



RESILIA Foundation HODV1S

This course helps individuals understand how operational decisions can have an impact on good cyber resilience. It shows how nurturing cyber resilience can support operational effectiveness and business efficiency.

The purpose of the foundation qualification is to understand how decisions impact good/bad cyber resilience. It has a comprehensive approach across all areas and teaches individuals how to make good cyber resilience an efficient part of business and operational management.

RESILIA Foundation

Price USD \$1,895

Links to local schedules, pricing and registration [US/Canada](#)

HP course # HODV1S

Category Security

Duration 3 days

Audience

The qualification is aimed at professionals within the following areas:

- IT and security functions
- Risk and compliance functions
- Core business functions including HR
- Finance
- Procurement
- Operations and Marketing
- Corporate Security Officer/ Manager
- IT Security Officer/ Manager
- Anyone who would benefit from cyber resilience expertise within the team, often including a local champion or mentor for all staff to refer to.

Prerequisites

There are no specific prerequisites for this course.

Recommended:

- RESILIA™ Best Practices Core Book from TSO
- Information Security Essentials (HL945S) or equivalent
- Basic understanding of Service Management
- ITIL Foundation Course

What you get

- Expert Instructor lead training
- Student Courseware Kit
- 3-month unlimited individual license to the RESILIA Foundation Video Self-paced (VISPEL) course for lecture review and exam preparation
- Official sample exams to help prepare for the Certification Exam

Benefits of RESILIA™ Certification

- Helps minimize any damage from a security breach and supports fast recovery.
- Helps build cyber resilience into your existing processes.
- Helps establish a common language for cyber resilience across your organization.
- Builds the confidence and insight to design and deliver cyber resilient strategies and services across your organization as well as with your customers and suppliers

Course outline

Chapter 01 - Course Introduction

Chapter 02 - What is Cyber Resilience

- What is Cyber Resilience
- Balance & Management Systems
- People, Process and Technology
- Cyber Resilience Needs
- Summary
- Quiz

Chapter 03 - Risk Management

- What is Risk Management?
- Risk Management in Action
- Summary
- Quiz

Chapter 04 - Managing Cyber Resilience

- Management of Cyber Resilience
- Adopt, Adapt & Improve
- Summary
- Quiz

Chapter 05 - Cyber Resilience CSI

- Cyber Resilience CSI and ITSM
- Maturity Models
- Control Objectives
- 7-Steps of Improvement
- CSI Approach to Cyber Resilience
- Summary
- Quiz

Chapter 06 - Cyber Resilience Strategy

- Cyber Resilience Strategy & ITSM
- Control Objectives
- ITSM Strategy & Cyber Resilience
- Segregation of Duties & Dual Controls
- Summary
- Quiz

Chapter 07 - Cyber Resilience Design

- Cyber Resilience Design and ITSM
- Control Objectives
- ITSM Design and Cyber Resilience
- Summary
- Quiz

Chapter 08 - Cyber Resilience Transition

- Cyber Resilience Transition & ITSM
- Control Objectives
- ITSM Transition and Cyber Resilience - Part 1
- ITSM Transition and Cyber Resilience - Part 2
- Summary
- Quiz

Chapter 09 - Cyber Resilience Operation

- Cyber Resilience Operation and ITSM
- Control Objectives
- ITSM Operation and Cyber Resilience - Part 1
- ITSM Operations and Cyber Resilience - Part 2
- Summary
- Quiz

Chapter10 - RESILIA Foundation Summary and Exam Prep

Learn more at

hpe.com/us/training/security