CISSP® CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL

DURATION: 5 DAYS

CYBER SECURITY

This 5-day concentrated course provides information security professionals with a fully-immersed, minimum-distraction CISSP training and certification experience. The course covers the 8 domains of the CISSP Common Body of Knowledge as reorganised and updated in 2021. The course will broaden and deepen your understanding of the domains and give you full preparation for the ISC2 CISSP examination.

CISSP is long regarded as the gold standard of security qualifications. It draws from a comprehensive, up-to-date, global common body of knowledge that ensures security leaders have a deep knowledge and understanding of new threats, technologies, regulations, standards, and practices.

LEARNING OUTCOMES

This program is designed to fully prepare you for the CISSP exam. Course attendees learn in detail about the ten domains covered under the ISC2 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.

PREREQUISITES

The course assumes you have at least a reasonable level of varied IT experience. Please note that to attain the CISSP certification you must have a minimum of 5 years of direct, full-time security professional work experience in 2 or more of the domains of the CISSP CBK. One year of work experience may be waived by ISC2 if you hold a four-year or higher college or university degree or approved credential. Candidates who do not meet these criteria may be given Associate status until conditions are met.

OUR TRAINERS MAKE THE DIFFERENCE

When you attend a training course there are actually two costs – the course fee, and the value of your time. You can see the fee. But whether you get value for your time and money depends totally on the quality of the course. Lots of things go into making a great course, but the single most important is always the trainer: their knowledge of the subject, their real world experience that they can draw upon in the class, their ability to answer questions, their communication skills. This is what makes the difference.ALC works only with the best.

WHO SHOULD ATTEND

The CISSP is designed for experienced security professionals who want to expand their knowledge and gain an int ernationally recognised accreditation. It is ideal for those working in positions such as: Security Consultant, Security Manager, IT Director/Manager, Security Auditor, Security Architect, Security Analyst, Security Systems Engineer, Chief InfoSec Officer, Director of Security, Network Architect.

EXAMINATION PROCEDURE

The CISSP exams are administered by Pearson Vue on behalf of ISC2. You must register for the exam online.

For information on dates or how to enrol for an exam please contact ALC.

COURSE CONTENTS

1. INTRODUCTION

- Course Overview
- Review and Revision Techniques
- The Exam, On the Day of the Exam, Exam Technique, After the Exam

2. SECURITY & RISK MANAGEMENT

- Understand, adhere to, and promote professional ethics
- Understand and apply security concepts
- Evaluate and apply security governance principles
- Determine compliance and other requirements
- Understand legal and regulatory issues that pertain to information security in a holistic context
- Understand requirements for investigation types
- Develop, document, and implement security policy, standards, procedures, and guidelines
- Identify, analyse, and prioritize Business Continuity (BC) requirements
- Contribute to and enforce personnel security policies and procedures
- Understand and apply risk management concepts
- Understand and apply threat modelling concepts and methodologies
- Apply Supply Chain Risk Management (SCRM) concepts
- Establish and maintain a security awareness, education, and training program

3. ASSET SECURITY

- Identify and classify information and assets
- Establish information and asset handling requirements
- Provision resources securely
- Manage data lifecycle
- Ensure appropriate asset retention (e.g., End-of-Life (EOL), End-of-Support (EOS))
- Determine data security controls and compliance requirements

4. SECURITY ARCHITECT & ENGINEERING

- Research, implement and manage engineering processes using secure design principles
- Understand the fundamental concepts of security models
- Select controls based upon systems security requirements
- Understand security capabilities of Information Systems (IS)
- Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements
- Select and determine cryptographic solutions
- Understand methods of cryptanalytic attacks
- Apply security principles to site and facility design
- Design site and facility security controls

5. COMMUNICATIONS AND NETWORK SECURITY

- Assess and implement secure design principles in network architectures
- Secure network components
- Implement secure communication channels according to design
- Secure network components
- Implement secure communication channels according to design

6. IDENTITY & ACCESS MANAGEMENT

- Control physical and logical access to assets
- Manage identification and authentication of people, devices, and services
- Federated identity with a third-party service
- Implement and manage authorization mechanisms
- Manage the identity and access provisioning lifecycle
- Implement authentication systems
- Manage the identity and access provisioning lifecycle
- Implement authentication systems

7. SECURITY ASSESSMENT & TESTING

- Design and validate assessment, test, and audit strategies
- Conduct security control testing
- Collect security process data (e.g., technical and administrative)
- Analyse test output and generate report
- Conduct or facilitate security audits

8. SECURITY OPERATIONS

- Understand and comply with investigations
- Conduct logging and monitoring activities
- Perform Configuration Management (CM) (e.g., provisioning, baselining, automation)
- Apply foundational security operations concepts
- Apply resource protection
- Conduct incident management
- Operate and maintain detective and preventative measures
- Implement and support patch and vulnerability management
- Understand and participate in change management processes
- Implement recovery strategies
- Implement Disaster Recovery (DR) processes
- Test Disaster Recovery Plans (DRP)
- Participate in Business Continuity (BC) planning and exercises
- Implement and manage physical security
- Address personnel safety and security concerns

9. SOFTWARE DEVELOPMENT SECURITY

- Understand and integrate security in the Software Development Life Cycle (SDLC)
- Identify and apply security controls in software development ecosystems
- Assess the effectiveness of software security
- Assess security impact of acquired software
- Define and apply secure coding guidelines and standards

alc

GET AHEAD OF THE GAME
GET CERTIFIED

1300 767 592
customerservice@alc-group.com
alctraining.com.au

f ALC.Training   @alcgroup   in alc-training