SPK'dan yeni **Bilgi Sistemleri** düzenlemeleri

Uğur Kağan Dinçsoy
Kıdemli Müdür
Risk Danışmanlığı
Deloitte Türkiye

Sermaye Piyasası Kurulu (SPK) çok sayıda şirketi ilgilendiren ve ilgi ile beklenen;

- Bilgi Sistemleri Bağımsız Denetim Tebliği (III-62.2) ile
- Bilgi Sistemleri Yönetimi Tebliği'ni (VII-128.9)

05 Ocak 2018 tarihinde yayımladı.

SPK tebliğlerin taslaklarını 2013 yılında yayımlamış ve bu tarihten itibaren aralarında Bağımsız Denetim Kuruluşları ve Türkiye İç Denetim Enstitüsü'nün de bulunduğu tebliğlerin sonuçlarından etkilenebilecek farklı kurumlardan görüşler toplamıştı.

Genel olarak taslak tebliğler ile büyük ölçüde aynı doğrultuda yayımlanan Bilgi Sistemleri Bağımsız Denetim Tebliği ve Bilgi Sistemleri Yönetimi Tebliği içerik bakımından Bilgi Sistemleri dünyasını hareketlendirecek bazı düzenlemeleri içerisinde barındırmaktadır.

Her iki tebliğe uyması gereken kurum ve kuruluşlar geniş bir yelpazede olup:

- Borsa İstanbul A.Ş.
- Borsalar ve piyasa işleticileri ile teşkilatlanmış diğer pazar yerleri,
- Emeklilik yatırım fonları
- İstanbul Takas ve Saklama Bankası A.Ş.
- Merkezi Kayıt Kuruluşu A.Ş.
- Portföy saklayıcısı kuruluşlar
- Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu A.Ş.
- Sermaye piyasası kurumları
- Halka açık ortaklıklar
- Türkiye Sermaye Piyasaları Birliği
- Türkiye Değerleme Uzmanları Birliği

olarak sınıflandırılmaktadır.

Bilgi Sistemleri Bağımsız Denetim Tebliği'nde göze çarpan ana alanlar ise;

- "Bilgi Sistemleri Bağımsız Denetim Faaliyetlerine İlişkin Genel Esaslar"
- "Bilgi Sistemleri Bağımsız Denetim Faaliyetinde Bulunma Şartları"
- "Bilgi Sistemleri Bağımsız Denetim Faaliyetlerine İlişkin Yükümlülükler ve Denetim Metodolojisi"
- "Bilgi Sistemleri Bağımsız Denetim Sonuçlarının Raporlanmasına İlişkin Esaslar"

olarak yer almaktadır.

Bu tebliğde öne çıkan ve Bilgi Sistemleri sektörünü hareketlendirecek hususları özetlemek gerekirse;

- Bilgi Sistemleri Denetçilerine CISA sertifikasyonu zorunluluğu:
- Tebliğ'de Bilgi Sistemi Denetimi yapacak personelde de CISA sertifikasyonu zorunlu tutulmaktadır. Bu gereksinimin özellikle ISACA (Information Systems Audit and Control Association) kuruluşunun düzenlediği CISA (Certified Information Systems Auditor) sınavına katılımı ve sektördeki sertifikalı Bilgi Sistemleri Denetçisi sayısında artış olmasını sağlayacaktır.
- Yönetim beyanı yükümlülüğü: Zorunlu tutulan Bilgi Sistemleri iç kontrolleri hakkında yönetim beyanı hazırlama yükümlülüğü, Bilgi Sistemleri iç kontrol ve iç denetim ekiplerinin planlarında bir aktivite olarak öne çıkacaktır.

- Bilgi Sistemleri Denetimleri: Tebliğ kapsamdaki firmalara farklı periyotlarda Bilgi Sistemleri Denetimi yükümlülüğü ile Bilgi Sistemleri Yönetim Tebliği'ne uyum yükümlüğü getirmiştir. Özetle;
  - Borsa İstanbul A.Ş., İstanbul Takas ve Saklama Bankası A.Ş., Merkezi Kayıt Kuruluşu A.Ş., borsalar ve piyasa işleticileri, teşkilatlanmış diğer pazar yerleri, merkezi saklama kuruluşları ve veri depolama kuruluşları için yılda bir,
  - Kısmî ve geniş yetkili aracı kurumlar, asgari öz sermaye yükümlülüğü 5 milyon TL'den fazla olan portföy yönetim şirketleri için iki yılda bir,
  - Asgari öz sermaye yükümlülüğü 5 milyon TL ve az olan portföy yönetim şirketleri ve Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu A.Ş. için üç yılda bir,

Bilgi Sistemleri Bağımsız Denetimi yaptırma zorunluluğu bulunmaktadır.

