New Horizons® Learning Centres

COURSE OUTLINE
IT TRAINING

RESILIA™ Foundation (Exam included)

Duration: **3 days**

Overview:

The RESILIA™ Foundation course starts with the purpose, key terms, the distinction between resilience and security, and the benefits of implementing cyber resilience. It introduces risk management and the key activities needed to address risks and opportunities. Further, it explains the relevance of common management standards and best practice frameworks to achieve cyber resilience. Subsequently, it identifies the cyber resilience processes, the associated control objectives, interactions and activities that should be aligned with corresponding ITSM activities. In the final part of the course, it describes the segregation of duties and dual controls related to cyber resilience roles and responsibilities.

Target Audience:

The RESILIA™ Foundation course audience includes all teams across the IT and Risk functions, including:

- IT Service Management
- Operations and Incident management
- IT Change & Release management

Key Participant Benefits:

Participants to this course learn about the methods and use of preventative, detective, and corrective controls allowing them to recognize risks and to operate effectively in a challenging environment. The course provides insights into common management standards and best practice frameworks that would assist in making decisions to anticipate, counter and/or recover accordingly from cyber-attacks. Participants on completing this course would be better positioned in an organisation to effectively govern, manage and comply with cyber resilience.

Read more…

Module 1: Introduction to Cyber Resilience

- Describe what cyber resilience is
- Identify the benefits of cyber resilience

Module 2: Cyber Resilience Risk Management

- Describe what risk management is
- Identify the purpose of risk management
- Identify the terms: risk, asset, vulnerability, threat

Module 3: Managing Cyber Resilience

- Purpose of a management system and how best practices and standards can contribute
- Purpose and scope of a management system
- Components of a management system
- Common management standards and best practice frameworks to cyber resilience
- Best practice frameworks to cyber resilience, ITIL, ISO/IEC 27001, NIST Framework
- Difference between management, governance & compliance

Module 4: Cyber Resilience Cyber Resilience Strategy

- Identify what cyber resilience strategy is intended to achieve
- Identify cyber resilience activities that should be aligned with IT service strategy

Module 5: Cyber Resilience Design

- What cyber resilience design is intended to achieve
- Cyber resilience aligned with IT service design

Module 6: Cyber Resilience Transition

- Understand the purpose of cyber resilience transition, the associated control objectives and their interactions with ITSM activities
- What cyber resilience transition is intended to achieve

Module 7: Cyber Resilience Operation

- Understand the purpose of cyber resilience operation, the associated control objectives and their interactions with ITSM activities
- What cyber resilience operation is intended to achieve

Module 8: Cyber Resilience Continual Improvement

- Identify what cyber resilience continual improvement is intended to achieve
- Recognise maturity models and their purpose

Module 9: Cyber Resilience Roles & Responsibilities

- Purpose and benefits of segregation of duties and dual controls