ISMS Part-I

27001

Ver.2022

ISO27001:2022 lead Implementor Course

By Jagbir Singh | jagbir@infocus-it.com

MTech(CS) | LLB |CISA | ISO27001LA |ISO22301LA|CEH|CHFI

Exercise A – Start here

5. Organizational controls	6. People controls	8. Technological controls
5.1. Policies for information security	6.1. Screening	8.1. User endpoint devices
5.2. Information security roles and responsibilities	6.2. Terms and conditions of employment	8.2. Privileged access rights
5.3. Segregation of duties	6.3. Information security awareness, education and training	8.3. Information access restriction
5.4. Management responsibilities	6.4. Disciplinary process	8.4. Access to source code
5.5. Contact with authorities	6.5. Responsibilities after termination or change of employment	8.5. Secure authentication
5.6. Contact with special interest groups	6.6. Confidentiality or non-disclosure agreements	8.6. Capacity management
5.7. Threat intelligence	6.7. Remote working	8.7. Protection against malware
5.8. Information security in project management	6.8. Information security event reporting	8.8. Management of technical vulnerabilities
5.9. Inventory of information and other associated assets	**7. Physical controls**	8.9. Configuration management
5.10. Acceptable use of information and other associated assets	7.1. Physical security perimeter	8.10. Information deletion
5.11. Return of assets	7.2. Physical entry	8.11. Data masking
5.12. Classification of information	7.3. Securing offices, rooms and facilities	8.12. Data leakage prevention
5.13. Labelling of information	7.4. Physical security monitoring	8.13. Information backup
5.14. Information transfer	7.5. Protecting against physical and environmental threats	8.14. Redundancy of information processing facilities
5.15. Access control	7.6. Working in secure areas	8.15. Logging
5.16. Identity management	7.7. Clear desk and clear screen	8.16. Monitoring activities
5.17. Authentication information	7.8. Equipment siting and protection	8.17. Clock synchronization
5.18. Access rights	7.9. Security of assets off-premises	8.18. Use of privileged utility programs
5.19. Information security in supplier relationships	7.10. Storage media	8.19. Installation of software on operational systems
5.20. Addressing information security within supplier agreements	7.11. Supporting utilities	8.20. Network security
5.21. Managing information security in the ICT supply chain	7.12. Cabling security	8.21. Security of network services
5.22. Monitoring, review and change management of supplier services	7.13. Equipment maintenance	8.22. Segregation of networks
5.23. Information security for use of cloud services	7.14. Secure disposal or re-use of equipment	8.23. Web filtering
5.24. Information security incident management planning and preparation		8.24. Use of cryptography
5.25. Assessment and decision on information security events		8.25. Secure development life cycle
5.26. Response to information security incidents		8.26. Application security requirements
5.27. Learning from information security incidents		8.27. Secure system architecture and engineering principles
5.28. Collection of evidence		8.28. Secure coding
5.29. Information security during disruption		8.29. Security testing in development and acceptance
5.30. ICT readiness for business continuity		8.30. Outsourced development
5.31. Legal, statutory, regulatory and contractual requirements		8.31. Separation of development, test and production environments
5.32. Intellectual property rights		8.32. Change management
5.33. Protection of records		8.33. Test information
5.34. Privacy and protection of PII		8.34. Protection of information systems during audit testing
5.35. Independent review of information security		
5.36. Compliance with policies, rules and standards for information security		
5.37. Documented operating procedures		

*New control, 2022

Activities Home – Task

Exercise-0	Your Objective from this course & Exercise
Exercise-1	Terms & Definitions pertaining to ISO27001
Exercise-2	Auditing Information Security Principles
Exercise-3	External and Internal Issues – list down the external and internal issues consider you company as case study for ISO27001 implementation.
Exercise-4	List down interested parties
Exercise-5	Write Scope statement
Exercise-6	Write your Information security policy
Exercise-7	Draw Organization chart as per your company structure (only to cover information security team & concerned team)
Exercise-8	Define Roles and responsibilities as per the organization chart in exercise -7
Exercise-9	Risk Assessment and Risk Assessment methodology. Asset base V/s Issue base Risk assessment
Exercise-10	Make a list of information asset (Inventory)
Exercise-11	Make a list of Risk / Issues as per your organization
Exercise-12	List down information security objectives of your organization
Exercise-13	Resource and Competence matrix
Exercise-14	Resource and Competence matrix
Exercise-15	Policy / process doc for Document control
Exercise-16	Define communication Plan /policy
Exercise-17	Risk treatment plan
Exercise-18	Define Internal Audit Schedule
Exercise-19	Internal Audit training
Exercise-20	Internal Audit Process
Exercise-21	Management Review Process
Exercise-22	Corrective action process Management Review Process
Exercise-23	Prepare Your own checklist - for Implemention & Audit
Exercise-24	Internal Audit template
Exercise-25	Non Confirmity Exercise
Exercise-26	NC – Template
Exercise-27	Final Audit Report - Template

