ISO 27001 RISK MANAGEMENT TRAINING

Certificate of Completion in ISO 27001 Risk Management Training

Course Code: M025/25

Duration: 16 Hours

Delivery Format: Hybrid

Target Audience:

- Top and Middle Management
- Organisation's selected Internal Auditors
- BCM Professionals (IT Officers, etc.) seeking to enhance their knowledge in BCMS.
- Executives seeking to implement BCMS in their organization
- IT and Non-IT Professionals who are interested to learn more about BCMS and its importance.

Program Outcomes:

Upon completion of this program, participants will be able to:

- Refresh their basic knowledge of ISO 22301:2019 and risk management skills.
- Have the proper attitudes in approaching Risk Assessment based on ISO 22301:2019.
- Be more than ready to take on the role and responsibilities of a Business Continuity Assessor, resulting in effective and efficient ISO 22301:2019 Risk mitigation skills.
- Gain "Hands-on" experience in Risk Assessment through a practical live workshop.

Detailed Syllabus

Module 1: Overview of Risk Management

Outcome: Participants will understand the basic concepts of risk management, the process model approach, ISO 31000 requirements, the integration with ISO 22301, and how risk treatment fits into business processes.

Topics:
- Understand the Basic Concepts of Risk Management based on ISO 31000
- Understand the process model approach to risk assessment
- Understanding ISO 31000 requirements in brief and integration with ISO 22301
- Understanding where risk and risk treatment sits into your business

Activities:
- Process-based risk assessment practicals.
- Exercises involving group activities and discussions.

Assessments:
- Implicitly assessed through participation in practical exercises and group discussions.

Module 2: Introduction to SWOT, PESTLE & FMEA Methodology

Outcome: Participants will understand the definitions, history, purpose, inputs, and outputs of SWOT, PESTLE, and FMEA methodologies and how technology can be used to assess risks.

Topics:
- Definition
- History and Purpose
- Inputs and Outputs
- How Technology to use the tool to assess risks

Activities:
- Exercises applying these methodologies.

Assessments:
- Implicitly assessed through participation in exercises.

Module 3: FMEA Methodology in Operational Risk Assessment

Outcome: Participants will be able to define failure modes, identify potential failure modes and effects, rate severity and occurrence, identify controls, assess risk using the Risk Profile Number (RPN), develop mitigation and contingency plans, assign responsibility, and manage risk through follow-up and re-evaluation.

Topics:
- Definition and Categories of Failure Modes
- Identifying Potential Failure Modes at Each Process Step
- Analyse Potential Failure Effects
- Rating Severity - Severity Rating Definition
- Determining Probable Causes
- Methods and Guidelines for Determining Causes
- Rating Occurrences - Occurrence Rating Definition
- Identifying Controls
- Type of Controls
- Rating Detection
- Assessing Risk
- The Risk Profile Number (RPN)
- Develop Mitigation and Contigency Plan
- Assign Responsibility
- Follow-Up and Re-Evaluation
- Manage the Risk

Activities:
- Detailed explanation and application of the FMEA process.

Assessments:
- Implicitly assessed through understanding and application of the methodology.

Module 4: Overview of Risk control process & Contingency planning in daily operations

Outcome: Participants will understand the risk control process and how to implement contingency planning in daily operations, including setting goals and core values/principles as controls.

Topics:

- Setting Goals and Core Values/Principles as controls

Activities:

- Discussions and explanations.

Assessments:

- Implicitly assessed through participation in discussions.

Module 5: Risks in Quality & Service delivery

Outcome: Participants will be able to identify policy risks, objectives risks, compliance risks, and conduct a Business Impact Analysis (BIA).

Topics:

- Policy risks
- Objectives risks
- Compliance risks
- Business Impact Analysis (BIA)

Activities:

- Group activity and exercises.

Assessments:

- Group activity output.

Module 6: Steps in planning for redundancy, recovery, restoration, and resumption

Outcome: Participants will understand the steps involved in planning for business continuity, including records and documentation requirements.

Topics:

- Records and documentation to be maintained during and after a crisis

Activities:

- Explanation of the steps and documentation.

Assessments:

- Implicitly assessed through understanding and discussion.