Bilgi Sistemleri Yönetimine İlişkin SPK Düzenlemelerinde

Kritik Değişiklikler ve Uyum Süreci

Fırat Dizdar

İnfina Yazılım Kalite Güvence Direktörü

Pınar Baş Eryüksel

İnfina Yazılım Kalite Uyum Direktörü

Sermaye Piyasası Kurulu tarafından yayımlanan VII-128.10 sayılı Bilgi Sistemleri Yönetimine İlişkin Usul Ve Esaslar Tebliği, 30 Haziran 2025 tarihinde yürürlüğe girecek. İnfina Yazılım olarak, bu yeni düzenlemeyi detaylı şekilde inceledik ve siz müşterilerimizi doğrudan etkileyebileceğini değerlendirdiğimiz başlıca yükümlülükleri, önceki tebliğde de yer alan ancak; uygulamada kritik önemde olan hususlarla birlikte aşağıda şekilde özetledik.

Her bir madde, Tebliğ kapsamında dikkatle ele alınması gereken bu konu başlıkları, sermaye piyasası kurumlarının bilgi sistemleriyle ilgili süreçlerini gözden geçirmesi ve gerekli uyum adımlarını atması açısından büyük önem taşımaktadır.

Kapsam ve Tanımlar

Yeni Tebliğ, sermaye piyasası kurumlarının yanı sıra kripto varlık hizmet sağlayıcılarını da kapsama alarak düzenleyici çerçeveyi genişletmiştir. Kurumların bilgi sistemleriyle ilgili kullandığı kavramlar (birincil/ikincil sistemler, bilgi varlığı, hassasiyet, çok faktörlü kimlik doğrulama vb.) tanımlanmış ve ortak bir dil oluşturulmuştur. Bu sayede yöneticilerin, tebliğin kapsamına giren varlık ve süreçleri daha net anlayabilmeleri hedeflenmiştir.

Risk Yönetimi

Kurumlar, bilgi sistemlerine ilişkin risk yönetimi süreçlerini oluşturmak ve güncel tutmak zorundadır. Tüm bilgi varlıklarını içerecek şekilde yılda en az bir kez risk analizi yapılmalı; önemli sistem değişikliklerinde analiz tekrarlanmalıdır. Üst yönetim, risklerin belirlenmesi, ölçülmesi ve raporlanması için kriterleri onaylamalı ve gerekli aksiyonların alınmasını sağlamalıdır. Ayrıca bilgi sistemlerindeki güvenlik açıkları ve tehditler hakkında güncel bilgi toplanarak uygun önlemler gecikmeden alınmalıdır.

Bilgi Güvenliği Politikası ve Organizasyonu

Her kurum, bilgi sistemlerinin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlayacak bir bilgi güvenliği politikası geliştirmeli ve bunu yılda en az bir kez gözden geçirmelidir. Bu politika, bilgi güvenliği süreçlerinde rollerin ve sorumlulukların tanımlanmasını, hedeflerin belirlenmesini, risk yönetimi süreçlerinin kurulmasını ve kontrollerin uygulanmasını içermelidir. Üst yönetim, bilgi güvenliği önlemlerinin uygulanmasını yakından gözetmek ve gerekli kaynakları ayırmakla yükümlüdür. Tebliğ, yönetim kurulunun onayıyla doğrudan üst yönetime bağlı çalışacak en az 5 yıl tecrübeli bir Bilgi Güvenliği Sorumlusu (CISO) atanmasını da gerektirmektedir. Bu sorumlu, bilgi sistemleriyle ilgili riskleri yönetime raporlayacak ve kurum içindeki bilgi güvenliği kontrollerinin takibinden sorumlu olacaktır. Personelin de bilgi güvenliği gereksinimleri ve güncel siber tehditler konusunda yılda en az bir kez eğitilmesi zorunlu hale getirilmiştir.

