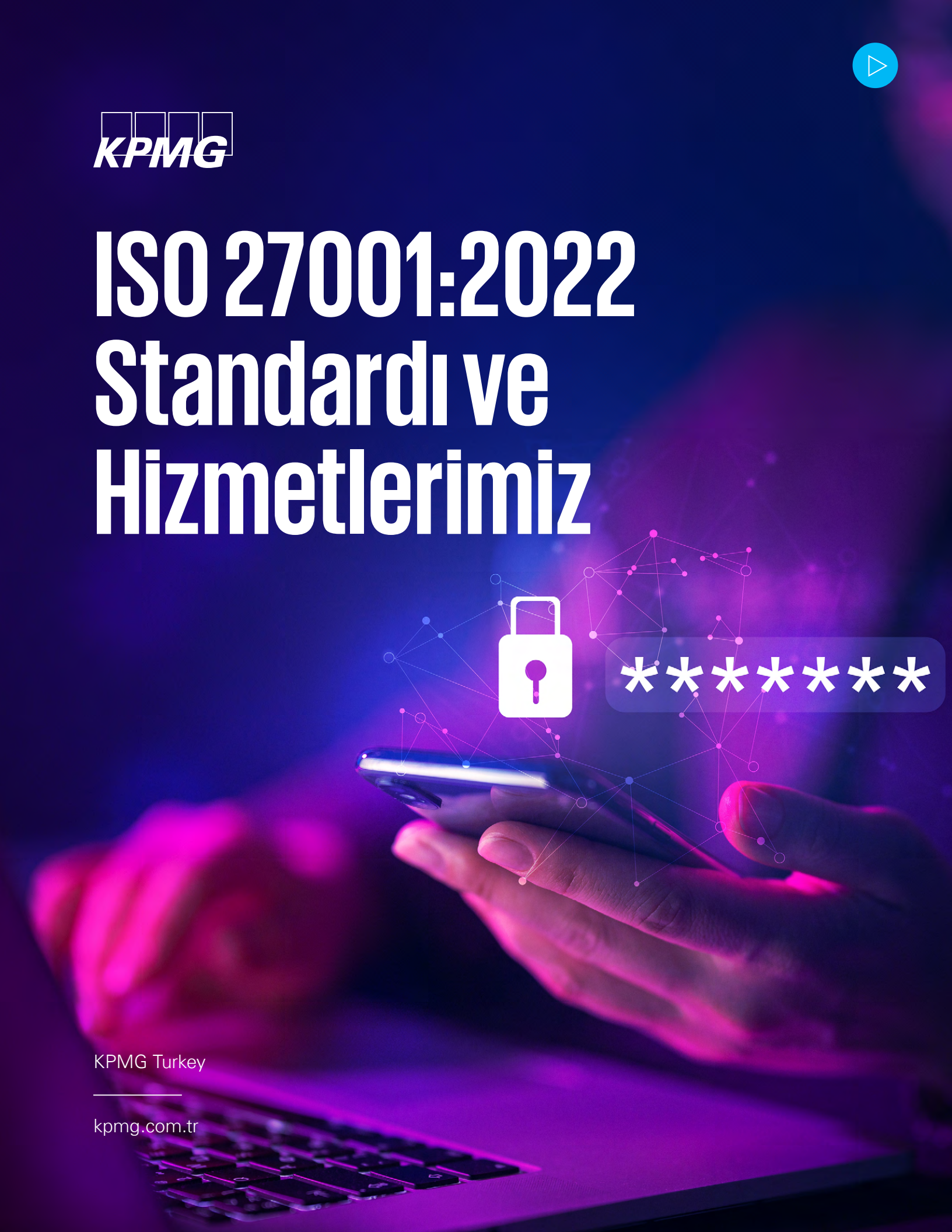
ISO 27001:2022 Standardı ve Hizmetlerimiz



KPMG Turkey

kpmg.com.tr

İçindekiler

ISO 27001 Bilgi Güvenliği Yönetim Sistemi Hakkında

ISO 27001, Uluslararası Standardizasyon Organizasyonu (ISO) tarafından yayımlanan, ISO 27000 bilgi güvenliği standartları ailesinin denetlemeye tabi olan standartlarından biridir.

