ISO 27001 Implementation Plan Report

Prepared by: Michael Jordan

Date: 6-23-2025

Introduction:

This report presents the gap analysis and implementation plan for SecureTech's ISO 27001 compliance. The primary focus areas are A.9 (Access Control), A.12 (Backups), and A.16 (Incident Response). The goal is to identify weaknesses in current practices and provide a prioritized plan to align SecureTech with ISO 27001 standards.

Control: A.9 Access Control

Gap Identified:

Sensitive systems lack multi-factor authentication (MFA), leaving privileged and administrative accounts vulnerable to unauthorized access and potential breaches.

Action Plan:

1. **Evaluate and Procure**: Assess MFA solutions compatible with SecureTech's infrastructure (e.g., Duo Security, Okta, Microsoft Authenticator).
2. **Pilot Implementation**: Test MFA deployment with a group of administrative users to identify and resolve technical and usability issues.
3. **Full Rollout**: Expand MFA implementation across all privileged and sensitive accounts in phases, starting with high-risk systems.
4. **Training:** Conduct training sessions for end users to ensure smooth adoption of MFA practices, addressing common troubleshooting scenarios.
5. **Audit and Monitor**: Periodically review MFA logs to ensure consistent adoption and identify potential misuse.

- **Priority:** High
- **Timeline:** 3 months
- **Responsible Team**: IT Security
- **Notes:** Budget allocated for MFA tools, with anticipated cost savings through vendor negotiations. Ensure alignment with GDPR and PCI DSS requirements for strong access control.

Control: A.12 Backups

Gap Identified:

SecureTech performs weekly backups without daily incremental backups, posing a significant risk of data loss in case of a system failure or breach

Action Plan:

1. **Infrastructure Assessment:** Evaluate current backup systems to ensure compatibility with daily incremental backups.
2. **Daily Backup Automation**: Configure existing tools to perform automated daily backups with error notifications to administrators.
3. **Failure Monitoring**: Implement automated alerts for failed backups and immediate administrator notifications.

- **Priority:** Medium
- **Timeline:** 2 months
- **Responsible Team**: IT Infrastructure
- **Notes:** Leverage existing tools to minimize costs; evaluate cloud backup options for additional redundancy.

Control: A.16 Incident Response

Gap Identified:

SecureTech currently logs incidents manually, leading to inconsistent tracking and delayed response times. There is no centralized logging system or integration with monitoring tools, increasing the risk of undetected or unresolved security events.

Action Plan:

1. **Tool Selection:** Evaluate and select a centralized logging and incident management system compatible with SecureTech's infrastructure (e.g., Splunk, ELK Stack, or open-source options).
2. **System Integration:** Integrate logging with existing monitoring tools (e.g., antivirus, firewall, intrusion detection systems) to enable real-time alerting.
3. **Response Playbook:** Develop a standardized incident response playbook defining roles, responsibilities, and workflows for different incident types.
4. **Training:** Conduct scenario-based training for the Incident Response Team, focusing on high-impact scenarios such as data breaches and ransomware attacks.

- **Audit and Review**: Perform quarterly audits of logged incidents to evaluate response effectiveness and refine procedures.
- **Priority:** High
- **Timeline:** 1 months
- **Responsible Team:** Incident Response Team

- **Notes:** Consider low-cost or open-source tools if budget constraints apply. Ensure integration covers both internal IT infrastructure and external services (e.g., cloud platforms). Align response workflows with GDPR breach notification timelines (72 hours)

Reflection and Justification:

1. The identified gaps overlap with issues found in past GDPR audits (e.g., access control and incident logging).
2. Implementing MFA (A.9) and centralized incident response (A.16) are high-priority due to the potential for data breaches.
3. The backup improvement (A.12) ensures business continuity and reduces risk of data loss. These actions are feasible within the set timelines and align with SecureTech's current resources.