Certified Information Systems Auditor (CISA) Eğitimi

Süre: **4 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

- **Bilgi sistemlerini ISACA'nın beş temel alanı kapsamında denetlemeyi, kontrol etmeyi ve güvenliğini değerlendirmeyi öğrenin.**
- **CISA sertifikasına hazırlanan deneyimli BT denetçileri, uyumluluk ve risk profesyonelleri için tasarlanmıştır.**
- **Uzman eğitmenler tarafından verilen program, Ağustos 2024 itibarıyla geçerli güncel CISA sınav içeriğini kapsar.**

Certified Information Systems Auditor (CISA), bilgi sistemleri denetimi, kontrolü ve güvenliği alanında çalışan profesyoneller için dünya çapında tanınan önemli sertifikalardan biridir. CISA, profesyonellerin mevcut iş deneyimlerini sistematik denetim bilgisiyle birleştirerek kurumların bilgi sistemlerini daha etkin biçimde değerlendirmelerine yardımcı olur.

CISA sertifikası, **DoD Approved 8570 Baseline Certification** kapsamında yer almakta ve **DoD 8140/8570 eğitim gereksinimlerini** karşılamaktadır.

CISA eğitimimiz boyunca katılımcılar, sınavın ve sertifikasyon kapsamının temelini oluşturan beş ana bilgi sistemleri denetim alanı üzerinde çalışır. Her alan, bilgi sistemlerinin denetlenmesi, yönetilmesi, geliştirilmesi, işletilmesi ve korunmasına ilişkin farklı konu başlıklarını içerir.

Program kapsamlı ve yoğun bir içeriğe sahiptir. Bu nedenle katılımcıların eğitim sırasında ele alınan konuları düzenli olarak tekrar etmeleri ve CISA sınavına yönelik bireysel çalışmalarını sürdürmeleri önerilir.

CISA'nın beş temel alanı şunlardır:

1. **Bilgi Sistemleri Denetim Süreci**
2. **BT Yönetişimi ve Yönetimi**
3. **Bilgi Sistemlerinin Edinimi, Geliştirilmesi ve Uygulanması**
4. **Bilgi Sistemleri Operasyonları ve İş Sürekliliği**
5. **Bilgi Varlıklarının Korunması**

Prerequisites

CISA konularını öğrenmeye başlamak için zorunlu bir eğitim ön koşulu bulunmamaktadır. Bununla birlikte CISA sertifikasını alabilmek için adayların ISACA tarafından belirlenen sertifikasyon koşullarını yerine getirmeleri gerekir.

Bu kapsamda adayların:

- CISA sınavını başarıyla tamamlaması,
- CISA sertifikasyon başvurusunda bulunması,
- ISACA'ya doğrudan 50 USD başvuru ücreti ödemesi,
- ISACA Mesleki Etik Kurallarına uyması,
- Sürekli Mesleki Eğitim (CPE) programının gerekliliklerini yerine getirmesi,

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Bilgi Sistemleri Denetim Standartlarına uygun hareket etmesi

beklenmektedir.

CISA sınavı; bilgi sistemleri denetimi, kontrolü ve güvenliğiyle ilgilenen kişilere açıktır. Ancak CISA sertifikasını alabilmek için bilgi sistemleri denetimi, kontrolü veya güvenliği alanında en az **5 yıllık profesyonel iş deneyimi** gerekmektedir.

Programın kapsamı ve yoğunluğu nedeniyle eğitim özellikle bilgi sistemleri denetimi konusunda deneyim sahibi profesyonellere yöneliktir. CISA sertifikasyonu; denetim, risk, güvenlik, yönetişim ve uyumluluk alanlarında kariyerini ileri taşımak isteyen profesyoneller açısından önemli bir yetkinlik göstergesidir.

Who Should Attend

CISA eğitimi; bir kurumun bilgi teknolojileri ve iş sistemlerini kontrol eden, izleyen, değerlendiren veya denetleyen profesyonellere yöneliktir.

