Siber Güvenlik

Topical Requirement

Kullanıcı Rehberi

The Institute of
Internal Auditors

İçindekiler

Konu Bazlı Gerekliliklere Genel Bakış

Konu Bazlı Gereklilikler, Uluslararası İç Denetim Standartları (Global Internal Audit Standards™) ve Küresel Rehberler ile birlikte Uluslararası Mesleki Uygulama Çerçevesi (International Professional Practices Framework®) nin temel bir bileşenidir. İç Denetçiler Enstitüsü, Konu Bazlı Gerekliliklerin, gerekli uygulamaların temel yetkiyi sağlayan Uluslararası İç Denetim Standartları ile birlikte kullanılmasını şart koşmaktadır. Daha ayrıntılı bilgi kaynağı olarak bu rehber boyunca Standartlara atıfta bulunulmaktadır.

Konu Bazlı Gereklilikler, meslek içinde kalite ve tutarlılığı teşvik etmek için iç denetçilerin yaygın risk alanlarını nasıl ele aldıklarını resmileştirir. Konu Bazlı Gereklilikler bir temel oluşturur ve bir Konu Bazlı Gerekliliğin konusuyla ilgili güvence hizmetlerinin yerine getirilmesi için ilgili kriterleri sağlar (Standart 13.4 Değerlendirme Kıstasları). Konu Bazlı Gerekliliklere uyum güvence hizmetleri için zorunludur ve danışmanlık hizmetleri sırasında değerlendirme için tavsiye edilir. Konu Bazlı Gereklilikler, güvence görevlerini yerine getirirken dikkate alınması gereken tüm potansiyel hususları kapsamayı amaçlamaz; daha ziyade, konunun tutarlı ve güvenilir bir şekilde değerlendirilmesini sağlamak için asgari bir gereklilik kümesi sağlamayı amaçlar.

Konu Bazlı Gereklilikler, IIA'nın Üçlü Hat Modeli ve Uluslararası İç Denetim Standartları ile açıkça bağlantılıdır. Yönetişim, risk yönetimi ve kontrol süreçleri, *Standart 9.1 Yönetişim, Risk Yönetimi ve Kontrol Süreçlerinin Anlaşılması* ile uyumlu olan Konu Bazlı Gerekliliklerin ana bileşenleridir. Üçlü Hat Modeline referansla, yönetişim yönetim kuruluna/yönetişim organına, risk yönetimi ikinci hatta ve kontroller veya kontrol süreçleri birinci hatta bağlanır. Yönetim hem birinci hem de ikinci hatta temsil edilirken, iç denetim fonksiyonu bağımsız ve objektif bir güvence sağlayıcı olarak üçüncü hatta gösterilir ve hiyerarşide yönetim kuruluna/yönetişim organına bağlıdır (İlke 8 Yönetim Kurulunun Gözetimi).

Uygulanabilirlik, Risk ve Mesleki Yargı

İç denetim birimleri, bir Konu Bazlı Gerekliliğin mevcut olduğu konularla ilgili güvence görevlerini yerine getirirken veya diğer güvence görevlerinde Konu Bazlı Gerekliliğin unsurları tespit edildiğinde, Konu Bazlı Gerekliliklere uyulmalıdır.

Standartlarda açıklandığı gibi, riski değerlendirmek iç denetim yöneticisinin planlamasının önemli bir parçasıdır. İç denetim planına dahil edilecek güvence görevlerinin belirlenmesi, kurumun stratejilerinin, hedeflerinin ve risklerinin en azından yıllık olarak değerlendirilmesini gerektirir (Standart 9.4 İç Denetim Planı). İç denetçiler, münferit güvence görevlerini planlarken, görevle ilgili riskleri değerlendirmek zorundadırlar (Standart 13.2 Görev Risk Değerlendirmesi).

Risk esaslı iç denetim planlama sürecinde bir Konu Bazlı Gereklilik hususu tespit edildiğinde ve denetim planına dahil edildiğinde, Konu Bazlı Gereklilikte ana hatlarıyla belirtilen gereklilikler, ilgili görevler kapsamında konuyu değerlendirmek için kullanılmalıdır. Buna ek olarak, iç denetçiler bir görev gerçekleştirdiklerinde (plana dahil olsun ya da olmasın) ve Konu Bazlı Gerekliliğin unsurları ortaya çıktığında, Konu Bazlı Gereklilik, görevin bir parçası olarak uygulanabilirlik açısından değerlendirilmelidir. Son olarak, başlangıçta planda olmayan ve konuyu içeren bir görev talep edilirse, Konu Bazlı Gereklilik uygulanabilirlik açısından değerlendirilmelidir.

Mesleki yargı, Konu Bazlı Gerekliliğin uygulanmasında kilit bir rol oynar. Risk değerlendirmeleri, iç denetim yöneticilerinin iç denetim planına hangi görevlerin dâhil edileceğine ilişkin kararlarını yönlendirir (Standart 9.4 İç Denetim Planı). Ayrıca, iç denetçiler her bir görevde hangi hususların ele alınacağını belirlemek için mesleki muhakemelerini kullanırlar (Standart 13.3 Görev Hedefleri ve Kapsamı, 13.4 Değerlendirme Kıstasları ve 13.6 Görev İş Programı). Ek A "Pratik Uygulama Örnekleri", iç denetçilerin Konu Bazlı Gerekliliğin geçerli olup olmadığını nasıl belirlediklerini açıklamaktadır.

Konu Bazlı Gereklilikteki her bir gerekliliğin uygulanabilirlik açısından değerlendirildiğine dair kanıtlar, herhangi bir gerekliliğin hariç tutulmasını açıklayan gerekçeler de dahil olmak üzere saklanmalıdır. Konu Bazlı Gerekliliğe uygunluk, “Görevlerin Kayıt Altına Alınması” başlıklı Standart 14.6’da açıklandığı gibi denetçinin mesleki muhakemesi kullanılarak belgelendirilmelidir.

