CISSP Fast Track

Certified Information Systems Security Professional®

Intensive 5-day course providing preparation for the CISSP exam

Presented by Les Bell

Certified Information Systems Security Professional (CISSP)® is a highly sought after certification for those who are looking to make a career in Information Security. It is established as one of the global standards for proficiency in several different security disciplines. It attests to an individual's ability to meet a stringent set of criteria as defined by the (ISC)²® and to their ability to comprehend a broad spectrum of information system security concepts, principles, and methodologies.

This intensive 5-day course has been designed to provide a comprehensive coverage of the material required in CISSP as well as thorough preparation for the actual exam.

Refer to our website for latest dates.

alc

www.alc-group.com.au

CISSP Fast Track

Certified Information Systems Security Professional®

The CISSP® Certification is one of the most sought-after security certifications available today. It is based on the CBK® (Common Body of Knowledge) which comprises ten subject domains that the (ISC)² compiles and maintains through ongoing peer review by subject matter experts.

CISSPs are expected to have a broad range of skills across security policy development and management, as well as technical understanding of a wide range of security controls across all disciplines within Information Security. The sheer breadth and depth of all that is involved with CISSP can seem daunting. This intensive course has been designed to provide a comprehensive coverage of the material as well as thorough preparation for the exam. The course features short tests at the end of each session to allow candidates to assess their knowledge and preparedness for the CISSP examination.

Objectives

The goal of this 5-day course is to provide information security professionals with a fully-immersed, minimum-distraction CISSP® training and exam preparation experience. The course will broaden and deepen your understanding of all ten CBK® domains to prepare you for the challenging CISSP examination.

What You Will Learn

This program is designed to fully prepare you for the CISSP® exam. Course attendees learn in detail about the ten domains covered under the (ISC)² Common Body of Knowledge (CBK), including an understanding of the related concepts, skill sets and technologies used to plan for, design, and manage each domain.

1. Security Management Practices
2. Access Control Systems
3. Physical Security
4. Telecommunications and Network Security
5. Cryptography
6. Security Architecture
7. Law, Investigation and Ethics
8. Operations Security
9. Business Continuity and Disaster Recovery Planning
10. Application and System Development

Who Should Attend

This course is designed for experienced security professionals who want to expand their knowledge and gain an internationally recognised accreditation. Whilst anyone can attend the course, please note that the CISSP® accreditation is only available to those who meet the (ISC)² entry requirements.

Pre-Requisites

The course assumes you have varied IT experience gained over a number of years. Please note that in order to be eligible to sit for the CISSP exam you must have either five years of experience in Information or Computer Security or else a tertiary degree and four years of experience in Information or Computer Security.

CISSP Hotline and Pre-Exam Support

All participants will have access to our CISSP hotline and online forum for questions, comments and resources. You will also gain exclusive access to our e-learning server which provides additional reading, external references, and practice tests and exercises.

Exclusive Warranty

ALC's course CISSP Fast Track is the result of extensive research and development combined with high-level expertise. ALC backs the quality of this course unreservedly with an exclusive warranty. If for whatever reason the unthinkable should happen and you do not pass the CISSP exam the first time, you are entitled to re-sit the entire course, or any part thereof, for free on any subsequent date.
Please note that this warranty applies to the course itself but does not include the actual (ISC)² exam which has to be booked separately direct with (ISC)².

Disclaimer

CISSP® is a registered Trademark of (ISC)², Inc (International Information Systems Security Certifications Consortium). The material for the ALC course CISSP Fast Track has been developed specifically for ALC and is not endorsed, sponsored or delivered by (ISC)², Inc. The goal of the course is to prepare professionals for the challenging CISSP® examination by covering the syllabus defined in the (ISC)² Common Body of Knowledge. ALC has been providing quality IT training since 1989.

CISSP Exam – Dates and Information

The CISSP exam is set, administered and marked by (ISC)² Inc., the International Information Systems Security Certifications Consortium. If you wish to do the exam you must register for the exam direct with (ISC)² at www.isc2.org. The current exam fee is US$549 if you register at least 16 days before the exam. Otherwise the exam fee is US$599.

