Siber Güvenlik

Topical Requirement

The Institute of
Internal Auditors

Siber Güvenlik Konu Bazlı Gereklilik

Uluslararası Mesleki Uygulama Çerçevesi (International Professional Practices Framework®), Uluslararası İç Denetim Standartları (Global Internal Audit Standards™), Konu Bazlı Gereklilikler ve Küresel Rehberlerden oluşmaktadır. Konu Bazlı Gereklilikler, zorunludur ve gerekli uygulamalar için temel yetkiyi sağlayan Uluslararası İç Denetim Standartları ile birlikte kullanılmalıdır.

Konu Bazlı Gereklilikler, belirli risk konularının denetlenmesi için asgari bir temel belirleyerek iç denetçiler için açık beklentiler ortaya koyar. Kurumun risk profili, iç denetçilerin konunun ilave yönlerini de dikkate almalarını gerektirebilir.

Konu Bazlı Gerekliliklere uyum, iç denetim hizmetlerinin yürütülmesindeki tutarlılığı artıracak ve iç denetim hizmetlerinin ve sonuçlarının kalitesini ve güvenilirliğini geliştirecektir. Nihayetinde, Konu Bazlı Gereklilikler iç denetim mesleğini yüceltir.

İç denetçiler, Uluslararası İç Denetim Standartlarına uygun olarak Konu Bazlı Gereklilikleri uygulamak zorundadır. Konu Bazlı Gerekliliklere uyum, güvence hizmetleri için zorunludur ve danışmanlık hizmetleri için tavsiye edilir.

Konu Bazlı Gereklilik, aşağıdaki durumlardan biri olduğunda uygulanabilir:

A. İç denetim planındaki bir görevin konusu bahsedilen konu olduğunda.
B. Bir görev gerçekleştirilirken söz konusu konu tespit edilmiştir.
C. Orijinal iç denetim planında yer almayan bir görev talebinin konusu bahsedilen konu olduğunda.

Konu Bazlı Gerekliliklerteki her bir gerekliliğin uygulanabilirlik açısından değerlendirildiğine dair kanıtlar belgelenmeli ve saklanmalıdır. Tüm gereklilik maddeleri her görev için geçerli olmayabilir; gereklilikler hariç tutulursa, gerekçesi belgelenmeli ve saklanmalıdır. Konu Bazlı Gerekliliklere uyum zorunludur ve kalite değerlendirmeleri sırasında dikkate alınacaktır.

Daha fazla bilgi için Siber Güvenlik Konu Bazlı Gereklilik Kullanıcı Rehberine bakın.

Siber Güvenlik

ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) siber güvenliği basitçe "Siber uzayın kullanımını siber saldırılara karşı koruma veya savunma yeteneği" olarak tanımlamaktadır. 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, genel kontrol ortamını güçlendirerek ve bir kuruluşun bilgi varlıklarını yetkisiz erişim, kesinti, değişiklik veya tahribattan koruyarak riski azaltır. Bilgisayarlar, ağlar, programlar, veriler ve hassas bilgiler çoğu kuruluşun kritik bileşenleri olduğundan, siber saldırılar genellikle önemli doğrudan ve dolaylı etkilere yol açabilir.

Siber Güvenlik Yönetişimi, Risk Yönetimi ve Kontrol Süreçlerinin Ölçülmesi ve Değerlendirilmesi

Bu Konu Bazlı Gereklilik, siber güvenlik yönetişimi, risk yönetimi ve kontrol süreçlerinin tasarım ve uygulamasını değerlendirmek için tutarlı ve kapsamlı bir yaklaşım sağlar. Gereklilikler, bir kuruluşta siber güvenliğin değerlendirilmesi için asgari bir temeli temsil eder.

YÖNETİŞİM: Siber Güvenlik Yönetişiminin Ölçülmesi ve Değerlendirilmesi

Gereklilikler:

İç denetçiler, kurumun siber güvenlik yönetişimiyle ilgili olarak aşağıdakileri değerlendirmek zorundadır:

A. Resmi bir siber güvenlik stratejisi ve hedefleri oluşturulur ve periyodik olarak güncellenir. Siber güvenlik hedeflerine ulaşılmasına ilişkin güncellemeler, siber güvenlik stratejisini desteklemek için kaynaklar ve bütçe hususları da dahil olmak üzere periyodik olarak yönetim kuruluna iletilir ve yönetim kurulu tarafından gözden geçirilir.

