ISO / IEC 27001:2022 Lead Implementer Course – Expert Guide

ISO 27001 Lead Implementer Certification does not only apply to information security. All the policies and controls under this standard are given to the whole organization. Hence, they can serve all the departments.

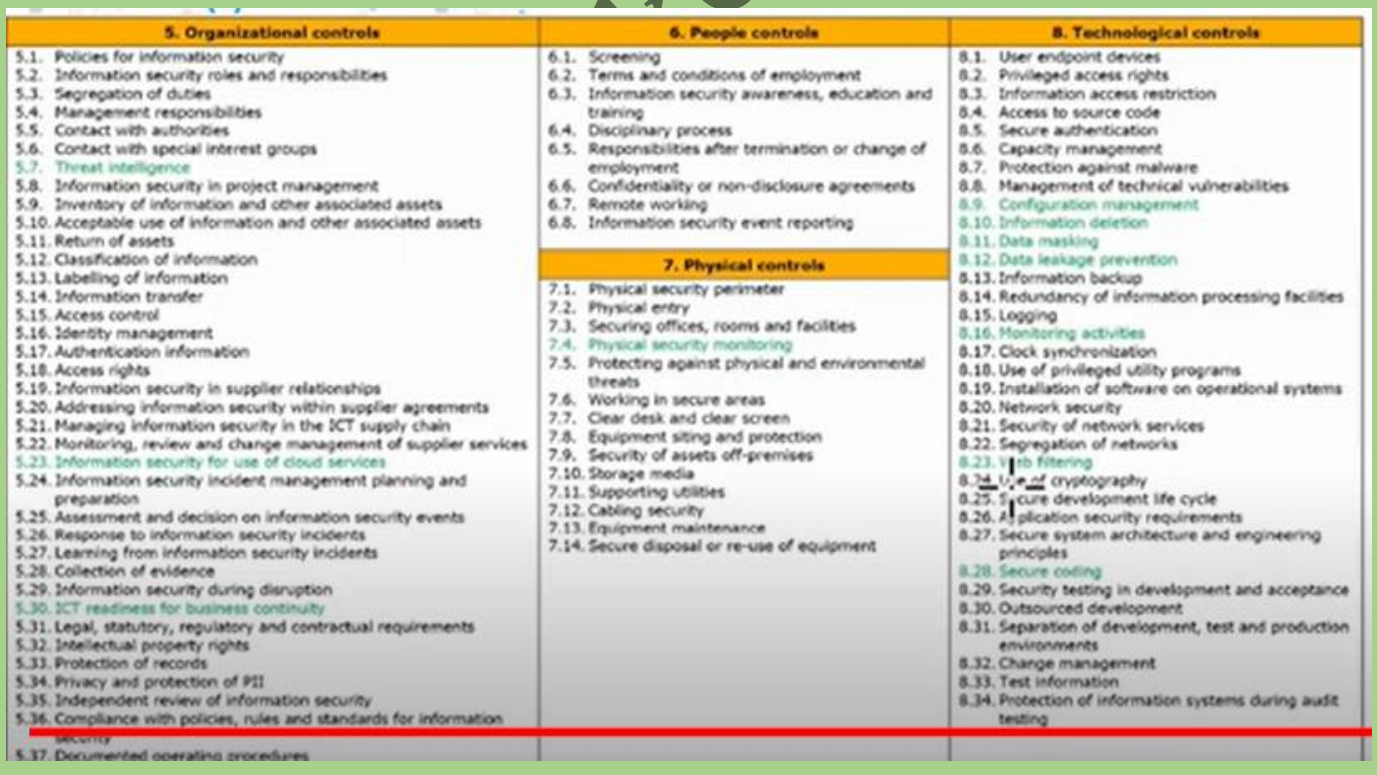
Exercise A:

Notes:

Annexure A policies and Controls, were 14 in ISO / IEC 27001:2013 in the older version. Currently, in the newly updated version, they are divided into 4 domains:

- People controls
- Physical controls
- Technological controls
- Organizational controls

