ISO 27001:2013
Scope of the ISMS
Determination of internal and external interested parties as ISMS prospective.
Understand needs and expectation of interested parties.
Interested parties' issue that can influence purpose, ISMS performance and strategic direction of the organization.
Roles, responsibility and authority is to be define and communicated in the organization those employees involved in managing your information security.
Information security policy to be established and authorised by top management.
Information Security Objective, their tracking and plan to meet the requirements, tracking the status of achievement of objectives.
Statement of Applicability which applied on your information security management system.
Methodology and criteria for **Risk assessment and risk treatment.**
Risk assessment plan, takes the controls you identified in your SOA and defines responsibility for implementation.
Evaluation and effectiveness risk assessment report to compiled with information security management system.
Inventory of assets to be monitored and nominate a person responsible for managing the information relating to that asset.
Acceptable use of assets policy that setting out clear rules for how your information system and other information assets must be used.
Acceptable use of assets demonstrates how you mitigate risk by managing what assets you make available and how.
Operating procedures for IT management that provides a framework for all management procedures to make sure that correct and secure information can be acquired.
Established and implement descriptions of the management processes and activities necessary to plan, operate and control the ISMS.
Secure system engineering principles is applying security while you develop your IT system.
Supplier security policy to protect information of your organization that might be not under your direct control.
Incident management procedure to be formed for control of security breach or incident in information security management system.
Business continuity procedure to be implemented for how you'll recover from critical activities within a set time frame.
Statutory, regulatory and contractual requirements to comply data management regulations.
Logs of user activities, exceptions, and security events
Planning of method of controlling the changes in the system due to changes in one part of the system.
Operate ISMS there are a variety of resources required which can include financial

resources, inventory, human skills, production resources and information/computer technology.
Plan and implement a communication process, Retain documented information on communication.
Competence evaluation of the employees and training calendar, training record and evaluation henceforth and keeping the records
Awareness of information security policy, objectives, process and other relevant information to the employees of the organization.
Documented information to be maintained (documented procedures and records) to support Information security management system.
Process flow, plan and controlled processes needed to meet requirements of ISMS.
Internal audit programme and results of internal audits of information security management system.
Results of the management review meeting on the agenda points described in the Standard.
The background of incidents and deviations, measures taken and the results of measures and corrective measures, and their effectiveness
Evidence of the results of the continuous improvement process

For More Details and requirements, Contact

support@siscertifications.com
web:- www.siscertifications.co.in
www.siscertifications.com
Contact number:- +91-9654721646