TONE at TOP®

Üst yönetime, yönetim kurullarına ve denetim komitelerine yönetişimle ilgili konularda kısa ve öz bilgiler sunar.

Sayı 127 | Şubat 2025

Yerleşik Riskleri İzlemek için Yeni Bir Araç

IIA, iç denetçilerin gündemdeki önemli konuları daha etkili biçimde ele alma çabalarını destekleyecek bir dizi yeni gereklilikten ilkini bu ay yayımlandı. IIA'nın Uluslararası Mesleki Uygulama Çerçevesi (UMUÇ) kapsamındaki en yeni bileşen olan Konu Bazlı Gereklilikler, tüm iç denetim departmanlarının (büyüklüğü, sahiplik yapısı, ya da coğrafi konumu ne olursa olsun) belirli bir konu alanında yönetişim, risk yönetimi ve kontrol süreçlerinin etkinliğini değerlendirirken aynı denetim metodolojisini uygulamasını sağlayacaktır.

Konu Bazlı Gereklilikler, iç denetim fonksiyonunun çalışmalarını ve iç denetimin yönetim kuruluna ve kuruma sağladığı bilgi ve içgörülerin değerini yükselten bir temel oluşturmaktadır. Tone at Top'ın bu sayısı, Konu Bazlı Gereklilikleri ve bu gerekliliklerin yönetim kurulu üyeleri ve kurumları için ne anlama geldiğini ele alıyor.

Yaygın, Yüksek Riskli Konular

İç denetçiler kuruma kattıkları değeri azami düzeye çıkarmak amacıyla süreçleri ve karar alma mekanizmalarını geliştirmek için bağımsız, objektif güvence ve danışmanlık sağlamaktadırlar. IIA, denetçilerin kurumların ihtiyaçlarını karşılamak için gerekli bilgi ve becerilere sahip olmalarını sağlamak amacıyla Standartlar'ını ve rehberlerini düzenli olarak geliştirip güncellemektedir. Konu Bazlı Gerekliliklerin yürürlüğe girmesi, geçen yıl uygulamaya alınan yeni Küresel İç Denetim Standartları™ ve diğer küresel rehberleri de içeren UMUÇ dönüşüm projesinin parçasıdır.

Konu Bazlı Gereklilikler "genellikle yüksek risk taşıyan ve yaygın nitelikte olan, sık denetlenen küresel konulara" yöneliktir. Konu Bazlı Gereklilikler, olgun risk alanlarını ele alacak ve yerleşik en iyi uygulamalar temelinde rehberlik sunacaktır. Siber güvenlik hakkındaki bir konu bazlı gereklilik bu ayın başında yayınlanmıştır ve diğer yedi konu bazlı gereklilik ise geliştirme aşamasındadır.

Planlanan Konu Bazlı Gereklilikler

Önümüzdeki birkaç yıl içinde yayımlanması beklenen Konu Bazlı Gereklilikler aşağıdaki başlıkları içermektedir:

Siber güvenlik	Yolsuzluk/rüşvet ile mücadele
Üçüncü taraf	İnsan yönetimi
Kültür	Suistimal riski yönetimi
İş yılmazlığı	Sürdürülebilirlik/ÇSY

İlk Konu Bazlı Gereklilik olarak siber güvenliğe öncelik verilmiştir çünkü kurumlar faaliyetlerinin çoğunda veya tamamında internete yüksek derecede bağımlıdır ve internet bazında sınırlarının korunması gerekmektedir.

İç denetçiler, siber güvenlik sorunlarının yarattığı tehdidin oldukça farkındadır. En güncel küresel IIA Risk in Focus raporunda, iç denetim liderleri siber güvenliği şu anda ve önümüzdeki yıllarda en yüksek risk olarak belirlemekle kalmamış, aynı zamanda önümüzdeki üç yıl boyunca kurumları için en büyük tehdit olmaya devam etmesini bekledikleri de belirtmişlerdir.

Bu ankete katılanlar yapay zekâ (AI), üretken yapay zekâ (GenAI) ve yeni diğer yeni teknolojilerle ilişkili riskleri içeren dijital bozulma hakkında da endişelidirler. Katılımcılar, dijital bozulmayı şu an ve önümüzdeki yıl için en önemli beş risk arasında alt sıralarda değerlendirmiş olsa da, önümüzdeki üç yıl için bu riski ikinci sıraya taşımışlardır. GenAI tehditlerin ve zafiyetlerin tespit edilmesini kolaylaştırırken, aynı zamanda kötü niyetli kişilerin daha karmaşık ve etkili saldırılar yapmasını da kolaylaştırmaktadır.

