BLM5102 Bilgisayar Sistemleri ve Ağ Güvenliği

Prof. Dr. Hasan Hüseyin BALIK

(3. Hafta)

İçerik

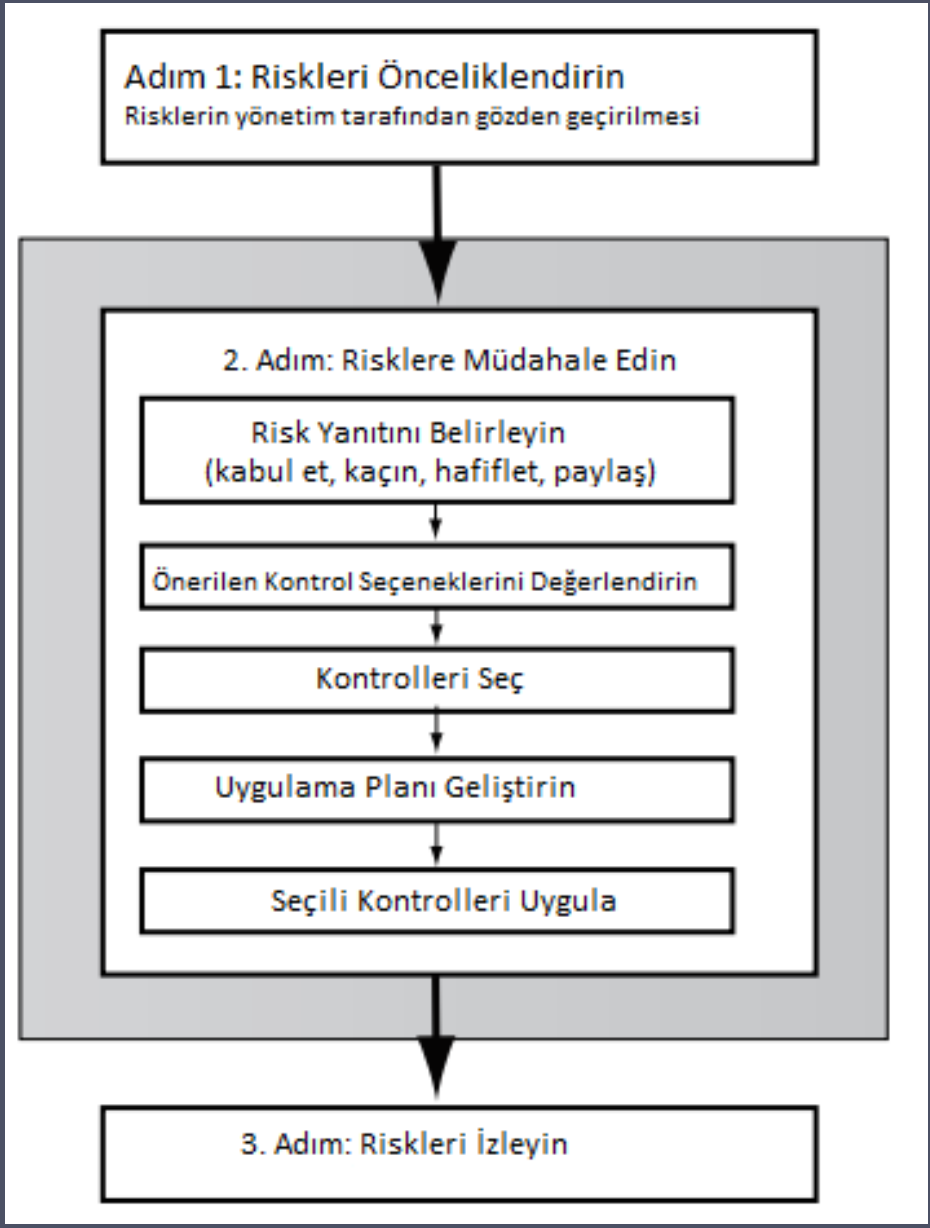
- 2.Yönetim Sorunları
  - 2.1. BT Güvenlik Yönetimi ve Risk Değerlendirmesi
  - 2.2.BT Güvenlik Kontrolleri, Planları ve Prosedürleri
  - 2.3.Fiziksel ve Altyapı Güvenliği
  - 2.4. İnsan Kaynakları Güvenliği
  - 2.5. Güvenlik Denetimi
  - 2.6. Bilişim Güvenliğinde Yasal ve Etik Hususlar

2.2.BT Güvenlik Kontrolleri, Planları ve prosedürler

2.2.İçerik

- BT Güvenlik Yönetimi Uygulaması
- Güvenlik Kontrolleri veya Önlemler
- BT Güvenlik Planı
- Kontrollerin Uygulanması
- Riskleri İzleme
- Vaka Çalışması: Gümüş Yıldız Madenleri

