KAMU İDARELERİNDE BİLGİ SİSTEMİ GÜVENLİK RİSKLERİNİN YÖNETİMİ

Erdal DAYIOĞLU
İç Denetçi
Tapu ve Kadastro Genel Müdürlüğü

ÖZET: *Bilgi sistemleri kurumların hedeflerine ulaşmasında ve bilginin doğru, güvenilir ve hızlı bir şekilde kullanılmasında etkinlik sağlamakta ve gün geçtikçe kurumsal fonksiyonların bilgi sistemleri olmadan yürütülmesi imkânsız hale gelmektedir. Bilgi sistemi güvenlik risklerine karşı uygun kontrol önlemleri geliştirilmediği takdirde bilgi sistemi kaynaklı hatalar, büyük itibar ve maddi kayıplara yol açabilmekte ve kritik kurumsal fonksiyonların yerine getirilmesini engelleyebilmektedir. Bu nedenle bilgi sistemleri süreçlerinin farklı bir yaklaşımla ele alınması, bilgi sistemi biriminin önceden tanımlı ve kontrol altında tutulan süreçlerle yönetilmesi ve düzenli olarak kontrollere tabi tutulması önem arz etmektedir. Bu nedenle bilgi sistemlerindeki güvenlik riskleri yönetilirken; dünya genelinde kullanılan ve ortak lisan olarak kabul gören uluslararası standartlardan, metotlardan, modellerden ve çerçevelerden yararlanılmalıdır. Bu çalışmada bilgi sistemleri güvenlik riskleri; bilgi güvenliği, mantıksal erişim ve fiziksel erişim riskleri olarak üç ayrı başlık altında incelenmiş ve bu risklere karşı risk yönetimi metoduna uygun olarak öneriler geliştirilmiştir. Belirtilen riskler ve önerilen kontrol önlemleri ile ilgili olarak, bu alanda görev yapan yöneticiler ve çalışanlar düzeyinde farkındalık yaratılacağı ve önerilerin kamu idarelerinin bilgi sistemi güvenlik risklerinin yönetiminde etkin bir şekilde kullanılabileceği değerlendirilmektedir.*

ANAHTAR KELİMELER: *Bilgi güvenliği, mantıksal erişim, fiziksel erişim, risk, kontrol, risk yönetimi.*

I. GİRİŞ

Risk kavramı, öngörülebilir zarara uğrama tehlikesini, risk yönetimi kavramı ise kurumun hedeflerine ulaş-

masını olumsuz yönde etkileyecek olası olay ve durumların önceden belirlenmesi, ölçülmesi ve en alt düzeye indirilmesi sürecini ifade etmektedir[1].

Bilgi sistemlerine dayalı süreçler, artık kurum ve kuruluşların varlıklarını devam ettirebilmeleri açısından olmazsa olmaz unsurlar arasında sayılmaktadır[2]. Bilgi sistemi süreçlerinin herhangi bir sebeple olumsuz yönde etkilenmesi aynı zamanda kurum veya kuruluşların asli işlevlerini sürdürememesi anlamına gelmektedir. Teknolojinin gelişmesi; iş, işlem, ürün ve hizmet çeşitliliğinin artması ve süreçlerin karmaşık hale gelmesi sistemler üzerindeki kontrolü zorlaştırmaktadır. Bu nedenle, kurum ve kuruluşlar olası bir zarara karşı kontrol önlemlerini önceden almalı ve gerekli altyapı yatırımlarını önceden yapmalıdır.

26 Aralık 2007 tarih ve 26738 sayılı Resmî Gazete'de yayımlanan Kamu İç Kontrol Standartları Tebliğinde, bilgi sistemleri kontrolleri ile ilgili standart ve şartlara yer verilmiş ve kamu idarelerinde bilişim yönetişimini sağlayacak mekanizmaların geliştirilmesi ve bilgi sistemlerinin sürekliliğini ve güvenilirliğini sağlayacak kontrollerin belirlenmesi gerektiği belirtilmiştir. Kamu idarelerinde bilgi sistemi güvenlik risklerinin yönetimi konusu, bugün hem akademik çevrede, hem de uygulayıcılar tarafından üzerinde ciddi olarak durulması ve geliştirilmesi gereken bir alan olarak kabul edilmektedir[3].

Bilgi sistemleri güvenlik riskleri ve bu risklere karşı alınacak önlemler bilgi güvenliği riskleri, mantıksal erişim riskleri ve fiziksel erişim riskleri olarak üç ayrı başlık altında aşağıda inceleme konusu yapılmıştır.

II) BİLGİ GÜVENLİĞİ RİSKLERİ

A) Bilgi Güvenliği Yönetimi

Bilgi güvenliği yönetimi, riskler göz önünde bulundurularak işlerde meydana gelebilecek aksaklıkların azaltılmasını, bilginin geniş çaplı tehditlerden korunmasını ve bilgi sistemi hizmetlerinin sürekliliğini sağlayacak bir kontrol yapısının kurularak sürdürülmesini hedeflemektedir[4]. Bu çerçevede bilgi sistemi hizmetlerinin ve fonksiyonlarının devamlılığının sağlanması için bir politika ve kontrol çerçevesi oluşturulması, yol gösterici dokümanların hazırlanması, bilgi sistemlerini güvenlik altına almak için uygulanan kontrol mekanizmalarının incelenmesi ve bilgi sistemlerinden alınan rapor ve çıktıların güvenilirliğinin ölçülmesi gerekmektedir[5].

"Bilgi güvenliği yönetimi, riskler göz önünde bulundurularak işlerde meydana gelebilecek aksaklıkların azaltılmasını, bilginin geniş çaplı tehditlerden korunmasını ve bilgi sistemi hizmetlerinin sürekliliğini sağlayacak bir kontrol yapısının kurularak sürdürülmesini hedeflemektedir"

B) Bilgi Güvenliği Riskleri

Genel olarak kamu kurumlarında bilgi sistemine yönelik güvenlik önlemleri, uygulayıcı birimlerin inisiyatiflerine bağlı kalmakta ve mevcut önlemlerin ku-

1 ATAN, Murat: Risk Yönetimi ve Türk Bankacılık Sektöründe Bir Uygulama, Doktora Tezi, Ankara 2002, s.5-6; DERİCİ, Onur/TÜYSÜZ, Zekeriya/SARI Aydın: Kurumsal Risk Yönetimi ve Sayıştay Uygulaması, Sayıştay Dergisi, S. 65, s.151-172; KUMAŞ, Erhan: e-Devlet Kapısı ve Risk Değerlendirme Metodolojisi, s.2; TEKTAŞ, Halil: Kamu İdarelerinde Kurumsal Risk Yönetim Sistemi, Mali Hukuk, S:138, Kasım-Aralık 2008, s. 26; Türkiye Bilişim Derneği: Bilişim Teknolojilerinde Risk Yönetimi, 2. Çalışma Grubu Raporu, Mart 2006, s.2; ÇALIKUŞU, Faruk / KARAMEHMET, Bilge/ DENİZCİ, Ömer Mert: Bilgi Güvenliği Yönetim Sistemi Kapsamında Risk Yönetim Modeli (senkronbilisim.net/BGYS.pdf), s.5.

