ISO/IEC 27001 CLIMATE CHANGE AMENDMENT INTEGRATION TRAINING

Course Title: ISO/IEC 27001 Climate Change Amendment Integration Training

Course Validity: 2 Days

Validity: Not Applicable

HRD Corp Scheme: Claimable

INTRODUCTION

This training provides participants with a structured understanding of the ISO/IEC 27001:2022 Climate Change Amendment and how it integrates into an organisation's Information Security Management System (ISMS). The amendment introduces new expectations for identifying, assessing and managing climate change–related threats that may affect information security, operational resilience and continuity of critical information assets. Participants will learn how to update ISMS documentation, incorporate climate considerations into risk assessments, strengthen supplier and infrastructure planning, and ensure readiness for certification audits.

OBJECTIVE(S):

- Understand the purpose, scope and intent of the ISO/IEC 27001 Climate Change Amendment.
- Analyse climate-related information security threats affecting digital and physical assets.
- Identify changes required within ISMS clauses, documentation and controls.
- Integrate climate change considerations into risk assessment and risk treatment.
- Strengthen ISMS planning, operational controls and organisational resilience.
- Align business continuity, disaster recovery and supplier management with climate risks.
- Prepare documentation and evidence required for certification bodies.
- Support continuous improvement of the ISMS under climate-related conditions.

TARGET GROUP(S):

- ISMS Implementation Teams and Information Security Officers

- IT, Cybersecurity and Network Administrators

- Risk Management and Business Continuity Personnel

- Internal Auditors and Compliance Officers

- Document Controllers and ISMS Coordinators

- Managers and Executives responsible for ISO/IEC 27001

ENTRY REQUIREMENT(S):

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

TOPIC(S):

1. Introduction to ISO/IEC 27001 and Climate Change Context

2. Climate Change Amendment: Requirements and Intent

3. Identifying Climate-Related Information Security Threats

4. Updating ISMS Context and Interested Parties

5. Integrating Climate Inputs into Risk Assessment

6. Adjusting Risk Treatment Plans and Controls

7. Climate Impacts on Assets, Infrastructure and Physical Security

8. Business Continuity, Disaster Recovery and Climate Resilience

9. Supplier and Outsourced Service Management under Climate Influence

10. Documentation Updates, Evidence Requirements and Audit Readiness

LIST OF REFERENCE BOOK(S):

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- ISO 31000: Risk Management Guidelines
- ISO 22301: Business Continuity Guidelines
- Climate Change and Information Security Reference Materials

LIST OF TEACHING AID(S):

- LCD projector
- ISMS documentation samples
- Risk assessment templates
- Climate risk mapping diagrams
- Case study worksheets
- Flip chart or whiteboard

METHODOLOGY(S):

- Interactive lecture
- Group discussion
- Case studies
- Documentation walkthrough
- Scenario-based exercises

TRAINING SCHEDULE

Day 1

Time	Activity / Topic
8:30 am – 9:00 am	Registration and Introduction
9:00 am – 10:15 am	Topic 1: ISO/IEC 27001 and Climate Change Context
10:15 am – 10:30 am	**Morning Tea Break**
10:30 am – 12:30 pm	Topic 2: Climate Change Amendment Requirements
12:30 pm – 1:30 pm	**Lunch Break**
1:30 pm – 3:30 pm	Topic 3–4: Climate Threats and ISMS Context Updates
3:30 pm – 3:45 pm	**Afternoon Tea Break**
3:45 pm – 5:00 pm	Topic 5: Climate-Integrated Risk Assessment

TRAINING SCHEDULE

Day 2

Time	Activity / Topic
8:30 am – 9:00 am	Recap of Day 1
9:00 am – 10:15 am	Topic 6: Risk Treatment Adjustments and Controls
10:15 am – 10:30 am	**Morning Tea Break**
10:30 am – 12:30 pm	Topic 7–8: Asset Protection and Climate-Resilient Continuity Planning
12:30 pm – 1:30 pm	**Lunch Break**
1:30 pm – 3:30 pm	Topic 9: Supplier and Outsourced Service Management
3:30 pm – 3:45 pm	**Afternoon Tea Break**
3:45 pm – 5:00 pm	Topic 10: Documentation Updates and Audit Preparation