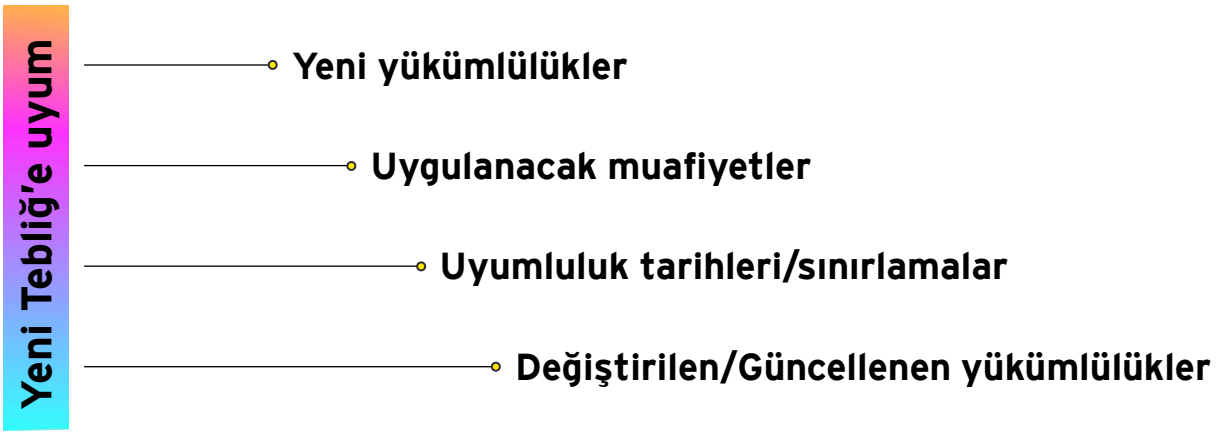

Bilgi Sistemleri Yönetimine İlişkin Usül ve Esaslar Tebliği Kılavuzu
The better the question. The better the answer.
The better the world works.
EY
Shape the future with confidence

Giriş

Bilgi Sistemleri Yönetimine İlişkin Usül ve Esaslar Tebliği (VII-128.10), 13 Mart 2025 tarihli Resmi Gazete'de yayımlanmıştır. Söz konusu Tebliğ'in 2. maddesinde tanımlanan Kurum, Kuruluş ve Ortaklıkların Tebliğ hükümlerine uyumluluk sağlaması zorunlu hale getirilmiştir.

5 Ocak 2018 tarihinde yayımlanan Bilgi Sistemleri Yönetimi Tebliği (VII-128.9) ile kıyaslamalı olarak hazırlanan Kılavuz, aşağıda yer alan kapsamda detaylandırılmıştır:

- VII-128.10 seri/sıra numaralı Tebliğ ile yürürlüğe girecek olan yeni yükümlülükler,
- VII-128.10 seri/sıra numaralı Tebliğ ile değiştirilen/güncellenen yükümlülükler,
- VII-128.10 seri/sıra numaralı Tebliğ hükümleri çerçevesinde uygulanacak muafiyetler,
- VII-128.10 seri/sıra numaralı Tebliğ hükümlerine uyum için gerekli süreler/sınırlamalar



1 Güncellenen Tebliğ'deki yeni konular

13 Mart 2025 tarihli Resmi Gazete'de yayımlanan Bilgi Sistemleri Yönetimine İlişkin Usül ve Esaslar Tebliği (VII-128.10) içerisinde Kurum, Kuruluş ve Ortaklıklar için uyum sağlanması gereken yeni yükümlülükler bulunmaktadır.

Tebliğ'e yeni eklenen, önem arz eden ve uyumluluk sağlanması beklenen hususlara ilişkin detaylar aşağıdaki tabloda detaylandırılmıştır.