Siber Güvenlik Konu Bazlı Gerekliliği, dikkate alınması gereken kontrol süreçlerine ilişkin bir temel sağlarken, siber riski çok yüksek olarak değerlendiren kuruluşların ek hususları değerlendirmesi gerekebilir.

Bir iç denetim yöneticisi, iç denetim fonksiyonunun bir Konu Bazlı Gereklilik alanı ile ilgili denetim görevlerini yerine getirmek için gerekli bilgiye sahip olmadığını tespit ederse, bu denetim görevi dış kaynak kullanarak yerine getirebilir (Standartlar 3.1 Yetkinlik, 7.2 İç Denetim Yöneticisinin Nitelikleri, 10.2 İnsan Kaynakları Yönetimi). Bu durumda bile, dış kaynak kullanımı iç denetim fonksiyonunu Konu Bazlı Gerekliliklere uyma sorumluluğundan kurtarmaz. İç denetim yöneticisi, uygunluğu sağlama konusundaki nihai sorumluluğu muhafaza eder. Ayrıca, iç denetim yöneticisi iç denetim kaynaklarının yetersiz olduğunu tespit ederse, iç denetim yöneticisi yetersiz kaynakların etkisi ve kaynak eksikliklerinin nasıl giderileceği hakkında yönetim kurulunu bilgilendirmek zorundadır (Standart 8.2 Kaynaklar).

Performans, Dokümantasyon ve Raporlama

İç denetçiler, Konu Bazlı Gereklilikleri uygularken, çalışmalarını Alan V: İç Denetim Hizmetlerinin Gerçekleştirilmesi ile uyumlu bir şekilde yürüterek Standartlara da uymak zorundadırlar. Alan V'teki standartlar, görevlerin planlanmasını (İlke 13 Görevlerin Etkili Şekilde Planlanması), görevlerin yürütülmesini (İlke 14 Görev Kapsamındaki İşlerin Yürütülmesi) ve görev sonuçlarının bildirilmesini (İlke 15 Görev Görev Sonuçlarının Raporlanması ve Eylem Planlarının İzlenmesi) açıklar.

Konu Bazlı Gerekliliğin kapsamı, denetçilerin mesleki muhakemesine dayalı olarak iç denetim planında veya görev çalışma kâğıtlarında belgelendirilebilir. Bir veya daha fazla iç

denetim görevi, gereklilikleri kapsayabilir. Ayrıca, tüm gereklilikler uygulanabilir olmayabilir. Konu Bazlı Gerekliliğin uygulanabilirlik açısından değerlendirildiğine dair kanıtlar, istisnaları açıklayan bir gerekçe de dâhil olmak üzere, muhafaza edilmelidir.

Ek C'deki isteğe bağlı araç, referans olarak ve iç denetçilerin yaptıkları işleri belgelemek için kullanılabilir.

Kalite Güvencesi

Standartlar, iç denetim yöneticisinin iç denetim fonksiyonunun tüm yönlerini kapsayan bir kalite güvence ve geliştirme programı oluşturmasını, uygulamasını ve sürdürmesini gerektirir (Standart 8.3 Kalite). Sonuçlar yönetim kuruluna ve üst yönetime iletilmek zorundadır. İletişim, iç denetim fonksiyonunun Standartlara uygunluğu ve performans hedeflerine ulaşması hakkında rapor vermek zorundadır.

Konu Bazlı Gerekliliklere uyum, kalite değerlendirme çalışmalarında değerlendirilecektir. Kalite incelemesine hazırlanmak için, iç denetçiler Ek C olarak verilen aracı kullanabilirler.

Siber Güvenlik

Siber güvenlik, herhangi bir kurumun çoğu teknolojik yönüyle ilgili geniş bir konudur. Bilgi teknolojisine ek olarak, siber güvenlik genellikle iş süreçlerinin bir parçasıdır ve iç denetçilerin güvence görevlerini planlarken, kapsamını belirlerken ve yerine getirirken siber bağlantılı riskleri değerlendirmelerini gerektirir.

ABD Ticaret Bakanlığı'nın bir parçası olan ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) siber güvenliği basitçe "Siber uzayın kullanımını siber saldırılara karşı koruma veya savunma yeteneği" olarak tanımlamaktadır. Siber Güvenlik Konu Bazlı Gerekliliği, kuruluşların yetkisiz kullanıcılardan ve kötü niyetli siber tehditlerden kaynaklanan riskleri azaltmak için güvence altına aldığı dış çevreye odaklanmaktadır. Siber güvenlik, NIST'in "gizlilik, bütünlük ve mevcudiyet sağlamak amacıyla bilgi ve bilgi sistemlerinin yetkisiz erişim, kullanım, ifşa, kesinti, değişiklik veya tahribata karşı korunması" olarak tanımladığı kapsamlı bilgi güvenliğinin bir alt kümesidir.

Siber Güvenlik Konu Bazlı Gereklilik şunları içerir:

- Yönetişim - kurumsal hedefleri, politikaları ve prosedürleri destekleyen, açıkça tanımlanmış temel siber güvenlik hedefleri ve stratejileri.
- Risk Yönetimi - siber riskleri derhal üst seviyeye taşımak (eskalasyon) için bir süreç de dahil olmak üzere siber tehditleri belirleme, analiz etme, yönetme ve izleme süreçleri.
- Kontroller - siber riski azaltmak için yönetim tarafından oluşturulan, periyodik olarak değerlendirilen kontrol süreçleri.

Dikkate Alınması Gerekenler

İç denetçiler, Siber Güvenlik Konu Bazlı Gerekliliğindeki gereklilikleri değerlendirmelerine yardımcı olması için aşağıdaki hususları kullanabilirler. Gerekliliklere çapraz atıfta bulunan bu hususlar açıklayıcıdır, ancak zorunlu değildir. İç denetçiler değerlendirmelerine neleri dâhil edeceklerini belirlerken mesleki muhakemelerine güvenmelidirler.