ISO 27001, finansal verilerin, bilgi varlıklarının ve müşterilere ait özel ve kişisel bilgilerin saklanması ve korunmasına yönelik olarak, başta insanlar olmak üzere süreçler ve bilgi sistemlerini kapsayan ve de sürekli iyileştirmeyi ilke edinen bir bilgi güvenliği yönetim sistemi çerçevesi sunmak amacıyla oluşturulmuştur.

ISO 27001 güncellenmiş – 25 Ekim 2022'de yeni versiyonu olan ISO/IEC 27001:2022 yayımlanmıştır.

ISO 27001 Bilgi Güvenliği Yönetim Sistemi

ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ AVANTAJLARI

- Bilgi güvenliği yönetimi için bir çerçeve sunar ve bilgi güvenliği kontrollerinizin etkinliğini düzenli olarak gözden geçirmeyi sağlar.
- Bilgi güvenliği risklerini yönetmek için bir çerçeve sunar. Böylece riskler için uygun metotlar, yönetim ve teknik uygulama kontrollerinin benimsemenize ve kullanmanıza yardımcı olur.
- Kuruluşunuzun tamamına ya da seçilmiş alanlarına/ süreçlerine kontrol uygulama esnekliği sağlar.
- Verilerinizin güvenliği ile ilgili sizi yönlendirip müşteri ve kurumsal memnuniyeti sağlamaya yardımcı olur.
- Bilgi güvenliğiyle ilgili olarak artan müşteri beklentilerine cevap vermeyi kolaylaştırır.
- Tedarikçi ilişkilerinizin gelişmesini, performans takip ve yönetimini sağlar.
- Bilgi güvenliğinin bir öncelik olduğunu gösterir. Böylece bir yönetim sisteminin yürürlükte olduğu konusunda paydaşlara ve 3 taraflara güvence verir.
- Kuruluşunuz genelinde bilgi güvenliği farkındalığının oluşmasını sağlar.
- Yasal şartlara uygunluk konusunda sizi yönlendirir ve uygunluğunuzu arttırır.

Genel Bakış

Genel olarak, 2013 revizyonuyla karşılaştırıldığında, ISO 27001:2022 revizyonundaki değişiklikler küçük ila orta ölçekli olarak değişim göstermektedir.

