# SPK Bilgi Sistemleri Düzenlemeleri'ne ne ölçüde uyumlusunuz?

Değerlendirme Raporu

**Nisan 2019**

The better the question. The better the answer.
The better the world works.

Building a better working world

# İçindekiler

# Giriş

Emre Beşli

EY Türkiye Şirket Ortağı
Risk Danışmanlık Hizmetleri Lideri

2006 yılında bankacılık sektöründeki uygulamayla hayatımıza giren ilk bilgi sistemleri denetimi mevzuatının üzerinden yaklaşık 15 yıl geçti. Bu süre zarfında bilgi sistemleri denetimi, kurumların öncelikli konuları arasına girmeyi başardı ve bankacılık dışı sektörlerde de yaygın olarak uygulanmaya başladı. Mevzuat gereklilikleri ise sadece bilgi sistemleri denetimi ile sınırlı kalmayıp, kurumların bilgi sistemleri yönetiminde esas alınacak ilkelerin de tanımlandığı birer rehber halini aldı. SPK'nın 5 Ocak 2018 tarihli bilgi sistemleri düzenlemeleriyle birlikte, bilgi sistemlerine ilişkin uyum ve denetim gereksinimleri sektörel açıdan en geniş sınırlarına ulaşmış bulunuyor.

Düzenlemelerle birlikte ülkemizdeki finansal kuruluşların ve halka açık şirketlerin, dijital dönüşümden kaynaklı riskleri etkin yönetmek üzere oluşturacakları kontrol ortamının güçlü bir olgunluk seviyesine sahip olması gerekiyor.

SPK Bilgi Sistemleri Düzenlemeleri'nin yayımlanmasının ardından, geçmiş örneklerde olduğu gibi fiili uygulamanın nasıl yürütüleceğine ilişkin bazı soruların ortaya çıktığını gözlemledik. Bu çerçevede konuyu etraflıca tartışmak amacıyla, EY Türkiye olarak 12 ve 14 Mart 2019 tarihlerinde Borsa İstanbul ev sahipliğinde bir etkinlik gerçekleştirdik. SPK ve Borsa İstanbul A.Ş. yetkililerinin de katıldıkları bu etkinlikte, 300'den fazla katılımcının katkısıyla birlikte düzenlemelerin uygulanmasına ilişkin meseleleri tartıştık ve mevcut durumu bir anket üzerinden değerlendirmeye çalıştık. Elinizdeki rapor, bu etkinlikte ele alınan konuların ve yapılan araştırmanın bir özetini içeriyor.

SPK'nın kurumların sürdürülebilir büyüme ve dijital dönüşüm yolculuklarını güvence altına almak üzere yayımlamış bulunduğu bilgi sistemleri düzenlemelerinin kurumlarımıza önemli bir değer katacağına inanıyor, raporumuzun bu yolculukta sizlere faydalı olmasını diliyoruz.

# 1

# Mevzuat

## Mevzuat Gereksinimleri Nelerdir?

SPK tarafından 5 Ocak 2018 tarihinde Bilgi Sistemleri Yönetimi Tebliği ve Bilgi Sistemleri Bağımsız Denetim Tebliği yayımlanmış, tebliğler yayımlanma tarihi itibarıyla yürürlüğe girmiştir.

Sermaye Piyasası Kanunu kapsamında faaliyet gösteren kurum, kuruluş ve ortaklıklar, bu düzenlemelere 5 Ocak 2018 tarihi itibarıyla uymakla yükümlü hale gelmiştir.

Uyum yükümlülüklerini sağlayabilmek adına düzenleme kapsamına giren tüm şirketlerin, öncelikli olarak Bilgi Sistemleri Yönetimi Tebliği kapsamında belirlenen ilkeleri ve kontrol hedeflerini sağlayacak Bilgi Teknolojileri kontrol ortamını oluşturması, izlemesi ve sürdürülebilir şekilde yönetmesi beklenmektedir.

Uyum yükümlülüğünün ikinci temel gereksinimi olarak ise, Bilgi Sistemleri Bağımsız Denetim Tebliği kapsamında belirtilen takvime uygun olarak şirketlerde bağımsız bilgi sistemleri denetimi gerçekleştirilmesi ve ek olarak şirketlerin yönetim beyanı hazırlamak üzere gerekli iç kontrol yapısını tasarlaması ve işletmeye başlaması beklenmektedir.

## Bilgi Sistemleri Yönetimi Tebliği

5 Ocak 2018 tarihli Bilgi Sistemleri Yönetimi Tebliği kapsamında kontrol alanları bazında ilkesel yaklaşımlar belirlenmiş olup bu doğrultuda tasarlanacak BT kontrol ortamına yönelik teknik gereksinim ve aksiyonların şirketlerin kendi organizasyonel ve operasyonel işleyişine göre belirlenmesi gerekmektedir. Bilgi Sistemleri Yönetimi Tebliği kapsamında düzenlenen BT kontrol alanları aşağıdaki gibidir:

- Bilgi sistemleri yönetiminin oluşturulması, hayata geçirilmesi
- Bilgi güvenliği politikası
- Üst yönetimin gözetimi ve sorumluluğu
- Bilgi sistemleri risk yönetimi
- Bilgi sistemleri kontrollerinin tesisi ve yönetilmesi
- Varlık yönetimi
- Görevler ayrılığı prensibi
- Fiziksel ve çevresel güvenlik
- Ağ güvenliği
- Kimlik doğrulama
- Yetkilendirme
- İşlemlerin, kayıtların ve verilerin bütünlüğü
- Veri gizliliği
- Dış kaynak hizmetlerinin yönetimi
- Müşteri bilgilerinin gizliliği
- Müşterilerin bilgilendirilmesi
- Üçüncü taraflarla bilgi değişimi
- Kayıt mekanizmasının oluşturulması
- Zaman senkronizasyonu
- Bilgi güvenliği ihlali (Halka açık şirketlere zorunlu değildir.)
- Bilgi sistemleri edinimi, geliştirilmesi ve bakımı
- Bilgi sistemleri sürekliliği
- Değişiklik yönetimi (Halka açık şirketlere zorunlu değildir.)

# Bilgi Sistemleri Bağımsız Denetim Tebliği

Bilgi sistemleri yönetimi ve işletimi kapsamında yer alan faaliyet, yazılım ve donanım gibi bilgi sistemi unsurları ile bu sistemler dahilinde tesis edilen kontrollerin Bilgi Sistemleri Yönetimi Tebliği'ne uyum açısından SPK tarafından yetkilendirilmiş olan bağımsız bilgi sistemleri denetçileri tarafından değerlendirilmesi gerekmektedir. Bu süreci düzenlemek üzere 5 Ocak 2018 tarihli Bilgi Sistemleri Bağımsız Denetim Tebliği yayımlanmıştır.

Bağımsız bilgi sistemleri denetimi ile, SPK BT düzenlemeleri kapsamındaki bilgi sistemlerinin ve bu sistemlere ilişkin kontrollerinin bilgi sistemleri yönetim ilkeleri doğrultusunda yeterlilik, etkinlik ve uyumluluğu hakkında görüş oluşturulması amaçlanmaktadır. Bağımsız bilgi sistemleri denetim görüşü türleri aşağıdaki gibidir:

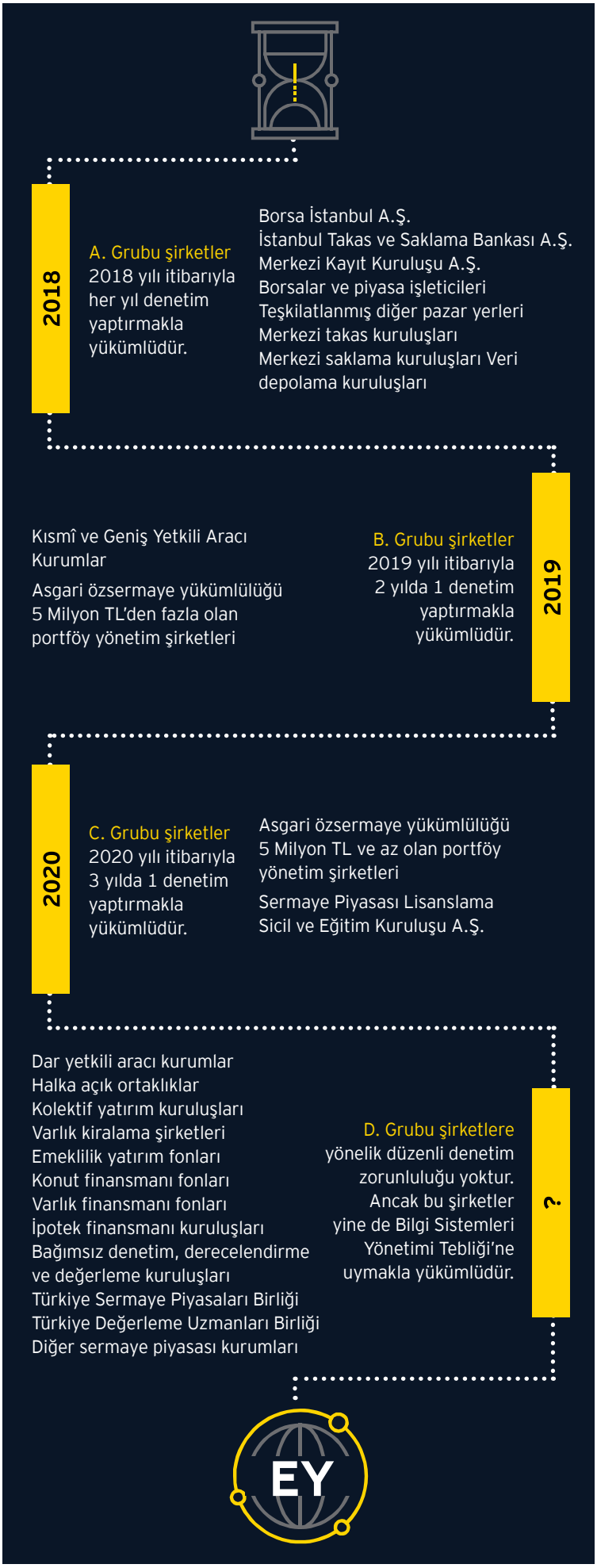
- Olumlu Görüş
- Olumsuz Görüş
- Şartlı Görüş
- Görüş Bildirmekten Kaçınma

Bilgi Sistemleri Bağımsız Denetim Tebliği kapsamında, Sermaye Piyasası Kanunu kapsamında faaliyet gösteren şirketlere yönelik, şirket tipi bazında denetim takvimi ve denetim sıklığı belirlenmiştir. Yandaki şekilde yer verildiği üzere;

- A Grubu şirketler 2018 itibarıyla her yıl,
- B grubu şirketler 2019 itibarıyla 2 yılda 1,
- C grubu şirketler ise 2020 itibarıyla 3 yılda 1 bağımsız bilgi sistemleri denetimi yaptırmakla yükümlüdür.

Halka açık şirketlerin de dahil olduğu D grubu şirketler için bu aşamada denetim zorunluluğu yoktur. Ancak bu şirketler yine de Bilgi Sistemleri Yönetimi Tebliği'ne uymakla yükümlüdür. Bununla birlikte, tüm halka açık şirketlere kademeli bir şekilde bilgi sistemleri denetimi yükümlülüğü getirilmesinin planlandığı bilinmektedir.

Bilgi Sistemleri Bağımsız Denetim Tebliği kapsamında belirtildiği üzere, Bilgi Sistemleri Bağımsız Denetim Sözleşmesinin ilgili denetim döneminin ilk 4 ayı içerisinde imzalanmış olması gerekmektedir. Bu doğrultuda, 2019 dönemi için denetime tabi olan şirketlerin 2019 Nisan ayı sonuna kadar sözleşmelerini imzalamış olmaları gerekmektedir. Sözleşmenin herhangi bir nedenle imzalanamaması halinde, konunun en geç durumun ortaya çıktığı tarihi izleyen ilk iş gününde SPK'ya bildirilmesi yükümlülüğü bulunmaktadır.



# 2

# Sıkça Sorulan Sorular

5 Ocak 2018 tarihli SPK Bilgi Sistemleri Düzenlemeleri'ne yönelik gerçekleştirilen etkinliklerde öne çıkan konular yan tarafta yer almaktadır.

### 1 5 Ocak 2018 tarihli Bilgi Sistemleri Düzenlemeleri'ne yönelik BT uygulama kapsamı nedir ve nasıl belirlenmelidir?

BT uygulamaları kapsamı belirlenirken aşağıdaki hususlar dikkate alınmalıdır;

- Finansal sistemler/muhasebe sistemleri kapsama dahil edilmelidir ancak kapsam için tek kriter finansal etki değildir.
- Sermeye Piyasası Kanunu ve alt düzenlemeleri kapsamında yürütülen tüm faaliyetleri destekleyen bilgi teknolojileri uygulamaları ve sistemlerinin SPK BT düzenlemeleri kapsamında değerlendirilmesi gerekmektedir.
- Finansal etkinin yanı sıra ilgili uygulamaların iş sürekliliğine, veri gizliliğine etkileri de değerlendirilmelidir.
- Risk odaklı bir yaklaşım gözetilerek sistem mimarisi kapsamında bir sistemdeki açığın/zaafiyetin diğer sistemlerdeki açıklıkları/zafiyetleri tetikleme ihtimali değerlendirilmelidir.
- Bu çerçevede, geniş bir uygulama kapsamının değerlendirmeye alınması beklenmektedir.

### 2 Halka açık şirketler için öngörülen bir denetim takvimi bulunmakta mıdır?

- Halka açık şirketler için denetim yükümlülüğünün kademeli bir şekilde getirilmesi planlanmaktadır.
- Kademeli geçiş planı için BIST endeks değerinin kullanılabileceği veya sektör bazında önceliklendirme yapılabileceği belirtilmiştir.

### 3 SPK Bilgi Sistemleri Bağımsız Denetim Tebliği kapsamında bulunmayan şirketlerin yönetim beyanı hazırlama yükümlülüğü var mıdır?

Yönetim Beyanı denetçiye verilen bir beyan olduğu için denetim yükümlülüğü bulunmayan şirketlerin yönetim beyanı hazırlama yükümlülüğü bulunmamaktadır.

### 4 Bulut bilişim altyapısını kullanmak SPK Bilgi Sistemleri Düzenlemeleri açısından bir uyumsuzluk teşkil eder mi?

- Bulut bilişim kavramı SPK BS Düzenlemelerine doğrudan bir uyumsuzluk teşkil etmemektedir.
- Ancak, birincil ve ikincil sistemlerin yurt içinde bulundurulması zorunluğu olduğu için bulut bilişim altyapısının da yurt içinde bulunması gerekmektedir.
- Ayrıca, bulut bilişim dış hizmet kapsamına girdiği için dış hizmet teminine yönelik yükümlülüklerinin de dikkate alınması gerekmektedir.

### 5 Uluslararası ölçekte çalışan şirketler/holdingler için SPK bilgi sistemleri denetim kapsamı yurtiçindeki şirketler/birimlerle mi kısıtlıdır?

- Mevzuatın konsolide denetimden ziyade solo denetimler üzerine hazırlandığı, konsolide denetim beklentisini olmadığı belirtilmiştir.
- Holdinglerin faaliyetlerini yurtiçi veya yurtdışında bağlı ortaklıklar ve iştirakler aracılığı ile gerçekleştirmesi durumunda, holding çatısı altındaki tüm bilgi sistemlerinin yönetim ilkelerine uygun bir şekilde tasarlanması, kontrollerin bu kapsamda tesis edilmesi ve denetlenmesinin hedeflenen amaca ulaşılması bakımından daha doğru olacağı belirtilmiştir.

### 6 Dış hizmetleri firmalarının SPK Bilgi Sistemleri Düzenlemeleri'ne uyumu konusunda nasıl güvence sağlanabilir?

- Herhangi bir dış kaynak kullanımında öncelikle SPK Bilgi Sistemleri Düzenlemeleri'ne uyum gözetilmelidir.
- Dış hizmet firmalarından ISAE 3402 raporu temin edilerek uyum konusunda bir güvence/değerlendirme sağlanabilir.
- ISAE 3402, KGK tarafından GDS 3402 standardı olarak yayımlanmıştır ve ülkemizde geçerlidir.
- ISAE 3402 raporu iki denetçi arasındaki iletişimi sağlayan bir denetim standardıdır. ISAE 3402 kapsamının SPK düzenlemelerini karşılayacak doğru kontrol ve kapsam dahilinde yapılması önemlidir.
- SPK BS düzenlemelerinden doğan yükümlülüklere, dış hizmet firmaları ile imzalanan sözleşmelerde yer verilmeli, eski tarihli sözleşmeler bu doğrultuda güncellenmelidir.

### 7 BDDK konsolide bilgi sistemleri denetimi geçiren şirketler için SPK uyum yükümlülüğü mevcut mudur?

- BDDK konsolide BT denetimine tabi şirketlerde, SPK BT denetiminin de ayrıca gerçekleştirilmesi gerekmektedir.
- Her iki denetimin kapsamında kesişen BT uygulamaları ve süreçleri bulunmakla birlikte, SPK bilgi sistemleri denetim kapsamının daha geniş olması beklenmektedir.