BT Güvenlik Yönetimi Kontrolleri ve Uygulaması



Güvenlik Kontrolü

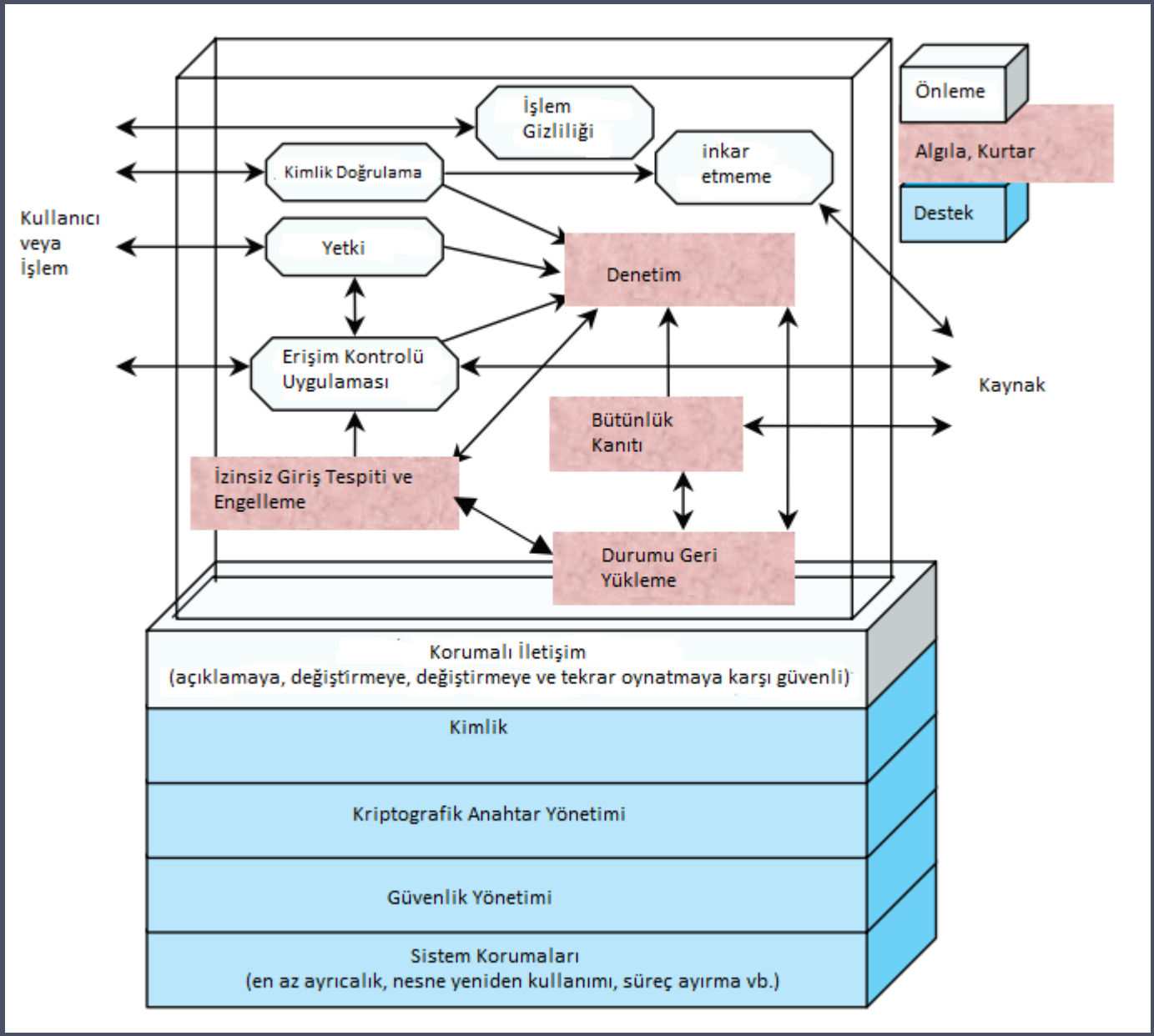
Kontrol şu şekilde tanımlanır:

"Bir güvenlik ihlalini ortadan kaldırarak veya önleyerek, neden olabileceği zararı en aza indirerek veya düzeltici eylemi etkinleştirmek için onu keşfederek ve raporlayarak riski azaltan bir eylem, cihaz, prosedür veya başka bir önlemdir"

Kontrol Sınıflandırmaları

- Yönetim kontrolleri
  - Kayıp riskini azaltmak ve kuruluşun misyonunu korumak için operasyonel ve teknik kontrollerin seçimini etkileyen güvenlik politikalarına, planlamaya, yönergelere ve standartlara odaklanmaktır
  - Bu kontroller, yönetimin ele alması gereken hususları ifade eder.
- Operasyonel kontroller
  - Güvenlik politikaları ve standartlarının doğru uygulanmasını ve kullanımını ele almak, güvenlik operasyonlarında tutarlılığı sağlamak ve tespit edilen operasyonel eksiklikleri düzeltmektir.
  - Bu kontroller, sistemlerden çok insanlar tarafından uygulanan mekanizmalar ve prosedürlerle ilgilidir.
  - Bir sistemin veya sistem grubunun güvenliğini artırmak için kullanılırlar.
- Teknik kontroller
  - Sistemlerde donanım ve yazılım güvenlik özelliklerinin doğru kullanımını içerir.
  - Bunlar, kritik ve hassas verileri, bilgileri ve BT sistem işlevlerini güvenceye almak için birlikte çalışan basitten karmaşık önlemlere kadar uzanır.