Part-1 | ISO27001:2022

- **What is Information Security | Information asset**
- **ISO27001 Intro**
- **How to read the ISO Standard | ISMS framework**
- **ISMS framework**

Clause 1. Scope

Clause 2. Normative References

Clause3. Terms and Definitions

Clause 4. Context of the organization

INTRO TO ISO27001

ISO 27001 is “ISO/IEC 27001 – “**Information security, cybersecurity and privacy protection — Information security management systems — Requirements**.”

It is the leading international standard focused on information security, published by the International Organization for Standardization (ISO), in partnership with the International Electrotechnical Commission (IEC). Both are leading international organizations that develop international standards.

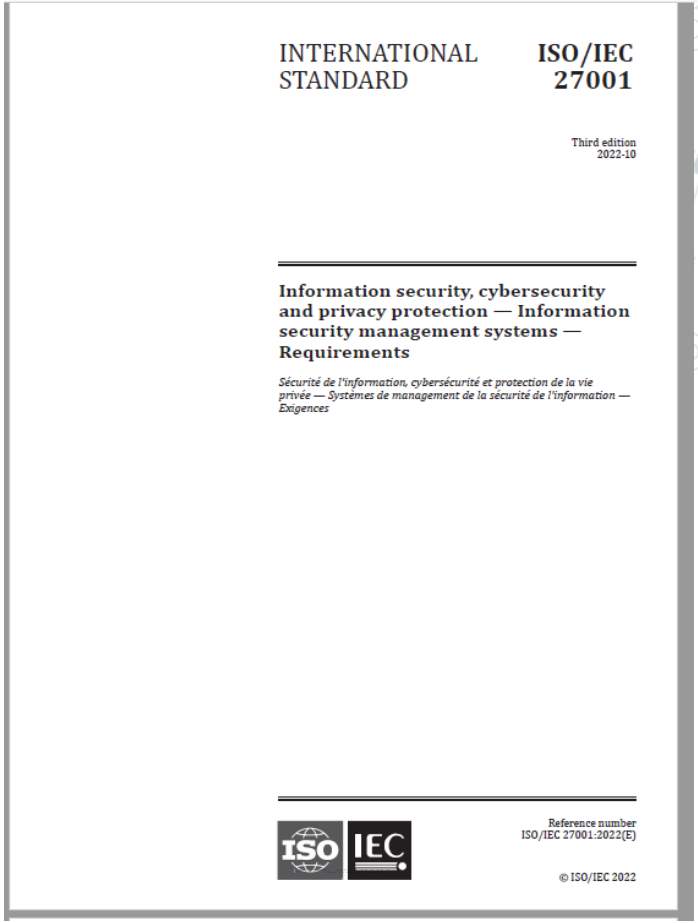
ISO-27001 is part of a set of standards developed to handle information security: the ISO/IEC 27000 series.

ISO27001:2022

1. **Introduction** – describes what information security is and why an organization should manage risks.
2. **Scope** – covers high-level requirements for an ISMS to apply to all types or organizations.
3. **Normative References** – explains the relationship between ISO 27000 and 27001 standards.
4. **Terms and Definitions** – covers the complex terminology that is used within the standard.
5. **Context of the Organization** – explains what stakeholders should be involved in the creation and maintenance of the ISMS.
6. **Leadership** – describes how leaders within the organization should commit to ISMS policies and procedures.
7. **Planning** – covers an outline of how risk management should be planned across the organization.
8. **Support** – describes how to raise awareness about information security and assign responsibilities.
9. **Operation** – covers how risks should be managed and how documentation should be performed to meet audit standards.
10. **Performance Evaluation** – provides guidelines on how to monitor and measure the performance of the ISMS.
11. **Improvement** – explains how the ISMS should be continually updated and improved, especially following audits.
12. **Reference Control Objectives and Controls** – provides an annex detailing the individual elements of an audit.