Madde	Uyumluluk sağlanması beklenen konular
Madde 14 - Bilgi sistemlerinin işletimi	▪ Bilgi sistemleri hizmetlerinin sürekliliği, kritik sistemlerin performans takibi, kapasite planlaması, güvenlik açıkları yönetimi ▪ Yapılandırma yönetimi, taşınabilir ortamların kullanımı ▪ Zararlı yazılımlara karşı koruma, elektronik posta güvenliği
Madde 26 - Uygulama Güvenliği	▪ Uygulama güvenliği kontrolleri ▪ Veri girişi ve doğrulama, çıktı bütünlüğü ▪ Hata mesajlarının güvenliği, hata kayıt ve bildirim mekanizması ▪ Çerez güvenliği, çerezlerin benzersiz olması ▪ Geçici kullanıcı erişimleri ▪ API erişim güvenliği, API trafik yönetimi, oturum zaman aşımı ▪ Kaynak kod güvenliği, zararlı girdi engelleme, yüklenen dosyaların güvenliği ▪ Mobil uygulamalarda SMS ile kimlik doğrulama kısıtı ▪ SIM kart ve operatör değişikliği kontrolleri ▪ Kritik işlemler için ek kimlik doğrulama, güvenli tek kullanımlık parola üretimi ▪ Aktif oturum bilgilendirme, başarısız kimlik doğrulama bildirimi ▪ Mobil uygulama güncellemeleri ▪ Cihaz güvenlik gereksinimleri, eşzamanlı oturum açma engeli ▪ Cihaz tanıma özelliği, cihaz güvenliği ve risk yönetimi, cihaz üreticisine bağlı kimlik doğrulama
Madde 29 - İç Denetim	▪ Yıllık denetim zorunluluğu ▪ Dış kaynak kullanımı yasağı ▪ İç denetçiler ve lisans zorunluluğu ▪ Denetim sonuçlarının raporlanması ▪ Aksiyon planı ve üst yönetim onayı, denetim raporu ▪ Yetkilendirme bildirimi

2 Güncellenen Tebliğ'deki değiştirilen/güncellenen hususlar

13 Mart 2025 tarihli Resmi Gazete'de yayımlanan Bilgi Sistemleri Yönetimine İlişkin Usül ve Esaslar Tebliği (VII-128.10) çerçevesinde değiştirilen/güncellenen yükümlülüklere ilişkin özet bilgiler aşağıdaki tabloda detaylandırılmıştır.

Değiştirilen / Güncellenen önemli hususlar
▪ Bilgi sistemlerinin yönetimine ilişkin politika ve prosedürlerin yazılı hale getirilerek yönetim kurulu veya üst yönetim tarafından onaylanması ▪ Bilgi sistemleri yönetimine ilişkin rol ve sorumlulukların yazılı hale getirilerek üst yönetim tarafından onaylanması ▪ Bilgi güvenliği politikasının yılda en az 1 defa gözden geçirilmesi ▪ Bilgi güvenliği sorumlusunun bilgi sistemleri yönetiminde sorumluluk almaması ve doğrudan üst yönetime bağlı çalışması ▪ Bilgi varlıklarının dikkate alınarak, yılda en az 1 defa gerçekleştirilecek risk yönetimi (*kriterlerin belirlenmesi, analizlerin gerçekleştirilmesi, risk seviyelerinin belirlenmesi, risklere yönelik aksiyonların belirlenmesi, iyileştirici faaliyetlerin takibi ve raporlanması*) çalışmaları ▪ Bilgi sistemleri kontrolleri nezdinde gerçekleştirilen değerlendirmelerin ve yapılan çalışmaların yılda en az 1 kez üst yönetime raporlanması ▪ Varlık envanterinin oluşturulmasında kullanılacak bilgiler ▪ Bilgi varlıklarının güvenlik sınıflarının belirlenmesine ilişkin oluşturulacak kılavuz ve üst yönetim tarafından onay ▪ Bilgi varlıklarına ilişkin hazırlanacak kullanım prosedürleri ve üst yönetim onayı ▪ Bilgi sistemi kapsamında sunulan hizmetler ve süreçler için oluşturulacak envanter ▪ Veri merkezlerine erişim esnasında uygulanacak güvenlik kontrolleri ve sürekliliğin/gizliliğin korunması adına uygulanacak kontroller

2 Güncellenen Tebliğ'deki değiştirilen/güncellenen hususlar

13 Mart 2025 tarihli Resmi Gazete'de yayımlanan Bilgi Sistemleri Yönetimine İlişkin Usül ve Esaslar Tebliği (VII-128.10) çerçevesinde değiştirilen/güncellenen yükümlülüklere ilişkin özet bilgiler aşağıdaki tabloda detaylandırılmıştır.

