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

Clause 9 Performance Evaluation:

9.1 Monitoring, measurement, analysis, evaluation

9.2 Internal audit

9.3 Management review

Monitoring, measurement, analysis and evaluation

The organization shall determine:

- When the monitoring and measurement shall be conducted
- The methods for monitoring, measuring analysis and evaluation
- What needs to be measured or monitored
- Who shall monitor and measure
- When the results for measuring and monitoring shall
- Who shall evaluate and analyze the results

N:B Documented information shall be available as evidence of the results

9.2 Internal Audit

9.2.1 General

1) The organization shall conduct internal audits within the stipulated intervals to determine it the Information security management systems conforms to:

- The organization's own requirements for its information security management
- The requirement of this document (Internal audit policy)

NB: The internal audit policy should be concise

2) Also, within the internal audit the organization shall determine if the internal audit is implemented and maintained

3) There is a need for internal audit training:

- Pick internal auditors from every department
- Train the internal auditors and this forms the basis of human resource competence

- You can hire external auditors to make sure that the internal audits meet the requirements for certification

4) Audit is all about judging something: is it wrong, or right? The following is the criteria:

- ISMS standard (ISO 27001: 2022)
- Interested party requirements
- ISMS documents
- Legal requirements

9.2.2 General

The organization shall

- Plan, establish, implement, maintain an audit programme (s), including the frequency, methods, responsibilities, planning requirements and methods
- Define the audit criteria and scope for each audit
- Ensure that the audit results are reported to the right management

NB: The documented information shall be available as evidence of implementation

Exercise 21:

Define an Internal audit schedule

Exercise 22:

- Make a document where you will be giving your own internal audit training
- Stick to the requirement that are only required for that function
- E.g. If you are giving training to the technical team just stick to that
- Be selective to the group functions

Exercise 23:

- Develop an Internal audit process
- Make sure to include the positive outcomes

9.3 Management Review

9.3.1 General

The top management shall review the organization's Information Security Management Systems (ISMS) at the stipulated intervals to ensure its continuing suitability adequacy and effectiveness

Exercise 24:

Develop a management Review process

9.3.2 General

The management review shall include consideration of:

- Actions from the previous management review
- External and internal issues that are relevant to Information Security Management Systems (ISMS)
- Changes and needs of the interested parties that are relevant to the Information Security Management Systems (ISMS)
- Changes in information security measures including:
- Non conformities and corrective actions
- Monitoring and measurement results
- Audit results
- Fulfillment of information security objectives
- Feedback from interested parties
- Results from risk assessment and status of the risk assessment
- Opportunities for continual improvement

9.3.3 Management Review Results

- The results for the management review shall contain decisions made towards opportunities for continual improvement and needs for change in Information Security Management Systems (ISMS)
- The results should be documented as evidence management review

Exercise 25:

Corrective actions Process Management Review Process

Clause 10 Improvement:

10.1 Continual Improvement

Ther organization shall keep improving the suitability, adequacy and effectiveness of Information Security Management System

10.2 Non conformity and corrective actions

After the internal audits has been pushed to the external or internal auditors there might be some non-conformities and therefore, this prompts:

- Reaction: whether the accept it or not
- corrective actions and control
- Dealing with the consequences

Address the non-conformities in a way that it does not occur or re-occur and this can be achieved by:

- Reviewing the non-conformity
- Determining the cause of the non-conformity
- Determining if there are similar non-conformity or if they possess a potential to occur
- Implementing any need action
- Reviewing the effectiveness of the corrective actions taken
- Making changes to the Information Security Management system
- Assessing the nature of the non-conformities and any corrective actions taken
- Checking results of any non-conformity actions taken