Iverson Associates Sdn Bhd (303330-M)
Suite T113 – T114, 3rd Floor, Centrepoint, Lebuh Bandar Utama
Bandar Utama, 47800 Petaling Jaya, Selangor Darul Ehsan
Tel: 03-7726 2678 Fax: 03-7727 9737 Website: www.iverson.com.my

Module Title : CISSP Certification Course
Duration : 5 days

OVERVIEW

Gain core knowledge and experience to successfully implement and manage security programs in this official (ISC)2 CISSP course.

This course is the most comprehensive review of information security concepts and industry best practices, and covers the eight domains of the official CISSP CBK (Common Body of Knowledge). You will gain knowledge in information security that will increase your ability to successfully implement and manage security programs in any organization or government entity. You will learn how to determine who or what may have altered data or system information, potentially affecting the integrity of those asset and match an entity, such as a person or a computer system, with the actions that entity takes against valuable assets, allowing organizations to have a better understanding of the state of their security posture. Policies, concepts, principles, structures, and standards used to establish criteria for the protection of information assets are also covered in this course.

This five-day program is comprised of a total of eight domains and includes:

- Official (ISC)2 Guide to the CISSP Common Body of Knowledge® (CBK)
- Official (ISC)2 CISSP Training Handbook
- Official (ISC)2 CISSP Flash Cards
- CISSP Certification Exam Voucher

WHAT YOU WILL LEARN

In-depth coverage of the eight domains required to pass the CISSP exam:

1. Security and Risk Management
2. Asset Security
3. Security Engineering
4. Communications and Network Security
5. Identity and Access Management
6. Security Assessment and Testing
7. Security Operations
8. Software Development Security

PREREQUISITES

Professionals with at least five years of experience and who demonstrate a globally recognized level of competence, as defined in the CISSP Common Body of Knowledge (CBK) in two or more of the eight security domains.

COURSE OUTLINE

Domain 1 Security and Risk Management

1.1 Understand and apply concepts of confidentiality, integrity, and availability
1.2 Evaluate and apply security governance principles
1.3 Determine compliance requirements
1.4 Understand legal and regulatory issues that pertain to information security in a global context
1.5 Understand, adhere to, and promote professional ethics
1.6 Develop, document, and implement security policy, standards, procedures, and guidelines
1.7 Identify, analyze, and prioritize Business Continuity (BC) requirements
1.8 Contribute to and enforce personnel security policies and procedures
1.9 Understand and apply risk management concepts
1.10 Understand and apply threat modeling concepts and methodologies
1.11 Apply risk-based management concepts to the supply chain
1.12 Establish and maintain a security awareness, education, and training program

Domain 2 Asset Security

2.1 Identify and classify information and assets
2.2 Determine and maintain information and asset ownership
2.3 Protect privacy
2.4 Ensure appropriate asset retention
2.5 Determine data security controls
2.6 Establish information and asset handling requirements

Domain 3 Security Architecture and Engineering

3.1 Implement and manage engineering processes using secure design principles
3.2 Understand the fundamental concepts of security models
3.3 Select controls based upon systems security requirements
3.4 Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)
3.5 Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

Domain 4 Communication and Network Security

4.1 Implement secure design principles in network architectures

4.2 Secure network components

4.3 Implement secure communication channels according to design

Domain 5 Identity and Access Management (IAM)

5.1 Control physical and logical access to assets

5.2 Manage identification and authentication of people, devices, and services

5.3 Integrate identity as a third-party service

5.4 Implement and manage authorization mechanisms

5.5 Manage the identity and access provisioning lifecycle

Domain 6 Security Assessment and Testing

6.1 Design and validate assessment, test, and audit strategies

6.2 Conduct security control testing

6.3 Collect security process data (e.g., technical and administrative)

6.4 Analyze test output and generate report

6.5 Conduct or facilitate security audits

Domain 7 Security Operations

7.1 Understand and support investigations

7.2 Understand requirements for investigation types

7.3 Conduct logging and monitoring activities

7.4 Securely provisioning resources

7.5 Understand and apply foundational security operations concepts

7.6 Apply resource protection techniques

7.7 Conduct incident management

7.8 Operate and maintain detective and preventative measures

7.9 Implement and support patch and vulnerability management

7.10 Understand and participate in change management processes

7.11 Implement recovery strategies

7.12 Implement Disaster Recovery (DR) processes

7.13 Test Disaster Recovery Plans (DRP)

7.14 Participate in Business Continuity (BC) planning and exercises

7.15 Implement and manage physical security

7.16 Address personnel safety and security concerns

Domain 8 Software Development Security

8.1 Understand and integrate security in the Software Development Life Cycle (SDLC)

8.2 Identify and apply security controls in development environments

8.3 Assess the effectiveness of software security

8.4 Assess security impact of acquired software

8.5 Define and apply secure coding guidelines and standards