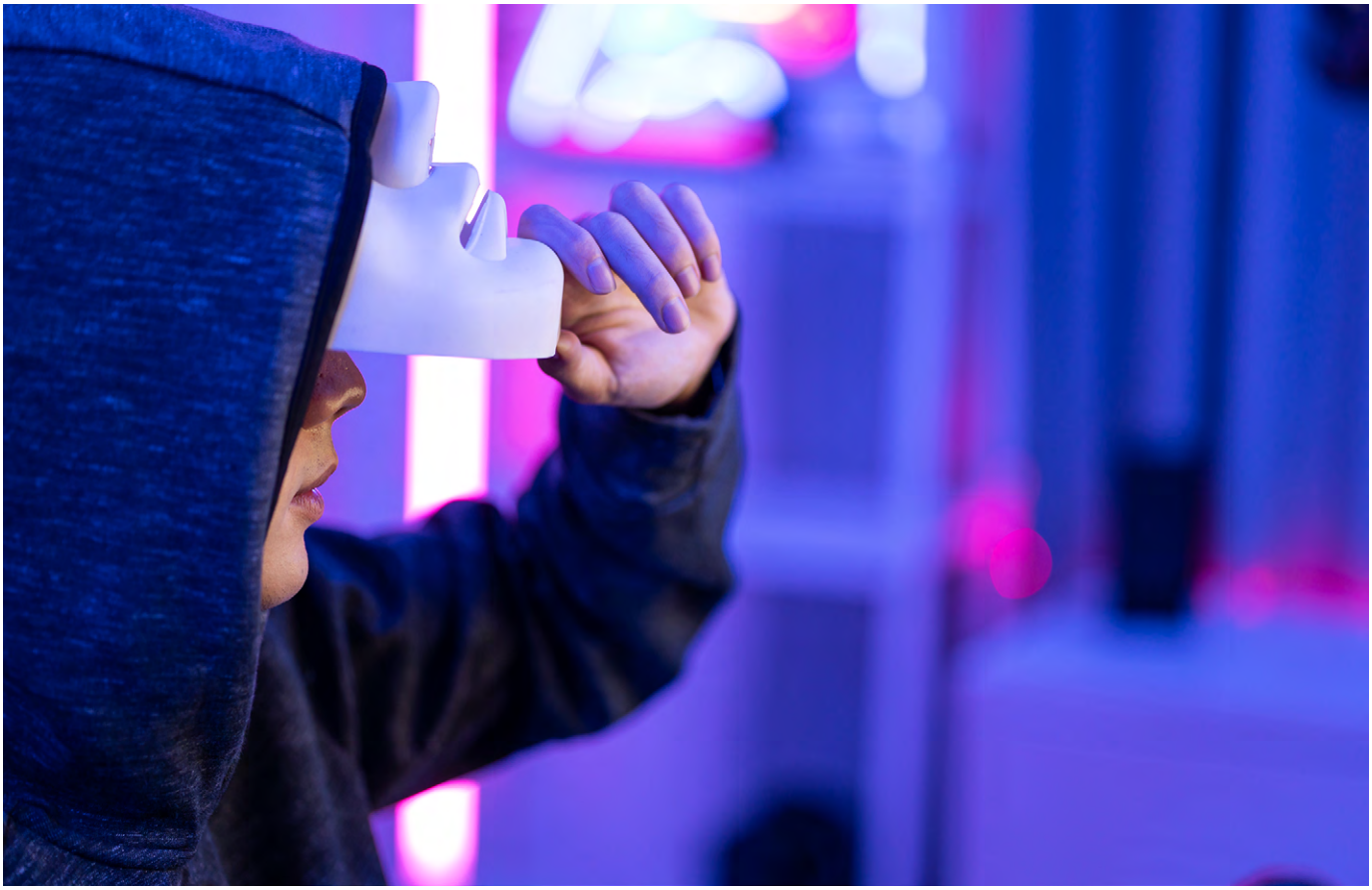
1 Uluslararası Standardizasyon Örgütü (ISO) tarafından 2013 yılında yayınlanan ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi Standardı Türkiye'de de yaygın olarak kullanılmaktadır.

2 Dünyanın önde gelen bilgi güvenliği standardı olan ISO 27001 güncellenmiş –ve 25 Ekim 2022'de yeni ISO/IEC 27001:2022 versiyonu yayınlanmıştır.

3 ISO 27001:2022 Standartında 4'ten 10'a kadar olan zorunlu maddelerin metni, esas olarak ISO 9001, ISO 14001 ve diğer ISO yönetim standartları ve Annex SL ile uyum sağlamak için kısmi oranda değiştirilmiştir.

4 Temel değişiklikler Ek A maddelerinde gerçekleştirilmiştir.

Ek A'daki kontrol sayısı 114'ten 93'e düşürülmüştür ve 2013 revizyonundaki 14 bölüm birleştirilerek 4 bölümde kategorize edilmiştir.



ISO 27001:2022 Geçiş Rehberi

Mevcut ISO 27001 sertifikalarının durumu ve ISO 27001:2022'e geçiş ile ilgili olarak Uluslararası Akreditasyon Forumu (IAF) tarafından bir rehber yayınlanmıştır.

IAF tarafından yayımlanan "ISO/IEC 27001:2022 için geçiş gereksinimleri" belgesine göre, halihazırda ISO 27001:2013'e göre sertifika sahibi organizasyonlar için, ISO 27001:2022'ye geçişin 31 Ekim 2025'e kadar tamamlanması gerekmektedir.

