Certified Information Security Manager (CISM) Eğitimi

Süre: **4 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

- **Kurumunuzun güvenlik mimarisini güvenle tasarlayın, uygulayın ve yönetin.**
- **Bilgi güvenliği yönetişimi ve risk yönetimi uzmanlığını geliştirmek isteyen güvenlik yöneticileri ve CISO'lar için tasarlanmıştır.**
- **ISACA ile uyumlu eğitim içeriğiyle CISM sınavına kapsamlı şekilde hazırlanın.**

Certified Information Security Manager (CISM) eğitimi; bilgi güvenliği operasyonlarının oluşturulması, geliştirilmesi ve yönetilmesine odaklanan kapsamlı bir programdır. CISM sertifikası, bilgi güvenliği yönetimi alanında profesyonel bilgi, uygulama deneyimi ve yönetim yetkinliğinin önemli göstergelerinden biridir.

Eğitim kapsamında yalnızca teorik güvenlik prensipleri değil; bilgi güvenliği programlarının oluşturulması, risklerin yönetilmesi ve güvenlik olaylarına müdahale edilmesi gibi uygulamaya dönük konular da ele alınır. Katılımcılar, sürekli değişen teknolojilerin ve güvenlik ihtiyaçlarının kurumun hedefleri doğrultusunda nasıl yönetilebileceğini öğrenir.

CISM yaklaşımı, bilgi güvenliğini yalnızca teknik bir konu olarak değerlendirmek yerine kurumsal hedeflerle ilişkilendirir. Böylece güvenlik profesyonellerinin bilgi güvenliği programları ile kurumun daha geniş kapsamlı iş hedefleri arasındaki bağlantıyı anlamalarına yardımcı olur.

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

Nitelikli bilgi güvenliği yöneticilerine duyulan ihtiyacın artmasıyla birlikte CISM, bilgi güvenliği yönetimi alanında uluslararası ölçekte tanınan profesyonel sertifikalardan biri haline gelmiştir. Sertifika özellikle güvenlik yönetişimi, risk yönetimi, güvenlik programlarının yönetimi ve olay yönetimi alanlarında uzmanlaşmak isteyen profesyonellere yöneliktir.

CISM dört temel domain üzerine kuruludur:

1. **Information Security Governance**
2. **Information Risk Management**
3. **Information Security Program Development and Management**
4. **Information Security Incident Management**

Bu eğitim, resmi ISACA CISM sınavını ve resmi ISACA Exam Prep Tool'u içerir.

Prerequisites

CISM konularını öğrenmek için zorunlu bir eğitim ön koşulu bulunmamaktadır. Bununla birlikte CISM sertifikasını elde edebilmek için adayların ISACA'nın sertifikasyon gerekliliklerini yerine getirmesi gerekir.

Bu gereklilikler şunlardır:

- CISM sınavını başarıyla tamamlamak
- CISM sertifikasyon başvurusunda bulunmak
- ISACA'ya doğrudan 50 USD başvuru ücreti ödemek
- ISACA Mesleki Etik Kurallarına uymak
- Sürekli Mesleki Eğitim (CPE) programına bağlı kalmak
- Bilgi güvenliği standartlarına uyum sağlamak

CISM sınavı bilgi güvenliği alanıyla ilgilenen kişilere açıktır. Ancak CISM sertifikasının alınabilmesi için en az **5 yıllık profesyonel bilgi sistemleri denetimi, kontrolü veya güvenliği deneyimi** gerekmektedir.

Who Should Attend

CISM, BT ve bilgi güvenliği alanındaki profesyonellere yönelik, dünya çapında tanınan bir sertifikasyondur. Eğitim özellikle aşağıdaki rollerde çalışan profesyoneller için uygundur:

- Güvenlik danışmanları ve yöneticileri
- BT direktörleri ve yöneticileri
- Güvenlik denetçileri ve mimarları
- Güvenlik sistemleri mühendisleri
- Chief Information Security Officer (CISO)
- Bilgi güvenliği yöneticileri
- IS/IT danışmanları
- Chief Compliance, Privacy veya Risk Officer rollerinde çalışan yöneticiler

Bu roller yalnızca önerilen hedef kitleyi göstermektedir. Katılımcılar kariyer hedefleri, kişisel gelişim planları veya profesyonel sorumlulukları doğrultusunda da eğitime katılabilir.