### 8 Bağımsız bilgi sistemleri denetimine tabi olmayan şirketler, SPK tarafından istendiği zaman denetlenebilir mi?

- Bağımsız bilgi sistemleri denetimine tabi olmayan şirketler muafiyet durumları haricinde Bilgi Sistemleri Yönetimi Tebliği'ne uymakla yükümlüdür.
- Sermaye Piyasası Kanunu'nun 88. ve 89. maddeleri uyarınca bir olumsuzluk gözlenmesi durumunda veya SPK Bilgi Sistemleri Düzenlemeleri'ne uyum durumunu sorgulamak amacı ile SPK tarafından istenildiği zaman bilgi sistemleri denetimi gerçekleştirilebilir.

### 9 Bağımsız bilgi sistemleri denetimi sonucunda tespit edilen eksikliklere, olumsuz/şartlı görüş içeren denetim raporlarına yönelik hangi aksiyonlar veya yaptırımlar uygulanabilir?

- Tespit edilen bulguların önemlilik derecesine göre farklı aksiyonlar ve yaptırımlar uygulanması mümkündür.
- Ülkemizdeki benzer düzenlemelerde idari para cezası uygulaması yaygındır.
- SPK tarafından uygulanabilecek yaptırımlara ek olarak, denetim yükümlülüğü olan şirketlerde Yönetim Beyanı hazırlama yükümlülüğü de olduğu için, uyum konusunda tespit edilen eksikliklere yönelik şirketlerin üst yönetimleri tarafından da çeşitli iç yaptırımlar uygulanabilir.

### 10 Küçük bir ekip ve kısıtlı kaynaklarla faaliyetlerini sürdüren şirketler için uyum yaklaşımı nedir?

- SPK Bilgi Sistemleri Düzenlemeleri kapsamında kontrol alanları bazında ilkesel yaklaşımlar belirlenmiş olup, söz konusu ilkelere yönelik tasarlanacak kontrol ortamı şirketin inisiyatifine bırakılmıştır. Dolayısıyla, küçük şirketlerde uyum modeli oluşturulurken şirketinin organizasyonel ve operasyonel yapısı ve işleyişine uygun bir yaklaşım belirlenebilir. Ancak bu modelde mevzuata uyum esas olmalıdır.

# 3

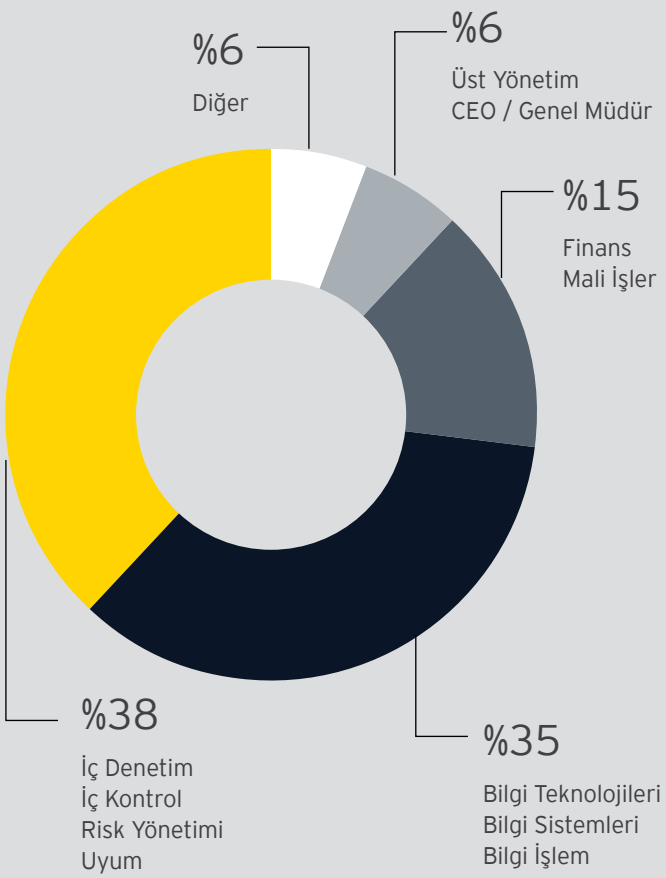
# Anket Sonuçları

## SPK Bilgi Sistemleri Düzenlemeleri Anketi

EY Türkiye'nin SPK Bilgi Sistemleri Düzenlemeleri anketi, kuruluşların düzenlemelere ne kadar uyumlu olduklarını düşündükleri, uyum konusunda alınacak aksiyonları nasıl yöneteceklerini, uyum sürecinde zorlanılacak konuların neler olabileceği konularında genel bir değerlendirmeyi amaçlamaktadır.

12 Mart ve 14 Mart 2019 tarihlerinde düzenlediğimiz anketimize; halka açık şirketler, aracı kurumlar, portföy yönetim şirketleri ve bir çok farklı sektörden katılımcılar yorumlarını iletmiştir.

Katılımcıların Görev Alanları



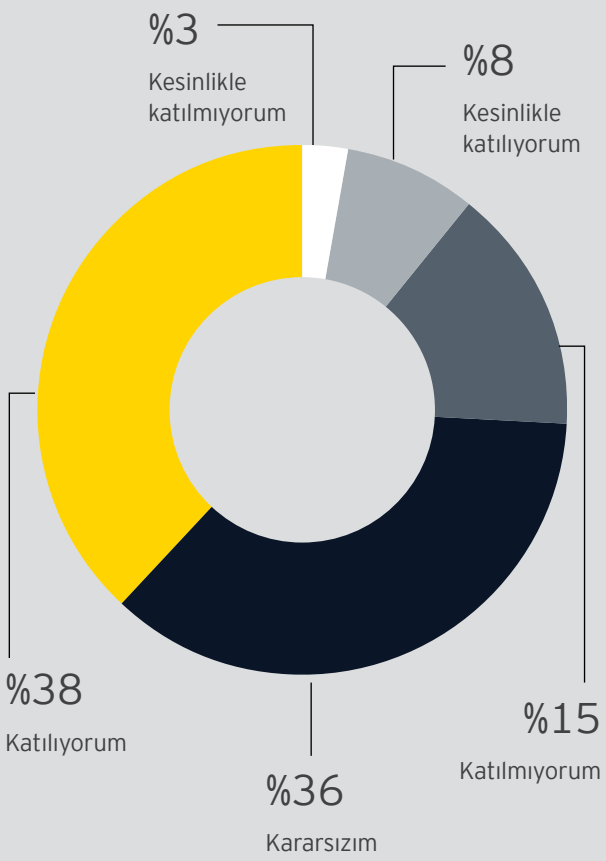

Anket sonuçları, kuruluşların uyum yolculuğunda üzerinde durmaları gereken noktaların altını çizip, potansiyel olgunlaşma noktalarını ortaya koymaktadır.

## 3.1 SPK Bilgi Sistemleri Düzenlemeleri'ne ne ölçüde uyumlusunuz ?

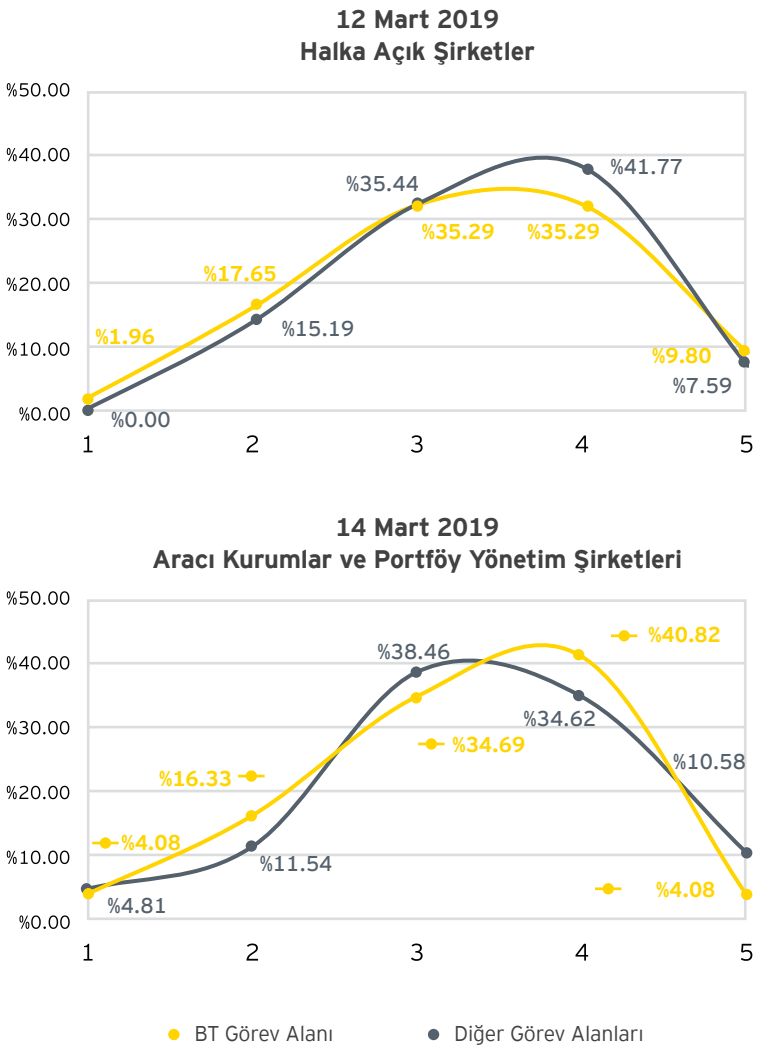
Anketin ilk sorusu olarak katılımcılara, şirketlerinin SPK Bilgi Sistemleri Düzenlemelerine ne kadar uyumlu olduğunu düşündükleri sorulmuştur.

