Bilgi Sistemleri Bağımsız Denetçiliği

Temel Denetim Bilgisi

- Denetim Kavramları ve İlkeleri
  - Denetimin Tanımı ve Amacı
  - Denetim Türleri (Finansal, Operasyonel, Uyum, BT)
  - Denetim Süreci Aşamaları
  - Bağımsız Denetimin Önemi
  - İç Kontrol Sistemleri
  - Güvence Denetimi Kavramı
  - Örnekleme Metodolojileri
  - Denetim Kanıtı Toplamış

Bilgi Sistemleri Temelleri

- Denetim Riskleri ve Kontroller
  - Denetim Riski Bileşenleri (Doğal, Kontrol, Tespit)
  - Risk Değerlendirme Teknikleri
  - Kontrol Türleri (Önleyici, Tespit Edici, Düzeltici)
  - İç Kontrol Çerçeveleri (COSO, CobiT)
  - Kontrol Amaçları ve Kontrol Faaliyetleri
  - BT Ortamında Kontrol Riskleri
  - Güvenlik Kontrollerinin Değerlendirilmesi
  - İş Süreçlerinde Kontroller
- İşletim Sistemleri Bilgisi
  - İşletim Sistemlerinin Temel Yapısı
  - Windows Sunucu İşletim Sistemleri
  - Linux/Unix İşletim Sistemleri
  - İşletim Sistemi Güvenlik Ayarları
  - Yama Yönetimi ve Güncelleme Süreçleri
  - Erişim Kontrol Mekanizmaları
  - Loglama ve İzleme Fonksiyonları
  - Sanallaştırma Ortamları
- Ağ ve Telekomünikasyon Temelleri
  - Ağ Topolojileri ve Mimarileri
  - TCP/IP Protokol Suiti
  - Yönlendiriciler ve Anahtarlar
  - Güvenlik Duvarları (Firewall)
  - VPN Teknolojileri
  - Kablosuz Ağ Güvenliği
  - Uzak Erişim ve Kontroller
  - Ağ İzleme ve Analiz Araçları

Denetim Standartları ve Metodolojileri

- Yazılım Geliştirme Yaşam Döngüsü (SDLC)
  - SDLC Modelleri (Şelale, Çevik, Spiral)
  - Gereksinim Analizi ve Tasarım
  - Yazılım Geliştirme ve Test Süreçleri
  - Devreye Alma ve Bakım
  - Proje Yönetimi İlkeleri
  - Kalite Güvencesi ve Kontroller
  - Yazılım Dokümantasyon Standartları
  - Kaynak Kod Yönetimi
- Uluslararası Denetim Standartları
  - ISACA IS Audit and Assurance Standards
  - IIA International Standards for the Professional Practice of Internal Auditing (ISPPIA)
  - COBIT Çerçevesi (Governance of Enterprise IT)
  - ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı
  - NIST Siber Güvenlik Çerçevesi
  - Uluslararası Muhasebe Standartları (IFRS) ile İlişkisi
  - Kamu Gözetimi Kurumu (KGK) Standartları
  - Etik Kurallar ve Davranış Standartları

BT Yönetişimi ve Risk Yönetimi

- BT Denetim Metodolojileri
  - Risk Tabanlı Denetim Yaklaşımı
  - Kontrol Odaklı Denetim Yaklaşımı
  - Süreç Denetimi ve Olgunluk
  - Performans Denetimi Teknikleri
  - Uygunluk Denetimi Yöntemleri
  - Güvenlik Açığı Tarama Metodolojileri
  - Penetrasyon Testi Yaklaşımları
  - Denetim Planlama ve Kapsam Belirleme
- BT Yönetişim Çerçeveleri
  - COBIT Yönetişim İlkeleri
  - ITIL Hizmet Yönetimi
  - ISO 38500 BT Yönetişimi Standardı
  - Kurumsal Yönetişim ve BT İlişkisi
  - BT Stratejisi ve Hedefleri
  - BT Yönetim Kurulu Sorumlulukları
  - BT Performans Ölçütleri
  - Değer Sunumu ve Optimizasyonu

Bilgi Güvenliği Denetimi

- BT Risk Yönetimi
  - BT Risk Tanımlama ve Sınıflandırma
  - Risk Değerlendirme Metodolojileri
  - Risk Azaltma ve Kabul Stratejileri
  - İş Etki Analizi (BIA)
  - Felaket Kurtarma Planlama (DRP)
  - İş Sürekliliği Yönetimi (BCM)
  - Kriz Yönetimi ve Müdahale
  - BT Risk Raporlaması
- Güvenlik Mimarisi ve Tasarımı
  - Güvenli Sistem Tasarım İlkeleri
  - Kurumsal Güvenlik Mimarisi
  - Ağ Güvenliği Bileşenleri
  - Uygulama Güvenliği Mimarisi
  - Yeni Güvenliği Mimarisi
  - Kimlik ve Erişim Yönetimi (AIM) Mimarisi
  - Bulut Güvenlik Mimarileri
  - Güvenlik Kontrollerinin Entegrasyonu

