HAZİNE BİLİŞİM SİSTEMLERİ DENETİM RAPORU* (ÖZET)

Bu raporda, Hazine Müsteşarlığı bilişim sistemleri tarafından üretilen bilgilerin güvenilir olup olmadığı sorusuna cevap aranmaktadır.

Hazine Müsteşarlığı, 1983 yılından başlayarak bilgi teknolojilerine dayalı olarak faaliyet göstermek üzere çeşitli projeler uygulamış ve yatırımlar yapmıştır. Bu çerçevede devletin borç stokuna ilişkin tüm bilgiler bilgisayar sistemlerine aktarılarak bu sistemler üzerinden yönetilmeye başlanmıştır. Bugün gelinen noktada Hazine Müsteşarlığı'nın bilişim faaliyeti, kurumun temel fonksiyonlarının icra edilebilmesi için vazgeçilmez hale gelmiştir.

Hazine Müsteşarlığı Devlet Borçları Saymanlığı tarafından takip edilen Dış Borçlara ilişkin hesaplar, 1995 yılından itibaren, tam, doğru ve uygun olmadıkları gerekçesiyle reddedilmiştir. Reddedilen hesaplarla ilgili olarak yapılan çalışmalar, 1997 yılından itibaren düzenli olarak hazırlanan "Hazine Hesapları İzleme Raporları" ile Meclise bildirilmiştir. Bu raporlarda Hazine Müsteşarlığının iç kontrol sisteminden ve borçların takip edildiği bilgisayar sisteminden kaynaklanan sorunlar üzerinde hassasiyetle durulmuştur.

Hazine Müsteşarlığı, uzun süredir bilişim sistemlerini yeniden yapılandırmaya yönelik çalışmalar yapmaktadır. Bu çalışmalar sırasında halen uygulanan sistemin bir çok eksiği tespit edilmiş ve yeni geliştirilmekte olan sistemde bunlara ilişkin önlemler alınmıştır.

Müsteşarlıkta yeni bir sisteme geçme çalışmalarının devam ettiği gözönünde bulundurularak, bilişim sistemlerinin denetimi, iç kontrollerle ilgili değerlendirmelere yönelik bir çerçevede gerçekleştirilmiştir. Mevcut sistemde yer

---

* *Hazine Bilişim Sistemleri Denetim Raporu, Sayıştay Genel Kurulu'nun;*
08.10.1998 tarih ve 4909 sayılı kararı ile kabul edilen Hazine Hesapları 1998 Yılı İzleme Raporu,
11.10.1999 tarih ve 4934 sayılı kararı ile kabul edilen Hazine Hesapları 1999 Yılı İzleme Raporu,
02.10.2000 tarih ve 4967 sayılı kararı ile kabul edilen Hazine Hesapları 2000 Yılı İzleme Raporu,
T.B.M.M. Plan ve Bütçe Komisyonunun;
31.12.1996 tarih, 1/492, 3/516 esas ve 68 nolu,2.12.1997 tarih, 1/633, 3/1046 esas ve 17 nolu,
21.6.1999 tarih, 1/3-3/122 esas ve 4 nolu, 5.12.2000 tarih ve 1/740-3/642 esas ve 8 nolu kararları üzerine,
Hazine Müsteşarlığı tarafından yapılan çalışmaları takip amacıyla hazırlanmış,
Sayıştay Genel Kurulunun 06.10.2003 tarih ve 5071/1sayılı kararı ile kabul edilerek Türkiye Büyük Millet Meclisine gönderilmesi uygun bulunmuştur.

alan bir çok güvenlik açığının yeni sistemle giderilmesi hedeflendiğinden, bunlara ilişkin detaylı testlere girilmemiştir.

Hazine bilişim sistemleri denetiminde, sistemin işlem ve uygulamalarının güvenliğini ve güvenilirliğini sağlayan iç kontroller incelenmiştir.

