




**SERVICE METHODOLOGY  
ISO 27001:2013  
INFORMATION  
SECURITY MANAGEMENT  
SYSTEM (ISMS)**


## INTRODUCTION TO ISO 27001:2013



ISO 27001:2013 enables an organization to identify Information Security Risks. Taking the account of threats, vulnerabilities, the impacts and protecting the organization without compromising its CIA (Confidentiality Integrity Availability) of information by adopting proper information Security Management System. The overall agenda of ISO 27001:2013 is to cover the below aspects.

- Provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System with physical & technical controls.
- Ensure the ISMS are integrated into organizations business processes.
- Create an organizational culture that encourages active participation of employees in the Information Security Management System.

## KICKOFF




Kickoff meeting is an essential tool to communicate and plan for the execution of the project with minimal obstruction and to complete the project within planned time and cost.


Agenda for the kick off meeting is:

- Project plan discussion: This includes discussion about accountability and responsibility of stake holders. milestones and deliverables in the project
- Scope of services and scope of certification
- Legal and regulatory requirements

## CREATION OF CORE TEAM

- 
- Appointment of CISO
  - Appointment of Information Security Management Committee
  - Appointment of Internal Auditors
  - BCP manager
  - Appointment of ISO Leader

## GAP ANALYSIS




During this phase we conduct a gap analysis to check how much of your current practices are in line with the standard requirements. Your current practices are verified against these four reference criteria

- ISO 27001:2013 standard requirements
- SOA
- Legal, statutory and regulatory requirements
- Client requirements
- Internal policies and procedures

The results of this analysis are presented in the form of a Gap Analysis Report. This report acts as the list of action items for the remainder of the project.

## ISMS AWARENESS TRAINING



ISMS awareness training will be conducted to the employees of your organization. The training session is to help employees to gain knowledge, understand the concepts of ISO 27001:2013, and align processes and practice towards achieving a secure and threat free work environment. When the staff has been trained they can think & act and contribute towards achieving the goals.

## RISK REGISTER & SOA

A Risk Management procedure shall be documented and used as reference to manage the identified risks in consultation with all process owners and functional heads. We use ISO 31000 & ISO 27005 Risk Management standard techniques to identify, analyze, evaluate, document, prioritize, treat & quantify the identified risks. This step creates a Risk Register.

Suitable Risk treatment plans are identified based on the risk appetite level and CIA factor of the company. The outcomes of such actions are calculated, recorded, evaluated and documented. The Statement of Applicability (SOA) defines and identifies the physical & technical controls applicable to your organization based on your business process and requirements.

## ASSET MANAGEMENT

We assist in developing asset management policies and procedures by coordinating with the functional heads and understanding about the process. The main objective of asset management is:

- To identify organizational assets and define appropriate protection responsibilities
- To prevent unauthorized disclosure, modification, removal or destruction of information stored on media
- To ensure that information receives an appropriate level of protection in accordance with its importance to the organization

## NETWORK / COMMUNICATION SECURITY:

We assist in developing Network security management policies and procedures by coordinating with the functional heads and understanding about the process. The main objective of network security is:

- To ensure the protection of information in networks and its supporting information processing facilities
- To maintain the security of information transferred within an organization and with any external entity

## INCIDENT MANAGEMENT

We assist in developing Incident management policies and procedures by coordinating with the functional heads and understanding about the process. The main objective of incident management is:

- To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses

## BUSINESS CONTINUITY MANAGEMENT

We assist in developing Business Continuity management policies and procedures by coordinating with the functional heads and understanding about the process. The main objective of Business continuity management is as follows:

- To ensure Information security continuity shall be embedded in the organization's business continuity management systems
- To ensure availability of information processing facilities

## PHYSICAL SECURITY:

We assist in developing Physical security policies and procedures by coordinating with the functional heads and understanding about the process. The main objective of Physical security is:

- To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities
- To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations


## HUMAN RESOURCE SECURITY:

We assist in developing HR policies and procedures by coordinating with the functional heads and understanding about the process. The main objective of HR security is:

- To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered
- To protect the organization's interests as part of the process of changing or terminating employment
- To ensure that adequate training has been given to all the employees and vendors with respect to information security




## DOCUMENTATION




Our experts will list the policies, processes, SOPs, applicable SOA and records that need to be defined and documented as per ISO 27001:2013 requirements by discussing with each department and function heads we assist you for creation of the necessary documentation.

## ESTABLISH ISMS CONTROLS




Once the policies, processes, Statement of Applicability (SOA) its controls and SOPs have been documented and list of records to be collected has been listed and personnel have been identified and trained on such activities, then the need is to operate, monitor and review the efficiencies of such processes.

## INTERNAL AUDITOR TRAINING




ISO 27001:2013 Internal Auditor (IA) Training will be provided to the identified personnel. This training will equip such personnel to analyze the need for IA, plan and schedule IA, prepare audit checklists, and conduct an IA and to document and report their observations to the top management.

## INTERNAL AUDIT



Our experts will oversee the conducting of internal audit by your internal audit team. This internal audit will identify still existing gaps in the system and demonstrate the level of preparedness to face the certification audit. This audit gives the organization a chance to identify and rectify all non-conformances before proceeding to the certification audit. The top management is apprised of the internal audit findings.

## ROOT CAUSE ANALYSIS (RCA) AND CORRECTIVE ACTIONS



All non-conformances identified during the internal audit, client or third party audits, or from Risk assessment and risk treatment methodology, risk register Incident Register, Vulnerability Assessment & Penetration Test (VAPT) Report, Malware attacks, downtime register, network issues, access controls, asset register, third party risk assessment reports, CIA-Information classification, internal & external attacks and any other sources have to be listed. RCA to be performed using techniques like Brainstorming and Fish-Bone methods. The optimal corrective actions are implemented. The effectiveness of such actions is documented and reviewed via a Corrective Action Report (CAR).

## MANAGEMENT REVIEW MEETING (MRM)



The MRM is an opportunity for all ISMS stakeholders to meet on scheduled intervals to review, discuss and plan actions on the below agenda points.

- Effectiveness of the current Management System with respect to ISMS
- Risk assessment & Risk Treatment plans and records
- Results on CIA (Confidentiality Integrity & Availability) of the information
- Audit findings and non-conformances from all sources
- Corrective Action plan to resolve any open items
- Continual Improvements made to the system
- Resources and trainings required
- Statutory and compliance aspects



## CERTIFICATION AUDIT: STAGE 1

When the level of preparedness has reached adequate levels, the process for certification begins.

An appointed auditor from the Certification Body (CB) verifies the Standard requirements via a stage 1 audit. This involves the auditor reviewing the policies, processes, SOPs, SOA, critical operational records, IA and MRM records. Any major deviations from the CB's expectations will be notified at this point for bringing in the necessary corrections. This reduces the chances of major non-conformances during the certification audit.

TOP Certifier will by liaise with all stakeholders and oversee smooth completion of the audit.

## CERTIFICATION AUDIT: STAGE 2

On successful completion of Stage 1 audit, the auditor focuses on a detailed audit of report and documentation of the Information Security Management System of the organization. TOPCertifier would have trained your personnel on the audit requirements and on confidently facing the audit. Our experts will be present to assist in any means necessary for the smooth functioning of the audit. TOPCertifier will assist your team to close any non-conformances identified during the audit. Upon successful completion of the certification audit, TOPCertifier will liaise with all stakeholders to draft, approve and release the final certificate.

## CONTINUATION OF COMPLIANCE

TOPCertifier will be part of your organization's compliance journey and assist you at regular intervals with necessary trainings, system support and updations, internal and external audits and regular renewal of your certification.