Tytuł szkolenia: RESILIA Foundation

Kod szkolenia: H0DV1S

Wprowadzenie

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.

Adresaci szkolenia

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

What you get

- Expert instructor led 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

The 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

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

Cel szkolenia

Czas i forma szkolenia

- 21 godzin (3 dni x 7 godzin), w tym wykłady i warsztaty praktyczne.

Plan szkolenia

Module 1: Course introduction

Module 2: What is cyber resilience?

- What is cyber resilience?
- Balance and management systems
- People, process, and technology
- Cyber resilience needs
- Summary
- Quiz

Module 3: Risk management

- What is risk management?
- Risk management in action
- Summary
- Quiz

Module 4: Managing cyber resilience

- Management of cyber resilience
- Adopt, adapt, and improve
- Summary
- Quiz

Module 5: Cyber resilience CSI

- Cyber resilience CSI and ITSM
- Maturity models
- Control objectives
- 7-Steps of improvement
- CSI approach to cyber resilience
- Summary
- Quiz

Module 6: Cyber resilience strategy

- Cyber resilience strategy and ITSM
- Control objectives
- ITSM strategy and cyber resilience
- Segregation of duties and dual controls
- Summary
- Quiz

Module 7: Cyber resilience design

- Cyber resilience design and ITSM
- Control objectives
- ITSM design and cyber resilience
- Summary
- Quiz

Module 8: Cyber resilience transition

- Cyber resilience transition and ITSM
- Control objectives
- ITSM transition and cyber resilience - Part 1
- ITSM transition and cyber resilience - Part 2
- Summary
- Quiz

Module 9: 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

Module 10: RESILIA Foundation

- Summary
- Exam preparation