Latest Annexure A Version ISO/IEC 27001:2022



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		8.9. Configuration management
5.10. Acceptable use of information and other associated assets	**7. Physical controls**	8.10. Information deletion
5.11. Return of assets	7.1. Physical security perimeter	8.11. Data masking
5.12. Classification of information	7.2. Physical entry	8.12. Data leakage prevention
5.13. Labelling of information	7.3. Securing offices, rooms and facilities	8.13. Information backup
5.14. Information transfer	7.4. Physical security monitoring	8.14. Redundancy of information processing facilities
5.15. Access control	7.5. Protecting against physical and environmental threats	8.15. Logging
5.16. Identity management	7.6. Working in secure areas	8.16. Monitoring activities
5.17. Authentication information	7.7. Clear desk and clear screen	8.17. Clock synchronization
5.18. Access rights	7.8. Equipment siting and protection	8.18. Use of privileged utility programs
5.19. Information security in supplier relationships	7.9. Security of assets off-premises	8.19. Installation of software on operational systems
5.20. Addressing information security within supplier agreements	7.10. Storage media	8.20. Network security
5.21. Managing information security in the ICT supply chain	7.11. Supporting utilities	8.21. Security of network services
5.22. Monitoring, review and change management of supplier services	7.12. Cabling security	8.22. Segregation of networks
5.23. Information security for use of cloud services	7.13. Equipment maintenance	8.23. Web filtering
5.24. Information security incident management planning and preparation	7.14. Secure disposal or re-use of equipment	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		

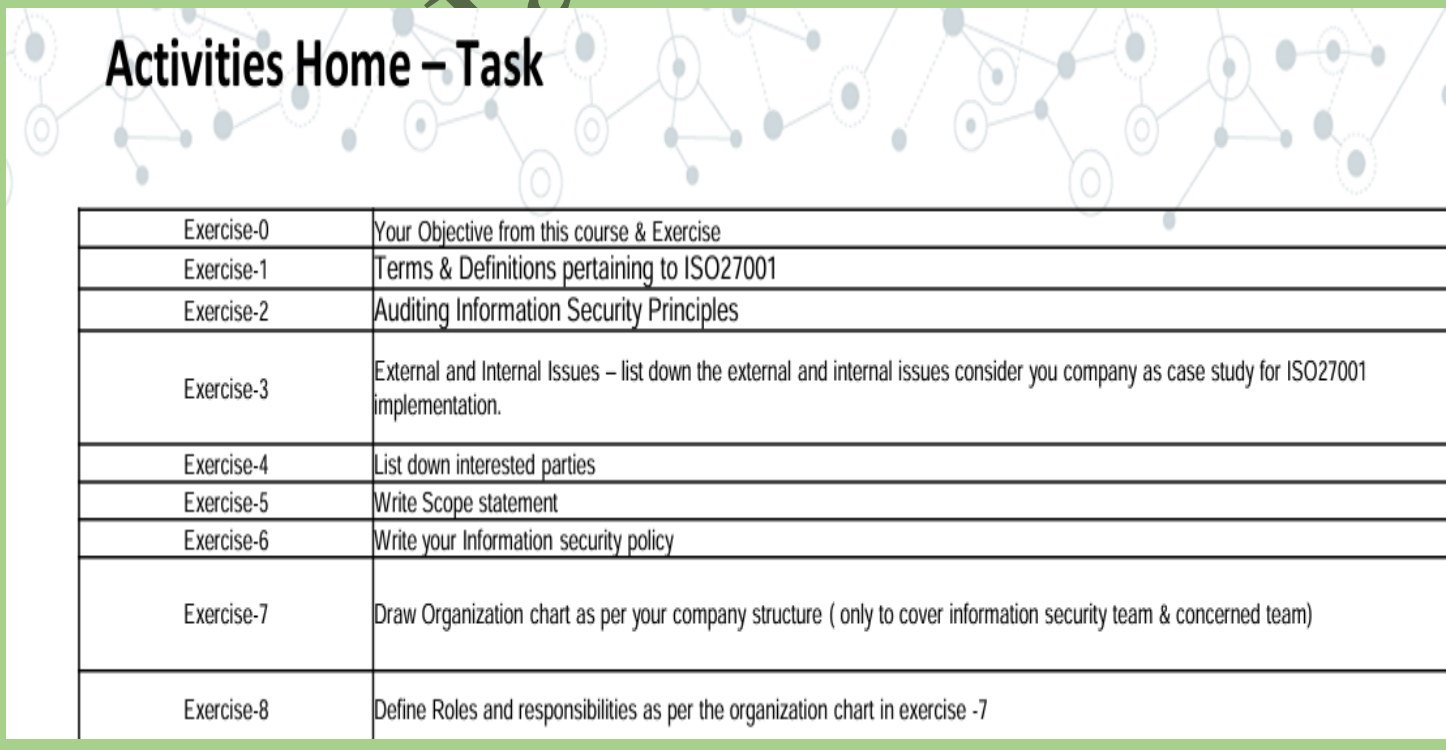
Exercise:

1. Go through the entire Annex A policies Version ISO/IEC 27001:2022 and digest the domains, then take a blank piece of a white paper, write (by-hand) everything that you can remember. Do not copy or review; trust your memory.
2. This helps your memory to lay a foundation and a framework for the course content. (Remember to include your full name and active email at the top of your paper)
3. Take a clear snapshot of the paper, create a folder on Google Drive 'ISO 27001:2022 Lead' and save the snapshot.
4. Send me the link to access the snapshot file on your Google drive via Facebook Messenger.
5. Facebook link: facebook.com/profile.php?id=61556175711538

   Follow me on my social media platforms to learn more about ISO / IEC 2700:2022 via my posts:

- Quora: quora.com/profile/The-Cyber-Hackers-Diary
- Pinterest: pinterest.com/hackersdiary
- YouTube: www.youtube.com/@CyberHackersDiary
- LinkedIn: linkedin.com/in/john-kimani-13831329b
- Facebook: facebook.com/profile.php?id=61556175711538

Part 1:



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

Introduction to ISO / IEC 27001:2022

- ISO -International Organization for Standards
- IEC - International Electrotechnical Commission
- ISO 27001:2022 is built in conjunction with IEC, with an aim to tackle information security
- ISO 27001:2022 - Information Security, Cyber Security and Privacy Protection, Information Security and Management Systems

ISO 27001:2022 Framework & it's purpose:

- ISO 27001:2022 outlines policies and strategies that enhance information security in an organization.
- It provides a framework through which policies and strategies can be exercised systematically and in a cost-effective manner
- It can serve different departments: Sales Dept., Finance Dept., ICT Dept.,
- The framework can handle any business size and location

ISO 27001 Document:

- The document entails the processes in which the strategies and policies can be established, implemented, maintained and continually improved
- It answers: what to do? when to do? how to do?

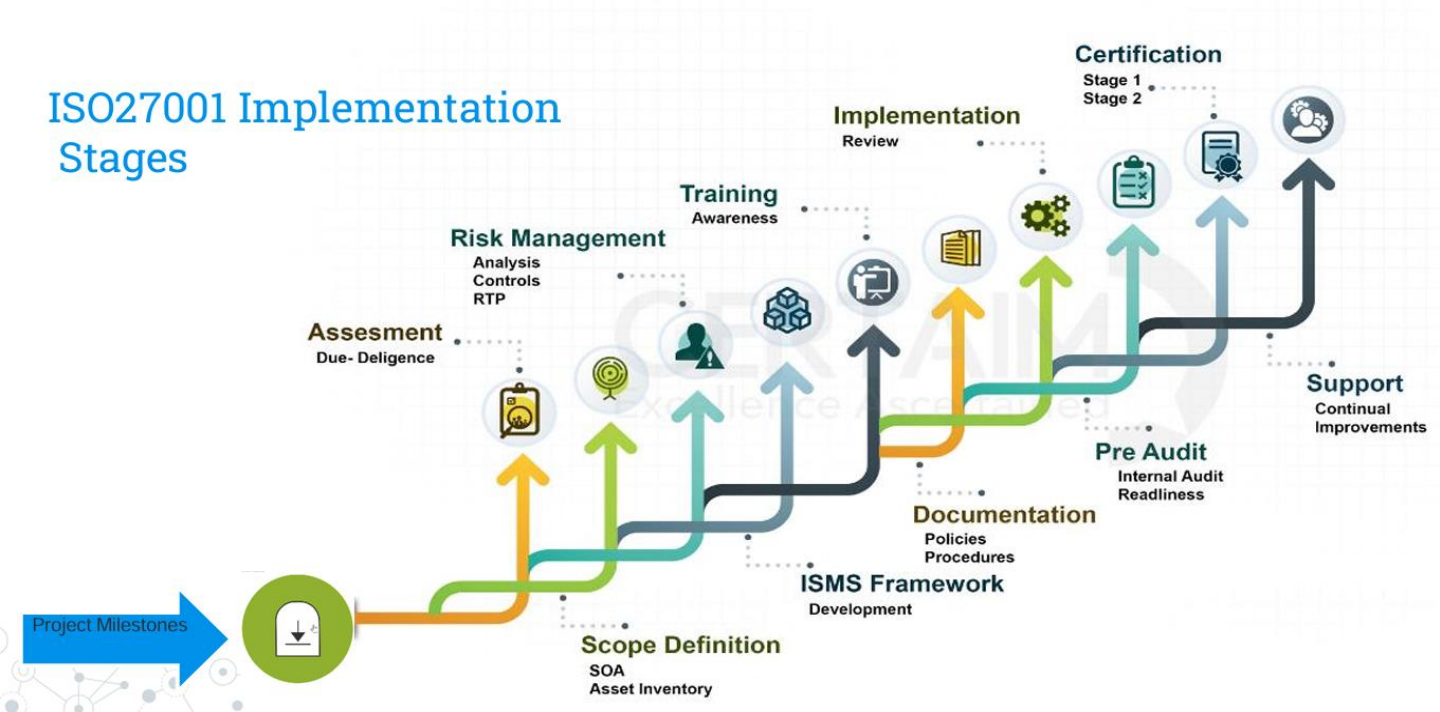
Goals for ISO 27001:

- Confidentiality: Information should be accessible to only authorized persons
- Integrity: Only the authorized persons can change the information
- Availability: Information should be conveniently accessible to authorized persons whenever they need it

Benefits of ISO 27001:

- Reduces the chances of security breaches within your organization
- Control of IT risks
- Lower costs
- Systematic detection of vulnerabilities
- Fulfillment of internationally recognized requirements
- A structured method to address compliance requirements
- Increase in trust with respect to partners, customers and public
- Competitive edge due to recognized standards
- Minimization of IT risks, potential damage and consequential costs
- Confidentiality of Information

ISO 27OO1 Implementation Stages:



As an ISO 27001 Lead Implementer your major role is going to involve:

- Documentation - Processes, strategies and policies
- Pushing the documentation to the whole team in the organization
- Conducting security awareness to the organization
- Internal auditing - checking if the implementation was done correctly. Any gaps can be filled at this point

Welcoming the certification body for auditing and certification (external auditors)

- Stage 1 auditing: They are going to check the documentation and the internal auditing to determine if the organization is in line with ISO 27001 standard. If it has gaps then they will classify it as non-conformity. If it has no gaps, it will be classified as Conformity and can be pushed to the next stage:
- Stage 2 auditing: They are going to check Risk Management, Assessment, scope and documentation
- As a Lead Implementer it is not all about documentation, you have to do everything. This includes showing continuous improvement through offering Awareness training
- You will keep records for the training for stage 2 auditing evidence
- After stage 2, the organization will be awarded with an ISO 27001 certification
- For Auditing standards in ISO 27001, you can refer to ISO 19011: auditing management systems effectively, principles of auditing, managing auditing programs and conducting audits

ISO 27001 Vs ISO 27002:

- ISO 27001: Gives the auditing requirements
- ISO 27002: Gives the implementation guidance of Annexure controls

Clause 1: Scope

- This document specifies the requirements for establishing, implementing, maintaining and continually improving Information Security Management Systems in an organization
- The requirements are generic and can be applied in any organization, regarless of size, location, type or nature

Clause 2: Normative References

ISO 27001 (Overview and vocabulary):

- Information Technology
- Security Techniques
- Information Security Management Systems