Veritabanı Sistemleri Denetimi

- Veritabanı Testleri ve Güvenlik Açığı Yönetimi
  - Sızma Testi Aşamaları ve Kapsamı
  - Güvenlik Açığı Sınıflandırması (CVSS)
  - Yama Yönetimi Süreçleri
  - Güvenlik Açığı Düzeltme Önceliklendirmesi
  - Penetrasyon Testi Raporlaması ve Takibi
- Veritabanı Mimarisi ve Bileşenleri
  - İlişkisel Veritabanı Yönetim Sistemleri (RDBMS)
  - NoSQL Veritabanları
  - Veritabanı Sunucu Yapılandırmaları
  - Veritabanı Yönetim Araçları
  - Veri Bütünlüğü ve Tutarlılığı
  - Yedekleme ve Geri Yükleme Mekanizmaları

Ağ ve Altyapı Denetimi

- Veritabanı Güvenliği ve Kontrolleri
  - Veritabanı Erişim Kontrolleri
  - Kullanıcı ve Rol Yönetimi
  - Şifreleme Mekanizmaları (Veri Saklama ve Tarihi)
  - Veritabanı Güvenlik Açıkları (SQL Injection, vb.)
  - Veritabanı Denetim Günlükleri ve İzleme
  - Veri Maskeleme ve Anonimleştirme
  - Veritabanı Güvenlik Duvarları (DBF)
  - Hassas Veri Keşfi
- Ağ Cihazları ve Konfigürasyonları
  - Yönlendirici ve Anahtar Güvenliği
  - Güvenlik Duvarı Kural Setleri
  - Saldırı Tespiti/Önleme Sistemleri (IDS/IPS)
  - VPN Türetilerine ve Kimlik Doğrulama
  - DNS Güvenliği
  - DHCP Güvenliği
  - SNMP Güvenliği
  - Ağ Segmentasyonu ve VLAN'lar

Uygulama Sistemleri Denetimi

- Sunucu ve Veri Merkezi Denetimi
  - Fiziksel Güvenlik Kontrolleri (Veri Merkezi)
  - Çevresel Kontroller (Soğutlık, Nem, Yangın)
  - Sunucu Güvenlik Konfigürasyonları
  - Sanallaştırma Platformları Denetimi
  - Depolama Alanı Ağı (SAN) Denetimi
  - Ağ Ekipmanları Bakım ve Yama Yönetimi
  - Güç Kaynağı ve Soğutma Sistemleri
  - Kablolama Standartları
- İş Uygulamaları Denetimi
  - Kurumsal Kaynak Planlama (ERP) Sistemleri
  - Müşteri İlişkileri Yönetimi (CRM) Sistemleri
  - Finansal Uygulama Kontrolleri
  - Tedarik Zinciri Yönetimi (SCM) Uygulamaları
  - Uygulama Girişi Kontrolleri
  - Yetkilendirme ve Rol Bazlı Erişim Kontrolleri
  - İş Süreci Otomasyonları Denetimi
  - Uygulama Entegrasyonları ve Arayüzler

Yeni Teknolojiler ve Denetim

- Web Uygulaması Güvenlik Denetimi
  - OWASP Top 10 Güvenlik Açıkları
  - Girdi Doğrulama ve Oturum Yönetimi
  - Çıktının Site Bellikleme (XSS) Kontrolleri
  - SQL Enjeksiyonu ve Kırmızı Enjeksiyonu
  - Güvenli Kodlama İlkeleri
  - API Güvenliği Denetimi
  - Web Uygulama Güvenlik Duvarları (WAF)
  - Güvenlik Testleri (Sızma, Kutu vb.)
- Bulut Bilişim Denetimi
  - Bulut Hizmet Modelleri (IaaS, PaaS, SaaS)
  - Bulut Dağıtım Modelleri (Özel, Genel, Hibrit)
  - Bulut Güvenliği Sorumluluk Paylaşım Modeli
  - Bulut Ortamında Veri Gizliliği ve Saklama
  - Bulut Güvenlik Standartları (CSA CCM)
  - Bulut Entegrasyonları ve API Güvenliği
  - Bulut Ortamında Denetim Logları
  - Bulut Tedarikçi Yönetimi
- Mobil ve IoT Denetimi
  - Mobil Uygulama Güvenlik Açıkları
  - Mobil Cihaz Yönetimi (MDM) Denetimi
  - Mobil Veri Koruma Mekanizmaları
  - IoT Cihaz Güvenliği Zafiyetleri
  - IoT Ağ Mimarisi Denetimi
  - IoT Veri Gizliliği ve Güvenliği
  - Gömülü Sistem Güvenliği
  - Kablosuz Protokol Güvenliği (Bluetooth, Zigbee)