Hazine bilişim sistemlerinin denetiminde dört aşamalı risk tabanlı bir denetim yaklaşımı uygulanmıştır Bu bağlamda;

1. Bilişim sisteminin karşı karşıya kaldığı risk ve tehditler belirlenmiş, meydana gelebilecek hata türleri ve düzensizlikler göz önünde bulundurulmuştur.

2. Bu hata ve düzensizlikleri önlemek veya tespit etmek için gereken kontrol süreçleri belirlenmiştir.

3. Bu gerekli süreçlerin sistemde tanımlanıp tanımlanmadığı ve uygun bir şekilde çalışıp çalışmadığı incelenmiştir.

4. Kontrol süreçleriyle ilgili zaaflar tespit edilmiş ve kontrol sisteminin riskleri minimize etmek için yeterli olup olmadığı değerlendirilmiştir.

Denetim çalışmalarında, Hazinede kurulması gereken kontroller, uluslararası alanda genel kabul görmüş standartlar ve iyi uygulama örnekleri ışığında belirlenmiştir. Belirlenen ana denetim konuları için hazırlanan kriter setleri, denetimin çerçevesini oluşturmakta ve Hazinede kurulması gereken iç kontroller için asgari yapıyı belirlemektedir.

Kriter setleri Hazinede yapılan toplantı ve mülakatlarla ele alınmış, yapılan gözlem ve testlerle elde edilen bulgular Hazine yönetimi ile birlikte değerlendirilmiştir.

Tüm bu çalışmalar gerçekleştirilirken denetim faaliyetinin uluslararası standartlara uygunluğunu sağlamak ve bir kısım teknik testleri gerçekleştirmek amacıyla, uluslararası denetim firmalarından PriceWaterhouse Coopers'tan danışmanlık hizmeti alınmıştır.

BULGULAR

Hazine Müsteşarlığının iç kontrol yapısı, Hazine bilişim sistemleri tarafından üretilen cetvel ve raporların güvenilirliğini etkileyen önemli zaaflar taşımaktadır. Ancak bu husus değerlendirilirken, Müsteşarlığın bu zaafların önemli bir kısmının farkında olduğu ve sorunların çözümü için büyük bir gayret gösterdiği gözönünde tutulmalıdır.

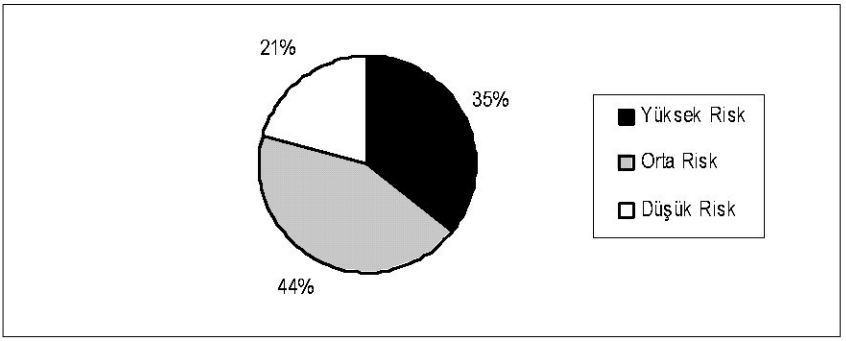
Denetim sırasında, Hazine bilişim sistemleri, kapsamlı bir kriter setine uygunluk bakımından incelenmiştir. Mevcut yapının kullanılan kriter setini önemli

ölçüde karşıladığı, ancak aşağıda tespit edilen konularda zafiyetler içerdiği belirlenmiştir. Raporda sadece olumsuz bulgulara yer verilmiştir.

