Bankacılığın yeni çağına hazır mısınız?

Mayıs 2020

KPMG Türkiye

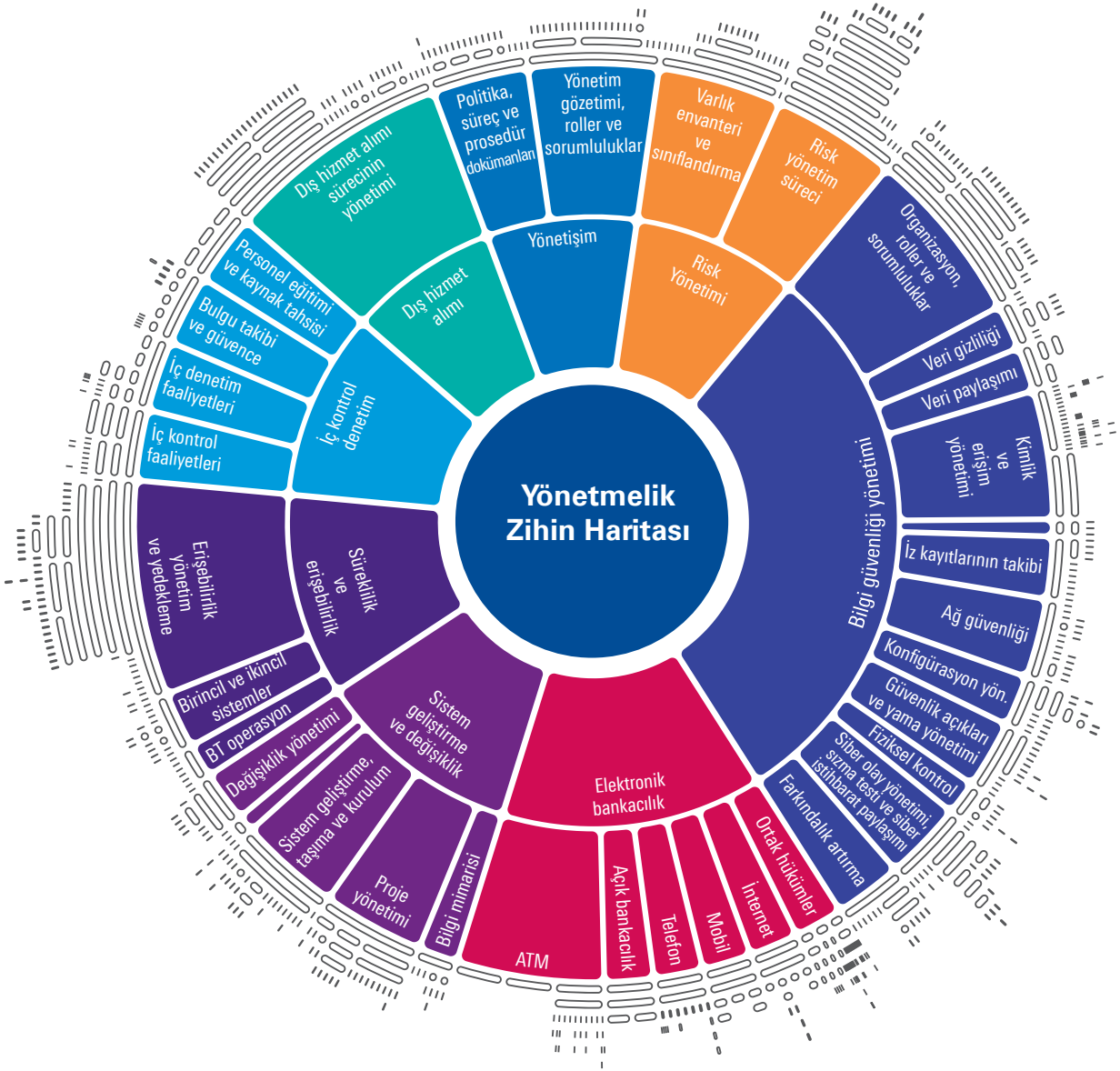
kpmg.com.tr

Yeni çağın bankacılığının kuralları değişti

2007 yılında hayatımıza giren ve bankaların bilgi sistemleri denetiminde çerçeveyi belirleyen **Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ (İlkeler Tebliği)** bu sene itibariyle 13 senelik ömrünü tamamlayarak yerini **Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik'e (Yönetmelik)** bırakıyor. Takvimsel olarak baktığımızda;

