Technical -Approach

ISO 27001 Information Security Management System (ISMS)

Infopercept

INVINSENSE

Emerging Threat Landscape

- Poor patch-management processes
- Ad hoc processes and procedures for managing operations
- Lack of post-incident “lessons learned” discipline

Process

People

- Lack of awareness for today’s threat landscape
- Lack of skilled resources
- Poorly defined security roles and responsibilities

Technology

- Poorly integrated and deployment of security products
- Inability to discover sophisticated attack techniques
- Lack of threat intelligence capabilities

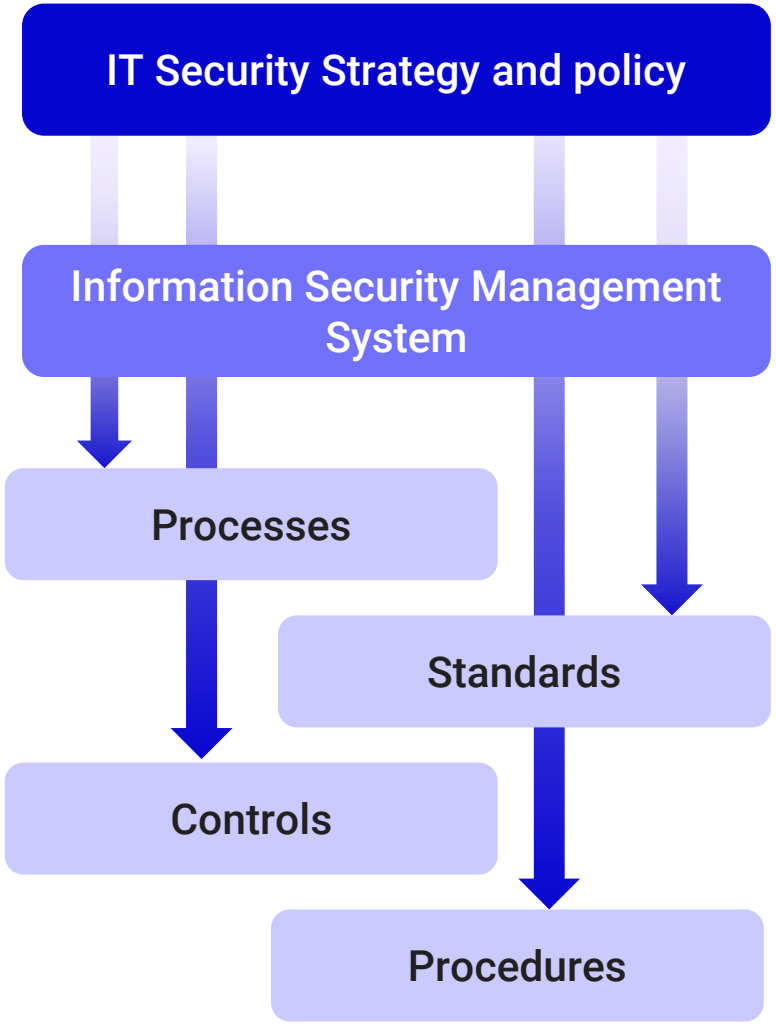
- Disruption of Services
- Exposure to targeted attacks
- Loss of Reputation

Introduction

Infopercept

What is ISMS?

- An ISMS enables an organization to systematically create and operate a management system for information security.
- By establishing an ISMS, an organization can initiate a formal process to help it determine the necessary security level requirements, create plans based on Risk Assessment and select countermeasures to mitigate Unacceptable Risk. With an ISMS, an organization can maintain and improve Confidentiality, Integrity, and Availability of its informational assets.
- In particular, by measuring the effectiveness of controls implemented through risk assessment within the ISMS, an organization is able to improve its information security in an efficient and effective manner.
- The most popular ISMS follows the ISO 27001 standard which offers an international certification scheme.



Elements Of Security

Network Security

- Firewall/Remote
- Gateway Mail
- Gateway Web
- Endpoint Security
- Software Integrity

Firewall/VPN
• Network Gateway Protection
• IPSEC VPN • Opt. Unified Threat Mgt

Gateway MAIL Security
• Anti-Spam • Anti Virus • Encryption • Reporting
• In/Out Bound Content Inspection • Policy Enforcement

Gateway WEB Security
• Web Surfing Control • Web Mail (See GW Mail)
• IM/P2P Control • Anti-virus/Malicious Code

Endpoint Security (Client/Server)
• Antivirus • Spyware • Spam • Websites • Firewall

System Integrity
• Patch Mgmt. • Change Control

Access Control

- Logical
  - Tokens
  - Management
  - NAC
- Physical

Access Control
• Identity Authentication • Authentication
• 2+Factors • Web/Network/SSO • Physical & Logical • Inside/Outside