2 CEVHER, Ezgi: Bilişim Teknolojileriyle Yaratılan Yeni Bir Yaklaşım: Yönetişim, Gazi Üniversitesi, MBA, 2003, s.1-6; AKIN, H.Bahadır: Bilişim Teknolojileri Evrimi ve Bilişim Teknolojilerinin Çağdaş İşletmelerde Stratejik Yönetim Üzerindeki Etkileri, s.239-251.

3 ÇAYIR, Sinan / GÜNEŞ, Asım / BÜK, Ozan: Türkiye'deki Kamu Kurumlarında Bilişim Teknolojileri Yönetimi, Akademik Bilişim, Ocak-Şubat 2008, s. 544; KUMAŞ, Erhan: Kurumlar üstü Bilgi Güvenliği Stratejisi, s.1-6; VURAL, Yılmaz / SAĞIROĞLU, Şeref: Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme, G.Ü.,Müh., Mim.Fak.Der., 2008, C: 23, s. 507-522; Devlet Planlama Teşkilatı, 8. Beş Yıllık Kalkınma Planı, Bilişim Teknolojileri ve Politikaları Özel İhtisas Komisyonu Raporu, Ankara 2001; Devlet Planlama Teşkilatı, Bilgi Toplumu Stratejisi (2006-2010); Devlet Planlama Teşkilatı, Bilgi Toplumu Stratejisi Eylem Planı (2006-2010).

4 ÇALIKUŞU / KARAMEHMET / DENİZCİ, s.2

5 TBB Çalışma Grubu,: Risk Yönetimi Prensipleri, Bankacılar Dergisi, 2006, S. 57, s. 28-29.

rumun tüm ihtiyaçlarını karşıladığından ve bilgi işlem güvenliği konusunda dikkate alınması gereken her konunun, kurumun amaçlarına uygun, sistematik ve kontrol edilebilir bir şekilde ele alındığından emin olunamamaktadır.

Bilgi sistemi ortamı için hazırlanan kapsamlı bir politika ve plan eksikliği, kamu kurumlarının çalışmalarının sürekliliğini her zaman garanti edememektedir[6]. Deprem, yangın veya benzeri bir afetin meydana gelmesi ve hizmet binasının zarar görmesi durumunda, sistem ve veri tabanı yedeklerine zamanında ulaşılamaması, hatta bunların tamamen kaybedilmesi söz konusu olabilir. Böyle bir durumda bilgi sistemlerine bağlı olarak yürütülen faaliyetlerde aksamalar meydana gelebilir ve ortaya çıkan aksamalar telafisi mümkün olmayan kayıplara neden olabilir.

Üst yönetici tarafından onaylanmış kapsamlı kriz yönetimi ve iş sürekliliği planı bulunmadan ve buna yönelik gerekli kaynaklar tahsis edilmeden, olası bir felaket durumunda kritik iş süreçlerinin ayağa kaldırılabilmesi ve operasyonların devamlılığının sağlanabilmesi mümkün görülmemektedir[7]. Ayrıca, sistem destek fonksiyonları ve ilgili bölümler arasında bir plana bağlı olarak koordine edilen bir çalışma olmadan, kurtarma çalışmalarının başarılı bir şekilde yürütülme şansı azalmaktadır. Olası bir felaket anında kritik fonksiyonların yürütülememesi, telafisi mümkün olmayan kayıplara yol açabilir.

Üst yönetimin ileriye dönük olarak felaket durumunda alınacak önlemleri planlaması, olası felaketlerin kötü sonuçlarını azaltabilir, sistemin çökmesi sonucu doğabilecek mali zararların, itibar kaybının ve faaliyetlerdeki yavaşlamanın önüne geçebilir veya bunların etkisini azaltabilir.

Bilgi sistemi ortamında depolanan verilerin her geçen gün arttığı ve verinin kurumsal süreçler için daha kritik bir rol oynadığı günümüzde verinin sistemin işlerliğini sağlayacak şekilde ana sistemin kurulduğu bina dışında yedeklenmemesi büyük risk oluşturmaktadır.

6 Sayıştay Başkanlığı: Hazine Bilişim Sistemleri Denetimi Raporu, Ekim 2003, s.26-27.

7 Sayıştay Denetim Raporu, s.30-33.

C) Bilgi Güvenliği Kontrol Önlemleri

1) Kamu kurumlarında bilgi sistemi ile ilgili güvenlik politikası oluşturulmalı ve üst yönetici tarafından onaylanarak tüm personele duyurulmalıdır. Bu politika kurum bazında yapılacak çalışmalarla düzenli olarak güncellenmeli ve uygun şekilde gözden geçirilmelidir.

Gözden geçirme işlemi, düzenli periyotlarla, yazılımlar, sistemler veya altyapı konusunda büyük değişiklikler ve güvenlikle ilgili önemli olaylar yaşandığında yapılmalıdır. Gözden geçirmelerde yapılacak incelemenin başlıca konusu, güvenlik politikasının ve mevcut kontrol yapısının etkinliği olmalıdır. Güvenlik politikasının etkinliğinin değerlendirilebilmesi için, güvenliği etkileyen olayların sayısı, tipi ve maliyetleri, gerçekleşen veya şüphelenilen olaylar neticesinde değiştirilen şifre sayısı gibi kriterler kullanılabilir.

Bu politika güvenlik planları, standartlar, prosedürler ve rehberlerle desteklenmelidir[8]. Güvenlik planı, prosedürler ve rehberler de uygun aralıklarla güncellenmelidir. Kullanıcılara, bilgi güvenliği konusundaki politikalar ve kendilerinden beklenen güvenlik önlemlerini tanıtıcı eğitimler verilmelidir. Kullanıcılar güvenlik politikaları hakkında yeterli bilgi sahibi olmalıdır.

Bu politika, bilgi işlem güvenliğinin genel tanımını, amaçlarını ve kapsamını, bilgi işlem güvenliği politika ve prensiplerini yönetimin desteklediğini göstermeye yönelik bir ifadeyi, kurum için önem arz eden konular hakkında güvenlik politikalarını, prensipleri, standartları ve uyumluluk gerekliliklerini içeren kısa açıklamaları (örneğin kanuni yükümlülüklere uyum, güvenlik eğitimi, virüs tespit ve virüs önleme politikaları, e-posta ve internet kullanımı, güvenlik kurallarının ihlali durumunda uygulanacak yaptırımları), bilgi işlem güvenliğinin tüm konuları için genel ve detaylı sorumlulukların tanımını, güvenlik politikasını desteklemeye yönelik diğer belgelere referansları, belirli bazı yazılımlar için detaylı güvenlik prosedürleri, belirli kullanıcıların uymaları gereken güvenlik kuralla-

8 VURAL / SAĞIROĞLU, s.522; SOĞUKPINAR, s.26-30.

rını ve fiziki güvenlik ile ilgili olarak genel ve detaylı sorumlulukların tanımını içermelidir[9].

