CISSP Certified Information Systems Security Professional

Learn via: **Classroom / Virtual Classroom / Online**

Duration: **5 Gün**

Overview

Güvenlik profesyonellerine yönelik olan bu eğitim, güvenlik alanına ve kullanılan teknolojilere dair tüm bilgileri ele almaktadır. Eğitim, bilgi sistemleri güvenlik profesyonelleri için ortak bilgi yapısını (CBK) oluşturan sekiz alandaki bilgileri ele almakta olup öğrencilere de CISSP sertifikasyonuna hazırlanmalarında yardımcı olmaktadır.

Eğitim, CBK'da açıklanan kavram ve tekniklerin gerçek dünyaya uygulanması imkanlarının ele alındığı, güvenlik sürecine teori tabanlı bir yaklaşım sunmaktadır. Ayrıca güvenlik yönetimi, mimari ve mühendisliğe iyi bir giriş sunmaktadır.

Eğitim, doğrudan CBK'ya yönelik sekiz oturumdan oluşmakta olup her birinde eğitmen tarafından yönlendirilen, teori bazlı tartışmalar yer almaktadır ve herhangi bir uygulamalı laboratuvar da yoktur.

İncelemeler:

CBT sınavına kaydolmak için adayın bir Pearson VUE test makbuzu alması gerekmektedir. Bu makbuzun fiyatı, bu eğitimin RRP'sine dahil değildir

https://www.isc2.org/certification-register-now.aspx

Sunum Yöntemi - **Uyarlamalı Bilgisayar Testi (CAT)**

Sınav süresi - **En çok 3 saat**

Soru sayısı - **100-150**

Soru formatı - **Çoktan seçmeli ve gelişmiş yenilikçi sorular**

Başarı notu - **Başarı notu 1000 puan üzerinden 700'dür**

S. Şu anki alanlara odaklanan malzemeler ile CISSP sınavına çalışıyor olsaydım ek bir eğitim almadan yeni sınava yeterince hazırlanır mıyım?

A. $(ISC)^2$ sınavları, sadece ders çalışarak öğrenilemeyecek, deneyim esaslı soruları içeren, deneyime dayalı sınavlardır. CISSP'ye dahil olan alanlarda deneyim sahibi iseniz ve bu alanları yeterince çalıştığınıza inanıyorsanız yeni sınava girmeye ve sınavı geçmeye yetkin olduğunuza güvenmelisiniz. $(ISC)^2$, sınavı geçeceğinizi garanti edemez.

Prerequisites

Delegates should have experience in at least two of the domains in the (CBK), for 5 years or more (4 years if they have achieved relevant industry or degree level certifications) to achieve full certification. Associate status can be achieved without the full 4/5 years experience; full certification will be assigned when the correct amount of experience is obtained.

- We recommend delegates have some knowledge of all CBK domains and are encouraged to read one or two of the books on the Reading List at ISC2.org.
- Bilginç IT Academy will provide a CISSP guide book as pre-reading. It is expected that delegates review the guide and gain an appreciation of the key concepts in each of the eight CISSP domains in advance of the course. However, we do not expect delegates to be familiar with all the details of the guide book in advance of the course itself.

We recommend that work completed in the classroom is complemented by extra reading to ensure success in the exam. The amount of extra reading required will depend on the amount of experience the delegate has. The 'mile wide, inch deep' description indicates the challenge to most delegates, not all will have 'hands on' experience spanning all 8 domains of the CBK.

Outline

Module 1. Security and Risk Management

- Understand and apply concepts of confidentiality, integrity and availability
- Apply security governance principles
- Compliance
- Understand legal and regulatory issues that pertain to information security in a global context
- Understand professional ethics
- Develop and implement documented security policy, standards, procedures, and guidelines
- Understand business continuity requirements
- Contribute to personnel security policies
- Understand and apply risk management concepts
- Understand and apply threat modelling
- Integrate security risk considerations into acquisition strategy and practice
- Establish and manage information security education, training, and awareness

Module 2. Asset Security

- Classify information and supporting assets
- Determine and maintain ownership
- Protect privacy
- Ensure appropriate retention
- Determine data security controls
- Establish handling requirements

Module 3. Security Engineering

- Implement and manage engineering processes using secure design principles
- Understand the fundamental concepts of security models
- Select controls and countermeasures based upon systems security evaluation models
- Understand security capabilities of information systems
- Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements
- Assess and mitigate the vulnerabilities in web-based systems
- Assess and mitigate vulnerabilities in mobile systems
- Assess and mitigate vulnerabilities in embedded devices and cyber-physical systems
- Apply cryptography
- Apply secure principles to site and facility design
- Design and implement physical security

Module 4. Communication & Network Security

- Apply secure design principles to network architecture
- Secure network components
- Design and establish secure communication channels
- Prevent or mitigate network attacks

Module 5. Identity & Access Management

- Control physical and logical access to assets
- Manage identification and authentication of people and devices
- Integrate identity as a service
- Integrate third-party identity services
- Implement and manage authorization mechanisms
- Prevent or mitigate access control attacks
- Manage the identity and access provisioning lifecycle

Module 6. Security Assessment & Testing

- Design and validate assessment and test strategies
- Conduct security control testing
- Collect security process data
- Analyse and report test outputs
- Understand the vulnerabilities of security architectures

Module 7. Security Operations

- Understand and support investigations
- Understand requirements for investigation types
- Conduct logging and monitoring activities
- Secure the provisioning of resources
- Understand and apply foundational security operations concepts
- Employ resource protection techniques
- Conduct incident management
- Operate and maintain preventative measures

Module 8. Software Security Development

- Understand and apply security in the software development lifecycle
- Enforce security controls in development environments
- Assess the effectiveness of software security
- Assess security impact of acquired software