T.C.
SAYIŞTAY BAŞKANLIĞI

BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ

2019 Yılı Sayıştay Denetim Raporu

Eylül 2020

İÇİNDEKİLER

TABLOLAR LİSTESİ

KISALTMALAR

TSE: Türk Standartları Enstitüsü

YÖK: Yükseköğretim Kurulu

BULGU LİSTESİ

B. Denetim Görüşünü Etkilemeyen Tespit ve Değerlendirmeler

1. Taşınmazların Cins Tashihi İşlemlerinin Tamamlanmaması

2. Kişisel Verileri Korunması Kanunu'nun Gereklerini Yerine Getirecek Kurumsal Altyapının Oluşturulmaması

3. Lisansı Olmayan Yazılımların Kullanılmasının Engellenmemesi

4. Bilişim Sistemleri Yönetişim Kontrollerinin Yetersiz Olması

5. Dış Tedarikle Yürütülen Bilişim Hizmetlerine İlişkin Sözleşmelerin Bilgi Güvenliği Yönünden Yetersiz Olması

6. Bilişim Sistemlerinin Sürekliliğini Güvence Altına Alacak Kontrollerin Yetersiz Olması

7. Bilişim Varlıkları Üzerinde Gerçekleştirilecek Değişikliklerin Yönetimiyle İlgili Kural ve Uygulamaların Yetersiz Olması

1. KAMU İDARESİ HAKKINDA BİLGİ

1.1. Mevzuat ve Görevler

Bilecik Şeyh Edebali Üniversitesi 2007 yılında, 29 Mayıs 2007 tarih ve 26536 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 5662 sayılı Kanunla kurulmuştur.

Üniversitenin örgüt yapısı, Yükseköğretim Kanunu ve Yükseköğretim Kurumları Teşkilat Kanununun üniversitelerin akademik ve idari örgütlenmesine ilişkin maddeleri ve ilgili yönetmelikler doğrultusunda fakülte, enstitü, yüksekokul, meslek yüksekokulu, koordinatörlük, araştırma ve uygulama merkezi ile Rektörlüğe bağlı bölümlerden oluşmuştur. Akademik ve idari birimlerin yönetimi ve yöneticilerin yetki ve sorumlulukları da aynı Kanunlar tarafından belirlenmiştir.

Yükseköğretim ile ilgili amaç ve ilkeleri belirlemek ve bütün yükseköğretim kurumlarının ve üst kuruluşlarının teşkilatlanma, işleyiş, görev, yetki ve sorumlulukları ile eğitim-öğretim, araştırma, yayım, öğretim elemanları, öğrenciler ve diğer personel ile esasları bir bütünlük içinde düzenleyen 2547 sayılı Yükseköğretim Kanunu 1981 yılından beri yürürlüktedir.

2547 sayılı Kanun'un 12'nci maddesinde Yükseköğretim Kurumlarının görevleri sayılmakta olup bu görevler sırasıyla;

a. Çağdaş uygarlık ve eğitim - öğretim esaslarına dayanan bir düzen içinde, toplumun ihtiyaçları ve kalkınma planları ilke ve hedeflerine uygun ve ortaöğretime dayalı çeşitli düzeylerde eğitim - öğretim, bilimsel araştırma, yayım ve danışmanlık yapmak,

b. Kendi ihtisas gücü ve maddi kaynaklarını rasyonel, verimli ve ekonomik şekilde kullanarak, milli eğitim politikası ve kalkınma planları ilke ve hedefleri ile Yükseköğretim Kurulu tarafından yapılan plan ve programlar doğrultusunda, ülkenin ihtiyacı olan dallarda ve sayıda insan gücü yetiştirmek,

c. Türk toplumunun yaşam düzeyini yükseltici ve kamu oyunu aydınlatıcı bilim verilerini söz, yazı ve diğer araçlarla yaymak,

d. Örgün, yaygın, sürekli ve açık eğitim yoluyla toplumun özellikle sanayileşme ve tarımda modernleşme alanlarında eğitilmesini sağlamak,

e. Ülkenin bilimsel, kültürel, sosyal ve ekonomik yönlerden ilerlemesini ve gelişmesini ilgilendiren sorunlarını, diğer kuruluşlarla işbirliği yaparak, kamu kuruluşlarına önerilerde bulunmak suretiyle öğretim ve araştırma konusu yapmak, sonuçlarını toplumun yararına sunmak ve kamu kuruluşlarınca istenecek inceleme ve araştırmaları sonuçlandırarak düşüncelerini ve önerilerini bildirmek,

f. Eğitim - öğretim ve seferberliği içinde, örgün, yaygın, sürekli ve açık eğitim hizmetini üstlenen kurumlara katkıda bulunacak önlemleri almak,

g. Yörelerindeki tarım ve sanayinin gelişmesine ve ihtiyaçlarına uygun meslek elemanlarının yetişmesine ve bilgilerinin gelişmesine katkıda bulunmak, sanayi, tarım ve sağlık hizmetleri ile diğer hizmetlerde modernleşmeyi, üretimde artışı sağlayacak çalışma ve programlar yapmak, uygulamak ve yapılanlara katılmak, bununla ilgili kurumlarla işbirliği yapmak ve çevre sorunlarına çözüm getirici önerilerde bulunmak,

h. Eğitim teknolojisini üretmek, geliştirmek, kullanmak, yaygınlaştırmak,

ı. Yükseköğretimin uygulamalı yapılmasına ait eğitim - öğretim esaslarını geliştirmek, döner sermaye işletmelerini kurmak, verimli çalıştırmak ve bu faaliyetlerin geliştirilmesine ilişkin gerekli düzenlemeleri yapmaktır.

1.2. Teşkilat Yapısı ve İnsan Kaynakları

Kamu İdaresinin üst yöneticisi olan rektör Cumhurbaşkanınca, dekanlar ise Yükseköğretim Kurulunca seçilir ve atanırlar0. Üniversitenin akademik organı Senato olup Üniversite Yönetim Kurulu ise idari faaliyetlerde Rektöre yardımcı olmaktadır.

Bilimsel özerkliğe ve kamu tüzelkişiliğine sahip olan Üniversite; 3 Fakülte, 2 Enstitü, 1 Yüksekokul, 7 Meslek Yüksekokulu ile, eğitim-öğretim hayatına başlamıştır. Bugün 8 Fakülte, 3 Enstitü, 1 Yüksekokul, 7 Meslek Yüksekokulu ve 11 Uygulama ve Araştırma Merkezi ile faaliyetine devam etmektedir. Kurumun Döner Sermaye İşletmesi de bulunmaktadır.

Üniversitede 598 akademik personel, 262 idari personel olmak üzere toplam 860 personel görev yapmaktadır.

Tablo 1: Akademik Personel Kadroları Tablosu

Unvan	Dolu	Boş	Toplam
Profesör	35	21	56
Doçent	47	54	101
Doktor Öğretim Üyesi	189	46	235
Öğretim Görevlisi	214	40	254
Araştırma Görevlisi	113	99	212
Toplam	**598**	**260**	**858**

Tablo 2: İdari Personel Kadroları Tablosu

Sınıfı	Dolu	Boş	Toplam
Genel İdari Hizmetler	204	202	406
Sağlık Hizmetleri Sınıfı	4	4	8
Teknik Hizmetler Sınıfı	44	72	116
Avukatlık Hizmetleri Sınıfı	1	1	2
Yardımcı Hizmetler Sınıfı	9	7	16
Toplam	**262**	**286**	**548**

Üniversitenin bağlı, ilgili ve ilişkili olduğu kurum ve idareler değerlendirildiğinde;

Üniversitenin ilgili yıl bütçesi hazırlanıp Anayasa'nın 130'uncu maddesi uyarınca Yükseköğretim Kurulu tarafından tetkik edilerek onaylanmakta, Milli Eğitim Bakanlığına sunulmakta ve merkezi yönetim bütçesinin bağlı olduğu esaslara uygun olarak işleme tabi tutulup yürürlüğe konmaktadır.

Yükseköğretim kurumlarının öğretimini planlamak, düzenlemek, yönetmek, denetlemek, yükseköğretim kurumlarındaki eğitim-öğretim ve bilimsel araştırma faaliyetlerini yönlendirmek, bu kurumların kanunda belirtilen amaç ve ilkeler doğrultusunda kurulmasını, geliştirilmesini ve üniversitelere tahsis edilen kaynakların etkili bir biçimde kullanılmasını sağlamak ve öğretim elemanlarının yetiştirilmesi için planlama yapmak maksadı ile kurulan Yükseköğretim Kurulunun görev alanı içerisinde Bilecik Şeyh Edebali Üniversitesi de bulunmaktadır.

Yükseköğretim Kurulu adına üniversiteleri, bağlı birimlerini, öğretim elemanlarını ve bunların faaliyetlerini gözetim ve denetim altında bulunduran Yükseköğretim Kuruluna bağlı Yükseköğretim Denetleme Kurulu, Kamu İdaresinin faaliyetlerini denetleme yetkisine

sahiptir.

Akademik bir organ olan Üniversitelerarası Kurulun üyeleri her üniversiteden bir rektör ve bir profesörün katılımından oluşmaktadır. Bu Kurulun görevleri 2547 sayılı Kanun'un 11'inci maddesiyle belirlenmiştir ve Bilecik Şeyh Edebali Üniversitesi de Kurulun üyesidir.

Bilecik Şeyh Edebali Üniversitesi diğer üniversiteler gibi mali yönetim yapısı ve işleyişi, kamu bütçelerinin hazırlanması, uygulanması, mali işlemlerin muhasebeleştirilmesi ve raporlanması ve mali kontrole ilişkin olarak 5018 sayılı Kanun'un verdiği görev ve yetkiye istinaden başta Hazine ve Maliye Bakanlığı düzenlemeleri olmak üzere ilgili diğer kurumların düzenlemelerine tabidir.

1.3. Mali Yapı

"Özel Bütçeli İdare" olarak, 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu'nun (II) sayılı cetvelinin (A) bölümünde sayılan Yükseköğretim Kurulu, Üniversiteler ve İleri Teknoloji Enstitüleri içerisinde yer alan Kamu İdaresi, Merkezi Yönetim Bütçe Kanunu ile verilen hazine yardımı ve öz gelirlerini kullanarak giderlerini finanse etmektedir.