Katılımcıların

**%46** 'sı şirketlerinin uyumlu olduğunu düşünmektedir.




BT alanında görev alan çalışanlar ile diğer alanlarda çalışanların kıyaslanması




1. Kesinlikle katılmıyorum 2. Katılmıyorum 3. Kararsızım 4. Katılıyorum 5. Kesinlikle Katılıyorum

BT ve BT dışı birimlerin kıyaslanması sonucunda verilen cevapların çok büyük ölçüde benzerlik gösterdiği tespit edilmiştir.

## 3.2 Bilgi Sistemleri Düzenlemeleri Uyum Sürecinde Yaşanabilecek Zorluklar

EY Türkiye, düzenleyiciler tarafından daha önce yayımlanmış ve yürürlüğe konulmuş uyum yükümlülüklerine ilişkin tecrübelerinden yola çıkarak, şirketlerin SPK Bilgi Sistemleri uyum yolculuğunda zorlanabilecekleri 8 ana konu başlığı belirlemiştir (*).

Anket katılımcılarına belirlenmiş konuların şirketlerinin uyum konusunda en önemli zorluğu 5'li skalada puanlamaları istenmiştir.

**1.** Organizasyon ve kültür değişim gereksinimleridir.

**2.** Yetkilendirme ve görevler ayrılığı prensibinin uygulanmasıdır.

**3.** Siber güvenliğin sağlanması ve teknik önlemlerin alınmasıdır.

**4.** Politika, prosedür ve yönetişim çerçevelerinin yaygınlaştırılmasıdır.

**5.** İş ve BT sürekliliğinin sağlanmasıdır.

**6.** Destek hizmeti firmalarından kaynaklanan risklerin yönetimidir.

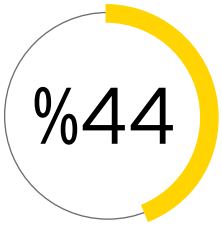
**7.** Teknik uyum konuları için gerekli olabilecek yazılım ve donanımların temini ve uygulanmasıdır.

**8.** Uyum için gerekli kaynakların (insan gücü ve yatırım) teminidir.

(*) Uyum konusunda yaşanabilecek başlıca 8 zorluk

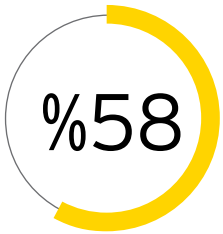
Katılımcıların yapmış oldukları cevaplar değerlendirilmiş ve katılımcıların cevaplarında en yüksek puanı alan uyum zorluğu konuları analiz edilmiştir. Analiz sonuçlarına göre;

**Bilgi Teknolojileri**




Uyum için gerekli kaynakların (insan gücü ve yatırım) temini

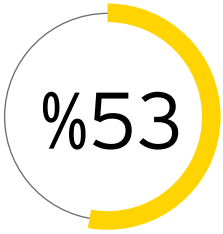
BT alanında görev yapan anket katılımcılarının %44'ü uyum konusunda en zor gördükleri konunun **"uyum için gerekli kaynakların (insan gücü ve yatırım) temini"** olduğunu belirtmiştir.




Siber güvenliğin sağlanması ve teknik önlemlerin alınması

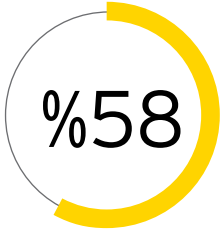
Bu alanda görev yapan katılımcıların %58'i ise uyum konusunda en az zorlanacakları konunun **"siber güvenliğin sağlanması ve teknik önlemlerin alınması"** olduğunu belirtmiştir.

**Diğer Görev Alanları**




Destek hizmeti firmalarından kaynaklanan risklerin yönetimi

BT dışı alanlarda görev yapan anket katılımcılarının %53'ü uyum konusunda en zor gördükleri konunun **"destek hizmeti firmalarından kaynaklanan risklerin yönetimi"** olduğunu belirtmiştir.




Politika, prosedür ve yönetişim çerçevelerinin yaygınlaştırılması

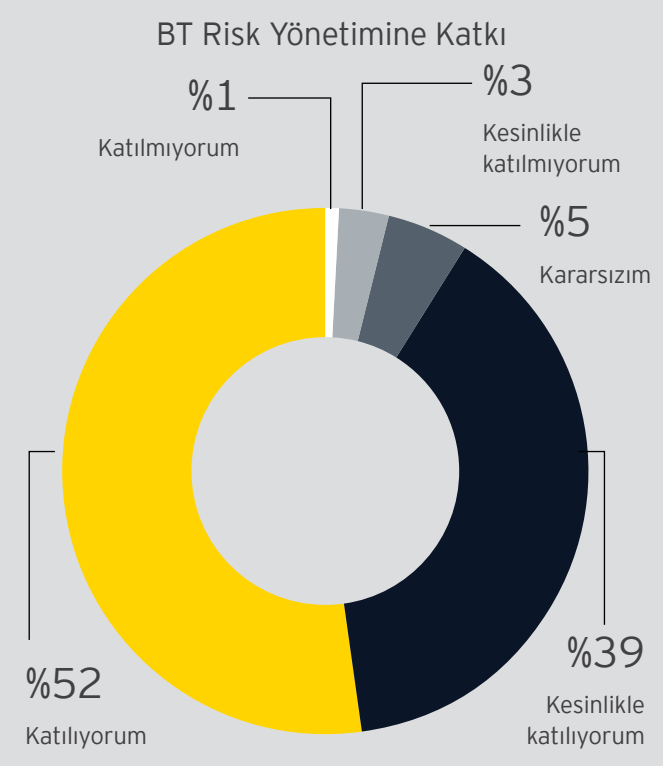
Bu alanda görev yapan katılımcıların %58'i ise uyum konusunda en az zorlanacakları konunun **"politika, prosedür ve yönetişim çerçevelerinin yaygınlaştırılması"** olduğunu belirtmiştir.

Anket sonuçlarından da çıkarılabileceği gibi, "Bilgi Teknolojileri" alanında görev yapan çalışanlar için hakim oldukları alanda aksiyon almak, diğer zorluklara kıyasla daha kolay bulunmuştur. Öte yandan, şirketlerin BT bütçe ve yatırımlarının yetersizliğini adresleyen sonuçlar, bu alanlardaki çalışanlar için en önemli zorluk olarak karşımıza çıkmaktadır. Ek olarak, uyum yolculuğunda görevlendirilecek insan kaynağı sadece BT ile sınırlandırılmamalı, süreç birimlerinden de ilgili kişilerin planlamalara dahil edilmesi gerektiği hatırlanmalıdır.

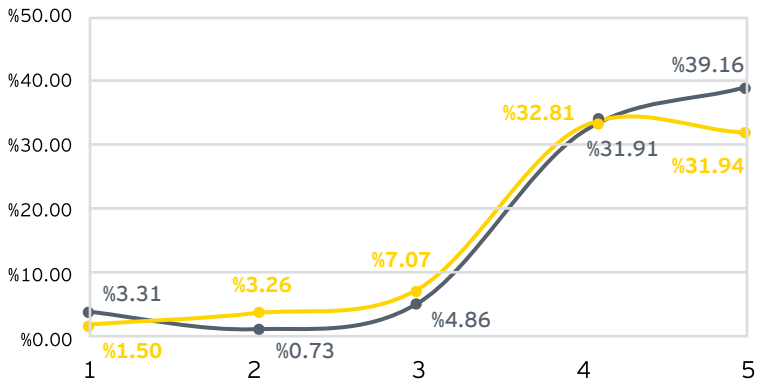
BT dışı alanlarda görevli katılımcılar ise, üçüncü tarafların yönetiminden kaynaklanabilecek riskleri önemli görmüştür. Bu değerlendirme bizlere uyum sürecinin tüm paydaşları kapsadığını hatırlatmıştır.

