Implementation of SME based on minimal control (ISO27001)

Overview:

SME implementation based on minimal control of ISO27001

Objective:

1. Focusing on critical control strength
2. Using low cost for implementation
3. Keeping documentation simple but effective.

Size: 50 to 100 Employees
Challenge: The company wants to implement ISO 27001 ISMS with minimal cost and effort while keeping all mandatory controls intact.
Goal: Achieve compliance with minimum effort while focusing on essential security practices

Steps of SME implementation:

Mandatory controls:

Phase	Activity	Mandatory Controls Addressed	Implementation Strategy
1. ISMS Scope Definition	Define boundaries of ISMS (e.g., include only critical systems handling customer data).	**Determining Scope**	Limit ISMS to systems handling sensitive customer information.
2. Leadership & ISMS Policy	Assign a security manager & create an ISMS policy.	**Information Security Policy**	CEO signs ISMS policy; Security Manager ensures implementation.
3. Risk Assessment	Identify risks & document mitigation strategies.	**Asset Management**	Use free/open-source risk assessment tools like OCTAVE or RiskIT.

4. Security Controls Implementation	Apply security controls like access control, logging, incident management.	**Access Control**, **Operations Security**	Enforce role-based access control (RBAC) and multi-factor authentication (MFA).
5. Documentation & Awareness	Train employees on security policies & incident reporting.	**HR Security**, **Incident Management**	Conduct online security awareness training (e.g., NIST guidelines).
6. Internal Audit & Continuous Improvement	Conduct an internal audit to check compliance.	**Internal Audit**	Perform quarterly self-audits using ISO 27001 audit templates.

Note:
While SMEs must retain all mandatory controls, adding selected optional controls can significantly improve security and future-proof compliance. Here are some recommended optional controls based on best practices:

Optional Controls for Enhanced Security:

Control	ISO 27001 Reference	Usefulness?	Implementation approach
Supplier Security Assessment	Supplier Security	Ensures third-party vendors don't introduce security risks.	Require basic security questionnaires for suppliers.
Security Patch Management	Security Updates	Prevents attacks from unpatched vulnerabilities	Automate updates
Threat Intelligence	Security Incident Monitoring	Helps SMEs stay updated on emerging cyber threats.	Subscribe to free cyber threat feeds
Mobile Device Management (MDM)	Mobile Security	Secures smartphones, tablets, and remote work devices.	Use Microsoft Intune or free MDM alternatives.