tabletop exercises led by the Incident Response Lead.
  - Annual refresher certification covering roles, escalation paths, and relevant regulations.
- **Frequency:** Initial onboarding (once), quarterly simulations, annual certification.

Justification for Recommendations

Clearly defined ownership (Incident Response Lead), structured escalation paths, and mandatory training directly address the audit's root cause—role confusion—thereby shortening detection-to- containment intervals, ensuring regulatory notifications are timely, and reducing business impact.

Anticipated Benefits

- **Faster response times** and reduced mean time to contain (MTTC).
- **Improved accountability**
- **Regulatory compliance confidence** via documented procedures and timely notifications.
- **Continuous learning culture** through post incident reviews and ongoing training, raising overall security maturity.