Yasal Düzenlemeler ve Uyum Denetimi

- Büyük Veri ve Yapay Zeka Denetimi
  - Büyük Veri Mimarileri ve Bileşenleri
  - Veri Ambarı ve Veri Gölü Güvenliği
  - Veri Analizi ve Hükme Öğrenmesi Algoritmaları
  - Yapay Zeka Modellerinin Güvenilirliği
  - Algoritmik Yanlılık ve Şeffaflık
  - Veri Kaynağı Bütünlüğü ve Kalitesi
  - Büyük Veri Gizliliği ve Uyum Sorunları
  - Yapay Zeka Denetim Çerçeveleri
- Kişisel Verilerin Korunması Hukuku
  - KVKK (Kişisel Verilerin Korunması Kanunu)
  - GDPR (General Data Protection Regulation)
  - Veri Sorumlusu ve Veri İşleyen Sorumlulukları
  - Kişisel Veri İşleme Şartları
  - Veri İhlali Bildirim Yükümlülükleri
  - Veri Saklama ve İmha Politikaları
  - Aydınlatma Metinleri ve Açık Rıza
  - Sınır Ötesi Veri Aktarımı

Denetim Araçları ve Teknikleri

- Sektörel Düzenleyiciler ve Diğer Uyumlar
  - Bankacılık Sektörü Düzenlemeleri (BDDK)
  - Sermaye Piyasası Kurulu (SPK) Düzenlemeleri
  - Sağlık Verileri Düzenlemeleri (HIPAA vb.)
  - Ödeme Kartı Endüstrisi Veri Güvenliği Standardı (PCI DSS)
  - İş Denetim Yönetmelikleri ve Standartları
  - Çevre ve İş Sağlığı Güvenliği Uyumları
  - Elektronik Ticaret Kanunu (ETK)
- Otomatik Denetim Yazılımları
  - CAATs (Computer Assisted Audit Tools and Techniques)
  - Veri Analiz Yazılımları (ACL, IDEA, Excel)
  - Sürekli Denetim ve İzleme Araçları
  - Güvenlik Açığı Tarayıcıları (Nessus, Qualys)
  - Sızma Testi Araçları (Metasploit, Nmap)
  - Log Yönetimi ve SIEM Sistemleri (Splunk, ELK)
  - Proje Yönetimi ve İş Akışı Araçları
  - GRC (Yönetişim, Risk ve Uyum) Yazılımları

Profesyonel Gelişim ve Etik

- Manuel Denetim Teknikleri
  - Belge İncelemesi
  - Gözlem ve Yerinde İnceleme
  - Mülakat ve Anketler
  - Walkthrough (Süreç Takibi)
  - Kontrol Testleri (Test of Controls)
  - Esaslı Testler (Substantive Tests)
  - Veri Odaklı Testler
  - Denetim Çalışma Kağıtları Hazırlığı
- Sertifikasyonlar
  - CISA (Certified Information Systems Auditor)
  - CISM (Certified Information Security Manager)
  - CISSP (Certified Information Systems Security Professional)
  - CRISC (Certified in Risk and Information Systems Control)
  - ISO 27001 Baş Denetçi
  - CEH (Certified Ethical Hacker)
  - ITIL V4 Foundation

Denetim Raporlarının ve İletişim

- Etik ve Profesyonel Sorumluluklar
  - Bağımsızlık ve Tarafsızlık
  - Mesleki Dikkat ve Özen
  - Gizlilik ve Veri Korunması
  - Mesleki Yetkinlik ve Sürekli Gelişim
  - Çıkar Çatışmaları Yönetimi
  - Denetim Etiği İhlalleri
  - Yasal ve Mevzuata Uyum
  - Sosyal Sorumluluk ve Sapmlık
- Denetim Raporu Yazımı
  - Rapor Yapısı ve İçeriği
  - Bulguların Net ve Anlaşılır Bizde Edilmesi
  - Kanıtlara Dayalı Sonuçlar
  - Önerel Geliştirme ve Prioritizasyon
  - Risk Derecelendirme Mekanizmaları
  - Yönetim Cevaplarının Değerlendirilmesi
  - Özel ve Yönetici Özeti
  - Teknik Terimlerin Açıklanması
- Paydaş İletişimi
  - Yönetimle Etkili İletişim
  - Denetlenen Birimle İlişkiler
  - Denetim Komitesi veya Kurul İletişimi
  - Sözlü Sunum Becerileri
  - Müzakere ve İkna Teknikleri
  - Geri Bildirim ve Takip Süreçleri
  - Çatışma Yönetimi
  - Denetim Sonuçlarının Yaygınlaştırılması