RİSK GRAFİKLERİ

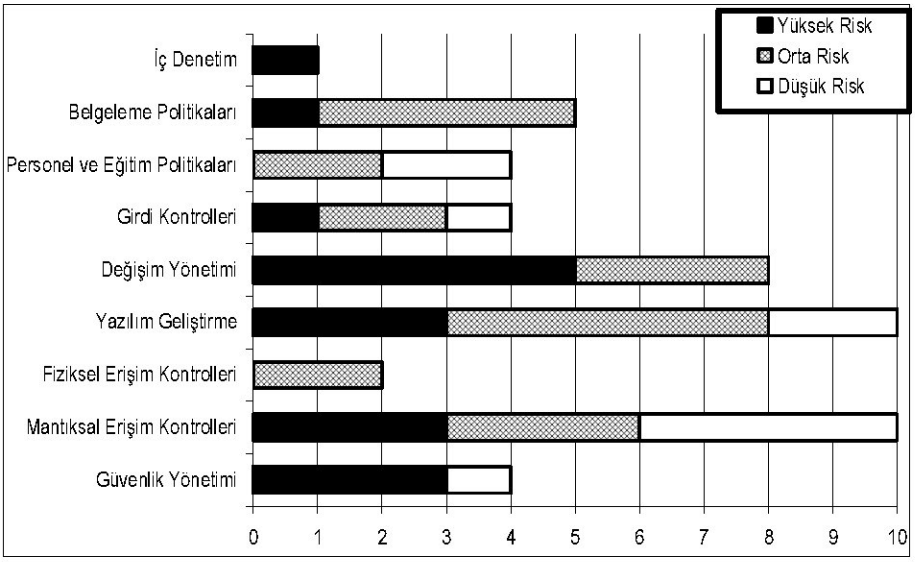
Şekil 1'de, bu raporda ortaya konulan toplam 48 bulgunun % 35'inin yüksek risk oluşturduğu görülmektedir.

Şekil 1 Risklerin dağılımı



Aşağıda yer alan 2. şekilde de, bulgularla ilgili risklerin konulara göre dağılımı görülmektedir. Örneğin, değişim yönetimiyle ilgili olarak tespit edilen 8 bulgunun 5'i yüksek risk, 3'ü orta düzeyde risk oluşturmaktadır.

Şekil 2 Risklerin konulara göre dağılımı



GÜVENLİK YÖNETİMİNE İLİŞKİN BULGULAR

Güvenlik yönetimi, kurumla ilgili riskler göz önünde bulundurularak, hizmetlerin sürekliliğini sağlayacak bir kontrol yapısının kurulmasını ve sürdürülmesini hedefler.

Bu konuda şu bulgular elde edilmiştir:

- Hazine Müsteşarlığının karşı karşıya bulunduğu risklerin belirlenmesine ve bunlara karşı bir güvenlik planı hazırlanmasına ilişkin herhangi bir çalışma yapılmamaktadır.
- Kurumda bilgi güvenliği ile ilgili standartlar belirlenmemiştir.
- Kurumun bir "Acil Durum Eylem Planı" ve "Kriz Yönetimi Planı" bulunmamaktadır.
- Kurumun bir "İş Sürekliliği Planı" bulunmamaktadır.

MANTIKSAL ERİŞİM KONTROLLERİNE İLİŞKİN BULGULAR

Bir bilgisayar sisteminde yer alan programların kullanımı, bu programlar vasıtasıyla ulaşılabilecek bilgilerin yetkisiz kişiler tarafından görülmesini veya değiştirilmesini engellemek amacıyla kısıtlanmalıdır. Mantıksal erişim kontrolleri, bu amaçla, kullanıcıların ve sistem yöneticilerinin programları kullanmalarını kontrol altına almak için uygulanan mekanizmalardır.

Bu konuda şu bulgular elde edilmiştir:

- Hazinede kullanılan, üretilen ve muhafaza edilen kaynaklar önemlerine ve gizliliklerine bağlı olarak sınıflandırılmamıştır.
- Hazine bilişim sistemlerinin şifreleme ve güvenlikle ilgili standartları belirlenmemiştir ve uygulamadaki ayarlar yeterli güvence sağlamamaktadır.
- Görev yeri değişen veya işten ayrılan personelin sistemlere erişim yetkilerinin derhal kaldırılması sağlanamamaktadır.
- Kullanıcıların sisteme erişimleri yetki ve sorumluluklarına bağlı olarak sınırlandırılmamaktadır.
- Kullanıcı bilgisayarlarının açık bırakılarak belirli bir süre kullanılmadığı durumlarda başkaları tarafından kullanılmasını önleyecek kontroller kullanılmamaktadır.