Konu Bazlı Gerekliliklerin Kullanılması

Konu Bazlı Gereklilikler, iç denetçilerin yaygın risk alanlarını ele alma biçimlerini resmiyete döker. Bu gereklilikler:

- İç denetim fonksiyonlarının kurumdaki riski azaltma çabalarında kullanabilecekleri bir taban çizgisi belirlemektedir.
- İlgili güvence hizmetleri için zorunludur ve danışmanlık hizmetlerinde dikkate alınmaları tavsiye edilmektedir.
- Bir Konu Bazlı Gerekliliğin sahada uygulanabilir olup olmadığının risk temelli denetim planında tespit edilmesini gerektirmektedir. Risk değerlendirmesinin iç denetim yöneticisinin planlamasında önemli bir unsur olduğu göz önüne alındığında, söz konusu değerlendirmenin kurumun stratejileri, hedefleri ve risklerinin değerlendirmesine dayanarak yapılmasını öngörmektedir.
- Her bir konu alanında denetim için küresel olarak tutarlı bir yaklaşım belirlemektedir; bu da iç denetim hizmet ve sonuçlarının güvenilirliğini iyileştirecektir.
- Siber güvenlik güvence hizmetlerinin yürütülmesi için ilgili kriterler sağlamaktadır.
- Kurumun genelini etkileyen alanlarda hem iş birimi hem de organizasyon genelinde uygulanmalıdır.
- Kurumun en azından radarında olması gereken yaygın riskleri tanımlamaktadır.
- Uygun siber risk kapsamı ve tutarlılığı sağlamak suretiyle değer katmaktadır.
- Bir güvence görevinde tüm boyutların ele alınması gerektiği anlamına gelmemektedir. Daha ziyade, konuya ilişkin tutarlı ve güvenilir bir değerlendirme için asgari gereklilikleri belirlemektedirler.

Bu gereklilikler, iç denetçilerin onları mantıklı ve yerinde kullanmalarını sağlayacak şekilde tasarlanmaktadır. Bu gerekliliklerin nasıl uygulanabileceğini anlamak amacıyla, iç denetim planlama sürecinde siber güvenliğin kurum için yaygın veya kapsamlı bir risk olarak belirlendiği ve bu konuda bir denetimin gerçekleştirileceği bir durumu düşünün. Bu durumun Konu Bazlı Gerekliliğin uygulanması gereken bir durum olduğu açıktır ancak tüm durumlar bu kadar açık olmayacaktır.

Örneğin, internet üzerinden satın alma siparişi talep süreciyle ilişkilendirilen siber riskler hakkında bilgi edinen ve tedarikçilere borçlar hesabı denetimi yapan bir iç denetim ekibini göz önünde bulunduralım. Siber güvenlik denetim planında genel bir kurumsal risk olarak tanımlanmamış olsa bile, iç denetim yine de Konu Bazlı Gerekliliği uygulayacaktır ama uygulama kapsamı daha dar olacaktır. Ekip, bu denetimde yönetişim veya risk yönetimi boyutundan ziyade siber güvenlik kontrolleri kısmına daha fazla zaman ayırabilir. İç denetçiler, görevi belirli bir kısımla sınırlandırmış olmalarının gerekçelerini kayıt altına alacaktırlar.

IIA Hakkında

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

The IIA

1035 Greenwood Blvd.
Suite 401
Lake Mary, FL 32746 ABD

Ücretsiz Abonelik

Ücretsiz abonelik kaydınızı yapmak için theiia.org/Tone adresini ziyaret edin.

Okuyucu Geribildirimi

Sorularınızı/Yorumlarınızı gönderin: **Tone@theiia.org.**

Siber Güvenlik Yönetişimi, Risk Yönetimi ve Kontrolleri

Belirtildiği üzere, Konu Bazlı Gereklilikler her bir konu alanındaki yönetişim, risk yönetimi ve kontrolleri ele alacaktır. Yönetişim şemsiyesinin altında, iç denetçiler kurumun yönetişim süreçlerinin siber güvenliği yeterince ele alıp almadığını değerlendirmek zorundadırlar. Siber güvenlik yönetişimi, şirketin amaçlarını, politikalarını ve prosedürlerini ileriye taşıyan ilgili hedef ve stratejileri tanımlamaktadır.