Certified Information Security Manager (CISM) Eğitimi

Süre: **4 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

CISM eğitimi, kurumunuzun güvenlik mimarisini tasarlamak, uygulamak ve yönetmek için ihtiyaç duyacağınız temel yönetim becerilerini geliştirmenizi amaçlar.

Program ISACA'nın bilgi güvenliği yönetimi yaklaşımıyla uyumludur ve katılımcıların CISM sınavına hazırlanmasına yardımcı olacak şekilde yapılandırılmıştır.

Eğitim sonunda katılımcıların;

- Bilgi güvenliği yönetişim yapısını değerlendirebilmesi,
- Bilgi güvenliği risklerini belirleyip yönetebilmesi,
- Kurumsal güvenlik programları geliştirebilmesi,
- Güvenlik programlarının performansını takip edebilmesi,
- Bilgi güvenliği olaylarına yönelik süreçleri yönetebilmesi,
- Güvenlik, uyumluluk ve yönetişim gereksinimlerini kurumsal hedeflerle ilişkilendirebilmesi

amaçlanmaktadır.

CISM Domain Ağırlıkları

CISM sınav kapsamındaki dört domain ve ağırlıkları şöyledir:

Domain	Sınav Ağırlığı
Domain 1: Information Security Governance	%17
Domain 2: Information Risk Management	%20
Domain 3: Information Security Program Development and Management	%33
Domain 4: Information Security Incident Management	%30
Toplam	**%100**

Outline

CISM'e Giriş

- Certified Information Security Manager (CISM) genel bakış
- Eğitimin hedefleri ve beklentiler
- Bilgi güvenliği nedir?
- Bilgi güvenliğinin temel hedefleri
- Bilgi güvenliği profesyonelleri için temel prensipler

Domain 1 – Information Security Governance

Bu bölüm, bilgi güvenliğinin kurum genelinde nasıl yönetileceğine ve güvenlik stratejisinin kurumsal hedeflerle nasıl ilişkilendirileceğine odaklanır.

Ele alınan konular:

- Bilgi güvenliği yönetişimine giriş
- Etkili bilgi güvenliği yönetişimi

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

- Yönetişim ve üçüncü taraf ilişkileri
- Bilgi güvenliği metrikleri
- Bilgi güvenliği yönetişim metrikleri
- Bilgi güvenliği stratejisi
- Bilgi güvenliği stratejisinin geliştirilmesi
- Stratejik kaynaklar ve kısıtlamalar
- Diğer güvenlik ve yönetişim çerçeveleri
- Uyumluluk gereksinimleri
- Stratejinin uygulanmasına yönelik aksiyon planları
- Kurumsal BT yönetişimi

Domain 2 – Information Risk Management

Bu bölüm, kurumların bilgi güvenliği risklerini tanımlaması, değerlendirmesi, izlemesi ve yönetmesine ilişkin temel uygulamaları kapsar.

Ele alınan konular:

- Bilgi risk yönetimi
- Risk yönetimine genel bakış
- Risk değerlendirmesi
- Bilgi varlıklarının sınıflandırılması
- Değerlendirme yönetimi
- Bilgi kaynaklarının değerlemesi
- Recovery Time Objectives (RTO)
- Güvenlik kontrol taban çizgileri
- Risklerin izlenmesi
- Eğitim ve farkındalık
- Bilgi risk yönetimi dokümantasyonu

Domain 3 – Information Security Program Development and Management

Bu bölümde kurumsal bilgi güvenliği programlarının oluşturulması, uygulanması ve sürekli olarak yönetilmesi ele alınır.