2) Kamu kurumlarında bilgi sistemi güvenlik planı oluşturulmalı ve üst yönetici tarafından onaylanıp tüm personele duyurulmalıdır. Bu plan bilgi varlıklarını, yapılan işleri ve riskleri; politikaları uygulayan birimlerin ve personelin idari ve teknik görev, yetki ve sorumluklarını; uygulanması ve uyulması gereken kuralları; alınan güvenlik önlemlerini ve kullanıcıların, yöneticilerin ve teknik personelin sorunlarını hangi kanallarla kimlere ne kadar zamanda rapor edeceklerini tanımlamalıdır.

Bu planda, bilgi sistemi güvenlik açıklarının ne şekilde tespit edileceğine ilişkin yöntemler, ağ cihazlarının hangi yöntemler ile nasıl korunacağı, sunuculardan kimlerin sorumlu olduğu ve yönetiminin nasıl yapılacağı, bilgisayar ağının nasıl yönetileceği, sistemde oluşan güvenlik risklerinin nasıl değerlendirileceği ve ne tür önlemler alınacağı, internet sunucularının güvenlik kriterlerinin nasıl sağlanacağı, sistem yöneticilerinin hangi koşullarda sistem bakımı nedeniyle e-posta mesajlarına ve dosyalara girebileceği, sistemi kimlerin hangi amaçlar için kullanabileceği, yasaklanmış kullanım şekillerinin ne olduğu, kriz ve acil durumlarda nasıl hareket edilmesi gerektiği, sisteme erişimde kimlik doğrulama ve yetkilendirmenin nasıl yapılacağı, sistemin fiziksel güvenliğinin nasıl sağlanacağı, değişim yönetimi metodolojisinin nasıl uygulanacağı ve verileri yedeklemenin nasıl yapılacağı hususlarına yer veren temel ilkeler ve prosedürler yer almalıdır.

Bu plan, kurum bazında yapılacak çalışmalarla düzenli olarak güncellenmeli ve uygun şekilde gözden geçirilmelidir.

3) Bilgi sistemi ile ilgili güvenlik politikası ve planı; standartlar, prosedürler ve rehberlerle desteklenmeli ve bu dokümanlar uygun aralıklarla güncellenmelidir. Bilgi güvenliği konusundaki politika, plan, standartlar, prosedürler ve kendilerinden beklenen güvenlik önlemleri konusunda kullanıcılar eğitilerek yeterli bilgi sahibi olmaları sağlanmalıdır[10].

4) Bilgi sistemleri kapsamında değişik görevlere yönelik riskleri ve sistemin kaybedilmesinin kurumsal fonksiyonların devamlılığına ne gibi etkileri olacağını belirleyen, felaketten etkilenebilecek tüm unsurları kapsayan ve kurtarma süresi boyunca bütün kritik iş süreçlerinin sürdürülmesini güvence altına alan acil durum ve kriz yönetimi planı, ilgili birimler arasında eşgüdüm sağlanmak suretiyle geliştirilmeli ve üst yönetici onayı ile yürürlüğe konulmalıdır[11].

Acil durum ve kriz yönetimi planında, acil durum düzeyleri ve senaryoları belirlenmeli, bunlara karşı gerçekleştirilecek faaliyetler ve acil durumdan sonra bilgi işlem faaliyetlerinin sürdürülebileceği alternatif yerler tespit edilmelidir. Acil durum planında donanım, yazılım, gerekli veriler, gerekli cihazlar, telekomünikasyon ve büro ekipmanlarının yenilenmesi konusunda tedarikçiler incelenmeli ve alternatif tedarikçiler belirlenmelidir.

Ayrıca, kritik tedarikçiler ile acil durumda alınacak hizmetlere ilişkin şartname ve sözleşmeler belirlenmeli, normal çalışma sisteminin kesintiye uğraması durumunda hangi hayati unsurların ne şekilde devam ettirileceği ve planın ne kadar sıklıkla test edileceği tespit edilmelidir.

5) Bilgi sistemi kapsamında vatandaşlara hizmet veren birimlere yönelik riskleri ve birimlerin faaliyetlerinde oluşabilecek herhangi bir gecikmenin ne gibi etkileri olacağını belirleyen ve felaketten etkilenmesi muhtemel faaliyetleri (bilgisayar sistemleri haricindeki işlemler dahil) kapsayan ve yeniden kurulum dönemi esnasında bütün kritik fonksiyonların devamlılığını sağlayan bir iş sürekliliği planı[12] hazırlanmalı ve üst yönetici onayı ile yürürlüğe konulmalıdır.

Söz konusu plan, üst yönetimin gözetiminde, kritik

9 VURAL / SAĞIROĞLU, s. 509-510. SOĞUKPINAR, s.26-30; Bilgi Güvenliği Politikası Oluşturma Kılavuzu, TÜBİTAK, Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, Mart 2008, Sayıştay Denetim Raporu, s.28-29.

10 VURAL / SAĞIROĞLU, s. 510-511.

11 Sayıştay Denetim Raporu, s.30-31.

12 TBB Çalışma Grubu, Risk Yönetimi Prensipleri, s. 31-32; Sayıştay Denetim Raporu, s.32-33.

birimler ve bilgi işlem birimi ile birlikte yürütülecek koordineli bir çalışma sonucunda oluşturulmalıdır. Bu yapılırken mevcut risklerle kaynaklar arasında denge gözetilmek suretiyle uygun çözüm yolları belirlenmelidir. Bu planda felaket düzeyleri, senaryolar ve bunlara karşı alınacak önlemler belirlenmelidir.

Planda, birimlerin kritik işlevleri ve bu işlevlere destek veren uygulamalar ile hangi uygulamaların öncelikle ayağa kaldırılacağı belirlenmeli, felaket sonrası iş süreçlerinin ve bilgi işlem operasyonlarının yürütülmesinde kullanılacak alternatif tesisler ve bölgeler, bu tesislerin güvenliği ve bu bölgelerde gerekli bilgisayar sistem donanımları ve iş destek ekipmanları (telefon, faks, yazıcı, kişisel bilgisayar gibi) tespit edilmelidir.
Kurtarma ve yeniden kurulma aşamasında sistem destek personelinin ve gerekli diğer personelin taşıyacağı sorumluluklar, felaket esnasında fonksiyonların bilgisayar sistemi olmaksızın yürütebilmesi için gerekli prosedürler yazılı olarak belirlenmelidir. Bu çerçevede, yeniden kurulum döneminde hangi işlerin manuel olarak yürütüleceği, bu sırada kullanılacak belgelerin ne olduğu ve bu belgelerin çoğaltılarak kullanmaya hazır şekilde tutulmasını sağlayacak önlemlerin neleri kapsadığı ortaya konulmalıdır. Donanım, yazılım, gerekli cihazlar, telekomünikasyon ve büro ekipmanlarının yenilenmesi ile ilgili şartname ve sözleşmelerin ön hazırlıkları yapılmalıdır. Ayrıca planın ne kadar sıklıkla test edilmesi gerektiği planda tespit edilmelidir.