▪ Kullanıcıların sisteme, aynı anda, aynı kullanıcı adı ve şifresiyle değişik bilgisayarlardan bağlanması mümkündür.

▪ İşletim sisteminde, ağ altyapısında ve yazılımlarda değişiklikler yapıldığında, sistemin güvenliğinin önceden belirlenmiş standartlarda tekrar sağlanması için, mantıksal erişim yolları analizi güncellenmemektedir.

▪ Kullanımına son verilen veya başka bir yere gönderilen bilgisayar malzemeleri üzerinde yer alan hassas verilerin ve yazılımın silinmesini öngören yazılı bir süreç bulunmamaktadır.

▪ Kuruma dışarıdan yetkisiz erişimi kontrol etmek için kurulan kontrol mekanizmaları tarafından belirlenen ve engellenen saldırılar yönetime raporlanmamaktadır.

▪ Sisteme uzaktan çevirmeli bağlantı kullanılmak suretiyle sağlanabilecek erişimlerle ilgili yeterli güvenlik önlemleri bulunmamaktadır.

FİZİKSEL ERİŞİM KONTROLLERİNE İLİŞKİN BULGULAR

Fiziksel erişim kontrolleri, kuruma ait bilgi sistemlerinin ve kullanıcıların bulunduğu binalara ve odalara fiziki olarak ulaşılmasını kontrol altında tutmaya yönelik olarak uygulanan kontrollerdir. Ayrıca bu kontroller ile bilişim sisteminin yangın, su baskını, nem, elektrik kesintisi gibi çevreden gelecek risklere karşı korunması da amaçlanır.

Bu konuda şu bulgular elde edilmiştir:

▪ Hazine bilişim sistemi donanımlarının yer aldığı binalara girişlerin kontrol edilmesi için kurulan sistemler etkin bir şekilde çalışmamaktadır.

▪ Bilgi İşlem Merkezi, Hazine Müsteşarlığı ve Dış Ticaret Müsteşarlığı personeli tarafından birlikte kullanıldığından sistem odasına erişimin sadece Hazine tarafından kontrol edilmesi mümkün bulunmamaktadır.

YAZILIM GELİŞTİRMEYE İLİŞKİN BULGULAR

Yazılım geliştirme üzerindeki kontroller, kurumların günlük operasyonlarını yürütmek için kullandıkları yazılımların oluşturulması esnasında kullanılan kontrol mekanizmalarıdır.

Bu konuda şu bulgular elde edilmiştir:

▪ Yazılımların geliştirmesine ve uygulamaya konmasına ilişkin faaliyetlerin sistematik bir şekilde yürütülmesi güvence altına alınmamıştır.

▪ Bilişim sistemiyle ilgili projelerin fizibilite çalışmalarının yeterli kalitede yapılmasını güvence altına alacak süreçler kullanılmamaktadır.

▪ Projelerin kurumun amaçları ile uyumlu olmasını sağlayacak yeterli kontroller bulunmamaktadır.

▪ Projelerin kalite kontrolü için kullanılan süreçler yetersizdir.

▪ Yazılımların nasıl test edileceğini belirleyen standartlar bulunmamaktadır.

▪ Kurumda geliştirilen yazılımlarla ilgili teknik belgelerin hazırlanması ve güncellenmesi güvenceye bağlanmamıştır.

▪ Kurumda geliştirilen yazılımlarla ilgili kullanıcı dokümanları zamanında hazırlanmamakta ve güncellenmemektedir.