Değiştirilen / Güncellenen önemli hususlar

- Uzaktan erişim sürecinde bilgi güvenliği sorumlusu onayının alınması ve erişilen cihaza yönelik uygulanacak güvenlik kontrolleri
- Kurum ağında uygulanacak güvenlik tedbirleri (*Whitelist/ Blacklist, DDoS, güçlü şifreleme protokolleri/ kimlik doğrulama kontrolleri*)
- Kimlik doğrulama esnasında uygulanacak kontroller
- Parola yönetiminde uygulanacak güvenlik önlemleri
- Ayrıcalıklı/ kullanıcı hesaplarında uygulanacak güvenlik kontrolleri
- Bilgi varlığı sorumlusu tarafından yürütülecek yetki gözden geçirme kontrolleri ve uygulanacak aksiyonlar
- Dış hizmet alımı sürecinde veya hizmetin sonlanması durumunda uygulanacak/yürütülecek faaliyetler (*sözleşme içerisinde bulunması gereken hükümler, hizmetin değerlendirilmesine ve raporlanmasına ilişkin hükümler*)
- Denetim izlerinin yönetilmesine ve takip edilmesine yönelik kontroller
- Bilgi güvenliği ihlallerinin yönetimi, ihlal esnasında işletilecek süreçler, müdahale planlarının testleri, kurumsal SOME kurulumu
- Yazılım geliştirme/değişiklik yönetimi süreçlerinde uygulanacak kontroller ve yürütülecek faaliyetler
- Felaket kurtarma merkezinin birincil sistemle aynı risklere maruz kalmaması, iş-etki analizlerinde RTO / RPO değerlerinin belirtilmesi
- Bilgi sistemleri sürekliliğini sağlama amacıyla yürütülecek faaliyetler (*geri dönüş testleri, kurula yapılacak bilgilendirmeler*)

3 Güncellenen Tebliğ'deki muafiyetler

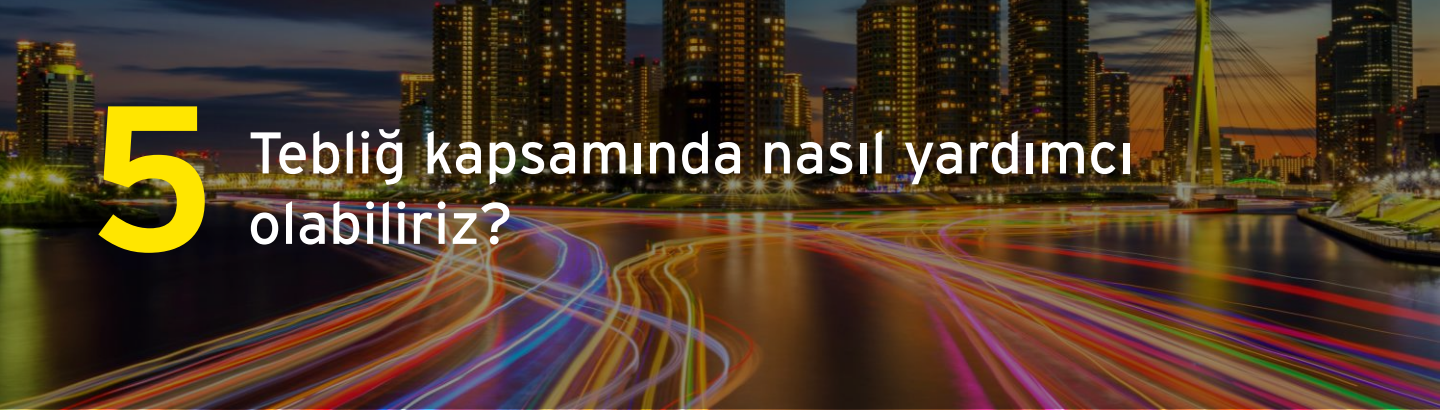
13 Mart 2025 tarihli Resmi Gazete'de yayımlanan Bilgi Sistemleri Yönetimine İlişkin Usül ve Esaslar Tebliği (VII-128.10) çerçevesinde uygulanacak olan muafiyetler aşağıdaki tabloda detaylandırılmıştır.