Network Access Control (NAC)
• Endpoint Control • Identify Mgt (Tokens)
• Central Manage • Reporting

Business Continuity

- Disaster Recovery
- Data Backup/Restore
- Environmental (UPS)
- Monitoring & Reporting

Disaster Recovery (System)
• Quick Recovery from Hardware/System Crash

Disaster Recovery (Data)
• Quick Recovery from Data Loss, or Corruption

Disaster Recovery (Environmental)
• Power Backup • Environmental Control

Network Continuity Monitoring/Reporting
Monitor Network Devices • Applications
• Services • Environmental Status & Report Failure

Compliance

- Reporting
- Monitoring
- Archiving
- SIM/SEM

(Security Information Event Mgt)

Network Monitoring
• Monitoring Network Traffic • Shape

Mail Archiving
• Usually for Compliance or Risk Reduction

SIM/SEM & Reporting
• Security Event Mgt, /Information Mgt (Logs...)
• Central Collection, Correlation & Reporting

Confidentiality

- (Encryption)
- Data At-Rest
- Disposal

Data Encryption
• Whole Disk (Laptop) • File/Folder
• Network Storage • Communications

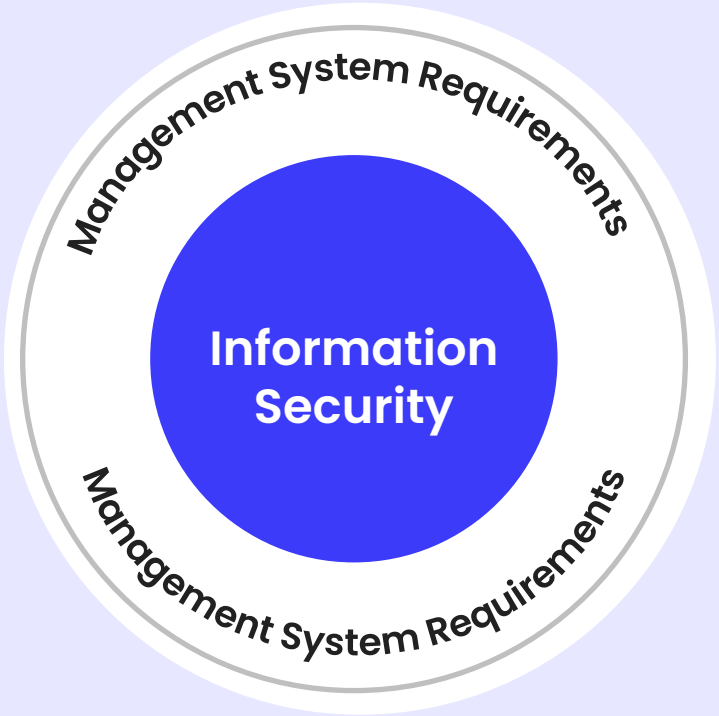
Risk Assessment

- Overall Risk
- Critical Assets
- Network Risk (CAAT)

Network Risk Assessment
• Network Device Vulnerability Scanning

Controls (ANNEX A And ISO/IEC 27002)

1. Security Policies
2. Organization of Information Security
3. Asset Management
4. Access Control
5. Communications Security
6. Physical and Environmental Security
7. Operations Security



8. Cryptography
9. Supplier Relationships
10. System Acquisition, Development and maintenance
11. Information Security aspects of business continuity management
12. Information Security incident management
13. Human resource security
14. Compliance

Management Commitment In Security Implementation

- Ensuring Policy and objectives are established
- Ensuring the integration of the iso/iec 27001 requirements
- Ensuring the necessary resources are available
- Communicating the importance of conformance with the ISMS requirement
- Ensuring the outcomes of the ISMS are met
- Directing and supporting person to contribute to ISMS effectiveness
- promoting continuous improvement
- Supporting other managers to demonstrate leadership