ISO framework and the purpose of ISO 27001

ISO framework is a combination of policies and processes for organizations to use. ISO 27001 provides a framework to help organizations, of any size or any industry, to protect their information in a systematic and cost-effective way, through the adoption of an Information Security Management System (ISMS).


INTERNATIONAL STANDARD

ISO/IEC 27001

Third edition
2022-10

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

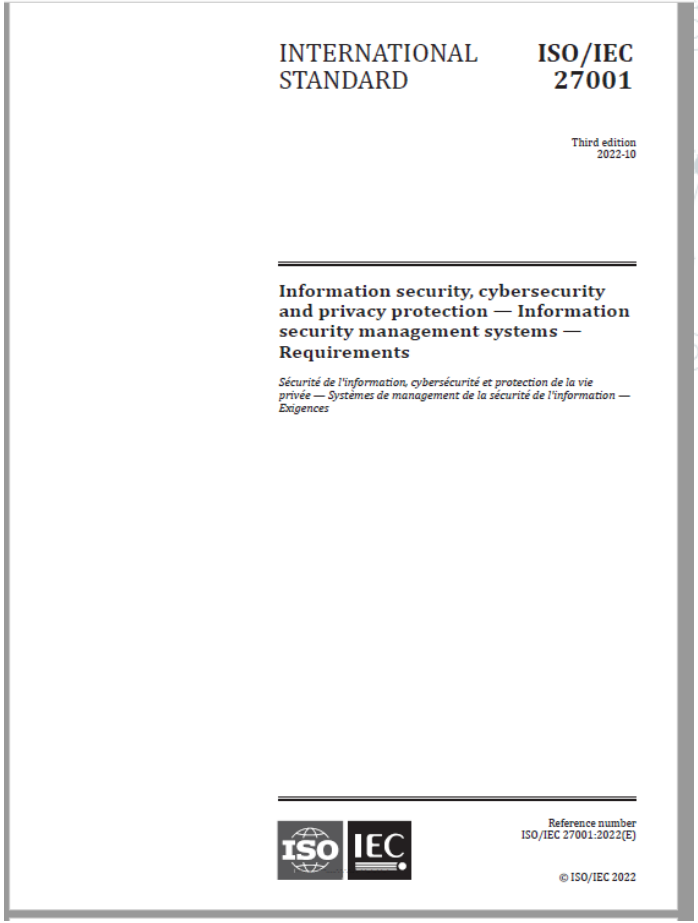
ISO IEC

Reference number
ISO/IEC 27001:2022(E)

ISO framework and the purpose of ISO 27001

This document specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.

This document also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this document are generic and are intended to be applicable to all organizations, regardless of type, size or nature.


INTERNATIONAL STANDARD

ISO/IEC 27001

Third edition
2022-10

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

ISO IEC

Reference number
ISO/IEC 27001:2022(E)

ISO27001:2022

What is Information

Data V/s Information

Where all the information is residing .?

Scope of information media > Only three where information resides ?

INFORMATION MEDIA

ELECTRONIC MEDIA

MIND

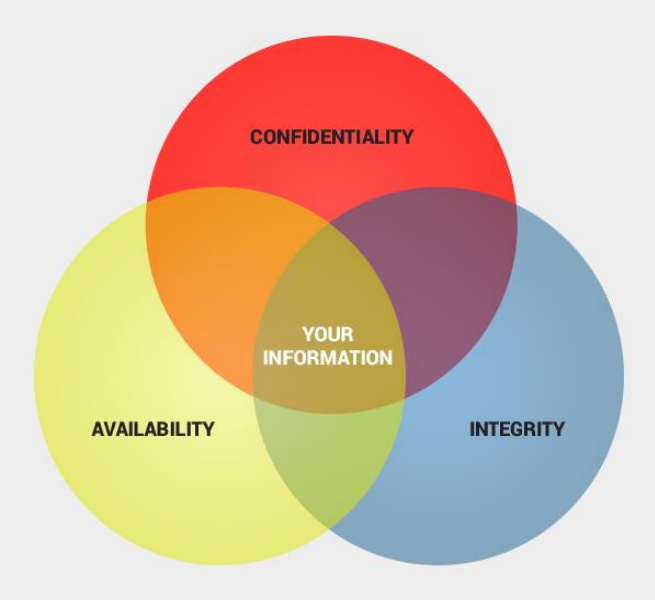
PRINT

MEDIA

What are the 3 ISMS security objectives?