- **14 Eylül 2007 İlkeler Tebliği yürürlüğe girdi.**
- **25 Aralık 2018 yeni yönetmelik taslağı görüşe açıldı.**
- **Sektör temsilcileri aracılığıyla sektörün, ilgili kurum ve kuruluşların görüş ve önerileri değerlendirilerek nihai taslak oluşturuldu.**
- **15 Mart 2020 yeni yönetmelik yayımlandı.**
  - Bilgi sistemlerinin yönetimi ile elektronik bankacılık hizmetlerinin sunulmasında gereken kontrollerin düzenlendiği Yönetmelik, Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) tarafından 31069 sayılı Resmi Gazete'de yayımlandı.
- **01 Temmuz 2020 tarihine kadar bankalara geçiş süreci tanındı.**
- **Uyum açısından belirlenen hedef tarihte yeni yönetmeliğin yürürlüğe girmesiyle birlikte, İlkeler Tebliği yürürlükten kaldırılacak.**

KPMG olarak, bilgi sistemlerinin ve elektronik bankacılık hizmetlerinin yönetiminde **güçlü bir yönetişim, risk yönetimi ve bilgi güvenliği yönetimi** yapısını temel alıyoruz. Söz konusu yapının kurulmasına yönelik hazırladığımız **Yönetmelik Zihin Haritası** ile her bir banka özelinde özgün çözümler yaratarak en iyi uygulamaların hayata geçirilmesini hedefliyoruz.



Yönetmelikle önemli değişiklikler ve yenilikler yapıldı

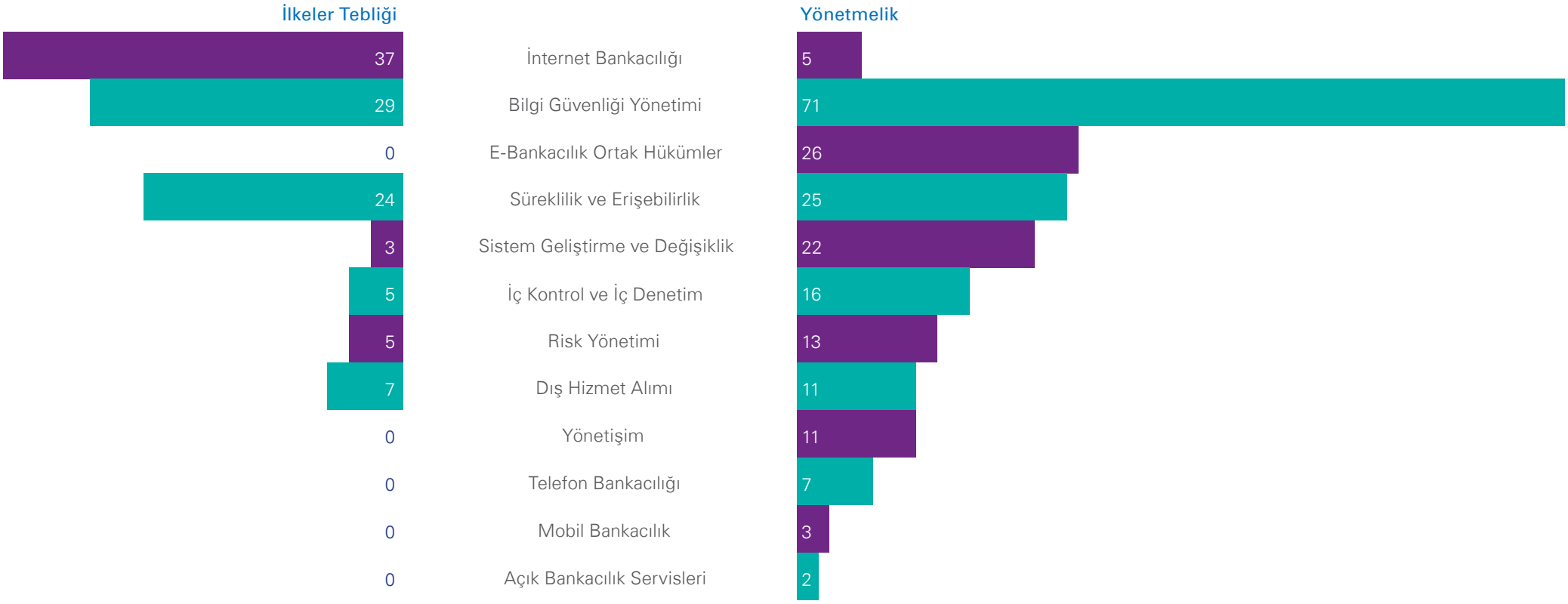
Mevzuatta **ilk kez tanımlanan komiteler ve fonksiyonlarla** banka organizasyon yapılarında önemli değişikliklerin gerçekleşeceği görülüyor. Bilgi güvenliği fonksiyonunun üst yönetime bağlı olarak tanımlanması, **siber olaylara müdahale tatbikatları** ve **ikincil merkez** üzerinden faaliyetleri sürdürmeye yönelik testlerin vurgulanması, **güvenlik ve süreklilik** çalışmalarının önceliklendirilmesi anlamına geliyor.