Kurumun 2019 yılı bütçesi 115.658.000 TL gelir ve 115.658.000 TL gider olarak hazırlanmıştır. 2019 yılı gelir gerçekleşmesi 131.699.568,79 TL olup, gelir bütçesi gerçekleşme oranı % 113'tür. 2019 yılı bütçe gideri 125.121.908,37 TL olarak gerçekleşmiştir. Gider bütçesi gerçekleşme oranı % 108'dir. Kurumun 2019 yılı bütçe gelir ve giderleri, bütçe ödeneği ile gerçekleşme oranları aşağıda gösterildiği gibidir.

Tablo 3: 2019 Yılı Bütçe Ödenekleri ve Bütçe Gider Gerçekleşmeleri Tablosu

Bütçe Giderinin Ekonomik Kodu	Bütçe Ödeneği (TL)	Gerçekleşme (TL)	Gerçekleşme Oranı (%)
01-Personel Giderleri	76.852.000,00	80.768.199,86	105
02-Sosyal Güvenlik Kurumlarına Devlet Primi Giderleri	10.661.000,00	11.281.526,61	106
03-Mal ve Hizmet Alım Giderleri	7.797.000,00	13.911.150,13	178
04-Faiz Giderleri	-	-	-
05-Cari Transferler	2.338.000,00	2.106.305,98	90
06-Sermaye Giderleri	18.010.000,00	17.054.725,79	95
07-Sermaye Transferleri	-	-	-
08-Borç Verme	-	-	-
09-Yedek Ödenek	-	-	-
TOPLAM	**115.658.000,00**	**125.121.908,37**	**108**

Tablo 4: 2019 Yılı Bütçe Gelir Tahminleri ve Bütçe Gelir Gerçekleşmeleri Tablosu

Bütçe Gelirinin Ekonomik Kodu	Bütçe Tahmini (TL)	Gerçekleşme (TL)	Gerçekleşme Oranı (%)
01-Vergi Gelirleri	-	-	-
03-Teşebbüs ve Mülkiyet Gelirleri	3.664.000,000	5.900.754,71	161
04-Alınan Bağış ve Yardımlar ile Özel Gelirler	110.243.000,00	118.807.350,00	107
05-Diğer Gelirler	1.751.000,00	6.991.464,08	399
06-Sermaye Gelirleri	-	-	-
08-Alacaklardan Tahsilat	-	-	-
09-Red ve İadeler (-)	-	-	-
TOPLAM	**115.658.000,00**	**131.699.568,79**	**113**

Dönem faaliyet geliri 129.702.992,05 TL, faaliyet gideri ise 122.194.638,38 TL olan Üniversitenin, 2019 yılını 7.508.353,67 TL olumlu faaliyet sonucu ile tamamladığı görülmüştür.

Kamu İdaresi bütçesi içinde yer almayan Üniversite Döner Sermaye İşletmesi 2019 yılını 219.542,83 TL dönem karı ile kapatmıştır. Kurum misafirhanesi bütçe içinde faaliyet göstermektedir.

1.4. Muhasebe ve Raporlama Sistemi

5018 sayılı Kanun'un 49'uncu maddesi gereğince genel yönetim kapsamındaki kamu idarelerinde uygulanacak muhasebe ve raporlama standartları, uluslararası standartlara uygun olarak Hazine ve Maliye Bakanlığı bünyesinde; Sayıştay Başkanlığı, Hazine ve Maliye Bakanlığı ve diğer ilgili kuruluş temsilcilerinin katılımıyla oluşturulacak olan Devlet Muhasebesi Standartları Kurulu tarafından belirlenmektedir. Dolayısıyla genel yönetim kapsamında olan üniversitelerin muhasebe ve raporlama standartları Kurul tarafından belirlenen kurallara tabidir. Kamu İdaresi ayrıca adı geçen Kanun'un 80'inci maddesinin Hazine ve Maliye Bakanlığına verdiği yetkiye istinaden Bakanlığın hazırladığı düzenlemelere tabi olup bu kapsamda çıkarılan Genel Yönetim Muhasebe Yönetmeliği'ndeki muhasebe ilkeleri ile hesap planını kullanmakta, mali tabloları hazırlamakta ve Merkezi Yönetim Muhasebe Yönetmeliği hükümlerine göre mali işlemlerini muhasebeleştirmektedir.

"Kamu İdaresi Hesaplarının Sayıştaya Verilmesi ve Muhasebe Birimleri ile Muhasebe Yetkililerinin Bildirilmesi Hakkında Usul ve Esaslar"ın 5'inci maddesi gereğince hesap dönemi sonunda Sayıştaya gönderilmesi gereken defter, tablo ve belgelerden denetime

sunulanlar aşağıda sayılmakta olup denetim bunlar ile Usul ve Esaslar'ın 8'inci maddesinde yer alan diğer belgeler dikkate alınarak yürütülüp sonuçlandırılmıştır.

- Birleştirilmiş veriler defteri,
- Geçici ve kesin mizan,
- Bilanço,
- Kasa sayım tutanağı,
- Banka mevcudu tespit tutanağı,
- Alınan çekler sayım tutanağı,
- Menkul kıymet ve varlıklar sayım tutanağı,
- Teminat mektupları sayım tutanağı,
- Değerli kâğıtlar sayım tutanağı,
- İdare taşınır mal yönetimi ayrıntılı hesap cetveli ile idare taşınır mal yönetimi hesabı icmal cetveli,
- Bütçe giderleri ve ödenekler tablosu,
- Bütçe gelirleri ekonomik sınıflandırılması tablosu,
- Faaliyet sonuçları tablosu.

Denetim görüşü, kamu idaresinin tabi olduğu geçerli finansal raporlama çerçevesi kapsamındaki temel mali tabloları olan bilanço ve faaliyet sonuçları tablosuna verilmiştir.

2. KAMU İDARESİNİN SORUMLULUĞU

Denetlenen kamu idaresinin yönetimi, tabi olduğu muhasebe standart ve ilkelerine uygun olarak hazırlanmış olan mali rapor ve tabloların doğru ve güvenilir bilgi içerecek şekilde zamanında Sayıştaya sunulmasından, bir bütün olarak sunulan bu mali tabloların kamu idaresinin faaliyet ve işlemlerinin sonucunu tüm önemli yönleriyle doğru ve güvenilir olarak yansıtmasından ve ister hata isterse yolsuzluktan kaynaklansın, bu mali rapor ve tabloların önemli hata veya yanlış beyanlar içermemesinden; kamu idaresinin gelir, gider ve malları ile bunlara ilişkin hesap ve işlemlerinin kanunlara ve diğer hukuki düzenlemelere uygunluğundan; mali yönetim ve iç kontrol sistemlerinin amacına uygun olarak

oluşturulmasından, etkin olarak işletilmesinden ve izlenmesinden, mali tabloların dayanağını oluşturan bilgi ve belgelerin denetime hazır hale getirilmesinden ve sunulmasından sorumludur.

3. SAYIŞTAYIN SORUMLULUĞU

Sayıştay, denetimlerinin sonucunda hazırladığı raporlarla denetlenen kamu idarelerinin gelir, gider ve malları ile bunlara ilişkin hesap ve işlemlerinin kanunlara ve diğer hukuki düzenlemelere uygunluğunu tespit etmek, mali rapor ve tablolarının güvenilirliğine ve doğruluğuna ilişkin görüş bildirmek, mali yönetim ve iç kontrol sistemlerini değerlendirmekle sorumludur.

4. DENETİMİN DAYANAĞI, AMACI, YÖNTEMİ VE KAPSAMI

Denetimlerin dayanağı; 6085 sayılı Sayıştay Kanunu, uluslararası denetim standartları, Sayıştay ikincil mevzuatı ve denetim rehberleridir.

Denetimler, kamu idaresinin hesap ve işlemlerinin kanunlara ve diğer hukuki düzenlemelere uygunluğunu tespit etmek ve mali rapor ve tablolarının kamu idaresinin tüm faaliyet ve işlemlerinin sonucunu doğru ve güvenilir olarak yansıttığına ilişkin makul güvence elde etmek ve mali yönetim ve iç kontrol sistemlerini değerlendirmek amacıyla yürütülmüştür.

Kamu idaresinin mali tabloları ile bunları oluşturan hesap ve işlemlerinin doğruluğu, güvenilirliği ve uygunluğuna ilişkin denetim kanıtı elde etmek üzere yürütülen denetimler; uygun denetim prosedürleri ve tekniklerinin uygulanması ile risk değerlendirmesi yöntemiyle gerçekleştirilmiştir. Risk değerlendirmesi sırasında, uygulanacak denetim prosedürünün belirlenmesine esas olmak üzere, mali tabloların üretildiği mali yönetim ve iç kontrol sistemleri de değerlendirilmiştir.

Denetimin kapsamını, kamu idaresinin mali rapor ve tabloları ile gelir, gider ve mallarına ilişkin tüm mali faaliyet, karar ve işlemleri ve bunlara ilişkin kayıt, defter, bilgi, belge ve verileri (elektronik olanlar dâhil) ile mali yönetim ve iç kontrol sistemleri oluşturmaktadır.

Bu hususlarla ilgili denetim sonucunda denetim görüşü oluşturmak üzere yeterli ve uygun denetim kanıtı elde edilmiştir.

5. İÇ KONTROL SİSTEMİNİN DEĞERLENDİRİLMESİ

İç kontrol sistemi, 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu'nun beşinci kısmında düzenlenmiştir. İç kontrol, idarenin amaçlarına, belirlenmiş politikalara ve mevzuata uygun olarak faaliyetlerin etkili, ekonomik ve verimli bir şekilde yürütülmesini, varlık ve kaynakların korunmasını, muhasebe kayıtlarının doğru ve tam olarak tutulmasını, malî bilgi ve yönetim bilgisinin zamanında ve güvenilir olarak üretilmesini sağlamak üzere idare tarafından oluşturulan organizasyon, yöntem ve süreçle iç denetimi kapsayan malî ve diğer kontroller bütünüdür.

Görev ve yetkileri çerçevesinde, malî yönetim ve kontrol süreçlerine ilişkin standartlar ve yöntemler Hazine ve Maliye Bakanlığınca, iç denetime ilişkin standartlar ve yöntemler ise İç Denetim Koordinasyon Kurulu tarafından belirlenir, geliştirilir ve uyumlaştırılır. Bunlar ayrıca, sistemlerin koordinasyonunu sağlar ve kamu idarelerine rehberlik hizmeti verir.