Teknik Güvenlik Kontrolleri



Kontrol Sınıfları

Kontrol sınıflarının her biri aşağıdakileri içerebilir:

- Destekleyici kontroller
  - Diğer birçok kontrolle ilişkili olan ve bunlar tarafından kullanılan yaygın, genel, temel teknik BT güvenlik yetenekleridir.
- Önleyici kontroller
  - Güvenlik politikalarını ihlal etme veya bir güvenlik açığından yararlanma girişimlerini engelleyerek güvenlik ihlallerinin oluşmasını önlemeye odaklanır
- Algılama ve kurtarma kontrolleri
  - İhlaller veya güvenlik politikaları ihlal girişimleri veya bir güvenlik açığının tespit edilen istismarı konusunda uyarıda bulunarak ve sonuçta ortaya çıkan kayıp BT kaynaklarını geri yüklemek için araçlar sağlayarak bir güvenlik ihlaline verilen yanıta odaklanır.

NIST SP800-53 Güvenlik Kontrolleri

Sınıfı	Kontrol Ailesi
Yönetim	Planlama
Yönetim	Program Yönetimi
Yönetim	Risk değerlendirmesi
Yönetim	Güvenlik Değerlendirmesi ve Yetkilendirme
Yönetim	Sistem ve Hizmet Alımı.
Operasyonel	Farkındalık ve Eğitim
Operasyonel	Konfigürasyon yönetimi
Operasyonel	Acil Durum Planlaması
Operasyonel	Olay Müdahalesi
Operasyonel	Bakım onarım
Operasyonel	Medya Koruması
Operasyonel	Personel Güvenliği
Operasyonel	Fiziksel ve Çevresel Koruma
Operasyonel	Sistem ve Bilgi Bütünlüğü
Teknik	Giriş kontrolu
Teknik	Denetim ve Hesap Verebilirlik
Teknik	Tanımlama ve Kimlik Doğrulama
Teknik	Sistem ve İletişim Koruması

ISO/IEC 27002 Güvenlik Kontrolleri 1/2

Kontrol Kategorisi	Amaç
Güvenlik politikaları	İş gereksinimlerine ve ilgili yasa ve yönetmeliklere uygun olarak bilgi güvenliği için yönetim yönlendirmesi ve desteği sağlamak.
Bilgi Güvenliği Organizasyonu	Kuruluş içinde bilgi güvenliğinin uygulanmasını ve işleyişini başlatmak ve kontrol etmek için bir yönetim çerçevesi oluşturmak; tele-çalışma ve mobil cihazların kullanımının güvenliğini sağlamak.
İnsan Kaynakları Güvenliği	Çalışanların ve yüklenicilerin sorumluluklarını anlamalarını ve atandıkları rollere uygun olmalarını sağlamak; çalışanların ve yüklenicilerin bilgi güvenliği sorumluluklarını bilmelerini ve yerine getirmelerini sağlamak; İstihdamı değiştirme veya sonlandırma sürecinin bir parçası olarak kuruluşun çıkarlarını korumak.
Varlık Yönetimi	Kurumsal varlıkları belirlemek ve uygun koruma sorumluluklarını tanımlamak; bilginin kuruluş için önemine göre uygun düzeyde koruma almasını sağlamak; Medyada saklanan bilgilerin yetkisiz ifşasını, değiştirilmesini, kaldırılmasını veya imha edilmesini önlemek.
Giriş kontrolu	Bilgi ve bilgi işleme tesislerine erişimi sınırlamak; yetkili kullanıcı erişimini sağlamak ve sistem ve hizmetlere yetkisiz erişimi engellemek; kullanıcıları kimlik doğrulama bilgilerini korumaktan sorumlu kılmak; sistemlere ve uygulamalara yetkisiz erişimi önlemek.
Kriptografi/Şifreleme	Bilgilerin gizliliğini, gerçekliğini ve/veya bütünlüğünü korumak için kriptografinin doğru ve etkin kullanımını sağlamak
Fiziksel ve Çevresel Güvenlik	Kuruluşun bilgi ve bilgi işleme tesislerine yetkisiz fiziksel erişimi, hasarı ve müdahaleyi önlemek; varlıkların kaybolmasını, hasar görmesini, çalınmasını veya tehlikeye atılmasını ve kuruluşun operasyonlarının kesintiye uğramasını önlemek.