  - Diğer Sermaye Piyasası Kanunu'na tabi kurum, kuruluş ve ortaklıklar için ise, Bilgi Sistemleri yönetim ilkelerine uyum öngörülmekle birlikte, bu aşamada bu tebliğ ile Bilgi Sistemleri Bağımsız Denetimi yaptırma yükümlülüğü getirilmemiştir.

Bu yükümlülükler özellikle Bilgi Sistemleri sektörünü olumlu etkileyecek ve Sermaye Piyasası Kurulu'nun mevzuata tabi firmalardaki Bilgi Sistemleri süreçlerinin olgunluk seviyesinin yükselmesini sağlayacaktır.

Aralarında Halka Açık Ortaklıkların da bulunduğu çok sayıda firmanın uyum sağlaması gerekecek Bilgi Sistemleri Yönetimi Tebliği'nde öne çıkan konular ise;

- Yönetim kurullarının Bilgi Güvenliği konusunu gündeme alıp politika seviyesinde kurum Bilgi Güvenliği aktivitelerini kontrol etmesi,
- Bilgi Sistemleri üzerinde tebliğ hükümlerine göre etkin bir kontrol mekanizması tesis edilmesi,
- Bilgi Sistemleri'nin, sızma testi konusunda ulusal veya uluslararası belgeye sahip gerçek veya tüzel kişiler tarafından periyodik olarak sızma testine tabi tutulması,
- Bilgi Sistemleri'ne ilişkin dış kaynak yoluyla alınan hizmetlerin yönetimi sürecinin tasarlanması ve tebliğ hükümlerine uyum sağlaması,
- 5 yıllık bir süre ile aktif olacak etkin bir denetim izi kayıt mekanizmasının oluşturulması,
- Bilgi Sistemleri'nin sürekliliğini sağlamak üzere Bilgi Sistemleri Süreklilik Planı hazırlaması ve bu çerçevede ikincil sistemlerini tesis etmesi,
- Birincil ve ikincil sistemlerin yurt içinde bulundurması,

olarak öne çıkmaktadır.

Bunun yanı sıra Bilgi Sistemleri Yönetimi Tebliği maddelerini incelediğimizde aksiyon alınması öne çıkan noktalar ve şirketlerin yükümlülükleri aşağıda yer almaktadır.

- **Madde 5:** Bu madde ile Bilgi Sistemleri süreçlerinin tesis edilmesi, politika, prosedür ve standartların oluşturulması ve bu dokümanların ilgili birimlerle paylaşılması gerekmektedir.
- **Madde 6:** Yönetim kurulu onaylı bir Bilgi Güvenliği Politikası'nın oluşturulması ve bu politika ile bilgi güvenliği kontrollerinin dokümante edilmesi, bilgi güvenliği organizasyonu ile rol ve sorumlulukların tesis edilmesi beklenmektedir.
- **Madde 7:** Üst Yönetim sorumluluğunu içeren maddede, üs yönetimin bilgi güvenliği alanındaki sorumlulukları, kritik projelerdeki gözden geçirme mekanizması, Bilgi Güvenliği Risk önetimi sürecinin oluşturulması, bilgi güvenliği sorumlusunun atanması ve iş sürekliliği planının oluşturulmasına ilişkin ibareler yer almaktadır.