Yönetişimle İlgili Hususlar

Yönetişim süreçlerinin siber güvenlik hedeflerine nasıl uygulandığını değerlendirmek için, iç denetçiler aşağıdakileri gözden geçirebilirler:

A. Yönetim kurulunun, baş bilgi güvenliği görevlisi (CISO) gibi bilgi güvenliği fonksiyonunun yöneticisi tarafından sağlanan siber güvenlik güncellemelerini periyodik olarak (genellikle üç ayda bir) incelediğine dair kanıtlar da dahil olmak üzere, resmileştirilmiş, belgelenmiş siber güvenlik stratejik planı ve hedefleri. Kanıtlar aşağıdakiler hakkında raporlamayı içerebilir:
    - Stratejik hedeflere ulaşılmasının izlenmesi.
    - Siber güvenlik amaç ve hedeflerini desteklemek için bütçe ihtiyaçları.
    - İyileştirme ilerlemesi de dahil olmak üzere risklere ve iç kontrollere odaklanılması.
    - Başarıyı ölçmek için anahtar performans göstergeleri (KPI'lar).
    - Siber güvenlik personelini işe almak, eğitmek ve geliştirmek için gereken insan kaynakları.

B. Siber güvenlik süreçlerini yönetmek için kullanılan politikalar, prosedürler ve diğer ilgili belgeler:
    - En az yılda bir kez gözden geçirilen ve güncellenen politikalar. Ortaya çıkan siber riskler, gözden geçirme ve güncellemelerin daha sık yapılmasını gerektirebilir.
    - Politika ve prosedürlerin siber güvenlik operasyonlarını desteklemek için yeterli olup olmadığını belirlemeye yönelik bir süreç.
    - Siber güvenlik süreçlerini ve iç kontrolleri güçlendirmek için yaygın olarak benimsenen çerçeveler (NIST, COBIT ve diğerleri).

C. Siber güvenlik hedeflerine ulaşılmasını destekleyen roller ve sorumluluklar, siber güvenlik işlevinin kurum içinde kurumsal destek elde etmek için yeterli görünürlüğe sahip bir seviyeye bağlı olmasını sağlayan bir yapı da dahil olmak üzere.
    - Siber güvenlik rollerini yerine getiren personelin bilgi, beceri ve yeteneklerini periyodik olarak değerlendirmek için bir süreç.

D. Mevcut ve ortaya çıkan siber riskler ve bilinen potansiyel güvenlik açıkları hakkında iletişim de dahil olmak üzere ilgili paydaşlarla (örneğin, üst yönetim, operasyonlar, risk yönetimi, insan kaynakları, hukuk, uyum, stratejik tedarikçiler ve diğerleri) iletişimin kanıtı. İletişim kanıtları toplantı tutanaklarını, raporları veya e-postaları içerebilir.

Risk Yönetimi Hususları

Risk yönetimi süreçlerinin siber güvenlik hedeflerine nasıl uygulandığını değerlendirmek için, iç denetçiler aşağıdakileri gözden geçirebilirler

A. Aşağıdakiler de dahil olmak üzere kurumun siber güvenlik riskini nasıl değerlendirdiği ve yönettiği:
   - Tehditler ve güvenlik açıkları, başlangıçta nasıl tespit edilir ve raporlanır.
   - Tehditler ve güvenlik açıkları, kurumsal hedeflere ulaşma riskini değerlendirmek için nasıl analiz edilir.
   - Tehditler ve güvenlik açıkları, riski kabul edilebilir bir seviyeye indirmek için eylem planları da dahil olmak üzere nasıl azaltılır.
   - Tehditler ve güvenlik açıkları, tehditler tamamen çözülene kadar sürekli raporlama için bir plan da dahil edilmek üzere nasıl izlenir.

B. Kurumun bilgi teknolojisi, kurumsal risk yönetimi, insan kaynakları, hukuk, uyum, operasyonlar, muhasebe ve finans gibi işlevsel alanlardan siber güvenlik risk yönetimine ilişkin periyodik girdileri nasıl elde ettiği. Bilgi edinmek için işlevler arası bir siber güvenlik ekibi veya BT yönlendirme komitesi kullanılabilir.

C. Kurumun siber güvenlik risk yönetimi için hesap verebilirliği ve sorumluluğu bir bireye veya ekibe nasıl atadığı.
   - Sorumlu kişi(ler) kurum genelinde devam eden siber güvenlik risk güncellemelerini periyodik olarak (üç ayda bir, aylık veya gerektiğinde) iletmelidir ve bu bildirim risk azaltma stratejileri için kaynak gereksinimlerini de içerebilir.

D. Tehdit veya risk seviyesinin nasıl değerlendirildiği, atandığı ve önceliklendirildiği de dahil olmak üzere siber güvenlik riskleri için eskalasyon (konunun üst seviyeye taşınması) süreçleri. İnceleme aşağıdakilerin belirlenmesini içerebilir:
   - Kurumun tanımlanmış risk seviyeleri - yüksek, orta ve düşük gibi - her bir risk seviyesinin ayrıntılı açıklamaları ve her bir risk kategorisi için eskalasyon prosedürleri.
   - Şu anda tanımlanmış olan siber güvenlik risklerinin listesi ve her bir risk olayının hafifletilme durumu.
   - Geçerli yasal, düzenleyici ve uyum gereklilikleri.
   - Hem finansal hem de finansal olmayan (örneğin itibar) risk etkileri.

E. Siber güvenlik risklerinin yönetime ve çalışanlara iletilmesine yönelik süreç:
   - Kurumsal farkındalığı test etmek ve izlemek için habersiz, simüle edilmiş kimlik avı kampanyaları gibi periyodik (en az yılda bir) çalışan siber güvenlik eğitimi.
   - Beklenen tamamlanma tarihleriyle birlikte mevcut siber güvenlik sorunlarının giderilmesine ilişkin güncellemeler.
   - Yönetim kurulu ve üst yönetime bildirilen güncellemeleri içeren uyumsuzlukların izlenmesi.

- Kurumun risk iştahı ve risk toleransı değiştiğinde tehditlerin yeniden değerlendirilmesi.