Muaf kurum/kuruluş/ortaklıklar	Muafiyet maddeleri
▪ Asgari özsermaye yükümlülüğünde Portföy Yönetim Şirketleri ve Bu Şirketlerin Faaliyetlerine İlişkin Esaslar Tebliği'nin 28. maddesinin 1.fıkrasının (a), (b) ve (c) bentlerine tabi portföy yönetim şirketleri ▪ Dar yetkili aracı kurumlar ▪ Varlık kiramala şirketleri ▪ İpotek 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	▪ 8. maddenin 5., 6. ve 7. fıkraları ▪ 10. maddenin 6. ve 7. fıkraları ▪ 12. maddenin 1. fıkrasının (b) bendi ▪ 13. maddenin 11. ve 13 fıkraları ▪ 14. maddenin 5., 6. ve 8. fıkraları ▪ 15. maddenin 3., 6., 7., 8. ve 9. fıkraları ▪ 16. maddenin 8. ve 9. fıkraları ▪ 17. maddenin 2. fıkrası ▪ 18. maddenin 2. fıkrası ▪ 22. maddenin 7., 9. ve 10. fıkraları ▪ 24. maddenin 7. ve 8. fıkraları ▪ 25. maddenin 4., 5., 6. ve 11. fıkraları ▪ 26. maddeyi ▪ 27. maddenin 3., 9., 10., 11. ve 15 fıkraları ▪ 28. madde ▪ 29. madde
▪ Borsa İstanbul A.Ş., ▪ İstanbul Takas ve Saklama Bankası A.Ş. ▪ Merkezi Kayıt Kuruluşu A.Ş. ▪ Türkiye Sermaye Piyasaları Birliği ▪ Türkiye Değerleme Uzmanları Birliği ▪ Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu A.Ş.	▪ 29. maddenin 7. fıkrası
▪ Bilgi Sistemleri Bağımsız Denetim Tebliği (III-62.2) hükümleri kapsamında, bilgi sistemleri bağımsız denetim zorunluluğu bulunmayan halka açık ortaklıklar	▪ 27.maddenin 1.fıkrası

4 Güncellenen Tebliğ'deki süreler/sınırlamalar

13 Mart 2025 tarihli Resmi Gazete'de yayımlanan Bilgi Sistemleri Yönetimine İlişkin Usül ve Esaslar Tebliği (VII-128.10) çerçevesindeki yükümlülükler nezdindeki uygulanması gereken hükümlerin uyumluluk sürelerine aşağıda yer verilmiştir.

Tebliğ'in yürürlülük tarihi	30.06.2025
Kripto varlık hizmet sağlayıcıları	Madde 27: 31.12.2025
Kripto varlık hizmet sağlayıcıları	Madde 29.3: 31.12.2026
Kurum, kuruluş, ortaklıklar	Tebliğ hükümleri: 31.12.2025
Kurum, kuruluş, ortaklıklar	Madde 29.3: 31.12.2026



5 Tebliğ kapsamında nasıl yardımcı olabiliriz?

Danışmanlık

Proje planlaması

- Kurum nezdinde yürütülen bilgi sistemleri süreçlerinin anlaşılması, detaylandırılması,
- Projenin nasıl gerçekleştirileceğinin ve zaman çizelgesinin oluşturulması

Durum analizi

- Kurum nezdinde yürütülen süreçlerin, Tebliğ'deki yükümlülüklere uyumluluk durumlarının değerlendirilmesi,
- Mevcut durum değerlendirmesi sonucunda düzeltilmesi / geliştirilmesi gereken alanların/süreçlerin tespiti

Aksiyon planı

- Düzeltici aksiyonların ve alınacak olan aksiyonlar çerçevesindeki ihtiyaçların tespiti
- Tebliğ'e uyum sağlanması amacıyla yol haritasının belirlenmesi ve uyum programının hazırlanması

Denetim

Denetimin planlanması

- Denetim kapsamının ve ekibinin belirlenmesi
- Kurum nezdinde yürütülen bilgi sistemleri faaliyetlerinin anlaşılması
- Denetimde ele alınacak süreçlerin belirlenmesi

Denetimin gerçekleştirilmesi

- Kurum nezdinde yürütülen süreçlerin, Tebliğ'de belirtilen yükümlülüklere istinaden işletildiğinin değerlendirilmesi,
- Mevcut durumun değerlendirilmesi ve gelişim alanlarının tespiti

Raporlama

- Kapsam dahilindeki süreçlerle ilgili gözlemler hakkında ilgili paydaşlarla karşılıklı mutabakat için görüşülmesi ve gözlemlerin paylaşılması
- Bağımsız denetim raporunun hazırlanması

