Cyber Security

Foundation & Practitioner®

"The ideal introduction for anyone who wants to get a good handle on **Cyber Security**"

VIEW COURSE INFORMATION >

AUSTRALIA'S NUMBER ONE SECURITY TRAINING PROVIDER

Cyber Security

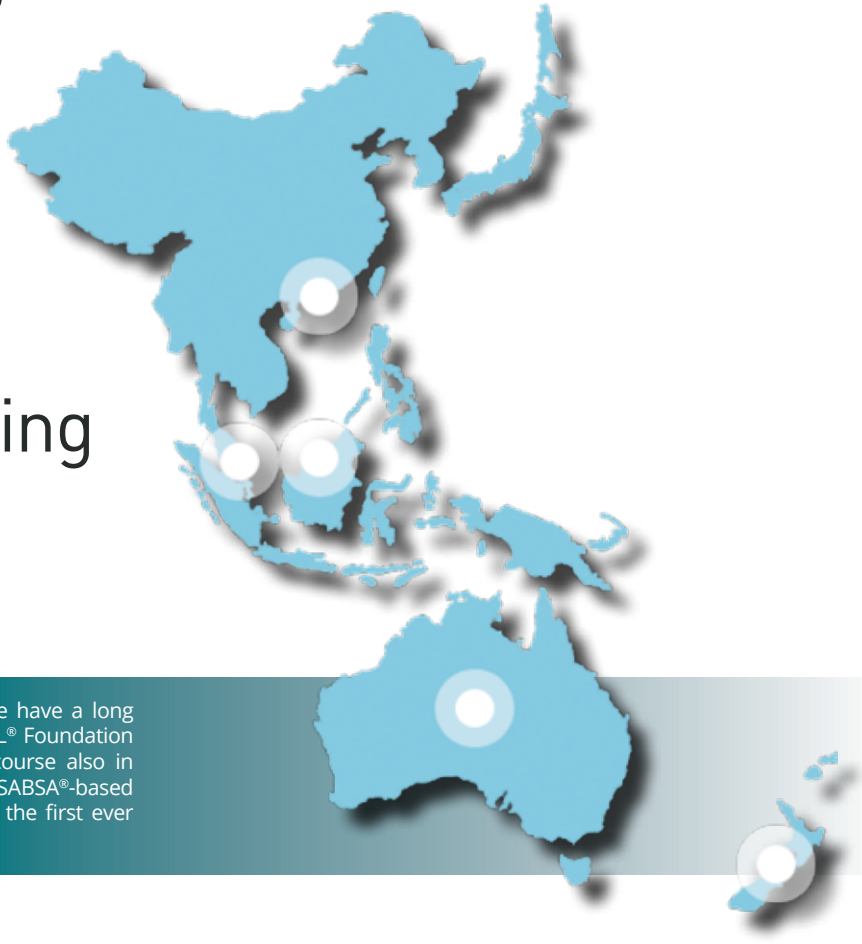
Sydney | Melbourne | Canberra

Brisbane | Perth

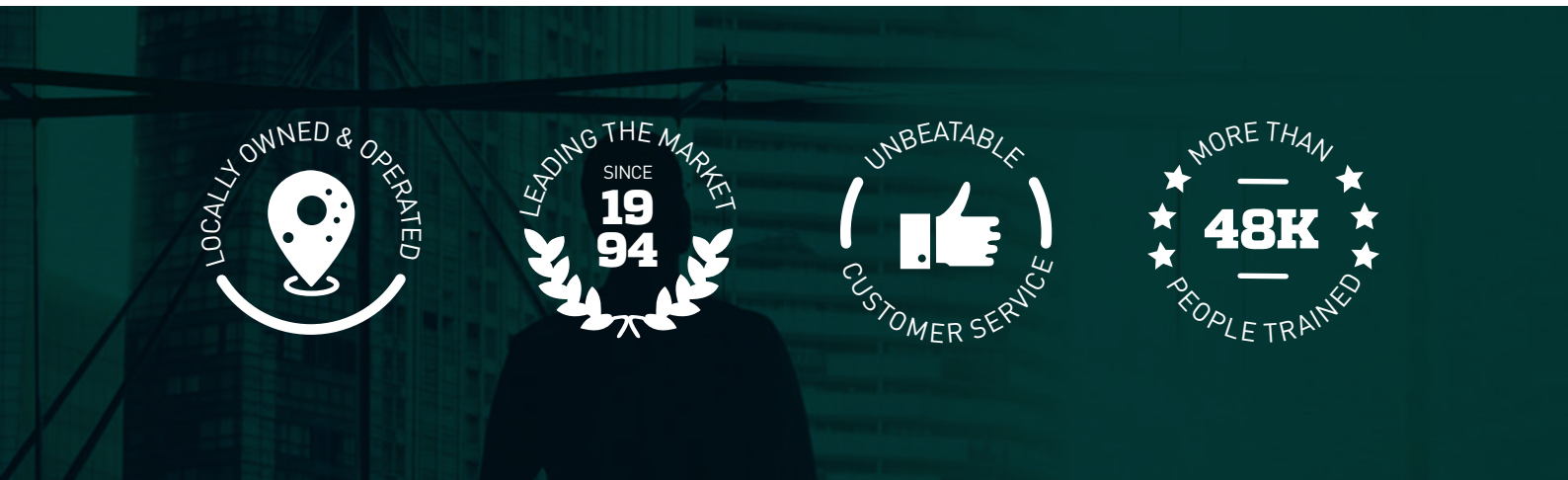
www.alccyber.com.au

Australia's leading provider of Information/Cyber Security Training

- Outstanding Trainers
- Industry Leading Qualifications
- Fully Accredited
- Customer Focus
- Competitive Pricing
- Top Locations



ALC has been presenting leading-edge IT training since 1994. We have a long background in best-practice certification training, with our first ITIL® Foundation Certificate course being held in 1999, and our first PRINCE2® course also in 1999. We have been offering COBIT® certification since 2006 and SABSA®-based information security courses since 2003.Now, in 2017 we launch the first ever **Cyber Security Foundation & Practitioner®** course.



SABSA® CISSP® CISM® CSX®

Director of Cyber Security

Peter Nikitser

Peter is Director, Cyber Security Services at ALC Group where he is responsible for the development and implementation of ALC Group's cyber security training program throughout the Asia-Pacific region and for managing ALC's broader range of cyber security services. Peter is exceptionally well qualified for this role and brings to bear a career spanning 30 years in IT with the last 15 years focussing on information security.

Prior to joining ALC Peter was Manager, Cyber Security & Risk Services at Deloitte Australia where he was responsible for the management and delivery of cyber security and risk services to Deloitte clients across Australia, including federal government, financial services, industry and critical infrastructure providers.