Bilgi Sistemleri Kontrolleri ve Siber Güvenlik

Tebliğ, kurumların bilgi sistemlerinde kapsamlı teknik ve idari kontroller tesis etmesini şart koşmaktadır. Ayrıcalıklı kullanıcı hesapları için çok faktörlü kimlik doğrulama (MFA) kullanımı zorunlu tutulmuş; kritik sistem ve uygulamalara erişimde de bağımsız birden fazla faktöre dayalı doğrulama gerekmektedir. Uzaktan erişimler sadece güncel cihazlardan yapılabilecek ve mutlaka çok faktörlü doğrulama ile korunacaktır. Kurum içi ağların güvenliği için segmentasyon öngörülmüş; istemci bilgisayarlar, sunucular ve yönetim sistemleri için ayrı ağlar oluşturulması, kablolu/kablosuz ağların ayrılması gibi önlemler belirtilmiştir. Denetim izi (audit log) mekanizmasının kurulması da önemli bir yükümlülüktür: Kritik sistemlerde yapılan işlemler, hassas verilere erişimler, yetki değişiklikleri gibi olayların adım adım kayıt altına alınması ve bu kayıtların en az 5 yıl güvenli şekilde saklanması gerekmektedir. Bu sayede olası bir ihlal veya hatanın kaynağı hızlıca tespit edilebilecektir. Ayrıca, kimlik doğrulama verilerinin güvenli iletimi, sistem yapılandırma değişikliklerinin takip edilmesi ve olağan dışı erişim denemelerinin izlenmesi gibi konularda da detaylı teknik tedbirler Tebliğ'de yer almaktadır.

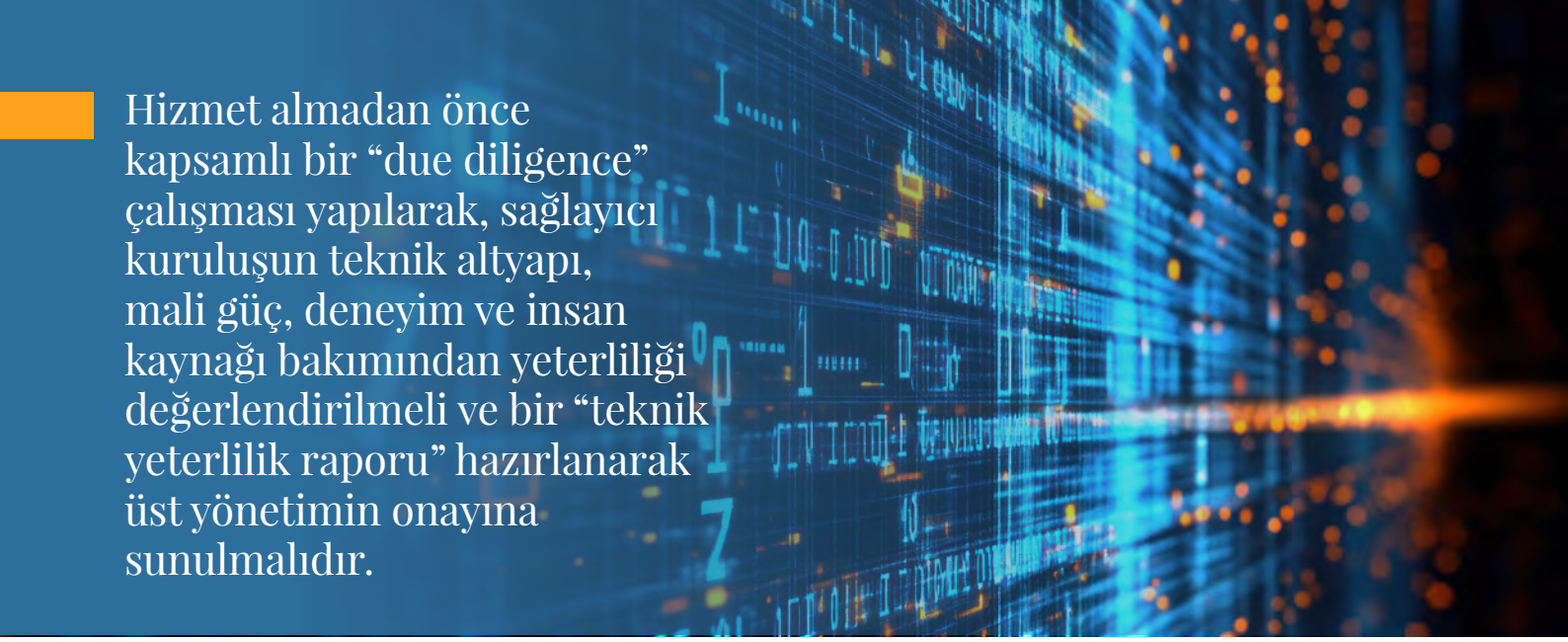
Kurumlar, bilgi sistemlerine ilişkin risk yönetimi süreçlerini oluşturmak ve güncel tutmak zorundadır.

