Prepared by: Michael Jordan

Date: 6-15-2025

Top Three ISO 27001 Controls to Prioritize

1. A.9 – Access Controls

Priority Action: Implement Multi-Factor Authentication (MFA) for all sensitive and privileged systems.

Justification:

Access without MFA significantly increases the risk of credential theft and unauthorized access to sensitive systems. As privileged accounts often hold administrative rights, a compromise could lead to data breaches, system outages, or regulatory noncompliance. This is a high-impact, high-likelihood vulnerability.

---

2. A.16 – Incident Response

Priority Action: Establish and test a centralized incident response logging and management process.

Justification:

SecureTech currently lacks consistent incident logging. Without clear records, the organization cannot detect, analyze, or respond to threats efficiently. This increases the time to contain breaches and limits the ability to comply with reporting requirements (e.g., GDPR, PCI DSS).

---

3. A.6 – Risk Management (Risk Register)

Priority Action: Create and maintain a formal risk register.

Justification:

A risk register provides visibility into the organization’s current and evolving information security risks. Without one, leadership cannot prioritize mitigation efforts, allocate resources properly, or demonstrate ISO 27001 control over risk treatment. This control underpins all others.

Implementation Plan for Each Priority Control

1. A.9 Access Controls – Implement MFA

Action Steps:

- Evaluate and select a suitable MFA provider (e.g., Duo, Okta, Microsoft Authenticator).
- Define systems and users requiring MFA (privileged accounts first, then high-risk roles).
- Pilot test MFA with a small group of admin users.
- Roll out MFA across all required systems in phases.
- Provide training and support materials to staff.

Timeline:

- **Week 1–2:** Tool evaluation and procurement
- **Week 3–4:** Pilot implementation
- **Week 5–8:** Full deployment
- **Week 9:** Staff training and feedback
- **Week 10:** Go-live and monitoring

Resources Needed:

- **Technology:** MFA solution license and integration tools
- **Personnel:** IT Security Team, System Administrators, Training Staff
- **Budget Estimate:** $5,000–$12,000 (tool licensing, integration, support)

Monitoring Success:

- Weekly MFA compliance reports
- Reduction in failed login attempts and unauthorized access alerts
- Internal audit review post-implementation

2. A.16 Incident Response – Centralized Logging and Process

Action Steps:

- Update the incident response policy to require logging of all incidents.
- Deploy a centralized Security Information and Event Management (SIEM) tool (e.g., Splunk, Graylog, ELK stack).
- Train the incident response team on the updated procedures and SIEM use.
- Test and simulate incidents to validate process effectiveness.

Timeline:

- **Week 1–2:** Tool selection and policy update
- **Week 3–4:** Install and configure SIEM/logging tool
- **Week 5:** Staff training
- **Week 6–8:** Simulations and tuning alerts

Resources Needed:

- **Technology:** SIEM/logging platform (open-source or commercial)
- **Personnel:** Incident Response Team, IT Admins
- **Budget Estimate:** $3,000–$10,000 depending on solution choice

Monitoring Success:

- Track number of incidents logged monthly
- Response time and closure rate metrics
- Quarterly tabletop exercises with post-mortem analysis

---

3. A.6 Risk Management – Develop a Risk Register

Action Steps:

- Identify key information assets and associated risks across departments.
- Establish a risk classification and scoring model (likelihood × impact).
- Create a centralized risk register in a secure, accessible format (e.g., Excel, GRC tool).
- Assign risk owners and define mitigation or acceptance strategies.
- Review and update the register quarterly.

Timeline:

- **Week 1:** Build risk assessment framework
- **Week 2–4:** Perform initial risk identification and analysis
- **Week 5:** Assign owners and mitigation actions
- **Week 6:** Finalize and publish risk register

Resources Needed:

- **Technology:** Spreadsheet or GRC tool (optional: ServiceNow, LogicGate)
- **Personnel:** GRC Team, Departmental Risk Owners, CISO
- **Budget Estimate:** Minimal for spreadsheet; $3,000+ for GRC platform

Monitoring Success:

- Quarterly risk register updates
- Mitigation actions tracked and completed
- Risk trends reported to leadership monthly

Summary Table of Prioritized Controls

Control	Action	Risk Addressed	Timeline	Budget Estimate
A.9 Access Control	Implement MFA	Prevent unauthorized access	10 weeks	$5K–$12K
A.16 Incident Response	Centralized logging & training	Improve threat detection & response	8 weeks	$3K–$10K
A.6 Risk Management	Create risk register	Track & treat security risks	6 weeks	Low (or GRC tool cost)