## 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)

Continual Improvement

## • Filling the Scoping Questionnaire $\bullet$ Kick off call with the client to gather basic understanding about the organization On-Boarding Understanding the scope Client • Getting on call and gathering further information about the process followed • Gathering further information about the security controls currently in place i.e. conducting the Test of Design(ToD) **Current State** • Understanding whether any security policies are currently documented Analysis • Identifying the Risks the organization is prone to, and drafting the risk register • Drafting the risk mitigation plan to remediate, accept or transfer the risk Conducting Risk • Map the existing controls to the ISO 27001 Standard requirements Control Mapping • Implementing controls according to ISO 27001 standard requirements • Suggesting corrective, Detective and compensatory controls • Drafting policies according to ISO 27001 standard requirements Implementation $\bullet \text{Sharing the policy drafting questionnaire, to gather information on drafting mandatory policy documents }$ • Conducting an internal audit, to Test the Effectiveness of Controls (ToE) • Prepare an internal audit report Conducting an • Report any further NC's post audit Internal Audit Conducting a stage I audit by the Accredated certification body • Document, process and policy verification verification • Stage I audit report along with corrrctive actions Stage I Audit • Verifying closure of findings from Stage I audit, before conducting stage II audit • Conducting stage II audit • Reviewing for the implemented controls according to standard requirements Stage II Audit • Conducting regular surveillence audits, to test whether the controls are operating effectively post certification