Prior to this Peter was Senior Security Consultant at CSC where he delivered services focussing on security architecture and Cyber Assurance. Previous positions have included defence, government, health, petroleum and mining sectors.

Peter is a founding member of AusCERT and assisted with the establishment of the Sri Lankan national CERT. His specialities are Enterprise Security Architecture, Digital Forensics, Healthcare, Risk Assessments and Cyber Security.

His formal qualifications include a Masters Degree in Information Technology (MInfTech) at Queensland University of Technology (QUT) in Brisbane, and a Bachelor of Science (BSc) at Australian National University (ANU) in Canberra. Peter holds certifications in CISSP, ISSAP, CISM, CRISC, CSX, CISMP, PCI-P, TOGAF and is the first person to attain SABSA Masters status in Australia.

www.alccyber.com.au

Cyber Security

FOUNDATION®

The course with maximum relevance. Fully takes into account appropriate sections from Australian Government Information Security Manual (ISM).

Course Overview

ALC's 3-day "flagship" Cyber Security Foundation® is the ideal course for anyone who needs to get a good all-round understanding of Cyber Security today. You don't have to be an aspiring security professional to do this course, it is suitable for everyone. But if you are wanting to start a career in Cyber Security then this course is a great starting point and pairs extra well with our Cyber Security Practitioner course.

The Cyber Security Foundation® course follows a robust syllabus that covers all the key areas. At the same time it provides maximum regional relevance by fully taking into account appropriate sections from the Australian Government Information Security Manual (ISM) and the New Zealand Government's Information Security Manual (NZISM).

