BCS Certificate in Information Security Management Principles Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Bu resmi **BCS CISMP** eğitimi, bilgi güvenliği alanında temel bilgi edinmek isteyen profesyoneller ile mevcut görevleri kapsamında bilgi güvenliği sorumluluğu bulunan çalışanlar için hazırlanmıştır.

BCS CISMP v10 müfredatına uygun olarak hazırlanan eğitim, katılımcıları resmi BCS CISMP sertifika sınavına hazırlar. Eğitim kapsamında sınav voucher'ı ve **BCS CISMP Kitabı (4. Baskı)** da sunulmaktadır.

Katılımcılar eğitim boyunca bilgi güvenliğinin temel prensiplerini ayrıntılı şekilde öğrenir. Gizlilik (Confidentiality), bütünlük (Integrity), erişilebilirlik (Availability), tehditler, zafiyetler, riskler ve güvenlik kontrolleri gibi temel kavramlar kapsamlı olarak ele alınır. Ayrıca bilgi güvenliği yönetimini etkileyen yasal düzenlemeler, uluslararası standartlar ve güncel teknolojiler incelenir.

Program sonunda katılımcılar, güvenlik prensiplerini iş süreçlerine uygulayabilecek, kurumsal güvenlik yönetimine katkı sağlayabilecek ve daha ileri seviye teknik veya yönetsel bilgi güvenliği sertifikaları için güçlü bir temel oluşturacaktır.

Prerequisites

Bu eğitime katılım için herhangi bir ön koşul bulunmamaktadır.

Who Should Attend

Bilgi güvenliği yalnızca BT ekiplerinin değil, kurum içerisindeki tüm birimlerin ortak sorumluluğudur. Bu eğitim özellikle aşağıdaki profesyoneller için uygundur:

- Bilgi güvenliği ekiplerinde görev alan çalışanlar
- BT yöneticileri ve sistem yöneticileri
- Bilgi güvenliği yöneticileri
- Bilgi varlığı sahipleri (Information Asset Owners)
- İş analistleri
- Proje yöneticileri
- Ürün sahipleri (Product Owners)
- Hizmet yönetimi profesyonelleri
- Risk, uyumluluk (Compliance) ve gizlilik uzmanları

Sürekli Mesleki Gelişim (CPD)

NCSC onaylı bu eğitim kapsamında katılımcılar, eğitim süresinin her saati için**1 CPD puanı** kazanabilir. Toplamda **15 CPD puanına** kadar kredi alınabilmektedir.

BCS Certificate in Information Security Management Principles Eğitimi

Süre: **5 Gün**

BİLGİNÇ
IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

Bu eğitimi tamamlayan katılımcılar;

- Bilgi güvenliği yönetiminin temel kavramlarını, prensiplerini ve sağladığı faydaları açıklayabilir.
- Bilgi güvenliğiyle ilgili hukuki, etik ve düzenleyici gereklilikleri değerlendirebilir.
- Risk yönetimi süreçlerini ve risk azaltma yöntemlerini uygulayabilir.
- Kurumsal yapı, yönetişim ve organizasyon kültürünün bilgi güvenliği üzerindeki etkisini analiz edebilir.
- Güvenlik standartlarını, çerçevelerini ve güvenlik teknolojilerini tanımlayabilir.
- Güvenli yazılım geliştirme süreçleri ve bilgi güvenliği yaşam döngüsünü açıklayabilir.
- Olay müdahalesi, iş sürekliliği ve felaket kurtarma süreçlerinde uygulanması gereken temel yaklaşımları değerlendirebilir.

Outline

Modül 1: Bilgi Güvenliğinin Temelleri

- Bilgi güvenliğinin temel kavramları
- Bilgi güvenliği ve veri gizliliği
- Gizlilik, bütünlük ve erişilebilirlik ilkeleri
- Kişisel verilerin korunmasına ilişkin temel düzenlemeler

Bu modül sonunda katılımcılar:

- Bilgi güvenliği terminolojisini açıklayabilir.
- Bilgi güvenliğinin kurumsal önemini değerlendirebilir.
- Veri gizliliğiyle ilgili temel yasal gereklilikleri tanımlayabilir.