The CISSP Certification examination consists of 250 multiple choice questions. Candidates have up to six hours to complete the examination. The CISSP examination will cover the 10 Information System Security domains in the Common Body of Knowledge (CBK).

CISSP Exam Dates

Exams are held by (ISC)² throughout the year.

For exam dates in your city please contact ALC at learn@alc-group.com.au or refer to the ALC web site (follow the CISSP link).

CISSP Fast Track

Certified Information Systems Security Professional®

Course Contents

1 Management Domain

Security management entails the identification of an organisation's information assets and the development, documentation, and implementation of policies, standards, procedures, and guidelines. Management tools such as data classification and risk assessment/analysis are used to identify threats, classify assets, and to rate system vulnerabilities so that effective controls can be implemented. This session covers:

- Basic Concepts - The CIA Triad
- Administrative, Technical and Physical Controls
- Roles & Responsibilities
- Change Control & Change Management
- Information Asset Management
- Security Architecture
- Risk Management Principles, Tools, Methodologies and Standards
- Policies, Standards, Guidelines & Procedures
- Data Classification
- Employment Policies and Practices
- Security Awareness Training
- Security Management Planning
- Information Security Management Systems

2 Security Architecture and Models Domain

The Security Architecture and Models domain contains the concepts, principles, structures, and standards used to design, monitor, and secure operating systems, equipment, networks, applications and those controls used to enforce various levels of availability, integrity, and confidentiality. The session covers:

- Platform Architectures
- Computer & Network Architectures
- Layered Models
- Operating System Principles
- Threats to Shared Environments
- Trusted Systems
  - Reference Monitors & Kernels, TCB
  - Operating Modes
- Security Models
- State Machine Models
  - Biba Matrix
  - Bell-LaPadula Matrix
  - Clark-Wilson
- Other Protection Technologies
- Comparison of Security Models
- Certification & Accreditation
  - TCSEC, ITSEC, Common Criteria

3 Applications and Systems Development Domain

This domain addresses the important security concepts that apply to application software development. It outlines the environment where software is designed and developed and explains the critical role software plays in providing information. This session covers:

- Introduction; Changes in the Environment
- Threat Agents: Hackers, crackers, phreaks and virus authors
- Vulnerabilities
  - Mobile Code: Agents, applets, ActiveX, Java
  - Buffer Overflows, Stack Smashing
- Malicious Code & Logic: Viruses, Trojans, Worms & Logic Bombs
- Attacks: Code alteration, flooding, salami, SQL injection, trapdoors, DoS, etc.
- Databases, Data Warehousing & Knowledge-based Systems
- System Development Life Cycle
  - SDLC Phases
- Iterative Development Models
- Programming Languages and Translators
- Object Oriented Design and Programming
- Mobile Code
- Security Features of Languages
- Safeguards, Mitigation and Controls

4 Operations Security Domain

Operations Security is used to identify the controls over hardware, media, and the operators and administrators with access privileges to any of these resources. Audit and monitoring are the mechanisms, tools, and facilities that permit the identification of security events and subsequent actions to identify the key elements and report the pertinent information to the appropriate individual, group, or process. This session covers:

- Goals of Operations Security
- Resources: Hardware, Software, Network, Media
- Administrative Management
- Principles of Privilege. Least Privilege, Rotation of Duties & Separation of Duties
- Due Care & Due Diligence
- Privacy and Protection
- Sensitive Information and Media
- Operations Controls
  - Operational Controls for Trusted Systems
  - Network & Telecomms Controls
  - Media Controls
  - Personnel Controls
  - Infrastructure Controls
- Configuration Management and Contingency Management
- Auditing
  - Concepts and Considerations
  - Audit Trails & Reporting
- Violation Analysis
- Monitoring
  - Concepts
  - Tools & Techniques
- Intrusion Detection
  - Use of IDS
  - Types of IDS
  - Intrusion Prevention Systems
- Penetration Testing
  - Techniques
- Inappropriate Activities
- Threats & Countermeasures
- Violations, Breaches and Reporting

5 Physical Security Domain

The physical security domain provides protection techniques for the entire facility, from the outside perimeter to the inside office space, including all of the information system resources.

