BİLGİ SİSTEMLERİ YÖNETİMİ TEBLİĞİ

Dr. Emre ERDİL
Bilgi İşlem, İstatistik ve Enformasyon Dairesi

İstanbul

Nisan 2018

Gündem

- Giriş
- Tarihçe
- Düzenlemenin Niteliği
- Tebliğin Bölümleri

Giriş

- 5 Ocak 2018 tarihinde Bilgi Sistemleri Yönetimi Tebliği'nin yayımlanması
- Geniş bir kapsam alanı
- Yeni yükümlülükler
- Tebliğ öncesinde yatırım kuruluşlarına ilişkin bilgi sistemleri düzenlemeleri

Bilgi Sistemleri Düzenlemeleri - Tarihçe

- Kaldıraçlı alım satım faaliyeti yürüten aracı kurumların bilgi işlem altyapısına yönelik bilgi işlem altyapısı ilkeleri
- Portföy aracılığı ve genel saklama faaliyetleri
- Yeni Sermaye Piyasası Kanunu ile Kurul'a verilen görev
- Tebliğ taslaklarının hazırlanması ve görüşe açılması
- Tebliğlerin yürürlüğe girmesi

Bilgi Sistemleri Düzenlemeleri – Neden İhtiyaç Var

- Bilgi sistemlerinin sermaye piyasası faaliyetlerindeki rolünün büyüklüğünün artması
- Altyapı ve destek faaliyeti olarak işlev gören bilgi sistemleri faaliyetlerinin işin asli unsurlarından biri haline gelmesi
- Sermaye piyasası faaliyetleri kapsamında bilgi sistemlerine yönelik risklerin oluşmaya ve artmaya başlaması

Düzenlemenin Niteliği

- İlkesel yaklaşım
- Teknik detayların olmaması
- Kontrol alanlarının gereksinimlerinin ilkesel olarak belirlenmesi
- Teknik gereksinimlerin Kurum, Kuruluş ve Ortaklıklarca belirlenmesi
- Kimlik doğrulama örneği
  - Risk değerlendirme sonucuna göre kimlik doğrulama yönteminin belirlenmesi
  - Belirlenen yöntemin Tebliğce düzenlenen kontrolleri sağlaması

Tebliğin Bölümleri

- **Birinci Bölüm**
  - Amaç, Kapsam, Dayanak ve Tanımlamalar
- **İkinci Bölüm**
  - Bilgi Sistemlerinin Yönetilmesi
- **Üçüncü Bölüm**
  - Bilgi Sistemleri Kontrolleri
- **Dördüncü Bölüm**
  - Muafiyetler ve Diğer Hususlar

Bilgi Sistemlerinin Yönetilmesi (Tebliğ 2. Bölüm)

- Bilgi sistemlerinin
  - Yönetsel hiyerarşi içinde yer alması
  - Kurumsal yönetim uygulamalarının parçası olması
- Bilgi sistemlerine ilişkin stratejilerin iş hedefleri ile uyumlu olması
- Bilgi güvenliği politikasının oluşturulması
  - Bilgi güvenliğini (gizlilik, bütünlük, erişilebilirlik) sağlamaya ilişkin ilkeler
  - Rol ve sorumlulukların tanımlanması
  - Bilgi sistemlerine ilişkin risklerin yönetimi

Bilgi Sistemlerinin Yönetilmesi (Tebliğ 2. Bölüm)

- **Üst yönetimin gözetimi ve sorumluluğu**
  - Bilgi güvenliği politikasının uygulanması
  - Bilgi sistemleri kontrollerinin tesisi
  - Kritik bilgi sistemi projelerinin gözden geçirilmesi, onaylanması
  - Bilgi sistemleri risklerinin yönetimi
  - Bilgi güvenliği ihlallerinin izlenmesi
  - Çalışanların bilgi güvenliği farkındalığının artırılması
  - Bilgi sistemleri güvenliği sorumlusunun belirlenmesi
  - İş sürekliliği planının hazırlanması