- **Madde 8:** Bilgi Sistemleri Risk Yönetimi sürecindeki detayların anlatıldığı maddede, Bilgi sistemleri Risk Yönetimi çalışmasında değerlendirilecek ana risklere yer verilmiş, bu çalışmada, dış kaynak bağımlılığı, siber risklerin çalışmaya konu olması, Bilgi Sistemleri bağımlılığı ve yetkilendirmeden dolayı oluşabilecek sorumluluk atamasını zorlaştıracak risklere değinilmesi beklenmektedir.
- **Madde 9:** Bilgi Sistemleri kontrol altyapısının detaylarının yer aldığı maddede, kontrollerin dokümante edilmesi, kontrol sahipliğinin belirlenmesi, kontrollerin periyodik olarak gerçekleştirilmesi ve sonuçların üst yönetime raporlanmasına yönelik ibareler yer almaktadır.
- **Madde 10:** Varlık yönetimi maddesinde, varlık envanterinin oluşturulması, varlık sınıflandırma çalışması ile kritik varlıklara yönelik alınması gereken tedbirlere ilişkin ifadeler yer almaktadır.
- **Madde 11:** Görevler ayrılığı prensibi ile ilgili maddede, Bilgi Sistemleri'ndeki yetkilendirme yapısındaki risklerin ve görevler ayrılığı prensiplerinin belirlenmesi, kişiye bağımlılığı azaltacak tedbirlerin alınması ve kritik rollerdeki personelin aktivitelerinin izlenebilmesine yönelik ek kontrollerin tesis edilmesine ilişkin ibareler yer almaktadır.
- **Madde 12:** Fiziksel ve çevresel güvenlik ile ilgili maddede, kritik bilgilerin yer aldığı fiziksel ortamlardaki erişim kontrolleri ile çevresel faktörlere ilişkin koruma tedbirlerinin uygulanmasına ilişkin ibareler yer almaktadır.
- **Madde 13:** Ağ yönetimi ile ilgili maddede, dışarıdan ve içeriden oluşabilecek risklere ilişkin oluşturulması gereken kontroller yer almaktadır. Bu maddede, mobil cihazlar, dış kaynak kullanımı, ağ ayrıştırılması, uzaktan bağlantı gibi faktörlere yönelik kontrollerin oluşturulması beklenmektedir.
- **Madde 14:** Kimlik doğrulama ile ilgili maddede, kullanılması gereken kimlik doğrulama yöntemleri, kimlik doğrulama bilgilerinin güvenliği ve seçilecek kimlik doğrulama yöntemi ile ilgili oluşturulması gereken dokümantasyona ilişkin detaylar yer almaktadır.
- **Madde 15**: Yetkilendirme sürecine yönelik kontrollerin yer aldığı maddede, periyodik yetki gözden geçirme sürecinin kurulması, yetkilendirme süreçlerinin oluşturulması ile yetkilendirme verilerinin güvenliğine ilişkin detaylar yer almaktadır.
- **Madde 16:** İşlemlerin, kayıtların ve verilerin bütünlüğüne yönelik alınması gereken tedbirleri içeren maddede, verilerin iletimi, saklanması ve işlenmesi anındaki kontrollerin kurgulanmasını ve dış kaynak kullanımında da aynı tedbirlerin yer alması beklenmektedir.
- **Madde 17:** Veri gizliliği ile ilgili maddede, verilerin öne derecelerinin belirlenmesi, önem derecelerine göre kontrollerin uygulanması ile şifreleme anahtarları sürecinin oluşturulmasına yönelik detaylar bulunmaktadır.
- **Madde 18:** Bilgi Sistemleri'ne ilişkin dış kaynak firmalarına ilişkin detayları düzenleyen maddede, sözleşme hususları, dış kaynak firmalarının uyması gereken hususlar ile dış kaynak performans yönetimine ilişkin kontroller yer almaktadır.
- **Madde 19 - 20:** Müşteri bilgilerinin gizliliği ve müşterilerin bilgilendirilmesi maddesinde, 6698 sayılı Kişisel Verilerin Korunması Kanunu'ndaki hususlar ile alınması gereken ek tedbirler ve müşterilerin bilgi güvenliği bilgilendirmesi ile şikâyet sürecine ilişkin mekanizmaların oluşturulmasına yönelik beklentiler yer almaktadır.
- **Madde 21:** Üçüncü taraflara bilgi değişimi maddesi, ilgili aktarımlara ve bu aktarımların gerçekleştiği ortamlara ilişkin koruma tedbirlerini içermektedir.
- **Madde 22 - 23:** Kayıt mekanizmasının oluşturulması maddesi, denetim izi kayıt mekanizmasına ilişkin kontrollere, iz kayıtlarının içermesi gereken bilgilere ve iz kayıtlarının en az 5 yıl süre ile saklanmasına yönelik bilgileri içermektedir. Bunun yanı sıra zaman senkronizasyonu sağlamak için atomik bir zaman referansı kullanmak zorunlu hale gelmiştir.
- **Madde 24:** Bilgi güvenliği ihlali süreci, bilgi güvenliği olay yönetimi sürecinin oluşturulmasın ve bu süreçte yer alan asgari kontrolleri içermektedir.
- **Madde 25:** Bilgi Sistemleri edinimi, geliştirilmesi ve bakımı maddesinde, uygulama geliştirme, test ve kabul süreçlerindeki kontrollere ilişkin detaylar yer almaktadır.
- **Madde 26:** Bilgi Sistemleri'nin Sürekliliği maddesinde, birincil ve ikincil sistemlerin yurt içinde bulunması bilgisi ile Bilgi Sistemleri süreklilik planı oluşturulması ve test süreci ile ilgili kontroller yer almaktadır.
- **Madde 27:** Değişiklik yönetimi maddesinde, değişiklik yönetimi kontrolleri, değişiklik kayıt ve onay mekanizmaları ile değişiklik eğitim ve test planlarına ilişkin bilgiler yer almaktadır.

Özellikle, Sızma Testleri Metodolojisi ile ilgili bir eki de içeren genelge, Bilgi Güvenliği, Bilgi Sistemleri Sürekliliği, İz Kayıtları Mekanizmaları, Değişiklik Yönetimi konularında detaylı kontrol hedefleri ile şirketlerin uyması gereken kontrol altyapılarını tanımlamaktadır.

Mevzuatta özellikle Sızma Testi, Birincil ve İkincil sistemleri yurt içinde bulundurulması ve dış kaynak kullanımının kontrol altına alınması beklentileri, firmaların tebliğe uyum konusunda acil aksiyon alması gereken noktalar olarak düşünülmektedir.