6) Yedekleme sisteminin kurulması, yedeklenecek veri miktarı, yedekleme sıklığı, yedeklenen verinin zaman içerisinde değişme oranı ve kabul edilebilir maksimum veri kaybı gibi parametrelere bağlıdır. Veri yedeklemesinin amacına uygun olarak gerçekleştirilebilmesi için bu konuda yönetim prensiplerini, yedeklemenin önemini, bu sistemin asgari olarak hangi unsurları içermesi gerektiğini tespit eden yedekleme politikası belirlenmeli ve üst yönetici onayı ile yürürlüğe konulmalıdır.

Yedekleme politikasının[13] yerine getirilmesi için, yedekleme donanımları ve altyapısı, hangi sıklıkla ve hangi türlerde yedek alınacağı, alınan yedeklerin ne kadar süre saklanacağı, yedekleme testinin hangi sıklıkta nasıl yapılacağı, yedekleme merkezinin ana sistemde meydana gelebilecek bir felaketten etkilenmeyecek kadar uzak bir mesafede olması[14] gibi konularda detaylı bir analiz çalışması yapılarak bir yedekleme planı[15] hazırlanmalı ve üst yönetici onayı ile yürürlüğe konulmalıdır. Yedekleme planının işletilmesi ve zaman içerisinde günün ihtiyaçlarına göre güncellenmesi sağlanmalıdır.

7) Bilgi sistemi ile ilgili risk değerlendirme yaklaşımı[16] yazılı olarak tanımlanmalıdır. Tanımlanan metodoloji, risk değerlendirmesinin karşılaştırılabilir ve yeniden elde edilebilir sonuçlar üretmesini sağlamalı, kabul edilebilir risk seviyelerini ortaya koymalı, sistem bünyesindeki varlıklar ve bu varlıklar için var olan tehditler ile gizlilik, bütünlük ve kullanılabilirlik kayıplarının varlıklar üzerinde olabilecek etkilerini ortaya koymalıdır[17].

Risk belirleme çalışmalarında potansiyel tehdit kaynakları [bu kapsamda doğal tehditler (sel baskınları, deprem gibi), çevresel tehditler (yangın çıkması, binaya ait borulardan birinin patlaması ve sistem odasına zarar vermesi) ve insan tehditleri (kötü niyetli kişilerin sisteme zarar vermesi veya yetkin olmayan veya eğitimsiz personelin istemeden sisteme zarar vermesi)] veya zayıflıklar (işten ayrılan personelin sistem ile ilişiğinin kesilmemesi gibi) değerlendirilmelidir[18].

Bilgi sistemi bünyesindeki riskleri önlemek için kontrol amaçları tanımlanmalı ve ihtiyaçları karşılayan kontroller alternatifli olarak yazılı şekilde belirlenmelidir. Belirlenen kontrollerin seçilme nedeni açıklanmalı ve uygulanacak kontrol faaliyetleri sonrasında arta kalan riskler konusunda yönetimin yazılı onayı alınmalıdır.

13 Veri Yedekleme Kılavuzu, TÜBİTAK, Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, Ocak 2008, s.16

14 Türkiye Bilişim Derneği, Bilişim Teknolojilerinde Risk Yönetimi, s.22

15 DİNÇKAN, s.17-18

16 BGYS Risk Yönetimi Süreci Kılavuzu, TUBİTAK, Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, 2007; Türkiye Bilişim Derneği: Bilişim Teknolojilerinde Risk Yönetimi, s.15.

17 Türkiye Bilişim Derneği: Kuruluşlarda Bilgi Güvenliği Yönetim Sistemi Uygulamasında ISO/IEC 27001:2005, 1. Çalışma Grubu Raporu, Nisan 2008, s.8.

18 Türkiye Bilişim Derneği: Bilişim Teknolojilerinde Risk Yönetimi, s.5-7.

Bilgi sistemi güvenlik risklerini yönetme amaçlı risk önleme planı hazırlanmalı, bu plan bilgi güvenliği risklerini yönetmek için gereken yönetim etkinliklerini, kaynaklarını, sorumluluklarını ve önceliklerini içermelidir. Hazırlanan risk önleme planı kapsamında yer alan güvenlik kontrolleri uygulanmalı ve kontrollerin etkinliği ölçülmelidir.

Bilgi sistemi güvenlik olaylarını anında tespit etme ve güvenlik ihlal olaylarına hemen yanıt verebilme yeteneğine sahip güvenlik prosedürleri oluşturulmalı ve güvenlik ihlalleri ile ilgili kayıtlar tutulmalı ve saklanmalıdır.

Risk analizi ve risk değerlendirmeleri düzenli olarak gözden geçirilmeli, bu kapsamda güvenlik açıkları, teknoloji değişimleri, yasalarda ve düzenleyici işlemlerdeki yapılan değişiklikler dikkate alınarak, kabul edilebilir risk düzeyleri tekrar değerlendirilmelidir.

8) Bilgi sistemi güvenlik yönetimi gerçekleştirilirken uluslararası standartlardan, metotlardan ve modellerden yararlanılmalı ve uluslararası alanda genel kabul görmüş güvenlik çerçevelerine uygun güvenlik standartları belirlenmelidir[19].

Bilgi sistemleri güvenlik yönetimi konusunda ISO 17799 standardı, kurumlarda bilgi güvenliği yönetim sistemi kurmayı hedeflemekte ve bilgi varlıklarına yönelik tehditler karşısında uygun koruma önlemlerinin alınmasını sağlayacak kurumsal bilgi güvenliği yönetimi altyapısının kurulmasında yararlanılmaktadır[20]. Bu standardın son hali 2007 yılında ISO 27000 olarak yeniden yayınlanmıştır[21]. Bilgi sistemi güvenlik yönetiminde bu standarttan yararlanılabilir.

Donanım ve hazır yazılımlar için ürün bazında bilgi güvenliğine ilişkin olarak ISO 15408 Ortak Kriterler (Common Criteria) standardı ve OECD Bilgi Güvenliği Politikası Rehberinde[22] yer alan ilkelerden yararlanılabilir. Güvenlik ihtiyaçlarının belirlenmesinde, Avrupa Komisyonu IDABC (Birlikte Çalışabilir Avrupa e-Devlet Hizmetlerinin İdareler, İşletmeler ve Vatandaşlara Sunumu) Programı tarafından geliştirilen Ortak İlgi Alanındaki Projeler İçin Güvenlik Anketi (PCI Security Questionnaire) kaynak ve referans olarak kullanılabilir[23].

