1. Option I (ISO 27001 Process)

- **Preparation:** This includes identifying the scope of the ISMS, determining the resources required, and establishing the project plan
- **Awareness and training:** This involves raising awareness among employees about the importance of information security and training them on the requirements of ISO 27001
- **Risk assessment:** This includes conducting a comprehensive risk assessment to identify and evaluate the risks to the organization's information assets
- **Statement of Applicability:** This involves documenting the security controls and policies that will be implemented to manage the identified risks
- **Implementation:** This involves putting the security controls and policies into practice, documenting the procedures, and ensuring that all employees are trained on their roles and responsibilities
- **Documentation:** This involves preparing and maintaining a set of security-related documents, including the ISMS policy, procedures, and records
- **Internal audit:** This involves conducting periodic internal audits to evaluate the effectiveness of the ISMS and identify areas for improvement
- **Management review:** This involves regularly reviewing the ISMS to ensure that it remains relevant and effective in addressing the organization's information security needs
- **Certification:** Upon completion of the implementation and internal audit processes, organizations may choose to seek certification from an accredited third-party certification body to demonstrate their compliance with ISO 27001

2. Option II (ISO 27001 Process)