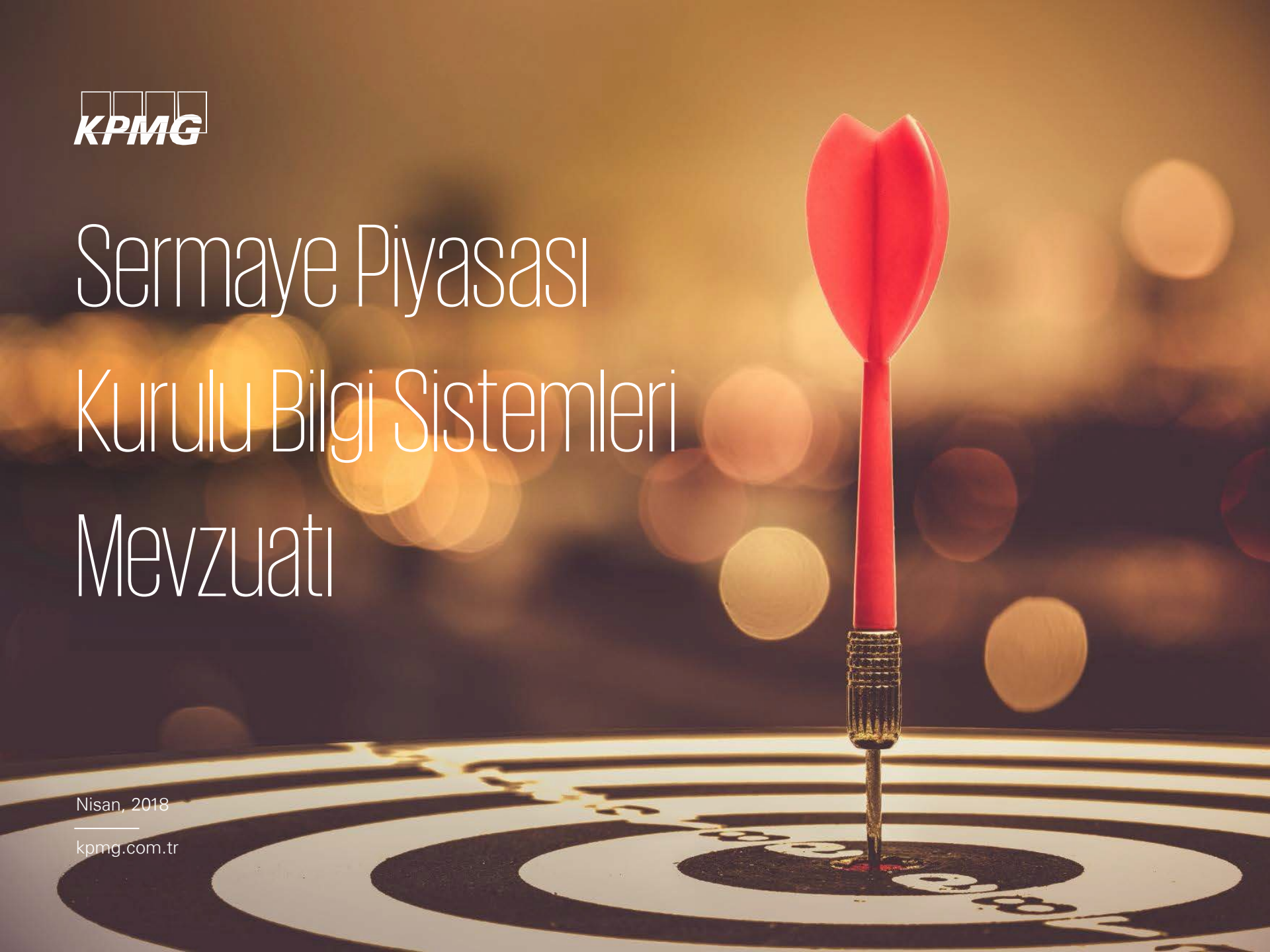


Sermaye Piyasası Kurulu Bilgi Sistemleri Mevzuatı

Nisan, 2018

kpmg.com.tr

Mevzuat

Bilgi Sistemleri Yönetimi ve Denetimi

Bilgi Sistemleri Yönetimi Tebliği ve Bilgi Sistemleri Bağımsız Denetim Tebliği 05.01.2018 tarih 30292 sayılı Resmi Gazete'de yayımlanmış ve yayımı tarihinde yürürlüğe girmiştir.

