Cyber Security

Foundation+Practitioner™

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

VIEW COURSE INFORMATION >

NUMBER ONE SECURITY TRAINING PROVIDER

Cyber Security

www.alctraining.com.my

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.

"I thought the course was excellent – I think the interaction between instructor and students is a large part of being able to learn and understand concepts/ideas especially with relevant examples. I think Peter did this well working with the class."

MARCH 2017

www.alctraining.com.my

Cyber Security

Foundation+Practitioner™

Duration: 5 Days

The course with maximum relevance for anyone wanting a career in cyber security.

ALC's 5-day Cyber Security Foundation+PractitionerTM 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.

Who Should Attend

The course is ideal 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 decurity
- 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

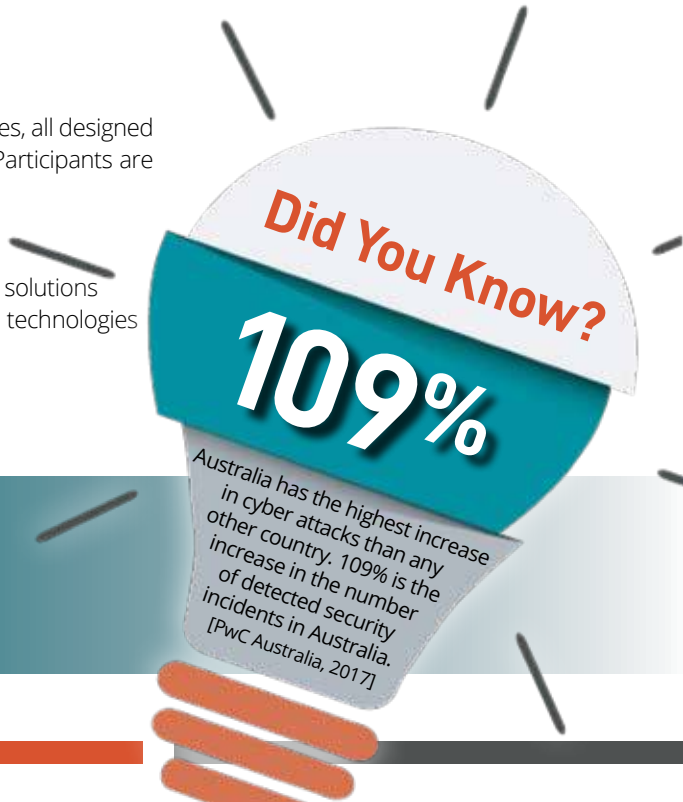
Learning Outcomes

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

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 sample Word and Excel templates for use. Exercises include:

- 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



"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. Cyber Security Concepts

- Cyber Security 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
- Laws, Regulations and Industry Standards
- Roles and Responsibilities
- Professional Organisations and Ethics
- Introduction to the Case Study
- **Exercise #1** – Development of a cyber asset register

2. Risk Management

- Risk Management Concepts and Definitions
  - The stages of risk
  - Systemic and systematic Risk, Risk Aggregation
  - Risk Acceptance, Reduction, Transfer and Avoidance
  - Risk Appetite and Tolerance
  - Governance, Risk Management and Compliance (GRC)
  - Risk Management Process
  - Quantitative, Semi-quantitative and Qualitative Risk
- Threats and Opportunities
  - Assessing the current threat landscape
  - Developing a threat taxonomy
  - Advanced Persistent Threats
  - Bring Your Own Device or Technologies
  - The Internet of Things
- Controls, Countermeasures and Enablers
- Business Impact Analysis
  - Sample Business Impact Analysis Template
  - Sample Business Impact Levels
- Practical session:
  Exercise #2.1 – Development of a threat taxonomy and identification of vulnerabilities
  Exercise #2.2 – Evaluate inherent risk, current controls, current risk, recommend controls and residual risk

3. Security Architecture

- Security Architecture Concepts and Definitions
- Security Architecture Frameworks
  - SABSA
  - TOGAF
- Security Architecture Design Principles
- Service Models
  - Insourcing
  - Outsourcing
  - Managed Services – Single provider, multiple provider and prime provider
  - Cloud Services – Cloud service models and Cloud deployment models
- **Exercise #3** – Recommendations for service provider models in addressing risks
  Exercise #4 – Identification of security architecture design principles