31.12.2005 tarihli ve 26040 (3. Mükerrer) sayılı Resmi Gazete'de yayımlanan İç Kontrol ve Ön Mali Kontrole İlişkin Usul ve Esaslar'ın 5'inci maddesinde, iç kontrol standartlarının, merkezi uyumlaştırma görevi çerçevesinde Hazine ve Maliye Bakanlığı tarafından belirlenip yayımlanacağı, kamu idarelerinin, malî ve malî olmayan tüm işlemlerinde bu standartlara uymakla ve gereğini yerine getirmekle yükümlü bulunduğu, ayrıca Kanun'a ve iç kontrol standartlarına aykırı olmamak koşuluyla, idarelerce görev alanları çerçevesinde her türlü yöntem, süreç ve özellikli işlemlere ilişkin standartlar belirlenebileceği belirtilmiştir.

Hazine ve Maliye Bakanlığı tarafından hazırlanarak 26.12.2007 tarihli ve 26738 sayılı Resmi Gazete'de yayımlanan Kamu İç Kontrol Standartları Tebliği ile kamu idarelerinde iç kontrol sisteminin oluşturulması, uygulanması, izlenmesi ve geliştirilmesi amacıyla 18 standart ve bu standartlar için gerekli 79 genel şart belirlenmiştir.

5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu ve ilgili diğer mevzuat uyarınca, Genel Sekreterlik tarafından iç kontrol sisteminin oluşturulması, uygulanması, izlenmesi ve geliştirilmesi çalışmaları çerçevesinde ilgili birimlerle ortak çalışma yapılarak Kamu İç Kontrol Standartlarına Uyum Eylem Planı hazırlanmıştır.

Bu kapsamda idarenin iç kontrol sistemleri değerlendirilmiş olup yapılan temel tespitler şunlardır:

Kurumda iç denetçi kadrosu bulunmaktadır, ancak henüz iç denetçi ataması yapılmamıştır.

Kamu Görevlileri Etik Davranış İlkeleri ile Başvuru Usul ve Esasları Hakkında Yönetmeliğin Ek 1'inde yer alan "Etik Sözleşmesi" Kurumda çalışan tüm personel tarafından imzalanmış ve bu sözleşmeler personelin özlük dosyalarında muhafaza altına alınmıştır.

Kurum organizasyon yapısı içerisinde görev, yetki ve sorumluluklar açık bir şekilde belirlenmiştir.

Yetki devri ve sınırlarının belirlendiği Yetki Devri Yönergesi oluşturulmuştur.

Kurum stratejik planı, Stratejik Planlama Ekibi tarafından birim stratejik plan çalışmaları doğrultusunda hazırlanmıştır.

İdarenin yürüteceği program, faaliyet ve projeleri ile bunların kaynak ihtiyacını, performans hedef ve göstergeleri içeren performans programı hazırlanmıştır.

İdare, bütçesini stratejik plan ve performans programına uygun olarak hazırlamıştır.

Kurumsal düzeydeki risklerin belirlenmesi için herhangi bir çalışma yürütülmemiştir.

Ön mali kontrol sistemi, "İç Kontrol ve Ön Mali Kontrole İlişkin Usul ve Esaslar"a uygun olarak kurulmuştur. İlgili mevzuat çerçevesinde, harcama yetkilisi ve muhasebe yetkilisi görevleri ayrı kişilere verilmiştir. Ön mali kontrol görevini yürüten kişiler, yasaklanan görevlerde, ihale, muayene ve kabul komisyonlarında görevlendirilmemiştir.

Kurumda yürütülen faaliyetlerin iş tanımları yapılmış ve bu işlerin iş akış şemaları çıkarılmıştır.

Kurumda, yönetimin ihtiyaç duyduğu bilgileri talep edilen formatlarda üretebilen çeşitli modüller kullanılmaktadır. Bu modüller arasında, kurumsal iş süreçleri, öğrenci bilgi sistemi, ek ders sistemi, portal, forum, tarihçe web sayfası, dashboard, iş takip sistemi ön planda yer almaktadır. Kurumda bilgi yönetimini koordine etmek amacıyla bir Veritabanı Sorumluları Komisyonu kurulmuştur. Komisyonun amacı, verilerin kaynağında, doğru ve zamanında, sistemlere girilmesini sağlamak, tüm sistemleri birbiriyle entegre hale getirmek ve karar destek süreçlerine altyapı oluşturmak olarak belirlenmiştir. Komisyon, ihtiyaç duyulduğunda, birim veritabanı sorumlularından veri talep etmektedir.

İdare Faaliyet Raporunda amaç ve hedeflere, faaliyetlere ve faaliyet sonuçlarına, göstergelere ve değerlendirmelere yer verilmiştir.

İç Kontrol İzleme ve Yönlendirme Kurulu üst yöneticinin onayı ile görevlendirilmiştir. "İç Kontrol Standartları Uyum Eylem Planı Gerçekleşme Sonuçları Raporu" yıllık bazda hazırlanmakta ve İç Kontrol İzleme ve Yönlendirme Kuruluna sunulmaktadır. Ancak bu rapor da içerik itibariyle, eylem planının maddelerini içeren ve takvime ilişkin bilgi veren bir formattan oluşmakta olup yeterli bilgi içermemektedir. Rapor, risk yönetimi ve iç kontrolün uygulanışını izlemek için yeterli değildir.

İç Kontrol Standartlarına Uyum Eylem Planı Kamu İç Kontrol Standartları Tebliğine uygun olarak iç kontrol standartları ve genel şartlara uygun olarak hazırlanmıştır. Ancak, planda döner sermayeli işletmeler için eylemler belirlenmemiştir.

Kurumların faaliyetlerinin büyük ölçüde bilişim sistemleri desteğiyle yürütülmesi sebebiyle günümüzde iç kontrollerin önemli bir kısmının bilişim ortamında oluşturulması gerekmektedir. Kurum iç kontrol sisteminin değerlendirilmesi sonucunda, bilişim sistemleri bünyesinde kurulması gereken iç kontrollerle ilgili önemli eksikler tespit edilmiştir. Bu hususlara raporun bulguları arasında yer verilmiştir.

Sonuç olarak; kurumsal risk yönetimi çalışmalarına başlanması, bilişim sistemleri iç kontrollerinin yeniden yapılandırılması, iç denetim biriminin kurulması ve İç Kontrol İzleme ve Yönlendirme Kurulunun iç kontrol sisteminin değerlendirilmesine yönelik faaliyette bulunması ile etkinlikle çalışan ve güvence sağlayan bir kontrol yapısına ulaşılmış olacaktır.

6. DENETİM GÖRÜŞÜ

Bilecik Şeyh Edebali Üniversitesi 2019 yılına ilişkin yukarıda belirtilen ve ekte yer alan, geçerli finansal raporlama çerçevesi kapsamındaki mali rapor ve tablolarının tüm önemli yönleriyle doğru ve güvenilir bilgi içerdiği kanaatine varılmıştır.

7. DENETİM BULGULARI

Raporda yer alan bulgular, denetimler sonucunda tespit edilen hususlara kamu idaresi tarafından verilen cevapların değerlendirilmesi suretiyle düzenlenmiştir.

A. DENETİM GÖRÜŞÜNÜN DAYANAKLARI

Herhangi bir denetim bulgusu tespit edilmemiştir.

B. DENETİM GÖRÜŞÜNÜ ETKİLEMEYEN TESPİT VE DEĞERLENDİRMELER

BULGU 1: Taşınmazların Cins Tashihi İşlemlerinin Tamamlanmaması

Kuruma ait bazı taşınmazların mevcut durumunun tapu kayıtlarıyla uyumlu olmadığı, dolayısıyla cins tashihi işlemlerinin tamamlanmadığı görülmüştür.

Kurum ve kuruluşların mülkiyetinde, yönetiminde veya kullanımında bulunan taşınmazların kaydına ve icmal cetvellerinin düzenlenmesine ilişkin usul ve esaslar, Kamu İdarelerine Ait Taşınmazların Kaydına İlişkin Yönetmelik ile düzenlenmiştir. Bu Yönetmelik'in *"Tanımlar"* başlıklı 4'üncü maddesinin b bendinde; binalar, arazi ve arsalar ile yer altı ve yer üstü düzenlerinin mevcut kullanım şekilleri ile tapu kayıtlarının farklılık göstermesi durumunda, tapu kayıtlarının mevcut kullanım şekli dikkate alınarak düzeltilmesi işleminin cins tashihi olarak adlandırıldığı belirtilmiştir.

Söz konusu yönetmeliğin *"Cins tashihlerinin yapılması"* başlıklı 10'uncu maddesinin 1'inci bendinde, kamu idarelerinin mülkiyet, yönetim veya kullanımlarında bulunan taşınmazların mevcut kullanım şekli ile tapu kayıtlarının birbirine uygun olmaması durumunda, taşınmazların mevcut kullanım şekli ile kayıtlara alınacağı ve kamu idarelerinin, taşınmazlarının cins tashihinin yapılması için gerekli işlemleri yapacakları belirtilmiştir.

Yine aynı maddede cins tashihinin, taşınmazın maliki durumunda olan kurumlar tarafından kullanıcı konumunda olan kurumların yazısı üzerine yapılacağı; taşınmazın bizzat malik kurum tarafından kullanılması durumunda ise, bu kurum tarafından tüm işlemlerin yerine getirileceği hüküm altına alınmıştır.

Aynı Yönetmelik'in "Kayıt değişikliği işlemleri" başlıklı 11'inci maddesinde ise kayıt değişikliği işlemlerinin nasıl yapılacağı maddeler halinde açıklanmıştır.

Ancak uygulamada, Üniversite yerleşkesi içerisinde ve ilçelerde yer alan ve üzerine bina yapılmış olan bazı taşınmazların mevcut durumunun tapu kayıtlarında halen tarla veya arsa olarak gösterildiği, dolayısıyla tapu kayıtlarının fiili durumu yansıtmadığı tespit edilmiştir. Kurum tarafından söz konusu kayıtların düzeltilmesi amacıyla cins tashihi ve taşınmaz işlemlerine başlanmış, bu çerçevede toplam 19 adet binanın cins tashihi işlemleri yapılmıştır.

Ancak, merkez kampüsünde ve ilçelerde bulunan 11 adet taşınmazın cins tashih işlemlerinin henüz tamamlanmadığı tespit edilmiştir. Bu işlemlerin gecikmesinin, Kurum yerleşke alanı içinde bulunan ve kamulaştırılması gereken alanlarla ilgili olarak kamulaştırma sürecine itiraz edilmesinden kaynaklandığı görülmüştür.