BT dış hizmetlere ilişkin yapılan düzenlemelerle dış hizmetlere ilişkin kontrol ve gözetimin de artırılması öngörülüyor.

İlkeler Tebliği ile Yönetmelik arasındaki farklar incelendiğinde, İlkeler Tebliği'ndeki birçok madde için kapsamın genişletilerek detaylı şekilde ele alındığı görülüyor. Detaylandırılan kapsam, uyum gereklilikleri için daha net bir yol çizmekle birlikte **stratejik düşünmeyi** de zorunlu hale getiriyor.

Yönetmelik ile detaylandırılan veya ilk defa ele alınan bölümlerin incelenmesi sonucunda, **İlkeler Tebliği ile Yönetmelik arasındaki farkları** gösteren grafiği sizler için sunduk.

İlkeler Tebliği ve Yönetmelik farkları



Bankacılıkta dönüşüm süreci başladı

KPMG olarak, **bankacılığın dönüşüm sürecinde** bilgi sistemlerinin yönetimine ilişkin tüm bileşenler için politika, prosedür, sorumluluk ve karar mekanizmalarını içeren **yönetişim**; uyum ve kontrol çalışmaları kapsamında ise **iç kontrol ve iç denetim** gerekliliklerinden oluşan bir çerçeve tasarladık.

Dijitalleşme kavramının da etkisiyle dijital kanallar için getirilen detaylı hükümler ve bir ilk olan **açık bankacılık servisleri** çerçevedeki önemli bir değişikliği oluşturuyor. Müşteri veya müşteri adına hareket eden taraf ile banka arasındaki iletişimin uçtan uca güvenli iletişimini hedefleyerek dünya bankacılık sistemine giriş yapan açık bankacılık servisleri dahil tüm dijital kanalların hassas veri yönetimi başta olmak üzere **bilgi sistemleri ile olan etkileşimi** kaçınılmaz.

Bilgi sistemleri ve elektronik bankacılık hizmetleri çerçevesi

Veri ve iş süreçleri odaklı bilgi varlığı yönetimi öne çıktı

Bankacılık yeni çağında daha fazla servis noktası sağlamak için teknolojisine üst düzey yetkinlikler kazandırıyor. Geliştirilen bilgi sistemleri, bir yandan yetkinliklerini arttırırken bir yandan da tehditlerin çeşitliliği ve etkileşim noktası artıyor. Yönetmelik tam olarak bu noktada devreye giriyor. **Temel yönetişim ve kontrol prensipleri**ne ek olarak, özellikle de **dijital bankacılık** için detaylandırdığı yöntemler ile bilgi sistemlerinin daha güvenilir olmasını ve erişim sürekliliğini sağlamaya yönelik tasarlanmış.