4. Implementing Security

- OSI and TCP/IP Models
- Network Fundamentals
  - Network Security
  - Network Topologies
  - Security Zones
  - Network Security Technologies
  - Virtualisation Benefits and Security Challenges
- Endpoint Security
  - Servers, desktops, laptops, tablets, mobile devices, wearables
  - Endpoint Security Technologies
  - Specialised Endpoint Systems
- Application Security
  - Software Development Lifecycle
  - OWASP Top 10
  - Web Application Firewall and Database Firewall
- Data Security
  - Data owners, data classification, labelling
  - Access control
  - Data governance and lifecycle
  - Data remanence
- Australian Signals Directorate Top 35 and Essential Eight
  - ASD Top 4
  - ASD Essential Eight
  - SANS Top 20 mapped to ASD Top 35 and other frameworks
- **Exercise #5** – Establish a data classification scheme
  Exercise #6 – Design a secure network topology incorporating network security zones, overlay the data classification scheme and placement of recommended controls

5. Cryptography

- Cryptography Key Terms and Concepts
- Symmetric Algorithms
- Asymmetric Algorithms
- Hashing Algorithms
- Non-Repudiation
- Cryptographic Attacks
- Implementing Cryptography in the Real World
- **Exercise #7** – Select appropriate symmetric, asymmetric and hashing algorithms and develop a draft encryption standard

6. Business Continuity and Disaster Recovery Planning

- Business Continuity Planning
  - NIST SP800-34 as a framework
- Disaster Recovery Planning
  - Relationship between the BCP and DRP
  - Events that trigger a BCP/DRP
- Developing the BCP and DRP
  - Application of NIST SP800-34
  - Initiation
  - Business Impact Analysis
  - Identification of preventive controls
  - Recovery strategies
  - Plan design and development and important BCP/DRP frameworks
  - Ongoing maintenance
- **Exercise #8** – Identify and rank the most important business operations

7. Incident Response

- NIST Cyber Security Framework
- Cyber Forensics
  - General phases of the forensic process
  - Anti-forensics
  - Forensic media analysis
  - Network forensics
  - Forensic analysis of software, Embedded devices and Electronic Discovery
- Incident Response Management
  - Security events and Security incidents
  - Incident Response Methodology using NIST SP800-61
- Security Assurance
  - Defining and implementing meaningful metrics
  - Configuration management
  - Minimum Security Baselines
  - Vulnerability Assessments
  - Penetration Testing
  - Security Audits
  - Security Assessments
  - Log reviews, retention, centralisation and analysis
  - Security Information and Event Management System (SIEM)
- **Exercise #9** – Examination of insourcing or using a managed service for incident response
  Exercise #10 – Develop the first part of a management report highlighting the most appropriate strategies for managing various risks and a high-level roadmap of activities

8. Cyber Security Foundation+Practitioner™ Exam

Two hours, multiple choice.

Testimonials

More then 48,000 people trained by ALC.

A very interesting course and has provided an excellent foundation for helping improve security practices at my company. It's also given me insights into future career paths.

IT PORTFOLIO MANAGER, INTERNATIONAL CHARITY

Great course & lots of content. Peter was very good & made course content very relevant.

SECURITY ANALYST, INTERNATIONAL BANK

Trainer is very experienced. The examples Peter showed were very interesting and relevant.

MANAGER, BUSINESS SERVICES SUPPORT TEAM, AUSTRALIAN BANK

I thought the course was excellent – I think the interaction between instructor and students is a large part of being able to learn and understand concepts/ ideas especially with relevant examples. I think Peter did this well working with the class.

ANALYST, DEPT DEFENCE

The course was excellent – content, process, style etc all very good.

ASSISTANT DIRECTOR IT SYSTEMS, GOVT DEPT

Peter is an extremely knowledgeable instructor and exhibited the right personality for effective learning for students across a broad skill set. My thanks and appreciation to Peter for his time and effort during the course.

DIRECTOR, DEPT DEFENCE

Thank you very much Peter, excellent material – very well presented.

IT OFFICER, GOVT AGENCY

Some topics were a refresher for me which is great. I wish I did this course much earlier in my role, I was able to understand majority of the topics as I had the experience. Course was a good speed for me and Peter took care to bring a lot of worldly experiences and analogies and examples.

INFORMATION SECURITY GOVERNANCE OFFICER, ENGINEERING AND INFRASTRUCTURE SERVICES

Great introductory course covering a good perspective of the overall cyber security space.

PROJECT MANAGER, PRIVATE CONSULTANT

Peter is very experienced and I am very impressed how he communicated on a very digestible and clear format.

