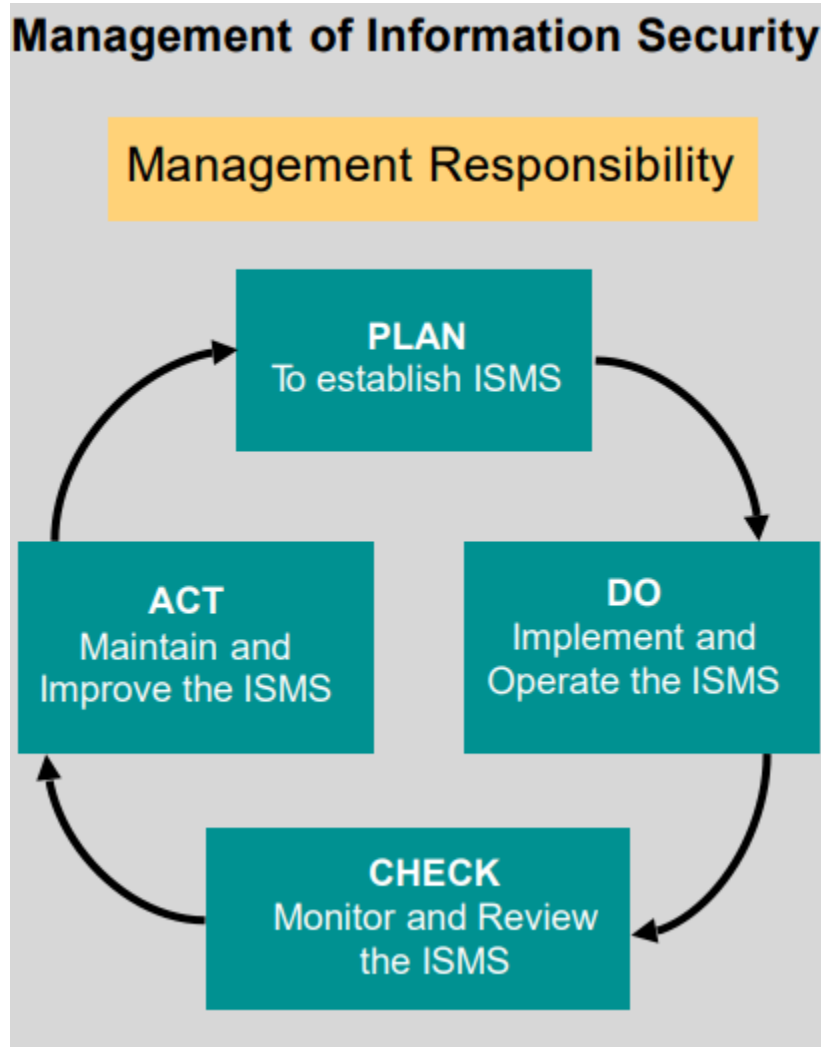


PDCA and Clauses

Plan(P) Do(D) Check(C) Act(A)



ISO/IEC 27001:2022: Clause 4 of 10

Clause 4: Context of Organization

- Understand the external and internal issues that affect the information security
- Identify interested parties and their requirements
- Establish the scope of ISMS
- Establish, implement, maintain and continually improve ISMS

ISO/IEC 27001:2022: Clause 5 of 10

Clause 5: Leadership

- Top Management to demonstrate leadership and commitment by ensuring ISMS policy, objectives, processes are established, necessary resources are provided and continual improvement is carried out
- Top Management to assign responsibility and authority for implementing and achieving conformance to ISMS

ISO/IEC 27001:2022: Clause 6 of 10

Clause 6: Planning

- Establish criteria and plan for risk assessment and necessary treatment
- Develop statement of applicability with identified controls as expected in Annex A of the standard
- Identify risks and opportunities and address them accordingly
- Establish ISMS objectives, responsibilities and timeline to achieve
- Carry out changes to ISMS in a planned manner

ISO/IEC 27001:2022: Clause 7 of 10

Clause 7: Support

- Provide resources for implementing ISMS
- Identify and acquire necessary competency required for ISMS
- Ensure awareness of ISMS, importance of conformance to it and consequences of non conformance
- Establish communication system to handle internal and external communication

ISO/IEC 27001:2022: Clause 8 of 10

Clause 8: Operation

- Conduct risk assessments and treatments as planned
- Take actions to address risks and opportunities as planned
- Keep record of documented information Establish criteria and plan for risk assessment and necessary treatment

ISO/IEC 27001:2022: Clause 9 of 10

Clause 9: Performance evaluation

- Establish measurement and management reporting framework to assess the performance of ISMS

- Plan and conduct internal audits to ensure compliance to ISMS and the applicable standards
- Top management to review periodically to check continuing suitability, adequacy and effectiveness of ISMS
- Organization to evaluate the information security performance and the effectiveness of the ISMS.

ISO/IEC 27001:2022: Clause 10 of 10

Clause 10: Improvement

- Plan actions to continually improve suitability, adequacy and effectiveness of ISMS
- Identify and respond to nonconformities as required
- Identify and eliminate causes of nonconformities