Bilgi Sistemlerinin Yönetilmesi (Tebliğ 2. Bölüm)

- **Bilgi Sistemleri Risk Yönetimi**
  - Bilgi sistemlerine ilişkin riskleri ölçmek, izlemek, işlemek ve raporlamak
  - Risk yönetimi süreç ve prosedürlerinin tesis edilmesi ve güncelliğinin sağlanması
  - Bilgi sistemlerinin artan ağırlığının dikkate alınması gerekmekte ve dinamik bir risk yönetim süreci öngörülmekte
  - Periyodik risk analizi
  - Zafiyet/teknik açıklıkların zamanında değerlendirilmesi
  - Periyodik sızma testi
    - Kuralları tebliğ ekinde belirlenmiş
    - Belge sahibi kişi/kurumlarca

Bilgi Sistemleri Kontrolleri (Tebliğ 3. Bölüm)

- **Kontrollerin tesisi ve yönetimi**
  - Bilgi güvenliğini sağlamak ve bilgi sistemlerinden kaynaklanan riskleri yönetmek için
  - Her kontrol süreci için:
    - Süreç sahibinin, faaliyetlerin ve sorumlulukların belirlenmesi
    - Süreçlerin hedef ve amaçlarının tanımlanması
    - Süreçlerin performansının ölçülebilir olması
  - Kontrollerin etkinlik, yeterlik ve uygunluğunun gözetimi ve önemli kontrol eksikliklerinin üst yönetime raporlanması

Bilgi Sistemleri Kontrolleri (Tebliğ 3. Bölüm)

- Varlık yönetimi & Görevler ayrılığı & Fiziksel ve çevresel güvenlik
- Ağ güvenliği & Zaman senkronizasyonu
- Kimlik doğrulama & Yetkilendirme
- İşlemlerin ve kayıtların bütünlüğü & Veri gizliliği
- Dış kaynak yönetimi
- Üçüncü taraflarla bilgi değişimi
- Müşteri bilgilerinin gizliliği & Müşterinin bilgilendirilmesi
- Kayıt mekanizmasının oluşturulması
- Bilgi sistemleri edinimi & Bilgi sistemleri sürekliliği
- Bilgi güvenliği ihlali & Değişim yönetimi

Bilgi Sistemleri Kontrolleri

- **Dış kaynak yönetimi** → dış kaynak yoluyla hizmet alımının getireceği riskleri yönetmek
- Gözetim mekanizması kurulması
  - İş sürekliliğine ilişkin gerekli önlemlerin alınması
  - Alınan hizmetin ölçülmesi ve değerlendirilmesinde sorumluluğun Kurum, Kuruluş ve Ortaklıklar'da olması
- Sözleşme imzalanması
- Erişim haklarının özel olarak değerlendirilmesi ve erişimler için risk değerlendirmesi yapılması
- Dış kaynak hizmetinin uygunluğunu takip edebilmek için sorumlu tayin edilmesi

Bilgi Sistemleri Kontrolleri

- **Bilgi sistemleri sürekliliği→** iş sürekliliği planının bir parçası olan bilgi sistemleri süreklilik planının hazırlanması
- Birincil ve ikincil sistem tesisi
  - Birincil ve ikincil sistemlerin yurtiçinde yer alması
  - 08/03/2018 tarihli SPK Bülteni → Bilgi sistemi bağımsız denetim zorunluluğu bulunmayan halka açık ortaklıkların bu aşamada birincil sistemlerini yurtiçinde bulundurma zorunlulukları bulunmamaktadır. Halka açık ortaklıklar, bilgi sistemleri bağımsız denetimine tabi olacakları dönem itibarıyla, birincil sistemlerini yurtiçinde tutmak zorunda olacaklardır.
- Süreklilik planının yıllık testi, gözden geçirilmesi, güncelliği
- Performans takibi, kapasite planlaması, yedekleme süreçlerinin tesisi
- Önemli dokümanlar ve parolaların güvenli bir şekilde saklanması

TEŞEKKÜRLER…