Who Should Attend

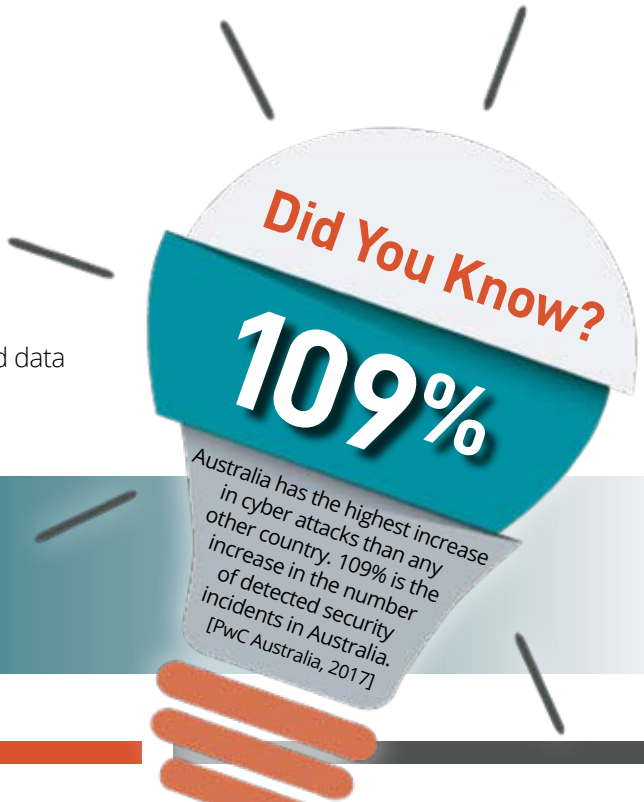
The course is ideal for:

- Anyone needing a robust introduction to Cyber Security
- Anyone planning to work in a position that requires cyber security knowledge
- Anyone starting a career in Information / Cyber security
- IT professionals wanting to transition their career into Cyber Security
- 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

Key areas covered include:

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



"The course was excellent. The instructor was highly knowledgeable and had an extremely personable approach. The learning materials were very good. The venue was most suited and lunch was excellent. Lastly, I am extremely confident that I have the right level of knowledge to proceed and succeed."

S. T., Department of Defence

"The ideal introduction for anyone who wants to get a good handle on **Cyber Security**"

Course Contents

1. Introduction

- Concepts and Definitions
- Difference between IT Security, Information Security and Cyber Security
- Assets, Threats & Vulnerabilities
- Likelihood, Consequence and Impact
- Inherent Risk, Current Risk and Residual Risk
- Cyber Security Strategy
- Supporting Business Goals and Objectives
- Cyber Security Policy Framework
- Awareness, Training and Education

2. Risk Management

- Risk Management Concepts and Definitions
- Risk Avoidance, Mitigation, Transfer and Acceptance
- Risk Appetite and Risk Tolerance
- Threats and Opportunities
- Assessing the current threat landscape
- Advanced Persistent Threats
- Bring Your Own Device or Technologies
- The Internet of Things
- Insourcing and Outsourcing
- Controls 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
- In-sourcing
- Managed Services
- Cloud Services

4. Cryptography

- Symmetric, Asymmetric and Hashing Algorithms
- Non-Repudiation
- Real-world Use Cases

5. Implementing Security

- Network Security – routers, switches, firewalls, intrusion detection and prevention
- Endpoint Security – servers, desktop systems, laptops, tablets and mobile devices
- Application Security
- OWASP Top 10
- Web Application Firewall
- Data Security
- Data owners, data classification, labelling
- Access control
- Data governance and lifecycle
- Data remanence

6. Business Continuity & Disaster Recovery Planning

- Business Continuity Planning
- Disaster Recovery Planning
- BCP/DRP Training and Awareness
- Testing and Maintenance of the BCP/DRP
- Security Assurance
- Vulnerability Assessments and Penetration Testing
- Minimum Security Baselines

7. Incident Response

- Detection
- Auditing, logging and security technologies
- Security Information and Event Management System
- Prevention
- Authorisation, encryption, firewalls, intrusion prevention, anti-malware
- Response
- Security events and incidents
- Legal aspects
- Incident Response Process
- Incident Management Team
- Computer Forensics

Cyber Security

PRACTITIONER®

This course provides you with the complete rounding of knowledge essential to be a Cyber Security expert.