İş Sürekliliği ve Yedekleme

Sermaye piyasası kurumları, iş sürekliliği planlarının bir parçası olarak bir "bilgi sistemleri süreklilik planı" hazırlamak ve kritik iş süreçlerinin kesintisizliğini sağlamakla yükümlüdür. Bu kapsamda, kurumlar her bir kritik süreç için kabul edilebilir maksimum kesinti süresini ve veri kaybı seviyesini tanımlamalıdır. Birincil ve ikincil sistemlerin yurt içinde bulundurulması zorunludur, yani ana veri merkezi ve yedek/afet kurtarma merkezi Türkiye sınırları içinde olmalıdır. İkincil sistemler, birincil sistemle aynı anda doğal afet risklerine maruz kalmayacak farklı bir coğrafi bölgede konumlandırılmalıdır. Kurumlar düzenli olarak yedekleme yapmak, yedeklerin en az bir kopyasını farklı bir lokasyonda güvenli şekilde saklamak ve bu yedeklerden geri dönüş testlerini yılda en az bir kez gerçekleştirmek durumundadır. Afet veya beklenmedik kesinti durumlarında, kritik hizmetlerin iş sürekliliği planında belirlenen sürede ikincil sistemler üzerinden devam ettirilmesi hedeflenmektedir.

Dış Hizmet Alımı (Outsourcing)

Tebliğ, bilgi teknolojileri hizmetlerinin dışarıdan temin edilmesi durumunda çok sıkı kurallar getiriyor. Kurumun üst yönetimi, dış hizmet alımının yaratacağı riskleri değerlendirecek ve ilişkileri yönetecek bir gözetim mekanizması tesis



Hizmet almadan önce kapsamlı bir “due diligence” çalışması yapılarak, sağlayıcı kuruluşun teknik altyapı, mali güç, deneyim ve insan kaynağı bakımından yeterliliği değerlendirilmeli ve bir “teknik yeterlilik raporu” hazırlanarak üst yönetimin onayına sunulmalıdır.