KPMG olarak, Yönetmelik uyumunu sağlamak ve yeni çağın bankacılığına ayak uydurmak için ilk adımı belirledik. **Yaklaşımımız verinin güvenliğini sağlamak** ve **erişim sürekliliği için gerekli yönetişim ve kontrol prensiplerini belirlemek**. Veri, sırasıyla bilgi varlıklarını, bilgi sistemlerini ve iş süreçlerimizin temelini oluşturuyor. Hedef yaklaşımımızda belirlediğimiz **aşağıdan-yukarıya / yukarıdan-aşağıya ilerleme yöntemi** ile veri özelinden iş süreçlerine giderek öncelikli gelişim alanlarını hızlıca belirleyebiliyor, bir yandan da iş süreçlerinden veriye ilerleyerek eksiksiz bir çözümün uygulanabilmesini sağlayabiliyoruz.

Aşağıdan yukarıya

Veriden iş süreçlerine doğru ilerleyerek; bankacılık faaliyetlerinde kullanılan ana ve referans veri, işlemsel veri, vb. verilerin bankanın bilgi sistemleri üzerinde taşınması, saklanması, iletimi ve işlenmesi ile birlikte iş süreçlerindeki öncelikli gelişim alanlarının belirlenmesi ve aksiyon alınması

Bilgi varlığı

- İş süreçleri
- Bilgi sistemleri
- Veri

Yukarıdan aşağıya

İş süreçlerinden veriye doğru ilerleyerek; süreç içerisindeki tüm verilerin belirlenen öncelikli gelişim alanları kapsamında bilgi sistemleri üzerinde gelişim alanlarına ilişkin iyileştirmelerin yapılarak verinin daha etkin yönetiminin sağlanması

- Tanım
- Sahiplik
- Görece değeri
- Organizasyon, rol ve sorumluluklar
- Güvenlik sınıfı
- Varlık envanteri
- Konum

Kurumsal mimari çerçevesi ile uçtan uca çözüm hedeflendi

Bankanın hedef ve stratejileri ile IT sistemleri arasındaki ilişkiyi yöneten ve kullanılması gereken teknolojilere yön veren yapı olarak tanımlanan kurumsal mimarinin sadece **bugünü** değil, **gelecek planlarını** da desteklemesi gerekiyor.

