alc
Cyber Solutions by Thales

CSF+P CYBER SECURITY

FOUNDATION + PRACTITIONER™

THE GO-TO COURSE TO TRANSITION YOUR CAREER OR UPSKILL YOUR TEAM

\ Private & Public Course Options
\ Face-to-Face or Virtual Instructor-led

LEADING IT SINCE '94
EST. 1994

alctraining.com.my

alc TRAINING
Cyber Solutions by Thales

AUSTRALASIA'S LEADING PROVIDER OF CYBER SECURITY TRAINING

TRAINING WITH ALC
SATISFACTION GUARANTEED

- Quality IT Training since 1994
- Outstanding Trainers
- Industry Leading Qualifications
- More than 60,000 Trained
- Customer Focus, Competitive Pricing

"The trainer was exceptional and I greatly valued his experience, expertise and good humour throughout. His rational advice, particularly around the exam technique and question style is invaluable for study preparation."

***

"Instructor has vast experience and expertise, I learned a lot from him.
Aside from the theoretical lessons, he shared real-life examples which made it easier to understand the theories."

***

"ALC admin staff were extremely helpful and responsive to emails. The trainer is extremely experienced and represents ALC and the cyber security industry extremely well. He displayed extremely high job knowledge and experience at all levels (strategic and tactical), but the thing that was impressive was him applying his experience to his students workspaces and on top of that; related course content to the students so that the learning content is applied better. I will be back to do another course with ALC!"

CSF+P CYBER SECURITY

FOUNDATION + PRACTITIONER™

DURATION: 5 DAYS

Cyber security certifications traditionally have been aimed at those who have been in the industry for many years and who are looking for a certification that validates both their knowledge and experience.

Cyber Security Foundation+Practitioner™ addresses the skills gap by providing a concentrated 5-day learning experience that covers the six key domains of cyber security but at a level targeted at those who do not yet have professional-level experience.

It is the standout course for anyone who needs a sound understanding of Cyber Security. It provides a solid base on which to build or transition your career and is the ideal course if you have a team to rapidly upskill.

LEARNING OUTCOMES

The course provides a solid understanding of the fundamentals and a comprehensive coverage of the six key domains of cyber security:

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

WHO SHOULD ATTEND

This course is designed for:

- Anyone needing a robust introduction to cyber security
- IT and other personnel wanting to transition their career into cyber security
- Anyone planning to work in a position that requires solid cyber security knowledge
- Anyone who has learned “on the job” and would benefit from a formal presentation to consolidate their knowledge

THE COURSE WITH MAXIMUM RELEVANCE

Nearly all cyber certifications are US-centric or UK/Euro-centric with examples and case studies of limited relevance to local audiences. CSF+P follows a robust syllabus that covers all the key areas you need to know. At the same time it provides maximum relevance by using local examples and case studies and by fully taking into account appropriate sections from the Australian Government Information Security Manual (ISM) including the ACSC Essential Eight.

COURSE CONTENT

CYBER SECURITY FOUNDATION+PRACTITIONER™ [5 DAYS]

1. Cyber Security Concepts

\ Cyber Security Concepts
- Defining cyber security
- Cyber security triad
- Cyber security landscape
- Defining assets, threats, vulnerabilities, likelihood, consequence, and risk

\ Cyber Security Strategy
- Business Strategy
- Governance, Risk Management and Compliance (GRC)
- Cyber Security Policy Framework

\ Laws & Regulations
- Privacy laws and principles
- International data protection legislation
- Privacy Impact Assessment (PIA)
- Cyber Crime Law
- Regulations and corporate industry requirements for Directors
- Intellectual property, issues, and attacks

\ Standards & Frameworks
- ISO/IEC 27001
- NIST Cybersecurity Framework
- Payment Card Industry Data Security Standard (PCI DSS)

\ Roles & Responsibilities
- Organisational structure
- Professional organisations

\ Training, and Awareness
- Cyber learning program
- NIST SP800-50r1
- Ethics in cyber security
- The effectiveness of training over time

52%

LACK OF SKILLS AND TRAINING

is the top obstacle to achieving digital trust, followed by Lack of Leadership Buy-In (42%) and Lack of Alignment with Business Goals (42%).

