RESILIA™ Foundation

Course Summary

Description

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™ 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.

Objectives

By the end of this course, students will be able to:

- The purpose, benefits, and key terms of cyber resilience.
- The purpose of 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.
- The purpose of cyber resilience strategy, the associated control objectives, and their interactions with ITSM activities.
- The purpose of cyber resilience design, the associated control objectives and their interactions with ITSM activities.
- The purpose of cyber resilience transition, the associated control objectives, and their interactions with ITSM activities.
- The purpose of cyber resilience operation, the associated control objectives, and their interactions with ITSM activities.
- The purpose of 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.

Topics

- Intro to Cyber Resilience
- Risk management
- Managing Cyber Resilience
- Cyber Resilience Strategy
- Cyber Resilience Design
- Cyber Resilience Transition
- Cyber Resilience Operation
- Cyber Resilience Continual Improvement
- Cyber Resilience Roles & responsibilities

RESILIA™ Foundation

Course Summary (cont’d)

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 & Program Management
- Risk and Compliance
  - Information Security management
  - Business Continuity managers

Prerequisites

There are no prerequisites for this course.

Duration

Three days

RESILIA™ Foundation

Course Outline

I. **Intro to Cyber Resilience**
  A. Describe what cyber resilience is
  B. Identify the benefits of cyber resilience
  C. Identify the terms
  D. Identify the purpose of balancing
  E. Identify the need for:
  F. Confidentiality
  G. Integrity
  H. Availability
  I. *Authentication*
  J. Nonrepudiation

II. **Risk management**
  A. Describe what risk management is
  B. Identify the purpose of risk management
  C. Identify the terms: risk, asset, vulnerability, threat
  D. Describe actions to address risks and opportunities:
  E. Establish context
  F. Establish criteria for risk assessment and acceptance
  G. Risk identification
  H. Risk analysis and evaluation
  I. Risk treatment
  J. Risk monitoring and review
  K. Identify the terms:
  L. Risk register
  M. Risk avoidance
  N. Risk modification
  O. Risk sharing
  P. Risk retention
  Q. Risk treatment plan
  R. Defence-in-depth

III. **Managing Cyber Resilience**
  A. Identify the purpose and scope of a management system
  B. Identify the components of a management system
  C. Recognize the relevance of common management standards and best practice frameworks to cyber resilience
  D. Describe the difference between management, governance, and compliance

IV. **Cyber Resilience Strategy**
  A. Identify what cyber resilience strategy is intended to achieve
  B. Identify cyber resilience activities that should be aligned with IT service strategy
  C. Describe the purpose and key features of the control objectives
  D. Identify interactions between the following ITSM processes and cyber resilience

V. **Cyber Resilience Design**
  A. Identify what cyber resilience design is intended to achieve
  B. Identify cyber resilience activities that should be aligned with IT service design
  C. Describe the purpose and key features of the control objectives
  D. Identify interactions between the following ITSM processes and cyber resilience

VI. **Cyber Resilience Transition**
  A. Identify what cyber resilience transition is intended to achieve
  B. Describe the purpose and key features of the control objectives
  C. Identify interactions between the following ITSM processes and cyber resilience

VII. **Cyber Resilience Operation**
  A. Identify what cyber resilience operation is intended to achieve
  B. Describe the purpose and key features of the control objectives
  C. Identify interactions between the following ITSM processes and cyber resilience

VIII. **Cyber Resilience Continual Improvement**
  A. Identify what cyber resilience continual improvement is intended to achieve
  B. Recognize maturity models and their purpose
  C. Describe the purpose and key features of the control objectives
  D. Describe how the seven-step improvement process can be used to plan cyber resilience improvements
  E. Describe how to use ITIL CSI approach to plan cyber resilience improvements

IX. **Cyber Resilience Roles & responsibilities**
  A. Describe segregation of duties and dual controls