

Örnek Yatırım A.Ş.

BİLGİ SİSTEMLERİ BAĞIMSIZ DENETİM RAPORU
2024

İçindekiler

Raporun Sunulduğu Merci.....	2
Giriş Paragrafı.....	2
Denetim Çalışmasına İlişkin Bilgi.....	2
Denetlenen Kurumun Bilgi Sistemlerine Dair Genel Bilgi.....	2
İç Kontrol ve İç Denetim Yapısına İlişkin Genel Değerlendirme.....	3
Denetçi Görüşü	4
Kısaltmalar ve Sözlük	5
Ek veya Dipnot Dizini	5

Raporun Sunulduđu Mercii

Bu rapor, Sermaye Piyasası Kurulu'na sunulmak üzere hazırlanmıştır. Kurul, sermaye piyasasının düzenlenmesi, denetlenmesi ve gözetimi alanlarında yetkili kamu otoritesi olup; bilgi sistemleri bağımsız denetim raporları aracılığıyla, ilgili kuruluşların teknoloji altyapılarının mevzuata uygunluğunu ve kontrol yeterliliğini denetlemeyi amaçlamaktadır. Bu kapsamda hazırlanan rapor, Kurul'un karar alma süreçlerine katkı sağlamak ve piyasa güvenliğini artırmak amacıyla sunulmaktadır.

Giriş Paragrafi

Bu rapor, Örnek Yatırım A.Ş.'nin bilgi sistemleri altyapısının ve bu sistemler üzerindeki kontrollerin, Sermaye Piyasası Kurulu'nun III-62.2 sayılı Bilgi Sistemleri Bağımsız Denetim Tebliğı uyarınca 2024 yılı itibarıyla değerlendirilmesi amacıyla hazırlanmıştır. Denetim, bağımsız ve tarafsız bir denetim firması olan XYZ Denetim ve Danışmanlık A.Ş. tarafından yürütölmüştür.

Denetim Çalışmasına İlişkin Bilgi

Denetim çalışmaları 15 Ocak 2024 ile 15 Mart 2024 tarihleri arasında gerçekleştirilmiş olup; saha çalışmaları, belge incelemeleri, kontrol testleri ve yetkililerle yapılan görüşmeleri kapsamıştır. Denetim, bilgi sistemleri genel kontrolleri (ITGC), uygulama kontrolleri, erişim yönetimi, yedekleme ve kurtarma süreçleri, değişiklik yönetimi ve veri güvenliği gibi başlıca alanları kapsamıştır.

Denetlenen Kurumun Bilgi Sistemlerine Dair Genel Bilgi

Örnek Yatırım A.Ş., portföy yönetimi ve yatırım danışmanlığı faaliyetlerini destekleyen merkezi bilgi işlem altyapısına sahiptir. Kurumun bilgi sistemleri, veri merkezi üzerinden çalışan fiziksel sunucular ile Amazon Web Services (AWS) platformu üzerinde barındırılan bulut tabanlı uygulamalardan oluşmaktadır. Ana uygulama bileşenleri arasında Elektronik Belge Yönetim Sistemi (EBYS), Müşteri İlişkileri Yönetimi (CRM), Finansal İşlem Platformu ve Log Yönetim Sistemi yer almaktadır.

İç Kontrol ve İç Denetim Yapısına İlişkin Genel Değerlendirme

Yapılan denetim sonucunda, kurum bünyesindeki bilgi sistemleri iç kontrol ortamının büyük ölçüde tanımlı ve dokümente edilmiş olduğu; ancak uygulamada bazı kontrollerin (örneğin, log inceleme sıklığı ve yedekleme doğrulama süreçleri) etkin bir şekilde işletilmediği gözlemlenmiştir. İç denetim birimi yıllık plan çerçevesinde faaliyet göstermekte olup, bilgi sistemleri risklerine yönelik değerlendirme sıklığı yetersiz bulunmuştur.