Modül 2: Bilgi Güvenliğinde Risk Yönetimi

- Risk kavramı
- Risk değerlendirme yöntemleri
- Risk yönetim süreci
- Risk azaltma stratejileri

Bu modül sonunda katılımcılar:

- Risk yönetiminin temel bileşenlerini açıklayabilir.
- Risk yaşam döngüsündeki süreçleri değerlendirebilir.

Modül 3: Bilgi Güvenliği Çerçeveleri

- Organizasyonel sorumluluklar
- Politika, prosedür ve standartlar
- Güvenlik yönetişimi
- Hukuki düzenlemeler
- Bilgi güvenliği standartları ve güvence yaklaşımları

Bu modül sonunda katılımcılar:

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

- Organizasyon yapısının bilgi güvenliğine etkisini açıklayabilir.
- Güvenlik yönetişimi prensiplerini değerlendirebilir.
- Yaygın güvenlik standartlarını ve çerçevelerini tanıyabilir.

Modül 4: Güvenlik Operasyonları

- Bilginin yaşam döngüsü
- Bilgi güvenliği yönetimi
- Teknik denetimler
- Sistem geliştirme süreçleri
- Güvenli yazılım geliştirme yaşam döngüsü (SDLC)

Bu modül sonunda katılımcılar:

- Güvenlik mimarisi modellerini açıklayabilir.
- Tehdit modelleme yöntemlerini tanımlayabilir.
- Güvenlik açıklarının belirlenmesi ve yönetimi konusunda bilgi sahibi olabilir.
- Yaygın siber saldırıları ve tehdit türlerini ayırt edebilir.

Modül 5: Güvenlik Yaşam Döngüsü ve DevSecOps

- Güvenlik yaşam döngüsü
- Güvenlik mimarisi
- DevSecOps yaklaşımı
- Tehdit modelleme
- Zafiyet analizi
- Zararlı yazılımlara karşı korunma yöntemleri

Bu modül sonunda katılımcılar:

- Bilgi güvenliği yaşam döngüsünü açıklayabilir.
- DevSecOps'un temel kavramlarını ve avantajlarını değerlendirebilir.

Modül 6: Teknik Güvenlik

- Ağ ve iletişim güvenliği
- Bulut güvenliği
- Harici hizmetlerin güvenliği
- BT altyapısının korunması
- Kriptografinin temel prensipleri

Bu modül sonunda katılımcılar:

- Ağ güvenliği prensiplerini açıklayabilir.
- Altyapı güvenliği için kullanılan teknik kontrolleri tanımlayabilir.

Modül 7: Fiziksel ve Çevresel Güvenlik

- Fiziksel güvenlik kontrolleri
- Teknik ve idari güvenlik önlemleri
- Temiz masa ve temiz ekran politikaları
- Donanım koruma yöntemleri
- Teslimat alanlarının güvenliği

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Güvenli veri ve ekipman imhası

Bu modül sonunda katılımcılar:

- Fiziksel güvenlik uygulamalarını ve en iyi uygulama yöntemlerini açıklayabilir.

Modül 8: Felaket Kurtarma ve Dijital Adli Bilişim

- Olay müdahale planlaması
- İş sürekliliği yönetimi
- Felaket kurtarma planları
- Dijital adli bilişimin temel prensipleri

Bu modül sonunda katılımcılar:

- Olay müdahale süreçlerini açıklayabilir.
- Felaket kurtarma yaklaşımını değerlendirebilir.
- Dijital delil toplama ve inceleme süreçlerinin temel mantığını anlayabilir.

Modül 9: Yeni Nesil Teknolojiler ve Bilgi Güvenliği

- Yeni teknolojilerin oluşturduğu güvenlik riskleri
- Yapay zekâ yönetişimi ve AI güvenliği
- Nesnelerin İnterneti (IoT)
- Operasyonel Teknolojiler (OT)

Bu modül sonunda katılımcılar:

- Gelişmekte olan teknolojilerin bilgi güvenliği üzerindeki etkilerini değerlendirebilir.

Modül 10: Sertifika Sınavına Hazırlık

- BCS CISMP sınav yapısının incelenmesi
- Sınav stratejileri
- Tam kapsamlı deneme sınavı
- Soru çözüm teknikleri ve genel tekrar