F. Kuruluşun olaylara müdahale ve kurtarma ile ilgili olarak uyguladığı ve aşağıdakileri içeren süreçler:

- Kuruluşun faaliyetleri zaman içinde değiştikçe gözden geçirilen ve güncellenen belgelenmiş bir plan. Plan şunları içermelidir:
  - Olayların nasıl tespit edildiği ve raporlandığı.
  - Daha fazla hasarı önlemek için olayların nasıl kontrol altına alındığı.
  - Kuruluşun nasıl toparlanacağı ve operasyonları sürdürmek için nasıl yanıt vereceği.
  - Alınan derslerin ve gelecekte benzer olayların nasıl önlenebileceğinin belirlenmesi için olayın nasıl analiz edileceği.
- Periyodik (en az yılda bir) test (masa başı tatbikatı) ve sonuçların üst yönetime ve ilgili paydaşlara raporlanması. Testler sonucunda eylem planları ortaya çıkabilir.

Kontrol Süreci Hususları

Kontrol süreçlerinin siber güvenlik hedeflerine nasıl uygulandığını değerlendirmek için, iç denetçiler aşağıdakileri gözden geçirebilirler

A. Yönetimin etkin bir siber güvenlik iç kontrol ortamı oluşturmaya yönelik yaklaşımı:

- Kurumsal risk değerlendirme süreci tarafından bildirilen yüksek riskleri azaltmak ve hassas, kritik, kişisel veya gizli verileri korumak için gerekli iç kontrollerin değerlendirilmesi ve uygulanması.
- Temel siber güvenlik kontrollerini sürdürmek için kaynak gereksinimlerinin belirlenmesi.
- İş ilişkisine başlamadan önce ve ilişki süresi boyunca satıcılardan gelen hizmet kuruluşu kontrolleri (SOC) raporlarının gözden geçirilmesini içeren tedarikçi tabanlı kontrollerin kontrol ortamının bir parçası olarak değerlendirilmesi.
- Siber güvenlik kontrollerinin riskleri azaltacak ve siber güvenlik hedeflerine ulaşılmasını destekleyecek şekilde işlediğine dair periyodik testler.
- İç kontrol eksikliklerinin giderilmesi veya iç denetim fonksiyonu ya da diğer güvence sağlayıcılar (örneğin, sızma testleri) tarafından gerçekleştirilen değerlendirmelerden elde edilen bulguların ele alınması süreci.

B. Kuruluşun siber güvenlik uzmanlarının teknik bilgiyi destekleme ve ortaya çıkan sorunlara ilişkin kurumsal farkındalığı iyileştirmeyle ilgili becerilerini artırmaya yönelik fırsatları nasıl belirlediği de dahil olmak üzere kuruluşun siber güvenlik uzmanlarını işe alma ve eğitmeye yönelik yetenek yönetimi süreci.

- Örnekler arasında eğitimlere katılım, bilgi paylaşım gruplarına dahil olma ve siberle ilgili sertifikaların alınmasını da içeren sürekli mesleki eğitim yer almaktadır.

C. Yönetimin, ortaya çıkan siber güvenlik tehditlerini ve güvenlik açıklarını günlük operasyonlara odaklanan sürekli bir temelde belirleme, önceliklendirme, izleme ve raporlama süreci. İnceleme, yapay zeka kullanımı gibi yeni veya gelişmekte olan teknolojilerle ilgili tehditleri ve güvenlik açıklarını değerlendirmek için süreçlerin oluşturulmasını içerebilir.

D. Donanım, yazılım ve tedarikçi hizmetlerinin seçimi, kullanımı, bakımı ve hizmetten çıkarılması dahil olmak üzere BT varlıklarını yaşam döngüsü boyunca yönetmek ve korumak için yönetimin oluşturduğu süreçler ve kontroller. Donanım; sunucuları, ağ ekipmanlarını (yönlendiriciler veya güvenlik duvarları gibi), masaüstü bilgisayarları, dizüstü bilgisayarları, cep telefonlarını, tabletleri ve çevre birimlerini içerir. Yazılım, işletim sistemlerini (Windows gibi), kurumsal kaynak planlama (ERP) yazılımını, uygulamaları, antivirüs programlarını ve diğerlerini içerir. Donanım ve yazılımla ilgili hususlar şunları içerebilir:
   - Kurumun şifreleme, antivirüs yazılımı, mobil cihaz yönetimi, karmaşık parola gereksinimleri, kimlik doğrulama için sanal özel ağ (VPN)/sıfır güven ağı (ZTN) kullanımı ve ürün yazılımının (firmware) periyodik olarak güncellenmesi.
   - Şirket tarafından verilen donanımın, verildikten sonra uygun bir güvenlik yapılandırmasına sahip olmasını ve varlıklar kullanımdan kaldırıldığında uygun şekilde elden çıkarılmasını sağlayan bir varlık yönetimi süreci.
   - Kullanıcı ve yönetici erişiminin sınırlandırılması, şifreleme (encryption) kullanımının sağlanması, veri tabanlarının yedeklenmesi ve test edilmesi ve güçlü ağ güvenlik kontrollerinin varlığını içeren veri tabanıyla ilgili kontroller.
   - Sistem geliştirme yaşam döngüsünde (SDLC) siber güvenlik tehditlerinin veya güvenlik açıklarının nasıl dikkate alındığı.
   - Geliştirme, güvenlik ve operasyonlar (DevSecOps) tarafından yazılım geliştirme sürecinin, güvenlik açıklarını proaktif olarak belirlemek için siber güvenliği içermesini sağlamak için kullanılan yaklaşım.

E. Aşağıdakiler dahil olmak üzere siber güvenliği güçlendirmek için kullanılan süreçler
   - Siber güvenlik riskini en aza indirmek için güvenlik ayarlarının yapılandırılması.
   - Mobil cihaz yönetimi (e-posta ve uygulamaların kullanımı dahil), siber güvenlik risklerini azaltacak ve bir kullanıcının cihazının tehlikeye girmesi durumunda uzaktan yönetilecek şekilde yapılandırılması.
   - Sabit diskte depolanan bilgiler gibi "bekleyen" veriler veya e-postaların şifrelenmesi gibi "aktarım halindeki" veriler için şifreleme kullanımı.
   - Sunucuların veya yazılımların (işletim sistemi gibi) en son güvenlik sürümleriyle yamalanması.