Bilgi Sistemleri Bağımsız Denetim Tebliği	Bilgi Sistemleri Yönetimi Tebliği
Bağımsız denetim kuruluşlarının yetkilendirilmesi ve denetim sonuçlarının raporlanmasına ilişkin usul ve esaslar	SPK tarafından kurum, kuruluş ve ortaklıkların bilgi sistemlerinin yönetimine ilişkin usul ve esaslar

08.03.2018 tarihinde SPK tarafından yapılan ek duyuru ile bilgi sistemleri bağımsız denetim zorunluluğu bulunmayan halka açık ortaklıkların BSY'nin 26/1 maddesi uyarınca, **birincil sistemlerini yurtiçinde bulundurma zorunlulukları ortadan kaldırılmıştır.**

Mevzuat

Denetim Periyodu

SPK tarafından yayımlanan tebliğ kapsamında denetime tabi olan Kurum, Kuruluş ve Ortaklıkların denetim periyotları ve denetim başlangıç tarihleri aşağıdaki tabloda yer almaktadır.

Denetim çalışmaları 1 Ocak – 31 Aralık dönemini kapsayacak şekilde gerçekleştirilecektir.

Kurum, Kuruluş ve Ortaklıkları	Denetim Periyodu	Denetim Başlangıç Tarihi
Borsa İstanbul A.Ş., İstanbul Takas ve Saklama Bankası A.Ş., Merkezi Kayıt Kuruluşu A.Ş., borsalar ve piyasa işleticileri, teşkilatlanmış diğer pazar yerleri, merkezi takas kuruluşları, merkezi saklama kuruluşları ve veri depolama kuruluşları	Her yıl	2018
Kısmî ve Geniş Yetkili Aracı Kurumlar, asgari özsermaye yükümlülüğü 5 Milyon TL'den fazla olan portföy yönetim şirketleri	2 Yılda bir	2019
Asgari özsermaye yükümlülüğü 5 Milyon TL ve az olan portföy yönetim şirketleri ve Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu A.Ş.	3 Yılda bir	2020
Dar yetkili aracı kurumlar, varlık kiralama şirketleri, ipotek finansmanı kuruluşları, Türkiye Sermaye Piyasaları Birliği, Türkiye Değerleme Uzmanları Birliği, bağımsız denetim, derecelendirme ve değerleme kuruluşları, halka açık ortaklıklar, varlık finansmanı fonları, kolektif yatırım kuruluşları, emeklilik yatırım fonları, konut finansmanı fonları	Periyodik denetim zorunluluğu bulunmamaktadır	

Mevzuat

Bilgi Sistemleri Bağımsız Denetim Sözleşmesi

- Denetim sözleşmesi, denetime tabi dönemin ilk 4 ayı içerisinde imzalanır. BDS 210 Bağımsız Denetimi Sözleşmesinin Şartları Üzerinde Anlaşmaya Varılması Standardı hükümleri, BS bağımsız denetim sözleşmesi bakımından kıyasen uygulanır. 20. Madde ile getirilen 4 aylık sınırlama, ilk denetim dönemi için uygulanmaz.

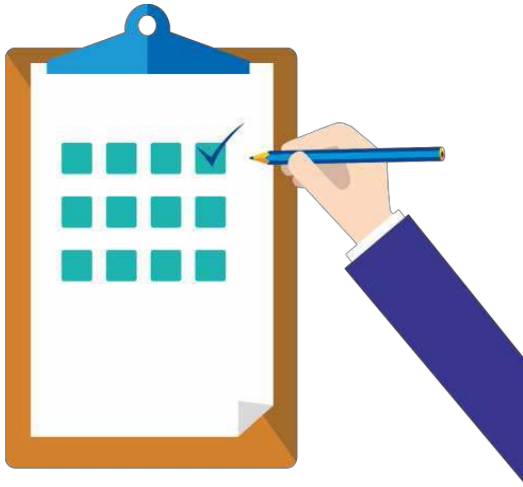
- Sözleşmenin imzalanmaması halinde, konu en geç durumun ortaya çıktığı tarihi izleyen ilk iş gününde Kurula bildirilir.

