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

Clause 7 Support:

7.1 Resources

7.2 Competence

7.3 Awareness

7.4 Communication

7.5 Documented information

7.1 Resources:

It is the responsibility of the Leadership entity (C- management) within the organization to ensure that the resources are available

These resources include:

- Humans i.e. employees, vendors
- Process i.e. Intellectual property, policies
- Technology; softwares, Servers, cloud, machines
- Organizations: Roles and Responsibilities

7.2 Competence:

- It may include experience, appropriate education, training
- It is vital to keep up-to-date with emerging advancements to ensure effective competence
- It is vital to ensure trainings: Seminars, in-house virtual training
- The HR is responsible for competence evaluation
- If there is an additional role is given, then it is essential to determine that the person is competent

Exercise 16:

- Title: Resources and Competence matrix
- Make a list of Resources required for ISMS and what qualifications they need to possess. They will be part of information security working group

7.3: Awareness

1) Every person working in the organization shall;

- be conversant with the security policies
- work with a cause for making the ISMS effective and maybe receive any benefits that comes with this
- face consequences if they fail to adhere to the security policy put into place

2) Awareness within an organization can be achieved by using:

- Do's and Dont's posters
- Information security awareness
- Awareness posters
- Quiz mailers

3) In case of a new employee, it is the duty of the HR to ensure that the policies are communicated to the new joinee; in the induction / orientation

4) It is the duty of the HR to offer trainings to the employees (monthly, quarterly); via simulations, quiz mailers. Also offer awards within the trainings for active contributors

5) It is essential to make a list of training records, calendars (for scheduling)

6) External auditors can be invited to ensure appropriate competence

7.4 Communication

Whenever you are communicating you should ensure that confidentiality and integrity is well conveyed

It is vital to create a communication matrix that entails:

- What to communicate
- When to communicate
- With whom to communicate to
- How to communicate

In your communication plan you should have the following:

- Communication plan
- Quick contact list
- Emergency list

You need to make a document named: Communication Plan (Process & policy)

7.5 Documented Information

7.5.1 General

All the documents should be approved by the top management

7.5.2 creating and updating

1) When creating a document, it shall ensure appropriate:

2) Identification and description (Title, date, author, reference number)

3) Format (language, graphics, software version) and media (paper, electronics)

4) Review and approval for suitability and adequency

5) It should be a live document that contains:

Document Statistics

Type Of Information	Document Data
Document Title	
Document Code	
Date of Last Release	
Document Validity	
Document Revision No	
Document Owner	
Document Reviewer	
Document Distribution List	
Security Classification	
Document Status	
Document Disposal Date	7 years from the Date of last release
Document Disposal Method	For Printed Format: Shred For Digital Format: Secure Delete

Document Change Control

Version #	Prepared By	Approved By	Approved On	Changes/ Amendments

7.5.3 Control of documented information

1) The document should be convenient for use

2) The document should be protected (confidential)

3) The following should be addressed:

- Distribution access, retrieval and use
- Storage and preservation
- Control of changes
- Retention and disposition

4) To protect the document from unauthorized access we can use classification of documents:

- Public (Newspapers, Websites) - Lacks confidentiality & Integrity
- Confidential
- Internal (Organization circulars)
- Restricted
- Super-restricted (requires special permission)

NB: Have a policy of classification and the treatment methods

Exercise 17:

- Create a policy and a process of document control
- Considering your company as a case study for ISO 27001:2022 implementation

Exercise 18:

- Create a communication plan
- Considering your company as a case study for ISO 27001:2022 implementation

Clause 8 Operations:

8.1: Operational planning and control

8.2: Information security risk assessment

8.3: Information security risk assessment

8.1 Operational Planning and control

1) The organization shall implement the actions in clause 6 via:

- Establishing the criteria for the processes
- Implementing the controls for the processes according to the criteria (Reffer to ISO 27002 Annexure A controls)

2) The implementation for controls is contained in ISO 27002

3) Make a progress document

8:2 Information security risk Assessment

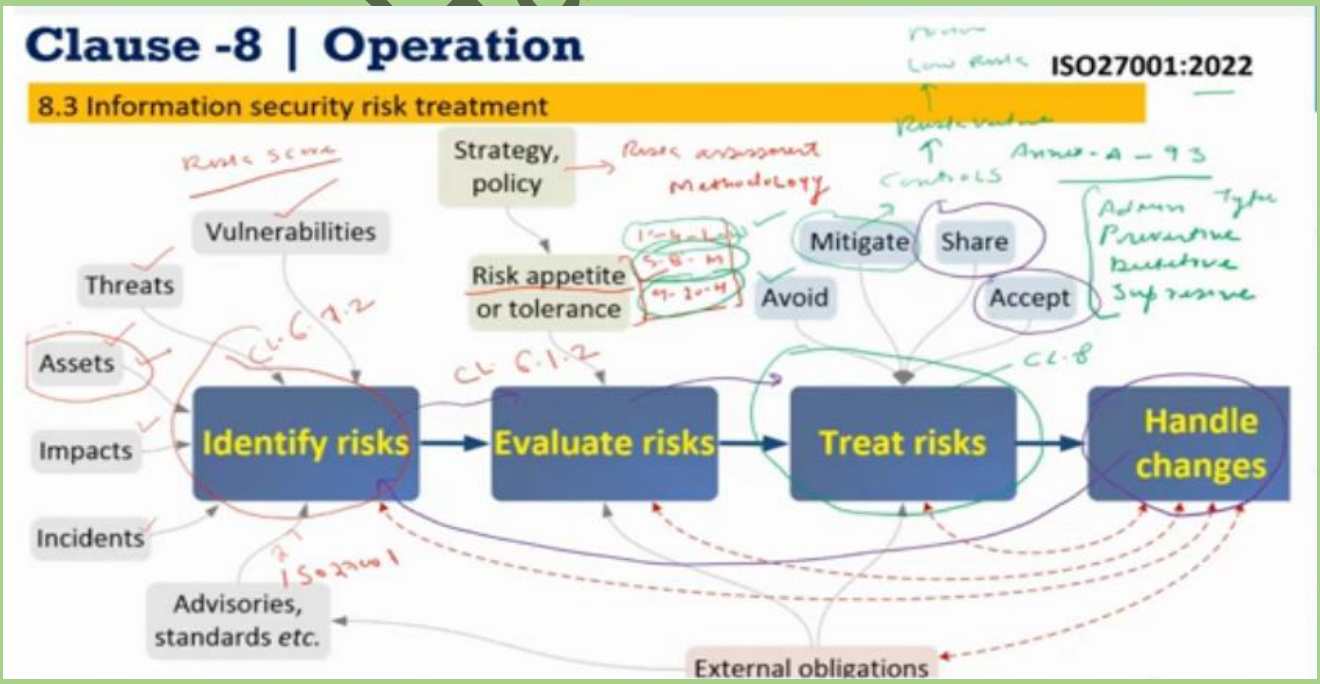
- The organization shall perform risk assessment at intervals or when significant changes occur
- The results of the risk assessment should be archived

8.3: Information Risk Treatment

Upon risk Identifications you can perform the following actions:

- Avoid the risk
- Mitigate the risk
- Share the risk - Third party (Insurance company)
- Acceptance - Going head-on

NB: Risk can never be 100 % eradicated Hence the residual risk requires later on security controls



Exercise 19:

- Prepare a Risk Treatment Plan
- Consider first writing the risk methodology and combine it with the risk treatment
- Considering your company as a case study for ISO 27001:2022 implementation

Exercise 20:

Create a Statement of Applicability (SOA) for your organization

Considering your company as a case study for ISO 27001:2022 implementation