- Çok faktörlü kimlik doğrulama (MFA) kullanımı ve periyodik olarak süresi dolan karmaşık parolalara sahip benzersiz (tekil) kullanıcı kimlikleri (ID) gibi kullanıcı erişim yönetimi.
- Performansı tehdit eden potansiyel siber güvenlik sorunlarının incelenmesine ve analiz edilmesine olanak tanıyarak, mevcudiyet ve kaynak kullanımının yeterli performans gösterip göstermediğini belirlemek için kontrollerin izlenmesi.
- Yazılım canlıya geçmeden önce siber güvenlik açıklarını tespit etmek ve ele almak için siber güvenliğin SDLC'ye entegrasyonu.

F. Kurumun nasıl kullandığı da dahil olmak üzere kurumun çevresini güvence altına alan ağla ilgili kontroller:
   - Ağ segmentasyonu.
   - Güvenlik duvarları.
   - Kullanıcı erişim kontrolleri.
   - Hem harici hem de dahili bağlantılar için sınırlamalar.
   - Birbirine bağlı ağlar için Nesnelerin İnternetini (IoT) çevreleyen kontroller.
   - Siber güvenlik saldırılarını önlemek, tespit etmek ve kurtarmak için izinsiz giriş tespit/önleme sistemleri (IDS/IPS).

G. E-posta, internet tarayıcıları, video konferans, mesajlaşma (Zoom, MS Teams ve diğerleri), sosyal medya, bulut ve dosya paylaşım protokolleri gibi hizmetler için geçerli olan uç nokta-iletişim güvenlik kontrollerini çevreleyen kontroller. Kontroller, belirli dosya uzantılarının (.exe dosyaları gibi) kullanımının kısıtlanmasını ve dosya paylaşımı için çok faktörlü kimlik doğrulamayı içerebilir.

Ek A. Pratik Uygulama Örnekleri

Aşağıdaki örnekler, Siber Güvenlik Konu Bazlı Gerekliliğinin uygulanabileceği senaryoları açıklamaktadır:

Örnek 1: Siber güvenlik, iç denetim planında yer alan bir iç denetim görevi için tanımlanmıştır.

İç denetim fonksiyonu risk bazlı planlama sürecini tamamladığında ve iç denetim planına siber güvenlikle ilgili bir veya daha fazla görev dahil ettiğinde, bu görevlerin yürütülmesinde Konu Bazlı Gereklilik zorunludur. Uyum, gerekliliklerin iç denetim planındaki bir veya daha fazla göreve dâhil edilmesiyle sağlanabilir.

Siber güvenlik geniş bir konudur ve Konu Bazlı Gerekliliktekı her gereklilik her görev için geçerli olmayabilir. İç denetçiler mesleki muhakemelerini kullanıp Siber Güvenlik Konu Bazlı Gerekliliğinin bir veya daha fazla şartının uygulanabilir olmadığını ve dolayısıyla bir görevin dışında tutulması gerektiğini belirlediklerinde, iç denetçiler bu şartların dışında tutulma gerekçelerini belgelendirmeli ve saklamalıdırlar. Örneğin, bazı gerekliliklerin hariç tutulmasının gerekçesi, iç denetim fonksiyonunun çeşitli siber güvenlik görevlerini rotasyon esasına göre yürütmesi veya görevdeki riskin öneminin düşük olduğunu tespit etmesi olabilir.

Örnek 2: Siber güvenlik riskleri, siber güvenliğe odaklanmayan bir denetim görevi sırasında tespit edilir.

İç denetçiler, siber güvenlikle doğrudan ilgili olmayan bir süreci değerlendirirken siber güvenlik risklerini tespit edebilirler. Örneğin, iç denetçiler, siber güvenliğe odaklanmayan bir görevde satıcılar hesabı sürecini değerlendiriyor olabilir ve görevi planlarken siber güvenlik risklerini kapsam dahilinde tanımlamamış olabilir. Ancak, ilk gözden geçirmeyi yaptıktan sonra, iç denetçiler bu tür risklerin kapsam dahilinde olması gerektiğini belirlerler; örneğin, ilk satın alma siparişi talebinin web tabanlı olarak gönderilmesiyle ilgili siber güvenlik risklerini tespit ederler (Standart 13.2 Görev Risk Değerlendirmesi).

İlgili riskler belirlendikten sonra, iç denetçiler Siber Güvenlik Konu Bazlı Gerekliliğini gözden geçirmeli ve hangi gerekliliklerin uygulanabilir olduğunu belirlemelidir. Bu örnekte, siber güvenlik yönetişim sürecini veya siber güvenlik risk yönetimi sürecini hariç tutabilirler. Siber Güvenlik Konu Bazlı Gerekliliğinin diğer gerekliliklerinin hariç tutulmasının gerekçesini görev çalışma kâğıtlarında belgelendirmeli ve belgeleri muhafaza etmelidirler.

Örnek 3: Başlangıçta iç denetim planında yer almayan bir siber güvenlik görevi talep edilir.

Yönetim kurulu, yönetim veya düzenleyici kurum gibi bazı paydaşlar, iç denetçilerden orijinal denetim planının dışında siber güvenlik değerlendirmeleri yapmalarını isteyebilirler. Örneğin, kurumlar bir siber saldırının hedefi olduklarında, yönetim kurulu siber güvenlik kontrollerinin değerlendirilmesi için iç denetim görevi talep edebilir. Konu Bazlı Gereklilik uygulanabilir olduğunda, gereklilikler değerlendirilmeli ve istisnalar belgelendirilmelidir.

