Official (ISC)²® CBK® Training Seminars for the CISSP®

Κωδικός Σεμιναρίου / Code
ISC2-CISSP-01

Αντικείμενο Εκπαιδευτικού Προγράμματος / Description
Led by an (ISC)² authorized instructor, this training seminar provides a comprehensive review of information security concepts and industry best practices, covering the 8 domains of the CISSP CBK.
Several types of activities are used throughout the course to reinforce topics and increase knowledge retention. These activities include open ended questions from the instructor to the students, matching and poll questions, group activities, open/closed questions, and group discussions. This interactive learning technique is based on sound adult learning theories.
This training course will help candidates review and refresh their information security knowledge and help identify areas they need to study for the CISSP exam and features:
• Official (ISC)² courseware
• Taught by an authorized (ISC)² instructor
• Student handbook
• Collaboration with classmates
• Real-world learning activities and scenarios

Σκοπός Εκπαιδευτικού Προγράμματος / Objectives
• Understand and apply the concepts of risk assessment, risk analysis, data classification, and security awareness and Implement risk management and the principles used to support it (Risk avoidance, Risk acceptance, Risk mitigation, Risk transference)
• Apply a comprehensive and rigorous method for describing a current and/or future structure and behavior for an organization's security processes, information security systems, personnel, and organizational sub-units so that these practices and processes align with the organization's core goals and strategic direction and address the frameworks and policies, concepts, principles, structures, and standards used to establish criteria for the protection of information assets, as well as to assess the effectiveness of that protection and establish the foundation of a comprehensive and proactive security program to ensure the protection of an organization's information assets
• Apply a comprehensive and rigorous method for describing a current and/or future structure and behavior for an organization's security processes, information security systems, personnel, and organizational sub-units so that these practices and processes align with the organization's core goals and strategic direction and examine the principles, means, and methods of applying mathematical algorithms and data transformations to information to ensure its integrity, confidentiality, and authenticity
• Understand the structures, transmission methods, transport formats, and security measures used to provide confidentiality, integrity, and availability for transmissions over private and public communications networks and media and identify risks that can be quantitatively and qualitatively measured to support the building of business cases to drive proactive security in the enterprise.
• Offer greater visibility into determining who or what may have altered data or system information, potentially affecting the integrity of those asset and match an entity, such as a person or a computer system, with the actions that entity takes against valuable assets, allowing organizations to have a better understanding of the state of their security posture.
• Plan for technology development, including risk, and evaluate the system design against mission requirements, and identify where competitive prototyping and other evaluation techniques fit in the process
• Protect and control information processing assets in centralized and distributed environments and execute the daily tasks required to keep security services operating reliably and efficiently.
• Understand the Software Development Life Cycle (SDLC) and how to apply security to it, and identify which security control(s) are appropriate for the development environment, and assess the effectiveness of software security

Που Απευθύνεται / Audience
This training course is intended for professionals who have at least 5 years of recent full-time professional work experience in 2 or more of the 8 domains of the CISSP CBK and are pursuing CISSP training and certification to acquire the credibility and mobility to advance within their current information security careers. The training seminar is ideal for those working in positions such as, but not limited to:
• Security Consultant
• Security Manager

- Security Analyst
- Security Systems Engineer
- IT Director/Manager
- Security Auditor
- Security Architect
- Chief Information Security Officer
- Director of Security
- Network Architect

Θεματικές Ενότητες / Topics

The CISSP CBK consists of the following 8 domains:

- Security and Risk Management (Security, Risk, Compliance, Law, Regulations, and Business Continuity)
  - o Confidentiality, integrity, and availability concepts
  - o Security governance principles
  - o Compliance
  - o Legal and regulatory issues
  - o Professional ethic
  - o Security policies, standards, procedures and guidelines
- Asset Security (Protecting Security of Assets)
  - o Information and asset classification
  - o Ownership (e.g. data owners, system owners)
  - o Protect privacy
  - o Appropriate retention
  - o Data security controls
  - o Handling requirements (e.g. markings, labels, storage)
- Security Engineering (Engineering and Management of Security)
  - o Engineering processes using secure design principles
  - o Security models fundamental concepts
  - o Security evaluation models
  - o Security capabilities of information systems
  - o Security architectures, designs, and solution elements vulnerabilities
  - o Web-based systems vulnerabilities
  - o Mobile systems vulnerabilities
  - o Embedded devices and cyber-physical systems vulnerabilities
  - o Cryptography
  - o Site and facility design secure principles
  - o Physical security
- Communication and Network Security (Designing and Protecting Network Security)
  - o Secure network architecture design (e.g. IP & non-IP protocols, segmentation)
  - o Secure network components
  - o Secure communication channels
  - o Network attacks
- Identity and Access Management (Controlling Access and Managing Identity)
  - o Physical and logical assets control
  - o Identification and authentication of people and devices
  - o Identity as a service (e.g. cloud identity)

- Third-party identity services (e.g. on-premise)
- Access control attacks
- Identity and access provisioning lifecycle (e.g. provisioning review)

• Security Assessment and Testing (Designing, Performing, and Analyzing Security Testing)
- Assessment and test strategies
- Security process data (e.g. management and operational controls)
- Security control testing
- Test outputs (e.g. automated, manual)
- Security architectures vulnerabilities

• Security Operations (Foundational Concepts, Investigations, Incident Management, and Disaster Recovery)
- Investigations support and requirements
- Logging and monitoring activities
- Provisioning of resources
- Foundational security operations concepts
- Resource protection techniques
- Incident management
- Preventative measures
- Patch and vulnerability management
- Change management processes
- Recovery strategies
- Disaster recovery processes and plans
- Business continuity planning and exercises
- Physical security
- Personnel safety concerns

• Software Development Security (Understanding, Applying, and Enforcing Software Security)
- Security in the software development lifecycle
- Development environment security controls
- Software security effectiveness
- Acquired software security impact

Μέθοδος Εκπαίδευσης / Method
Classic

Διάρκεια Προγράμματος / Duration
6 days

Διάρκεια Εξέτασης / Duration of Exams
Candidates are given six hours to complete the 250 question CISSP exam wich can be taken at a Pearson VUE Test Center (www.pearsonvue.com/isc2).

Προϋποθέσεις Συμμετοχής / Prerequisites
The CISSP candidate must have at least 5 years of paid full-time experience in 2 or more of the above domains.

Χρήσιμες Πληροφορίες για τους Συμμετέχοντες / Useful Information
-