Kurumun kullanımında ve yönetiminde bulunan taşınmazların cins tashihi işlemlerinin ilgili mevzuat hükümleri çerçevesinde tamamlanması gerekmektedir.

BULGU 2: Kişisel Verileri Korunması Kanunu'nun Gereklerini Yerine Getirecek Kurumsal Altyapının Oluşturulmaması

Kurum'un, 6698 sayılı Kişisel Verilerin Korunması Kanunu'na uyum göstermek için kapsamlı bir çalışma yürüttüğü, ancak altyapı niteliğinde olan beş hususta yetersizlikler olduğu tespit edilmiştir.

a. Kişisel Verilere Kimlerin Erişim Sağlamaya Yetkili Olduğunun Belirlenmemesi

6698 sayılı Kişisel Verilerin Korunması Kanunu çerçevesinde kişisel verilere erişim ve işleme yetkisini haiz olacak "Veri İşleyenlerin" henüz belirlenmediği ve ilgili iş süreçlerinin tanımlanmadığı görülmüştür.

Kişisel Verilerin Korunması Kanunu'nun *"Tanımlar"* başlıklı 3'üncü maddesinde kişisel verilerle ilgili sorumlu kişiler şu şekilde tanımlanmıştır:

"Bu Kanunun uygulanmasında; (...)

ğ) Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi, (...)

ı) Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi,

ifade eder"

Yürütülen çalışmalar kapsamında; Kurum'da Genel Sekreter'in veri sorumlusu olarak görevlendirildiği, ancak, veri işleyenlerin henüz görevlendirilmediği görülmüştür. Kanun'a uyum çalışmanın ilk aşaması olması gereken, Kuruma ait bilişim sistemlerinde yer alan kişisel verilere halihazırda hangi personelin erişim sağladığının tespit edilmesi için yürütülen çalışmalar da henüz tamamlanmamıştır.

İlgili mevzuata uyumun sağlanabilmesi amacıyla;

- Kurum'da kişisel veri işlemekle ilgili yetkilendirme, yetkiyi kaldırma ve yetki kullanımını izleme süreçlerinin belirlenmesi,
- Kişisel verilere halihazırda erişim sağlayan personelin belirlenmesi,
- Bu personelin Veri İşleyen olarak görevlendirilmesi veya kişisel verilere erişim yetkilerinin kaldırılması,

gerekmektedir.

b. Kişisel Veri Envanterinin ve İlgili İş Süreçlerinin Oluşturulmaması

2016 yılında kabul edilen Kişisel Verilerin Korunması Kanunu'na uyum için öngörülen iki yıllık süre dolmasına rağmen, kişisel veri envanterinin oluşturulmadığı; Kurum bünyesinde tutulması gereken kişisel verilerin ve bu verilerin işlenmesine ilişkin kurumsal süreçlerin henüz belirlenmediği görülmüştür.

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 4'üncü maddenin 1'inci bendi *"Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir."* hükmünü getirmiştir. Kanun'un 5'inci maddesi kişisel verilerin işlenme şartlarını, 6'ncı maddesi özel nitelikli kişisel verilerin işlenme şartlarını, 7'nci maddesi kişisel verilerin aktarılmasını, 9'uncu maddesi de kişisel verilerin yurt dışına aktarılmasını düzenlemektedir. Bu maddelerde yer alan hükümlerin tatbik edilebilmesi, kişisel verilerin envanterinin çıkarılmasına bağlıdır. Kurumlar, öncelikle ellerinde hangi kişisel veriler olduğunu belirlemeli, bunun ardından bu verilerin işlenme, aktarım, muhafaza ve silinmesine ilişkin süreçleri yürütmelidir.

Söz konusu kanuna dayalı olarak çıkarılan ve 01/01/2018 tarihinde yürürlüğe giren Veri Sorumluları Sicili Hakkında Yönetmelik'in *"Tanımlar"* başlıklı 4'üncü maddesinin (h) bendinde "kişisel veri işleme envanteri" şu şekilde tanımlanmaktadır:

"Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter (...)"

İlgili Yönetmelik'in *"İlke, usul ve esaslar"* başlıklı 5'inci maddesinin (ç) bendinde şu hükme yer verilmiştir:

"Sicile kayıtla yükümlü olan veri sorumluları, Kişisel Veri İşleme Envanteri hazırlamakla yükümlüdür. Sicil başvurularında Sicile açıklanacak bilgiler Kişisel Veri İşleme Envanterine dayalı olarak hazırlanır."

Söz konusu envanter hazırlama yükümlülüğü, veri sorumlularının sicile kayıt olmalarından önce, 6698 sayılı Kanun'da öngörülen iki yıllık süre içinde tamamlanması gereken bir yükümlülüktür.

Ancak yapılan incelemelerde kişisel veri envanterinin oluşturulmadığı, bu çerçevede aşağıda belirtilen hususların yerine getirilmediği tespit edilmiştir:

- Kurum bilişim sistemlerinde *halihazırda tutulan* kişisel verilerin neler olduğu, bu verilerin ne zaman ve kimlerden toplandığı, ne şekilde kullanıldığı ve depolandığı belirlenmemiştir,
- Kurumda *tutulması gereken* kişisel verilerin neler olduğu ve halihazırda tutulan verilerden silinmesi gerekenler olup olmadığı belirlenmemiştir,
- Kişisel verileri işleme amaçları ve hukuki sebepleri tanımlanmamıştır,
- Kişisel verilerin muhafaza süreleri belirlenmemiştir,
- Kişisel verilerin güvenliğine ilişkin alınması gereken önlemler belirlenmemiştir,

- Kişisel verilerin Kurum dışına ve yurt dışına aktarılması koşulları tanımlanmamıştır,
- Kişilerin rızasının alınma ve bilgilendirme yöntemleri tanımlanmamıştır,
- Yukarıdaki hususlara ilişkin kurumsal süreçler belirlenmemiştir.
- Kurum bünyesinde kişisel verileri ve ilgili süreçleri yönetecek altyapı kurulmamıştır; kişisel veri envanterini muhafaza edecek ve ilgili kurumsal süreçleri yönetecek yazılımlar bulunmamaktadır.

İlgili mevzuata uyumun sağlanabilmesi amacıyla, kişisel veri envanterinin ve ilgili süreçlerin ivedilikle oluşturulması ve bu hususlara ilişkin gerekli iç düzenlemelerin yapılması gerekmektedir.

c. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi İşlemlerinin Yapılmaması

Kurumda, kişisel verilerin işlenmesine ilişkin şartlar ortadan kalkmasına rağmen kişisel verilerin veri sorumlusu tarafından silinmesi, yok edilmesi veya anonim hale getirilmesi işlemlerinin yapılmadığı görülmüştür.

Kişisel Verilerin Korunması Kanunu'nun *"Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi"* başlıklı 7'nci maddesinde şu hükümlere yer verilmiştir:

"(1) Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.

(2) Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır.

(3) Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir."

Söz konusu Kanun hükmü çerçevesinde çıkarılan ve 01/01/2018 tarihinde yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 1'inci maddesine göre;

"Bu Yönetmeliğin amacı, tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esasları belirlemektir."

Yönetmeliğin *"Kişisel veri saklama ve imha politikasına ilişkin esaslar"* başlıklı 5'inci maddesi ile Veri Sorumluları Siciline kayıt olmakla yükümlü olan veri sorumluları, kişisel veri işleme envanterine uygun olarak kişisel veri saklama ve imha politikası hazırlamakla yükümlü tutulmuşlardır. Yönetmeliğin 6'ncı maddesinde bu politikanın içeriğinde yer alması gereken asgari hususlar tespit edilmiştir.

Yönetmeliğin diğer hükümlerinde kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi işlemleri tanımlanmış ve bu işlemler için zorunlu süreler belirlenmiştir.

Kurum bünyesinde yürütülen, 27001 sayılı BGYS standardına uyum çalışmaları kapsamında bir veri imha politikasının belirlendiği, ancak bu politikanın kapsamının sınırlı olduğu ve kişisel verilerle ilişkilendirilmediği görülmüştür.

Kurumda kişisel verilerin silinmesine, yok edilmesine veya anonim hale getirilmesine ilişkin süreç ve kuralların ivedilikle belirlenmesi ve uygulamaya geçilmesi gerekmektedir.

ç. Kişisel Verilere İlişkin Olarak Tutulan Erişim Kayıtlarının ve Bu Kayıtların Korunması İçin Alınan Önlemlerin Yetersiz Olması

Kurumda, bilişim ortamında kişisel verilere erişime ilişkin olarak tutulması gereken kayıtların (logların) tanımlanmadığı, mevcut kayıtların kanuni yükümlülüklerin yerine getirilmesi için yeterli olmadığı ve tutulan kayıtların bütünlüğünün korunması için alınan önlemlerin yetersiz olduğu görülmüştür.

Kişisel Verilerin Korunması Kanunu'nun *"Veri güvenliğine ilişkin yükümlülükler"* başlıklı 12'nci maddesinde şu hükümler yer almaktadır:

"(1) Veri sorumlusu;

a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

c) Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır (...)

(3) Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır."

Söz konusu kanun maddesi, veri sorumlusuna kişisel verilerin ne tür işlemlere tabi tutulduğunun kapsamlı şekilde izlenmesi yükümlülüğünü getirmektedir. Bu izlemenin yapılabilmesi için, kişisel verileri işlemek veya depolamak için kullanılan bilgisayar programları tarafından oluşturulan erişim kayıtları (loglar) temel bilgi kaynağı konumundadır. Bu kayıtlar, kişisel verilere kimin, hangi uygulamadan ve ne zaman eriştiğini gösteren kayıtlardır.

Veri Sorumluları Sicili Hakkında Yönetmelik'in *"Tanımlar"* başlıklı 4'üncü maddesinin (h) bendinde tanımlanan "kişisel veri işleme envanteri"nin sağlıklı bir şekilde çalışabilmesi de erişim kayıtlarının düzenli bir şekilde tutulmasına, güvenli bir ortamda ve erişilebilir bir formatta saklanmasına bağlıdır.

Kişisel verilerle ilgili altyapının sağlıklı şekilde çalışması, bu verilere erişime ilişkin kayıtların bütünlüğünün korunması, yani kayıtların değiştirilemeyecek şekilde saklanması ön şartına bağlıdır. Kurulan altyapının, erişim kayıtlarının değiştirilmesine izin vermemesi gereklidir. Bu, kritik erişim kayıtlarının saklanmasında, 5070 sayılı Elektronik İmza Kanunun 3'üncü maddesinde tanımlanan ve bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve/veya kaydedildiği zamanı gösteren Zaman Damgasının veya aynı seviyede güvence veren bir yöntemin kullanılması ile sağlanabilmektedir.