The basic goal of ISO 27001 is to protect three aspects of information:

- **Confidentiality**: only the authorized persons have the right to access information.
- **Integrity**: only the authorized persons can change the information.
- **Availability**: the information must be accessible to authorized persons whenever it is needed.

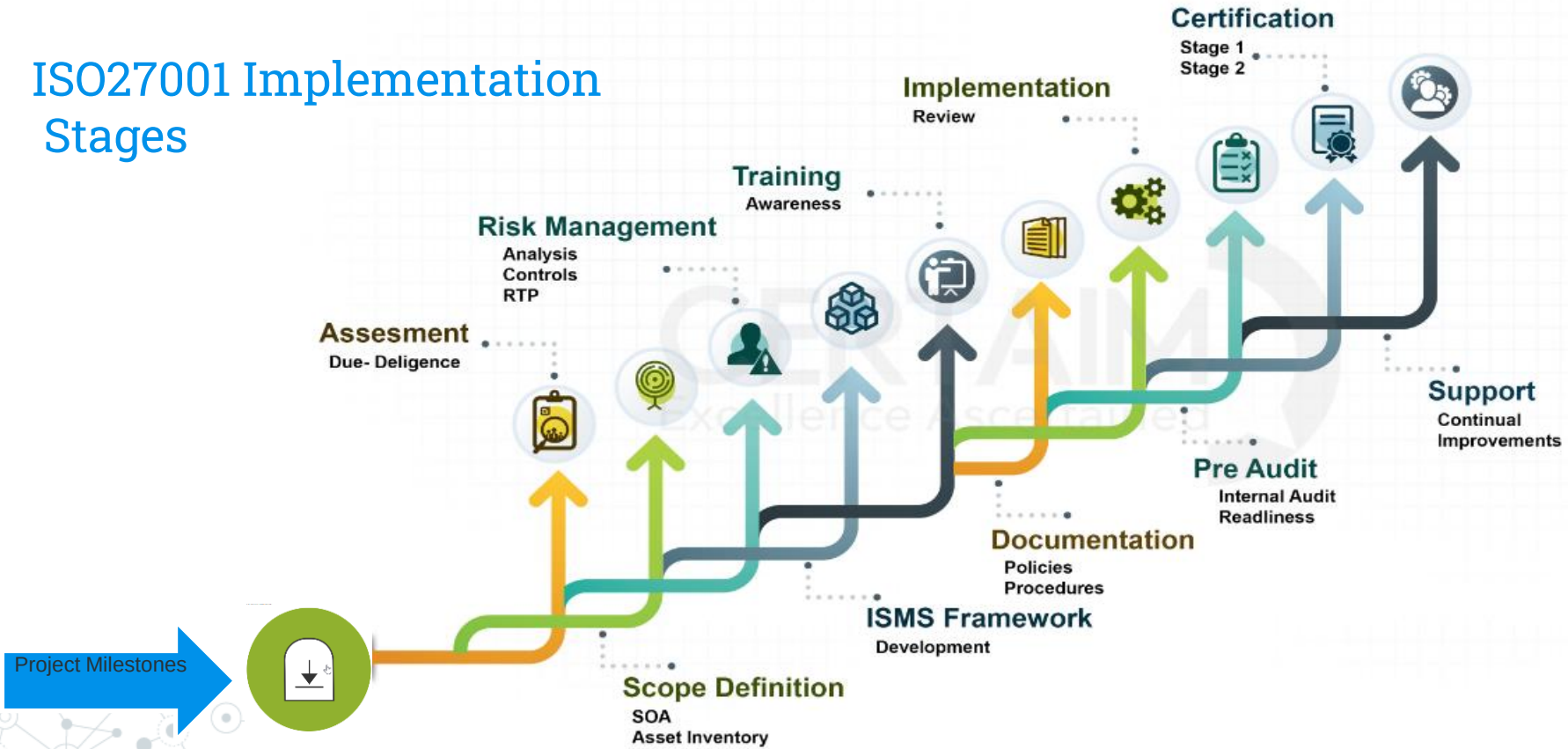


What is the benefit of ISO27001

ISMS Implementation - Mile stones

S.No.	Action item	Deliverables
1	Context & Scope	Information Security Scope Statement , context statement
2	Leadership	InfoSec management group , ISMS RACI Chart ,ISMS Policy
3	Planning	Information security Risk management Process , Statement of applicability
4	Support	ISMS Communication Chart ,ISMS Document management
5	operations	ISMS Manual ,Information Security Policies and procedures, Final Risk management Document Final Statement of Applicability
6	Performance monitoring	Information Security Objectives, Information Security matrices, Internal Audit ISMS Performance Monitoring
7	Improvement into ISMS	Corrective Action Plan, Closure of all internal audit NC, Management Review Meetings
8	Certification	Stage1 Audit & Stage2 Audit

ISO27001 Implementation Stages



ISMS Implementation - Mile stones

S.No.	Action item	Deliverables
1	Context & Scope	Information Security Scope Statement , context statement
2	Leadership	InfoSec management group , ISMS RACI Chart ,ISMS Policy
3	Planning	Information security Risk management Process , Statement of applicability
4	Support	ISMS Communication Chart ,ISMS Document management
5	operations	ISMS Manual ,Information Security Policies and procedures, Final Risk management Document Final Statement of Applicability
6	Performance monitoring	Information Security Objectives, Information Security matrices, Internal Audit ISMS Performance Monitoring
7	Improvement into ISMS	Corrective Action Plan, Closure of all internal audit NC, Management Review Meetings
8	Certification	Stage1 Audit & Stage2 Audit

Clause -1 | Scope

This document specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.

This document also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this document are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

Clause -2 | Normative references

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

Clause -3 | Terms and definitions