Gerekliliğin iletişim bölümü, yönetim kurulunun siber güvenlik stratejisi, risk, hedefler ve kontroller hakkında ne tür belgelerle bilgilendirildiğini ele alır ve stratejik girişimlerin siber güvenliği destekleyip desteklemediğini göz önünde bulundurur. Bu bölüm siber güvenlik amaçlarına ulaşmak için oluşturulan politika ve prosedürler ile rol ve sorumlulukları, paydaşlarla yürütülen etkileşimi ve siber güvenlik amaçlarını karşılamaya yönelik kaynak gereksinimlerini de ele almaktadır.

Siber güvenlik risk yönetimi bölümü, siber tehditlerin belirlenmesi, analiz edilmesi, yönetilmesi ve izlenmesi için bir süreç oluşturulması gerekliliğini ortaya koymaktadır. Bu kapsamda, belirlenen risklerin hızlı bir şekilde üst yönetime iletilmesini sağlayacak bir sürece de ihtiyaç duyulduğunu belirtir. Temel amaç, siber güvenlik risk yönetiminin kurumsal risk yönetimi açısından öncelik olmasını sağlamaktır.

Siber güvenlik kontrolleri, siber riskleri azaltmak için periyodik olarak değerlendirilen süreçlerdir. Yedi kontrol süreci, iç denetçilerin siber güvenlik denetimi yaparken değerlendirmeleri gereken temel ve önemli hususları kapsar.

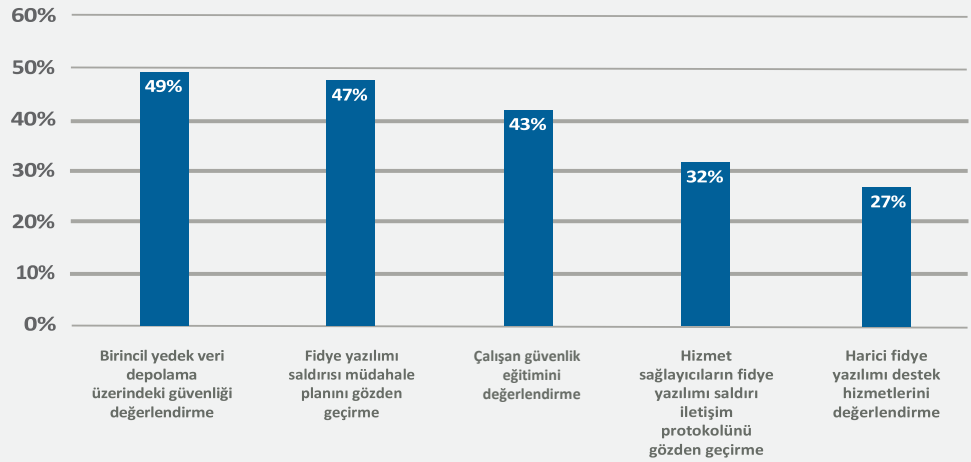
Yaygın ve Gelişen Risklerin Ele Alınması

Derin ve bütünsel bilgi birikimleri sayesinde iç denetçiler kurumu etkilemesi daha muhtemel olan belirli bazı riskleri fark etme konusunda benzersiz bir yetkinliğe sahiptir. "İç Denetimin Siber Güvenliğe Katkısı" başlıklı şema, iç denetimin güvence ve bilgi sağladığı mevcut katkı alanlarının çoğunu ortaya koymaktadır.

Farklı sektörlerden iç denetim liderleri ve diğer uzmanlardan oluşan küresel bir grup tarafından geliştirilen Konu Bazlı Gereklilikler iç denetim mesleğinin yaptığı işleri daha da ileri taşıyarak denetçilerin yaygın ve gelişen riskleri daha iyi ele almalarını sağlayacaktır.

İç Denetimin Siber Güvenliğe Katkısı

Danışmanlık ve istihdam firması Jefferson Wells'e göre *"İç denetim ekiplerinin bilgi güvenliğini kurum içinde ya da üçüncü bir tarafın yardımıyla bağımsız olarak değerlendirme uygulaması yıllar içinde istikrarlı bir şekilde devam etmiştir."* Bununla birlikte, belirli bazı siber güvenlikle ilişkili görevler için iç denetim ekiplerini kullanan şirketlerin yüzdesini gösteren aşağıdaki şema, birçok kurumun iç denetimin sunabileceği bilgi ve danışmanlıktan bütünüyle faydalanmadıklarına işaret etmektedir.