etmek zorundadır. Bu mekanizma çerçevesinde: dışarıdan alınan hizmetlerin kurumun kendi risk yönetimi, bilgi güvenliği ve müşteri mahremiyeti ilkelerine uygunluğu sağlanmalıdır; kurumun verileri dış hizmet sağlayıcıya aktarılıyorsa, hizmet sağlayıcının bilgi güvenliği uygulamaları en az kurumunki kadar güçlü olmalıdır. Outsourcing yapılan BT hizmetinin, kurumun yasal yükümlülüklerini yerine getirmesine engel teşkil etmemesi ve denetimine mani olmaması gerekir. Hizmet almadan önce kapsamlı bir “due diligence” çalışması yapılarak, sağlayıcı kuruluşun teknik altyapı, mali güç, deneyim ve insan kaynağı bakımından yeterliliği değerlendirilmeli ve bir “teknik yeterlilik raporu” hazırlanarak üst yönetimin onayına sunulmalıdır. Ayrıca olası yoğunlaşma riski (aynı tedarikçiye aşırı bağımlılık) analiz edilmeli ve hizmetin ikame edilebilirliğine yönelik bir çıkış stratejisi belirlenmelidir. Dış hizmet alımına ilişkin tüm şartlar mutlaka yazılı bir sözleşmeye bağlanmalı ve bu sözleşme hem kurum hem hizmet sağlayıcı tarafından imzalanmalıdır. Tebliğ, bu hizmet sözleşmelerinde asgari olarak bulunması gereken maddeleri de tek tek saymaktadır: örneğin alınan hizmetin kapsamı ve seviyesi, hizmet seviyesine ilişkin tanımlar, sözleşmenin süresi, beklenmedik şekilde hizmetin kesintiye uğraması durumunda uygulanacak yaptırımlar, sözleşme sona erdiğinde kurum verilerinin kuruma iade edilip hizmet sağlayıcı bünyesinde tamamen imha edilmesi yükümlülüğü, hizmet sırasında ve sonrasında sağlayıcının kurumla ilgili bilgileri gizli tutması, eğer hizmet kapsamında bir ürün geliştiriliyorsa bunun fikri mülkiyet haklarına dair hükümler, alt yükleniciler kullanılacaksa aynı yükümlülüklerin alt sözleşmelerde de yer alması, vb. Özellikle hizmet sağlayıcının derhal güvenlik ihlali ve veri sızıntısı gibi olayları kuruma bildirmesi şartı kritik öneme sahiptir. Kurum, yaptığı sözleşmelerle hizmet aldığı şirketlere kendi tabi olduğu düzenleyici yükümlülüklerin de aynen uygulanmasını sağlamak durumundadır. Kritik hizmetler için kurum yönetimi, tedarikçinin performansını, güvenlik ihlallerini, finansal durumunu ve sözleşmeye uyumunu izlemek üzere yeterli uzmanlığı olan sorumlular atamalı; bu kişiler yılda en az bir kez durumu değerlendiren bir raporu yönetime sunmalıdır. Son olarak, dış hizmet sağlayıcılara kurum sistemlerine verilmiş erişim hakları düzenli risk değerlendirmesine tabi tutulmalı, sadece işi yapmak için gereken en az yetki verilmeli ve iş bitince tüm erişimler derhal kapatılmalıdır.

Sızma Testleri (Penetrasyon Testleri)

Tebliğ kapsamında, kurumların bilgi sistemlerinin yılda en az bir kez yetkin bağımsız kişilerce sızma testine tabi tutulması zorunludur. Bu testler, kurumun bilgi sistemlerindeki zayıflıkları ve açıklıkları önceden tespit edip gidermeyi amaçlar. Özellikle bilgi güvenliği süreçlerinde görev almayan ve ulusal veya uluslararası sertifikaya sahip uzmanlar tarafından gerçekleştirilmelidir. SPK, gerekli gördüğünde bu testlerin yapılmasını ekstra olarak da isteyebilecektir. Tebliğ ekinde (EK-1) sızma testlerinin nasıl yapılacağına dair usul ve esaslar belirtilmiş-

tir. Sızma testi raporları, test tamamlandıktan sonraki bir ay içinde ve en geç her yıl 31 Ocak tarihine kadar SPK'ya gönderilmelidir. Yönetim kurulları, test sonuçlarında ortaya çıkan bulgular için bir aksiyon planı onaylayarak gerekli iyileştirmelerin en kısa sürede yapılmasını temin etmelidir. Bu yükümlülük, kurumların sistem açıklarını proaktif şekilde kapatmalarını ve düzenleyici otoriteyle paylaşmalarını amaçlar. Aksi halde SPK'nın ciddi yaptırımlar uyguladığı görülmektedir – nitekim yakın zamanda bazı aracı kurumlar, sızma testlerini Tebliğ'in gereklerine uygun yapmadıkları için 155.567 TL ile 466.701 TL arasında değişen idari para cezaları almıştır.