[ISACA Digital Trust Report, 2023]

2. Risk Management

\ Risk Management Concepts
- Assets – tangible and intangible
- Risk definition
- Risk management process overview
- Threats, likelihood, vulnerabilities, consequences
- Business Impact Level schedule
- Various states of risk (inherent, current, residual)
- Specialised risk topics (systemic, systematic, distribution, aggregation)
- Risk Appetite and Tolerance

\ Risk Management
- ISO/IEC 31000 Risk Management Process
- Risk Assessment – Identification, Analysis, and Evaluation
- Risk Treatment
- Risk Register and Risk Treatment Plan
- Risk Monitoring Metrics – KPIs, KRIs, KCIs

\ Threats
- Evolution of the Threat Landscape
- Advanced Persistent Threats
- Lockheed Martin Cyber Kill Chain®
- Developing a threat taxonomy
- Threat characteristics
- Common types of malicious software
- Common malware attack methods
- Surface Web, Deep Web, and Dark Web
- Social Engineering Attacks
- Applets
- Bring Your Own Device
- The Internet of Things

\ Controls
- Definitions
- Types of controls
- Categories of controls
- Defence-in-depth concept
- Application of controls for defence-in-depth

\ Defence-in-Depth Controls

\ CERT NZ Critical Controls

\ ACSC Essential Eight
- Strategies to mitigate Targeted Cyber Intrusions
- The Essential Eight

3. Security Architecture

\ Governance & Architecture
- Governance & Architecture Overview
- Common Architecture Frameworks
- Security Architecture Design Principles – Viega & McGraw, and Saltzer & Schroeder

\ Certification & Accreditation
- Evaluation Standards – Common Criteria, TCSEC, ITSEC, CTCPEC, AISEP
- Common Criteria – Evaluation Assurance Levels
- Internet Engineering Task Force
- FIPS Standards for Encryption
- FIPS 140-3

\ Service Models
- Insourcing, outsourcing, and managed services
- Single provider, multiple providers, and prime provider

\ Cloud Computing
- Characteristics of Cloud Computing
- Cloud Computing Building Block Technologies
- Cloud Service Categories
- Cloud Deployment Models
- Shared Responsibility Model
- Cloud Vulnerabilities & Risks
- Hypervisor – Types 1 and 2
- Server Virtualisation – Benefits and Security Issues
- Storage Virtualisation
- Cloud Access Security Brokers
- Assessing Cloud Environments
- Cloud Security Alliance Top Threats to Cloud Computing

\ Cryptography
- Symmetric algorithms
- Asymmetric algorithms
- Hashing algorithms
- Commercial National Security Algorithm Suite
- Message Authentication Code
- Digital Signatures

\ Emerging Technologies
- Artificial Intelligence – origins, types, ethical use and caution
- Quantum Computing –classical state, quantum state, topoconductors, challenges
- BlockChain

4. Physical Security

- Perimeter Security
  - Fences, gates and bollards
  - Guards, dogs and lighting
  - CCTV
- Building Security
  - Lock grades and key types
  - Lock picking, bump keys and bump guns
  - Adjacent buildings and shared tenancy
  - Demarcation issues
  - Server rooms and storage
  - Doors, windows, and walls
  - Local crime
  - Access control cards
  - RFID Tags
  - Contraband checks
- Physical Access Control
  - Tailgating
  - Mantraps
  - Turnstiles
  - Dumpster diving
  - Motion detectors
- Environmental Controls
  - Electricity
  - Emergency power
  - Electromagnetic interference
  - HVAC for environmental control
  - Fire Suppression Agents
  - Sprinkler Systems

5. Network Security

- Network Fundamentals
  - OSI Model
  - TCP/IP Model – Original and Updated
  - Encapsulation and De-encapsulation
  - Port numbers and TCP/UDP flags
  - TCP three-way handshake
  - Voice over IP (VoIP)
  - Domain Name System (DNS)
  - IP Addressing – Classful, Classless, RFC1918
  - IP Masquerading and Network Address Translation
  - IP version 4 and IP version 6
  - Network Topologies
  - Network Security Zones
  - Zero Trust Networks
- Network Security
  - Firewalls
  - Firewall Designs
  - Firewall Implementation Issues
  - Intrusion Detection and Prevention Systems (IDPS)
  - Secure Email Gateway (SEG)
  - Secure Web Gateway (SWG)
  - Data Loss Prevention (DLP)
  - Public Key Infrastructure (PKI)
  - IEE 802.1x Extensible Authentication Protocol (EAP)
  - Remote Authentication Dial-in User Service (RADIUS)
  - Internet Protocol Security (IPSec)