Bu çerçevede Kurum'da yürütülen çalışmalar kapsamında şu hususlar tespit edilmiştir:

- Kişisel verilerin işlenmesinin izlenmesine ilişkin gözetim ve denetim süreçleri tanımlanmamıştır.
- Yazılımlar tarafından tutulan/yönetilen/erişilen kişisel veriler kategorize edilmemiş; hangilerinin "kişisel veri" veya "özel nitelikli kişisel veri" niteliği taşıdığı tanımlanmamış, dolayısıyla hangi kişisel verilerin kritik nitelikte olduğu belirlenmemiştir,
- Kritik nitelikteki kişisel verilere erişimi izlemek için yazılımlar tarafından tutulması gereken erişim kayıtları belirlenmemiştir,
- Halihazırda yazılımlar tarafından tutulmakta olan kişisel verilere erişim kayıtlarının değiştirilmesini önlemek için yeterli önlem alınmamıştır.

Kişisel verilerin korunmasıyla ilgili mevzuata uyum sağlanabilmesi amacıyla, kişisel verilerin bilişim ortamında ne tür işlemlere tabi tutulduğunun izlenmesi için gerekli gözetim ve denetim süreçlerinin tanımlanması, kişisel verilere erişim kayıtlarının belirlenmesi ve tutulması ve bu kayıtların bütünlüğünü güvence altına alacak kontrol mekanizmalarının ihdas edilmesi gerekmektedir.

d. Kişisel Verileri İşleyen Yüklenicilerle İmzalanan Sözleşme Hükümlerinin Yetersiz Olması

Kurumda hizmet alımı yöntemiyle yürütülen bilişim hizmetleri çerçevesinde yüklenicilerle yapılan sözleşmelerin, Kişisel Verilerin Korunması Kanunu'nun gereklerinin yerine getirilmesi açısından yetersiz kaldığı tespit edilmiştir.

Kişisel Verilerin Korunması Kanunu'nun *"Tanımlar"* başlıklı 3'üncü maddesinde şu tanımlara yer verilmiştir:

"(...) ğ) Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi,

h) Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini, (...)

ifade eder."

Söz konusu Kanun'un *"Veri güvenliğine ilişkin yükümlülükler"* başlıklı 12. maddesi şu şekildedir;

"(1) Veri sorumlusu;

a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

c) Kişisel verilerin muhafazasını sağlamak,

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır

(2) Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.

(3) Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır (...)"

Kurumun, personel bilgi sistemi ve elektronik bilgi yönetim sistemi ile ilgili hizmetlerinin, hizmet alımı yöntemiyle yükleniciler tarafından yerine getirildiği görülmüştür. Yürütülen işlerin niteliği gereği bu sistemlerde önemli miktarda kişisel veri bulunmaktadır. Yüklenici, kendi personeli aracılığıyla, kişisel verilerin tutulduğu veri tabanını yönetmekte ve kişisel verilere erişebilmektedir. Dolayısıyla yüklenici, 6648 sayılı Kanun'da tanımlanan "veri işleyen" konumunda bulunmaktadır. Kanun'un 12'nci maddesinde kişisel verilerin veri sorumlusu adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde sorumluluğun müşterek olduğu açıkça belirtilmiştir. İlgili maddede veri sorumlusunun veri işleyenler üzerindeki denetim yetkisi de tanımlanmıştır.

Bu durumda, kişisel verilerin yönetilmesi bakımından bir veri işleyen olarak yüklenicinin sorumluluklarının ve denetim gibi Kanun'un zorunlu kıldığı süreçlerin nasıl yürütüleceğinin taraflar arasında yapılan sözleşmeler çerçevesinde tanzim edilmesi gereklidir. Ancak, Kurum tarafından imzalanan sözleşmelerde 6648 sayılı Kanun ve ilgili alt düzenlemelerde aranan birçok hususun eksik bırakıldığı tespit edilmiştir. Bu hususların eksikliği, kişisel verilerin işlenmesi süreçlerinde mevzuata aykırılıklara ve önemli risklerin açığa çıkmasına sebep olmaktadır.

Tespit edilen önemli hususlar şunlardır:

- İlgili yazılımlar tarafından hangi kişisel verilerin işleneceği sözleşmelerde açıkça tanımlanmamıştır. Sonradan ortaya çıkan haller çerçevesinde kaydedilmesi gerekebilecek kişisel verilerin tanımlanması ve yükleniciye bildirilmesine ilişkin süreç belirlenmemiştir. (6648, madde 5),

- Yazılımlar tarafından işlenen kişisel verilere ilişkin aydınlatma yükümlülüğünün ve açık rızanın alınması süreçlerinin Kurum gözetiminde ilgili yazılımlar tarafından yürütülmesi temin edilmemiştir (madde 5 ve 10),

- Özel nitelikli kişisel verilerin ilgili yazılımlar tarafından hiçbir şekilde kaydedilmemesi güvence altına alınmamıştır (madde 6),
- Kişisel verilerin Kurum tarafından belirlenecek koşullar çerçevesinde yüklenici tarafından silinmesi, yok edilmesi ve anonim hale getirilmesine ilişkin süreçler tanımlanmamıştır (madde 7),
- Kişisel verilerin, ilgili kişilerin ve Kurum'un açık izni alınmadan Kurum dışına veya yurt dışına aktarılması kısıtlanmamıştır (madde 8 ve 9),
- İlgili kişilerin kişisel verilerine ilişkin taleplerinin yerine getirilme süreçleri ve süreleri tanımlanmamıştır (madde 11),
- İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde işletilecek süreçler tanımlanmamıştır (madde 12),
- Veri güvenliğine ilişkin teknik ve idari şartlar tanımlanmamıştır (madde 12),
- Kurum'un, veri güvenliğine ve kişisel verilerin işlenmesine ilişkin olarak, kendi uygun göreceği vakitte bizzat kendi elemanları veya görevlendireceği kişiler aracılığıyla denetim ve gözetim yetkisine sahip olduğu belirtilmemiştir (madde 12),
- Kişisel verilere ilişkin genel hükümlerin ihlal edilmesi veya yüklenicinin ihmali dolayısıyla Kurum'un veya Kurum çalışanlarının bir cezai müeyyide ile karşılaşması durumunda yükleniciye uygulanacak müeyyideler tanımlanmamıştır (madde 17 ve 18).
- Kişisel verilere ilişkin olarak sözleşmelerde yer verilecek hükümlerin ihlalinin Kurum tarafından sözleşmenin askıya alınması veya feshedilmesi sebeplerinden biri olacağı belirtilmemiştir.
- Hizmet akdinin sona ermesi veya sözleşmenin feshedilmesi durumunda kişisel verilerin yok edilmesi yükümlülüğünün nasıl yerine getirileceği ve buna ilişkin süreçler tanımlanmamıştır.

Hizmet alımı yöntemiyle yürütülen işlerde kişisel verilerin mevzuata uygun şekilde işlenmesine özel önem verilmelidir. Bu amaçla, kişisel verilerin kullanımıyla ilgisi olan

yürürlükteki tüm sözleşmelerin gözden geçirilmesi, mevzuata uygun olacak şekilde tadil edilmesi ve yeni sözleşmelerin yapılmasında yukarıda belirtilen hususlara dikkat edilmesi gerekmektedir.

Sonuç olarak; Kurum'da Kişisel Verilerin Korunması Kanunu'na uyum amacıyla yürütülen çalışmaların amacına ulaşabilmesi için, veri envanterinin oluşturulması, ilgili iş süreçlerinin yetkilendirme, güvenlik ve gözetime ilişkin kontrolleri içerecek şekilde ihdas edilmesi ve yükleniciler tarafından yürütülen çalışmaların mevzuata uygunluğunun sağlanması gerekmektedir.

BULGU 3: Lisansı Olmayan Yazılımların Kullanılmasının Engellenmemesi

Kurum bilgisayarlarında, kullanıcılar tarafından indirilerek yüklenmiş olan çok sayıda lisanssız program kullanıldığı, mevzuata aykırı olan bu durumun bilişim sistemlerini saldırıya açık hale getirdiği belirlenmiştir.

Fikir ve sanat eserleri üzerinde sahiplerinin mali ve manevi menfaatleri, 5846 sayılı Fikir ve Sanat Eserleri Kanunu dairesinde himaye görmektedir. Söz konusu Kanun'un 2'nci maddesi ile bilgisayar programları korumaya tabi ilim ve edebiyat eserleri arasında sayılmıştır. Kanun, lisanslı yazılımlar (bilgisayar programları) üzerindeki mali haklarla bu hakların ihlali halinde uygulanacak müeyyideleri de belirlemektedir.

Söz konusu Kanun'la, belirli bir lisansı olan ücretli yazılımların lisanssız kopyalarının indirilmesi ve kullanılması yasaklanmış ve müeyyidelere bağlanmıştır.

Lisanslı Yazılım Kullanılması hakkındaki 2008/17 sayılı Başbakanlık Genelgesi ile kamu kurulumlarında bilgisayar programlarının edinilmesine ilişkin esaslar düzenlenmiştir. Söz konusu Genelge, kurumların ihtiyaç duydukları lisans sayısının karşılığının bütçede gösterilmesi gerektiğini belirtmektedir.

Buna ek olarak Genelge'de, lisanssız yazılımlarının bulundurulması ve kullanımının önlenmesi maksadıyla kamu kurumları tarafından yapılacak çalışmalar şu şekilde belirlenmiştir:

"Lisanssız yazılımlarının bulundurulması ve kullanımının önlenmesi maksadıyla kamu kurum ve kuruluşları;

- *Lisans hakları kamu kurum ve kuruluşuna ait olmayan tüm programların, bilgisayar ve medyalardan silinmesi ve lisanslı olanların temin edil*mesi,*(...)*
- *Lisans sicili oluşturularak kurumun sahip olduğu yazılım ve lisansların takip edilmesi,*
- *Kullanılan yazılımların yasal olarak kurum tarafından sağlanmış orijinaller olup olmadığının ve yazılım siciline uygunluğunun belirli aralıklarla denetlenmesi, (...)*

hususlarında gereken *tedbirleri alacaklardır."*

Yapılan incelemede, bilgi işlem birimi tarafından kurulumu yapılan bilgisayarlara sadece lisanslı yazılımların yüklendiği görülmüştür. Ancak kullanıcıların kendilerine tahsis edilen kurumsal bilgisayarlara yazılım yüklemeleri kısıtlanmamıştır. Sorumlularla yapılan görüşmeler ve örnek olarak seçilen bilgisayarlar üzerinde yapılan incelemeler sonucunda, bilgisayarlara kullanıcılar tarafından indirilen çok sayıda lisanssız yazılım kullanıldığı belirlenmiştir.