▪ Geliştirilen yazılımların hangi şartları yerine getirmesi durumunda uygulamaya sokulacağı belirlenmemiştir.

▪ Yeni yazılımlar uygulamaya alındıktan sonra, bunlar üzerinde herhangi bir denetim veya inceleme yapılmamaktadır.

▪ Kurumda etkin bir kütük yönetim metodolojisi kullanılmamaktadır.

DEĞİŞİM YÖNETİMİNE İLİŞKİN BULGULAR

Değişim yönetimi, kurum tarafından hazırlanan programlar üzerinde, kullanıcıların ihtiyaçları veya sistemin gereklilikleri sonucu yapılması gereken değişikliklerin kontrollü bir şekilde gerçekleştirilmesini hedefler. Bu değişikliklerin bilgi sistemlerinin genel işleyişi ve genel güvenlik seviyesi üzerinde herhangi bir olumsuz etki yapmamasını sağlamak amacıyla çeşitli kontrol mekanizmaları kurulur.

Bu konuda şu bulgular elde edilmiştir:

▪ Hazine Müsteşarlığının yazılı bir değişim yönetimi metodolojisi bulunmamaktadır.

▪ Kurumda bilişim sistemleriyle ilgili tüm değişiklik isteklerinin tek bir merkezde toplandığı, takip edildiği ve raporlandığı bir yapı bulunmamaktadır.

▪ Değişikliklerin ne şekilde test edileceğini ve belgeleneceğini gösteren standartlar bulunmamaktadır.

▪ Sadece onaylanmış ve test edilmiş yazılımların uygulama ortamına aktarıldığını güvence altına alacak yeterli kontroller bulunmamaktadır.

▪ Yazılım geliştiren personelin uygulama ortamına erişmeleri ve uygulama ortamında yazılım değişikliği yapmaları engellenmemiştir. Programcıların, programlar ve veriler üzerinde yaptıkları değişiklikler log dosyalarında takip edilmemektedir.

▪ Tüm kullanıcılarda aynı versiyon programın çalışmasını sağlayan bir uygulama bulunmamaktadır.

▪ Yazılımlar üzerinde acilen yapılan değişiklikler log dosyalarında takip edilmemekte, bunlara ilişkin özel bir raporlama ve gözetim mekanizması bulunmamaktadır.

▪ Yazılım kodlarının korunması, programların sınıflandırılması ve değişik versiyonlarının muhafaza edilmesi ile ilgili yeterli kontrol mekanizmaları bulunmamaktadır.

GİRDİ KONTROLLERİNE İLİŞKİN BULGULAR

Sisteme girişi yapılan veriler, sistemler tarafından üretilen her türlü bilginin ve raporun temelini teşkil etmektedir. Verilerin sisteme yalnızca yetkili kişiler tarafından, doğru kaynaklara dayanarak ve doğru bir şekilde girilmesini sağlamak üzere oluşturulan kontroller girdi kontrolleri olarak adlandırılmaktadır.

Bu konuda şu bulgular elde edilmiştir:

▪ Sistemde yer alan veriler üzerinde yapılan değişiklikler belgelenmemekte ve yeterli şekilde kontrol edilmemektedir.

▪ Sisteme kaydedilecek veriler için standart veri giriş formları kullanılmamaktadır. Verilerin kaydedilmesini takiben, ilgili belgelerin onaylanarak saymanlığa intikal ettirilmesine ilişkin süreçler yetersizdir.

▪ Kaynak niteliğinde olmayan belgelerle kayıt yapılmasını engelleyecek prosedürler geliştirilmemiştir.

▪ Aynı verinin sisteme mükerrer kaydedilmesini önleyecek otomatik uyarı mekanizmaları kurulmamıştır.

PERSONEL VE EĞİTİM POLİTİKALARINA İLİŞKİN BULGULAR

Bilişim sistemlerinin kaynaklanan sorunların büyük bir kısmı insanlar tarafından yapılan hata, ihmal ve suistimallerden kaynaklanmaktadır. Bu nedenle kurumların, personelin hata yapma riskini düşürecek kontroller kurmaları önem kazanmaktadır.

