Managing Cyber Security Risk Training Course – 3 days

BENEFIT

Learn how to develop and deploy an effective cyber security strategy to mitigate cyber risks and cyber crime.

Format:Classroom sessions from 09:00 to 17:00

QUALIFICATION

Build your career by achieving Managing Cyber Security Risk (CCRMP).

- Exam included in course.
- The world's first accredited cyber security management course.

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

The three-day Managing Cyber Security Risk classroom training course delivers the knowledge and practical skills to develop and deploy effective cyber security risk management strategies.

Drawing on real-life case studies, an experienced senior information risk consultant will provide you with insights to enable you to create a blueprint for a plan that not only includes the implementation of technical measures (controls) but also takes into account the people, processes, governance, leadership and culture in your organisation.

WHAT WILL YOU LEARN

- The nature of cyber risk and types of cyber attack.
- The difference between cyber security and cyber resilience.
- Lessons from life with examples of real cyber breaches.
- An understanding of current cyber security standards and best practices:

- PAS 555
- 10 Steps to Cyber Security
- 20 Critical Controls for Cyber Defence
- Cyber Essentials scheme
- ISO 27001 and integrated management systems
- Links to other standards, including ISO9001 and ISO20000
- Other frameworks such as COBIT 5, PCI DSS, RESILIA

- The role and the importance of people, processes and technology.
- Approaches to risk management, cyber incident response and business continuity.
- How ISO 27001 provides a backbone for protecting your organisation.
- Why ISO 22301 is essential to achieving cyber resilience in the event of an attack

And, because it's important to prove that your plan is working:
- How to demonstrate cyber security assurance to stakeholders including your board, staff, partners and customers.

The course also includes a case- study workshop that explores tackling cyber security within a fast-growing international organisation.

Gain the Managing Cyber Security Risk (CCRMP) qualification
This course will prepare you for an examination on the last day of the training programme. Successful candidates will be awarded the Managing Cyber Security Risk (CCRMP) qualification, issued by the International Board for IT Governance Qualifications (IBITGQ). There is no extra charge for taking the exam at the end of the course.

This course also qualifies for 21 CPD/CPE credits.

WHO SHOULD ATTEND THIS COURSE

• Senior directors (CEO, CIO, CSO) responsible for strategic and business planning.
• IT and information security managers responsible for cyber security.
• ISO 27001 Lead Implementers and Lead Auditors.
• Professionals who hold CISA, CISM, CISSP, CRISC or CISMP certifications, who wish to apply current knowledge to the broader context of cyber   security.
• Risk and compliance managers or consultants who require an understanding of cyber security risk management outcomes and processes.

ENTRY REQUIREMENTS

While there are no formal entry requirements, we assume that delegates are senior managers, directors or consultants. Knowledge of information technology is desirable but not essential, as the key objective of this training course is to help you to understand and mitigate the business risks associated with the use of cyberspace.