ISO 27001 Control	Process	Responsible	Key Activities/Steps
Information Security Policies (A.5)	Develop and Maintain Information Security Policies	Information Security Officer	- Identify policy needs based on risks and compliance requirements. - Develop policies covering data classification, acceptable use, incident response, etc. - Review and update policies annually.
Human Resources Security (A.7)	Employee Onboarding and Offboarding	HR Department / IT Team	- HR initiates background checks and security training for new hires. - IT creates and maintains user accounts and access privileges. - Ensure access is revoked upon employee departure.
Access Control (A.9)	User Access Management	IT Team	- Establish access control lists for each system and resource. - Grant access based on least privilege principle. - Regularly review and update access permissions.

Cryptography (A.10)	Data Encryption Process	Security Team	- Identify sensitive data requiring encryption. - Implement encryption protocols for data in transit and at rest. - Manage encryption keys securely.
Information Security Incident Management (A.16)	Incident Response Process	Incident Response Team	- Establish an incident response plan and team. - Detect, report, and assess security incidents. - Respond to incidents according to the defined procedures.
Business Continuity Management (A.17)	Business Continuity and Disaster Recovery	BCP/DR Team	- Identify critical processes and systems. - Develop and maintain a business continuity and disaster recovery plan. - Regularly test and update the plan.