- Terminology & Definitions
- Changes in the Environment
- Characterization of Systems
- Physical Threats
- Site Selection, Facility Design and Configuration
- Water & Plumbing
- Power and HVAC
- Boundary Protection & Lighting, Fences and Gates
- CCTV
- Building Materials
- Locks, Keys and Key Control Systems
- Fire Prevention, Protection & Detection
- Fire Suppression
- Computing Facility Requirements
- Securing Storage Areas
- Portable Device Security
- Media Protection & Disposal
- Personnel Access Controls
  - Cards & Badges
  - Biometrics
- Physical Security in Distributed Processing
- Office Area Physical Security Controls

6 Cryptography Domain

The cryptography domain addresses the principles, means, and methods of disguising information to ensure its integrity, confidentiality and authenticity:

- Basic Concepts and Definitions
- Goals of Cryptography
- Stream vs Block Ciphers
- Hash Functions
- Message Digests & Message Authentication Codes
- Symmetric Ciphers
- Public-Key Ciphers
- Digital Signatures
- Hybrid Cryptosystems
- Applications of Cryptography
  - Digital Certificates and PKI
  - Email Security
  - SSL
  - SSH
- Methods of Attack
- Import/Export Regulations

7 Access Control Systems and Methodology Domain

Access controls are mechanisms that work together to create a security architecture to protect the assets of the information system.

- Information Protection Requirements, Basic Concepts and Threats
- Security Technologies and Tools, Types of Controls
- Identification and Authentication Techniques
- Passwords, One-Time Passwords, Tokens, SmartCards, Biometrics
- Access Control Techniques
- Centralised vs Remote Authentication Access Controls, RADIUS, TACACS,etc.
- 802.1x Port-based Authentication
- Decentralised Access Control, Single Signon, Kerberos, SESAME
- Controls
  - Discretionary vs Mandatory Access Controls
  - Rule-Based Access Control, Role-Based Access Control, Lattice-Based
- Access Control, Access Control Lists, Capabilities
  - Data Ownership and Custodianship
  - Types of Attacks
  - Intrusion Detection and Auditing
  - Management Activities

8 Business Continuity Planning / Disaster Recovery Planning Domain

The Business Continuity Planning/ Disaster Recovery Planning (BCP/DRP) domain addresses the preservation and recovery of business operations in the event of outages.

- Key Terms & References
- Definitionsof BCP & DRP
- Other Incident Response Plans
- BCP Responsibilities
- BCP Process
  - Overview
  - Critical Function Identification
  - Supporting Resources
  - Business Impact Analysis
  - Plan Development
  - Plan Content
  - Off-site Storage
  - Alternative Sites
  - Backup Processing
  - Other Elements
  - Recovery Organisation & Team Structure
  - Other Items
- Testing and Plan Maintenance
  - Considerations for Testing
  - Types of Testing
- Stages in an Incident
- Disaster Recovery Time Line
- Software Escrow

9 Telecommunications and Network Security Domain

The telecommunications, network, and Internet security domain discusses the: Network Structures, Transmission methods, Transport formats, Security measures used to provide availability, integrity, and confidentiality, and finally Authentication for transmissions over private and public communications networks.

- Key Terminology
- LANs & WANs
- ISO/OSI Layers & Characteristics
- TCP/IP Layers & Characteristics
- Physical Media Characteristics and Devices
- Physical Layer Attacks and Controls
- Network Layer Principles
  - Addresses and Routing
  - Attacks and Controls
- Transport Layer Principles
  - Attacks and Controls: Port Scanning, IDS
- Application Layer Protocols
- Types of Protection
  - Firewalls & IPS
  - Virtual Private Networks
- Honeypots and Honeynets
- Network Security Assessment
- Penetration Testing

10 Law, Investigation and Ethics Domain

The Law, Investigations, and Ethics domain addresses:

- The Legal and Ethical Environment
- Types & Categories of Computer Crime Laws
- Corporate Governance and Audit Requirements
- Privacy Requirements
- Intellectual Property: Trade Secrets, Patents, Copyright
- Records Retention
- Industrial Relations
- Legal Liability
- Privacy & Other Personal Rights
- Computer Crime
- Legal Aspects of Cryptography
- Computer Crime Investigation
  - Incident Response
  - Investigation Process
  - Computer Forensics
  - Rules of Evidence & Legal Proceedings
- Computer Ethics
  - The Ten Commandments
  - Ethics & The Internet
  - (ISC)² Code of Ethics

Les Bell - CISSP

Course Instructor

Les Bell has a long, varied and distinguished background in the computer industry as a consultant, educator, writer, software developer and international seminar presenter. His interests cover a very wide range including operating systems, security, programming languages, software development and the Internet.