Clause 3: Terms and definitions

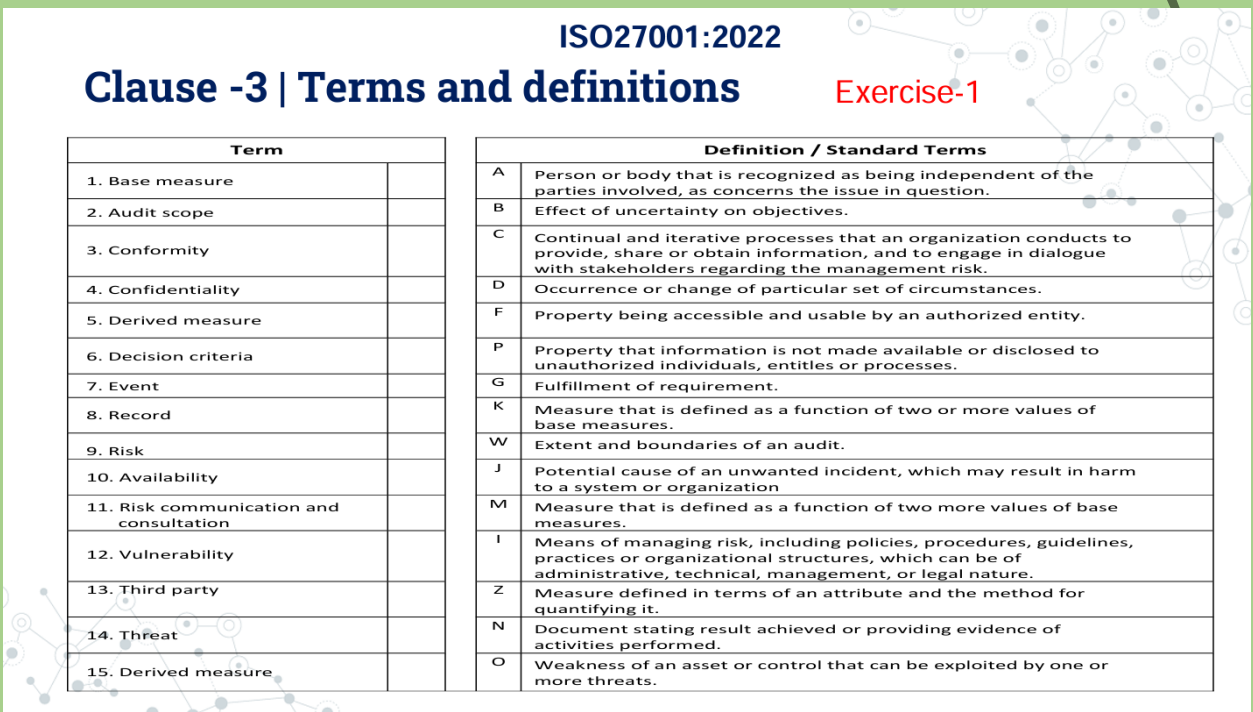
Refer to:

- ISO Online Browsing platform
- IEC Electropedia

Exercise 1:

Instructions:

- We have two categories in this exercise:
- Terms (1-15)
- Definition / Standard terms (A-O)
- Match the Definitions / Standards with the term that suits best



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:

Instructions:

- We have two categories in this exercise:
- Management principle(s) (1-9)
- Case scenarios (1-15)
- Match the case scenario with the management principles that suits best
- **N:B** Management Principle(s) can apply in more than one scenario

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 expectation of interested parties

4.3: Understanding the scope of Information Management Systems (ISMS)

4.4: Information Security Management (ISMS)

Notes:

- In CL 4 we need first to understand the needs and expectation of the interested parties (Sub-CL 4.2).
- The interested parties involve of who is gaining? (Employees, vendors, suppliers). So, we need to create a list
- Then, we need to Identify their needs and expectations (What they expect from ISO 27001:2022)
- We need to think practically, Its practical work
- In Sub-CL 4.1 we need to understand the context of the organization. (@ Exercise 3).
- Context means the requirement from the ISO 27001:
- (information / Assets), people, organization, product / services), systems / processes).

N:B CL 4 is very important. It will help you understand the whole organization

ISO27001:2022

Clause -4 | Context of the organization

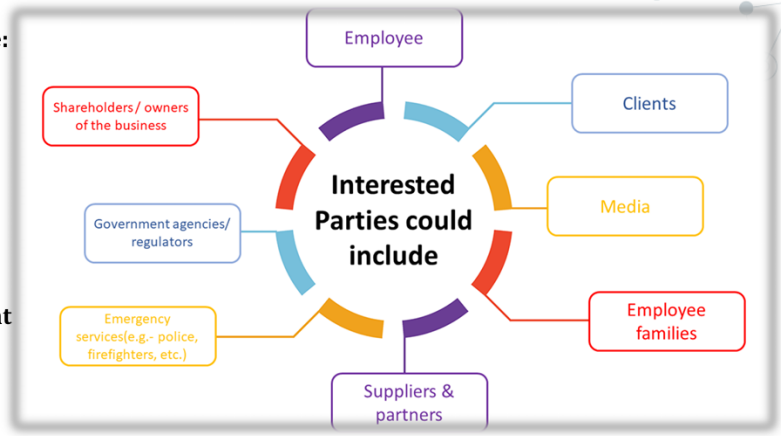
4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