Ayrıca, bilgi güvenliği yönetimi konusunda kurumsal hedeflere uyumluluk açısından yaklaşan COBIT (Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri - Control Objectives for Information and Related Technology) kapsamında yer alan planlama ve organizasyon, uygulama, hizmet verme ve destekleme, gözlemleme ve değerlendirme kriterlerinden yararlanılabilir[24]. COBIT çerçevesi, başarısızlıkla sonuçlanabilecek projeleri, yatırım yanlışlarını, güvenlik açıklarını, müşteri / kullanıcı ihtiyaçlarıyla uyumlu olmayan çözümleri, muhtemel sistem kayıplarını üst yönetime görünür kılmayı amaçlamaktadır. COBIT bu yönleriyle bilgi sistemleri yönetişim modelinin oluşturulmasına yardımcı olmakta ve risk odaklı bir kontrol çerçevesi sunmaktadır. Bu model bilgi güvenliği süreç iyileştirmelerinde bir kaynak olarak kullanılabilir[25].

9) Bilgi güvenliği altyapısının oluşturulmasında e-Dönüşüm Türkiye Projesi Birlikte Çalışabilirlik Esasları Rehberinde[26] ve Kamu Bilgi ve İletişim Teknolojisi Projeleri Hazırlama Kılavuzunda[27] yer alan esaslara uyulmalıdır.

19 VURAL / SAĞIROĞLU, s. 520, Türkiye Bilişim Derneği: Kuruluşlarda Bilgi Güvenliği Yönetim Sistemi Uygulamasında ISO/IEC 27001:2005, s. 6-8, Sayıştay Denetim Raporu, s.29

20 ÖZBİLGİN, İzzet Gökhan: Bilgi Teknolojileri Denetimi ve Uluslararası Standartlar, Sayıştay Dergisi, sayı:49, s. 126; Türkiye Bilişim Derneği: Bilgi Teknolojilerinde Yönetişim, 1. Çalışma Grubu Raporu, Nisan 2008, s.39-42.

21 ÇALIKUŞU / KARAMEHMET / DENİZCİ, s.1-8; Türkiye Bilişim Derneği: Kuruluşlarda Bilgi Güvenliği Yönetim Sistemi Uygulamasında ISO/IEC 27001:2005, s.6-7; VURAL / SAĞIROĞLU, s. 507-522

22 OECD Bilgi Sistemlerinin Güvenliğine İlişkin Rehber İlkeleri, [C (2002/131 FINAL], s.1-9

23 Devlet Planlama Teşkilatı, Kamu Bilgi ve İletişim Teknolojisi Projeleri Hazırlama Kılavuzu, Temmuz 2009, s.14-15.

24 ÇAYIR / GÜNEŞ / BÜK s. 541; Türkiye Bilişim Derneği: Bilişim Teknolojilerinde Risk Yönetimi, s.33-51; UZUNAY, Vildan: COBİT (Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri - Control Objectives for Information and related Technology), (www.bumko.gov.tr/KONTROL/Genel/dg.ashx?...DIL=1...COBIT...).

25 Türkiye Bilişim Derneği: Bilgi Teknolojilerinde Yönetişim, S.21-27.

26 Devlet Planlama Teşkilatı, e-Dönüşüm Türkiye Projesi, Birlikte Çalışabilirlik Esasları Rehberi, Ekim 2007, s. 27-36.

27 Kamu Bilgi ve İletişim Teknolojisi Projeleri Hazırlama Kılavuzu, s.14-15.

III) MANTIKSAL ERİŞİM RİSKLERİ

A) Mantıksal Erişim Kontrolleri

Bilgi sisteminde yer alan programların kullanımı, sistemde yetkisi olmayan kişilerin bilgiye erişimini veya bilginin değiştirilmesini engellemek amacıyla kısıtlanmalıdır. Mantıksal erişim kontrolleri, bu amaçla kullanıcıların ve sistem yöneticilerinin programları kullanmalarını kontrol altına almak için uygulanan mekanizmalardır.

Bilgi kaynaklarının korunması ve sisteme yetkisiz girişlerin önlenmesi için sistemde kurulu yazılımlara girişi kontrol altında tutacak mantıksal erişim kontrollerinin oluşturulması gerekir. Mantıksal erişim kontrolleri kurulurken, öncelikle kurum içerisinde üretilen ve kullanılan bilgilere ilişkin bir risk değerlendirmesi yapılır. Bunu takiben bilgi sistemlerine ilişkin olarak kullanıcıların hangi bilgiye hangi seviyede ulaşabileceği belirlenir ve bunu sağlayacak şekilde şifreleme politikaları ve diğer kontroller tespit edilir.

"Bilgi sisteminde yer alan programların kullanımı, sistemde yetkisi olmayan kişilerin bilgiye erişimini veya bilginin değiştirilmesini engellemek amacıyla kısıtlanmalıdır. Mantıksal erişim kontrolleri, bu amaçla kullanıcıların ve sistem yöneticilerinin programları kullanmalarını kontrol altına almak için uygulanan mekanizmalardır"

Bilgi sistemlerinin kritik işlevleri yerine getirmesi sebebiyle bu sistemlerin güvenliğinin sadece kullanıcıların inisiyatifine bırakılmaması ve sistem üzerinden erişim kontrolleri oluşturulması büyük önem arz etmektedir.

B) Mantıksal Erişim Riskleri

Risk analizine ve yetki-sorumluluk esasına dayalı olarak bir kaynak sınıflandırması yapılmamış olması, mantıksal erişim risklerine ilişkin olarak kurulması gereken kontrollerin yeterli bir şekilde belirlenememesi riskini doğurmaktadır. Bunun bir sonucu olarak, önemli olan ve risk altında bulunan bir kaynağın korunması için gerekli mantıksal erişim kontrolleri uygulanmazken, önem derecesi ve riski daha düşük bir kaynak için daha yüksek mantıksal erişim kontrolleri uygulanabilir. Yetki ve sorumluluk taşımayan bir kişi bilgiye ulaşabilir ve sistemde herhangi bir işlem gerçekleştirebilir[28].

Kurumdan veya görev yaptığı birimden ayrılan veya görevine son verilen personelin sisteme erişim yetkilerinin bir süre için sistemde ve programlarda aktif durumda kalabilmesi sisteme yetkisiz erişim yapılması riskini artırmaktadır. Personel yer değişikliklerinin takibindeki gecikme, kullanıcıların sisteme erişim yetkilerinin görev ve sorumlulukları ile uyumlu olmamasına neden olabilmektedir.

İşletim sisteminde, ağ altyapısında ve yazılımlarda değişiklikler, sistemin güvenliğini sağlamak amacıyla önceden tasarlanmış olan mantıksal erişim kontrollerinin yetersiz hale gelmesine yol açabilir. Bilgi sistemine yapılan saldırıların yönetime düzenli olarak raporlanmaması halinde kurum yönetimi bu saldırılardan haberdar olamadığından, risk değerlendirme çalışmaları yapılırken veya yeni yatırımlara karar verilirken bu tehditler göz önünde bulundurulamayabilir[29].