6. Endpoint Security

- Endpoint Security
  - Servers, desktops, laptops, tablets, mobile devices, wearables
  - Endpoint Detection and Response (EDR)
  - Extended Detection and Response (XDR)
  - Specialised Endpoint Systems
- Application Security
  - Systems Development Life Cycle
  - OWASP Top 10
  - STRIDE Threat Modelling
  - DREAD Threat Modelling
  - Web Application Firewall
  - Database Activity Monitor
- Data Security
  - Data ownership roles and responsibilities
  - Data classification and labelling
  - Authentication, Authorisation and Accounting (AAA)
  - Access control
  - Privileged Access Management (PAM)
  - Access control models and implementation
  - Data governance and lifecycle
  - Data remanence
- 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
  - Security logging
  - Security Information and Event Management (SIEM)
  - Security Orchestration Automation & Response (SOAR)
  - Security events and incidents
  - Incident Response Methodology using NIST SP800-61r3
- Business Continuity and Disaster Recovery
  - Business Continuity Planning
  - Disaster Recovery Planning
  - Standards and Frameworks
  - NIST SP800-34
  - Business Continuity Institute Good Practice Guide
- Digital Forensics
  - General phases of the forensic process
  - Digital forensics challenges
  - Anti-forensics
  - Forensic media analysis
  - Network forensics
  - Embedded device forensics
  - eDiscovery
- Security Assurance
  - Configuration management
  - Minimum Security Baselines
  - Security Audits
  - Security Assessments
  - Security Testing
  - Vulnerability Assessments
  - Penetration Testing
- 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

ALC TRAINING
NOW A PART OF THALES CYBER SERVICES ANZ

ALC is pleased to announce that as of March 2023 ALC has become a part of Tesserent Academy, the education division of Thales Cyber Services ANZ.

ALC is well-known as a leading provider, since 1994, of quality training for business and government throughout Australia, New Zealand and SE Asia. Thales Cyber Services is the largest provider of cyber security services in Australia and New Zealand. The combination of resources ensures that ALC will continue to lead the way in cyber security training and other key areas of Enterprise IT.

Key portfolio streams are:

- Cyber Security
  (SABSA®, CISM®, CRISC®, CISSP®, CCSP®, ISO 27001, NIST, Cyber Security Foundation+Practitioner™)
- New Ways of Working (Agile, Scrum, DevOps)
- Project Management
  (AgilePM®, PRINCE2®, MSP®, P3O®, MoP®)
- IT Service Management
  (ITIL® 4 – Foundation and all Specialist levels)
- Enterprise (TOGAF®, Business Analysis, DevOps, Change Management, Business Relationship Management)
- IT Governance (COBIT®, CGEIT®)
- Privacy(CIPM, CIPT, CIPP/E CDPSE)

Highlights

ALC has a strong background in training and a proven track record of being at the leading edge with a series of firsts:

- CISSP and CISM training since 2005
- World's first SABSA Foundation Certificate course in Sydney in March 2007
- Longest-serving provider of ITIL training in Australia, since August 1999
- Project management training since 1994 and PRINCE2 since 1999

Training Specialists

Training for us is not a sideline activity – it is all that we do. And we have been doing it since March 1994. We are a team of dedicated and capable people who care about what we do. We give it single-minded focus and offer commitment, professionalism, verve and enthusiasm.

PROFESSIONAL LEVEL
CYBER SECURITY CERTIFICATIONS

PUBLIC COURSE DATES ON WEB

FACE-TO-FACE & LIVE VIRTUAL

HELP BRIDGE THE SKILLS GAP WITH ALC - THE TRAINING YOU NEED NOW, AND INTO THE FUTURE. ADDITIONAL CERTIFICATIONS ON OFFER INCLUDE:

- NIST Cybersecurity Framework Practitioner®
- CISSP® Cert. Info. Systems Security Professional
- CISM® Certified Information Security Manager
- CRISC® Certified in Risk & Info.Systems Control
- SABSA® Foundation
- CISA® Certified Information Systems Auditor
- CCSP® Certified Cloud Security Professional
- ISO 27001 Foundation
- ISO/IEC 27001 – ISMS Lead Implementer
- ISO/IEC 27001 – ISMS Lead Auditor

Have Teams to Train?

Private Training Available for All Courses

Have a team to train or want our trainer to come to you to deliver a course? Get in touch today for an obligation free quotation for a private virtual or private in-house event today!

WHAT YOU GET WHEN YOU TRAIN WITH ALC

QUALITY. Many things go into making a great training course but the most important is always the trainer. Everyone claims they have great trainers. What we can say is that we have a long history of sourcing the best. That has been our business model for more than 30 years. For certain subjects our trainers are in fact world leaders. And for other subjects they are all outstanding – people with extensive experience who have distinguished themselves as training professionals over many years. They are enthusiastic about what they do and make learning an engaging experience.

RELIABILITY. We have a proven track record of helping more than 60,000 people in the region pass their exams.

VALUE. Quality usually comes at a premium but we work hard at all levels to ensure competitive pricing. Whether you're a small, medium or large organisation or a private individual, we make sure you get excellent value for your money.

CUSTOMER SERVICE. Our team is totally committed to providing the best customer service at all times. We will walk that extra mile.

GET AHEAD OF THE GAME WITH CYBER SECURITY TRAINING

(03) 2035 9258
customerservice@alc-group.com
alctraining.com.my

Celebrating over 30 years of training excellence!

AUSTRALASIA'S #1 TRAINING PROVIDER

ALC.Training

@alcgroup

alc-training

alc
Cyber Solutions by Thales