Certified ISO 27001 Practitioner Eğitimi

Süre: **4 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

- **ISO 27001:2022 uyumlu bir ISMS yapısını planlayın, uygulayın ve denetleyin.**
- **Bilgi güvenliği, risk, denetim ve uyumluluk süreçlerinden sorumlu profesyoneller için tasarlanmıştır.**
- **Dokuz uygulamalı egzersiz sayesinde gerçek denetim becerileri geliştirin.**

Certified ISO 27001 Practitioner eğitimi, katılımcıların ISO/IEC 27001 standardının gereksinimlerini ve temel prensiplerini anlamasını ve bu gereksinimlere uygun bir Information Security Management System (ISMS) oluşturabilmesini amaçlayan uygulamalı bir programdır.

Eğitim, özellikle **ISO/IEC 27001:2022** standardında tanımlanan bilgi güvenliği yönetim sistemi yapısına odaklanır. Katılımcılar, bir ISMS'in yalnızca nasıl kurulacağını değil, aynı zamanda nasıl sürdürüleceğini, denetleneceğini ve sertifikasyon sürecine nasıl hazırlanacağını da öğrenir.

Program kapsamında bilgi varlıklarının belirlenmesi, tehdit ve zafiyetlerin değerlendirilmesi, risk analizi, risk treatment, Statement of Applicability hazırlanması, dokümantasyon, monitoring, auditing ve continual improvement gibi temel uygulamalar ele alınır.

Eğitimin önemli bir bölümü denetim becerilerine ayrılmıştır. Katılımcılar, audit planning, interview techniques, audit trail takibi, documented evidence incelemesi, nonconformity tespiti, corrective action süreçleri ve audit reporting gibi konuları uygulamalı olarak çalışır.

Program sonunda katılımcılar, ISO 27001:2022 uyumlu bir ISMS'in planlanması, uygulanması, iç denetiminin yürütülmesi ve resmi sertifikasyon denetimine hazırlanması konusunda kapsamlı bilgi kazanır.

Eğitim sonrasında katılımcılara bağımsız **APMG Certified ISO27001 Practitioner** sınavına girebilmeleri için voucher sağlanır. Başarılı adaylar elektronik APMG sertifikası ve dijital badge almaya hak kazanır.

Prerequisites

Bu eğitime katılım için herhangi bir resmi ön koşul bulunmamaktadır.

Certified ISO 27001 Practitioner Eğitimi

Süre: **4 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Who Should Attend

Program özellikle aşağıdaki profesyoneller için uygundur:

- Information Security professionals
- IT Security specialists
- Risk professionals
- Internal Auditors
- Compliance professionals
- Governance specialists
- ISO 27001 implementation ekipleri
- ISO 27001 audit süreçlerinde görev alan profesyoneller
- ISO 27001 uyumluluk programlarını yöneten Project Manager'lar

What You Will Learn

Eğitimin sonunda katılımcılar:

- ISO/IEC 27001:2022 gereksinimlerini ayrıntılı şekilde açıklayabilir
- Information asset'leri tanımlayabilir
- Asset'lerle ilişkili threat, vulnerability ve risk'leri belirleyebilir
- ISMS implementation programını planlayabilir
- Uygulama için gerekli zaman ve kaynakları değerlendirebilir
- Risk assessment ve risk management süreçlerini yürütebilir
- Statement of Applicability hazırlayabilir
- ISMS dokümantasyon ihtiyaçlarını belirleyebilir
- Monitoring ve auditing süreçlerini planlayabilir
- ISO 27001 Stage 1 ve Stage 2 certification audit süreçlerine hazırlanabilir
- Best-practice audit methodology yaklaşımını uygulayabilir
- Information security audit hazırlayabilir, yönetebilir ve raporlayabilir
- ISMS'in ISO 27001'e uygunluğunu değerlendirebilir
- Audit interview techniques kullanabilir
- Audit trail takip edebilir
- Documented evidence inceleyebilir
- Risk assessment ve business continuity süreçlerini denetleyebilir
- Nonconformity belirleyebilir
- Corrective action süreçlerini takip edebilir
- Surveillance audit ve certification maintenance gereksinimlerini açıklayabilir
- Governance, audit ve risk management arasındaki ilişkiyi değerlendirebilir
- Continual improvement faaliyetlerini destekleyebilir

Outline

Gün 1

Modül 1: Neden ISO 27001 Sertifikasyonu?