Bilgisayar sistemlerine uzaktan erişim gerektiren iş amaçları belirlenmediğinde sistem güvenliğine veya işlem güvenilirliğine zarar verilebilmesi mümkün olabilir. Bunun gibi, bilgi işlem ekipmanı imha edildiğinde veya başka bir yere gönderildiğinde belleğindeki bilgiler uygun yöntemlerle temizlenmezse kurum için kritik bilgiler kurum dışına çıkabilir veya yetkisiz kişilerin eline geçebilir.

Kullanıcılar ve sistem yöneticileri, sistem tarafından şifrelerini önceden belirlenen sürelerin sonunda değiştirmeye zorlanmaması şifre güvenliğini zayıflatmaktadır. Aynı şekilde belirli bir süre bilgisayarını kullanmayan ve masasından ayrılan personelin bilgi-

28 SOĞUKPINAR, İ: Veri ve Ağ Güvenliği Ders Notları, s.46; Sayıştay Denetim Raporu, s.35-36.

29 Sayıştay Denetim Raporu, s.46.

sayarlarının korunmaması durumunda, yetkisi olmayan kişilerin bu bilgisayarları kullanarak sisteme erişmeleri ve işlem yapmaları riski doğmaktadır.

Kullanıcıların aynı anda birden çok bilgisayardan sisteme bağlanabilmesi, gerçek bir kullanıcının sisteme bağlı olduğu bir anda yetkisiz bir kullanıcının da aynı kullanıcı adı ve şifresi ile sisteme erişmesi riskini doğurmakta ve denetim izi gibi önemli kontroller üzerindeki güvenilirliği de azaltmaktadır. Bunun gibi, aynı kullanıcının birden fazla bilgisayarda çalışmasının gerekli olduğu durumlarda da bir bilgisayarda sisteme eriştikten sonra oturumu kapatmadan başka bir bilgisayarda çalışmaları olanaklı olduğu için, yetkisiz kişilerin ilk bilgisayarda açık bırakılan oturumu kullanarak sisteme erişmeleri mümkün hale gelebilmektedir.

C) Mantıksal Erişim Kontrol Önlemleri

1) Bilgi sistemi ortamında oluşturulan tüm kaynaklar için yetki ve sorumluluk esasına dayalı olarak bir risk değerlendirmesi gerçekleştirilmeli ve kurum kaynakları sınıflandırmalıdır. Yapılan kaynak sınıflandırması, mantıksal erişim kontrollerinin belirlenmesi seviyesinde ana kriterlerden biri olarak kullanılmalıdır[30]. Bu kaynak sınıflandırması göz önünde bulundurularak veriye erişim uygun bir şekilde kısıtlanmalıdır. Ayrıca kaynak sınıflandırması ile yetki ve sorumluluk çerçevesi düzenli aralıklarla gözden geçirilmeli ve değişen koşullara göre güncellenmelidir.

2) Bilgi sistemleri sadece bilgi işlem birimi süreçlerini değil, tüm kurumsal süreçleri bünyesinde barındırmaktadır. Bunun sonucu olarak uluslararası uygulamalara uygun olarak bilgi sistemlerinin sistem sorumluluğu üst yönetici tarafından görevlendirilen kişilere verilmelidir.

3) Kullanıcıların yetkilerini gösteren listeler güncel şekilde tutulmalıdır. Görev yeri değişen veya işten ayrılan personelin sisteme erişim yetkilerinin derhal kaldırılması konusunda alınan kontrol tedbirinin uygulanabilirliğini sağlayacak önlemler alınmalıdır[31].

4) İşletim sisteminde, ağ altyapısında ve yazılımlarda değişikliklerin mevcut sistemler üzerinde mantıksal erişim kontrolleri açısından ne gibi değişikliklere neden olacağı analiz edilmelidir. Bu kapsamda, uygulama ortamına aktarılmadan mantıksal erişim kontrollerini zayıflatacak hususlarla ilgili risk analizi yapılmalı ve bu analiz sonuçlarına göre gerekli önlemler alındıktan sonra değişiklikler uygulamaya sokulmalıdır[32].

5) Bilgi işlem ekipmanının imha edilmesine veya başka bir yere gönderilmesine karar verildiğinde, belleğindeki bilginin formatlanarak bilginin temizlendiğinden emin olunmalıdır[33]. Bilgi işlem ekipmanının imhası veya elden çıkarılması ile ilgili olarak yazılı bir prosedür hazırlanmalıdır.

6) Sisteme yapılan saldırıların yönetime düzenli olarak raporlanması sağlanmalı ve bu husus yazılı bir prosedüre bağlanmalıdır[34].

7) Bilgisayar sistemlerine uzaktan erişim uygun bir şekilde kısıtlanmış olmalıdır. Bu bağlantılar, sadece yazılı olarak belirlenen geçerli iş amaçları için kullanılmalı ve bu iş amaçları yapılan işlemin mahiyetini, geçerliliğini ve güvenilirliğini etkilememelidir.

Uzaktan erişim için geçerli iş amaçları yazılı olarak belirlenmelidir[35]. İş amaçları dışında erişimin engellenmesi ve bu bağlantıların sistem güvenliğine zarar vermemesi amacıyla kontroller oluşturulmalıdır.

8) Belirli bir süre kullanılmayan bilgisayarlarda oturumun otomatik olarak kapanması veya şifre ile korunan ekran koruyucuların devreye girmesi sağlanmalıdır[36]. Bu kontrollerin ne kadar sürede devreye gireceği kullanıcı profilinin bir değerlendirmesi yapılarak belirlenebilir.

9) Kullanıcıların sisteme, aynı anda, aynı kullanıcı adı ve şifresiyle değişik bilgisayarlardan bağlanmasını önleyecek kontroller uygulamaya konulmalıdır[37].

30 Sayıştay Denetim Raporu, s.36.

31 KUMAŞ, Erhan: e-Devlet Kapısı ve Risk Değerlendirme Metodolojisi, s.4; Sayıştay Denetim Raporu, s.40-41

32 Sayıştay Denetim Raporu, s.44.

33 Sayıştay Denetim Raporu, s.35-36.

34 Sayıştay Denetim Raporu, s.46.

35 Sayıştay Denetim Raporu, s.35-36.

36 Sayıştay Denetim Raporu, s.42.

37 Sayıştay Denetim Raporu, s.42.

Eğer kullanıcıların ihtiyaç gereği bilgisayarda birden çok oturum açmaları gerekiyorsa, bu işlemi hangi bilgisayarlarda gerçekleştirebilecekleri belirlenebilir ve yalnızca bu terminali kullanarak oturum açmaları veya roaming profile (gezici profil: aynı kullanıcının değişik yerlerde ve bilgisayarlarda çalışmasına ihtiyaç olduğunda bu profil kullanılarak kullanıcı adı güvenlik altına alınmaktadır) kullanmaları sağlanabilir[38].