ISO/IEC 27002 Güvenlik Kontrolleri 2/2

Kontrol Kategorisi	Amaç
Operasyon Güvenliği	Bilgi işleme tesislerinin doğru ve güvenli çalışmasını sağlamak; bilgi ve bilgi işleme tesislerinin kötü amaçlı yazılımlara karşı korunmasını sağlamak; veri kaybına karşı korumak; olayları kaydetmek ve kanıt oluşturmak; operasyonel sistemlerin bütünlüğünü sağlamak; teknik güvenlik açıklarının kötüye kullanılmasını önlemek; Denetim faaliyetlerinin operasyonel sistemler üzerindeki etkisini en aza indirmek.
İletişim Güvenliği	Ağlardaki ve destekleyici bilgi işleme tesislerindeki bilgilerin korunmasını sağlamak; bir kuruluş içinde ve harici bir varlıkla aktarılan bilgilerin güvenliğini sağlamak.
Sistem Edinimi, Geliştirme ve Bakım	Kamusal ağlar üzerinden hizmet sağlayan bilgi sistemlerine ilişkin gereksinimler de dahil olmak üzere, bilgi güvenliğinin tüm yaşam döngüsü boyunca bilgi sistemlerinin ayrılmaz bir parçası olmasını sağlamak; bilgi güvenliğinin bilgi sistemlerinin geliştirme yaşam döngüsü içinde tasarlanmasını ve uygulanmasını sağlamak; test için kullanılan verilerin korunmasını sağlamak.
Tedarikçi İlişkileri	Kuruluşun tedarikçiler tarafından erişilebilen varlıklarının korunmasını sağlamak; Tedarikçi anlaşmaları doğrultusunda üzerinde anlaşılmış bir bilgi güvenliği ve hizmet sunumu düzeyini sürdürmek.
Bilgi Güvenliği Olay Yönetimi	Güvenlik olayları ve zayıflıkları hakkında iletişim de dahil olmak üzere bilgi güvenliği olaylarının yönetimine tutarlı ve etkili bir yaklaşım sağlamak.
Bilgi Güvenliği Sürekliliği	BT sürekliliğini organizasyonun iş sürekliliği yönetim sistemlerine yerleştirmek; bilgi işleme tesislerinin kullanılabilirliğini sağlamak.
Uyma	Bilgi güvenliği ve herhangi bir güvenlik gereksinimi ile ilgili yasal, yasal, düzenleyici veya sözleşmeye dayalı yükümlülüklerin ihlallerini önlemek; bilgi güvenliğinin kurumsal politika ve prosedürlere uygun olarak uygulanmasını ve işletilmesini sağlamak.

Detaylı NIST SP800-53 Güvenlik Kontrolleri 1/3

Giriş kontrolu	Erişim Kontrolü Politikası ve Prosedürleri, Hesap Yönetimi, Erişim Uygulaması, Bilgi Akışı Uygulaması, Görevlerin Ayrılması, En Az Ayrıcalık, Başarısız Giriş Denemeleri, Sistem Kullanım Bildirimi, Önceki Oturum Açma (Erişim) Bildirimi, Eşzamanlı Oturum Kontrolü, Oturum Kilitleme, Oturum Sonlandırma, İzin Verilen Eylemler Tanımlama veya Kimlik Doğrulama Olmadan, Güvenlik Nitelikleri, Uzaktan Erişim, Kablosuz Erişim, Mobil Cihazlar için Erişim Kontrolü, Harici Bilgi Sistemlerinin Kullanımı, Bilgi Paylaşımı, Herkese Açık İçerik, Veri Madenciliği Koruması, Erişim Kontrol Kararları, Referans Monitör
Farkındalık ve Eğitim	Güvenlik Bilinci ve Eğitimi Politika ve Prosedürleri, Güvenlik Bilinci, Eğitim, Rol Tabanlı Güvenlik Eğitimi, Güvenlik Eğitimi Kayıtları
Denetim ve Hesap Verebilirlik	Denetim ve Hesap Verebilirlik Politikası ve Prosedürleri, Denetim Olayları, Denetim Kayıtlarının İçeriği, Denetim Depolama Kapasitesi, Denetim İşleme Hatalarına Müdahale, Denetim İnceleme, Analiz ve Raporlama, Denetim Azaltma ve Rapor Oluşturma, Zaman Damgaları, Denetim Bilgilerinin Korunması, İnkar Etmeme, Denetim Kayıt Tutma, Denetim Oluşturma, Bilgi Açıklamasının İzlenmesi, Oturum Denetimi, Alternatif Denetim Yeteneği, Kuruluşlar Arası Denetim
Güvenlik Değerlendirmesi ve Yetkilendirme	Güvenlik Değerlendirmesi ve Yetkilendirme Politikaları ve Prosedürleri, Güvenlik Değerlendirmeleri, Sistem Arabağlantıları, Eylem Planı ve Kilometre Taşları, Güvenlik Akreditasyonu, Sürekli İzleme, Sızma Testi, Dahili Sistem Bağlantıları
Konfigürasyon yönetimi	Konfigürasyon Yönetimi İlkesi ve Prosedürleri, Temel Konfigürasyon, Konfigürasyon Değişikliği Kontrolü, Güvenlik Etki Analizi, Değişiklik için Erişim Kısıtlamaları, Konfigürasyon Ayarları, En Az İşlevsellik, Bilgi Sistemi Bileşen Envanteri, Konfigürasyon Yönetim Planı, Yazılım Kullanım Kısıtlamaları, Kullanıcı Tarafından Yüklenen Yazılım
Acil Durum Planlaması	Acil Durum Planlama Politikası ve Prosedürleri, Acil Durum Planı, Acil Durum Eğitimi, Acil Durum Planı Testi, Alternatif Depolama Sahası, Alternatif İşleme Sahası, Telekomünikasyon Hizmetleri, Bilgi Sistemi Yedekleme, Bilgi Sistemi Kurtarma ve Yeniden Oluşturma, Alternatif İletişim Protokolleri, Güvenli Mod, Alternatif Güvenlik Mekanizmaları

