**Global Knowledge Course Name:** CISSP Prep Course (Code 9840)

**Course Overview:**
Prepare for the most important security certification with superior prep materials and test-taking tips.
The CISSP has clearly emerged as the key certification for security professionals. In fact, an informal survey of information security jobs on a major employment web site revealed that over 70% of the positions required CISSP certification! Corporations are demanding experienced information security professionals, with the certifications to prove it, to protect their information and assets.

Our course offers the most exhaustive survey of the CISSP information, test-taking techniques, and preparation materials available in the industry to ensure that you fully understand the objectives of the exam as defined in the (ISC)² Common Body of Knowledge (CBK).

In order to give you the best chance of success on the CISSP test, we have created our own study guides, CISSP book reviews, summary charts, and practice exams that include all the latest, most relevant information covered in the new (ISC)² Official CISSP Examination Guide.

Attend this course and take home your free copy of the CISSP: Certified Information Systems Security Professional Study Guide (3rd Edition) by Sybex and a CISSP certification practice exam from Self Test Software.

This course includes 1-year access to our 50-book Online Security Reference Library with titles specially selected to reinforce course concepts.

**What You'll Learn:**

- How to identify and correctly answer the five types of CISSP hard questions
- Techniques for committing key facts and figures to memory for test preparation
- Why you should NOT take the exam the day after completing the CISSP Prep course
- Critical test-taking tips and study techniques for the CISSP exam
- Proven techniques for scoring well on the CISSP exam
- Key aspects of security policy development and security management practices

**Who Needs to Attend:**

- CISSP certification is beneficial to IT consultants, managers, security policy writers, privacy officers, information security officers, network administrators, security device administrators, and security engineers.

- CISSP designation requires passing the CISSP exam (administered separately) and having four years' experience in one or more of the 10 domains of the CBK.

**Course Content:**

Access Control Systems and Methodologies

- Access control concepts, methodologies, and implementation
- Access controls: detective, corrective, and preventative
- Access control techniques in centralized and decentralized environments
- Access control risks, vulnerabilities, and exposures

Security Architecture and Models

- Secure operating system principles, concepts, mechanisms, controls, and standards
- Secure architecture design, modeling, and protection
- Security models: confidentiality, integrity, and information flow
- Government and commercial security requirements
- Common criteria, ITSEC, TCSEC, IETF, IPSEC
- Technical platforms
- System security preventative, detective, and corrective measures

Disaster Recovery and Business Continuity Planning

- Business continuity planning, business impact analysis, recovery strategies, recovery plan development, and implementation
- Disaster recovery planning, implementation, and restoration
- Compare and contrast disaster recovery and business continuity

Security Management Practices

- Organizational security roles
- Identification of information assets
- Security management planning
- Security policy development; use of guidelines, standards, and procedures
- Security awareness training
- Data classification and marking
- Employment agreements and practices
- Risk management tools and techniques

Law, Investigation, and Ethics

- Computer crime detection methods
- Applicable computer crime, security, and privacy laws
- Evidence gathering and preservation methods
- Computer crime investigation methods and techniques
- Civil, criminal, and investigative law

- Intellectual property law
- (ISC)² and IAB ethics application

Physical Security

- Prevention, detection, and correction of physical hazards
- Secure site design, configuration, and selection elements
- Access control and protection methods for facility, information, equipment, and personnel

Operations Security

- Resource protection mechanisms and techniques
- Operation security principles, techniques, and mechanisms; principles of good practice and limitation of abuses
- Operations security preventative, detective, and corrective measures
- Information attacks
- Access Control Subversion

Cryptography

- Cryptographic concepts, methods, and practices
- Construction of algorithms
- Attacks on cryptosystems
- Ancient cryptography and modern methods
- Public and private key algorithms and uses
- Key distribution and key management
- Digital signature construction and use
- Methods of attack, strength of function

Telecommunications and Network Security

- Overview of communications and network security
- Voice communications, data communications, local area, wide area, and remote access
- Internet/intranet/extranet, firewalls, routers, and network protocols
- Telecommunication and network security preventative, detective, and corrective measures

Application and System Development

- System development process and security controls
- System development life cycle, change controls, application controls, and system and application integrity
- Database structure, concepts, design techniques, and security implications
- Object-oriented programming
- Data warehousing and data mining

Review and Q&A Session

- Review concepts introduced in previous sessions
- Answer specific questions or concerns regarding CISSP preparation material

Testing-Taking Tips and Study Techniques

- Tips for additional preparation for the CISSP exam
- Additional resources
- Techniques for scoring well on the exam