Cyber Security Foundation + Practitioner™

Duration: 5 days

ALC's 5-day Cyber Security Foundation+Practitioner™ course is designed for anyone who wants a sound understanding of Information / Cyber Security and a solid base on which to build their career. It is ideal for someone wanting to start a career in Cyber, or to transition their career. There are no pre-requisites to attend.

The course follows a robust syllabus that covers all the key areas you need to know. At the same time it provides maximum regional relevance by fully taking into account appropriate sections from the Australian Government Information Security Manual (ISM).

Who Should Attend

This course is designed for:

- Anyone starting a career in Information / Cyber security
- IT professionals wanting to transition their career into Cyber Security
- Anyone needing a robust introduction to Cyber Security
- Anyone planning to work in a position that requires cyber security knowledge
- Anyone with information / cyber security responsibilities
- Anyone who has learned "on the job" but who would benefit from a formal presentation to consolidate their knowledge
- Professionals familiar with basic IT and information security concepts and who need to round out their knowledge

Learning Outcomes

The key objective of the course is for each participant to be able to leave the course with a very solid understanding and appreciation of the fundamentals of Cyber Security:

- Cyber Security Concepts
- Risk Management
- Security Architecture
- Implementing security in networks, endpoint systems, applications and data
- Cryptography
- Business Continuity and Disaster Recovery Planning
- Incident Response

Course Contents

1. Cyber Security Concepts

- Cyber Security Concepts and Definitions
- Cyber Security Strategy
- Laws, Regulations and Industry Standards
- Roles and Responsibilities
- Professional Organisations and Ethics
- Introduction to the Case Study

2. Risk Management

- Risk Management Concepts and Definitions
- Threats and Opportunities
- Controls, Countermeasures and Enablers
- Business Impact Analysis

3. Security Architecture

- The key role of security architecture
- Concepts and Definitions
- Security Architecture Frameworks
- Security Architecture Design Principles
- Service Models
- OSI and TCP/IP Models
- Cryptography

4. Implementing Security

- Network Security
- Endpoint Security
- Application Security
- Data Security
- Essential Eight

5. Cryptography

- Cryptography Key Terms and Concepts
- Symmetric Algorithms
- Asymmetric Algorithms
- Hashing Algorithms
- Non-Repudiation
- Cryptographic Attacks
- Implementing Cryptography in the Real World

6. Business Continuity and Disaster Recovery Planning

- Business Continuity Planning
- Disaster Recovery Planning
- BCP/DRP Training and Awareness
- Testing and Maintenance of the BCP/DRP

7. Incident Response

- NIST Cyber Security Framework
- Cyber Forensics
- Incident Response Management
- Security Assurance

8. Cyber Security Foundation + Practitioner™ Exam

The exam is held in the classroom at the end of Day 5. The exam is 2 hours in duration and comprises two parts. In Part A there are 80 questions worth 1 mark each. In Part B there are 10 questions worth 2 marks each. The pass mark is 65%. There is only one correct answer to each question and no marks are deducted for incorrect answers.

The Cyber Security Foundation+Practitioner Certificate is issued to those who successfully pass the exam