As a consultant Les has worked on a variety of projects on intranets, web servers and email gateways. He has been involved in security since the mid-1980's in areas such as firewall design, penetration testing, forensic investigation and expert witness work. His client list includes major banks and insurance companies, telecommunications agencies, government departments and computer multinationals.

As an educator Les has developed and personally presented, both on a public and in-house basis, an impressive range of courses and seminars on information security, Linux, TCP/IP, e-commerce and operating systems. His seminars have been presented to outstanding reviews throughout Australia and New Zealand as well as several countries around the world including Singapore, Malaysia, Indonesia, Hong Kong, Beijing, the UK, and Ireland.

As a technical journalist Les has written many series of articles covering a wide range of topics including operating systems, programming languages and software development. He was Founding Editor of Your Computer magazine, Founding Editor of the international journal PC Support Advisor and writes a monthly Linux column to PC User magazine. He also contributes articles on Linux and security to other leading IT publications.

In all his work Les brings to bear a hard-hitting and practical perspective. Rather than getting bogged down in theory for it's own sake, Les's objective and skill is to take a complex subject and explain it in such a way as to make it both understandable and useful. Les is renowned for his encyclopedic knowledge and has no spare time. He is a Certified Information Systems Security Professional (CISSP) and a Red Hat Certified Engineer. Les is based in Sydney, Australia.

HOW TO REGISTER

1.	Register Online **www.alc-group.com.au**
2.	Send your details by email **learn@alc-group.com.au**
3.	Fax the Enrolment Form below to: **Fax: +61 2 9299 5455**
4.	Any queries please call Customer Service **Tel: 1300 767 592** or +61 2 9299 5400
5.	Post the completed Enrolment Form to: **ALC Education & Consulting Pty Ltd** GPO Box 598, Sydney NSW 2001

COURSE DETAILS

FEES: (per delegate) **A$**

CISSP® Fast Track 5-day Prep Course 3150 +GST

NOTE: Fees do not include the CISSP examination which must be separately booked direct with (ISC)².

VENUE: The course will be held at a high quality centrally-located venue. Full details will be on your confirmation letter and can also be found under the Schedule tab on our web site.

COURSE INFORMATION: The course is held from 9.00am to 5.00pm and registration is from 8.30am. Fees include lunch, refreshments and all course materials.

TERMS and GUARANTEE: To ensure your admission to the course, fees are payable in advance. To guarantee your satisfaction we offer a money-back or full credit policy. Details will be on your confirmation letter and our website. Cancellations with full refund will be accepted up to 10 working days before the course. After that time no refunds can be given, but substitutions may be sent at any time.

ENROLMENT FORM
- CISSP® Fast Track 5-day Prep Course

ALC Education & Consulting Pty Ltd is an independent Australian company dedicated to the provision of top quality training and professional services for business and government. ALC has no affiliations with any vendor of hardware or software and is therefore able to provide totally unbiased education, advice and support.

	NAME	POSITION	CITY
1	Mr/Mrs/Miss/Ms		
	Email	Mobile	
2	Mr/Mrs/Miss/Ms		
	Email	Mobile	

TRACK CODE: A B C D R

Organisation: _____

Address: _____

Postcode: _____ Phone: ( ) _____ Fax: ( ) _____

1. ☐ Cheque payable to *ALC Education & Consulting Pty Ltd* 2. ☐ Purchase Order No.: _____

3. Charge to: ☐ Master Card ☐ Visa ☐ Amex Cardholder Name: _____

Card No.: _____

Exp Date: ____/____ Signature: X _____

Person Making Booking:	Mr/Mrs/Miss/Ms	**Send Invoice To:**	Mr/Mrs/Miss/Ms
	Position Phone		Position Phone
	Email		Email

A.B.N. 53 100 351 675