Yönetim Beyanı Hakkında Bilgi

Örnek Yatırım A.Ş. yönetim kurulunca onaylanmış olan ve bilgi sistemlerine ilişkin iç kontrollerin yeterliliğine dair güvence veren "yönetim beyanı", denetim görüşünün oluşturulmasında dikkate alınmıştır. Beyan, Tebliğin 1 numaralı ekinde yer alan şekle uygun olarak sunulmuştur.

Geçmiş Denetim Bulguları ile Karşılaştırma

2023 yılında yapılan bilgi sistemleri bağımsız denetimi sonucunda belirlenen 4 adet kontrol zayıflığından 3'ü giderilmiş, bir tanesi (yedekleme test prosedürü eksikliği) ise halen devam etmektedir. Bu durum, denetim görüşünün şartlı olarak verilmesinde etkili olmuştur.

Denetlenen Kurum Tarafından Sunulan Aksiyon Planı

Kurul tarafından talep edilen aksiyon planı, kurum yönetim kurulunun 10 Nisan 2024 tarihli kararı ile onaylanmıştır. Plan, öncelikli olarak log inceleme periyotlarının yeniden tanımlanmasını, yedekleme planının her 3 ayda bir test edilmesini ve bilgi sistemleri iç kontrol çerçevesinin güncellenmesini içermektedir.

Denetçi Görüşü

Sayın Örnek Yatırım A.Ş. Yönetim Kurulu'na,

Bilgi sistemleri kontrollerinin denetlenen nezdinde VII-128.9 sayılı Bilgi Sistemleri Yönetimi Tebliği'nde belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması Örnek Yatırım A.Ş. Yönetimi'nin sorumluluğundadır.

Yapmış olduğumuz denetim, denetlenen bilgi sistemleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve III-62.2 sayılı Bilgi Sistemleri Bağımsız Denetim Tebliği'nde belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri kontrollerinin uygunluğu ile tasarımı ve işleyiş etkinliğinin denetim ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve nihayetinde bulgulara dayalı bir görüş bildirilmesini içermektedir.

Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğu kanaatindeyiz.

Ancak aşağıdaki hususlar, denetim görüşümüzün "**şartlı görüş**" olarak ifade edilmesine neden olmuştur:

- Log yönetimine ilişkin prosedürler belirlenmiş olmakla birlikte, uygulama kontrollerinin yeterince sistematik ve izlenebilir olmadığı gözlemlenmiştir.
- Yedekleme süreçleri düzenli şekilde işletilmekte, ancak test edilme sıklığı ve doğrulama kayıtları açısından iyileştirme gerektirmektedir.

Yukarıda belirtilen kontrol eksiklikleri, sistemlerin sürekliliği ve bilgi güvenliği açısından orta düzeyde bir risk oluşturmaktadır. Bu sebeple;

Görüşümüze göre, Örnek Yatırım A.Ş.'nin bilgi sistemleri, 31 Aralık 2024 tarihi itibarıyla yürürlükte olan ilgili düzenlemelere, VII-128.9 sayılı Bilgi Sistemleri Yönetimi Tebliği'nde belirtilen usul ve esaslara uygun olarak kısmen yeterli ve uygun kontroller içermektedir.

Yukarıdaki bulguların, sistem güvenliği ve operasyonel süreklilik üzerinde orta düzeyde bir risk oluşturduğu değerlendirilmiştir. Dolayısıyla, görüş "**şartlı**" şeklinde ifade edilmiştir.

İsim Soyisim

XYZ Denetim ve Danışmanlık A.Ş.

Sorumlu Bilgi Sistemleri Denetçisi

İstanbul, 30 Mart 2024

İmza

Kısaltmalar ve Sözlük

AWS: Amazon Web Services

CRM: Customer Relationship Management

ITGC: Information Technology General Controls

EBYS: Elektronik Belge Yönetim Sistemi

Ek veya Dipnot Dizini

- Ek-1: Yönetim Beyanı (İmzalı Kopya)