ISO Online browsing platform: available at https://www.iso.org/obp

IEC Electropedia: available at https:// www.electropedia .org/

ISO27001:2022

Clause -3 | Terms and definitions

Exercise-1

Term	
1. Base measure	
2. Audit scope	
3. Conformity	
4. Confidentiality	
5. Derived measure	
6. Decision criteria	
7. Event	
8. Record	
9. Risk	
10. Availability	
11. Risk communication and consultation	
12. Vulnerability	
13. Third party	
14. Threat	
15. Derived measure	

	Definition / Standard Terms
A	Person or body that is recognized as being independent of the parties involved, as concerns the issue in question.
B	Effect of uncertainty on objectives.
C	Continual and iterative processes that an organization conducts to provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management risk.
D	Occurrence or change of particular set of circumstances.
F	Property being accessible and usable by an authorized entity.
P	Property that information is not made available or disclosed to unauthorized individuals, entitles or processes.
G	Fulfillment of requirement.
K	Measure that is defined as a function of two or more values of base measures.
W	Extent and boundaries of an audit.
J	Potential cause of an unwanted incident, which may result in harm to a system or organization
M	Measure that is defined as a function of two more values of base measures.
I	Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature.
Z	Measure defined in terms of an attribute and the method for quantifying it.
N	Document stating result achieved or providing evidence of activities performed.
O	Weakness of an asset or control that can be exploited by one or more threats.

Exercise-2

ISO27001:2022

Auditing Information Security Principles

#	Management Principle	#	Management Principle	#	Management Principle
1	Awareness of the need for information security	2	Assignment of responsibility for information security	3	Incorporating management commitment and the interests of stakeholders
4	Enhancing societal values	5	Risk assessments determining appropriate controls to reach acceptable levels of risk	6	Security incorporated as an essential element of information networks and systems
7	Active prevention and detection of information security incidents;	8	Ensuring a comprehensive approach to information security management;	9	Continual reassessment of information security and making of modifications as appropriate