Course Overview

The Cyber Security Practitioner® is all about applying the theory. It builds upon and reinforces the material learnt in the Foundation module. The course makes strong use of a case study, along with workshops and exercises. Participants will be provided with sample Word and Excel templates for use.

Who Should Attend

The Practitioner module is suitable for anyone who has previously taken the Foundation module. Because the content focuses on the practical side it would typically attract those who have a more serious career interest in security.

The 5-day combined course is ideal for those who have 2 years or less experience in security or those who are already in IT and now want to transition into security.

Learning Outcomes

The key objective of the Practitioner module is for each participant to be able to apply the theory learnt from the Foundation course to a case study.

During this module you will:

- Develop an asset register
- Identify threats and determine risks, and make recommendations
- Create a data classification scheme and use this for managing risks with cloud solutions
- Identify and discuss the advantages and disadvantages of different encryption technologies
- List and prioritise business- critical operations for business continuity
- Identify and discuss various approaches to security assurance
- Identify risk remediation strategies and include in a brief management report

Did You Know?

85%

A Global Cyber Security Status report by ISACA® has revealed that 85% of those who participated in the survey believed that there is a shortage of skilled cyber security professionals. (ISACA®, 2015)

57% The same report by ISACA® has revealed that 57% believe their organisation is NOT prepared for a sophisticated cyber attack. (ISACA®, 2015)

Also, 53% believe it is difficult to identify who has an adequate level of skills & knowledge. (ISACA®, 2015) **53%**

www.alccyber.com.au

> *The trainer's level of professional experience combined with a capacity to communicate personably and effectively with a diverse group added to my experience and contributed greatly to the amount of information I was able to bring away with me from the course. I could not recommend them highly enough either as a trainer or as a potential consultant.*
>
> **S.M., NEC Australia**

Course Contents

1. Introduction
- Introduction of Case Study

2. Review of Concepts & Risk Management
- Exercise #1: Development of a cyber asset register
- Exercise #2: Development of a threat taxonomy
- Exercise #3: Identification

3. Review of Service Provider Models
- Exercise #4: Recommendations for service provider models in addressing risks

4. Review of Data Classification & Object Labelling
- Exercise #5: Establish a data classification scheme
- Exercise #6: Strategies to safeguard data held and managed in the cloud

5. Review of Security Architecture
- Exercise #7: Safeguarding data in transit using encryption
- Workshop #1: List the advantages and disadvantages of encryption

6. Review of Business Continuity
- Exercise #8: Identify and rank the most important business operations
- Workshop #2: List the advances and disadvantages of choosing security audits, vulnerability assessments and penetration tests

7. Review of Reporting to Management
- Exercise #9: Develop the first part of a management report highlighting the most appropriate strategies for managing various risks.

Information Security Courses Available from ALC

- Cyber Security Foundation®
- Cyber Security Foundation+Practitioner
- CISSP® Certified Information Systems Security Professional
- CCSP® Certified Cloud Security Professional
- CISM® Certified Information Security Manager
- CISA® Certified Information Systems Auditor
- CRISC® Certified in Risk and Information Systems Control
- SABSA® Foundation
- SABSA® Advanced A1: Risk, Assurance & Governance
- SABSA® Advanced A3: Architecture & Design
- SABSA® Advanced A4: Incident, Monitoring & Investigations
- ISO/IEC 27001 - ISMS Lead Implementer
- ISO/IEC 27001 - ISMS Lead Auditor
- ISO/IEC 27001:2013 Foundation
- Fundamentals of Incident Handling
- Advanced Incident Handling
- Creating a Computer Security Incident Response Team
- Managing a Computer Security Incident Response Team
- Digital Evidence Fundamentals
- Digital Forensics Practitioner
- Architecting Secure Cloud
- Information Security for Executives
- Security Metrics: the Key to Effective Security Management
- Securing Your TOGAF® Environment

FOR MORE DETAILS CONTACT
learn@alctraining.com.au

alc

Ready to book your next course with ALC Training?

Australia's Number One Security Training Provider

www.alctraining.com.au