Ek B. Çerçevelerle Eşleştirme

Kurum, COBIT veya NIST gibi risk yönetimi ve yönetişim çerçevelerini kullanarak kendi siber güvenlik gayreti içinde olabilir. İç denetçiler bu çerçeveleri temel alan denetim programları ve test prosedürleri geliştirmiş olabilirler. İç denetçiler, yeterli kapsamı sağlamak için amaçladıkları siber güvenlik kontrol testlerini Konu Bazlı Gereklilikle bağdaştırmalıdır. Aşağıdaki tablo, Siber Güvenlik Konu Bazlı Gerekliliğini yaygın olarak kullanılan üç çerçeveyle eşleştirmektedir: NIST Siber Güvenlik Çerçevesi 2.0, COBIT 2019 ve NIST 800-53. Bu çerçeveler ücretsiz olarak temin edilebildikleri için eşleştirilmiştir.

Yönetişim Gereklilikleri	Çerçeve Referansları		
	NIST CSF 2.0	NIST 800-53	COBIT 2019
A. Resmi siber güvenlik stratejisi ve hedefleri oluşturulur ve periyodik olarak güncellenir. Siber güvenlik stratejisini desteklemek için kaynaklar ve bütçe hususları da dahil olmak üzere, siber güvenlik hedeflerine ulaşılmasına ilişkin güncellemeler periyodik olarak yönetim kuruluna iletilir ve kurul tarafından gözden geçirilir.	GV.RM-01; GV.RM-02; GV.RM-03; GV.RM-04; GV.OC-02; GV.RR-03; GV.RR-04; GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-03	PM-1, PM-4; AT-2; AT-3; PM-9; PM-28	EDM01; EDM03; EDM04; APO06; APO01; APO10; APO12
B. Siber güvenlikle ilgili politika ve prosedürler oluşturulur, periyodik olarak güncellenir ve kontrol ortamını güçlendirir.	GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-02; GV.OV-03; GV.SC-01; GV.SC-03; GV.RR-03	AC-1, PM-9; AC-1; AT-1; CA-1; CM-1; IA-1; IR-1; MP-1; PE-1	EDM01; EDM02; EDM03; APO01; APO11
C. Siber güvenlik hedeflerini destekleyen roller ve sorumluluklar belirlenmiştir ve bu rolleri dolduranların bilgi, beceri ve yeteneklerini periyodik olarak değerlendirmek için bir süreç mevcuttur.	GV.RR-02; GV.RR-04; GV.SC-02; GV.OC-02	PM-13; AT-2; AT-3	EDM02; APO01; APO07

D. İlgili paydaşlar, siber güvenlik ortamındaki mevcut güvenlik açıklarını ve yeni ortaya çıkan tehditleri tartışmak ve bunlara karşı harekete geçmek için devreye girer. Paydaşlar arasında üst yönetim, operasyonlar, risk yönetimi, insan kaynakları, hukuk, uyum, satıcılar ve diğerleri yer alır.	GV.OC-02; GV.RM-01; GV.RM-05; GV.RM-07; GV.OV-03; GV.SC-03	AC-1; CM-1	EDM05; EDM01.01; EDM03; MEA01.02; APO01; APO08; APO11; APO13; MEA02
Risk Yönetimi Gereklilikleri	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. Kurumun risk değerlendirme ve risk yönetimi süreçleri siber güvenlik tehditlerinin ve bunların stratejik hedeflere ulaşılması üzerindeki etkilerinin tanımlanmasını, analiz edilmesini, azaltılmasını ve izlenmesini içermektedir.	GV.RM-01; GV.RM-03; GV.OC-01	AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
B. Siber güvenlik risk yönetimi kurum genelinde yürütülür ve şu alanları içerebilir: bilgi teknolojisi, kurumsal risk yönetimi, insan kaynakları, hukuk, uyum, operasyonlar, tedarik zinciri, muhasebe, finans ve diğerleri.	GV.RM-01; GV.RM-05; GV.RR-01; GV.RR-02; GV.OC-03; GV.SC-07	PM-29; AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
C. Siber güvenlik risk yönetimi için hesap verebilirlik ve sorumluluk oluşturulur ve riski azaltmak ve ortaya çıkan siber güvenlik tehditlerini belirlemek için gereken kaynaklar da dahil olmak üzere siber güvenlik risklerinin nasıl yönetildiğini periyodik olarak izleyecek ve raporlayacak bir kişi veya ekip belirlenir.	GV.RR-01; GV.RR-02; GV.RR-03; GV.0V-01; GV.OV-02; GV.OV-03	PM-9; PM-29	EDM03; APO01; APO10; APO12

D. Kuruluşun yerleşik risk yönetimi kılavuz ilkelerine göre kabul edilemez bir düzeye yükselen herhangi bir siber güvenlik riskini (ortaya çıkan veya daha önce tanımlanmış) hızla eskale etmek veya geçerli yasal ve düzenleyici gerekliliklere uymak için bir süreç oluşturulur. Siber güvenlik riskinin hem finansal hem de finansal olmayan etkileri dikkate alınmalıdır.	GV.RM; ID.RA; RS.MA-04	CA-7; RA-3; RA-7	EDM03; APO01, APO10; APO12
E. Siber güvenlik risk farkındalığının yönetime ve çalışanlara iletilmesi ve sorunların, boşlukların, eksikliklerin veya kontrol hatalarının yönetim tarafından periyodik olarak gözden geçirilerek raporlanması ve düzeltilmesi için bir süreç oluşturulmuştur.	PR.AT; GV.RR.01; GV.RR-04; GV.PO	AT-2	APO01; APO02; EDM03; MEA03
F. Kurum tespit, kontrol altına alma, kurtarma ve olay sonrası analizi içeren bir siber güvenlik olay müdahale ve kurtarma süreci uygulamıştır. Olay müdahale ve kurtarma süreci periyodik olarak test edilmektedir.	RS; RC	IR-4; IR-5; IR-6; IR-7; IR-8; IR-10; SA-15	DSS02; DSS03; DSS04; DSS05.07
Kontrol Süreci Gereklilikleri	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. Kurumun sistemlerinin ve verilerinin gizliliğini, bütünlüğünü ve mevcudiyetini korumak için hem dahili kontrollerin hem de tedarikçi tabanlı kontrollerin yürürlükte olmasını sağlayan bir süreç oluşturulmuştur. Kontroller, kurumsal siber güvenlik hedeflerine ulaşılmasını ve sorunların zamanında çözülmesini teşvik edecek şekilde işlediklerini belirlemek için periyodik olarak değerlendirilir.	ID.IM-01; ID.IM-02; ID.IM-03; PR; DE; RS; RC; ID.RA06; GV.RM-05; GV.SC; ID.IM-02; RS.MA-01; DE.CM-06	AC-3; AC-4; AC-10; AC-13; AC-17; PM-30; RA-3; SA-9; SR-2	MEA02; MEA04; EDM03; APO09; APO10; DSS01