## 3.3 Düzenlemelere İlişkin Alınacak Aksiyonların İş Süreçleri ve BT Kaynaklı Risklerin Yönetimine Katkı Endeksi

Düzenlediğimiz etkinliklerde katılımcılara; düzenlemelerle birlikte alınacak aksiyonların şirketlerin BT ve iş süreci kaynaklı risklerine olumlu etkisi olup olmayacağı ayrı sorular olarak yöneltilmiştir.




**Aksiyonların İş Süreçleri ve BT Kaynaklı Risklerin Yönetimine Katkı Endeksi**




- Aksiyonlar şirketimin BT kaynaklı risklerinin yönetilmesine olumlu katkıda bulunacaktır.
- Aksiyonlar şirketimin iş süreçlerine ve süreç risklerinin yönetilmesine olumlu katkıda bulunacaktır.

1. Kesinlikle katılmıyorum 2. Katılmıyorum 3. Kararsızım 4. Katılıyorum 5. Kesinlikle Katılıyorum

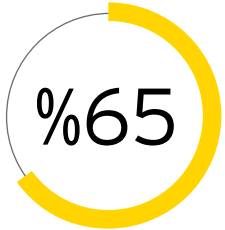
**%92** Düzenlemelerle birlikte alınacak aksiyonların BT kaynaklı risklerin yönetilmesine olumlu katkıda bulunacağını düşünen katılımcıların %92'si, uyum programının iş süreçlerine ve süreç risklerine de olumlu etkisi olacağını düşünmektedir.

## 3.4 Düzenlemelere İlişkin Uyum Programını Uygulayacak Teknik Yeterlilik

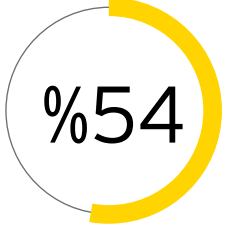
Anket katılımcılarına şirketlerindeki; BT, İç Denetim, İç Kontrol, Risk Yönetimi ekiplerinin SPK Bilgi Sistemi uyum programını uygulayabilecek teknik yeterliliğe sahip olup olmadıkları sorulmuştur.

"BT, İç Denetim, İç Kontrol, Risk Yönetimi" katılımcılarının cevapları diğer görev alanlarından katılımcılarının cevapları ile kıyaslanmıştır.

**BT, İç Denetim, İç Kontrol, Risk Yönetimi**



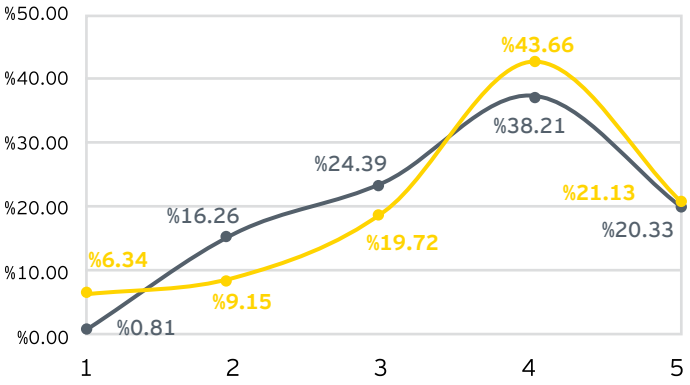

**Diğer Görev Alanları**




**Katılıyorum ve kesinlikle katılıyorum diyen katılımcıların tüm katılımcılara oranı**

Anket sonuçları ilgili birimlerin öz değerlendirmeleri ile, şirket içerisindeki diğer birimlerin düşünceleri arasında farklılıklar olduğunu göstermektedir.

**Aracı Kurumlar ve Portföy Yönetim Şirketleri'nin Cevaplarının Halka Açık Şirketlerle Kıyaslanması**




- Halka Açık Şirketler
- Aracı Kurumlar ve Portföy Yönetim Şirketleri

1. Kesinlikle katılmıyorum 2. Katılmıyorum 3. Kararsızım 4. Katılıyorum 5. Kesinlikle Katılıyorum

# 4

# Öneriler

5 Ocak 2018 tarihli SPK Bilgi Sistemleri Düzenlemeleri'ne yönelik uyum konusunda şirketlerin öncelikle düzenlemeler nezdinde eksiklilerini belirlemesi, sonrasında da bu eksikliklere yönelik iyileştirici aksiyon planlarını, bir uyum programı dahilinde uygulamaya başlaması gerekiyor.

2018 dönemi için hali hazırda SPK bilgi sistemleri denetimi geçirmiş olan Borsa İstanbul A.Ş. BT Ağ, Güvenlik ve Risk Yönetimi Direktörü Sn. Erdinç Tutam bu uyum programını uygulayacak şirketlere şu şekilde öneride bulunuyor:

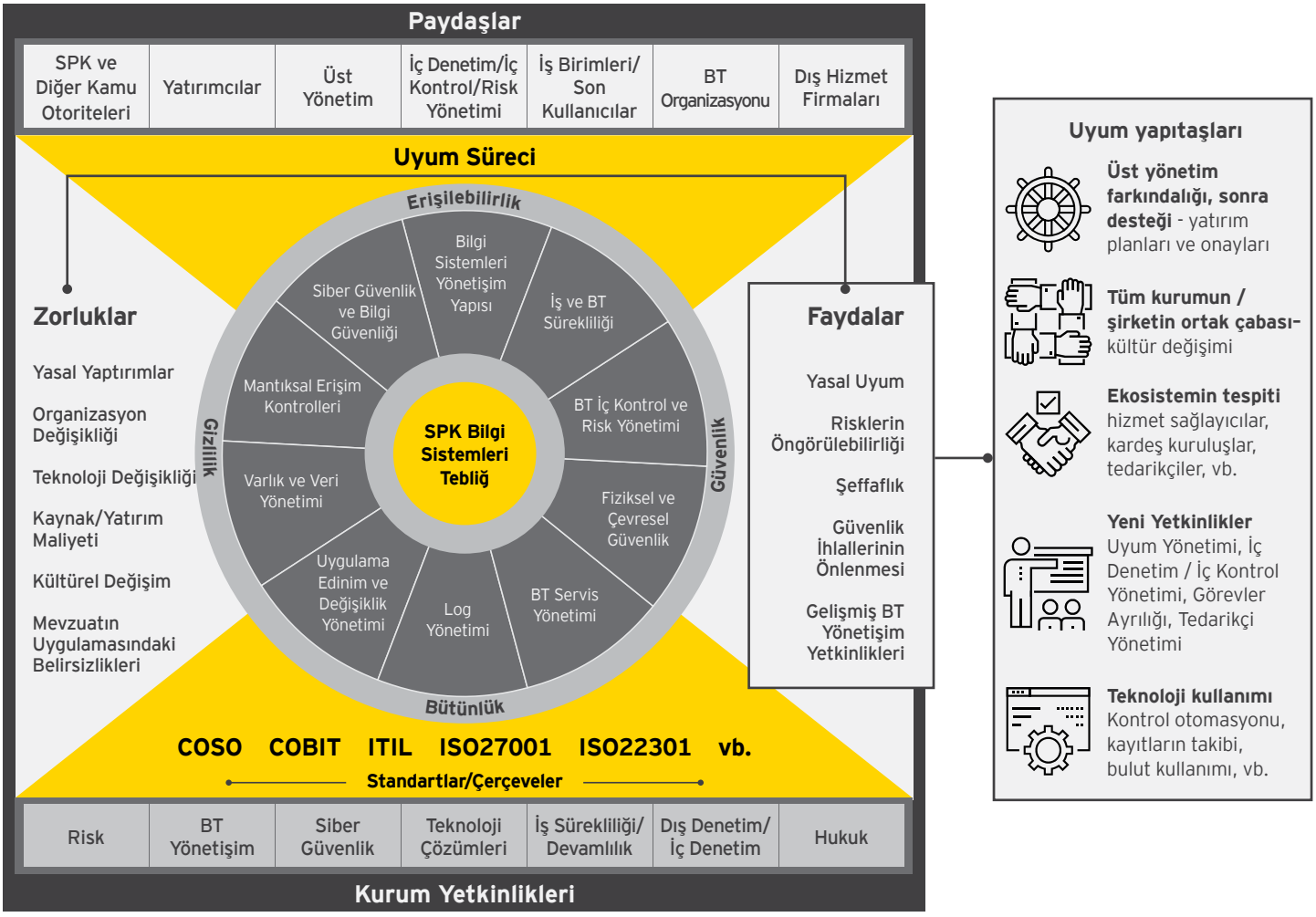
*"Borsa İstanbul'un kanun ve mevzuatlarla gerçekleştirmiş olduğu borsacılık faaliyetinin kritiklik durumu nedeniyle aslında borsanın her zaman bir bilgi güvenliği ve iş sürekliliği yönetimi sistemi vardı. Bu sistemler uzun süredir zaten burada işletiliyor, sürekli olarak iyileştiriliyor. Ayrıca biz SPK denetimine de aşinaydık. Zira 2016 yılı için, 2017'de tebliğ öncesinde Borsa İstanbul A.Ş. bünyesinde SPK'nın talebiyle bağımsız bilgi sistemleri denetimi de gerçekleştirildi. Dolayısıyla, aslında Borsa İstanbul, genel anlamda hazırdı diyebiliriz. 2018 yılında SPK BT Tebliğleri'nin yayımlanmasından sonra da bir fark analizi çalışması yaptırdık. Özellikle fark analizinin bize çok faydası olduğuna inanıyorum. Yani bizim aslında mevcutta var olduğunu düşündüğümüz yönetim sistemlerinin iyileştirilmesi adına bir takım ödevler çıktı bize ve 2018 yılında bu ödevleri tamamladıktan sonra da denetim gerçekleşti. Fark analizi yaptırdığımız için, aslına bakarsanız denetim bizim için birkaç konu haricinde rahat geçti diyebilirim. Dolayısıyla önümüzdeki dönemde bu işi yapacak, bu denetimi geçirecek kurumların öncelikli olarak böyle bir fark analizi çalışmasını geçirmesini tavsiye ediyorum."*