10) Kullanıcılar ve sistem yöneticileri, sistem tarafından, şifrelerini önceden belirlenen sürelerin sonunda değiştirmeye zorlanmalıdır. Sistem, kullanıcıların ve sistem yöneticilerinin kullandıkları belirli sayıda şifreyi (örneğin son on şifreyi) geriye dönük olarak hafızasında tutmalı ve yeni şifre olarak bunların kullanılmasına izin vermemelidir[39].

11) Kullanıcıların ve sistem yöneticilerinin, zorunlu şifre değişikliklerinde (maksimum şifre ömrü parametresi oluşturulduğunda), şifrelerini ardı ardına değiştirip (örneğin on kez değiştirip) tekrar aynı şifreyi kullanmalarını engellemek amacıyla şifreler için minimum şifre ömrü de tanımlanmalıdır[40].

IV) FİZİKSEL ERİŞİM RİSKLERİ

A. Fiziksel Erişim Kontrolleri

Bilgi işlem biriminin bulunduğu alan kurumun çok kritik işlevlerini yerine getirmesi açısından önem taşımaktadır. Bu nedenle fiziksel erişim kontrollerinin uygulanması zorunluluğu olmalıdır.

Fiziksel erişim kontrollerinin amacı, bilgi sistemini oluşturan temel unsurlardan biri olan bilgisayar donanımına yetkisiz kişilerin fiziki olarak ulaşmasını engelleyici mekanizmaların kurulmasını sağlamaktır. Ayrıca bu kontroller ile bilişim sisteminin yangın, su baskını, nem, elektrik kesintisi gibi çevreden gelecek risklere karşı korunması da amaçlanır[41].

38 Sayıştay Denetim Raporu, s.42.

39 Sayıştay Denetim Raporu, s.39-40.

40 Sayıştay Denetim Raporu, s.40.

41 Türkiye Bilişim Derneği: Bilişim Teknolojilerinde Risk Yönetimi, s.5-7.

Fiziksel erişim kontrolleri, bilgi sistemlerinin ve kullanıcıların bulunduğu binalara ve odalara fiziki olarak ulaşılmasını kontrol altında tutmaya yönelik olarak uygulanan kontrollerdir. Bu kontroller bilgi işlem merkezinde bulunan ve kuruma ait tüm bilgi işlem operasyonlarının yürütüldüğü, bilgilerin saklandığı ana bilgisayarlara (server) ulaşılmasını da kontrol altında tutmaya yöneliktir[42].

"Fiziksel erişim kontrolleri, bilgi sistemlerinin ve kullanıcıların bulunduğu binalara ve odalara fiziki olarak ulaşılmasını kontrol altında tutmaya yönelik olarak uygulanan kontrollerdir"

B) Fiziksel Erişim Riskleri

Bilgi işlem biriminin ve sistem odasının bulunduğu alana güvenlik kameraları ve manyetik kartla açılan kayar kapı konulmaması veya kullanılan kapının dayanıksız olması ve bir manyetik geçiş kartı kullanımıyla bu kapıdan birden fazla kişinin geçmesinin mümkün olması fiziksel güvenliği olumsuz etkileyen unsurlardır.

Bilgi işlem birimi ziyaretçileri için bu alanın dışında ayrı bir görüşme odası bulunmaması, refakatçi kullanılmaması veya randevu alma mekanizmasının uygulanmaması bir risk olarak tanımlanmalıdır. Bunun gibi sistem odasının ne şekilde korunacağına ilişkin yönetsel onay içeren prosedürlerin bulunmaması da fiziksel güvenliği olumsuz etkileyebilmektedir.

Deprem ve sel gibi gerçekleşmesi muhtemel doğa olayları ile yangın ve boru patlaması gibi çevreden ve insandan kaynaklanan olaylar da bilgi işlem birimi ve sistem odasının fiziksel ve çevresel güvenliğini yönünden değerlendirilmesi gereken bir risk faktörüdür[43].

C) Fiziksel Erişim Kontrol Önlemleri

1) Bilgi işlem biriminin bulunduğu bina ve mekânların giriş ve çıkışlarında kullanılan sistem gerekli güvenlik

42 Sayıştay Denetim Raporu, s.47-48.

43 Türkiye Bilişim Derneği: Bilişim Teknolojilerinde Risk Yönetimi, s.5-7.

riskleri göz önünde bulundurularak gözden geçirilmelidir. Örneğin manyetik kartla geçilmesi uygulaması varsa bu kartlara anti pass-back özelliği verilmesi sağlanarak çıkış yapılmadan tekrar giriş yapılmasına izin verilmemelidir. Manyetik kartla açılan kayar kapı aynı anda birden çok kişinin geçmesine elverişli olmamalıdır[44].

2) Sistem odası yangın çıkış ve donanım tahliye kapıları olmalı ve bu kapılar fiziksel güvenliği sağlayacak ve içeriden açılacak nitelikte olmalıdır. Bu kapının içine ve dışına kameralar konulmalı ve kameralar kapıyı görecek şekilde konumlandırılmalıdır.

3) Güvenlik gereken tüm bölgelerde kapılar kilitli tutulmalıdır. Güvenlik görevlilerinin iş tanımlarında, kilitli olması gereken kapıların uygun aralıklarla güvenlik birimince kontrol edilmesine yönelik ifadeler yer almalıdır.

4) Bilgi işlem birimi ziyaretçileri için bu alanın dışında ayrı bir görüşme odası oluşturulmalıdır. Bilgi işlem birimine ziyaretçi alınması için farklı bir prosedür izlenmelidir. Refakatçi kullanımı veya randevu alma mekanizması düzenli bir şekilde uygulanmalıdır.

5) Bilgi işlem birimi ve sistem odasındaki kontrol prosedürleri ile donanımların korunmasına ve bakımına uygulanacak prosedürler yazılı olarak belirlenmeli ve onaylanmalıdır. Ayrıca merkez ve taşra birimlerinde bilgisayar donanımlarının korunmasına ilişkin bir kontrol prosedürü oluşturulmalı ve ilgili birimlere bildirilmelidir.

6) Bilgi sistemlerine yönelik olarak hassas ve korunması gereken varlıklar ve bu varlıklara yönelik fiziksel erişim tehditleri[45] (sel baskınları, deprem gibi doğadan kaynaklanan tehditler; yangın çıkması, binaya ait borulardan birinin patlaması gibi çevreden kaynaklanan tehditler; kötü niyetli, yetkin olmayan veya eğitimsiz kişiler gibi insandan kaynaklanan tehditler) risk yönetimi metodolojisine uygun olarak belirlenmeli ve önemlerine göre sınıflandırılmalıdır. Kurulmuş olan fiziki erişim kontrolleri, risk değerlendirmesi sonucu belirlenecek tehditler göz önünde tutulmak suretiyle gözden geçirilmeli ve sürekli iyileştirilmelidir.