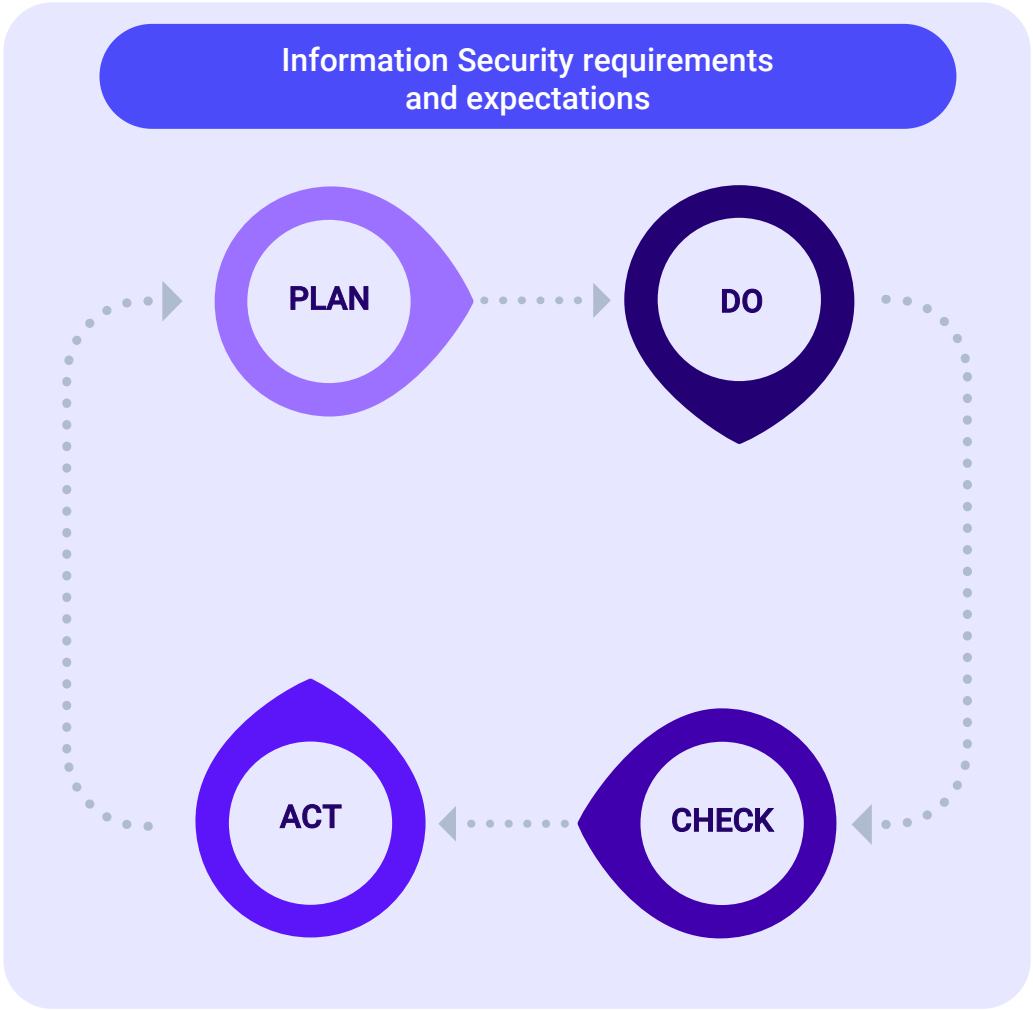
Proposed Methodology

Infopercept

Our Methodology For ISMS

PDCA Approach

- Plan Phase – conduct gap analysis and provide road map for ISO 27000 implementation.
- Do Phase – Improve all ISMS documentation including policies and procedures, Risk analysis according to ISO 27000 and assist in implementation
- Check Phase – ISMS internal audits, coordination during certifying audit
- Act Phase – post audit follow-up (including CAPA reports and assistance in implementation to close the audit points)



Our Approach

Infopercept

Our Approach for ISMS

PHASE 1	PHASE 2	PHASE 3	PHASE 4
PLAN	**DO**	**CHECK**	**ACT**
• Understand Business processes • Finalize on the ISMS Scope • Review of Control • Perform ‘As-Is’ analysis Current State Assessment) • Plan for ISO 27001:2013 Implementation	• Perform ISMS Implementation Training • Assist in Improving the Asset Inventory • Assist in preparing the Information Risk Management • Perform Vulnerability Assessment and Penetration Testing, • Drafting necessary Information Security Policies • Assist in Implementation of Information Security Policies	• Perform ISMS Internal Audit • Discuss Internal Audit Findings with ISMS Coordinator • Assist in preparing Audit Response Plan • Prepare Corrective and Preventive Action Reports	• Assist in implementation of Audit Response Plan

Objective: To conduct Gap Analysis and prepare plan for implementation of ISMS

Phase 1- Plan

Activities	Deliverables
• Understand the core and supporting business functions • Understand and discuss the information security requirements of the organization • Finalize on the ISMS Scope • Review security architecture • Review existing documents like policies, procedures, forms etc related to ISMS • and other certification achieved by an organization. • Perform 'As-Is' analysis (Current State Assessment)	• Gap Analysis Report including a broad roadmap for ISMS
Client Requirements	**Expected Duration**
• Provide Business Objectives, • Provide information on Critical business processes, critical IT Processes, Quality Processes • Existing P&P • Existing security processes, service processes and documentation	<Based on Scope>

