Syllabus - CISSP

CPU d.o.o. Milentija Popovića 9, Sava Centar DJ 5, 11070 Novi Beograd
Tel: +381 11 3111 527, 3111 824, office2@cpu.rs, www.cpu.rs

Days 1, 2

---

1. Security and Risk Management

- Concepts of confidentiality, integrity and availability
- Security governance principles
- Compliance
- Legal and regulatory issues
- Professional ethics
- Security policy, standards, procedures, and guidelines
- Business continuity requirements
- Personnel security policies
- Risk management concepts
- *Test*

2. Asset Security

- Security Principles
- Identification, Authentication, Authorization, and Accountability
- Access Control Models, Techniques and Technologies
- Access Control Administration
- Access Control Methods and Types
- Access Control Monitoring
- *Test*

Days 3, 4

---

3. Security Engineering

- Security engineering and secure design principles
- Fundamental concepts of security models
- Systems security evaluation models and controls and countermeasures
- Methods of Encryption
- Security capabilities of information systems
- Vulnerabilities of security architectures
- Database security
- Software and System Vulnerabilities and Threats
- Vulnerabilities in Mobile Systems
- Cryptography
- Site and Facility Design Considerations
- Physical security
- *Test*

CPU d.o.o. Milentija Popovića 9, Sava Centar DJ 5, 11070 Novi Beograd
Tel: +381 11 3111 527, 3111 824, office2@cpu.rs, www.cpu.rs

Days 5, 6

4. Communication and Network Security

- Network architecture and secure design principles
- OSI and TCP/IP models
- IP networking
- Implications of Multi-Layer Protocols
- Converged Protocols
- Wireless networks
- Secure network components
- Secure communication channels
- Network Attacks
- *Test*

Days 7, 8

5. Identity and Access Management

- Physical and Logical Access to Assets
- Identification and Authentication of People and Devices
- Identity Management Implementation
- Identity as a Service
- Integrate Third-Party Identity Services
- Implement and Manage Authorization Mechanisms
- Prevent or Mitigate Access Control Attacks
- Identity and Access Provisioning Lifecycle
- *Test*

6. Security Assessment and Testing

- Assessment and Test Strategies
- Conduct security control testing
- Vulnerability assessment
- Penetration testing
- Log reviews
- Code review and testing
- Test coverage analysis
- Collect Security Process Data
- Internal and Third-Party Audits
- *Test*

CPU d.o.o. Milentija Popovića 9, Sava Centar DJ 5, 11070 Novi Beograd
Tel: +381 11 3111 527, 3111 824, office2@cpu.rs, www.cpu.rs

Days 9, 10

7. Security Operations

- Investigations
- Evidence collection and handling
- Reporting and documenting
- Digital forensics
- Logging and monitoring activities
- Intrusion detection and prevention
- Provisioning of Resources through Configuration Management
- Foundational security operations concepts
- Resource Protection
- Conduct incident management
- Preventative Measures against Attacks
- Patch and Vulnerability Management
- Change and Configuration Management
- The Disaster Recovery Process
- Business Continuity and Other Risk Areas
- Physical security
- Personnel Safety
- *Test*

8. Software Development Security

- Security in the Software Development Life Cycle
- Development methodologies
- Maturity models
- Operation and maintenance
- Configuration management
- Security controls in development environments
- Security weaknesses and vulnerabilities at the source-code level
- Assess the Effectiveness of Software Security
- Assess Software Acquisition Security
- *Test*

CPU d.o.o. Milentija Popovića 9, Sava Centar DJ 5, 11070 Novi Beograd
Tel: +381 11 3111 527, 3111 824, office2@cpu.rs, www.cpu.rs