CISSP – Certified Information Systems Security Professional

Days: 5

Prerequisites: Students should have certifications in A+, Network+, or Security+, or possess equivalent professional experience. Students may have one or more of the following certifications or equivalent experience: MCSE, SCNP, CCNP, RHCE, LCE, CNE, SSCP, SANS, or GIAC.

Audience: Students pursuing CISSP training want to establish themselves as credible computer security professionals through a study of all CISSP Common Body of Knowledge domains. Validating this knowledge is the goal of certification; therefore, students attending this training should also meet the requirements needed to sit for the CISSP certification exam. Candidates must have a minimum of five years cumulative paid work experience in two or more of the eight domains of the CISSP CBK. Earning a four year college degree or regional equivalent or an additional credential from the ISC2 approved list will satisfy one year of the required experience. Education credit will only satisfy one year of experience. A candidate that doesn't have the required experience to become a CISSP may become an Associate of ISC2 by successfully passing the CISSP examination. The Associate of ISC2 will then have six years to earn the five years required experience.

Description: The Certified Information Systems Security Professional (CISSP) is the most globally recognized certification in the information security market. CISSP validates an information security professional's deep technical and managerial knowledge and experience to effectively design, engineer, and manage the overall security posture of an organization. The broad spectrum of topics included in the CISSP Common Body of Knowledge (CBK®) ensure its relevancy across all disciplines in the field of information security.

Successful candidates are competent in the following eight domains:

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations
- Software Development Security

OUTLINE:

LESSON 1: SECURITY GOVERNANCE THROUGH PRINCIPLES AND POLICIES

LESSON 2: PERSONNEL SECURITY AND RISK MANAGEMENT CONCEPTS

LESSON 3: BUSINESS CONTINUITY PLANNING

LESSON 4: LAWS, REGULATIONS, AND COMPLIANCE

LESSON 5: PROTECTING SECURITY OF ASSETS

LESSON 6: CRYPTOGRAPHY AND SYMMETRIC KEY ALGORITHMS

LESSON 7: PKI AND CRYPTOGRAPHIC APPLICATIONS

LESSON 8: PRINCIPLES OF SECURITY MODELS, DESIGN, AND CAPABILITIES

CISSP – Certified Information Systems Security Professional