ISO 27001 Gap Analysis and Implementation Plan

Prepared by: Michael Jordan
Date: 6-23-2025

Objective

This report outlines the existing gaps between SecureTech's current security practices and ISO/IEC 27001 requirements. It provides a structured and prioritized implementation roadmap to close these gaps, strengthen the overall security posture, and align with global compliance standards.

Preparation

The gap analysis builds upon findings from prior GDPR audits, highlighting shared compliance issues such as incident response deficiencies and data protection weaknesses. The assessment focused on the most critical ISO 27001 control areas for SecureTech, specifically:

- **A.9 Access Control**
- **A.16 Incident Response**
- **A.12 Backups**

Step 1: Conducting the Gap Analysis

ISO 27001 Control	Gap Identified
A.12 Backups	Only weekly backups performed; lacks daily incremental backups.
A.9 Access Control	MFA not implemented on critical administrative systems.
A.16 Incident Response	Security events not consistently logged; absence of centralized log management.

Analysis Highlights

- **Backups (A.12):** The absence of daily backups elevates the risk of significant data loss in case of malware or system failure.

- **Access Control (A.9):** Missing MFA for administrative users introduces high risk of unauthorized access.
- **Incident Response (A.16):** Fragmented logging hinders timely detection, escalating security incident impacts.

Step 2: Developing the Implementation Plan

Control	Action Plan	Priority	Timeline	Team Responsible	Notes
A.16 Incident Response	- Deploy centralized log management. - Integrate logging with monitoring systems. - Provide staff training on log analysis.	High	1 month	Incident Response Team	Explore open-source tools. Set up automated detection alerts.
A.9 Access Control	- Acquire and implement MFA tools. - Enforce MFA on all admin accounts. - Provide user training.	High	3 months	IT Security	Budget for licensing. Plan phased rollout with fallback options.
A.12 Backups	- Enable daily incremental backups. - Automate alerts for failures. - Perform regular backup recovery tests.	Medium	2 months	IT Infrastructure	Optimize use of existing backup tools. Control upgrade costs.

Step 3: Prioritizing Actions

Criteria Used

- **Impact:** Potential security and compliance risks if unaddressed
- **Feasibility:** Realistic timeline and resource alignment
- **Cost:** Efficiency in relation to the reduction of risk

Priority	Control	Justification
1	A.9 Access Control	Weak access protection mechanisms present a critical vulnerability.
2	A.16 Incident Response	Without centralized logs, detection and resolution are delayed.
3	A.12 Backups	Inadequate backup frequency endangers business continuity.

Step 4: Finalizing the Implementation Plan

Control: A.16 Incident Response

- **Gap Identified:** Decentralized and inconsistent incident logging
- **Action Plan:**
  - Implement a centralized logging infrastructure
  - Integrate it with real-time monitoring platforms
  - Train teams on log review and response
- **Priority:** High
- **Timeline:** 1 month
- **Responsible Team:** Incident Response Team
- **Notes:** Utilize cost-effective, open-source options and set up automated notifications

Control: A.9 Access Control

- **Gap Identified:** Lack of multi-factor authentication for critical systems
- **Action Plan:**
  - Acquire and install MFA software
  - Enforce MFA policies for admin and privileged accounts
  - Deliver comprehensive user training sessions
- **Priority:** High
- **Timeline:** 3 months
- **Responsible Team:** IT Security
- **Notes:** Training is essential to reduce friction and improve adoption rates

Control: A.12 Backups

- **Gap Identified:** No daily incremental backup capabilities

- **Action Plan:**
    - Upgrade or configure systems to support daily backups
    - Automate alerting on failed backup tasks
    - Conduct monthly restore tests to validate backup integrity
- **Priority:** Medium
- **Timeline:** 2 months
- **Responsible Team:** IT Infrastructure
- **Notes:** Look into enhancing existing backup tools before procuring new ones

Step 5: Reflection and Validation

Key Insights

- The most urgent risks lie within **access control** and **incident response**, directly impacting SecureTech's ability to detect, prevent, and mitigate threats.
- A phased implementation strategy that considers cost, impact, and feasibility offers the most practical path to achieving ISO 27001 compliance.
- Continued monitoring, stakeholder alignment, and periodic reassessment will ensure the effectiveness and sustainability of the controls implemented.