6 Neden EY?

Dünyada ve Türkiye'de EY

EY olarak uluslararası ve yerel çapta birçok sektörden firmaya ve kamu kurumuna danışmanlık, güvence, vergi, strateji ve kurumsal finansman hizmetleri sunuyoruz. 150'den fazla ülkede, 700'den fazla ofisimiz ve 395.000'den fazla çalışanımızla tüm sektörlerden firmalara, hükümetlere ve uluslararası organizasyonlara geniş bir yelpazedeki politika ve iş sorunlarını çözmelerinde destek veriyoruz.

Tek bir çalışma stratejisi, ortak inovasyon ve bilgi paylaşım kültürü çatısı altında, dünya genelindeki yerel ofislerimizi bir arada tutan ağımızla kapsamlı profesyonel hizmetler sunuyoruz. Bu benzersiz "Tek firma" yaklaşımımız, tüm çalışanlarımızın müşterilere coğrafi ve kurumsal sınırları aşan bir hizmet vermesini sağlıyor.

EY Türkiye olarak 40 yılı aşkın süredir danışmanlık, güvence, vergi, strateji ve kurumsal finansman olmak üzere dört profesyonel hizmet alanında müşterilerimize destek oluyoruz. 5 büyük şehirdeki (İstanbul, Ankara, İzmir, Bursa, Adana) 6 ofisimizde, 1.800'den fazla çalışanımızla Türkiye'deki en büyük profesyonel hizmet firmalarından biriyiz.

Küresel uzmanlığımızı ve yerel kaynakları özelleştirilmiş çözümlerle birleştirerek müşterilerimize artı değer sağlıyoruz.

Hizmetlerimiz

EY olarak, dünya genelinde pek çok sektörden firmaya pazar stratejisi geliştirmeden teknolojiye, süreç iyileştirme ve organizasyonel dönüşüme kadar geniş bir çerçevede hizmet sunuyoruz. Veri, yapay zekâ ve ileri teknolojiden yararlanarak müşterilerimizin geleceği güvenle şekillendirmelerine, günümüzde ve gelecekte karşılaşabilecekleri sorunlara çözüm üretmelerine destek oluyoruz. Daha iyi bir çalışma dünyası oluşturmak amacıyla müşterilerimiz, çalışanlarımız ve içinde yer aldığımız toplum için var gücümüzle çalışıyoruz. Sadece geleceğe uyum sağlamakla kalmıyor, tüm paydaşlarımızla birlikte geleceği hep birlikte güvenle şekillendiriyoruz.

EY | Daha iyi bir çalışma dünyası oluşturuyoruz

EY olarak, müşterilerimiz, çalışanlarımız, toplum ve dünyamız için değer yaratırken sermaye piyasalarında güveni inşa ediyor ve bu şekilde daha iyi bir çalışma dünyası oluşturuyoruz.

Veri, yapay zekâ ve ileri teknolojiden yararlanarak müşterilerimizin geleceği güvenle şekillendirmesine, günümüzde ve gelecekte karşılaşabilecekleri sorunlara çözüm üretmelerine yardımcı oluyoruz.

EY ekipleri olarak bağımsız denetim, danışmanlık, güvence, hukuk, kurumsal finansman, strateji ve vergi hizmetleri sunuyoruz. Dünya çapında 150'den fazla ülkede, küresel ağımız, kapsamlı iş birliklerimiz ve güçlü sektörel deneyimizle müşterilerimize hizmet veriyoruz.

Hep birlikte geleceği güvenle şekillendiriyoruz.

ey.com/tr

linkedin.com/ernstandyoung
instagram.com/eyturkiye
x.com/EY_Turkiye
facebook.com/ErnstYoungTurkiye

İletişim

Feyyaz Burak Baysal
Teknoloji Risk Hizmetleri Lideri – EY Türkiye
burak.baysal@tr.ey.com

Tunç Tütüncüoğlu
Teknoloji Risk Hizmetleri Direktörü – EY Türkiye
tunc.tutuncuoglu@tr.ey.com

Kurtuluş Atıcı
Teknoloji Risk Hizmetleri Müdürü – EY Türkiye
kurtulus.atici@tr.ey.com

Shape the future with confidence