B. Siber güvenlik operasyonları için teknik yetkinliklerin geliştirilmesi ve sürdürülmesine yönelik eğitim fırsatlarını içeren bir yetenek yönetimi süreci oluşturulur ve periyodik olarak gözden geçirilir.	PR.AT-01; PR.AT-02; GV.RR-03	AT-2; AT-3; IR-2; PM-14	APOO7; DSS04
C. Ortaya çıkan siber güvenlik tehditlerini ve güvenlik açıklarını sürekli olarak izlemek ve raporlamak ve siber güvenlik operasyonlarını iyileştirmeye yönelik fırsatları belirlemek, önceliklendirmek ve uygulamak için bir süreç oluşturulur.	ID.RA-02; ID.RA-03, ID.RA-04	CA-7; PM-31; RA-5	DSS03.05
D. Siber güvenlik, donanım, yazılım ve tedarikçi hizmetleri de dahil olmak üzere tüm BT varlıklarının yaşam döngüsü yönetimine (seçim, kullanım, bakım ve hizmetten çıkarma) dahil edilir.	ID.AM; PR.PS-03; PR.IR; DE.CM-09; ID.AM-08; ID.RA-09; PR.PS-06	AU-9; CM-7; SC-49; SC-51; CM-2; SA-3; SA-10; SA-15; SA-17; SA-20; AU-6; IR-7	DSS05.03; BAI03; BAI09; BAI03; BAI11; DSS05.01; DSS02; DSS03; DSS06.06
E. Yapılandırma, son kullanıcı cihaz yönetimi, şifreleme, yama, kullanıcı erişimi yönetimi ve mevcudiyetin ve performansın izlenmesi dahil olmak üzere siber güvenliği teşvik etmek için süreçler oluşturulur. Siber güvenlikle ilgili hususlar yazılım geliştirmeye (DevSecOps) dahil edilir.	PR.PS-01; PR.PS-06; PR.DS-01; PR.DS-02; PR.PS-05; DE.CM-03	CM-6; SI-2; AC-3; CA-7; SA-4; AC-16; AC-18	BAI10; DSS05; DSS06.03; DSS01.03; MEA01
F. Ağ erişim kontrolleri ve segmentasyonu; güvenlik duvarlarının kullanımı ve yerleştirilmesi, dış ağlardan ve dış ağlara sınırlı bağlantılar; sanal özel ağ (VPN)/sıfır güven ağ erişimi (ZTNA), Nesnelerin İnterneti (IoT) ağ kontrollerinin dahil edilmesi ve saldırı tespit/önleme sistemleri (IDS ve IPS) gibi ağla ilgili kontroller oluşturulur.	PR.IR; DE.CM-01	AC-6; AC-17; AC-18; AC-20; SC-7; SC-10; CA-8	DSS05.02

G. E-posta, internet tarayıcıları, video konferans, mesajlaşma, sosyal medya, bulut ve dosya paylaşım protokolleri gibi hizmetlere ilişkin uç nokta iletişim güvenlik kontrolleri oluşturulmuştur.	PR.DS-01; PR.DS-02; PR.DS-10; PR.IR	AC-2; AC-16; AU-10; CA-3; SI-8; SI-20; SC-8	BAI10

Ek C. İsteğe Bağlı Dokümantasyon Aracı

İç denetçilerden, risk değerlendirmesine dayalı olarak gerekliliklerin uygulanabilirliğini belirlerken mesleki muhakemelerini kullanmaları ve belirli gerekliliklerin istisnalarını uygun şekilde belgelendirmeleri beklenir. Konu Bazlı Gereklilik, iç denetim planında veya denetçinin mesleki muhakemesine dayalı olarak görev çalışma kâğıtlarında belgelendirilebilir. Bir veya daha fazla iç denetim görevi, gereklilikleri kapsayabilir. Ayrıca, tüm gereklilikler uygulanabilir olmayabilir. Aşağıdaki yazdırılabilir form, Siber Güvenlik Konu Bazlı Gerekliliğine uygunluğun belgelenmesi için bir seçenek sunar, ancak kullanımı zorunlu değildir.

Siber Güvenlik - Yönetişim

Gereklilik	Yürütülen Teminat veya İstisna Gerekçesi	Dokümantasyon Referansı
A. Resmi siber güvenlik stratejisi ve hedefleri oluşturulur ve periyodik olarak güncellenir. Siber güvenlik stratejisini desteklemek için kaynaklar ve bütçe hususları da dahil olmak üzere, siber güvenlik hedeflerine ulaşılmasına ilişkin güncellemeler periyodik olarak yönetim kuruluna iletilir ve kurul tarafından gözden geçirilir.		
B. Siber güvenlikle ilgili politika ve prosedürler oluşturulur, periyodik olarak güncellenir ve kontrol ortamını güçlendirir.		
C. Siber güvenlik hedeflerini destekleyen roller ve sorumluluklar belirlenmiştir ve bu rolleri dolduranların bilgi, beceri ve yeteneklerini periyodik olarak değerlendirmek için bir süreç mevcuttur.		
D. İlgili paydaşlar, siber güvenlik ortamındaki mevcut güvenlik açıklarını ve yeni ortaya çıkan tehditleri tartışmak ve bunlara karşı harekete geçmek için devreye girer. Paydaşlar arasında üst yönetim, operasyonlar, risk yönetimi, insan kaynakları, hukuk, uyum, satıcılar ve diğerleri yer alır.		