Lisanssız yazılım kullanımı, Kurumu, kötü amaçlı yazılım, fidye yazılımı, casus yazılım, virüs vb. birçok güvenlik tehdidi ile karşı karşıya bırakmaktadır. İnternet üzerinden temin edilen lisanssız yazılımların bünyesinde genellikle kötü amaçlı yazılımlar barınmaktadır. Kullanıcılar, bu yazılımları indirmekle kendi kullandıkları bilgisayarları, bu bilgisayarların bağlı bulunduğu sistemleri, sistemlerde yer alan verileri ve diğer kullanıcıları, dolayısıyla Kurumun bilişim sistemlerinin tamamını risk altına sokmaktadır.

Kurumda yürütülen çalışmalarda şu hususlar tespit edilmiştir:

- Lisanssız yazılım kullanımı önemli bir güvenlik ihlali olarak değerlendirilmemektedir,
- Kurum personeli lisanssız yazılım kullanımı ile ilgili riskler hakkında yeterli bilgiye sahip bulunmamaktadır,
- Kuruma ait bilgisayarlara lisanssız yazılım yüklenmesi, iç düzenlemeler ve teknik kontroller ihdas edilmek suretiyle önlenmemiştir,
- Kurumsal bilgisayarların taranması suretiyle lisanssız yazılımların tespit edilip kaldırılmasına yönelik bir çalışma yürütülmemektedir,
- Lisanssız yazılım kullandığı tespit edilen personel hakkında ilgili mevzuat hükümleri işletilmemektedir,

- Lisansı bulunmayan yazılımlar arasında kurumsal ve akademik çalışmaların devam ettirilmesi için kullanılması gerekli olanların olup olmadığı tespit edilmemiştir, dolayısıyla bu ihtiyaçların bütçelendirilmesi veya alternatiflerinin aranması sağlanmamaktadır.

Bu çerçevede Kurum'da yürütülen işlerin aksamasını önlemek ve mevzuata uyumu temin etmek amacıyla, Kurum bünyesinde lisanssız program kullanımının engellenmesi gerekmektedir. Maliyeti kısa süre içinde karşılanamayacak ve kullanımı gerekli görülen yazılımlarla yürütülen işlerin aksamaması, aynı zamanda mevzuata uyumun sağlanması için orta ve uzun vadeli planlar hazırlanması değerlendirilmelidir.

BULGU 4: Bilişim Sistemleri Yönetişim Kontrollerinin Yetersiz Olması

Kurum üst yönetimiyle bilişim sistemlerini yöneten birim arasındaki ilişkinin, orta ve uzun vadeli stratejiler ve planlar ile gözetim ve denetim faaliyetleri çerçevesinde yürütülmesinde yetersizlik olduğu gözlemlenmiştir

5018 Sayılı Kamu Mali Yönetimi ve Kontrol Kanunu'nun, 55'inci maddesinde iç kontrol şu şekilde tanımlanmıştır:

"İç kontrol; idarenin amaçlarına, belirlenmiş politikalara ve mevzuata uygun olarak faaliyetlerin etkili, ekonomik ve verimli bir şekilde yürütülmesini, varlık ve kaynakların korunmasını, muhasebe kayıtlarının doğru ve tam olarak tutulmasını, malî bilgi ve yönetim bilgisinin zamanında ve güvenilir olarak üretilmesini sağlamak üzere idare tarafından oluşturulan organizasyon, yöntem ve süreçle iç denetimi kapsayan malî ve diğer kontroller bütünüdür…"

İç kontrol özetle, idarenin sağlıklı çalışmasını etkileme ihtimali olan risklerin tanımlanması ve bu riskleri ortadan kaldıracak eylem ve süreçlerin oluşturulmasıdır. Kurumların faaliyetlerinin büyük ölçüde bilişim sistemleri desteğiyle yürütülmesi sebebiyle günümüzde iç kontrollerin önemli bir kısmının bilişim ortamında oluşturulması gerekmektedir. Nitekim Maliye Bakanlığı tarafından 5018 sayılı kanuna dayanılarak 2007 yılında yayınlanan Kamu İç Kontrol Standartları Tebliği'nde bu husus standarda bağlanmıştır. Tebliğde yer alan 12 numaralı *"Bilgi sistemleri kontrolleri"* standardında, idarelerin, bilgi sistemlerinin sürekliliğini ve güvenilirliğini sağlamak için gerekli kontrol mekanizmalarını geliştirmeleri gerektiği vurgulanmış ve *"İdareler bilişim yönetişimini sağlayacak mekanizmalar geliştirmelidir"* denilmiştir.

Bilişim sistemleri kontrolleri arasında yer alan yönetişim kontrollerinin amacı, güvenli ve yeterli bir bilişim ortamının sağlanması için kurumsal strateji ve amaçlara uygun yönetim, karar alma, yönlendirme ve izleme mekanizmalarının oluşturulmasını sağlamaktır. Bu kontroller kuruma, alt düzeydeki ayrıntılı kontrollerin varlığı ve etkinliği konusunda makul bir güvence sağlar.

Etkin bir bilişim sistemleri yönetişim yapısının kurulması; kurumun stratejik hedeflerine ulaşmasını, paydaş ihtiyaçlarına uygun ürünler ortaya çıkarmasını, bilişim sistemleri ile ilgili riskleri yönetmesini, kaynakları daha etkin kullanmasını, bilgi güvenliği gereklerine ve yasal mevzuata uygun çalışmasını destekler.

Yürütülen denetim çerçevesinde iç kontrollerin etkinliği değerlendirilirken bilişim sistemleri kontrolleri incelenmiş, Kurumda bilişim sistemlerinin geliştirilmesi ve güvenliğe kavuşturulması amacıyla çok kapsamlı ve yetkin çalışmalar yürütüldüğü, ancak yönetişim alanında kurulan kontrollerin yetersiz olduğu görülmüştür.

a. Kurumda Yazılı ve Müstakil Bir Bilişim Sistemleri Stratejisinin Oluşturulmaması

Kurum bilişim sistemlerine ilişkin çalışmaların yazılı ve müstakil bir planlama süreci çerçevesinde yürütülmediği, bunun, bilişim sistemlerinin üst yönetim tarafından yakından izlenmesini ve yönetilmesini öngören kontrollerin işletilmesinde yetersizliğe sebep olduğu görülmüştür.

e-Devlet Hizmetlerinin Yürütülmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik'in *"Kamu kurum ve kuruluşlarının görev ve sorumlulukları"* başlıklı 7'nci maddesinde, kamu kurum ve kuruluşlarının bilişim stratejileri hazırlaması gerektiği şu şekilde ifade edilmiştir:

"*b) Kamu kurum ve kuruluşları, ulusal stratejiler ve planlar ile mevcut kurumsal stratejik planlarıyla uyumlu, kurumun e-Devlet hizmetleri sunumu amacıyla yapacakları yatırım, teknoloji tercihleri, kurumsal kapasite, tasarruf planları, fayda-maliyet, iş planı gibi unsurları kapsayacak bilişim stratejilerini hazırlar."*

Kurumun bilişim sistemleri ile ilgili hedefler, yatırımlar ve eylemler müstakil bir strateji ile yönetilmediğinden, bunların kurumun ana stratejisi ve amaçları ile ne derecede uyumlu olduğunun Kurum üst yönetimi tarafından izlenmesinin oldukça güç olduğu gözlenmiştir.

Kurumun, üst yönetimin ve ilgili paydaş birimlerin katılımıyla yazılı ve müstakil bir bilişim sistemleri stratejisi oluşturması gerekmektedir.

b. Bilişim Sistemlerine İlişkin Planlama, Koordinasyon ve İzlemenin Sağlanmasına Yönelik Kurumsal Bir Mekanizmanın Bulunmaması

Kurum üst yönetiminin, bilişim sistemlerine ilişkin planlama, koordinasyon ve izleme faaliyetlerine etkin olarak katılmasını sağlayacak kurumsal süreç ve yapıların oluşturulmadığı gözlenmiştir.

Kurum bilişim sistemlerinin yönetişimini sağlamak üst yönetimin sorumluluğundadır. Bazı kurumlarda bu amaçla üst yönetimin içinde yer aldığı bir Bilişim Sistemleri Yönlendirme Kurulu veya eşdeğeri yapılar oluşturulmuştur.

Ancak, mevcut durumda Kurum üst yönetiminin bilişim sistemleri ile ilgili kararlara katılımının; görevlendirmelerin yapılması, bütçelerin ve satın alma süreçlerinin onaylanması ve genel çalışma çerçevesini belirleyen iç düzenlemelerin yapılması gibi faaliyetlerle sınırlı kaldığı görülmüştür. Bilişim ile ilgili kararlarda üst yönetimi, bilişim sistemleri yöneticilerini ve bilişim sistemlerinden doğrudan etkilenen önemli birimlerin yöneticilerini (paydaşları) bir araya getiren organ, kurul ve mekanizmalar ihdas edilmemiştir .

Kurum üst yönetiminin, bilişim sistemleriyle ilgili temel kararların alınması sürecine katılmasını, alınan kararların yürütülmesi sürecinde koordinasyonu sağlamasını ve sonuçları izlemesini temin edecek kurumsal mekanizma ve süreçlerin oluşturması gerekmektedir.

c. Bilişim Sistemlerine İlişkin Faaliyetlerin İç Denetime Tabi Tutulmaması

Kurum bilişim sistemlerinin üst yönetim adına iç denetime tabi tutulmadığı görülmüştür.

Kamu İç Kontrol Standartları Tebliği 17 numaralı standartta *"İdareler fonksiyonel olarak bağımsız bir iç denetim faaliyetini sağlamalıdır."* denilmektedir.

27002 sayılı "Bilgi teknolojisi - Güvenlik teknikleri" adını taşıyan TSE standardının "Bilgi güvenliğinin bağımsız gözden geçirilmesi" başlıklı 18.2.1 numaralı bölümü, bağımsız gözden geçirmenin önemini vurgulamaktadır:

"Kuruluşun bilgi güvenliğine ve uygulamasının (örneğin; bilgi güvenliği için kontrol amaçları, kontroller, politikalar, prosesler ve prosedürler) yönetimine olan yaklaşımı belirli

aralıklarla veya önemli değişiklikler meydana geldiğinde bağımsız bir şekilde gözden geçirilmelidir."

