MTBM

ISO/IEC 27001 RISK ASSESSMENT TRAINING

REGISTERED HRD CORP TRAINING PROVIDER

HRD CORP CLAIMABLE

Course Title: ISO/IEC 27001 Risk Assessment Training

Course Validity: 2 Days

Validity: Not Applicable

HRD Corp Scheme: Claimable

INTRODUCTION

This training provides participants with a comprehensive and practical understanding of information security risk assessment as required under ISO/IEC 27001. The course explains how to identify, analyse and evaluate risks that threaten the confidentiality, integrity and availability of organisational information assets. Participants will learn the complete risk assessment workflow, beginning with asset identification, threat and vulnerability analysis, impact evaluation, likelihood assessment, risk rating and risk prioritisation. Through practical examples, risk scenario exercises and hands-on workshops, participants will gain the competence to conduct structured, repeatable and evidence-based risk assessments that strengthen ISMS implementation, support compliance obligations and enhance overall information security posture.

OBJECTIVE(S):

- Understand ISO/IEC 27001 risk assessment and treatment requirements.
- Learn how to identify information assets, threats and vulnerabilities.
- Establish risk criteria aligned with organisational context.
- Conduct qualitative or semi-quantitative risk assessments.
- Determine risk likelihood, impact and overall risk levels.
- Select and justify risk treatment options linked to Annex A controls.
- Develop risk registers and risk treatment plans.
- Strengthen ISMS risk management and audit readiness.

TARGET GROUP(S):

- Information security officers
- IT managers and cybersecurity personnel
- Risk management and compliance teams
- Internal auditors and ISO coordinators
- System administrators and network engineers
- Anyone involved in ISMS development or security governance

ENTRY REQUIREMENT(S):

- Able to read, write and communicate verbally in Malay/English

TOPIC(S):

1. Introduction to Information Security Risk Management
2. ISO/IEC 27001 Risk Assessment and Treatment Requirements
3. Asset Identification, Classification and Ownership
4. Threat and Vulnerability Identification Techniques
5. Establishing Likelihood, Impact and Risk Criteria
6. Conducting Risk Assessment and Prioritisation
7. Selecting Risk Treatment Options and Linking to Annex A Controls
8. Developing Risk Registers, Treatment Plans and Monitoring Activities

LIST OF REFERENCE BOOK(S):

- ISO/IEC 27001: Information Security Management Systems
- ISO/IEC 27002: Information Security Controls
- ISO 31000: Risk Management Guidelines

LIST OF TEACHING AID(S):

- LCD projector
- Computer
- Whiteboard with accessories
- Flip chart with accessories
- Risk register templates and security assessment worksheets

METHODOLOGY(S):

- Lecture
- Group discussions
- Case studies
- Practical risk assessment workshops
- Scenario-based activities

TRAINING SCHEDULE

Day 1

Time	Activity / Topic
8:30 am – 9:00 am	Registration and Introduction
9:00 am – 10:15 am	Topic 1: Introduction to Information Security Risk Management
10:15 am – 10:30 am	**Morning Tea Break**
10:30 am – 12:30 pm	Topic 2: ISO/IEC 27001 Risk Assessment and Treatment Requirements
12:30 pm – 1:30 pm	**Lunch Break**
1:30 pm – 3:30 pm	Topic 3: Asset Identification, Classification and Ownership
3:30 pm – 3:45 pm	**Afternoon Tea Break**
3:45 pm – 5:00 pm	Topic 4: Threat and Vulnerability Identification Techniques

TRAINING SCHEDULE

Day 2

Time	Activity / Topic
8:30 am – 9:00 am	Recap of Day 1
9:00 am – 10:15 am	Topic 5: Establishing Likelihood, Impact and Risk Criteria
10:15 am – 10:30 am	**Morning Tea Break**
10:30 am – 12:30 pm	Topic 6: Conducting Risk Assessment and Prioritisation
12:30 pm – 1:30 pm	**Lunch Break**
1:30 pm – 3:30 pm	Topic 7: Selecting Risk Treatment Options and Annex A Mapping
3:30 pm – 3:45 pm	**Afternoon Tea Break**
3:45 pm – 5:00 pm	Topic 8: Developing Risk Registers, Treatment Plans and Monitoring