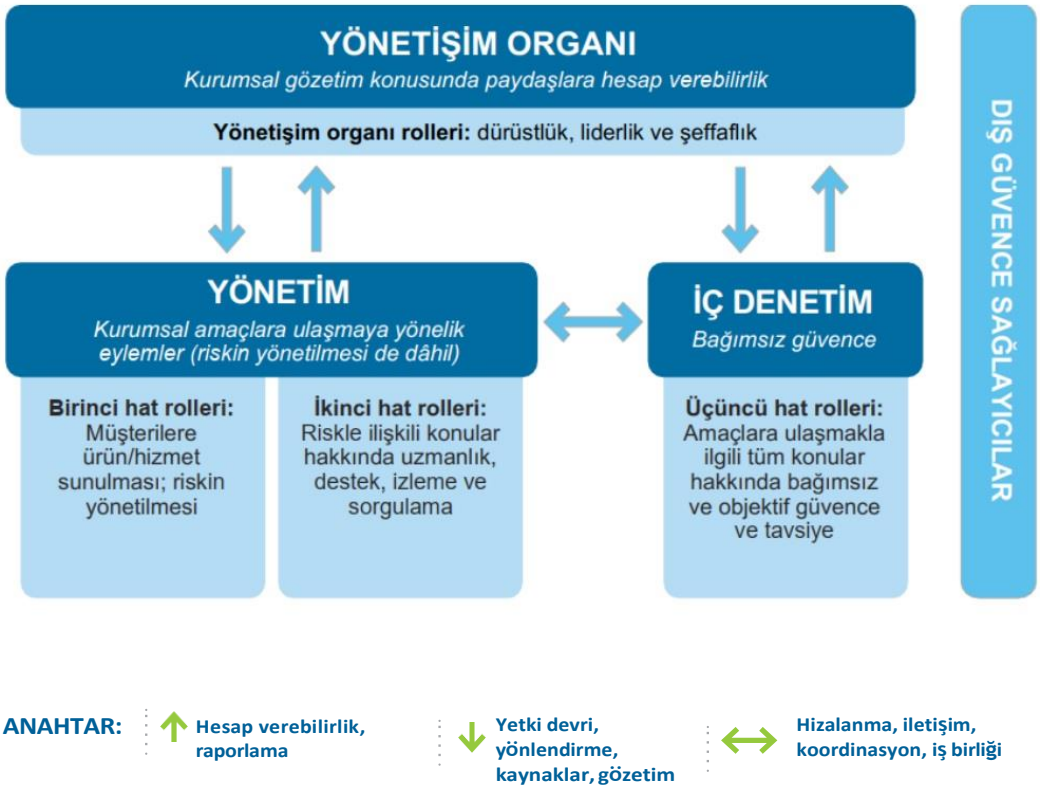


Kaynak: 2024 Internal Audit Priorities Annual Survey, Jefferson Wells.

Üçlü Hat Modeliyle Bağlantılı Konu Bazlı Gereklilikler

IIA, Konu Bazlı Gereklilikleri geliştirirken Üçlü Hat Modelini kullanmıştır. Bu kapsamda, yönetişim ve gözetim unsurları kurumun yönetişim organına, risk yönetimi ikinci hatta, kontroller ve kontrol süreçleri ise birinci hatta karşılık gelir. Üçüncü hat olan iç denetim fonksiyonu ise bağımsız güvence sağlar.

IIA'nın Üçlü Hat Modeli



YÖNETİM KURULU ÜYELERİ İÇİN SORULAR

1. En büyük zafiyetlerimiz nelerdir?
2. Kurum ne tür siber saldırılara maruz kalabilir?
3. Bu saldırıların arkasında ne tür saldırganlar olabilir?
4. Bu saldırgan ne elde etmek istiyor olabilir — işleri aksatmak, veri veya ticari bilgi varlıklarını çalmak, fidye almak ya da başka bir amacı mı var?
5. Bir saldırıyı nasıl gerçekleştirebilirler?
6. Bir saldırı olduğunu nasıl bileceğiz? Anında müdahale etmeye hazır mıyız?
7. İç denetimin siber güvenlik risklerini ele alma konusunda sunabileceği güvence ve danışmanlıktan en iyi şekilde faydalanıyor muyuz?
8. Siber güvenliğe yardımcı olması için yapay zekâ kullanıyor muyuz? Eğer kullanıyorsak, nasıl kullanıyoruz? Eğer kullanmıyorsak, yapay zekâ kullanmayı düşündük mü?