Geçiş için toplamda **36** aylık bir süre belirlenmiştir.

Standardın yayımlanmasından sonraki ilk 12 ay içinde önceki versiyona göre ilk belgelendirme tetkikleri yapılmaya devam edebilecektir.

Standardın yayımlanmasının üzerinden 12 ay geçtikten sonra ilk belgelendirmeler mutlaka yeni versiyona göre yapılacaktır.

3 yıllık geçiş süreci sonunda 2013 versiyonuna ait tüm sertifikalar geçerliliğini kaybedecektir.

ISO 27001:2022 Ana Madde Değişikliklerine İlişkin Genel Bakış:

ISO 27001:2013	ISO27001:2022
MADDE 4.2	Madde 4.4'e (Bilgi güvenliği yönetim sistemi), BGYS'nin bir parçası olarak süreçler ve bunların etkileşimleri için planlama gerektiren bir ibare eklenmiştir.
MADDE 4.4	Madde 4.4'e (Bilgi güvenliği yönetim sistemi), BGYS'nin bir parçası olarak süreçler ve bunların etkileşimleri için planlama gerektiren bir ibare eklenmiştir.
MADDE 5.3	Madde 5.3'te (Kurumsal roller, sorumluluklar ve yetkiler), rollerin iletişiminin kuruluş içinde dahili olarak yapıldığını açıklığa kavuşturmak için bir ifade eklenmiştir.
MADDE 6.2	Madde 6.2'ye (Bilgi güvenliği hedefleri ve bunlara ulaşmak için planlama), hedeflerin izlenmesini gerektiren (d) maddesi eklenmiştir.
MADDE 6.3	BGYS'deki bir değişikliğin planlı bir şekilde yapılmasını gerektiren Madde 6.3 (Değişikliklerin planlanması) eklenmiştir.
MADDE 7.4	Madde 7.4'te (İletişim), iletişim için süreçlerin ayarlanmasını gerektiren (e) maddesi silinmiştir.
MADDE 8.1	Madde 8.1'de (Operasyonel planlama ve kontrol), güvenlik süreçleri için kriterlerin oluşturulması ve bu kriterlere göre süreçlerin uygulanması için yeni gereksinimler eklenmiştir. Aynı fıkrada, hedeflere ulaşmak için planların uygulanması şartı kaldırılmıştır.
MADDE 9.3	Madde 9.3'te (Yönetim gözden geçirmesi), ilgili taraflardan gelen girdilerin, onların ihtiyaçları, beklentileri ve BGYS ile ilgili olması gerektiğini açıklayan yeni madde 9.3.2 c) eklenmiştir.
MADDE 10	Madde 10'da (İyileştirme), alt maddeler yer değiştirmiştir, bu nedenle ilki Sürekli iyileştirme (10.1) ve ikincisi Uygunsuzluk ve düzeltici faaliyet (10.2) olup, bu maddelerin metni değişmemiştir.

ISO 27001: 2022 ISO 27001 :2013 EK-A Madde Değişiklikleri Adresleme

ISO 27001:2013	ISO 27001:2022
A.6.1.4 Özel ilgi gruplarıyla iletişim	A.5.7 Tehdit istihbaratı
A.15.x Tedarikçi ilişkileri	A.5.23 Bulut hizmetlerinin kullanımı için bilgi güvenliği.
A.17.1.3 Bilgi güvenliği sürekliliğinin doğrulanması, gözden geçirilmesi ve değerlendirilmesi	A.5.30 İş sürekliliği için BİT hazırlığı
A.9.2.5 Kullanıcı erişim haklarının gözden geçirilmesi	A.7.4 Fiziksel güvenlik
A.14.2.5 Güvenli sistem mühendisliği ilkeleri	A.8.9 Konfigürasyon yönetimi
A.18.1.3 Kayıtların korunması	A.8.10 Veri imha
A.14.3.1 Test verilerinin korunması	A.8.11 Veri maskeleme
A.12.6.1 Teknik güvenlik açıklarının yönetimi	A.8.12 Veri sızıntısının önlenmesi
A.12.4.x Kayıt ve izleme	A.8.16 İzleme faaliyetleri
A.13.1.2 Ağ hizmetlerinin güvenliği	A.8.23 Web filtreleme
A.14.2.1 Güvenli geliştirme politikası	A.8.28 Veri Kodlama

ISO 27001:2022 Size Nasıl Yardımcı Olabiliriz?