Düzenlemeden etkilenen şirketlerin odaklanması için öne çıkan konular aşağıdaki şekilde özetlenebilir.

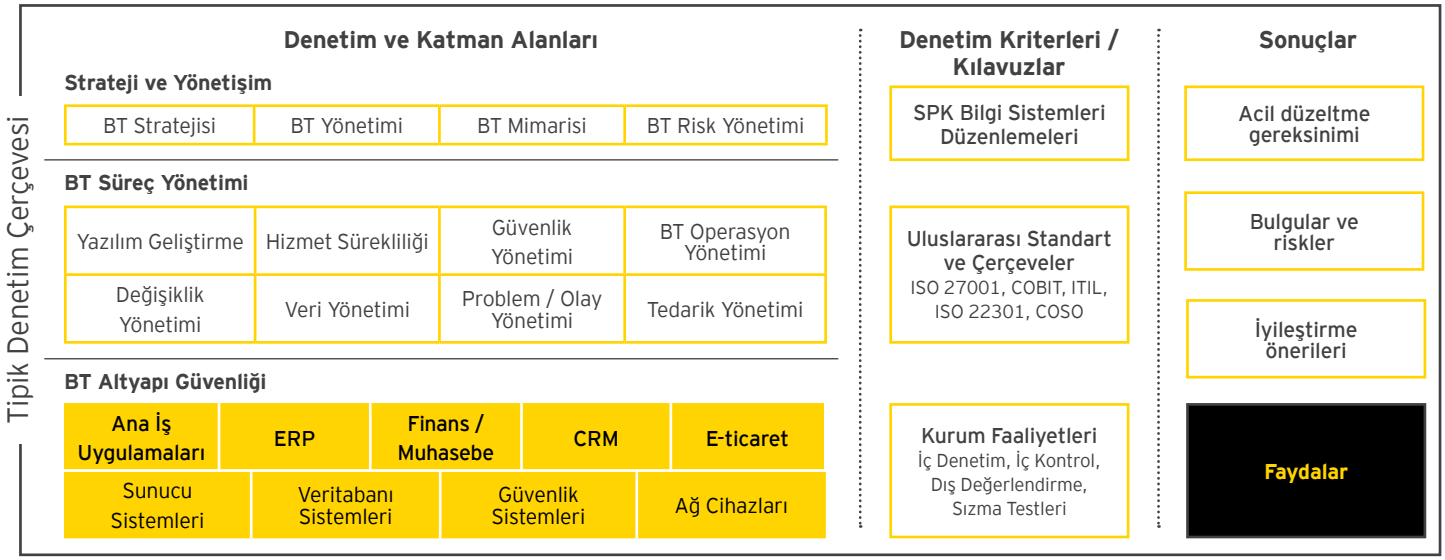
- Fark Analizi
- Erken Adaptasyon
- BT Değil Tüm Organizasyon
- Yatırım İhtiyaçları
- Yönetim Desteği ve Farkındalığı
- Aksiyon Planlama

# Operasyonel ve Teknoloji Uyum Yol Haritası

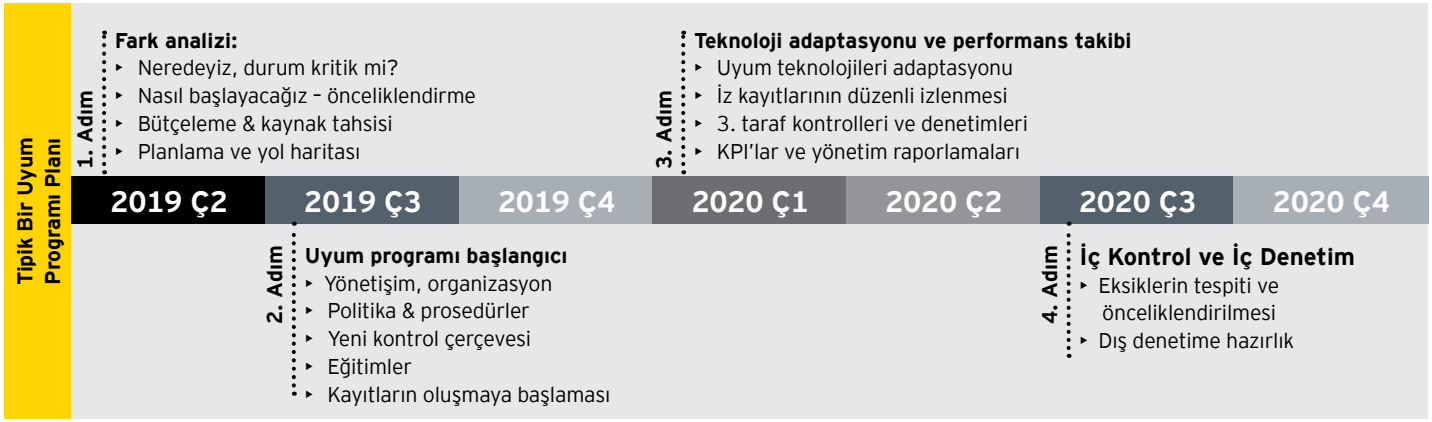
5 Ocak 2018 tarihli SPK Bilgi Sistemleri düzenlemelerine yönelik uyum programı oluşturulurken, uyum sürecine ekosistemdeki tüm kritik paydaşların da dahil olduğu değerlendirilmelidir. Bu kapsamda düzenlemelere uyum gereksinimlerinin getirmiş olduğu zorluklar ve sağlayacağı faydaların yönetiminde ilgili tüm paydaşların beklentileri, rolleri ve sorumluluklarının da dikkate alınması ve uyum programının temelini oluşturacak uyum yapıtaşlarının bu doğrultuda değerlendirilmesi önerilmektedir.




Uyum programının tasarımı aşamasında, stratejik ve operasyonel yol haritasına baz teşkil edecek kontrol ortamı çerçevesinin doğru belirlenmesi büyük önem taşımaktadır. Bu doğrultuda, aşağıda da yer verilen tipik bir denetim çerçevesi bazında ele alınan denetim katman ve alanlarının, ilgili denetim kriterleri/kılavuzlar ışığında uyum programı kapsamında ele alınması değerlendirilmelidir.



Henüz uyum yolculuğunun başında olan şirketler için, tasarlanacak uyum programının hızlı, doğru ve etkin uygulanabilirliği ve özellikle sürdürülebilirliği büyük önem taşımaktadır. Uyum programından beklenen hedeflere ulaşılabilmesi için, programın etkin bir plan dahilinde yürütülmesi ve uyum sürecine yönelik belirtilen temel aksiyon önerilerinin değerlendirilmesi gerekmektedir. Tipik bir uyum programı kapsamında planlanması önerilen çalışmalara, dikkate alınması gereken bulgu alanlarına ve risklere aşağıda yer verilmiştir.




## Uyum Sürecine Yönelik Temel Aksiyon Önerileri

### Neler yapmalı?

Üst yönetimin farkındalığı arttırılıp, desteği alınmalıdır.

Fark analizi yaptırılmalıdır.

Uyum program planlanmalı, riskli alanlara göre önceliklendirilmeli ve maliyetlendirilmelidir.