Faaliyet alanının etkinliği dolayısıyla, esasen bilişim sistemlerinin yönetimiyle sorumlu birim, Kurum'un en güçlü birimleri arasında bulunmaktadır. Örneğin yeni bir yazılım geliştirildiğinde, kurumsal süreçlerin nasıl yürütüleceğini, kurumsal ve kişisel bilgilerin nasıl işleneceğini ve nasıl korunacağını, vb. kritik önemdeki birçok konuyu bilişim sistemlerinden sorumlu birim belirlemektedir.

Ancak, bilgi işlem biriminin sahip olduğu bu gücün kurum lehine kullanıldığı hususunda üst yönetime güvence temin edecek gerekli planlama ve gözetim mekanizmalarının kurulmadığı görülmüştür. Bilişim sistemleriyle ilgili olarak üst yönetim tarafından yürütülen kurumsal süreçler, bilişim kaynaklarının etkin bir şekilde yönetilmesi ve kararların doğru alınması için yeterli bilgiyi sağlamamaktadır.

Kuruma ait bilişim sistemleri, oldukça karmaşık, birbirini etkileyen ve dış dünyadan etkilenen iç içe geçmiş süreçlerle işletilmektedir. Bu karmaşık yapı içinde üst yönetim, bilişim alanında kurumsal hedeflere ulaşılmasını güvence altına alacak izleme, sonuçları değerlendirme, gerektiğinde hedef ve planları revize etme faaliyetlerini yerine getirememektedir. Esasen, bu faaliyetlerin yürütülmesi için gerekli altyapıyı sağlayacak olan, bilişim sistemlerini yöneten birimlerin üst yönetim adına denetlenmesi sağlanmamıştır.

Bu hususlara ek olarak, Kurum'da bir iç denetim birimi kurulmamış olması sebebiyle bilişim sistemleri alanında denetim yapılması için gereken altyapı henüz bulunmamaktadır.

Kurumun ivedilikle bir iç denetim birimini oluşturması, bunu yaparken de bilişim sistemleri denetimini rutin faaliyetler arasında yer alacak şekilde planlaması gerekmektedir.

Sonuç olarak, bilişim sistemlerinin Kurum amaçlarına uygun çalışmasını ve işlevlerini doğru bir şekilde yerine getirmesini sağlayacak etkin bir bilişim sistemleri yönetişim yapısının oluşturması, bu amaçla bilişim sistemlerine ilişkin planlama süreçlerinin ve yönetişim mekanizmalarının ihdas edilmesi ve bilişim sistemleri denetiminin düzenli olarak yapılması gerekmektedir.

BULGU 5: Dış Tedarikle Yürütülen Bilişim Hizmetlerine İlişkin Sözleşmelerin Bilgi Güvenliği Yönünden Yetersiz Olması

Kurumda hizmet alımı yöntemiyle tedarik edilen bilişim hizmetlerine ilişkin olarak imzalanan sözleşmelerde yer verilen hükümlerin bilgi güvenliğini temin etmek için yeterli olmadığı tespit edilmiştir.

Hizmet İşleri Genel Şartnamesi'nin *"Gizlilik"* başlığını taşıyan 13'üncü maddesi şu şekildedir:

"Yüklenici, işle ilgili olarak elde ettiği her tür bilgi ve dokümanı özel ve gizli tutacak ve idarenin önceden yazılı izni olmaksızın sözleşmeye ait herhangi bir detayı ifşa etmeyecek veya yayınlamayacaktır. Türk yargı mercilerinin kararları saklı kalmak kaydıyla, sözleşmenin amaçları doğrultusunda herhangi bir ifşa veya yayınlama gerekliliği konusunda bir uzlaşmazlık ortaya çıkarsa idarenin bu konudaki kararı nihai olacaktır. Gizlilik yükümlülüğü, sözleşmenin herhangi bir nedenle sona ermesinden sonra da devam eder."

Söz konusu şartnamenin *"Kontrol teşkilatı ve yetkileri"* başlığını taşıyan 26'ncı maddesinde şu ifadeye yer verilmiştir:

"Sözleşmeye bağlanan her türlü iş, idare tarafından görevlendirilen kontrol teşkilatının denetimi altında, yüklenici tarafından yönetilir ve gerçekleştirilir."

Hizmet Alımlarına Ait Tip Sözleşme'nin *"Kontrol Teşkilatı, görev ve yetkileri"* başlığını taşıyan 18'inci maddesi şu şekilde tanzim edilmiştir:

"İşin, sözleşme ve eklerine uygun olarak yürütülüp yürütülmediği İdare tarafından görevlendirilen Kontrol Teşkilatı aracılığıyla denetlenir. Kontrol Teşkilatı, Genel Şartnamenin Dördüncü Bölümünde belirtilen yetkileri kullanır ve görevleri yerine getirir"

Bilgi işlem varlıklarını ilgilendiren ve dış tedarik yoluyla alınan hizmetlerde, yükleniciler tarafından erişilebilen kurumsal bilgi varlıklarının korunması büyük önem taşımaktadır. Kurum, kendi birimleri tarafından yürütülen hizmetlerde, bilgi varlıklarını korumak amacıyla kurallar koyabilmekte ve uygulamayı izleyerek denetleyebilmektedir. Bu hizmetlerin yükleniciler tarafından yerine getirilmesi durumunda ise aynı güvenceleri sağlayabilmek için bu faaliyetler üzerinde özel kontroller tesis edilmesi gerekmektedir.

Yukarıda belirtilen, kurumların satın alma süreçlerinde kullandıkları ve genel amaçlarla geliştirilmiş sözleşme ve şartname şablonlarında yer alan ifadeler, bilgi güvenliği ile ilgili gerekliliklerin yerine getirilmesi için yeterli bulunmamaktadır. Örneğin, yükleniciye ait olan ve sözleşme konusu hizmetlerde kullanılan bilişim sistemlerinin Kurum tarafından denetimine izin veren açık bir sözleşme hükmü bulunmadıkça, Kurum kontrol teşkilatının bu tür bir denetimi yapmasına yüklenicinin rıza göstermesi beklenmemektedir.

Bu sebeple dış tedarik yoluyla alınan bilişim hizmetlerine ilişkin sözleşmelerde, kamu menfaatlerinin korunması amacıyla ek düzenlemeler yapılmasına ihtiyaç bulunmaktadır. Genel sözleşme ve şartname şablonlarında yer alan gizlilik, gözden geçirme ve kontrol teşkilatı ile ilgili hususlara ek olarak, sözleşmelere, bilişime mahsus ihtiyaçları karşılayacak maddelerin eklenmesi gerekmektedir.

27002 sayılı "Bilgi teknolojisi - Güvenlik teknikleri" standardı, tedarikçilerle ilişkilerin ne şekilde tanzim edilmesi gerektiğini belirlemektedir. Söz konusu standartta "*Tedarikçi ilişkileri için bilgi güvenliği politikası"* başlığını taşıyan 15.1.1 numaralı kontrol şu şekilde tanımlanmıştır:

"Tedarikçinin kuruluşun varlıklarına erişimi ile ilgili riskleri azaltmak için bilgi güvenliği gereksinimleri tedarikçi ile kararlaştırılmalı ve yazılı hale getirilmelidir (...)

Kuruluş, politikada özellikle kuruluşun bilgilerine erişen tedarikçileri ele alarak bilgi güvenliği kontrollerini tanımlamalı ve zorlamalıdır."

Aynı standartta *"Tedarikçi hizmetlerini izleme ve gözden geçirme"* başlığı altında tanımlanan 15.2.1 numaralı kontrol şu şekildedir:

"Kuruluşlar, düzenli aralıklarla tedarikçi hizmet sunumunu izlemeli, gözden geçirmeli ve tetkik etmelidir."

İlgili düzenlemelerde tanımlandığı şekilde dış tedariklerde Kurum, kendisine ve kullanıcılarına ait bilgilerin güvenliğinin sağlanması için gerekli tüm tedbirleri almakla yükümlüdür. Dış tedarik sürecinde bilgi varlıklarının bu şekilde korunması, tedarik edilen bilişim hizmetleri kapsamında kullanılan, yükleniciye ait tüm sistem ve süreçlerin, Kurum tarafından belirlenmiş risk yönetimi, güvenlik ve gizliliğe ilişkin ilkelere uygunluğunun sağlanmasını gerektirir. Yani yüklenicinin Kurum'un bilgi güvenliği kurallarına uyması temin edilmeli ve bu uygunluğun sağlanıp sağlanmadığı Kurum tarafından denetlenmelidir.

Bu amaçla, yüklenicilerin Kurum verilerine erişim sağlamasını gerektiren bilişim hizmetleri ile ilgili bilgi güvenliği çerçevesinin sözleşme ve şartnamelerde açıkça tanımlanması gereklidir. Yüklenicilere verilecek, bilişim sistemlerine erişim yetkileri, işin gerektirdiği bilgiyi kapsayacak şekilde sınırlandırılmalı, sözleşmeler de buna uygun şekilde tanzim edilmelidir.

Bu çerçevede, Kurum tarafından dış tedarik yoluyla alınan bilişim hizmetlerine ilişkin olarak "Üçüncü Taraf Güvenlik Politikası" hazırlandığı, ancak bu belgenin yeterli kapsamda olmadığı görülmüştür. Bilgi güvenliği ile ilgili hususlara kısmen hizmet alımına ilişkin şartnamelerde yer verilmektedir. Ancak, yürütülen hizmetlere ilişkin bir risk değerlendirmesi yapılmadığı için ihdas edilmesi gereken kontroller somut bir şekilde tanımlanamamakta, sözleşmelerde kullanılan soyut ifadeler bilişime ilişkin riskleri yönetmek için yetersiz kalmaktadır.