Bilgi Güvenliği Yönetim Sistemi kurulum ve denetimi anlamında tecrübeli ve denetçi sertifikalı (CB DDO, ISO27001) danışman ekibimizle, geçiş sürecinizi zamanında ve sorunsuz bir şekilde tamamlamanızı sağlamak amacıyla aşağıdaki başlıklarda standart gereksinimlerine ve kurumunuzun ihtiyaçlarına özgü hizmetler sunmaktayız.

ISO 27001:2013-ISO 27001:2022 Geçiş Değerlendirme Desteği

- Mevcut BGYS süreçlerinin ve dokümantasyonların gözden geçirilmesi.
- Varlık envanterinin güncellenmesi.
- Risk yönetiminin gözden geçirilerek yeni versiyona uyarlanması.
- Uygulanabilirlik bildirgesinin güncellenmesi. (Bu çalışma, ISO 27001:2013 standardına atıf yapılarak gerçekleştirilecektir)

ISO 27001:2022 Geçiş Eğitimi

- ISO 27001:2013 ve ISO27001:2022 standartları arasındakı farklar.
- ISO27001:2022 standarına geçiş süresinde alınması gereken aksiyonlar. (siber dayanıklılık, yasal regülasyonlar, teknik kontroller)

ISO 27001:2022 Yeni Belgelendirme Süreci Danışmanlık Desteği

- BGYS kapsam ve süreçlerinin belirlenmesi.
- Politika ve prosedürlerin hazırlanması.
- Bilgi güvenliği farkındalığının arttırılması.
- Varlık envanterinin oluşturulması.
- Risk yönetim metodolojisi ve risk analiz çalışmaları.
- İç denetim desteği.

CB DDO & ISO 27001:2022 Entegre Danışmanlık Desteği

- CB DDO & ISO 27001 gerekisinimlerine uygun olarak kapsamın belirlenmesi; süreçlerin, politka ve prosedürlerin değerlendirilmesi.
- CB DDO ve ISO 27001 gereksinimlerine uygun olarak varlık envanterinin ve uygulanacak tedbirlerin oluşturulması.
- Risk yönetim metodolojisini oluşturulması ve uygulanması.
- DDO ve ISO 27001:2022 eşleştirme tablolarının hazırlanması.

ISO 27001:2022 İç Denetim ve Yönetim Gözden Geçirme Faaliyetleri Desteği

- İç denetim planlama, uygulama ve raporlama aşamalarında uçtan uca destek sağlanması.
- Uygunsuzluklara yönelik düzeltici faaliyetlerin belirlenmesi.
- Yönetim gözden geçirme toplantılarına katılım sağlanarak destek sunulması.
- Dış denetim süreçlerine destek verilmesi.

İletişim:

Sezgin Topçu
Yönetişim, Risk &
Uyum ve Teknoloji
Risk Lideri,
Şirket Ortağı
stopcu@kpmg.com

Ümit Yalçın Şen
Siber Güvenlik
Hizmetleri Lideri,
Şirket Ortağı
umitsen@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
Folkart Towers Adalet Mah. Manas
Bulvarı No:39 B Kule Kat: 35
Bayraklı 35530 İzmir
T : +90 232 464 2045

Bursa
İnallar Cadde Plaza, Balat
Mahallesi Mudanya Yolu Sanayi
Caddesi No: 435 K:5
D:19-20 Nilüfer
T : +90 224 503 80 00

kpm.com.tr
kpmveri.com