#	Scenario – Note > Some scenarios may demonstrate correct implementation of one or more principle(s) OR may be violating one or more principle(s).	Principle (Srl. #)
1	The Data Privacy policy of the organization focusses on giving respect to privacy of all the Interested Parties and mitigation of all risks for the same	
2	The process owners of the organization review their residual risks (as a disciplined activity) every six months and updates the approved residual risks	
3	Five delivery executives of the online shopping portal company, do not collect the identity of the person to whom delivery made, as per delivery policy & process	
4	The Housing Society declares a special Information Security awareness training to enhance the knowledge of the residents on the subject and give an idea of prioritization of risks – for the benefit of the residential colony member's benefit	
5	The school principal investigated the incident of the Artificial Intelligence examination paper of final year vanishing from his locker	
6	The Car rental company collects the identity of the person hiring car without driver and in one case of Ms Jene, did not collect the driving license	
7	The General Manager who also happens to be in Governance Board of the automotive company, wanted the R&D manager to give presentation on the new steering technology used for which the R&D Manager in the upcoming Tech. conference – the R&D manager refused to do so as per organization's risk assessment control of R&D department	
8	The Passenger lost his boarding pass after security clearance – wanted to go back to check-in counter to get the duplicate boarding pass – security personnel escorted to check-in counter to verify and ensure that this person is the same and boarding pass belongs to the same person	
9	Incident records in the DR server got corrupted… and the main server also went down. at the same time this was already identified an approved residual risk (low probability) that both might go down at the same time	
10	The incident details (including causes) were envisaged as new ones – updated into ISMS KEDB and Risk Assessments	
11	The traditional way of risk assessments in Excel is replaced by locally developed tool with Risk Assessments for C, I & A done separately, as part of Board decision taken	
12	The College has introduced an online training module for giving training on Information Security Management Systems (ISO 27001:2022) for benefit of college staff and students	
13	The Zonal Sales Manager recommended termination of the Sales Man as he stole the mobile of the Board Member visiting office for a meeting (left mobile on table before going to washroom) – entire incident was captured in CCTV	
14	The Business Continuity Plan includes testing of Encrypted Data Retrieval to ensure the Data Integrity reliability – risk assessment shows the approved residual risk of the failure of the De-encryption (low possibility)	
15	The organization does Gap Analysis towards GDPR compliance (as per Board Instructions) for the purpose complying to GDPR, if applicable to business	

Clause -4 | Context of the organization

4.1 Understanding the organization and its context

4.2 Understanding the needs and expectations of interested parties

4.3 Determining the scope of the information security management system

4.4 Information security management system

In order to understand the context of the organization you first need to identify the interested parties and once interested parties are identified we have to list down the internal and external issues.

Clause -4 | Context of the organization

4.1 Understanding the organization and its context

4.2 Understanding the needs and expectations of interested parties

In order to understand the context of the organization you first need to identify the interested parties and once interested parties are identified we have to list down the internal and external issues.

Clause -4 | Context of the organization

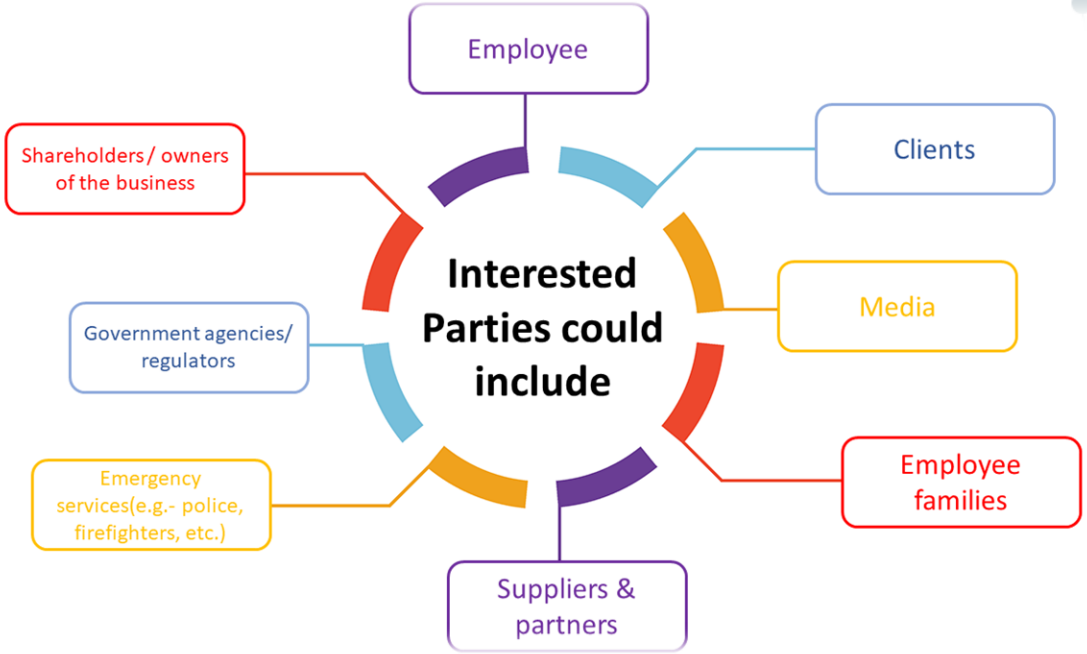
4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

a) interested parties that are relevant to the information security management system;

b) the relevant requirements of these interested parties;

c) which of these requirements will be addressed through the information security management system.