Kurumun dış tedarik yoluyla yürütülen bilişim hizmetlerine ait sözleşmelere ilişkin şu hususlar tespit edilmiştir:

- Sözleşmelerde, yüklenicilere ait sistem ve süreçlerin, Kurumun kendi risk yönetimi, güvenlik ve gizliliğe ilişkin ilkelerine uygun olmasını güvence altına alacak hükümlere yer verilmemiştir,
- Yüklenicilerin Kurum bilişim varlıklarına erişiminin nasıl yönetileceği ve izleneceği tanımlanmamıştır,
- Yüklenici ve personeli tarafından kullanılabilecek erişim türleri (uzaktan erişim vb.), erişilecek verinin kritiklik derecesi ve erişimin bilgi güvenliği üzerindeki etkileri tanımlanmamıştır,
- Yükleniciler tarafından erişilen gizli veya kişisel nitelikteki verilerin gizliliğinin ve güvenliğinin nasıl korunacağı belirlenmemiştir,
- Yüklenici personelinin işten ayrılması veya sözleşme kapsamındaki hizmetin sonlanması durumunda yüklenici personelinin erişim haklarının iptal edilme süreci tanımlanmamıştır,
- Bilgi güvenliğine ilişkin olarak yüklenici bünyesinde alınan tedbirler üzerinde Kurumun denetim/ gözden geçirme hakkı ve bu hakkın nasıl kullanılacağı tanımlanmamıştır,
- Yüklenicinin, hizmet kapsamında gerçekleşen güvenlik ihlallerini bildirme yükümlülüğü tanımlanmamıştır.

Kurum tarafından hizmet alımı yöntemiyle yürütülen bilişim hizmetlerine ilişkin olarak yürürlükte olan sözleşmelerin, bilgi güvenliğini temin edecek ve yukarıda belirlenen hususları da içerecek şekilde tadil edilmesi ve yeni sözleşmelerin bu hususları karşılayacak şekilde tanzim edilmesi gerekmektedir.

BULGU 6: Bilişim Sistemlerinin Sürekliliğini Güvence Altına Alacak Kontrollerin Yetersiz Olması

Kurumda, bilişim sistemleriyle yürütülen hizmetlerin kesintiye uğraması veya bir felaketle karşı karşıya kalması durumunda, söz konusu hizmetlerin sürekliliğinin sağlanması için alınması gereken kontrollerin yetersiz olduğu tespit edilmiştir.

Kamu İç Kontrol Standartları Tebliği'nde 11 ve 12 No'lu Standartlarda şu kontroller tanımlanmıştır:

"İdareler, faaliyetlerin sürekliliğini sağlamaya yönelik gerekli önlemleri almalıdır."

"Bilgi sistemlerinin sürekliliğini ve güvenilirliğini sağlayacak kontroller yazılı olarak belirlenmeli ve uygulanmalıdır."

E-Devlet Hizmetlerinin Yürütülmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik'in *"Kamu kurum ve kuruluşlarının görev ve sorumlulukları"* başlıklı 7'nci maddesinde şu hükümlere yer verilmiştir:

"d) Kamu kurum ve kuruluşları, e-Devlet hizmetlerini kullanım kolaylığı ve kullanıcı memnuniyetini sağlayacak şekilde; ulusal ve uluslararası standartlara uygun olarak, işlevsel, güvenli, talebe cevap verebilir ve kesintisiz şekilde sunar (...)"

m) Kamu kurum ve kuruluşları herhangi bir felaket anında sistemlerin kesintiye uğramaması için gerekli tedbirleri alır."

Kurumlarda sistemlerin kesintiye uğramaması için alınan tedbirler, iş sürekliliği ve felaket kurtarma planları ve bu planların ifası için gerekli olan altyapılarla sağlanmaktadır.

İş sürekliliği planı, bilişim hizmetlerinde herhangi bir kesinti meydana gelmesi durumunda yapılacak çalışmaları tanımlayan bir belgedir. Bu belgede kesinti durumunda kimin hangi görevi yerine getireceği, hangi sistemlerin öncelikle ele alınacağı, öncelikli kurtarma adımlarının neler olduğu, tahliye prosedürlerinin neler olduğu, can ve mal

kayıplarının en aza indirilmesi için gerekli prosedürlerin neler olduğu, planının kim tarafından ve nasıl aktif hale getirileceği gibi hususlara yer verilir.

Benzer şekilde felaket kurtarma planı bir felaket sonrası bilişim alt yapısının yeniden aktif hale getirilmesini ele alır. Bu plan iş sürekliliği planının içinde bir bölüm olarak yer alabileceği gibi müstakil bir plan olarak da hazırlanabilir. İster iş sürekliliğinin bir parçası ister ayrı bir plan olsun felaket kurtarma planları iş sürekliliği planıyla uyumlu olmak zorundadır.

İş sürekliliği planı ne kadar detaylı ve doğru hazırlanmış olursa olsun test edilmedikçe güvenilir değildir. Bu tür planların zayıf noktalarının; birbiriyle çelişen ve hatalı sıralanmış adımların, eksik kalan görevlendirmelerin ve tespiti yapılmamış ihtiyaçların görülebilmesi bir test yapılması ile mümkün olacaktır.

Kurum bilişim sistemlerinde yapılan incelemede iş sürekliliğini sağlamak amacıyla çeşitli belgeler oluşturulduğu, iş sürekliliği planının hangi süreçlerle hazırlanacağının belirlendiği ancak planın henüz hazırlanmadığı görülmüştür. Ancak bu süreç tasarımı, bilgi işlem birimi bünyesinde yürütülmüş olup üst yönetim tarafından onaylanmamıştır. Dolayısıyla sürekli ve tutarlı bir şekilde uygulanması güvence altına alınmamıştır.

Kuruma ait bir felaket kurtarma merkezi (FKM) kurulması için ihale yapıldığı ancak sürecin henüz tamamlanmadığı ve bir felaket kurtarma planının henüz hazırlanmamış olduğu görülmüştür. Bu tür bir plan hazırlanarak test edilmedikçe, kurulmuş altyapının ihtiyaç anında uygun şekilde kullanılamaması riski bulunmaktadır.

Kurum bünyesinde bilişim sistemleri iş sürekliliği ve felaket kurtarma planlarının hazırlanması ve üst yönetimce onaylanarak yürürlüğe konması, bu planların test edilmesi ve güncelliğinin korunması ve felaket kurtarma merkezi çalışmalarının tamamlanması gerekmektedir.

BULGU 7: Bilişim Varlıkları Üzerinde Gerçekleştirilecek Değişikliklerin Yönetimiyle İlgili Kural ve Uygulamaların Yetersiz Olması

Kurumun bilişim sistemleri üzerinde gerçekleştirilecek değişikliklerin yönetilmesi için kullanılacak kuralların ve süreçlerin ve acil durumlarda bu süreçlerin nasıl işletileceğinin belirlenmemiş olduğu görülmüştür.

27002 sayılı "Bilgi teknolojisi - Güvenlik teknikleri" standardında konuyla ilgili tanımlanan kontrol şu şekildedir:

"12.1.2 Değişiklik Yönetimi

Bilgi güvenliğini etkileyen, kuruluş iş prosesleri, bilgi işleme tesisleri ve sistemlerdeki değişiklikler kontrol edilmelidir."

Kurumun bilişim varlıklarını ve süreçlerini etkileyebilecek tüm değişikliklerin kontrollü bir şekilde gerçekleştirilmesi gereklidir. Değişikliklerin, bunlardan etkilenecek bileşen ve sistemler tanımlanmadan yürütülmesi, farklı sistemlerin aksamasına sebep olabilir. Söz konusu değişikliklerin, ilgili etkileşimleri izlemeye ve gerekli tedbirleri almaya imkân tanıyacak şekilde planlanarak yürütülmesi gerekmektedir. Örneğin, yazılım güncellemeleri gibi bazı değişikliklerin test edilmeden hayata geçirilmesi bilişim hizmetlerinde önemli aksamalara sebep olabilmektedir.

Bilişim sistemlerinin yapısı gereği, ne kadar planlama yapılırsa yapılsın, bazı değişikliklerin acil nitelik taşıması ve herhangi bir planlama ve bildirim sürecine imkân tanımayacak şekilde ivedilikle uygulanması söz konusu olabilmektedir. Acil durum değişikliklerinde, değişikliğe ilişkin sürecin gecikmesi kurumu yüksek maliyetler ile karşı karşıya getirebilir. İvedi müdahaleyi gerektiren bu tür durumlarda rutin değişikliklerin yönetimi için tasarlanmış süreçlerin işletilmesi mümkün olmayabilir. Ancak doğurduğu yüksek riskler sebebiyle acil durum değişikliklerinin sonradan takip edilmesi büyük önem taşır. Bu önemi sebebiyle acil durumlarda yapılan değişikliklere ilişkin ayrı bir süreç işletilmesi ve bu değişikliklerin geriye dönük olarak ilgilere bildirilmesi, etkilerinin izlenmesi ve gerekli tedbirlerin alınması sağlanmalıdır.

Kurum bilişim sistemlerinde yapılması planlanan değişikliklerde son kullanıcılarla iletişim kurulduğu ve akademik takvim izlenerek yapılan değişikliklerin etkisinin en aza indirilmesine çalışıldığı belirlenmiştir. Ancak bu uygulama değişikliklerin etkisinin izlenmesi için yeterli değildir ve bilgi işlem biriminin çabası ile yürütülmekte olup, zorunlu bir süreç niteliğinde değildir. Değişikliklerin sisteme ve iş sürekliliğine etkisinin değerlendirilmesi ve onaylanarak işletilmesi söz konusu olmamaktadır.

Bilişim sistemleriyle ilgili değişiklik talep ve önerilerinin yönetim süreçlerinin ve acil durum değişikliklerine ilişkin süreçlerin belirlenmesi, değişikliklerin hangilerinin onaya tabi

olacağının, değerlendirmenin kimler tarafından yapılacağının, ret ve kabul kriterlerinin tanımlanması gerekmektedir.

T.C. SAYIŞTAY BAŞKANLIĞI
06520 Balgat / ANKARA
Tel: 0 312 295 30 00; Faks: 0 312 295 48 00
e-posta: sayistay@sayistay.gov.tr
http://www.sayistay.gov.tr

8. EKLER

EK 1: İZLEME

Önceki Yıl/Yıllar Sayıştay Denetim Raporuna İlişkin İzleme Tablosu			
Bulgu Adı	**Yıl/Yıllar**	**İdare Tarafından Yapılan İşlem**	**Açıklama**
Bilimsel Araştırma Projelerinde Hatalı ve Eksik Uygulamalar Bulunması.	2017	Tam Olarak Yerine Getirildi	Sayıştay raporunda belirtilen bulgulara ilişkin kurum tarafından düzeltici işlemler tesis edilmiştir. BAP proje otomasyonu ile bütçeler ve süreler titizlikle takip edilmektedir.