CEO, TECHNOLOGY SERVICES PROVIDER

Cyber Security

CAREER PATH

PROFESSIONAL

CISSP® Certifed Information Systems Security Professional 5 DAYS

CISSP® is long regarded as the gold standard of security qualifications. This 5-day accelerated course provides information security professionals with a fully-immersed, minimum-distraction CISSP CBK training and certification experience. The course will broaden and deepen your understanding of all CBK domains as required for the (ISC)2 CISSP accreditation examination

CCSP® Certified Cloud Security Professional 5 DAYS

Gain a thorough understanding of the information security risks and mitigation strategies critical to data security in the cloud in this (ISC)² Certified Cloud Security Professional (CCSP) Exam Preparation course. This course covers the six domains of the Official (ISC)² CCSP Common Body of Knowledge (CBK®) and prepares you to take the CCSP exam to become a Certified Cloud Security Professional.

CISM® Certified Information Security Manager 5 DAYS

CISM is one of the most important InfoSec qualifications in the world today. CISM defines the core competencies and standards of performance expected of world-class information security managers. It provides executive management with the assurance that those who have earned their CISM have the experience and knowledge to offer effective security management and advice.

CRISC® Certified in Risk and Information Systems Control 3 DAYS

CRISC is one of the most highly sought-after qualifications. It is the only certification that prepares and enables IT professionals for the unique challenges of IT and enterprise risk management and positions them to become strategic partners to the enterprise. This three day course comprehensively covers the full CRISC syllabus and prepares you for a first-time pass in the CRISC exam.

SECURITY ARCHITECTURE

SABSA® - Foundation 5 DAYS

SABSA is the world's most successful security architecture. It is the leading open-use best practice method for delivering cohesive information security solutions to enterprises. This 5-day Foundation Certificate program has been designed to provide participants with a thorough coverage of the knowledge required for the SABSA Foundation Level Certificate.

SABSA® - Advanced 5 DAYS

ALC offers all three SABSA Advanced modules: A1 – Risk & Assurance; A3 - Architecture & Design; A4 : Incident Monitoring & Investigations. Each course is 5 days duration.

ISO 27000 FOR ISMS

ISO/IEC 27001: 2013 ISMS Lead Implementer 5 DAYS

Teaches how to scope and deploy an Information Security Management System within the organisation. Update your Project Management skillset to lead a team through the deployment of ISMS. You will play a pivotal role in ensuring security management adheres to the internationally recognised ISO standard.

ISO/IEC 27001: 2013 Lead Auditor (5 days)

Candidates and organisations with a working knowledge of Information Security Management Principles and their associated concepts are invited to qualify for the ISO/IEC 27001: 2013 Lead Auditor certification. Combining exercises, tutorials and role play our qualified instructors engage candidates with a thorough working knowledge of how an ISMS audit should be run.

INCIDENT MANAGEMENT

Fundamentals of Incident Handling 5 DAYS

This 5-day course based on the world-acclaimed SEI syllabus provides a strong introduction to the main incident handling tasks and critical thinking skills that will help an incident handler perform their daily work. It will provide an overview of the incident handling arena, including CSIRT services, intruder threats, and the nature of incident response activities.

Advanced Incident Handling 5 DAYS

This 5-day course is for computer security incident response team (CSIRT) technical personnel with several months incident handling experience. It addresses techniques for detecting and responding to current and emerging computer security threats and attacks that are targeted at a variety of operating systems and architectures. Prepares incident handlers for system compromises at the privileged (root or administrator) level.

Managing Incident Response Teams 5 DAYS

Provides managers of computer security incident response teams (CSIRTs) with a pragmatic view of the issues they will face in operating an effective team. Also provides comprehensive overview of the incident handling process and the types of tools and infrastructure needed to be effective.

Digital Forensics Fundamentals 4 DAYS

Three-day course provide a solid and practical coverage of the principles of identifying, preserving and analysing digital evidence, such as computers, mobile phones, and online sources. Covers industry best practice when conducting forensic analysis of electronic devices as well as end-to-end process and legal requirements for chain of evidence and chain of custody. The course is targeted at Investigators, would-be digital evidence examiners, law-enforcement personnel, information security professionals and anyone wanting to get started with handling and investigating digital evidence.

Cyber Security

Foundation+Practitioner™

REFER TO OUR WEBSITE FOR DATES

ALSO AVAILABLE FOR IN-HOUSE PRESENTATION

FOR MORE DETAILS CONTACT
learn@alctraining.com.my

This is the ideal course for anyone who wants to start a career in cyber security, or if you have a team to upskill into cyber security.

alc

Ready to book your next course with ALC Training?

Number One Technology Training Provider

www.alctraining.com.my