# RESILIA™ Practitioner

| | | | |
|---|---|---|---|
| **Certificate:** | RESILIA™ Practitioner | **Course ID:** | RESILIA-P |
| **Duration:** | 2 days (virtual) classroom | **Language:** | English |
| **Course Delivery:** | Classroom, Exam, eBooks | **PMI® PDUs:** | 16 |
| **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™ Practitioner course starts by revisiting the concepts and knowledge acquired in the Foundation course and requires you to bring that knowledge into practical activities in interesting real-life scenarios. The course begins with distinguishing among the terms: asset, risk, threat and vulnerability. It determines the key activities needed to address risks and opportunities as well as to create and manage a risk register and a risk treatment plan. Further, it explains the purpose and use of the control objectives for cyber resilience processes, and the interactions and activities that are aligned with corresponding ITSM activities. In the final part of the course, it describes the application of the seven-step improvement process to plan cyber resilience improvements, the ITIL CSI approach to cyber resilience and the segregation of duties and dual controls related to cyber resilience roles and responsibilities.

**Audience:**

The RESILIA™ Practitioner 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 this level will:

- Be able to carry out risk management.
- Be able to manage the controls relevant to cyber resilience strategy and align these with IT service management (ITSM).
- Be able to manage the controls relevant to cyber resilience design and align these with ITSM.
- Be able to manage the controls relevant to cyber resilience transition and align these with ITSM.
- Be able to manage the controls relevant to cyber resilience operation and align these with ITSM.
- Be able to manage the controls relevant to cyber resilience continual improvement and align these with ITSM.
- Be able to evaluate need for segregation of duties and dual controls.

**Benefits of Taking This Course:**
In this course, participants are exposed to various scenarios where they can apply their foundation level knowledge and concepts of cyber resilience controls and procedures. This strategy will enable participants to manage and operate effectively in a challenging cyber centric environment. The course takes into consideration the limitations of traditional security controls to combat today's sophisticated cyber attacks. This proactive approach to design and use new and effective controls along with industry compliance standards would assist in making decisions to prevent, detect, respond, and recover from today's evolving cyber-threats. With completing this course, you will be well versed and highly equipped in an organization to govern, manage, and comply with cyber resilience.

**Prerequisites:**
RESILIA™ Foundation Certification.

**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: 3-4
- Format: Multiple Choice
- Number of questions: 50
- Duration: 135 minutes
- Exam Format: Closed book exam
- Proctoring: Live or web-proctored

**Agenda:**

| Day 1 | Day 2 |
|---|---|
| M1: Course Introduction<br>M2: Risk Management<br>M3: Cyber Resilience Strategy<br>M4:Cyber Resilience Design | Recap and discussion<br>M5: Cyber Resilience Transition<br>M6: Cyber Resilience Operation<br>M7: Cyber Resilience Continual Improvement<br>M8: Segregation of Duties and Dual Controls |

PROJECT STRATEGY CONSULTING GROUP
IMPROVING THE CLIENT CONDITION

RESILIA™

PEOPLECERT PARTNER

## COURSE OUTLINE

**Module 1: Course Introduction**

1.1 Let us get to know each other
1.2 Course learning objectives
1.3 Course agenda
1.4 Activities
1.5 Module end questions
1.6 Course book structure
1.7 RESILIA certification

**Module 2: Risk Management**

2.1 Distinguish between the terms: risk, asset, vulnerability, and threat
2.2 Determine the actions needed to address risks and opportunities and explain their purpose
2.3 Create and manage a:
a) Risk register
b) Risk treatment plan

**Module 3: Cyber Resilience Strategy**

3.1 Explain the purpose and use of the control objectives:
a) Establish governance
b) Manage stakeholders
c) Identify and categorize stakeholders
d) Create and manage cyber resilience policies
e) Manage audit and compliance
3.2 Explain how ITSM processes and cyber resilience interact

**Module 4: Cyber Resilience Design**

4.1 Explain the purpose and use of the control objectives:
a) Human resource security
b) System acquisition, development, architecture and design
c) Supplier and 3rd party security
d) Endpoint security
e) Cryptography
f) Business continuity
4.2 Explain how ITSM processes and cyber resilience interact

**Module 5: Cyber Resilience Transition**

5.1 Explain the purpose and use of the control objectives:
a) Asset management and configuration management
b) Classification and handling
c) Data transportation and removable media
d) Change management
e) Testing
f) Training
g) Documentation management
h) Information retention
i) Information disposal
5.2 Explain how ITSM processes and cyber resilience interact

**Module 6: Cyber Resilience Operation**

6.1 Explain the purpose and use of the control objectives:
a) Access control
b) Network security management
c) Physical security
d) Operations security
e) Incident management
6.2 Explain how ITSM processes and cyber resilience interact

**Module 7: Cyber Resilience Continual Improvement**

7.1 Explain the purpose and use of the control objectives:
a) Audit and review
b) Control assessment
c) Key Performance Indicators
d) Business continuity improvements
e) Process improvements
f) Remediation and improvement planning
7.2 Apply the seven-step improvement process to plan cyber resilience improvements
7.3 Apply the ITIL CSI approach to cyber resilience

**Module 8: Segregation of Duties and Dual Controls**

8.1 Apply the concepts of segregation of duties and dual controls to an organizational context