Information Systems Security Professional Training Course

19 - 23 Oct 2026

Cairo

3700 € (Per Person)

Ref: #CYB9530_272479

Course Introduction / Overview:

This comprehensive course is designed to provide a complete and in-depth understanding of the eight domains of the $(ISC)^2$ Common Body of Knowledge (CBK) for the CISSP certification. It is an essential program for professionals seeking to prove their knowledge across a wide array of security practices and principles. The curriculum delves deep into information security governance, risk management frameworks, and the core tenets of security architecture and engineering. As emphasized by renowned author Shon Harris in her seminal work, "CISSP All-in-One Exam Guide," a successful security professional must not only understand technical controls but also master the managerial and operational aspects of securing an enterprise. This course, offered by BIG BEN Training Center, bridges that gap by blending theoretical knowledge with practical application. Participants will explore everything from cryptography concepts and network security protocols to incident response and disaster recovery planning. The program is structured to build a strategic mindset, enabling attendees to design, implement, and manage a best-in-class cybersecurity program, making them invaluable assets to any organization in today's complex threat landscape.

Target Audience / This training course is suitable for:

- Security Consultants and Managers.
- IT Directors and Managers.
- Security Auditors and Architects.
- Security Systems Engineers.
- Chief Information Security Officers (CISOs).
- Network Architects.
- Security Analysts.
- Professionals seeking CISSP certification.

Target Sectors and Industries:

- Financial Services and Banking.
- Information Technology and Telecommunications.
- Healthcare and Pharmaceuticals.
- Governmental and Public Sector Agencies.
- Consulting and Professional Services.
- Energy and Utilities.
- Retail and E-commerce.
- Defense and Aerospace.

Target Organizations Departments:

- Information Technology (IT) Department.
- Cybersecurity and Information Security Teams.
- Internal Audit and Compliance Departments.
- Risk Management Department.
- Legal and Regulatory Affairs.
- Network Operations Center (NOC).
- Security Operations Center (SOC).
- Software Development and Engineering.

Course Offerings:

By the end of this course, the participants will have able to:

- Master the eight domains of the CISSP Common Body of Knowledge (CBK).
- Develop and implement robust security and risk management frameworks.
- Design secure architectures for complex enterprise environments.
- Understand advanced cryptography and its applications in data protection.
- Secure communication channels and network infrastructures effectively.
- Implement comprehensive identity and access management (IAM) solutions.
- Conduct thorough security assessments and testing to identify vulnerabilities.
- Manage security operations and lead incident response efforts.
- Integrate security into the software development lifecycle (SDLC).
- Align information security strategies with organizational goals and objectives.
- Prepare effectively for the CISSP certification examination.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, engaging, and directly applicable to real-world challenges. We move beyond traditional lecture-based formats to create an immersive learning environment that fosters deep understanding and practical skill development. The course is built upon a foundation of expert-led instruction, where complex topics like security governance and risk management frameworks are broken down into understandable concepts. This is heavily supplemented with case studies drawn from actual security incidents, allowing participants to analyze and deconstruct complex scenarios. A significant portion of the training is dedicated to collaborative group exercises and workshops, where attendees work in teams to solve security problems, design security architectures, and develop incident response plans. These interactive sessions encourage peer-to-peer learning and the exchange of diverse perspectives. Regular Q&A sessions, practice exam questions, and hands-on simulations ensure that participants can immediately apply what they have learned and receive constructive feedback, solidifying their knowledge and building confidence for both the CISSP exam and their professional roles.

Course Agenda (Course Units):

Unit One: Security and Risk Management

- Foundations of information security governance and principles.
- Understanding legal, regulatory, and compliance requirements.
- Developing and implementing security policies, standards, and procedures.
- Business continuity and disaster recovery planning fundamentals.
- Contributions to personnel security policies.
- Risk management concepts and the risk assessment lifecycle.
- Threat modeling methodologies and applications.

Unit Two: Asset Security and Security Architecture

- Classifying information and supporting assets.
- Determining and maintaining data ownership and stewardship.
- Data security controls and privacy protection measures.
- Implementing secure design principles in system architecture.
- Understanding fundamental concepts of security models.
- Assessing and mitigating vulnerabilities in systems and architectures.
- Cryptography concepts and secure communication protocols.
- Applying security principles to site and facility design.

Unit three: Communication and Network Security

- Implementing secure network architecture and design principles.
- Securing network components and communication channels.
- Understanding TCP/IP, OSI models, and secure network protocols.
- Managing wireless network security and mobile device security.
- Implementing secure remote access and VPN solutions.
- Preventing and mitigating network-based attacks.
- Securing voice, multimedia, and virtualized networks.

Unit Four: Identity and Access Management and Security Testing

- Controlling physical and logical access to assets.
- Managing identification, authentication, and authorization mechanisms.
- Implementing centralized and decentralized access control models.
- Understanding identity as a service (IDaaS) and federated identity.
- Designing and performing security assessment and testing strategies.
- Conducting vulnerability assessments and penetration testing.
- Analyzing and reporting on security test outputs.
- Facilitating internal and third-party security audits.

Unit Five: Security Operations and Software Development Security

- Managing security operations and logging and monitoring activities.
- Implementing effective incident response and management procedures.
- Operating and maintaining preventative and detective measures.
- Managing patch and vulnerability management programs.
- Integrating security into the software development lifecycle (SDLC).
- Applying secure coding standards and guidelines.
- Evaluating the security of software and applications.
- Final review of all domains and comprehensive exam preparation strategies.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

How does the principle of 'defense in depth' evolve in the context of cloud computing and IoT, and what new challenges does this present for a CISSP professional?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by focusing on the strategic mindset required of a true security leader, rather than just rote memorization for an exam. While many programs concentrate solely on test-passing techniques, our curriculum is engineered to cultivate a deep, conceptual understanding of the interconnectedness between the eight CISSP domains. We emphasize a managerial perspective, teaching participants how to think like a CISO by aligning security initiatives with business objectives, managing risk appetite, and communicating complex security concepts to non-technical stakeholders. The methodology integrates real-world case studies that go beyond textbook examples, challenging participants to apply principles of security architecture and incident response to nuanced, contemporary scenarios. Our instructors facilitate Socratic discussions and collaborative problem-solving sessions that force participants to defend their decisions and consider alternative viewpoints. This approach ensures that graduates not only possess the knowledge to pass the CISSP exam but also have the critical thinking skills and practical wisdom to design, lead, and manage a robust and resilient information security program in any organization.