Uyum programı takip edilmeli, üst yönetime raporlanmalıdır.

Kontrol ortamı teknolojiyle desteklenmelidir.

### Neler yapmamalı?

Uyum konusu yalnızca BT işi olarak görülmemelidir.

Plan yapmadan yatırım yapılmamalıdır.

Görevler ayrılığı hayat kurtarır, yolsuzluk engeller. "Biz uygulayamayız" denilmemelidir.

Bilgi Mimarisi envanterine sahip çıkılmalı, gölge BT'ye izin verilmemelidir.

## Tipik Bir Denetim Tespit Konu Başlıkları

- Bilgi sistemleri mimarisi problemleri
- Yönetişim problemleri
- Bilgi sistemleri değişiklik yönetimi problemleri
- Süreklilik yönetimi problemleri
- Risk, uyum ve iç kontrol problemleri
- Bilgi güvenliği / siber güvenlik yönetimi problemleri
- Yüksek yetkili kullanıcıların yönetimi
- Denetim izleri yönetimi
- Görevler ayrılığı ilkesinin ihlali

## Dış Hizmet Firmaları İçin Aksiyon Önerileri

Üçüncü taraflardan kaynaklanan risklerin yönetimi için, SPK Bilgi Sistemleri Düzenlemeleri Yönetim Tebliği'nin 18. maddesinde belirtildiği gibi, aşağıda belirtilmiş kavramları içeren bir "Gözetim Mekanizması" oluşturulmalı ve etkin bir şekilde işletilmelidir.

# 5

# Sonuç

5 Ocak 2018 tarihli SPK Bilgi Sistemleri Düzenlemeleri'ne yönelik gerçekleştirilen etkinliklere, halka açık şirketler, aracı kurumlar ve portföy yönetim şirketlerinin üst düzey yöneticileri, iç denetim, iç kontrol ve BT birimi yöneticileri ve ekipleri katılım sağlamıştır. Etkinlikler boyunca ilgili katılımcılardan edinilen geri bildirimler neticesinde şirketlerin uyum yol haritasındaki temel ihtiyaç alanları belirlenmiştir.

Etkinlik boyunca sorulan sorular ve anket sonuçları değerlendirildiğinde genel olarak SPK Bilgi Sistemleri Düzenlemleri'ne uyum yükümlülüğü bulunan şirketler için aşağıdaki hususların, yol haritasında bulunması gereken temel ihtiyaç alanları dahilinde olduğu değerlendirilmiştir;

- SPK Bilgi Sistemleri Düzenlemeleri kapsamındaki yükümlülükler konusunda şirketlerin üst yönetiminin farkındalığının artırılması
- SPK Bilgi Sistemleri Düzenlemeleri kapsamındaki yükümlülükler ve bu doğrultudaki teknik gereksinimler konusunda, şirketler bünyesindeki ilgili ekiplerin yetkinliğinin / farkındalığının artırılması
- Şirketler nezdinde SPK Bilgi Sistemleri Düzenlemleri kapsamına giren bilgi teknolojileri süreçleri, sistemleri ve altyapı bileşenlerinin mevzuata uygun olarak belirlenmesi
- Şirketlerin SPK Bilgi Sistemleri Düzenlemeleri'ne ne ölçüde uyumlu olduğunun tespitine yönelik mevcut durum analizi gerçekleştirmesi, eksikliklerini ve aksiyon planlarını belirleyerek üst yönetim gözetiminde bir uyum programı oluşturması ve uygulaması
- Uyum programı kapsamındaki organizasyonel, operasyonel, teknoloji yatırım ihtiyaçlarının belirlenerek yatırım planı oluşturulması
- En önemli paydaşlardan olan dış hizmet firmaları, özellikle teknoloji şirketleri nezdinde SPK Bilgi Sistemleri Düzenlemeleri'ne uyum konusunda güvence sağlayacak aksiyonların alınması
- Bağımsız bilgi sistemleri denetim yükümlülüğü bulunan firmalar için yönetim beyanı metodolojisinin oluşturulması var bu doğrultuda beyana mesnet teşkil edecek çalışmaların gerçekleştirilmesi
- Bağımsız bilgi sistemleri denetim yükümlülüğü bulunan firmalar için bağımsız denetimi gerçekleştirecek firma konusunda karara varılması ve denetim sözleşmelerinin imzalanması

EY Türkiye olarak, farklı yetkinliklere sahip güçlü ekibimizle farklı uzmanlıklar gerektiren bu uyum yolculuğunuz boyunca sizleri aşağıdaki hizmet alanlarımızla her dönemeçte desteklemeye hazırız.

**Danışmanlık Hizmetleri**

- EY Teknolojik Uyum Programı
- Yönetim Beyanı Danışmanlığı
- KVKK Uyum Danışmanlığı

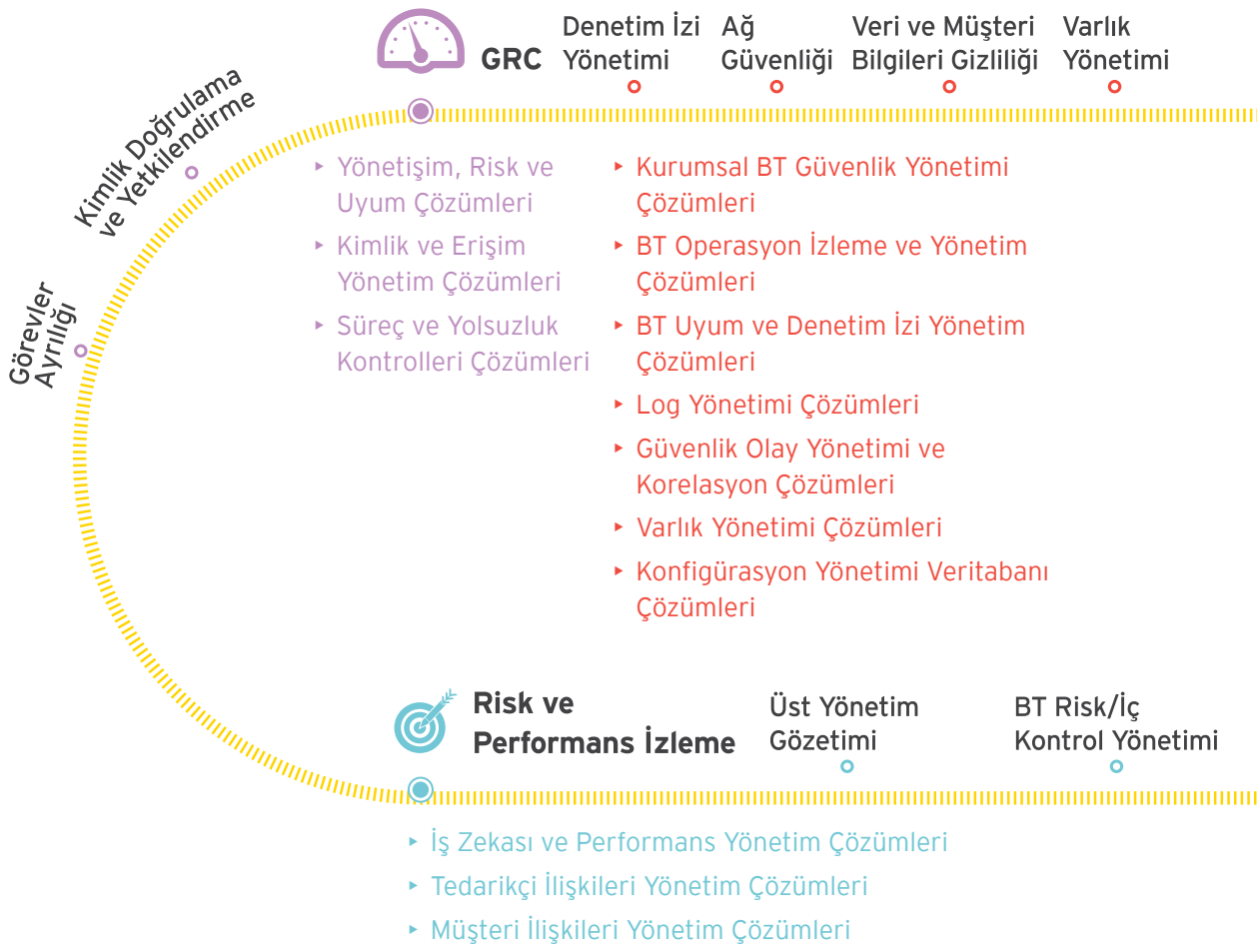
**Denetim Hizmetleri**

- SPK Bağımsız Bilgi Sistemleri Denetimi
- Dış Hizmet Firmaları
- ISAE 3402 Denetimi
- Sızma Testi

# SPK BT Düzenlemeleri EY Teknolojik Uyum Programı

Değişen yasal düzenlemeler, siber suçlara açık hale gelen iş hayatı, sürekli karşımıza çıkan, ezber bozan iş modelleri ve iş gücünde meydana gelen değişiklikler ve hassas sosyoekonomik ortam BT fonksiyonun günümüzde çok daha risk odaklı, kontrollü ve sürdürülebilir yönetimini gerektirmektedir.

