



**CERTIFIED INFORMATION
SYSTEMS AUDITOR (CISA)
EĞİTİMİ
5 GÜN**



Digital Vizyon
Akademi

www.digitalvizyon.net



Eđitim Programı Hakkında

Bilgi sistemleri ve teknolojileri çağımızın en kritik bileşenlerinden biridir. Bu sistemlerin doğru ve etkili bir şekilde yönetilmesi, iş süreçlerinin kesintisizliği, müşteri bilgilerinin güvenliği ve bir organizasyonun genel başarısı için kritik öneme sahiptir. İşte tam da bu noktada, bilgi sistemleri denetçilerinin rolü devreye girer.

CISA Nedir?

CISA (Certified Information Systems Auditor), ISACA tarafından verilen ve uluslararası olarak tanınan prestijli bir sertifikadır. CISA sahibi bireyler, bilgi sistemlerinin denetimine, kontrolüne ve değerlendirilmesine dair geniş ve derin bilgiye sahip olduklarını kanıtlarlar.

Eđitimin Amacı Nedir?

CISA eğitiminin amacı, katılımcılara bilgi sistemleri denetiminin temel prensiplerini, en iyi uygulamalarını ve güncel yaklaşımlarını öğretmektir. Aynı zamanda katılımcıları CISA sınavına da hazırlar.

Kimler Katılmalı?

- Bilgi sistemleri ve IT denetçileri
- IT yöneticileri ve danışmanları
- Risk ve uyumluluk profesyonelleri
- Herhangi bir şekilde IT denetim süreçleriyle ilgilenen veya bu alanda kariyer yapmayı planlayan bireyler

Eđitimin İçeriđi Neleri Kapsar?

CISA eğitimi, ISACA'nın belirlediđi temel beş bölüme odaklanır:

- IS Denetiminin İşlevi ve Özelliđi
- IT Yönetimi ve Yönetişimi
- Bilgi Sistemlerinin Edinimi, Geliştirilmesi ve Bakımı
- Bilgi Varlıklarının Korunması
- Operasyonel ve İş Sürekliliđi



Neden CISA?

CISA sertifikasyonu, bilgi sistemleri denetiminde global bir standart olarak kabul edilir. Bu sertifikasyona sahip bireyler, işverenler ve müşteriler tarafından bilgi sistemlerinin denetimi, kontrolü ve güvencesi konularında uzman olarak görülürler. Ayrıca CISA sertifikası olan profesyoneller genellikle daha yüksek maaşlar ve kariyer fırsatlarına sahip olabilirler.

Sonuç

Teknoloji ve bilgi sistemlerinin her geçen gün daha da kritik hale geldiği bir dünyada, CISA eğitimi ve sertifikasyonu, bireylerin ve organizasyonların bu alandaki yetkinliklerini kanıtlamaları ve fark yaratmaları için mükemmel bir fırsattır.

Eğitim İçeriği

General Information About the Exam

- About the CISA Exam
- Answering Questions
- Exam Scoring
- Certification Steps
- Example Questions

Domain 1: Information System Auditing Process

- **Planning**
 - IS Audit Standards, Guidelines and Codes of Ethics
 - Business Processes
 - Types of Controls
 - Risk-based Audit Planning
 - Types of Audits and Assessments
- **Execution**
 - Audit Project Management
 - Sampling Methodology
 - Audit Evidence Collection Techniques
 - Data Analytics
 - Reporting and Communication Techniques
 - Quality Assurance and Improvement of the Audit Process

Domain 2: Governance and Management of IT

- **IT Governance and IT Strategy**
 - IT-related Frameworks
 - IT Standards, Policies and Procedures
 - Organizational Structure
 - Enterprise Architecture
 - Enterprise Risk Management
 - Maturity Models



- Laws, Regulations and Industry Standards Affecting the Organization
- **IT Management**
 - IT Resource Management
 - IT Service Provider Acquisition and Management
 - IT Performance Monitoring and Reporting
 - Quality Assurance and Quality Management of IT

Domain 3: Information Systems Acquisition, Development and Implementation

- **Information Systems Acquisition and Development**
 - Project Governance and Management
 - Business Case and Feasibility Analysis
 - System Development Methodologies
 - Control Identification and Design
- **Information Systems Implementation**
 - Testing Methodologies
 - Configuration and Release Management
 - System Migration, Infrastructure Deployment and Data Conversion
 - Post-implementation Review

Domain 4: IS Operations and Business Resilience

- **Information Systems Operations**
 - Common Technology Components
 - IT Asset Management
 - Job Scheduling and Production Process Automation
 - System Interfaces
 - End-user Computing
 - Data Governance
 - Systems Performance Management
 - Problem and Incident Management
 - Change, Configuration, Release and Patch Management
 - IT Service Level Management
 - Database Management
- **Business Resilience**
 - Business Impact Analysis
 - System Resiliency
 - Data Backup, Storage and Restoration
 - Business Continuity Plan
 - Disaster Recovery Plans

Domain 5: Information Asset Security and Control

- **Information Asset Security Frameworks, Standards and Guidelines**
 - Privacy Principles
 - Physical Access and Environmental Controls
 - Identity and Access Management
 - Network and End-point Security
 - Data Classification



- Data Encryption and Encryption-related Techniques
- Public Key Infrastructure
- Web-based Communication Technologies
- Virtualized Environments
- Mobile, Wireless and Internet-of-things Devices
- **Security Event Management**
 - Security Awareness Training and Programs
 - Information System Attack Methods and Techniques
 - Security Testing Tools and Techniques
 - Security Monitoring Tools and Techniques
 - Incident Response Management
 - Evidence Collection and Forensics