- Bir yetkili kuruluşun, Kurum, Kuruluş ve Ortaklıklara vereceği bilgi sistemleri bağımsız denetim hizmetinin azami süresinin belirlenmesinde 13/1/2011 tarihli ve 6102 sayılı Türk Ticaret Kanununun 400 üncü maddesinin ikinci fıkrası hükmü uygulanır.

  - "Bir bağımsız denetleme kuruluşu denetçisi yedi yıl arka arkaya o şirket için denetleme raporu vermişse, o denetçi en az iki yıl için değiştirilir." ifadesi ile bağımsız denetim kuruluşu yerine kuruluş denetçisinin rotasyonu zorunlu kılınmıştır.

- İmzalanan sözleşmeler en geç 6 iş günü içinde Kurul'a gönderilmek zorundadır.

- Yetkili kuruluşla denetlenen anlaşarak sözleşmeyi sona erdiremezler. Ancak denetlenen yazılı gerekçe göstermek koşuluyla Kurul onayı ile sona erdirebilir.



Mevzuat

Denetim Kapsamı – Bilgi Sistemleri Denetimi

SPK Bilgi Sistemleri Yönetimi Tebliği'nde belirtilen ve denetime konu olacak bilgi sistemlerinin yönetimine ilişkin konu başlıkları aşağıda yer almaktadır:

Denetim Kapsamı Maddesi	COBIT 4.1	ISO27001
Bilgi Sistemleri Yönetimi	✓	✓
Bilgi Güvenliği Politikası	✓	✓
Üst Yönetimin Gözetimi ve Sorumluluğu	✓	✓
Bilgi Sistemleri Risk Yönetimi	✓	✓
Bilgi Sistemleri Kontrollerinin Tesisi ve Yönetimi		
Varlık Yönetimi	✓	✓
Görevler Ayrılığı Prensibi	✓	✓
Fiziksel ve Çevresel Güvenlik	✓	✓
Ağ Güvenliği	✓	✓
Kimlik Doğrulama	✓	✓
Yetkilendirme	✓	✓
İşlemlerin, Kayıtların ve Verilerin Bütünlüğü	✓	✓
Veri Gizliliği	✓	✓
Bilgi Sistemlerine İlişkin Dış Kaynak Yoluyla Alınan Hizmetlerin Yönetimi	✓	✓
Müşteri Bilgilerinin Gizliliği		
Müşterilerin Bilgilendirilmesi		
Üçüncü Taraflarla Bilgi Değişimi	✓	✓
Kayıt Mekanizmasının Oluşturulması		
Bilgi Güvenliği İhlaili	✓	✓
Bilgi Sistemleri Edinimi, Geliştirilmesi ve Bakımı	✓	✓
Bilgi Sistemleri Sürekliliği	✓	✓
Değişiklik Yönetimi	✓	✓

Mevzuat

Denetim Kapsamı – Sızma Testi

Sızma testi konusunda ulusal veya uluslararası belgeye sahip gerçek veya tüzel kişiler tarafından en az yılda bir kez sızma testi yaptırılması zorunlu tutulmuştur.

Bilgi sistemleri sızma testine ilişkin uygulanacak metodoloji tebliğ kapsamında belirlenmiş olup, gerçekleştirilecek testler asgari olarak aşağıdaki gibi belirlenmiştir;

Kapsam

- İletişim Altyapısı ve Aktif Cihazlar
- DNS Servisleri
- Etki Alanı ve Kullanıcı Bilgisayarları
- E-posta Servisleri
- Veritabanı Sistemleri
- Web Uygulamaları
- Mobil Uygulamalar
- Kablosuz Ağ Sistemleri
- Dağıtık Servis Dışı Bırakma Testleri
- Sosyal Mühendislik Testleri

Sızma Testi Raporu

- Sızma testi, tebliğ kapsamında gerçekleştirilecek bilgi sistemleri denetimi raporundan bağımsız olarak ayrı bir rapor olarak hazırlanacaktır.
- Yönetim Kurulunca onaylanan ve sızma testi sonucunda çıkan bulguların en kısa sürede giderilmesini amaçlayan bir aksiyon planı çerçevesinde takip edecek bir yapı kurulmalıdır.
- Sızma testleri sonucunda ortaya çıkan tespitler, gerek görülmesi halinde teftiş kurullarının iç denetim planına dahil edilmelidir.
- Sızma testi raporları, tamamlanmasını müteakip bir ay içinde Kurula gönderilmelidir.

