CSF+P® CYBER SECURITY FOUNDATION+ PRACTITIONER

DURATION: 5 DAYS

CYBER SECURITY

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 Security, 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).

LEARNING OUTCOMES

The key objective is for each participant to complete the course and retain a very solid understanding and appreciation of the fundamentals of Cyber Security:

- Cyber Security Concepts
- Risk Management & Assurance
- Security Architecture
- Physical Security
- Network Security
- Endpoint Security
- Incident Response

One of the special features of this course is its mix of theory and practical exercises, all designed to maximise understanding and retention. Strong use is made of a case study. Participants are provided with a download link where sample Word and Excel templates for the case study may be found, along with useful artefacts referenced in the material. Exercises include:

- Develop an asset register
- Identify threats, determine risks, and make recommendations
- Evaluate service provider models, contrasting risks and opportunities
- Discuss risks associated with storing data in the cloud
- Select security architecture design principles
- List and prioritise business-critical operations for business continuity
- Evaluate the benefits of an in-house incident response capability versus using a managed service model

WHO SHOULD ATTEND

- **This course is desgined 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

COURSE CONTENTS

1. CYBER SECURITY CONCEPTS
- Cyber Security Concepts
- Cyber Security Strategy
- Laws & Regulations
- Standards & Frameworks
- Roles & Responsibilities
- Introduction to the Case Study
- Practical session:
- Exercise #1 – Development of a cyber asset register

2. RISK MANAGEMENT
- Risk Management Concepts and Definitions
- Risk Management
- Threats and Opportunities
- The Internet of Things
- Controls and Enablers
- Defence-in-Depth Controls
- CERT NZ Critical Controls
- ACSC Essential Eight
- Practical session:
- Exercise #2.1 – Development of a threat taxonomy and identification of vulnerabilities
- Exercise #2.2 – Evaluate current controls and current risk level

3. SECURITY ARCHITECTURE
- Security Architecture Concepts and Definitions
- Certification and Accreditation
- Service Models
- Cloud Computing
- Cryptography
- Emerging Technologies
- Practical session:
- Exercise #3 – Recommendations for service provider models in addressing risks
- Exercise #4.1 – Identify the challenges associated with using cloud solutions
- Exercise #4.2 – Identify security architecture design principles

5. PHYSICAL SECURITY
- Perimeter Security
- Building Security
- Physical Access Control
- Environmental Controls

5. NETWORK SECURITY
- Network Fundamentals
- Network Security

6. ENDPOINT SECURITY
- Endpoint Security
- Application Security
- Data Security
- Practical session:
- Exercise #5.1 – Complete the risk assessment from exercise 2 by recommending controls
- Exercise #5.2 – Create a data classification scheme

7. INCIDENT RESPONSE
-
- Incident Response Management
- Business Continuity and Disaster Recovery
- Digital Forensics
- Security Assurance
- Practical session:
- Exercise #6 – Identify and rank the three most important business operations
- Exercise #7 – Examination of insourcing or using a managed service for incident response
- Mock Exam