PURPLE GRIFFON
The IT Service Management Training & Consultancy Specialists

Course Title: Cyber Incident Response Management Foundation	**Course Duration**: 1.0 Day
Exam: Included	**Exam Type**: Proctored Exam
Qualification: Cyber Incident Response Management Foundation Certificate	

Course Syllabus

Our Cyber Incident Response Management Foundation training course will explain the following:

- Key definitions and legal requirements that underpin incident response.
- The incident reporting requirements of the GDPR, PCI DSS and NIS Directive.
- The components of the cyber kill chain, common cyber threats and common threat actors.
- The structure, role and responsibilities of the incident response team.
- The three phases of the CREST incident response process.
- The role of digital forensics in gathering evidence.
- The steps required to formulate and test an incident response plan.
- The role of business impact analysis.
- Applying incident response techniques to common risk scenarios.

Course Overview

Are you looking for the opportunity to train with Cyber Security Experts and learn how to plan and implement an effective Cyber Incident Response Programme?

Our one-day Cyber Incident Response Management Foundation training course will teach you how to protect your organisation from a disruptive incident such as a cyber attack or data breach.

Course Learning Outcomes

Cyber Incident Response Management Foundation training course gives you the knowledge to create and test an incident response plan designed to mitigate the impact of cyber attacks on your organisation.

It will also help you understand the incident reporting requirements of the EU General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS) and NIS Directive.

Our Cyber Incident Response Management Foundation training course will cover the following topics:

- The basic principles of incident response and business continuity.
- Common cyber threats and their potential impact.
- The role of the cyber incident response team.
- The three phases of the CREST incident response process.

Audience

Our Cyber Incident Response Management Foundation training course is aimed at Managers who are already involved in Incident Management with either an information security or data protection background. Individuals with little experience who are keen to enter the field or broaden their knowledge of cyber incident management with a professional qualification. It is also applicable to the following roles:

- Business Managers
- Compliance Managers
- IT Managers
- Help Desk Managers
- Project Managers
- Risk Managers
- Information Security Managers
- ISO 27001 Lead Auditors
- PCI QSAs

Entry-Level Requirements

There are no formal entry-level requirements, however we recommend that you have a good general understanding of cyber security principles and controls that underpin the protection of confidentiality, integrity and availability of data.

Recommended Reading

It is recommended that you purchase and read the following textbooks before our Cyber Incident Response Management Foundation training course:

- The True Cost of Information Security Breaches and Cyber Crime
- The Cyber Security Handbook – Prepare for, respond to and recover from cyber attacks
- Disaster Recovery and Business Continuity

What's Included

Our Cyber Incident Response Management Foundation training course includes full course materials (PDF files), the examination and certificate of attendance.

Please Note: You will need a laptop for the duration of your training course and exam.

Exam Information

You will take the Cyber Incident Response Management Foundation (CIRM F) set by IBITGQ (International Board for IT Governance Qualifications) at the end of the Cyber Incident Response Management Foundation training course:

- Delivery Method: Online
- Duration: 60 Minutes
- Questions: 40
- Format: Multiple-Choice
- Pass Mark: 65%

What's Next

Modern organisations face the constant threat of cyber attacks. Creating an effective cyber risk strategy to identify and mitigate the risk of cyber crime is the only way to ensure your survival. However, cyber security management planning can be complex and costly. With so many best practices and standards to choose from, how do you get started on your plan?

Our three-day Managing Cyber Security Risk training course will give you the knowledge to create a plan that not only includes the selection of technical countermeasures (controls) but also considers the people, processes, governance, leadership and culture of your organisation.

Additional Information

How will I receive my exam results and certificates?

Provisional exam results will be available immediately on completion of the exam. Confirmed exam results will be issued within ten working days from the date of the exam.

Certificates for those who have achieved a passing grade will be issued within ten working days from the date of the exam.

Results notifications and certificates are sent directly to candidates by the relevant exam board in electronic format; please note that hard copy exam certificates are not issued.