



Leading Your Business Transformation

A background image showing a blurred office scene with several people in business attire. Overlaid on the right side of the image are three white gear icons of varying sizes, arranged in a cluster. A dark blue horizontal band spans across the middle of the image, containing the text "RESILIA™ Foundation".

RESILIA™ Foundation

Fifalde Consulting Inc.
+1-613-699-3005

1. Course 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.

2. 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
 - 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

3. Learning Objectives:

Individuals certified at RESILIA™ 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.

4. Benefits of Taking This Course:

“This course, for the first time brings together the cyber resilience best practices based on a process based life cycle refined, improved and tested over a quarter century to assure success.” - Moyn Uddin, Lead Author of the ITpreneurs RESILIA training program, and Author of the RESILIA™: Cyber Resilience Best Practice Guide from AXELOS.

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 organization to effectively govern, manage and comply with cyber resilience.

5. Prerequisites:

There are no prerequisites for this course.

6. Course Materials:

Participants receive a copy of the classroom presentation material and a Participant Handbook.

7. About the 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
- Pass rate: 60%
- Exam Format: closed book exam
- Proctoring: Live or Web-proctored

8. Agenda:

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

M5: Cyber Resilience Strategy	Assignment	
M6: Cyber Resilience Design		
End of Day Case Study Assignment		

9. 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
- Topics Covered in This Module
 1. Qualification Learning Objectives
 2. Learning Level of the Syllabus
 3. Certification
 4. Exam Instructions
 5. Tips for Taking Exam

Fifalde Consulting Inc. is a trusted independent advisor, helping organizations maximize efficiencies and increase value to their IT services. We specialize in the delivery of Information Technology Service Management (ITSM) and Information Security Management (ISM) consulting and training services, using best practices such as the Information Technology Infrastructure Library (ITIL®), TIPA®, TOGAF®, and standards such as ISO/IEC 20000, 27001, 38500 and others. Fifalde's team includes a network of the most accredited consultants and trainers in the IT industry.

For more information on what Fifalde can offer your organization, please visit fifalde.com



Leading Your Business Transformation