CISSP: Mastering Information Systems Security Architecture

2027 □□□□ 26 – 15
Lisbon (Portugal)



CISSP: Mastering Information Systems Security Architecture

Ref: 20230727_132811 Duration: 5 Days Location: Lisbon (Portugal) Fees: 10600 GBP

Why This Course

As cyber threats grow more sophisticated and businesses become increasingly dependent on digital ecosystems, the demand for highly skilled information security professionals has never been greater. The CISSP certification is recognized globally as the gold standard for security expertise, validating deep technical knowledge and strategic leadership in cybersecurity.

The Comprehensive 2-Week CISSP Training Program provides a thorough and practical journey through all eight domains of the CISSP Common Body of Knowledge CBK. Designed for security professionals, IT leaders, and risk practitioners, this program equips participants with the knowledge, frameworks, and hands-on experience needed to design, implement, and manage robust security programs.

Through expert-led sessions, real-world exercises, and detailed exam preparation modules, participants will build the confidence and competence required to excel both in their roles and on the CISSP certification exam.

What You'll Learn and Practice

By the end of this program, participants will be able to:

- Understand and apply core concepts across all eight CISSP domains.
- Design, implement, and manage comprehensive information security programs.
- Identify, assess, and mitigate risks using industry best practices.
- Strengthen their readiness for the CISSP certification exam.
- Gain practical hands-on experience through case studies, labs, and exercises.

The Program Flow

Day 1: Security and Risk Management

- Fundamental principles of information security and confidentiality, integrity, availability CIA.
- Security governance frameworks and compliance requirements.
- Legal, regulatory, and contractual obligations.
- Professional ethics and code of conduct for security practitioners.

Workshop: Building a security governance framework for an enterprise.



Day 2: Asset Security

- Information and asset classification models.
- Defining asset ownership and responsibilities.
- Data protection and privacy considerations.
- Data security controls across the asset lifecycle.

Exercise: Creating a data classification and handling policy.

Day 3: Security Architecture and Engineering I

- Security models, principles, and architectural frameworks.
- Evaluation models and security assurance methodologies.
- Security capabilities and system design considerations.
- Identifying vulnerabilities within system architectures.

Case Study: Assessing architectural weaknesses in a corporate environment.

Day 4: Security Architecture and Engineering II

- Cryptography fundamentals and their practical applications.
- Physical site design and facility security requirements.
- Physical protection controls and threat mitigation.
- Cloud, virtualization, and emerging infrastructure security.

Lab: Designing a secure data center layout.

Day 5: Communication and Network Security

- Designing secure network architectures and topologies.
- Securing network components and communication channels.
- Preventing and detecting network-based attacks.
- Network security technologies and countermeasures.

Simulation: Responding to a live network intrusion scenario.

Day 6: Identity and Access Management

- Physical and logical access control mechanisms.
- Authentication, authorization, and accounting technologies.
- Identity as a Service IDaaS and federated identity management.
- Attacks on identity systems and mitigation strategies.

Exercise: Implementing a multi-factor authentication roadmap.



Day 7: Security Assessment and Testing

- Designing security assessment and testing strategies.
- Techniques for testing security controls and processes.
- Methods for collecting and analyzing security data.
- Conducting internal and external security audits.

Activity: Preparing a security assessment plan for a critical system.

Day 8: Security Operations I

- Managing investigations and incident response processes.
- Disaster recovery planning and resilience strategies.
- Business continuity planning and implementation.
- Logging, monitoring, and security event management.

Workshop: Building an incident response workflow.

Day 9: Security Operations II

- Resource and asset protection techniques.
- Incident containment and eradication procedures.
- Preventive and detective security measures.
- Patch, vulnerability, and configuration management.

Lab: Conducting a vulnerability assessment.

Day 10: Software Development Security

- Integrating security into the Software Development Lifecycle SDLC.
- Security controls for development and testing environments.
- Ensuring software security effectiveness and quality.
- Managing the impact of acquired and third-party software.

Case Study: Reviewing an insecure application design.

Practical Wins for Participants

- The ability to design and implement end-to-end information security programs.
- Strengthened skills in identifying, assessing, and mitigating cybersecurity risks.
- A stronger capability to align security initiatives with business objectives.
- Full readiness and confidence to pass the CISSP certification exam.



Beyond the Course

After completing the program, participants will return to their organizations equipped with advanced security expertise, a holistic understanding of the CISSP domains, and the practical experience needed to drive security governance and resilience. They will be ready to contribute at a higher strategic level and play an essential role in safeguarding digital assets and organizational continuity.

