



## RESILIA Foundation

The RESILIA Foundation qualification takes delegates through a lifecycle approach to organisational cyber resilience, from creating a strategy aligned to business objectives through to operational cyber resilience activities. The course is suitable for anyone who needs an awareness of how to protect an organisation's information assets, as well as how to recover from a cyber breach.

### Course Contents:

- Module 1: Introduction to cyber resilience
- Module 2: Risk management
- Module 3: Managing cyber resilience
- Module 4: Cyber resilience strategy
- Module 5: Cyber resilience design
- Module 6: Cyber resilience transition
- Module 7: Cyber resilience operation
- Module 8: Cyber resilience improvement
- Module 9: Roles and responsibilities
- Module 10: Exam preparation

**Course Options:** 30 and 60 day courses are available

**Prerequisites:** This course does not require any existing knowledge of cyber resilience.

**Exam details:** 50 multiple choice questions. 110 minute duration with a 66% pass mark. Exam can be taken online with a web proctor. Students must have completed the RESILIA Foundation course before requesting their exam voucher.

**Suitable for:** The entire organisation, including the boardroom, IT, risk and business professionals, so that they better understand the risks and benefits of effective Cyber Resilience.

The certification is aimed at IT and security, risk functions and all core business functions including HR, finance, procurement, operations and marketing.

### Further Information

RESILIA offers practical guidance, training and learning for the entire organization, including the boardroom, IT, risk and business professionals, so that they better understand the risks and benefits of effective Cyber Resilience.

The certification is aimed at IT and security, risk functions and all core business functions including HR, finance, procurement, operations and marketing.

RESILIA training can be used to raise staff awareness of threats, and change staff behaviours to minimise risk.

RESILIA best practice uses a lifecycle approach to aid effective deployment and management of Cyber Resilience in an organization. The lifecycles are complementary to ITIL as they follow the same Strategy, Design, Transition, Operation and Continuous Improvement structure. The best practice covers what activities, controls and management processes should be in each lifecycle.

Organizations already using ITIL for service management will find that Cyber Resilience can easily be integrated into this existing management systems, with Cyber Resilience controls and management becoming an extension of existing business-as-usual processes.

# RESILIA™ PRACTITIONER

## RESILIA Practitioner

The RESILIA Practitioner qualification builds on knowledge acquired during the RESILIA Foundation training and challenges delegates to apply and adapt cyber resilience best practice. This practical course is built round a case study and set of exercises to bring cyber resilience to life.

### Course Contents:

- Module 1: Cyber resilience implementation
- Module 2: Cyber resilience strategy
- Module 3: Cyber resilience design
- Module 4: Cyber resilience transition
- Module 5: Cyber resilience operation
- Module 6: Cyber resilience improvement
- Module 7: Exam preparation

**Course Options:** 30 and 60 day courses are available

**Prerequisites:** Exam delegates must hold the RESILIA Foundation certificate.

**Exam details:** 50 multiple choice questions. 135 minute duration with a 60% pass mark. Exam can be taken online with a web proctor. Students must have completed the RESILIA Practitioner course before requesting their exam voucher.

**Suitable for:** Professionals with responsibility for IT and security functions or risk and compliance operations within an organisation. Other core business areas including HR, Finance, Procurement, Operations and Marketing, will also benefit from having cyber resilience expertise within their teams.