PURPLE GRIFFON
The IT Service Management Training & Consultancy Specialists

Course Title: Managing Cyber Security Risk	**Course Duration**: 3.0 Days
Exam: Included	**Exam Type**: Proctored Exam
Qualification: Managing Cyber Security Risk (CCRMP) Certificate	

Course Syllabus

Our Managing Cyber Security Risk training course will cover the following:

- The geopolitical, legal and regulatory context of cyber risk.
- Cyber governance structures.
- How to conduct a cyber security risk assessment.
- The current cyber threat landscape.
- The use of cyber threat intelligence.
- Introduction to the cyber security maturity model.
- Publicly available control frameworks and standards.
- How to implement an integrated management system to assist in cyber security.
- Key aspects of cyber resilience and incident response.
- How to manage a cyber incident.
- How to develop and implement a cyber resilience framework.

Course Overview

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.

Course Learning Outcomes

Our Managing Cyber Security Risk training course will help you:

- Understand the geopolitical, legal and regulatory context of cyber risk;
- Identify and assess threats and potential vulnerabilities and determine business impacts by conducting a risk assessment;
- Appreciate how cyber governance structures help organisations protect their critical assets and meet regulatory compliance objectives;
- Understand existing cyber security frameworks and standards to determine appropriate technical, procedural and personnel controls; and
- Identify and respond to cyber security incidents.

Audience

Our Managing Cyber Security Risk training course is suitable for:

- Senior Directors (CEO, CIO) who need to ensure their organisation is protected.
- IT Directors or Managers responsible for developing and implementing a cyber security risk management strategy.
- ISO27001 Lead Implementers and Lead Auditors.
- Information Security Managers responsible for cyber security.
- 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 who require an understanding of cyber security risk management outcomes and processes.
- Risk and IS Consultants who wish to advise clients on the practical implementation of cyber security risk management.

Entry-Level Requirements

There are expected to have a practical understanding of information security.

Recommended Reading

It is recommended that you purchase one or more of the following:

- IT Governance – An International Guide To Data Security and ISO27001/ISO27002
- CyberWar, CyberTerror, CyberCrime & CyberActivism
- Insider Threat - A Guide To Understanding, Detecting & Defending Against The Enemy From Within

What's Included

Our Managing Cyber Security Risk training course includes the following:

- Full Course Materials (PDF)
- Managing Cyber Security Risk Examination
- A Certificate Of Attendance

Exam Information

Managing Cyber Security Risk Examination:

You will take the Managing Cyber Security Risk exam set by IBITGQ (International Board for IT Governance Qualifications) at the end of our Managing Cyber Security Risk training course.

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

What's Next

Are you looking to start a career in Cyber Security? You can now train with Cyber Security Experts for a complete introduction to cyber security threats, cyber security controls, security frameworks and incident management.

Our one-day Certified Cyber Security Foundation training course is fully aligned with CyBOK v1.1 (Cyber Security Body of Knowledge), which is approved by the NCSC (National Cyber Security Centre).

Additional Information

Data, applications and communication associated with cyber space are used as low-cost and effective IT resources by almost all organisations worldwide. With an increased reliance on the Internet comes a growing and persistent risk of being attacked and compromised, either by accident or with malicious criminal intent. Managing and mitigating this risk is now essential to the survival of all such organisations.