FACT SHEET

RESILIA™

RESILIA™ CERTIFICATIONS

RESILIA provides a management system and framework for organizations to adopt cyber resilience best practice and for individuals to learn how to effectively prevent, respond to and recover from cyber-attacks. The training and certification helps build cyber resilience across the organization, providing individuals with the understanding and confidence to react and act on cyber security risks more effectively.

WHY YOU NEED CYBER RESILIENCE:

- 37.3 Million users experienced phishing attacks in 2013 (Kaspersky Lab)
- Human error is involved in more than 95% of security incidents (IBM '2014 Cyber Security Intelligence Index' report)
- 50% of users open emails and click on phishing links within the first hour (Verizon '2015 Data breach investigations' report)
- 205 days: the average number of days between an initial compromise and when the victim discovers the attack (Mandiant)
- 73% of large organizations suffered from infection by viruses or malicious software in the past year, up from 59% a year ago (BIS, 2014 Information Security Breaches Survey).

KEY FEATURES:

- Provide best practice guidance that can be easily adopted and integrated into existing processes encompassing people, process and technology
- Assist in defining what good cyber resilience looks like and how it will support business strategy
- Built using the ITIL® lifecycle, organizations can fully maximize their existing investment in IT service management and build on a common business language to add Cyber Resilience as a capability layer on top of existing IT and business operations, security, incident management and risk functions.

With RESILIA you can KEEP:

- your most precious information safe
- a positive market reputation
- strong customer confidence
- a cyber aware and cyber vigilant workforce

WHO ARE THE CERTIFICATIONS DESIGNED FOR?

IT and Security functions: all professionals within IT Service Management, Information Security, Business Analysis, IT Project Management, IT Development, IT and Security Architecture and leadership roles (CTO (Chief Technology Officer), CISO (Chief Information and Security Officer), Head of IT).

The Risk function: all Risk Management professionals from CRO (Chief Risk Officer), Head of Risk, Risk Manager, Heads of Compliance and Business Continuity to risk and business analyst roles.

All core business functions, HR, Finance, Procurement, Operations and Marketing, will benefit from having cyber resilience expertise within the team, often including a local champion or mentor for all staff to refer to. RESILIA certifications are designed for all staff from leadership roles (HR Director, CFO, Operations Director) to management and operational teams.

AXELOS GLOBAL BEST PRACTICE

KEY BENEFITS OF RESILIA:

ORGANIZATIONS

IMPROVE YOUR BUSINESS WITH RESILIA

- It provides a management system and framework to help identify what good cyber resilience looks like
- It helps organizations balance their prevention, detection and correction priorities; their people, process and technology priorities and their risks and opportunities based on a defined risk appetite
- It provides the confidence they need to recognize, respond to and recover from cyber-attacks effectively
- It helps to build a common language and collaboration across your entire IT and Security teams as well as other critical departments. It provides the framework to define, act on and embed the right processes for effective cyber resilience across the entire organization.

INDIVIDUALS

SUCCESFULLY MANAGE YOUR CAREER WITH RESILIA

- Have the confidence, knowledge and skills required to effectively respond to and recover from a cyber-attack
- Have the breadth and depth of knowledge to design and deliver cyber resilience initiatives across both IT and business services
- Have the ability to differentiate yourself from your peers by developing skills and knowledge with a recognized certification in an increasingly important area
- Take advantage of the career opportunities available and better qualified, cyber aware individuals
- Have the confidence to liaise with senior management, information security teams, risk managers and external vendors about cyber resilience strategies and initiatives
- Become part of a growing global community of cyber resilience professionals
- Take the first step towards becoming a Cyber Security professional.

OBJECTION HANDLING: FOR ORGANIZATIONS & INDIVIDUALS

Q. Isn't Cyber Resilience the role of the Information Security teams? It doesn't have anything to do with me/do I really need to invest in training for the rest of the business on this?

A. Individuals are frequently those that are responsible for the breaches – everyone in the company has a role to play. You are equally as responsible for the resilience of your organization as the Information Security teams.

The role of Information Security has traditionally been to prevent and detect cyber-attacks through the use of technical controls. However cyber-attacks have evolved and it's not a question of if your organization will be attacked but when. Organizations need to have a greater cyber resilience capability so that they can respond to and recover from these attacks.

Q. Why should I do the RESILIA certification as opposed to CISSP, CISM, CISA, COBIT, the various SANS courses, etc.?

A. Existing qualifications like CISSP, CISM, CISA etc., are aimed at security professionals and as such have a more technical focus. In the case of CISSP this includes elements of physical security, with strategies and controls designed to prevent and detect cyber-attacks. RESILIA has been designed to highlight the importance of strategies and controls that respond and recover from attack and is aimed at IT, security, risk and the wider business who need a greater understanding of cyber resilience as part of their existing responsibilities and strategies.

Q. My organization is already compliant with IS27001. Why do we need to do anything more?

A. IS27001 is a standard with a set of controls that need to be implemented in order to be compliant. However compliance does not equal security. All of the organizations you have seen in the headlines who have suffered a cyber-attack were compliant. By adopting RESILIA you are implementing a framework that goes to the heart of your organization's strategy to embed cyber resilience behaviours that will help you effectively respond and recover from cyber-attacks.

Q. How does RESILIA fit with existing frameworks? (NIST, ISF, ISO 27001, etc.)

A. RESILIA has been designed to complement existing standards, policies and frameworks, providing a strategic approach that can easily adapted by all types of organizations.

Q. Do RESILIA certifications really align themselves with ITIL?

A. The ITIL framework, developed originally for the delivery of effective, business-focused IT services is now used successfully for the management and provision of other services. The Cyber Resilience Best Practice covers a range of cyber resilience practices and activities across the ITIL lifecycle and describes how some of the processes and activities described by ITIL can be used to support an organization's cyber resilience strategy. RESILIA has been developed by AXELOS, the owners and custodians of ITIL.

THE BETTER UNDERSTANDING YOU HAVE OF CYBER RESILIENCE, THE BETTER YOU WILL BE ABLE TO EFFECTIVELY PREVENT, RESPOND TO AND RECOVER FROM CYBER-ATTACKS.