RESILIA™ Foundation

Exercises

RESILIA™ Foundation Exercises

Welcome to your Exercises

This document contains all the exercises that will support your studies during the course. It's very important to complete them as part of your exam preparation.

You will find our suggested solutions in the accompanying Exercise Solutions document.

IP and Copyright Information

Contents

Module 1 Lesson 1

Exercise – Cyber Resilience Controls

Plan to spend 30 minutes on this exercise.

Exercise

There are three types of Cyber Resilience control:

- Preventative controls are intended to prevent incidents that jeopardize cyber resilience
- Detective controls are intended to identify the occurrence of an incident that jeopardizes cyber resilience, so that the organization can respond appropriately.
- Corrective controls are intended to respond to the incident and correct the situation.

List some examples of each of these types of control.
What examples can you think of from your own organization?

Module 2 Lesson 1

Exercise – Risk

Plan to spend 30 minutes on this exercise.

Exercise

In this lesson you learned that a risk is created by a threat exploiting a vulnerability to impact an asset.

Think about your own organization. Make a list of some different types of assets and for each one identify some threats and vulnerabilities.

Module 2 Lesson 2

Exercise – Risk Evaluation

Plan to spend 20 minutes on this exercise.

Exercise

In this lesson you were shown an example of a matrix for defining qualitative risk levels.

Draw a risk matrix and use it to evaluate the risks that you identified in the last exercise.

IMPACT

HIGH			
MEDIUM			
LOW			
	LOW	MEDIUM	HIGH

LIKELIHOOD

Module 4 Lesson 1

Exercise – Stakeholders for Cyber Resilience

Plan to spend 30 minutes on this exercise.

Exercise

Stakeholders for Cyber Resilience include anyone who might gain a benefit or suffer a loss from a cyber-resilience incident, as well as anyone who might be involved in helping to prevent, detect or correct incidents.

Make a list of categories of stakeholders from your organization, and in each case describe their interest in cyber resilience.

Module 4 Lesson 2

Exercise – Business Relationship Management

Plan to spend 30 minutes on this exercise.

Exercise

The business relationship management process provides links between an organization and its customers at a strategic and tactical level. It ensures that the service provider understands the business requirements of its customers and that its customers understand the provider's capabilities, including the constraints it must work within.

Make a list of some specific ways that business relationship management can contribute to cyber resilience. Perhaps think about some issues or scenarios from your own organization.

Module 5 Lesson 1

Exercise – Business Impact Analysis

Plan to spend 30 minutes on this exercise.

Exercise

For each business activity, Business Impact Analysis asks ‘if this business activity were disrupted, what damage would the business suffer?’ Business activity includes things like billing, sales, shipping, manufacture of goods and the payment of salaries.

Make a list of some of the activities of your organization. In each case what would be the impact of disruption to that activity? How soon would the impact be felt?

Module 6 Lesson 1

Exercise – Asset Classification

Plan to spend 30 minutes on this exercise.

Exercise

An asset classification scheme should include handling instructions or a handling guide for each of the classifications so that users know when and how to handle the assets in terms of confidentiality but also integrity and availability.

List some examples of issues that should be addressed by handling instructions.

Module 7 Lesson 2

Exercise – Cyber Resilience Events

Plan to spend 30 minutes on this exercise.

Exercise

ITIL® defines an event as '*a change of state that has significance for the management of an IT service or other configuration item*'.

Make a list of examples of cyber resilience occurrences that have significance in your organization. Categorise them as informational, warning or exception.

Module 8 Lesson 1

Exercise – Responding to a Changing Environment

Plan to spend 30 minutes on this exercise.

Exercise

Cyber resilience has to adapt and respond to continually changing threat, business and technology environments.

List some examples from your own experience.