BLACKBIRD FOR TRAINING

Certified Information Systems Security Professional (CISSP) Preparation

2027 □□□□□ 24 – 20
Cairo (Egypt)



Certified Information Systems Security Professional (CISSP) Preparation

Ref: 20228765_224520 Duration: Cairo (Egypt) Fees: 4900 GBP

Why This Course

In an era where digital transformation drives every industry, cybersecurity has become a cornerstone of organizational trust and continuity.

The Certified Information Systems Security Professional CISSP certification, governed by ISC ², stands as the most globally respected credential for professionals who design, implement, and manage enterprise-level security programs.

This intensive program prepares participants to master the eight domains of the CISSP Common Body of Knowledge CBK, combining deep technical understanding with strategic management insight.

Through real-world scenarios, guided labs, and structured exam preparation, participants will gain the skills and confidence to safeguard complex systems, mitigate risks, and lead secure digital transformations.

What You'll Learn and Practice

By joining this program, you will:

- Master the CISSP CBK's eight core domains — from security and risk management to software development security.
- Understand global information security standards, policies, and frameworks.
- Learn to design and manage comprehensive security architectures and governance structures.
- Apply best practices in access control, cryptography, and network defense.
- Develop expertise in incident response, business continuity, and disaster recovery planning.
- Gain exam-focused insights, strategies, and practical case analysis to ensure success in the CISSP exam.
- Build the mindset and capability to lead enterprise-level security initiatives.



The Program Flow

Day 1: Security and Risk Management

- Understanding confidentiality, integrity, and availability CIA triad.
- Legal, regulatory, and compliance frameworks.
- Security governance principles and organizational roles.
- Risk management methodologies and threat modeling.
- Ethics, professional standards, and information assurance policies.
- Case study: Building a security governance model for a multinational firm.

Day 2: Asset Security and Security Architecture

- Data classification, ownership, and lifecycle protection.
- Asset management and secure data handling.
- Security models, frameworks, and system architecture design.
- Defense-in-depth strategies and system hardening.
- Workshop: Designing a secure enterprise network architecture.

Day 3: Communication, Network, and Identity Management

- Secure network components and protocols.
- Network attacks, intrusion detection, and prevention systems.
- Identity and access management IAM frameworks.
- Authentication, authorization, and identity federation.
- Hands-on lab: Configuring access control and monitoring tools.

Day 4: Security Operations and Software Development Security

- Operational security controls and administrative procedures.
- Incident response planning, forensics, and threat intelligence.
- Business continuity and disaster recovery management.
- Secure coding practices and software development lifecycle SDLC.
- Case simulation: Responding to a data breach and system compromise.

Day 5: Exam Strategy and Integrated Case Workshop

- Review of all eight CISSP domains with key concepts and exam insights.
- High-priority topics and memory aids for complex concepts.
- Full-length mock exam with discussion and analysis.
- Group exercise: Designing a holistic enterprise security program.
- Action plan: Personal roadmap for CISSP success and professional advancement.



Individual Impact

- Gain mastery across all domains of cybersecurity management and governance.
- Strengthen technical and analytical thinking to solve complex security challenges.
- Build leadership capacity to design, implement, and monitor enterprise security systems.
- Enhance professional credibility with globally recognized CISSP readiness.
- Develop a strategic mindset to balance security, usability, and compliance.

Work Impact

- Strengthen the organization's information security posture and resilience.
- Improve compliance alignment with international standards ISO 27001, NIST, GDPR.
- Reduce risk exposure through proactive management and secure design.
- Enable secure digital innovation, cloud adoption, and technology transformation.
- Cultivate a culture of security awareness and accountability across departments.

Training Methodology

This program integrates technical mastery, real-world simulation, and structured exam preparation to ensure participants are ready for both the certification and the workplace.

Learning methods include:

- Interactive domain-based lectures aligned with the CISSP CBK.
- Guided labs and architecture design workshops.
- Case-based learning on data breaches, cloud security, and incident management.
- Timed quizzes and diagnostic assessments mirror the CISSP exam format.
- Comprehensive study toolkits, flashcards, and exam strategy materials.

Beyond the Course

Upon completion, participants will be equipped to confidently pursue the CISSP certification and take leadership roles in securing enterprise systems and infrastructures.

Graduates of this program emerge as trusted cybersecurity leaders — capable of translating security frameworks into actionable strategies that protect assets, ensure compliance, and enable sustainable digital growth.