Ele alınan konular:

- Bilgi güvenliği program yönetimine genel bakış
- Bilgi güvenliği programının hedefleri
- Bilgi güvenliği programının temel kavramları
- Güvenlik programının teknoloji kaynakları
- Bilgi güvenliği programının geliştirilmesi
- Bilgi güvenliği program çerçevesi
- Güvenlik programı yol haritası
- Enterprise Information Security Architecture (EISA)
- Güvenlik programının yönetimi ve idaresi
- Güvenlik programı hizmetleri ve operasyonel faaliyetler
- Güvenlik kontrolleri
- Güvenlik programı metrikleri ve izleme
- Operasyonel performansın ölçülmesi
- Bilgi güvenliği programlarında karşılaşılan yaygın zorluklar

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

Domain 4 – Information Security Incident Management

Bu bölüm, bilgi güvenliği olaylarının hazırlanma, müdahale, kurtarma ve olay sonrası değerlendirme aşamalarının yönetimine odaklanır.

Ele alınan konular:

- Olay yönetimine genel bakış
- Olay yönetimi prosedürleri
- Olay yönetimi kaynakları
- Olay yönetimi hedefleri
- Olay yönetimi metrikleri ve göstergeleri
- Olay yönetimi prosedürlerinin tanımlanması
- İş sürekliliği ve felaket kurtarma prosedürleri
- Olay sonrası faaliyetler ve incelemeler

Etik, Mevzuat ve Profesyonel Sorumluluklar

Eğitim kapsamında ayrıca CISM profesyonellerinin karşılaşabileceği etik ve düzenleyici konular ele alınır:

- ISACA Mesleki Etik Kuralları
- Kanunlar ve düzenlemeler
- Kurum içerisindeki politikalar ile kanunlar arasındaki ilişki
- Etik ve internet
- Certified Information Security Manager profesyonel sorumlulukları

ISACA Ürün Erişim Sürelerinde Değişiklik

16 Nisan 2026 İtibarıyla Geçerli Güncelleme

ISACA, **16 Nisan 2026** itibarıyla Exams, QAE, Online Review Courses, sponsorlu olmayan Webinars ve Virtual Workshops dahil olmak üzere çeşitli ürünlerin erişim sürelerini **12 aydan 6 aya** düşürmektedir.

Yeni Erişim Süreci

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 kullanabilmesi için **6 aylık erişim süresi** başlar. İlgili ürüne bağlı olarak bu süre;

- Eğitim içeriğine erişmeyi,
- Sınav planlamayı,
- Sınava girmeyi

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

kapsar.

Bu Değişiklik Katılımcılar İçin Ne Anlama Geliyor?

Review Manuals: Uzun süreli erişim devam eder.

QAE Databases & Online Review Courses: Aktivasyondan sonra 6 ay boyunca erişilebilir.

Exams: Aktivasyondan itibaren 6 ay içerisinde planlanmalı ve tamamlanmalıdır.

Katılımcıların erişim haklarından maksimum düzeyde yararlanabilmeleri için ürünlerini zamanında aktive etmeleri ve çalışma ile sınav programlarını erkenden planlamaları önerilir.

Sınav ve Değerlendirme

Bu eğitimin ücretine **resmi ISACA CISM sınavı** ve **resmi ISACA Exam Prep Tool** dahildir.

CISM sertifikasını elde etmek için adayların sınavı başarıyla tamamlamanın yanı sıra ISACA'ya sertifikasyon başvurusunda bulunması, 50 USD başvuru ücretini doğrudan ISACA'ya ödemesi, ISACA Mesleki Etik Kurallarına uyması ve Sürekli Mesleki Eğitim (CPE) programına bağlı kalması gerekir.

CISM sertifikasının verilebilmesi için adayların ayrıca en az**5 yıllık profesyonel bilgi sistemleri denetimi, kontrolü veya güvenliği deneyimine** sahip olması gerekmektedir.

16 Nisan 2026 itibarıyla geçerli yeni ISACA erişim politikasına göre, ürün aktive edildikten sonra katılımcıların eğitim içeriğine erişmek, sınavlarını planlamak ve sınava girmek için **6 aylık süreleri** bulunmaktadır. Bu nedenle aktivasyon ve sınav planlamasının zamanında yapılması önerilir.