# RESILIA$^{TM}$ Foundation

| | | | |
|---|---|---|---|
| **Certificate:** | RESILIA$^{TM}$ Foundation | **Course ID:** | RESILIA-F |
| **Duration:** | 3 days (virtual) classroom | **Language:** | English |
| **Course Delivery:** | Classroom, Exam, eBooks | **PMI® PDUs:** | 24 |
| **Accreditor:** | Axelos | | |

AXELOS RESILIA™: Cyber Resilience Best Practice is designed to help commercial and government organizations around the world prevent, detect and correct any impact cyber attacks will have on the information required to do business. Adding RESILIA to the existing AXELOS global best practice portfolio, including ITIL® and PRINCE2®, brings a common cyber resilience best practice for security, IT service management and business. Active cyber resilience is achieved through people, process and technology.

The RESILIA$^{TM}$ 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.

**Audience:**

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

- IT Service Management
  - Operations and Incident management
  - IT Change & Release management
  - IT Supplier & Vendor management
- Business Analysis and Design
  - Business analysts
  - IT Architects
- Development
- IT Project & Programme Management
- Risk and Compliance
  - Information Security management
  - Business Continuity managers

**Learning Objectives:**

Individuals certified at RESILIA$^{TM}$ Foundation will have demonstrated their knowledge of:

- The purpose, benefits, and key terms of cyber resilience.
- Risk management and the key activities needed to address risks and opportunities.
- The purpose of a management system and how best practices and standards can contribute.
- Cyber resilience strategy, the associated control objectives, and their interactions with ITSM activities.
- Cyber resilience design, the associated control objectives and their interactions with ITSM activities.
- Cyber resilience transition, the associated control objectives, and their interactions with ITSM activities.
- Cyber resilience operation, the associated control objectives, and their interactions with ITSM activities.
- Cyber resilience continual improvement, the associated control objectives, and their interactions with ITSM activities.
- The purpose and benefits of segregation of duties and dual controls.

### Prerequisites:

There are no prerequisites for this course.

### Follow-on Courses:

RESILIA™ Practitioner Course.

### Technical Requirements:

For eBooks:

- Internet is required only for downloading the eBook. The eBooks can be read offline.
- Available on: Desktop, Laptop, Tablet, SmartPhone, eReader.
- Recommended PDF reader: Adobe Reader.

### Examination:

- Syllabus scope: understand and recognize RESILIA™: Cyber Resilience Best Practice
- Bloom's level: 1-2
- Format: Multiple Choice
- Number of questions: 50
- Duration: 100 minutes
- Exam Format: closed book exam
- Proctoring: Live or Web-proctored

### Agenda:

| Day 1 | Day 2 | Day 3 |
|---|---|---|
| M1: Course Introduction<br>M2: Intro to Cyber Resilience<br>M3: Risk Management<br>M4: Managing Cyber Resilience<br>M5: Cyber Resilience Strategy<br>M6: Cyber Resilience Design<br>End of Day Case Study Assignment | M6: Cyber Resilience Design<br>M7: Cyber Resilience Transition<br>M8: Cyber Resilience Operation<br>End of Day Case Study Assignment | M8: Cyber Resilience Operation<br>M9: Cyber Resilience Continual Improvement<br>M10: Cyber Resilience Roles and Responsibilities<br>M11: Exam Preparation Guide |

Copyright © 2015 The Project Strategy Consulting Group, Inc., in association with its partner entities. All rights reserved.
RESILIA™ AND ITIL® are trade marks of AXELOS Limited. All rights reserved. Material is reproduced under license from AXELOS.
PMI and "Registered Education Provider" are registered marks of the Project Management Institute.

## COURSE OUTLINE:

**Module 1: Course Introduction**

- Course Learning Objectives
- Course Agenda
- Activities
- Module End Questions
- Course Book Structure
- RESILIA Certification
- Summary

**Module 2: Introduction to Cyber Resilience**

- What is Cyber Resilience?
- Module Learning Objectives
- Module Topics
- Defining Cyber Resilience
- Balancing in Cyber Resilience
- Characteristics of Cyber Resilience
- Summary
- End of Module Quiz

**Module 3: Risk management**

- Understanding Risk Management: Discussion
- Module Learning Objectives
- Module Topics
- Defining Risk Management
- Addressing Risks and Opportunities
- Summary
- End of Module Quiz

**Module 4: Managing Cyber Resilience**

- Why and What of Management Systems?
- Module Learning Objectives
- Module Topics
- Management Systems
- Common Management Standards and Frameworks
- Summary
- End of Module Quiz

**Module 5: Cyber Resilience Strategy**

- What is Strategy?
- Module Learning Objectives
- Module Topics
- Cyber Resilience Strategy and Activities
- Security Controls at Cyber Resilience Strategy
- Interaction Between ITSM Processes and Cyber Resilience
- Summary
- End of Module Quiz

**Module 6: Cyber Resilience Design**

- Why Cyber Resilience Design?
- Module Learning Objectives
- Module Topics
- Cyber Resilience Design Activities
- Security Controls at Cyber Resilience Design
- Aligning ITSM Processes with Cyber Resilience Processes
- Summary
- End of Module Quiz

**Module 7: Cyber Resilience Transition**

- Why Cyber Resilience Transition?
- Module Learning Objective
- Module Topics
- Basics of Cyber Resilience Transition
- Cyber Resilience Transition: Controls
- Interaction Between ITSM Processes and Cyber Resilience
- Summary
- End of Module Quiz

**Module 8: Cyber Resilience Operation**

- The Purpose of Cyber Resilience Operation
- Module Learning Objectives
- Module Topics
- Security Controls in Cyber Resilience Operation
- Interaction Between IT Processes and Cyber Resilience
- Interaction Between ITSM Functions and Cyber Resilience
- Summary
- End of Module Quiz

**Module 9: Cyber Resilience Continual Improvement**

- Continual or Continuous Improvement
- Module Learning Objectives
- Module Topics
- Maturity Models
- Continual Improvement Controls
- The Seven-Step Improvement Process
- The ITIL CSI Approach
- Summary
- End of Module Quiz

**Module 10: Cyber Resilience Roles & responsibilities**

- Module Learning Objectives
- Module Topics
- Segregating Duties
- Dual Controls
- Summary
- End of Module Quiz

**Module 11: Exam Preparation Guide**

- Module Learning Objectives
- Qualification Learning Objectives
- Learning Level of the Syllabus
- Certification
- Exam Instructions
- Tips for Taking Exam