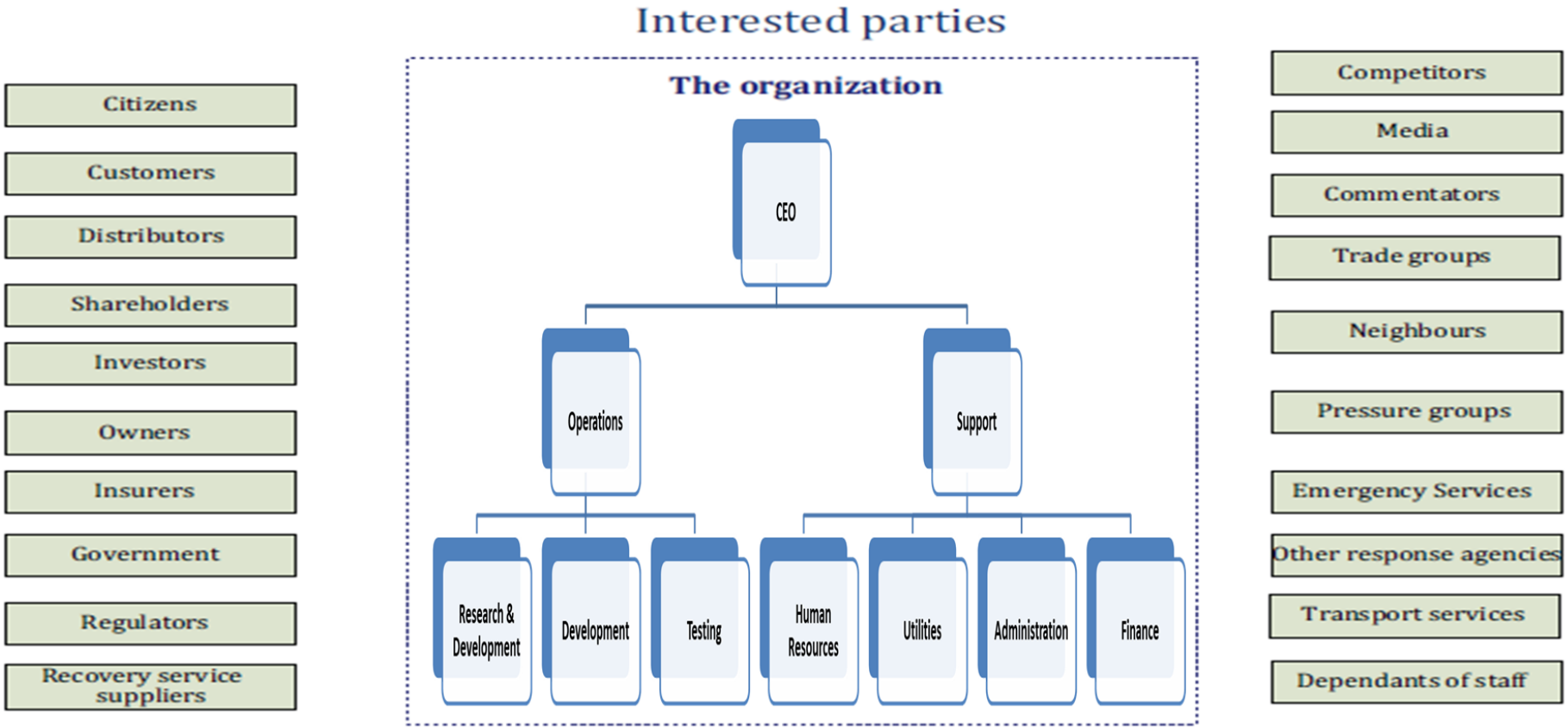
Clause -4 | Context of the organization

Exercise -3

External and Internal Issues – list down the external and internal issues consider you company as case study for ISO27001 implementation.

