PURPLE GRIFFON
The IT Service Management Training & Consultancy Specialists

Course Title: Certified Cyber Security Foundation & Practitioner	**Course Duration**: 5.0 Days
Exam: Included	**Exam Type**: Proctored Exam
Qualification: Certified Cyber Security Foundation (C CS F) & Certified Cyber Security Practitioner (C CS P)	

Course Syllabus

Certified Cyber Security Foundation Syllabus:

Module 1: Understanding Cyber Security Fundamentals

- The impacts of cyber incidents and events on an organisation.
- Identify the current threat landscape.
- The CIA triad.
- The roles of people, processes and controls in cyber security.

Module 2: Information Security & Governance

- Explain information governance.
- The role of organisational governance and its link to security.
- Introducing the ISO 27014 standard.
- Define a security steering committee.
- Who is responsible for cyber security?

Module 3: Threat, Vulnerability, Risk Assessment & Management

- Definitions of risk, vulnerability, threat and assets.
- The purpose of a risk-based approach.
- Describe risk in terms of impact and likelihood.
- Consider risk and mitigation options.
- The current risk appetite of an organisation.
- Review the use of heat maps.

Module 4: Understanding Security Controls

- The four control categories: preventive, deterrent, detective and corrective.
- The four control types: physical, procedural, personal and technical.
- Understand the concept of Cloud computing.
- Summarise Cloud computing responsibilities.
- Recall symmetric, asymmetric and hybrid cryptography.

Module 5: Information Security Frameworks

- The purpose of policies, standards, procedures and guidelines.
- The need for security awareness.

- The relationship between legislation and cyber security, i.e. the GDPR, CMA.
- Contractual requirements including the PCI DSS (Payment Card Industry Data Security Standard).
- Standards bodies including ISO/IEC and NIST.

Module 6: The Security Lifecycle

- Recognise secure coding practices.
- Examples of testing strategies, such as fuzzing and regression testing.
- The importance of patch management.
- Explain change management.
- The use of independent assurance including ISO 27001.

Module 7: The Need For Operational Compliance

- The purpose of auditing.
- Discuss methods of monitoring such as IDS, IPS and SIEM.
- Explain the five phases of incident management.

Certified Cyber Security Practitioner Syllabus:

- Typical malware attacks and how to detect and respond to them.
- Adversarial behaviours and the frameworks used to understand malicious operations.
- Fundamental concepts of security operations and incident management.
- Digital forensic techniques and their application.
- Introducing cryptography.
- How security can be ensured at the operating system and hypervisor levels.
- Distributed systems security.
- Authorisation, authentication and accountability, and their relationship with access control.
- Prevention, detection and mitigation of cyber attacks on software applications.
- Web and mobile device cyber security.
- Secure software design and the secure software lifecycle.
- Implementing network security.
- Hardware security and how it is measured and protected.
- Research trends and characteristics in the (CPS) cyber-physical systems security field.
- Challenges and opportunities of physical layer and telecommunications security.

Course Overview

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

Course Learning Outcomes

Our Certified Cyber Security Combined Foundation & Practitioner training course will give you the skills required to deliver infrastructure, application, information and operational cyber security by implementing appropriate technical and organisational controls.

It also prepares you to pass the internationally recognised IBITGQ (C CS F) and (C CS P) examinations on the first attempt.

Audience

Our Certified Cyber Security Combined Foundation & Practitioner training course is particularly suitable for anyone starting, or wanting to start, a career in Cyber Security. It will also benefit operational staff, business directors and managers who wish to improve their understanding of cyber security and its impact on their organisation.

Entry-Level Requirements

Our Certified Cyber Security Combined Foundation & Practitioner training course has no entry-level requirements, but it is beneficial for you to have basic IT knowledge.

Recommended Reading

We recommend that you purchase and read the following textbook before the Certified Cyber Security Foundation training course:
Information Security Management Principles – Third Edition

What's Included

Our Certified Cyber Security Combined Foundation & Practitioner 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. Our course materials include an interactive PDF and an online quiz tool for knowledge testing. Full details on how to access the exam will be provided by email 1–2 days before sitting the exam.

Exam Information

You will take the Certified Cyber Security Foundation (C CS F) and Certified Cyber Security Practitioner (C CS P) exams set by IBITGQ (International Board for IT Governance Qualifications):

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

What's Next

Our five-day BCS Certificate In Information Security Management Principles (CISMP) training course covers the range of concepts, approaches and techniques that are applicable to the BCS Foundation Certificate in Information Security Management Principles.

Additional Information

Our Certified Cyber Security Combined Foundation & Practitioner training course focuses on building the introductory knowledge associated with the CyBOK categories:

- Human, Organisational & Regulatory Aspects
- Attacks & Defences
- Systems Security
- Software & Platform Security
- Infrastructure Security