Detaylı NIST SP800-53 Güvenlik Kontrolleri 2/3

Tanımlama ve Kimlik Doğrulama	Tanımlama ve Doğrulama Politikası ve Prosedürleri, Tanımlama ve Doğrulama (Kurumsal Kullanıcılar), Cihaz Tanımlama ve Doğrulama, Tanımlayıcı Yönetimi, Doğrulayıcı Yönetimi, Doğrulayıcı Geri Bildirimi, Kriptografik Modül Doğrulama, Tanımlama ve Doğrulama (Kurumsal Olmayan Kullanıcılar), Hizmet Tanımlama ve Doğrulama, Uyarlamalı Tanımlama ve Doğrulama, Yeniden kimlik doğrulama
Olay Müdahalesi	Olay Müdahale Politikası ve Prosedürleri, Olay Müdahale Eğitimi, Olay Müdahale Testi, Olay Yönetimi, Olay İzleme, Olay Raporlama, Olay Müdahale Yardımı, Olay Müdahale Planı, Bilgi Dökülmesine Müdahale, Entegre Bilgi Güvenliği Analiz Ekibi
Bakım onarım	Sistem Bakım Politikası ve Prosedürleri, Kontrollü Bakım, Bakım Araçları, Lokal Olmayan Bakım, Bakım Personeli, Zamanında Bakım
Medya Koruması	Medya Koruma Politikası ve Prosedürleri, Medya Erişimi, Medya İşaretleme, Medya Depolama, Medya Taşıma, Medya Temizliği, Medya Kullanımı, Medya indirme (download)
Fiziksel ve Çevresel Koruma	Fiziksel ve Çevresel Koruma Politikası ve Prosedürleri, Fiziksel Erişim Yetkileri, Fiziksel Erişim Kontrolü, İletim Ortamı için Erişim Kontrolü, Çıkış Cihazları için Erişim Kontrolü, Fiziksel Erişimin İzlenmesi, Ziyaretçi Erişim Kayıtları, Güç Ekipmanları ve Kablolama, Acil Durum Kapatma, Acil Güç, Acil Aydınlatma, Yangından Korunma, Sıcaklık ve Nem Kontrolleri, Su Hasarlarından Korunma, Teslim ve Kaldırma, Alternatif Çalışma Sahası, Bilgi Sistemi Bileşenlerinin Yerleşimi, Bilgi Sızıntısı, Varlık İzleme ve Takibi
Planlama	Güvenlik Planlama Politikası ve Prosedürleri, Sistem Güvenlik Planı, Davranış Kuralları, Güvenlik İşlemleri Kavramı, Bilgi Güvenliği Mimarisi, Merkezi Yönetim
Personel Güvenliği	Personel Güvenliği Politikası ve Prosedürleri, Pozisyon Riski Belirleme, Personel Taraması, Personel Fesih, Personel Transferi, Erişim Sözleşmeleri, Üçüncü Kişi Personel Güvenliği, Personel Yaptırımları
Risk değerlendirmesi	Risk Değerlendirme Politikası ve Prosedürleri, Güvenlik Sınıflandırması, Risk Değerlendirmesi, Güvenlik Açığı Taraması, Teknik Gözetim Önlemleri Anketi

Detaylı NIST SP800-53 Güvenlik Kontrolleri 3/3

Sistem ve Hizmet Alımı	Sistem ve Hizmet Edinme Politikası ve Prosedürleri, Kaynakların Tahsisi, Sistem Geliştirme Yaşam Döngüsü, Edinme Süreci, Bilgi Sistemi Dokümantasyonu, Güvenlik Mühendisliği İlkeleri, Harici Bilgi Sistemi Hizmetleri, Geliştirici Yapılandırma Yönetimi, Geliştirici Güvenlik Testi ve Değerlendirmesi, Tedarik Zinciri Koruması, Güvenilirlik, Kritiklik Analiz, Geliştirme Süreci, Standartlar ve Araçlar, Geliştirici Tarafından Sağlanan Eğitim, Geliştirici Güvenlik Mimarisi ve Tasarımı, Kurcalamaya Karşı Direnç ve Algılama, Bileşen Orijinalliği, Kritik Bileşenlerin Özelleştirilmiş Geliştirmesi, Geliştirici Taraması, Desteklenmeyen Sistem Bileşenleri
Sistem ve İletişim Koruması	Sistem ve İletişim Koruma Politikası ve Prosedürleri, Uygulama Bölümleme, Güvenlik İşlevi Yalıtımı, Paylaşılan Kaynaklarda Bilgi, Hizmet Reddi Koruması, Kaynak Kullanılabilirliği, Sınır Koruması, İletim Gizliliği ve Bütünlüğü, Ağ Bağlantısının Kesilmesi, Güvenilir Yol, Kriptografik Anahtar Oluşturma ve Yönetimi, Kriptografik Koruma , İşbirliğine Dayalı Bilgi İşlem Cihazları, Güvenlik Niteliklerinin İletimi, Açık Anahtar Altyapı Sertifikaları, Mobil Kod, İnternet Üzerinden Ses Protokolü, Güvenli Ad/Adres Çözümleme Hizmeti (Yetkili Kaynak, Özyinelemeli veya Önbelleğe Alma Çözümleyicisi, Mimari ve Sağlama), Oturum Orijinalliği, Bilinen Durumda Başarısız , İnce Düğümler, Honeypot'lar, Platformdan Bağımsız, Duran Bilginin Korunması, Heterojenlik, Gizleme ve Yanlış Yönlendirme, Gizli Kanal Analizi, Bilgi Sistemi Bölümleme, Değiştirilemeyen Yürütülebilir Programlar, Honeyclient, Dağıtılmış İşleme ve Depolama, Bant Dışı Kanallar, Operasyon Güvenliği ty, Proses İzolasyonu, Kablosuz Bağlantı Koruması, Port ve I/O Cihaz Erişimi, Sensör Yeteneği ve Verileri, Kullanım Kısıtlamaları, Patlama Odaları (dinamik koşturma ortamları)
Sistem ve Bilgi Bütünlüğü	Sistem ve Bilgi Bütünlüğü Politikası ve Prosedürleri, Kusur Giderme, Kötü Amaçlı Kod Koruması, Bilgi Sistemi İzleme, Güvenlik Uyarıları Önerileri ve Yönergeleri, Güvenlik İşlevselliği Doğrulaması, Yazılım Ürün Yazılımı ve Bilgi Bütünlüğü, Spam Koruması, Bilgi Girişi Doğrulaması, Hata İşleme, Bilgi İşleme ve Saklama, Öngörülebilir Arıza Önleme, Kalıcılık, Bilgi Çıkışı Filtreleme, Bellek Koruma, Arızaya Karşı Güvenli Prosedürler
Program yönetimi	Bilgi Güvenliği Program Planı, Kıdemli Bilgi Güvenliği Görevlisi, Bilgi Güvenliği Kaynakları, Eylem Planı ve Kilometre Taşları Süreci, Bilgi Sistemi Envanteri, Bilgi Güvenliği Performans Ölçütleri, Kurumsal Mimari, Kritik Altyapı Planı, Risk Yönetim Stratejisi, Güvenlik Yetkilendirme Süreci, Görev/İş Süreci Tanımı, İçeriden Tehdit Programı, Bilgi Güvenliği İş Gücü, Test Eğitimi ve İzleme, Güvenlik Grupları ve Dernekleri ile İletişim, Tehdit Farkındalık Programı