Phase 1- Sample Deliverables

Summary of Gap Analysis results by Area

	Number of Requirements	Qty Compliant	%	Qty Partially compliant	%	Qty Non-compliant	%	Qty Not Applicable
Security Policy	2	2	100	0	0	0	0	0
Organisation Of Information Security	11	11	100	0	0	0	0	0
Asset Management	5	3	60	2	40	0	0	0
Human Resources Security	9	7	78	2	22	0	0	0
Physical And Environmental Security	13	12	92	1	8	0	0	0
Communications And Operations	32	25	78	5	16	0	0	2
Access Controls	25	25	100	0	0	0	0	0
IS Acquisitions, Development And Maintenance	16	13	81	2	13	0	0	1
Info Security Incident Management	5	3	60	1	20	1	20	0
Business Continuity Management	5	5	100	0	0	0	0	0
Compliance	10	8	80	1	10	0		
OVERALL RESULTS Qty	**133**	**114**		**14**		**1**		
OVERALL RESULT for Final Graphic Analysis	**129**	**114 of 129**	**88%**	**14 of 129**	**11 %**	**1 of 129**		

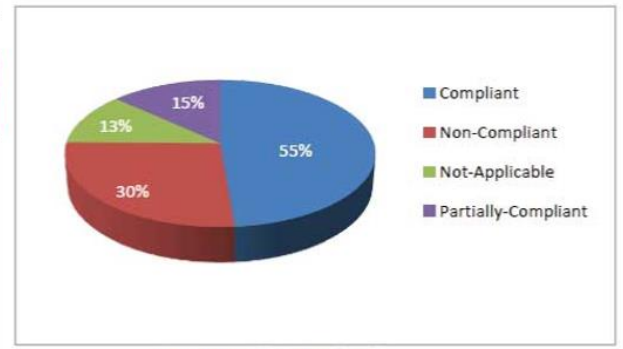


Figure 1 Compliance Dashboard

Phase 2- Do

Activities	Deliverables
• Performing ISMS training • Reviewing existing asset management practices • Updating and improving existing Information Security Policies • Assistance in improving of Information Security Policies • Assist in improving the Service Risk Management;	• Finalize ISMS Documentation • Do Handholding in ISMS Improvement
Client Requirements	**Expected Duration**
• Documentation and Technical details where necessary	<Based on Scope>

Information Security Awareness

01. Think about this

- What is Information?
- What happens when it is stolen?
- How important are safeguards without an “informed” employee?
- How do you as an employee play a part?

02. About the Session

Today we will

- Understand the basic information security concepts
- Know about specific policies
- Know our responsibilities towards information security
- Know what to do when an incident happens

Phase 3- Check (Internal Audit ISMS)

Activities	Deliverables
• Management Review meeting on Gap Analysis • Management Discussion on implemented policies & procedures • Perform ISMS Internal Audit • Discussing Internal Audit Findings with ISMS co-coordinators • Assist in preparing Audit Response Plan • Prepare Corrective and Preventive Action Report	• Internal Audit Report • Corrective and Preventive Action Reports
Client Requirements	**Expected Duration**
• Provide information on Critical business processes, critical IT Processes Necessary reports • Existing Documentation and Records	<Based on Scope>

Objective: To maintain and improve ISMS

Phase 4- Act (Post Audit Follow-up)

Activities	Deliverables
• Assist in implementation of Audit Response Plan (Corrective and Preventive Action Reports)	• High Level Recommendation on email
Client Requirements	**Expected Duration**
• List on implementation done base on recommendations	<Based on Scope>

Objective: Calling authoritative body and award client with its ISO 27001 Certificate

Certification Audit By Authoritative Body*

Activities	Deliverables
• Assist in implementation of Audit Response Plan (Corrective and Preventive Action Reports)	• High Level Recommendation on email
Client Requirements	**Expected Duration**
• List on implementation done base on recommendations	<Based on Scope>

About Infopercept

Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

Our specialized core team comprises experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, latest trends, and security innovations; ensuring that you always get the best security approach & solution for your specific business needs exactly the way you want it to be.

Imprint
© Infopercept Consulting Pvt. Ltd.

Address
3rd floor, Optionz Complex
Opp. Hotel Regenta,
CG Road, Navrangpura,
Ahmedabad - 380 009,
Gujarat, India.

Contact Info
M: +91 9898857117
W: www.infopercept.com
E: sos@infopercept.com

Global Office

United State of America
+1 516 713 5040

United Kingdom
+44 2035002056

Sri Lanka
+94 702 958 909

Kuwait

India
+91 9898857117

Infopercept