Bu bölüm ISO 27001 sertifikasyonunun kurumsal değerini ve bilgi güvenliği yönetimindeki rolünü ele

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

alır.

Konular:

- ISO 27001 sertifikasyonunun amacı
- Certification benefits
- Information security governance
- Kurumsal güven ve güvence
- Compliance ve risk yönetimine katkısı

Modül 2: Information Security Management System

Bu bölüm ISMS yapısının temel özelliklerini inceler.

Konular:

- ISMS nedir?
- ISMS'in amacı
- Yönetim sistemi yaklaşımı
- Information security lifecycle
- ISMS'in kurumsal süreçlerle entegrasyonu

Modül 3: Temel Tanımlar

ISO 27001 ve ISMS uygulamalarında kullanılan önemli terminoloji açıklanır.

Modül 4: ISO 27001

Bu bölüm ISO/IEC 27001:2022 standardının yapısını ve gereksinimlerini ele alır.

Konular:

- Standardın yapısı
- ISO 27001 requirements
- Management system clauses
- Bilgi güvenliği kontrollerinin rolü

Modül 5: ISMS'in Uygulanması

Konular:

- Implementation planning
- Project structure
- Roles and responsibilities
- Resources
- Timescales
- Implementation roadmap

Modül 6: Information Security Policy Tanımlama

Katılımcılar kurumsal Information Security Policy'nin kapsamını ve içeriğini değerlendirir.

Modül 7: ISMS Scope Tanımlama

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

Konular:

- ISMS boundary
- Organisational scope
- Technical scope
- Interfaces ve dependencies

Egzersiz 1: ISMS Scope

Katılımcılar örnek bir organizasyon için uygun ISMS scope tanımlar.

Modül 8: Information Assets

Konular:

- Information asset nedir?
- Asset categories
- Asset identification
- Asset ownership
- Asset inventory

Egzersiz 2: Assets

Katılımcılar belirli bir iş senaryosunda bilgi varlıklarını belirler.

Modül 9: Risk Assessment

Konular:

- Threat identification
- Vulnerability identification
- Risk identification
- Impact ve likelihood
- Risk assessment methodology

Egzersiz 3: Risk Assessment

Katılımcılar belirlenen asset'ler için risk değerlendirmesi gerçekleştirir.

Gün 2

Modül 10: Risk Measurement

Konular:

- Risk scoring
- Risk criteria
- Risk evaluation
- Risk acceptance
- Risk prioritisation

Modül 11: Control Objectives Belirleme

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

Katılımcılar tespit edilen risklere uygun control objective ve treatment seçeneklerini değerlendirir.

Egzersiz 4: Risk Treatment / Controls

Katılımcılar risklere karşı uygulanabilecek control ve treatment seçeneklerini belirler.

Modül 12: Information Security Overview

Bu bölüm bilgi güvenliği kontrollerinin genel yapısını ve ISMS içerisindeki rolünü ele alır.

Modül 13: Statement of Applicability Hazırlama

Konular:

- Statement of Applicability nedir?
- Control selection
- Control exclusion
- Gerekçelendirme
- SoA documentation

Egzersiz 5: Statement of Applicability

Katılımcılar örnek bir ISMS için SoA hazırlar.

Modül 14: Countermeasures

Konular:

- Countermeasure selection
- Practical controls
- Control effectiveness
- Uygulanabilir güvenlik önlemleri oluşturma

Modül 15: Governance'ın Rolü

Bu bölüm governance yapılarının ISO 27001 uygulamasındaki rolünü ele alır.

Konular:

- Governance principles
- Management oversight
- Accountability
- Risk ownership

Modül 16: Information Security ve Management Roles

Konular:

- Management responsibilities
- Information security roles
- Role separation
- Accountability
- Communication

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Egzersiz 6: Information Security and Management Roles

Katılımcılar örnek bir organizasyon için uygun görev ve sorumluluk dağılımı oluşturur.

Gün 2 Ödevi

Katılımcılar örnek bir ISMS üzerinde uygulama çalışması gerçekleştirir.