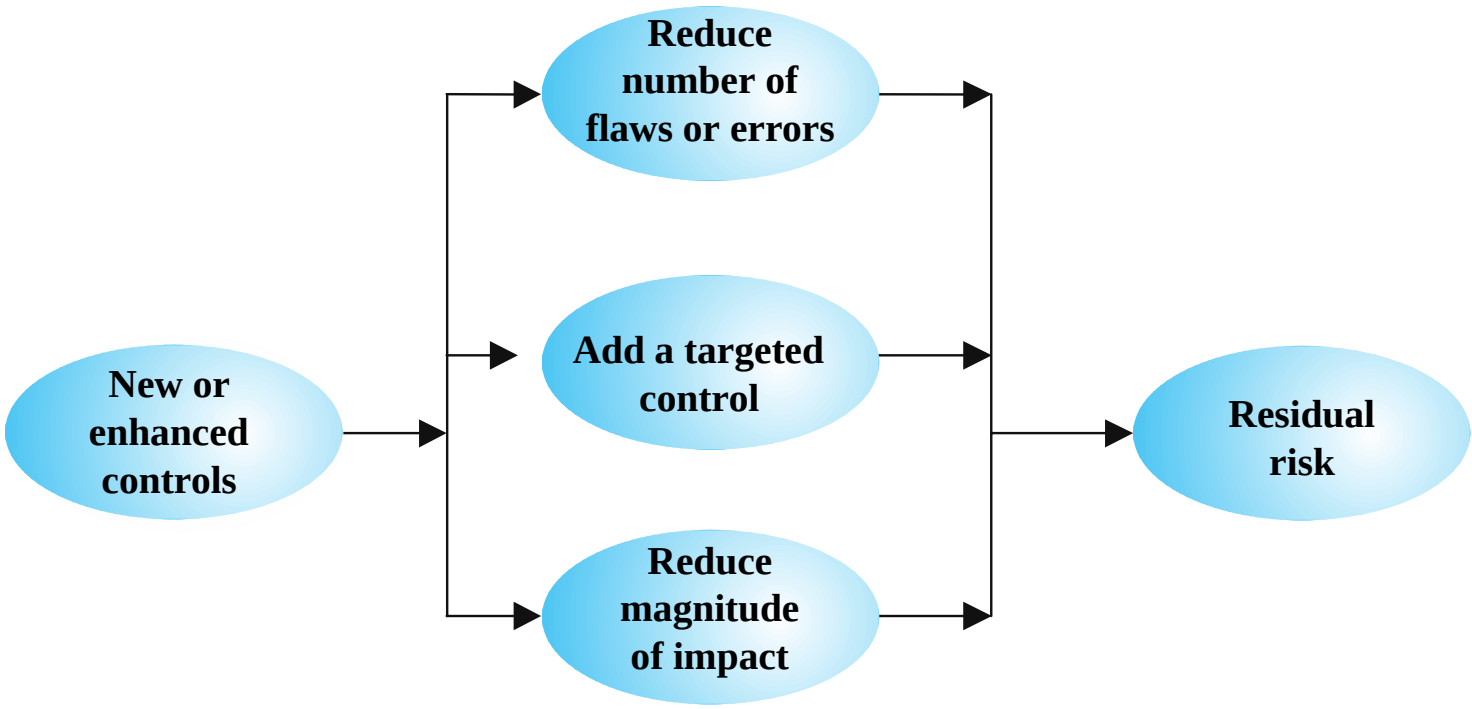


Figure 15.3 Residual Risk

Maliyet Fayda Analizi

Mevcut kaynaklar göz önüne alındığında, kuruluşa en büyük faydayı sağlayan kontrolleri belirlemek için yönetim tarafından yürütülmelidir.