Özellikle aşağıdaki görevlerde çalışan profesyoneller için uygundur:

- IS/IT denetçileri ve danışmanları
- BT uyumluluk yöneticileri
- Chief Compliance Officer (CCO)
- Risk ve gizlilik yöneticileri
- Bilgi güvenliği yöneticileri ve direktörleri
- Güvenlik yöneticileri ve güvenlik mimarları

Bu liste yalnızca genel bir hedef kitle çerçevesi sunmaktadır. Profesyoneller kariyer hedefleri, mevcut görevleri ve kişisel gelişim planları doğrultusunda da programa katılabilir.

What You Will Learn

Eğitimin sonunda katılımcıların CISA'nın beş temel alanına ilişkin kapsamlı bilgi edinmeleri hedeflenmektedir:

- Bilgi Sistemleri Denetim Süreci
- BT Yönetişimi ve Yönetimi
- Bilgi Sistemlerinin Edinimi, Geliştirilmesi ve Uygulanması
- Bilgi Sistemleri Operasyonları ve İş Sürekliliği
- Bilgi Varlıklarının Korunması

Outline

Domain 1: Bilgi Sistemleri Denetim Süreci

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

Bu bölümde katılımcılar bilgi sistemleri denetiminin planlanması ve yürütülmesine ilişkin temel uygulamaları ele alır.

Başlıca konular:

- Risk bazlı BT denetim stratejisinin geliştirilmesi
- Belirli denetim çalışmalarının planlanması
- Denetimlerin IS denetim standartlarına uygun yürütülmesi
- Risk yönetimi ve kontrol uygulamalarının hayata geçirilmesi

Domain 2: BT Yönetişimi ve Yönetimi

Bu bölüm, kurumların BT yönetişim yapılarının ve yönetim uygulamalarının değerlendirilmesine odaklanır.

Başlıca konular:

- BT yönetişim yapısının etkinliğinin değerlendirilmesi
- BT organizasyon yapısı ve insan kaynakları yönetimi
- Kurumsal BT politikaları, standartları ve prosedürleri
- Kalite Yönetim Sisteminin yeterliliği
- BT yönetimi ve izleme kontrolleri
- BT kaynak yatırımlarının değerlendirilmesi
- BT sözleşme stratejileri ve politikaları
- Kurumsal BT risklerinin yönetimi
- İzleme ve güvence uygulamaları
- Kurumsal iş sürekliliği planlarının değerlendirilmesi

Domain 3: Bilgi Sistemlerinin Edinimi, Geliştirilmesi ve Uygulanması

Bu bölümde bilgi sistemlerinin yaşam döngüsü boyunca uygulanan proje ve kontrol süreçleri incelenir.

Başlıca konular:

- Bilgi sistemlerinin edinimi, geliştirilmesi, bakımı ve kullanımdan kaldırılması için iş gerekçesinin hazırlanması
- Proje yönetimi uygulamaları ve kontrolleri
- Proje yönetimi süreçlerinin gözden geçirilmesi
- Gereksinim, edinim, geliştirme ve test aşamalarındaki kontroller
- Bilgi sistemlerinin kullanıma hazır olup olmadığının değerlendirilmesi
- Proje planlarının incelenmesi
- Uygulama sonrası sistem değerlendirmeleri

Domain 4: Bilgi Sistemleri Operasyonları ve İş Sürekliliği

Bu bölüm, bilgi sistemlerinin günlük operasyonlarının sürdürülebilirliği ve iş sürekliliği uygulamalarına odaklanır.

Başlıca konular:

- Kurumsal hedeflerin periyodik olarak değerlendirilmesi
- Hizmet seviyesi yönetimi
- Üçüncü taraf yönetim uygulamaları

- Operasyon ve son kullanıcı prosedürleri
- Bilgi sistemleri bakım süreçleri
- Veritabanlarının bütünlüğü ve optimizasyonuna yönelik veri yönetimi uygulamaları
- Kapasite ve performans izleme araçları ile teknikleri
- Problem ve olay yönetimi uygulamaları
- Değişiklik, konfigürasyon ve sürüm yönetimi
- Yedekleme ve geri yükleme süreçlerinin yeterliliği
- Felaket durumlarında uygulanacak kurumsal felaket kurtarma planlarının değerlendirilmesi

Domain 5: Bilgi Varlıklarının Korunması

Bu bölümde kurumların bilgi varlıklarını korumak için kullandığı güvenlik kontrolleri ve prosedürler ele alınır.