Mevzuat

Denetim Kapsamı – Yönetim Beyanı

Denetlenen Kurum, Kuruluş ve Ortaklıklar, bilgi sistemlerine ilişkin iç kontrolleri hakkında denetim dönemi itibariyle güvence veren ve yönetim kurulu tarafından onaylanmış olan yönetim beyanını bilgi sistemleri denetçisine sunmakla yükümlüdür. Yönetim beyanı kapsamında açık ve kesin ifadelerle asgari olarak yer alması gereken ifadeler tebliğ kapsamında belirtilmiştir.

Kapsam

- Denetlenen Kurum, Kuruluş ve Ortaklıklar, hazırlayacakları yönetim beyanı çerçevesinde bilgi sistemlerine ilişkin iç kontrollerin etkinlik, yeterlilik ve uyumluluğuna ilişkin kanaat oluştururken, Tebliğde uymak ile yükümlü olduğu bilgi sistemleri bağımsız denetim kapsamını dikkate almalıdır.
- Yönetim beyanı sadece bilgi sistemlerine ilişkin iç kontroller hakkında düzenlenir. Yönetim beyanı oluşturulurken alınan destek hizmetleri de göz önünde bulundurulmalıdır.
- Yönetim beyanı çalışmasında 1 Ocak – 31 Aralık döneminin esas alınması beklenmektedir.

Mevzuat

Denetim Kapsamı – Muafiyet

SPK Bilgi Sistemleri Yönetimi Tebliği içerisinde muaf olunan durumlara ilişkin tanımlamalar aşağıdaki şekilde yapılmıştır;

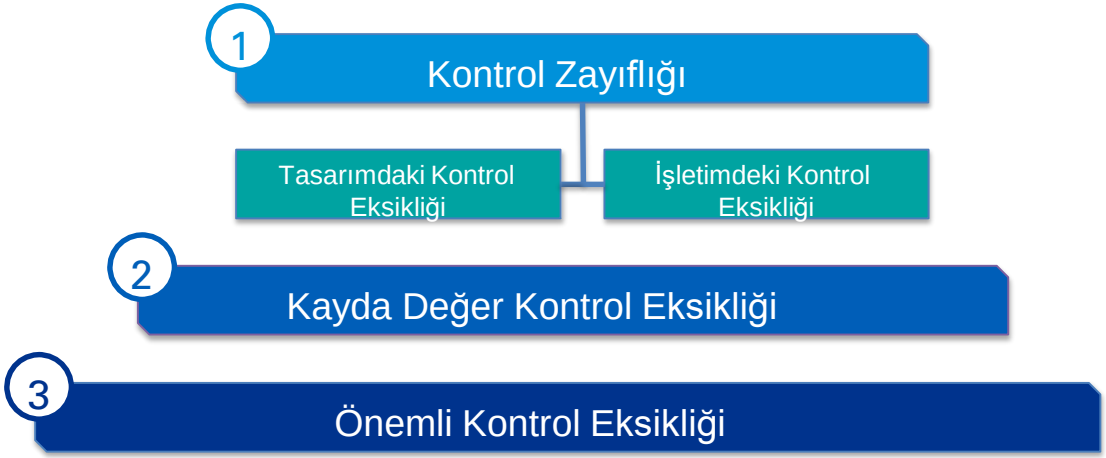
Kurum, Kuruluş ve Ortaklıkları	Muaf Olunan Tebliğ Maddesi	Muaf Olunan Tebliğ Maddesinin Fıkrası ve Benti
Asgari özsermaye yükümlülüğü 5 milyon TL ve daha az olan portföy yönetim şirketleri ve Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu A.Ş.	Bilgi Güvenliği İhlali (Madde 24) Değişiklik Yönetimi (Madde 27)	-
Dar yetkili aracı kurumlar, varlık kiralama şirketleri, ipotek finansmanı kuruluşları, Türkiye Sermaye Piyasaları Birliği, Türkiye Değerleme Uzmanları Birliği, bağımsız denetim, derecelendirme ve değerleme kuruluşları, halka açık ortaklıklar, varlık finansmanı fonları, kolektif yatırım kuruluşları, emeklilik yatırım fonları, konut finansmanı fonları	Üst Yönetimin Gözetimi ve Sorumluluğu (Madde 7)	5
	Bilgi Sistemleri Risk Yönetimi (Madde 8)	4,5
	Kimlik Doğrulama (Madde 14)	3
	Yetkilendirme (Madde 15)	3
	Veri Gizliliği (Madde 17)	2
	Bilgi Sistemlerine İlişkin Dış Kaynak Yoluyla Alınan Hizmetlerin Yönetimi (Madde 18)	4
	Kayıt Mekanizmasının Oluşturulması (Madde 22)	2
	Bilgi Güvenliği İhlali (Madde 24)	-
	Bilgi Sistemleri Edinimi, Geliştirilmesi ve Bakımı (Madde 25)	1 (b,d,ğ)
	Bilgi Sistemleri Sürekliliği (Madde 26)	3
	Değişiklik Yönetimi (Madde 27)	-