Niteliksel veya niceliksel olabilir

Riskteki azalmayla gerekçelendirilen maliyeti göstermelidir

Bir kontrolün uygulanıp uygulanmamasının etkisi ile maliyet tahminini karşılaştırmalıdır

Yönetim, kontrol seçeneklerinden birini seçer

Riski çok fazla veya yeterince azaltıp azaltmadığını, çok maliyetli veya uygun olup olmadığını değerlendirir.

Temelde bir iş kararıdır

BT Güvenlik Planı

- ……ların ayrıntılarını sağlar:
  - Ne yapılacak
  - Hangi kaynaklara ihtiyaç var?
  - Sorumlu kim
- Amaç, risk profilinde tespit edilen eksiklikleri iyileştirmek için gereken eylemleri detaylandırmaktır.

İçermeli

- Riskler, önerilen kontroller, eylem önceliği
- Seçilen kontroller, gerekli kaynaklar
- Sorumlu personel, uygulama tarihleri
- Bakım gereksinimleri

Uygulama planı

Risk (Varlık/Tehdit)	İnternet yönlendiricisine hacker saldırısı
Risk Seviyesi	Yüksek
Önerilen Kontroller	• Harici telnet erişimini devre dışı bırak • Ayrıcalıklı komut kullanımının ayrıntılı denetimini kullan • Güçlü yönetici şifreleri için politika belirle • Yönlendirici yapılandırma dosyası için yedekleme stratejisini belirle • Yönlendirici yapılandırması için değişiklik kontrol politikasını ayarla
Öncelik	Yüksek
Seçili Kontroller	• Önerilen tüm kontrolleri uygula • Etkilenen personel için eğitim ile ilgili prosedürleri güncelle
Gerekli kaynaklar	• Yönlendirici yapılandırmasını değiştirmek ve doğrulamak, politika yazmak için 3 gün BT ağ yöneticisi zamanı • Ağ yönetim personeli için 1 günlük eğitim
Sorumlu kişiler	Ali Çokbilen, Baş Ağ Sistem Yöneticisi, Kurumsal BT Destek Ekibi
Başlangıç-Bitiş Tarihi	3 Kasım 2022 – 6 Kasım 2022
Diğer Öneriler	Yapılandırma ve politika kullanımının periyodik olarak test edilmesi ve gözden geçirilmesi gerekir

Güvenlik Planı Uygulaması

BT güvenlik planı belgeleri:

- Seçilen her kontrol için yapılması gerekenler
- Sorumlu personel
- Kaynaklar ve zaman çerçevesi

Tanımlanan personel:

- Yeni veya gelişmiş denetimler uygulayın
- Sistem yapılandırma değişikliklerine, yükseltmelere veya yeni sistem kurulumuna ihtiyaç duyabilir
- Yeni veya genişletilmiş prosedürlerin geliştirilmesini de içerebilir
- Yönetim tarafından teşvik edilmeli ve izlenmeli

Uygulama tamamlandığında yönetim, sistemi operasyonel kullanım için yetkilendirir.

Uygulama
Takip et

- Güvenlik yönetimi döngüsel bir süreçtir
  - BT sistemlerindeki ve risk ortamındaki değişikliklere yanıt vermek için sürekli olarak tekrarlanır
- Uygulanan kontrolleri izleme ihtiyacı
- Güvenlik etkileri için değişiklikleri değerlendirin
  - Aksi takdirde güvenlik ihlali olasılığını artırır

Bir dizi yönü içerir

- Güvenlik kontrollerinin bakımı
- Güvenlik uyumluluğu kontrolü
- Değişiklik ve konfigürasyon yönetimi
- Olay yönetimi