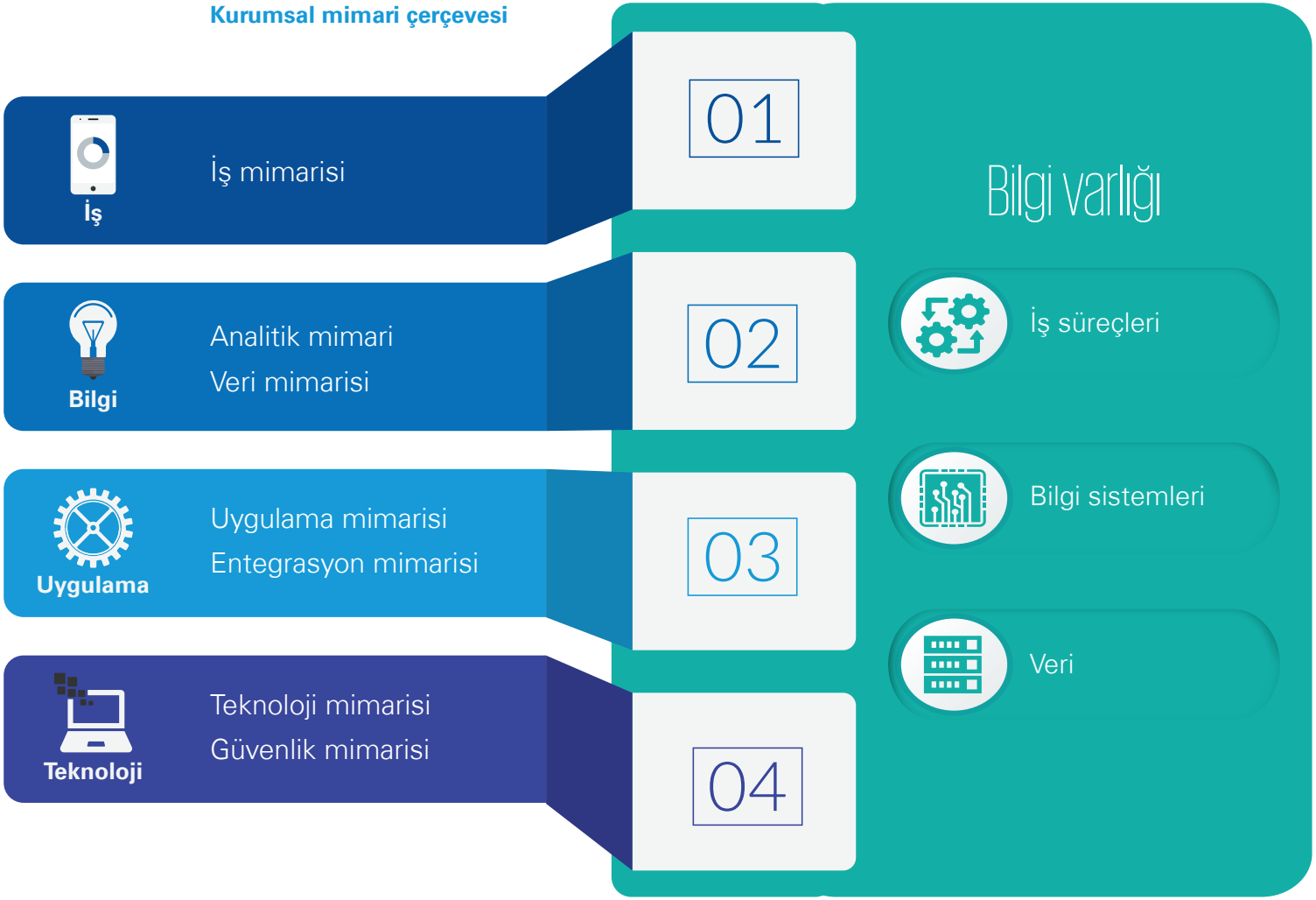
KPMG olarak **kurumsal mimari çerçevesi** yaklaşımımız; iş, bilgi, uygulama ve teknoloji alanlarında gruplanarak banka genelinde bir sinerji oluşmasına altyapı sağlıyor; **zamanında ve gerekli işlevsellik düzeyine sahip bir bilgi sistemi** için uçtan uca çözüm sunuyor.

Bilgi, bir banka için değeri olan ve bu nedenle de uygun yönetişimin ve kontrol prensiplerinin belirlenmesi gereken bir varlık olduğundan; **bilgi varlığı** kurumsal mimari çerçevesi yaklaşımımız için merkez kabul ediliyor. Temelinde **veri ve iş süreçleri** bulunan bilgi varlığı üzerine inşa edilen her bir mimari yapıyla bir **kurumsal mimari** oluşturuluyor ve **bütünleşik kullanımı** ile maksimum fayda sağlanıyor.

Bankacılık için hem yeniliklerin değerlendirilmesi hem de söz konusu düzenlemelere uyum sağlanması kapsamında sunduğumuz çözümü esas alarak bir **kurumsal mimari tasarımın** oluşturulması ve **uygulanması**yla birlikte de **sürdürülebilir bir kurumsal mimari çerçevesi** hazırlıyoruz.

Bilgi sistemleri ve elektronik bankacılık hizmetleri çerçevesi

Kurumsal mimari çerçevesi



Bilgi sistemleri bileşenlerine bütünleşik çözüm yaklaşımımız

Yönetişim

Yönetim gözetimi	Organizasyon/komiteler	Birim/fonksiyon	Roller/sorumluluklar	Sorumluluklar	İş planları
Politika ve standartlar	Süreçler/prosedürler	Veri sözlüğü	Veri envanteri	Varlık envanteri	Risk envanteri

Risk yönetimi

- Kapsam belirlenmesi
- Risklerin analizi
- Tehdit ve güvenlik açıklarının tespiti
- Risklerin belirlenmesi
- Risk etki hesaplamasının yapılması
- Varlıkların risk olasılıklarının ve etki değerlerinin belirlenmesi
- Riskin derecelendirilmesi
- Risklere aksiyon belirleme
- Riskin azaltılması
- Riskten kaçınma
- Riskin kabulü
- Riskin transferi
- Risk değerlendirme raporu
- İzleme ve gözden geçirme

