Building Blocks

Course Outline

The CISSP Exam Preparation Boot Camp reflects the most recent updates and changes to the CISSP exam and the Official (ISC)² Guide to the CISSP CBK (effective April 15 2015).

This intensive 5-day course provides students with an understanding of the 8 domains of security represented by the (ISC)² CISSP Common Body of Knowledge regarding Information, Infrastructure, and Physical security.

These 8 domains represent a vendor neutral overview of the Information Technology spectrum related to security management practices. Through a series of lectures, discussions and practice quizzes, the student will gain knowledge of these concepts and gain an understanding of the areas of study required prior to taking the CISSP exam.

Course Type

This is an exam preparation course taught in class with an instructor via lecture, discussion, and practice quizzes.

Audience

The CISSP certification is relevant for middle to senior level Managers, and network engineers, security planners, administrators, and practitioners in the security field, seeking a higher understanding regarding the theory and models of information security and the relationship to effective, practical security implementations.

Prerequisite

TThe CISSP candidate must have at least 5 years of paid full-time experience in 2 or more of the domains.

Upon completion of this course, participants will be able to:

- Understand information security and risk management concepts and practices and their relationship to the needs of the business
- Differentiate between the tools available for the protection of information
- Explain the mechanisms required to provide assurance of information security controls
- Understand the threats and vulnerabilities to information technology

Building Blocks Technologies, Inc. • 170 Laurier Avenue West, Suite 700 • Ottawa, Ontario K1P 5V5 • T: 613.230.6255 • F: 613.599.0859 • www.bblockstech.com
© 2016 Building Blocks Technologies, Inc. All Rights Reserved.

Building Blocks

Course Topics

CISSP® Domains

The CISSP domains are drawn from various information security topics within the (ISC)^2 CBK. The CISSP CBK consists of the following 8 domains:

Security and Risk Management
(Security, Risk, Compliance, Law, Regulations, Business Continuity)

- Understand and apply concepts of confidentiality, integrity and availability
- Apply security governance principles
- Compliance
- Understand legal and regulatory issues that pertain to information security in a global context
- Professional ethics
- Security policies, standards, procedures, and guidelines

Asset Security
(Protecting Security of Assets)

- Classify information and supporting assets (e.g., sensitivity, criticality)
- Determine and maintain ownership (e.g., data owners, system owners, business/mission owners)
- Protect privacy
- Ensure appropriate retention (e.g., media, hardware, personnel)
- Determine data security controls (e.g., data at rest, data in transit)
- Establish handling requirements (markings, labels, storage, destruction of sensitive information)

Security Engineering
(Engineering and Management of Security)

- Implement and manage engineering processes using secure design principles
- Understand the fundamental concepts of security models (e.g., Confidentiality, Integrity, and Multi-level Models)
- Select controls and countermeasures based upon systems security evaluation models
- Understand security capabilities of information systems (e.g., memory protection, virtualization, trusted platform module, interfaces, fault tolerance)
- Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements
- Assess and mitigate vulnerabilities in web-based systems (e.g., XML, OWASP)
- Assess and mitigate vulnerabilities in mobile systems
- Assess and mitigate vulnerabilities in embedded devices and cyber-physical systems (e.g., network enabled devices, Internet of things (IoT)
- Apply cryptography
- Apply secure principles to site and facility design
- Design and implement physical security

Communication and Network Security
(Designing and Protecting Network Security)

- Apply secure design principles to network architecture (e.g., IP & non-IP protocols, segmentation)
- Secure network components
- Design and establish secure communication channels
- Prevent or mitigate network attacks

Identity and Access Management
(Controlling Access and Managing Identity)

- Control physical and logical access to assets
- Manage identification and authentication of people and devices
- Integrate identity as a service (e.g., cloud identity) Integrate third-party identity services (e.g., on-premise)Implement and manage authorization mechanisms
- Prevent or mitigate access control attacks
- Manage the identity and access provisioning lifecycle (e.g., provisioning, review)

Security Assessment and Testing
(Designing, Performing, and Analyzing Security Testing)

- Design and validate assessment and test strategies
- Conduct security control testing
- Collect security process data (e.g., management and operational controls)
- Analyze and report test outputs (e.g., automated, manual)
- Conduct or facilitate internal and third party audits

Security Operations
(e.g., Foundational Concepts, Investigations, Incident Management, Disaster Recovery)

- Understand and support investigations
- Understand requirements for investigation types
- Conduct logging and monitoring activities

Software Development Security
(Understanding, Applying, and Enforcing Software Security)

- Understand and apply security in the software development lifecycle
- Enforce security controls in development environments
- Assess the effectiveness of software security
- Assess security impact of acquired software

© 2016 Building Blocks Technologies, Inc. All Rights Reserved.