Cyber Incident Response Management Foundation

Duration: 1 Day

Overview:

Find out how to effectively manage and respond to a disruptive incident, such as a data breach or cyber attack, and take appropriate steps to limit the damage to your business, reputation and brand.

This course will provide an introduction to developing a cyber incident response programme to protect your business.

Qualification:

Cyber Incident Response Management (CIRM F) qualification (ISO 17024-certificated). Exam included in course. This course qualifies for 7 CPE/CPD points.

Course Overview

Cyber attacks are now classed as the top threat to organisations. With the average cost of a cyber attack being £857,000 the financial implications for businesses are not something to ignore. It's not just the financial loss but the damage to brand and reputation that businesses need to plan for.

This course will teach you the components of the cyber kill chain, recognise common cyber threats and understand common threat actors. Plus, how to define the structure, role and responsibilities of the cyber incident response team.

Who should attend this course?

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.

Job titles:
- Business managers
- Compliance managers
- IT managers
- Helpdesk managers
- Project managers
- Risk managers
- Information security managers
- ISO 27001 lead auditors
- PCI QSAs

What does the Cyber Incident Response Management Foundation training course cover?

- Understand key definitions and legal requirements that underpin incident response.
- Identify the components of the cyber kill chain, recognise common cyber threats and understand common threat actors.
- Define the structure, role and responsibilities of the incident response team.
- Comprehend the seven stages of incident response.
- Propose the steps to formulate and test an incident response plan and define the scope of a business impact analysis.
- Apply incident response techniques to common risk scenarios.
- Know the role of cyber resilience in supporting incident response management.
- Manage communications and reporting requirements under the General Data Protection Regulation (GDPR) and the Directive on security of network and information systems (NIS Directive).

Course agenda:

- What is incident response management?
- Cyber risk
- The cyber incident response team
- The cyber incident response process
- The cyber incident response plan
- Cyber incident response scenarios
- Scenario practical exercise
- Cyber resilience

What's included in this course?

- A professional training venue with lunch and refreshments;
- Full course materials (digital copy provided as a PDF file);
- The Cyber incident Response Management exam; and
- A certificate of attendance.

What equipment should I bring?

The exam is an online exam. You will need to bring a 'pop-up enabled' laptop/tablet to the venue. Full details on how to access the exam will be provided by email 1–2 days before sitting the exam.

The Cyber incident Response Management exam

Attendees take the CIRM F, ISO 17024-certificated, exam set by IBITGQ at the end of the course. This is a one-hour multiple-choice online exam, consisting of 40 questions. Candidates need to achieve a minimum of 65% to pass. There is no extra charge for taking the exam.

What qualifications will I receive?

Cyber Incident Response Management (CIRM F).

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.

Can exams be retaken?

Yes, if you are unsuccessful on the first attempt you can retake the exam for an additional fee. You can email us to schedule the retest for the exam.

Are there any prerequisites for this course?

There are no formal entry requirements but this is a professional course. It is assumed that attendees will have a good general understanding of cyber security principles and controls that underpin the protection of confidentiality, integrity and availability of data, gained through practical experience or reading.

Is there any recommended reading?

We would recommended purchasing one or more of the following:
- True Cost of Information Security Breaches and Cyber Crime
- Assessing Information Security - Strategies, Tactics, Logic and Framework
- Disaster Recovery and Business Continuity