Gün 3

Modül 17: ISMS Denetimi

Bu bölüm ISO 27001'e uygun bir ISMS'in nasıl denetleneceğini açıklar.

Konular:

- Internal audit
- Audit objectives
- Audit criteria
- Audit evidence
- Audit scope

Modül 18: Formal Certification Audit'e Hazırlık

Katılımcılar resmi ISO 27001 sertifikasyon sürecine hazırlanmak için gerekli adımları inceler.

Egzersiz 7: Internal Audit

Örnek bir ISMS üzerinde iç denetim çalışması yapılır.

Modül 19: Stage 1 ve Stage 2 Certification Audits

Konular:

- Stage 1 audit
- Stage 2 audit
- Readiness review
- Certification decision
- Audit findings

Modül 20: Sertifikasyonun Sürdürülmesi

Konular:

- Surveillance audits
- Recertification
- Ongoing compliance
- Continual monitoring
- Certification maintenance challenges

Modül 21: Auditors

Bu bölüm denetçi rolünü ve gerekli yetkinlikleri ele alır.

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

Konular:

- Auditor responsibilities
- Independence
- Objectivity
- Competence
- Professional behaviour

Modül 22: Auditlerde Standardların Rolü

Katılımcılar standardların audit criteria ve evidence değerlendirmesindeki rolünü inceler.

Modül 23: Audit Terms and Definitions

Temel audit terminolojisi gözden geçirilir ve soru-cevap ile pekiştirilir.

Gün 4

Modül 24: Auditing Principles

Konular:

- Integrity
- Fair presentation
- Professional care
- Confidentiality
- Independence
- Evidence-based approach

Modül 25: Audit Programme Yönetimi

Konular:

- Audit programme planning
- Scope
- Objectives
- Resources
- Audit scheduling
- Auditor selection

Egzersiz 8: Internal Audit Preparation

Katılımcılar örnek bir iç denetim için plan ve hazırlık oluşturur.

Modül 26: Audit Gerçekleştirme

Konular:

- Opening meeting
- Interviews
- Document review
- Sampling
- Following audit trails

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Evidence collection
- Evaluating conformity

Modül 27: Audit Findings Raporlama

Konular:

- Audit findings
- Conformities
- Nonconformities
- Observations
- Audit summary
- Reporting

Egzersiz 9: Internal Audit

Katılımcılar uygulamalı bir internal audit senaryosu gerçekleştirir ve bulguları raporlar.

Modül 28: Audit Follow-Up

Konular:

- Corrective action
- Root cause
- Action tracking
- Closure of findings

Modül 29: Audit ve Risk Management İlişkisi

Bu bölüm audit sonuçlarının risk management süreçleriyle nasıl ilişkilendirildiğini açıklar.

Modül 30: Continual Improvement

Konular:

- Continual improvement
- Lessons learned
- ISMS performance
- Corrective actions
- Improvement opportunities

Modül 31: Awareness Training'in Değeri

Bu bölüm güvenlik farkındalığı ve kullanıcı eğitimlerinin ISMS başarısındaki rolünü ele alır.

Kurs Sonu Bilgi Değerlendirmesi

Eğitimin sonunda katılımcıların temel kavramları ve uygulama becerileri Knowledge Assessment ile değerlendirilir.

Certified ISO 27001 Practitioner Eğitimi

Süre: **4 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Sınav ve Sertifikasyon

Katılımcılar eğitim sonrasında bağımsız **APMG Certified ISO27001 Practitioner** sınavına girer.

Sınav, APMG Proctor platformu üzerinden online olarak gerçekleştirilir ve katılımcılara eğitim sonrasında sınav voucher'ı sağlanır.

Sınav Formatı

- **Format:** Objective Testing
- **Soru sayısı:** 4 ana soru
- **Her soru:** 20 puan
- **Toplam puan:** 80
- **Geçme puanı:** 40/80
- **Başarı oranı:** %50
- **Süre:** 2 saat
- **Kitap kullanımı:** Closed book
- **Sınav yöntemi:** Online / Remote Proctored

Başarılı adaylar APMG tarafından elektronik sertifika ve dijital badge almaya hak kazanır.