Clause -4 | Context of the organization

Exercise -3



Clause -4 | Context of the organization

4.1 Understanding the organization and its context

Information (Assets)	People	Organization	Product/Services	Systems/Process

ISO27001:2022

Clause -4 | Context of the organization

4.1 Understanding the organization and its context

1. **Organizational structure**. Knowing the roles, accountabilities, and hierarchy in the organization
2. **Organizational drivers**. The organization's values, mission, and vision, expressed in its internal culture, policies, objectives, and strategies, can help define its information security policies, objectives, and strategies.
3. **The way the organization does things**. Knowing how processes work (both isolated and interconnected), how information flows, and how decisions are made will make it easier to integrate information security processes and controls with business operations and management activities.
4. **Available resources**. Knowing what equipment, technologies, systems, capital, time, personnel, and knowledge you already have in your organization can help you guide your acquisitions, as well as the development not only of solutions, but also the competencies required to keep information secure
5. **Contractual relationships**. Understanding the relationships with suppliers and customers can allow an organization to include, in the **scope** of its ISMS, controls needed to better manage the customers and suppliers' requirements

ISO27001:2022

Clause -4 | Context of the organization

4.1 Understanding the organization and its context

1. **Organizational structure**. Knowing the roles, accountabilities, and hierarchy in the organization
2. **Organizational drivers**. The organization's values, mission, and vision, expressed in its internal culture, policies, objectives, and strategies, can help define its information security policies, objectives, and strategies.
3. **The way the organization does things**. Knowing how processes work (both isolated and interconnected), how information flows, and how decisions are made will make it easier to integrate information security processes and controls with business operations and management activities.
4. **Available resources**. Knowing what equipment, technologies, systems, capital, time, personnel, and knowledge you already have in your organization can help you guide your acquisitions, as well as the development not only of solutions, but also the competencies required to keep information secure
5. **Contractual relationships**. Understanding the relationships with suppliers and customers can allow an organization to include, in the **scope** of its ISMS, controls needed to better manage the customers and suppliers' requirements

Clause -4 | Context of the organization

Exercise -4

#	Interested Parties	Need & Expectations (Requirements)
1	Business Owners- INFOCUS-IT	• To Safeguard Confidential, Restricted and Internal information against unauthorized disclosure/Misuse. • Focus on continuous strengthening of information security strategies • The trade secrets should be kept limited to authorized personnel only • To ensure correct and secure operations of information processing facilities. • Business Facility protection against natural disasters, malicious attack or accidents • Compliance w.r.t. to all legal requirements as per the requirement of the standard ISO27001.
2	Employees	• Awareness of Information Security / ISO27001 for INFOCUS-IT • Resource availability to comply Information Security / ISO27001 INFOCUS-IT Policy • Privacy and protection of personally identifiable Information
3	Customers	• Information security aspects of business continuity management. • Management of information security incidents and improvements
4	Suppliers /Vendors / Service Providers	• Robust information security systems to support business transactions with supported Service Level Agreement.
5	Legal and Regulatory Bodies	• Complaisance of applicable Legal and Statutory guidelines/procedure.
6	Banking, financial Institutions & Business Forums	• To Avoid fraudulent nature of transactions and safeguard organization business data from cyber Breach

Clause -4 | Context of the organization

Exercise -4

List down interested parties

Clause -4 | Context of the organization

4.3 Determining the scope of the information security management system

The organization shall determine the boundaries and applicability of the information security

management system to establish its scope.

When determining this scope, the organization shall consider:

a) the external and internal issues referred to in 4.1;

b) the requirements referred to in 4.2;

c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.

The scope shall be available as documented information.

Clause -4 | Context of the organization

4.3 Determining the scope of the information security management system

Exercise -4

Write Scope statement

Clause -4 | Context of the organization

4.3 Determining the scope of the information security management system

Exercise -4

Write Scope statement

How Can we Help you

We Provide exclusive Risk Assessment Services to assist you with implementation of Information Security Practices into your organization

Risk Advisory Services

Third Party Risk Assessment

Gap Assessment Services

Cyber Security Audit & Consultancy Services

INFOCUS-IT | support@infocus-it.com | 91-8178210903

ISMS Part-II

27001

Ver.2022

ISO27001:2022 lead Implementor Course

By Jagbir Singh | jagbir@infocus-it.com

MTech(CS) | LLB |CISA | ISO27001LA |ISO22301LA|CEH|CHFI