Bu konuda şu bulgular elde edilmiştir:

- Kurum çalışanlarının kişi bazında görev tanımları bulunmamaktadır.
- Kurumda birbiriyle bağdaşmayacak nitelikteki görevler belirlenmemiş ve bunların farklı kişiler tarafından yürütülmesi güvence altına alınmamıştır.
- Kilit konumdaki personelin izin kullanmasını veya rotasyona tabi tutulmasını zorunlu kılan politika ve prosedürler bulunmamaktadır.
- Personel temini ile ilgili genel uygulamalar, bilişim sisteminin ihtiyacı olan nitelikli iş gücünün temin edilmesini güçleştirmektedir.

BELGELEME POLİTİKALARINA İLİŞKİN BULGULAR

Kurumun belgeleme politikalarının yetersiz olması, personelin hatalı veya yetkisiz işlem yapma riskini yükseltebilir. Ayrıca, sistemde bir hata meydana geldiği zaman, eğer işlemler yeterli bir şekilde belgelenmemişse, hatanın sebebinin tespiti de güçleşebilir.

Bu konuda şu bulgular elde edilmiştir:

- Kurumda, temel konulardaki politikaların belirlenmesine yönelik olarak alınan kararlar, yeterli şekilde belgelenmemektedir.
- Kurumda yürütülen süreçler (iş akışları) yeterli şekilde belgelenmemekte, teamüllere ve kişilere bağlı olarak yürütülmektedir.
- Bilgi İşlem Merkezinin faaliyetleriyle ilgili belgeleme usulleri yeterli değildir.
- Sisteme girilen verilerle bu verilerin kaynağını oluşturan belgeler arasında uygun bir irtibat kurulmamaktadır.
- Sistemdeki verilerin kaynağını oluşturan belgelerin arşivlenmesiyle ilgili düzenlemeler yetersizdir.

İÇ DENETİME İLİŞKİN BULGULAR

İç denetim, bir kurum yönetimince görevlendirilen denetim elemanları tarafından, kurumun sistem ve usullerini değerlendirmek ve hesaplardaki yolsuzluk, maddi hata, yanlışlık ve verimsiz uygulama ihtimallerini asgariye indirmek amacıyla yapılan denetimdir.

Bu konuda şu bulgu elde edilmiştir:

- Kurumda iç denetim mekanizması çalışmamaktadır.

Hazine bilişim sistemlerinin denetimi sonucunda tespit edilen risklerle ilgili grafikler aşağıda verilmiştir.

SONUÇ

1. Hazine Müsteşarlığında şu anda kullanılmakta olan bilişim sisteminin hesaplara esas olan cetvelleri güvenilir bir şekilde üretmeye yeterli olmadığı tespit edilmiştir.

2. Yeniden tanzim edilerek Sayıştaya verilen 1995-2002 yıllarına ait dış borç hesapları, tam, doğru ve uygun olmadıkları gerekçesiyle Sayıştay Genel Kurulunun 06.10.2003 tarih ve 5071/1 sayılı kararı ile reddedilmiştir.

Reddedilen Hazine hesaplarına uygunluk verilebilmesi için;

- Hazine bilişim sistemlerinin yeniden yapılandırılması çalışmaları tamamlanmalıdır.

- Yeni sistemde, Hazine Bilişim Sistemleri raporunda değinilen ve sistemin güvenilirliğini zedeleyen kontrol zaafları giderilmelidir.

Sistem tarafından üretilen cetvel ve bilgiler, 2003 yılı uygunluk bildirimi çalışmalarından önce, Hazine Müsteşarlığının da görüşü alınmak suretiyle Sayıştay Genel Kurulu tarafından belirlenecek esaslar çerçevesinde, Devlet Borçları Saymanlığına intikal ettirilerek Sayıştaya verilmelidir.