Başlıca konular:

- Bilgi güvenliği politikaları, standartları ve prosedürleri
- Sistem ve mantıksal güvenlik kontrollerinin tasarlanması, uygulanması ve izlenmesi
- Veri sınıflandırma süreçleri ve prosedürlerinin tasarlanması, uygulanması ve izlenmesi
- Fiziksel erişim ve çevresel kontrollerin tasarlanması, uygulanması ve izlenmesi
- Bilgi varlıklarının saklanması, geri alınması, taşınması ve güvenli biçimde imha edilmesine yönelik süreçler

2024 CISA Sınav İçeriği ve Domain Ağırlıkları

1 Ağustos 2024 itibarıyla CISA Exam Content Outline (ECO) güncellenmiştir. Beş temel domain başlığı korunurken sınav içerisindeki ağırlıklarda değişiklik yapılmıştır.

Domain	2019 ECO	2024 ECO
Domain 1: Information Systems Auditing Process	%21	%18
Domain 2: Governance and Management of IT	%17	%18
Domain 3: Information Systems Acquisition, Development and Implementation	%12	%12
Domain 4: Information Systems Operations and Business Resilience	%23	%26
Domain 5: Protection of Information Assets	%27	%26
Toplam	**%100**	**%100**

ISACA Ürün Erişim Sürelerinde Değişiklik

16 Nisan 2026 İtibarıyla Geçerli Güncelleme

ISACA, **16 Nisan 2026** tarihinden itibaren sınavlar, QAE ürünleri, Online Review Courses, sponsorlu olmayan webinarlar ve Virtual Workshops dahil olmak üzere çeşitli ürünlerin erişim sürelerini 12 aydan **6 aya** indirmektedir.

Yeni Erişim Süreci Nasıl İşliyor?

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

1. Atama ve Aktivasyon Süresi

Satın alınan ürünlerin, satın alma tarihinden itibaren 6 ay içerisinde kullanıcıya atanması ve aktive edilmesi gerekir.

2. Erişim ve Tamamlama Süresi

Ürün aktive edildikten sonra katılımcının ürünü kullanmak için 6 aylık erişim süresi bulunur. Bu dönem; eğitim içeriğine erişme, sınav planlama ve uygun olduğu durumlarda sınava girme süreçlerini kapsar.

Katılımcılar İçin Ne Anlama Geliyor?

- **Review Manuals:** Katılımcılar uzun süreli erişime sahip olmaya devam eder.
- **QAE Databases & Online Review Courses:** Aktivasyondan sonra 6 ay kullanılabilir.
- **Exams:** Aktivasyondan itibaren 6 ay içerisinde planlanmalı ve tamamlanmalıdır.

Katılımcıların erişim sürelerini en verimli şekilde kullanabilmeleri için ürünlerini zamanında aktive etmeleri ve çalışma/sınav programlarını buna göre planlamaları önerilir.

CISA Sınavı ve Değerlendirme

Bu eğitim CISA sınavını içerir ve sınav ISACA tarafından sunulur.

CISA sınav içeriği beş ana domain üzerine kuruludur. Domain ağırlıkları, Ağustos 2024'te yürürlüğe giren güncel Exam Content Outline doğrultusunda belirlenmiştir.

ISACA'nın Nisan 2026'da yürürlüğe giren yeni erişim politikasına göre sınav erişiminin aktivasyondan itibaren **6 ay içerisinde planlanması ve sınavın bu süre içerisinde tamamlanması** gerekir.

CISA sertifikasını elde etmek için sınavın tamamlanmasının yanı sıra adayların ISACA'ya sertifikasyon başvurusu yapması, 50 USD başvuru ücretini ödemesi, Mesleki Etik Kurallarına uyması, Sürekli Mesleki Eğitim (CPE) programına bağlı kalması ve Bilgi Sistemleri Denetim Standartlarını karşılaması gerekir.

CISA sertifikasyonunun alınabilmesi için ayrıca bilgi sistemleri denetimi, kontrolü veya güvenliği alanında en az **5 yıllık profesyonel iş deneyimi** şartı bulunmaktadır.