Bakım Onarım

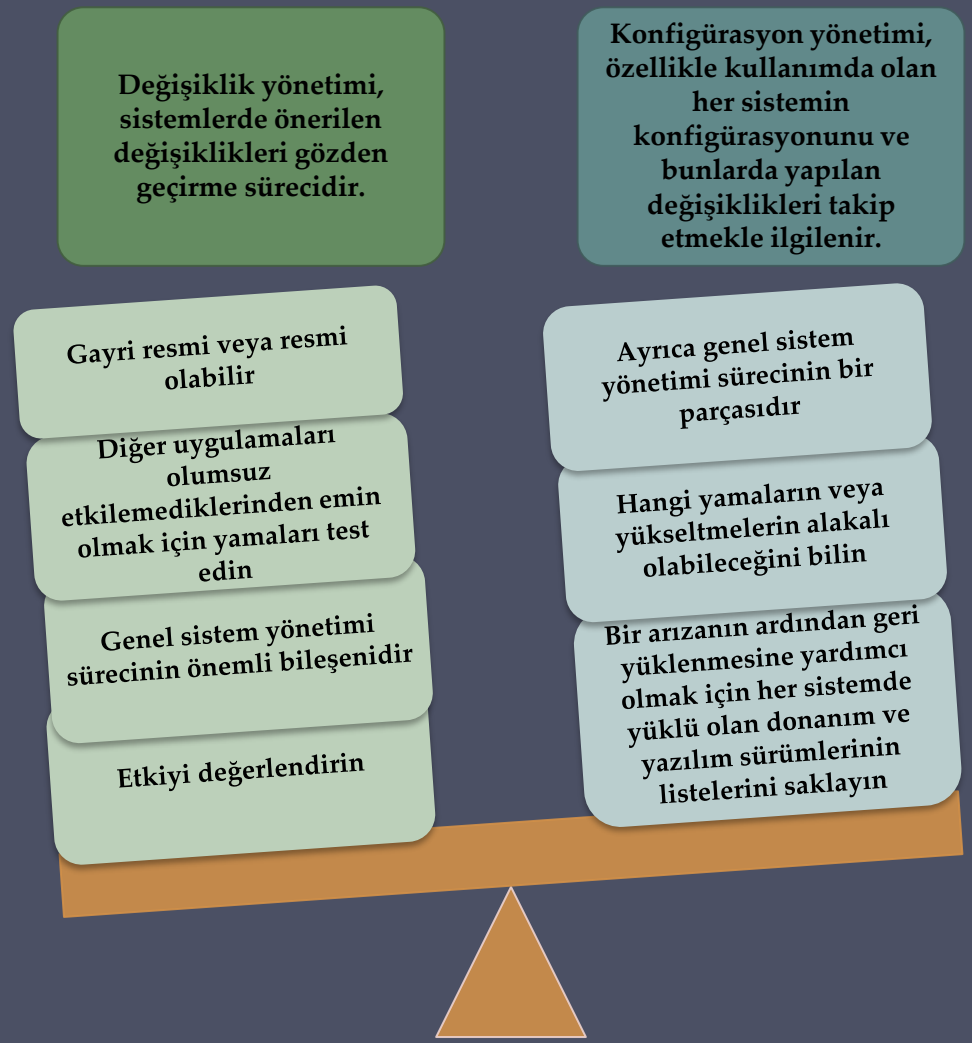
- Sürekli doğru işleyişi ve uygunluğu sağlamak için uygulanan kontrollerin sürekli bakımına ve izlenmesine ihtiyaç var
- Amaç, kontrollerin amaçlandığı gibi çalışmasını sağlamaktır

Görevler

Güvenlik Uyumluluğu

- Güvenlik süreçlerini gözden geçirmek için denetim sürecidie
- Amaç, güvenlik planına uygunluğu doğrulamaktır
- Dahili veya harici personel kullanılır
- Genellikle aşağıdakileri doğrulayan kontrol listelerinin kullanımına dayanır:
  - Uygun politikalar ve planlar oluşturuldu
  - Uygun kontroller seçildi
  - Bakımlar yapıldı ve doğru kullanıldı
- Genellikle daha geniş kapsamlı genel denetimin bir parçasıdır.

Değişiklik ve Konfigürasyon Yönetimi



Vaka Çalışması: Gümüş Yıldız Madenleri

- Risk değerlendirmesi göz önüne alındığında, bir sonraki aşama olası kontrolleri belirlemektir.
- Değerlendirmeye göre, birçok kategorinin kullanımda olmadığı açıktır.
- Sistemlerin yamalanmaması veya yükseltilmemesiyle ilgili genel sorun
- Acil durum planlarına ihtiyaç var
- SCADA: izinsiz giriş tespit sistemi ekleyin
- Bilgi bütünlüğü: depolamayı daha iyi merkezileştirin
- E-posta: yedekleme sistemi sağlayın

Gümüş Yıldız Madenleri: Uygulama planı

Risk (Asset/Threat)	Risk Seviyesi	Önerilen Kontroller	Öncelik	Seçilen Kontroller
Tüm riskler (genel olarak uygulanabilir)		1. Sunucular için yapılandırma ve periyodik bakım politikası 2. Kötü amaçlı kod (SPAM, casus yazılım) önleme 3. Sunucularda denetim izleme, analiz, azaltma ve raporlama 4. Acil durum planlaması ve olay müdahale politikaları ve prosedürleri 5. Sistem yedekleme ve kurtarma prosedürleri	1	1. 2. 3. 4. 5.
Reliability and integrity of SCADA nodes and network	Yüksek	1. Saldırı tespit ve müdahale sistemi	2	1.
Depolanan dosya ve veritabanı bilgilerinin bütünlüğü	Ekstrim	1. Kritik belgelerin denetimi 2. Belge oluşturma ve saklama politikası 3. Kullanıcı güvenliği eğitimi ve eğitimi	3	1. 2. 3.
Mali, Tedarik ve Bakım/Üretim Sistemlerinin Kullanılabilirliği ve Bütünlüğü	Yüksek	-	-	(Genel Kontol)
Posta hizmetlerinin kullanılabilirliği, bütünlüğü ve gizliliği	Yüksek	1. Acil durum planlaması—yedek e-posta hizmeti	4	1.