SPK'nın, şirketlerimizin sürdürülebilir büyüme yolculuğunu güvence altına almak üzere yayımlamış olduğu 5 Ocak 2018 tarihli Bilgi Sistemleri düzenlemeleriyle birlikte, Sermaye Piyasası Kanunu kapsamında faaliyet gösteren şirketlerin bilgi teknolojileri süreç ve sistemlerini ilgili düzenlemelere uyumlu hale getirme yükümlülüğü doğmuştur.



Kurumunuzu ulusal ve uluslararası rekabette ileri taşıyacak bu uyum yolculuğu boyunca, size her dönemeçte sunacağımız **metodolojilerimiz, uluslararası ve yerel iş ortaklıklarımız, risk ve teknolojik birikimlerden oluşan yetkinliklerimizle** sizleri desteklemeyi hedefliyoruz.

**BT Yönetişim**

Değişiklik/ Proje Yönetimi

BT Servis Yönetimi

- Geliştirme ve BT Operasyon Çözümleri
- Test Otomasyon Çözümleri
- DevOps Çözümleri
- Servis Yönetimi Çözümleri

**Kurumsal Dayanıklılık**

İş ve BT Sürekliliği

Fiziksel Güvenlik

- Yedekleme ve Kurtarma Yönetimi Çözümleri
- Veri Koruma ve Bilgi Yönetimi Çözümleri
- Kriz İletişim Platformu
- İş Sürekliliği Yönetimi Çözümleri
- İş Etki Analiz Çözümleri

Güvenlik Olay Yönetimi

Bilgi Güvenliği Yönetim Sistemi

**Siber Güvenlik**

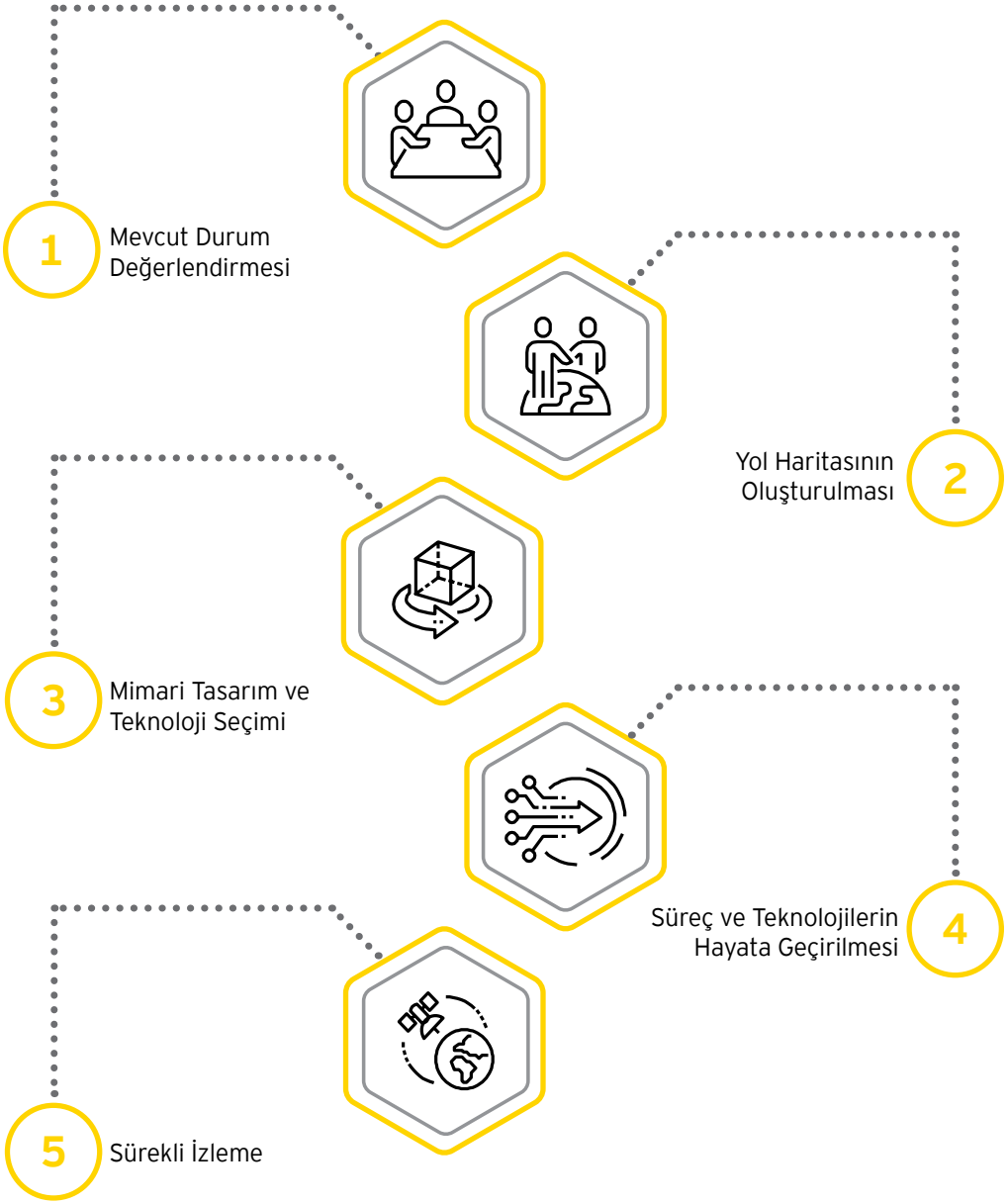
**Hukuk**

- Veri Yönetişim Çözümleri
- Veri Kaybı Önleme Çözümleri
- Elektronik Belge ve Kayıt Yönetim Sistemi
- Açık Rıza ve Aydınlatma Yönetim Çözümleri
- Veri Yaşam Döngüsü Çözümleri
- Mobil Cihaz Yönetimi Çözümleri
- Ağ Erişim Kontrol Çözümleri
- İhlal Algılama ve Önleme Sistemleri

Dış Hizmet Firma Yönetimi

Müşteri Bilgilendirmesi

## EY Teknolojik Uyum Yolculuğu




- Uyum/SPK Bilgi Sistemleri Denetimlerinde Başarı
- Teknolojik İş Ortaklıkları
- Hızlı/Çevik Dönüşüm
- Kaynak Yönetiminde Verimlilik
- Sürekli Kontrol

**EY** | Assurance | Tax | Transactions | Advisory

**EY Hakkında**

EY bağımsız denetim, vergi, kurumsal finansman ve danışmanlık hizmetlerinde bir dünya lideridir. Anlayışımız ve kaliteli hizmetlerimiz dünya ekonomisi ve sermaye piyasalarında güvenin oluşmasına katkıda bulunmaktadır. EY, güçlü yönetim ekibiyle tüm paydaş gruplarına verdiği sözleri yerine getirmekte ve bu şekilde çalışanları, müşterileri ve içinde yer aldığı diğer çevreler için daha iyi bir çalışma hayatı oluşturulmasında önemli bir rol üstlenmektedir.

EY adı küresel organizasyonu temsil eder ve Ernst & Young Global Limited'in her biri ayrı birer tüzel kişiliğe sahip olan, bir veya daha çok, üye firmasını temsil edebilir. Sınırlı sorumlu bir Birleşik Krallık şirketi olan Ernst & Young Global Limited müşteri hizmeti sunmamaktadır. Daha fazla bilgi için lütfen ey.com adresini ziyaret ediniz.



ey.com/tr
vergidegundem.com
facebook.com/ErnstYoungTurkiye
instagram.com/eyturkiye
twitter.com/EY_Turkiye

## İletişim

**Emre Beşli**
EY Türkiye Şirket Ortağı
Risk Danışmanlık Hizmetleri Lideri

emre.besli@tr.ey.com

**Ümit Yalçın Şen**
EY Türkiye Şirket Ortağı
Siber Güvenlik Hizmetleri Lideri

umit.sen@tr.ey.com

**Feyyaz Burak Baysal**
EY Türkiye Şirket Yardımcı Ortağı
Teknoloji Risk Hizmetleri Lideri

burak.baysal@tr.ey.com

**Esra Uzalp**
EY Türkiye Direktörü
Teknoloji Risk Hizmetleri

esra.uzalp@tr.ey.com