Güvenlik yönetimi

- Bilgi mimarisinin tanımlanması
- Veri gizliliği
- Veri paylaşımı
- Bütünlük kontrolleri
- Siber olay yönetimi
- Siber güvenlik tatbikatı
- Güvenlik açıkları ve yama yönetimi
- Sızma testi
- Siber istihbarat paylaşımı
- Kimlik ve erişim yönetimi
- İz kayıtlarının oluşturulması ve takibi
- Ağ güvenliği
- Güvenlik konfigürasyon yönetimi
- Fiziksel güvenlik kontrolleri

Sistem geliştirme ve değişiklik yönetimi

- Proje yönetimi
- Uygulama kontrolleri
- Değişiklik yönetimi
- Sistem geliştirme, taşıma ve kurulum

Süreklilik ve erişebilirlik yönetimi

- BT operasyon yönetimi
- Erişebilirlik yönetimi ve yedekleme
- İş hedeflerinin belirlenmesi
- İş etki analizi
- Felaket senaryolarının testi
- Süreklilik testlerinin yönetimi

BS dış hizmet

- Dış hizmet gözetim mekanizmasının oluşturulması
- Dış hizmet alanlarının belirlenmesi
- İletişim bilgilerinin ilgililerle paylaşılması
- Dış hizmet seviyesine uyumun takibi
- Dış hizmet sözleşmesine uyumun takibi

İç kontrol ve iç denetim

İç kontrol ve iç denetim organizasyon yapısının tesisi	İç kontrol sonucu eksikliklerin giderilmesi	İç kontrol toplantılarında öneri sunulması	İç denetim kapsam belirlenmesi
İç denetim sıklığı ve döngüsünün belirlenmesi	Kritik BS servislerinin, süreçlerin, varlıkların kontrolü	Personel eğitimi ve kaynak tahsisi	Bulgu takibi ve güvence sağlanması

KPMG olarak sizlere ne tür hizmetler sunabiliriz?

Değerlendirme

Yönetmelik'e uyum seviyesi değerlendirilerek mevcut durum analizinin gerçekleştirilmesi, eksikliklerin belirlenmesi ve iyileştirme alanlarının ortaya çıkarılması

Tasarım ve iyileştirme

KPMG Kurumsal Mimari Çerçevesi referans alınarak, değerlendirme sonucunda belirlenen konu başlıkları için Yönetmelik'e uyumun detay planlamasının yapılması ve mimari tasarımın oluşturulması

Uygulama

Tasarım ve iyileştirme kapsamında oluşturulan mimari tasarımdaki alanların önceliklendirilmesi, önceliklendirilen her bir alan için çözümün hayata geçirilmesi ve Yönetmelik maddelerine uyumun sağlanması

İzleme ve kontrol

Yönetmelik'e uyumun sürdürülebilirliğinin sağlanması amacıyla düzenli olarak izlemenin sağlanması ve periyodik kontrollerin gerçekleştirilmesi

İletişim:

Emin Alper Karaçar
Şirket Ortağı,
BT Lideri ve Kamu
Sektörü Lideri
Danışmanlık Hizmetleri
akaracar@kpmg.com

Gökhan Mataracı
Direktör,
Veri ve Analitik Lideri
Danışmanlık Hizmetleri
gmataraci@kpmg.com

Servet Gözel
Direktör,
Bilgi Teknolojileri Danışmanlığı
servetgozel@kpmg.com

Detaylı bilgi için:
KPMG Türkiye
Clients & Markets
tr-fmmarkets@kpmg.com

İstanbul
İş Kuleleri Kule 3 Kat 1-9
34330 Levent İstanbul
T : +90 212 316 6000

Ankara
The Paragon İş Merkezi Kızılırmak Mah. Ufuk Üniversitesi
Cad. 1445 Sok. No:2 Kat:13 Çukurambar 06550 Ankara
T: +90 312 491 7231

İzmir
Heris Tower, Akdeniz Mah. Şehit Fethi Bey Cad. No:55
Kat:21 Alsancak 35210 İzmir
T: +90 232 464 2045

kpmg.com.tr
kpmgvergi.com