İç Denetim ve Raporlama

Kurumlar, bilgi sistemleri yönetimine ilişkin iç denetim fonksiyonlarını güçlendirmek durumundadır. Tebliğ, her yıl en az bir kere bilgi sistemleriyle ilgili iç denetim yapılmasını şart koşuyor. Bu denetim, kurumun bilgi sistemlerinin tasarımı veya işletimiyle doğrudan ilgisi olmayan kişilerce gerçekleştirilmelidir. Özellikle denetimi yapacak personelin SPK tarafından aranan Bilgi Sistemleri Bağımsız Denetim Lisansına sahip olması zorunlu tutulmuştur. İç denetim sonuçları üst yönetime ve yönetim kuruluna raporlanacak; rapordaki bulgulara göre Bilgi Güvenliği Sorumlusu tarafından aksiyon planı hazırlanıp üst yönetimin onayına sunulacaktır. Yönetim kurulu, bilgi sistemleri alanındaki iç denetim bulgularının kapatılmasını ve alınan aksiyonların izlenmesini gözetmekle yükümlüdür. Denetim sonunda hazırlanan faaliyet raporunda, tamamlanan veya devam eden denetimlerin durumu, denetim planına uyum ve kapatılmayan bulgular gibi bilgiler ayrıntılı şekilde yer alacaktır. Ayrıca, kurumların atadığı bilgi sistemleri iç denetçilerini göreve başlar başlamaz 10 iş günü içinde SPL'ye (Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu A.Ş.) bildirmesi gerekmektedir.

Sonuç olarak, SPK VII-128.10 sayılı Tebliğ, sermaye piyasası kurumlarının bilgi teknolojileri yönetiminde uymaları gereken çerçeveyi netleştiren kapsamlı bir düzenlemeler bütünü sunmaktadır. Bu kapsamda, kurumların bilgi sistemlerine ilişkin tüm politika, süreç, kontroller ve altyapılarını gözden geçirmeleri; yeni yükümlülükler doğrultusunda gerekli iyileştirmeleri yapmaları büyük önem taşımaktadır. Tebliğ; risk yönetimi, dış hizmet ilişkileri, bilgi güvenliği, iş sürekliliği ve iç denetim gibi konularda sadece teknik değil, aynı zamanda yönetişim boyutuyla da kapsamlı bir dönüşüm çağrısı niteliğindedir.

Bu çerçevede kurumların, "Hangi alanlarda risk taşıyoruz?" ve "Hangi alanlara yatırım yapmalıyız?" sorularını kendilerine sorması, sadece yasal uyum açısından değil, kurumsal itibarın korunması bakımından da kritik öneme sahiptir. Zira Sermaye Piyasası Kurulu'nun son dönemde bu başlıklarda uyguladığı yaptırımlar, uyumsuzluk halinde karşılaşılabilecek mali ve itibari riskleri açıkça ortaya koymaktadır.

İnfina Yazılım olarak en temel önceliğimiz, iş ortaklarımızın bu süreçte sorunsuz bir şekilde uyum sağlamalarını temin etmek; gerek sistemsel gerekse operasyonel anlamda Tebliğ'in tüm gerekliliklerini eksiksiz şekilde karşılayabilmelerine destek olmaktır. Müşterilerimizin herhangi bir idari yaptırımla karşılaşmaması, iş sürekliliklerinin ve bilgi güvenliği altyapılarının en yüksek standartta sürdürülmesi, bizim açımızdan yalnızca bir yükümlülük değil, aynı zamanda temel bir sorumluluktur.

Bu hedef doğrultusunda, bizler de İnfina Yazılım olarak sunduğumuz hizmetlerin Tebliğ ile tam uyumlu olmasını sağlamak amacıyla bazı alanlarda teknik ve operasyonel yatırımlar gerçekleştirmeyi planlıyoruz. Bu yatırımlar; siz değerli müşterilerimize sunduğumuz hizmetin kalitesini ve regülasyon uyumluluğunu artırmakla kalmayacak, aynı zamanda karşılıklı güvenin daha da pekişmesini sağlayacaktır.

Kurumsal sorumluluğumuzun bilinciyle, yeni Tebliğ dönemine birlikte güçlü ve hazırlıklı adım atmak için sizlerle iş birliğimizi sürdüreceğiz.

SEPAM
Sermaye Piyasaları Araştırma Merkezi

Sermaye piyasaları politikalarına katkıda bulunmak için kurulduk

www.sepam.org.tr