TRAINING SERVICES

RESILIA® Foundation

RESILIA® Foundation

Leading to the RESILIA® Foundation Certification

Duration: 30 or 60 days
Pre-requisites: None
Delivery Methods: Self-Paced Online

Course Overview

The RESILIA Foundation qualification takes delegates through a lifecycle approach to organisational cyber resilience, from creating a strategy aligned to business objectives through to operational cyber resilience activities. The course is suitable for anyone who needs an awareness of how to protect an organisation's information assets, as well as how to recover from a cyber breach.

- 30 or 60 days online access Fully accredited
- Includes videos, quizzes, exercises, official syllabus and sample exams
- RESILIA Manual EBook
- Exam Voucher
- Tutor support available via email

Target Group

The RESILIA® Foundation qualification is aimed at IT and security functions, risk and compliance functions and core business functions including: HR, Finance, Procurement, Operations and Marketing. The awareness learning is for the entire organization. The leadership engagement delivers specialised training and learning for the leaders within an organisation.

Knowledge Objectives

Attending a RESILA Foundation course will:

- Enable you to understand the security responsibilities of all stakeholders across the service supply chain.
- Allow you to understand the characteristics of a well-protected organisation.
- Become more effective in your role as a Cyber Resilience practitioner.
- And of course enhance your career prospects and earning potential.

- Provides the breadth and depth of expertise necessary to develop Cyber Resilience Strategy and Design
- Easily adopt Cyber Resilience into existing Strategy and Design
- Confidence that your strategy design supports Cyber Resilience Best Practice.
- Professional differentiation as these roles are typically qualified in ITSM/ITIL®, not Cyber Resilience
- Greater collaboration with colleagues across the IT function as you embed Cyber Resilience Best Practice.
- Demonstrate subject matter expertise through certification
- Differentiate themselves from other SMEs and technical candidates for desirable positions in the fast-growing information Cyber Security /Resilience specialisation.

Course Content
10 modules covering an introduction to cyber resilience, the cyber resilience lifecycle from strategy to improvement, plus cyber resilience roles.

Modules in this course:

- Module 1: Introduction to cyber resilience
- Module 2: Risk management
- Module 3: Managing cyber resilience
- Module 4: Cyber resilience strategy
- Module 5: Cyber resilience design
- Module 6: Cyber resilience transition
- Module 7: Cyber resilience operation
- Module 8: Cyber resilience improvement
- Module 9: Roles and responsibilities
- Module 10: Exam preparation

Examination

- Exam duration: 110 minutes
- Exam format: Closed book, multiple choice
- Exam delivery: online, webcam proctored.
- Exam pass mark: 33/50 questions

This course does not require any existing knowledge of cyber resilience. Completion of an accredited course is a mandatory pre-requisite for the exam