* Bilgi sistemleri bağımsız denetim zorunluluğu bulunmayan halka açık ortaklıklar BSY'nin Bilgi Sistemleri Sürekliliği Madde 26'nın 1'nci fıkrasından muaftır.

Mevzuat

Denetim Kapsamında Tespitlere İlişkin Önemlilik Kavramları

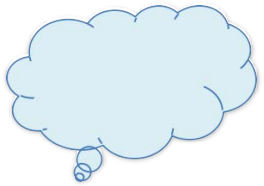
Bilgi sistemleri denetçisi, incelemeleri neticesinde ulaştığı tespitlere konu kontrol zayıflıkları ve eksikliklerini önemlilik kavramına göre tasnif etmede aşağıda belirtilen kriterleri kullanır:



Mevzuat

Denetim Raporu

Görüş



Bilgi Sistemleri Bağımsız Denetim Görüş Oluşturulması

Denetçiler, herhangi bir önemli kontrol eksikliği bulunmadığı ve denetim kapsamında herhangi bir eksiklik ve engelleme ile karşılaşılmadığı durumda tebliğin ekinde bulunan formata uygun olarak olumlu görüş bildirirler.

Şartlı ve olumsuz görüş için gereklilikler, BDDK Bilgi Sistemleri denetimlerindeki gerekliliklere paraleldir.

Bildirim

Bilgi sistemleri bağımsız denetim raporunun kesinleşmesi ve Kurul'a bildirimi

Rapor, denetçi tarafından imzalandıktan bir iş günü sonra denetlenen tarafından yönetim kuruluna iletilir. Denetlenen kuruluş, raporu en geç 5 iş günü içerisinde yönetim kurulu kabul kararıyla birlikte Sermaye Piyasası Kurulu'na iletir.

Rapor, denetim dönemi bitimini izleyen 30 gün içerisinde tamamlanarak kurula gönderilmelidir.