B. Kontrol ortamını güçlendirmek için siber güvenlikle ilgili politika ve prosedürler oluşturulur ve periyodik olarak güncellenir.

C. Siber güvenlik hedeflerini destekleyen roller ve sorumluluklar belirlenmiştir ve rolleri dolduran bireylerin 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, operasyon birimleri, risk yönetimi, insan kaynakları, hukuk, uyum, tedarikçiler ve diğerleri yer alır.

RİSK YÖNETİMİ: Siber Güvenlik Risk Yönetiminin Ölçülmesi ve Değerlendirilmesi

Gereklilikler:

İç denetçiler, kurumun siber güvenlik risk yönetimiyle ilgili olarak aşağıdakileri değerlendirmek zorundadır:

A. Kurumun risk değerlendirme ve risk yönetimi süreçleri siber güvenlik tehditlerinin ve bunların stratejik hedeflere ulaşma üzerindeki etkilerinin tanımlanmasını, analiz edilmesini, hafifletilmesini ve izlenmesini içerir.

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 belirlenmiştir. Riskleri 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. Kurumun yerleşik risk yönetimi kılavuz ilkelerine veya geçerli yasal ve düzenleyici gerekliliklere göre kabul edilemez bir seviyeye ulaşan herhangi bir siber güvenlik riskini (yeni ortaya çıkan veya önceden tanımlanmış) hızla üst seviyeye taşıyıp ele almak (eskale etmek) için bir süreç oluşturulur. Siber güvenlik riskinin finansal ve finansal olmayan etkileri dikkate alınmalıdır.

E. Siber güvenlik risk farkındalığını yönetime ve çalışanlara iletmek ve yönetimin sorunları, boşlukları, eksiklikleri veya kontrol başarısızlıklarını zamanında raporlama ve düzeltme ile periyodik olarak gözden geçirmesi için bir süreç oluşturulmuştur.

F. Kurum tespit, kontrol altına alma, kurtarma ve olay sonrası analizi içeren bir siber güvenlik olayı müdahale ve kurtarma süreci uygulamıştır. Olay müdahale ve kurtarma süreci periyodik olarak test edilmektedir.

KONTROLLER: Siber Güvenlik Kontrol Süreçlerinin Ölçülmesi ve Değerlendirilmesi

Gereklilikler:

İç denetçiler, kurumun siber güvenlik kontrol süreçleriyle ilgili olarak aşağıdakileri değerlendirmek zorundadır:

A. Kuruluşun sistemlerinin ve verilerinin gizliliğini, bütünlüğünü ve mevcudiyetini korumak için hem dahili kontrollerin hem de tedarikçi tabanlı kontrollerin yürürlükte olmasını sağlamak için bir süreç oluşturulur. Kontrollerin kurumsal siber güvenlik hedeflerine ulaşılmasını ve sorunların hızlı bir şekilde çözülmesini destekleyecek şekilde işleyip işlemediğini belirlemek için periyodik olarak değerlendirmeler yapılır.

B. Siber güvenlik operasyonlarıyla ilgili teknik yetkinliklerin geliştirilmesi ve sürdürülmesine yönelik eğitimleri içeren bir yetenek yönetimi süreci oluşturulmuştur. Süreç periyodik olarak gözden geçirilir.

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 oluşturulmuştur.

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 edilmiştir.

E. Yapılandırma (konfigirasyon), son kullanıcı cihaz yönetimi, şifreleme, yama, kullanıcı erişimi yönetimi ve mevcudiyet ve performansın izlenmesi dahil olmak üzere siber güvenliği güçlendirmek için süreçler oluşturulur. Siber güvenlikle ilgili hususlar yazılım geliştirmeye (DevSecOps) dahil edilir.

F. Ağ erişim kontrolleri ve segmentasyon; 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 kontrolleri 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 hizmetler için 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 adresini ziyaret edin.

Telif Hakkı

Şubat 2025

The Institute of Internal Auditors

Küresel Genel Merkez
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, ABD
Telefon +1-407-937-1111
Faks: +1-407-937-1101