Siber Güvenlik - Risk Yönetimi

Gereklilik	Yürütülen Teminat veya İstisna Gerekçesi	Dokümantasyon Referansı
A. Kurumun risk değerlendirme ve risk yönetimi süreçleri siber güvenlik tehditlerinin ve bunların stratejik hedeflere ulaşılması üzerindeki etkilerinin tanımlanmasını, analiz edilmesini, azaltılmasını ve izlenmesini içermektedir.		
B. Siber güvenlik risk yönetimi kurum genelinde yürütülür ve şu alanları içerebilir: bilgi teknolojisi, kurumsal risk yönetimi, insan kaynakları, hukuk, uyum, operasyonlar, tedarik zinciri, muhasebe, finans ve diğerleri.		
C. Siber güvenlik risk yönetimi için hesap verebilirlik ve sorumluluk oluşturulur ve riski azaltmak ve ortaya çıkan siber güvenlik tehditlerini belirlemek için gereken kaynaklar da dahil olmak üzere siber güvenlik risklerinin nasıl yönetildiğini periyodik olarak izleyecek ve raporlayacak bir kişi veya ekip belirlenir.		
D. Kuruluşun yerleşik risk yönetimi kılavuz ilkelerine göre kabul edilemez bir düzeye yükselen herhangi bir siber güvenlik riskini (ortaya çıkan veya daha önce tanımlanmış) hızla eskale etmek veya geçerli yasal ve düzenleyici gerekliliklere uymak için bir süreç oluşturulur. Siber güvenlik riskinin hem finansal hem de finansal olmayan etkileri dikkate alınmalıdır.		

Gereklilik	Yürütülen Teminat veya İstisna Gerekçesi	Dokümantasyon Referansı
E. Siber güvenlik risk farkındalığının yönetime ve çalışanlara iletilmesi ve sorunların, boşlukların, eksikliklerin veya kontrol hatalarının yönetim tarafından periyodik olarak gözden geçirilerek raporlanması ve düzeltilmesi için bir süreç oluşturulmuştur.		
F. Kurum tespit, kontrol altına alma, kurtarma ve olay sonrası analizi içeren bir siber güvenlik olay müdahale ve kurtarma süreci uygulamıştır. Olay müdahale ve kurtarma süreci periyodik olarak test edilmektedir.		

Siber Güvenlik - Kontrol Süreçleri

Gereklilik	Yürütülen Teminat veya İstisna Gerekçesi	Dokümantasyon Referansı
A. Kurumun sistemlerinin ve verilerinin gizliliğini, bütünlüğünü ve mevcudiyetini korumak için hem dahili kontrollerin hem de tedarikçi tabanlı kontrollerin yürürlükte olmasını sağlayan bir süreç oluşturulmuştur. Kontroller, kurumsal siber güvenlik hedeflerine ulaşılmasını ve sorunların zamanında çözülmesini teşvik edecek şekilde işlediklerini belirlemek için periyodik olarak değerlendirilir.		
B. Siber güvenlik operasyonları için teknik yetkinliklerin geliştirilmesi ve sürdürülmesine yönelik eğitim fırsatlarını içeren bir yetenek yönetimi süreci oluşturulur ve periyodik olarak gözden geçirilir.		

Gereklilik	Yürütülen Teminat veya İstisna Gerekçesi	Dokümantasyon Referansı
C. Ortaya çıkan siber güvenlik tehditlerini ve güvenlik açıklarını sürekli olarak izlemek ve raporlamak ve siber güvenlik operasyonlarını iyileştirmeye yönelik fırsatları belirlemek, önceliklendirmek ve uygulamak için bir süreç oluşturulur.		
D. Siber güvenlik, donanım, yazılım ve tedarikçi hizmetleri de dahil olmak üzere tüm BT varlıklarının yaşam döngüsü yönetimine (seçim, kullanım, bakım ve hizmetten çıkarma) dahil edilir.		
E. Yapılandırma, son kullanıcı cihaz yönetimi, şifreleme, yama, kullanıcı erişimi yönetimi ve mevcudiyetin ve performansın izlenmesi dahil olmak üzere siber güvenliği teşvik etmek için süreçler oluşturulur. Siber güvenlikle ilgili hususlar yazılım geliştirmeye (DevSecOps) dahil edilir.		
F. Ağ erişim kontrolleri ve segmentasyonu; güvenlik duvarlarının kullanımı ve yerleştirilmesi, dış ağlardan ve dış ağlara sınırlı bağlantılar; sanal özel ağ (VPN)/sıfır güven ağ erişimi (ZTNA), Nesnelerin İnterneti (IoT) ağ kontrollerinin dahil edilmesi ve saldırı tespit/önleme sistemleri (IDS ve IPS) gibi ağla ilgili kontroller oluşturulur.		
G. E-posta, internet tarayıcıları, video konferans, mesajlaşma, sosyal medya, bulut ve dosya paylaşım protokolleri gibi hizmetlere ilişkin uç nokta iletişim güvenlik kontrolleri oluşturulmuştur.		

İç Denetçiler Enstitüsü Hakkında

İç Denetçiler Enstitüsü (IIA), 255.000'den fazla küresel üyeye hizmet veren ve dünya çapında 200.000'den fazla Sertifikalı İç Denetçi® (CIA®) sertifikası vermiş olan uluslararası bir meslek kuruluşudur. 1941 yılında kurulan IIA, dünya çapında iç denetim mesleğinin standartlar, sertifikalar, eğitim, araştırma ve teknik rehberlik alanlarındaki lideri olarak tanınmaktadır. Daha fazla bilgi için www.theiia.org.

Sorumluluk Reddi

IIA bu belgeyi bilgilendirme ve eğitim amacıyla yayınlamaktadır. Bu materyalin belirli bireysel durumlara kesin cevaplar sağlaması amaçlanmamıştır ve bu nedenle sadece bir rehber olarak kullanılması amaçlanmıştır. IIA, herhangi bir özel durumla doğrudan ilgili bağımsız uzman tavsiyesi alınmasını tavsiye eder. IIA, bu materyale tek başına güvenen hiç kimse için sorumluluk kabul etmez.

Telif Hakkı

Şubat 2025

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101