KPMG

Uyum Çalışmaları

Metodoloji

Uyum Çalışmaları

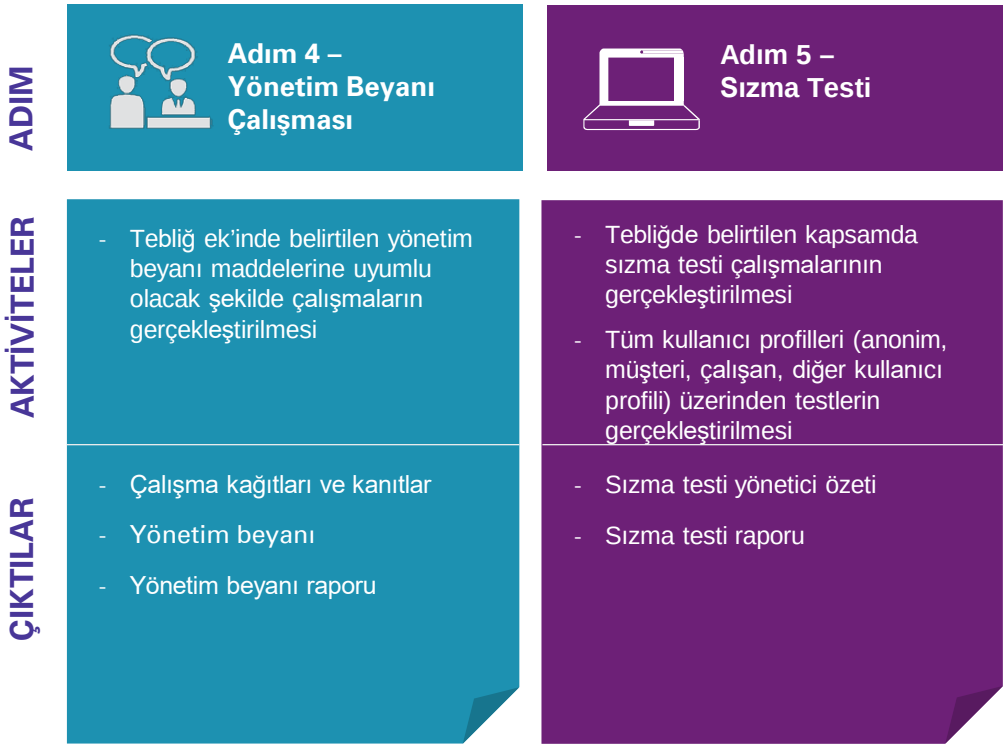
Mevzuatla uyumlu hale gelmek için, öncelikle Tebliğ kapsamında alınması gereken önlemler çerçevesinde bir mevcut durum analizi gerçekleştirilmesini öneriyoruz. İkinci adımda, oluşturulan aksiyon planı kapsamında tespitlere ilişkin önerilerin ve yapılacak geliştirmelerin dokümante edilmesi çalışmaları yürütülmelidir. Üçüncü adımda ise, mevzuat çerçevesinde bulunan maddeler kapsamında bilgi sistemleri denetim çalışmaları yürütülerek, denetime ilişkin rapor çalışmaları gerçekleştirilir.

ADIM	Adım 1 – Mevcut Durum Analizi	Adım 2 – Eksikliklerin İyileştirilmesi	Adım 3 – Bilgi Sistemleri Denetimi
AKTİVİTELER	- Tebliğ kapsamındaki maddelere uyum analizi - Eksikliklerin belirlenmesi - Aksiyon planının oluşturulması	- Tespitlere ilişkin önerilerin ve yapılacak geliştirmelerin dokümante edilmesi	- İlgili mevzuat doğrultusunda uyulması gereken maddeler kapsamında denetim çalışmalarının gerçekleştirilmesi - Yönetim beyanının değerlendirilmesi
ÇIKTILAR	- BT Mevcut Durum Analiz Raporu - BT Süreç İyileştirme ve Aksiyon Planı ve Takvimi	- Üst Yönetim Bilgilendirme Sunumları - Süreç Modeli ve Rol, Yapı ve Araç Önerileri - BT Kontrol Ortamının İyileştirilmesi Kapsamında Hazırlanan Dokümantasyonlar	- Denetim raporu

Metodoloji

Uyum Çalışmaları

Denetim Tebliği'nin eki olan «Yönetim Beyanına İlişkin Esaslar» kapsamında yönetim beyanı çalışmaları gerçekleştirilmelidir. Beşinci adım olarak ise, Yönetim Tebliği'nin ekinde yer alan «Bilgi Sistemleri Sızma Testleri Usul ve Esasları» kapsamında sızma testi çalışmaları yürütülmelidir.



KPMG

Teşekkürler

İletişim

Sinem Cantürk
Şirket Ortağı,
Bilgi Sistemleri Risk Yönetimi
Bölüm Başkanı,
Finansal Hizmetler Sektör Lideri

T: +90 212 316 60 00 - 6037
E: scanturk@kpmg.com

KPMG Türkiye
İstanbul, Levent
İş Kuleleri Kule 3, Kat 2-9
Levent/İstanbul

www.kpmg.com.tr