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

b) the relevant requirements of these interested parties;

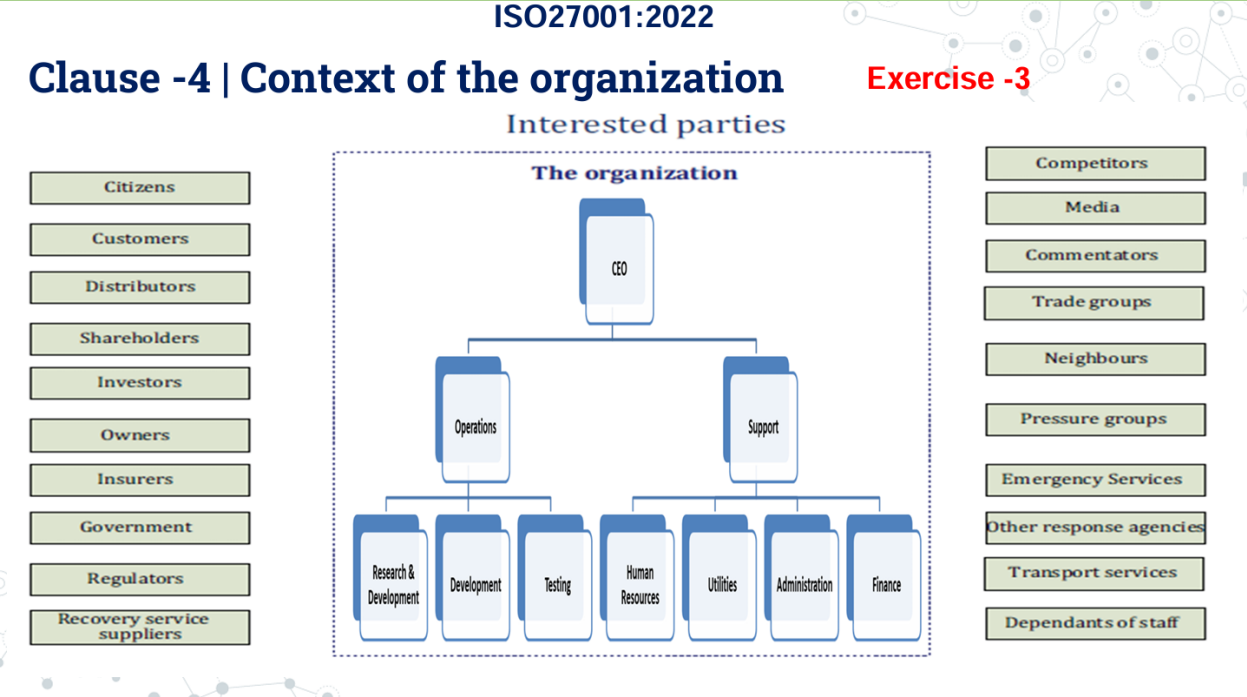
c) which of these requirements will be addressed through the information security management system.



Exercise 3:

Instructions:

- List down the interested parties
- List down their issues based on ISO 27001:2022
- Consider your company as a case study for ISO 27001:2022 implementation
- This exercise is complex and can take weeks



Exercise 4:

Activity A Instructions:

- From the sample below; create your own list (Interested parties / needs & expectations)
- Consider your company as a case study for ISO 27001:2022 implementation

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

Activity B Instructions:

- Fill in the table below
- Considering your company as a case study for ISO 27001:2022 implementation

Clause -4 | Context of the organization

4.1 Understanding the organization and its context

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

Notes Cont.

Sub-CL 4.3; When determining the scope of the Information Management System (ISMS), the organization shall consider:

- The internal and external issues referred to in sub-CL 4.1
- The requirements referred to in sub-CL 4.2
- Interfaces and dependencies between activities performed by other organizations
- The scope will be available as a documented information

Exercise 5:

Instructions:

- Develop a scope of statement
- Considering your company as a case study for ISO 27001:2022 implementation

Exercise 6:

Instructions:

- Write your Information Security Policy
- Considering your company as a case study for ISO 27001:2022 implementation

Exercise 7:

Instructions:

- Draw Organization chart as per your company structure (only to cover information security team & concerned team)
- Considering your company as a case study for ISO 27001:2022 implementation

Exercise 8:

Instructions:

- Define Roles and responsibilities as per the organization chart in exercise -7
- Considering your company as a case study for ISO 27001:2022 implementation