V) SONUÇ

Bilgi sistemleri, kamu idarelerinin gelecekteki hedeflerini elde etmede kullanacakları en önemli araçlardan biridir. Bilgi sistemlerine ilişkin risklerin kontrolündeki eksiklik, sistemi korunmasız bırakabilir, kritik kurumsal fonksiyonların yerine getirilmesini engelleyebilir ve telafisi mümkün olmayan kayıplara yol açabilir.

"Bilgi sistemlerine ilişkin risklerin kontrolündeki eksiklik, sistemi korunmasız bırakabilir, kritik kurumsal fonksiyonların yerine getirilmesini engelleyebilir ve telafisi mümkün olmayan kayıplara yol açabilir"

Bir zincirin gücü, onu oluşturan halkalardan en zayıfının gücü kadardır. Kullanılmakta olan bir zincir, en zayıf halkasından kopar ve fonksiyonunu yerine getiremez hâle gelir. Bu nedenle bilgi sistemleri sıkı bir şekilde kontrol edilmeli ve bilgi sistemi birimi önceden tanımlı ve kontrol altında tutulan süreçlerle yönetilmelidir. Bilgi sistemleri kişilerin kafasında kalan, sistematik şekilde yapılanmayan ve kurumsallaşmayan unsurlar içermemelidir.

Kamu idarelerinde bilgi sistemi güvenlik risklerinin yönetimi konusu, üzerinde ciddi olarak durulması ve geliştirilmesi gereken bir alan olarak kabul edilmektedir. Bu alanda kontroller, gerekli süreçlerin kurulup kurulmadığını, kurulan süreçlere ne kadar uyulduğunu, verimlilik, gizlilik, doğruluk, bütünlük, süreklilik, uyum ve güvenilirlik konularını ve bunların bilgi sistemi kaynakları üzerindeki etkilerini inceleyecek şekilde tasarlanmalıdır. Bu yapılırken dünya genelinde kullanılan ve ortak lisan olarak kabul gören uluslararası standartlardan, metotlardan, modellerden ve çerçevelerden yararlanılmalıdır.

44 Sayıştay Denetim Raporu, s.50.

45 Türkiye Bilişim Derneği: Bilişim Teknolojilerinde Risk Yönetimi, s.5-7.

KAYNAKLAR

1. AKIN, H.Bahadır: Bilişim Teknolojileri Evrimi ve Bilişim Teknolojilerinin Çağdaş İşletmelerde Stratejik Yönetim Üzerindeki Etkileri.
2. ATAN, Murat: Risk Yönetimi ve Türk Bankacılık Sektöründe Bir Uygulama, Doktora Tezi, Ankara 2002.
3. BGYS Risk Yönetimi Süreci Kılavuzu, TUBİTAK, Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, 2007.
4. Bilgi Güvenliği Politikası Oluşturma Kılavuzu, TUBİTAK, Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, Mart 2008.
5. CEVHER, Ezgi: Bilişim Teknolojileriyle Yaratılan Yeni Bir Yaklaşım: Yönetişim, Gazi Üniversitesi, MBA, 2003.
6. ÇALIKUŞU, Faruk / KARAMEHMET, Bilge / DENİZCİ, Ömer Mert: Bilgi Güvenliği Yönetim Sistemi Kapsamında Risk Yönetim Modeli. (senkronbilisim.net/BGYS.pdf)
7. ÇAYIR, Sinan / GÜNEŞ, Asım / BÜK, Ozan: Türkiye'deki Kamu Kurumlarında Bilişim Teknolojileri Yönetimi, Akademik Bilişim, Ocak-Şubat 2008, s. 541-544.
8. DERİCİ, Onur, TÜYSÜZ, Zekeriya, SARI Aydın: Kurumsal Risk Yönetimi ve Sayıştay Uygulaması, Sayıştay Dergisi, S. 65, s. 151-172.
9. Devlet Planlama Teşkilatı, 8. Beş Yıllık Kalkınma Planı, Bilişim Teknolojileri ve Politikaları Özel İhtisas Komisyonu Raporu, Ankara 2001.
10. Devlet Planlama Teşkilatı, Bilgi Toplumu Stratejisi (2006-2010).
11. Devlet Planlama Teşkilatı, Bilgi Toplumu Stratejisi Eylem Planı (2006-2010).
12. Devlet Planlama Teşkilatı, e-Dönüşüm Türkiye Projesi, Birlikte Çalışabilirlik Esasları Rehberi.
13. Devlet Planlama Teşkilatı, Kamu Bilgi ve İletişim Teknolojisi Projeleri Hazırlama Kılavuzu, Temmuz 2009.
14. KUMAŞ, Erhan: Kurumlarüstü Bilgi Güvenliği Stratejisi.
15. KUMAŞ, Erhan: e-Devlet Kapısı ve Risk Değerlendirme Metodolojisi.
16. OECD Bilgi Sistemlerinin Güvenliğine İlişkin Rehber İlkeleri, [C (2002/131 FINAL]
17. ÖZBİLGİN, İzzet Gökhan: Bilgi Teknolojileri Denetimi ve Uluslararası Standartlar, Sayıştay Dergisi, S.49, s. 123-128.
18. SOĞUKPINAR, İ: Veri ve Ağ Güvenliği Ders Notları.
19. Sayıştay Başkanlığı: Hazine Bilişim Sistemleri Denetimi Raporu, Ekim 2003.
20. TBB Çalışma Grubu,: Risk Yönetimi Prensipleri, Bankacılar Dergisi, 2006, S. 57, s.15-32.
21. TEKTAŞ, Halil: Kamu İdarelerinde Kurumsal Risk Yönetim Sistemi, Mali Hukuk, sayı:138, Kasım-Aralık 2008, s. 26-41.
22. Türkiye Bilişim Derneği: Bilişim Teknolojilerinde Risk Yönetimi, 2. Çalışma Grubu Raporu, Mart 2006.
23. Türkiye Bilişim Derneği: Bilgi Teknolojilerinde Yönetişim, 1. Çalışma Grubu Raporu, Nisan 2008.
24. Türkiye Bilişim Derneği: Kuruluşlarda Bilgi Güvenliği Yönetim Sistemi Uygulamasında ISO/IEC 27001:2005, 1. Çalışma Grubu Raporu, Nisan 2008.
25. UZUNAY, Vildan: COBİT (Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri - Control Objectives for Information and Related Technology), (www.bumko.gov.tr/KONTROL/Genel/dg.ashx?...DIL=1...COBIT...)
26. Veri Yedekleme Kılavuzu, TUBİTAK, Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, Ocak 2008.
27. VURAL, Yılmaz / SAĞIROĞLU, Şeref: Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme, G.Ü.,Müh., Mim.Fak.Der., 2008, C. 23, s. 507-522