Asset	Threat Type	Confidentiality (C)	Integrity (I)	Availability (A)	Justification
Firewall	**Misconfiguration**	**3**	**4**	**2**	A misconfigured firewall can expose some network data (C), severely affect security rules (I), but may not always cause immediate downtime (A).
Security Camera	**Hacking**	**2**	**4**	**3**	A hacked camera may reveal video feeds (C), altered footage impacts forensic evidence (I), and disabling it reduces security monitoring (A).
Backup Drive	**Data Corruption**	**4**	**3**	**2**	Backups contain sensitive data (C), but minor corruption might still allow partial restoration (I). If unavailable, recovery is delayed (A).
Router	**Unauthorized Access**	**3**	**2**	**4**	Attackers may intercept some data (C), but direct integrity impact is limited (I). A compromised router can cause network outages (A).
Web Server	**DDoS Attack**	**1**	**3**	**4**	Web servers often host public data (C), but service disruption affects transactions (I). Availability is crucial for user access (A).
Database Server	**SQL Injection**	**4**	**2**	**3**	Databases store highly sensitive data (C). If attacked, data integrity may be partially compromised (I). Downtime impacts business operations (A).

ISO 27001 SME Implementation Plan (200+ Employees)

Overview

- **Focus**: Strengthening critical security controls while keeping implementation cost-effective.
- **Approach**: Mandatory ISO 27001 controls + 20% additional non-mandatory controls for enhanced security.

- **Reason for Non-Mandatory Controls**: Larger employee base increases risks related to insider threats, supply chain security, and third-party access.

Implementation Phases & Controls

Phase	Activity	Mandatory Controls (ISO 27001)	Implementation Strategy	Additional Non-Mandatory Controls (20%)	Reason for Additional Controls
1. ISMS Scope Definition	Define the ISMS boundary, including critical assets handling customer data.	Clause 4.3 - Scope Definition	Expand scope to include supply chain and vendor interactions.	Annex A.15 - Supplier Relationships	Increased vendor access to systems requires supplier risk management.
2. Leadership & ISMS Policy	Assign a dedicated security team & establish ISMS policy.	Clause 5.2 - Information Security Policy	Create a policy that is signed by leadership and communicated via training.	**N/A**	**N/A**
3. Risk Assessment	Identify, document, and mitigate risks using a risk assessment	Annex A.8 - Asset Management	Use free tools (OCTAVE, RiskIT) for risk assessment.	Annex A.17 - Business Continuity Management	A larger workforce needs clear business continuity planning for emergencies.

	framework.				
4. Security Controls Implementation	Implement key security measures (Access Control, Logging, MFA).	Annex A.9 - Access Control, Annex A.12 - Operations Security	Enforce role-based access control (RBAC), MFA, and endpoint protection.	Annex A.14 - System Development Security	Larger companies develop and integrate custom applications requiring security controls.
5. Documentation & Awareness	Train employees on security policies, phishing awareness, & incident reporting.	Annex A.7 - HR Security, Annex A.16 - Incident Management	Conduct regular training using NIST guidelines.	Annex A.6 - Organization of Information Security	Larger teams require clearly defined responsibilities to prevent insider threats.
6. Internal Audit & Continuous Improvement	Conduct internal audits to ensure compliance.	Clause 9.2 - Internal Audit	Perform quarterly audits using ISO 27001 templates.	Annex A.13 - Communication Security	More employees mean increased risk of data leaks via email, requiring secure communication policies.

Key Benefits of Additional Non-Mandatory Controls (20%)

1. **Supplier Security (Annex A.15):** With a larger workforce, vendor and third-party risks increase, requiring supplier security assessments.

2. **Business Continuity (Annex A.17):** A larger organization needs robust disaster recovery & business continuity planning.

3. **System Development Security (Annex A.14):** If the company builds internal tools or applications, secure development practices reduce risks.

4. **Defined Roles & Responsibilities (Annex A.6):** Prevents unauthorized access by ensuring clear job functions.

5. **Secure Communications (Annex A.13):** Larger teams mean more sensitive information flows via email, requiring encryption & DLP policies.