SİSTEM DENETİMİNDE İÇ DENETİMİN ROLÜ VE BİLGİ GÜVENLİĞİ

O. Selçuk YILMAZ
İç Denetçi,
İzmir Büyükşehir Belediyesi
İZSU Genel Müdürlüğü

ÖZET: *Bilişim teknolojilerine yönelik yasal alt yapının sürekli olarak geliştirilmekte olması, kurumların bu teknolojilere yaptıkları yatırımların boyutlarının giderek büyümesi ve nihayet kurumların iş ve işlemlerini yürütürken artık bilişim teknolojilerine bağımlı hale gelmesi, kamu kaynaklarının yürürlükteki mevzuata uygun olarak tutumlu, verimli ve etkin şekilde kullanılıp kullanılmadıklarını denetleme ihtiyacını beraberinde getirmektedir. Bilgi işlem donanım ve yazılım uygulamaları gelişen bilişim teknolojisine paralel olarak kamu kurum ve kuruluşlarında giderek yerleşik düzen kazanmaya başlamıştır. Bu uygulamaların işlevsel ve fonksiyonel işleyişiyle ilgili risk teşkil eden girdi, bilgi işleme, çıktı ve sistem kontrollerinin gerçekleştirilmesinde iç denetimin hangi yöntemler kullanılarak, nasıl yerine getirileceği önemlidir. Outsourcing - Dış Kaynak Kullanımı yoluyla bilgisayar teknolojileri satın alınması durumunda da iç denetim yaklaşımının nasıl ve ne yönde gerçekleşeceği üzerinde durulması gereken diğer önemli bir husustur. Kurumsal hizmet anlayışının yerine getirilmesi ve bilgi varlığı güvenliğinin sağlanmasında; bilgi-yazılım ve donanım varlıklarının güvenliğine yönelik bilgi güvenliğinin temel bileşenleri "Gizlilik", "Bütünlük" ve "Kullanılabilirlik" kriterlerine uygun olarak hareket edilmesi gerekmektedir. Bütün bu hususlardan yola çıkarak denetimde nelere dikkat edileceği bu makale içeriğinde kapsamlı olarak inceleme ve değerlendirmeye tabi tutulmuştur.*

ANAHTAR KELİMELER: *Bilgi Varlıkları, Bilgi Güvenliği, Şifre ve Ağ Güvenliği, Yetkilendirilmiş Erişim, İç Denetim,*

Giriş:

Kamu kurumlarının gereksinim duydukları bilgisayar teknolojileri uygulamaları hizmet konularına göre farklı yapılarda ortaya çıkmaktadır. Bilgi işlem hizmet ve faaliyetlerinin genel olarak finansman ve muhasebe ile ilgili yanının bulunmasının ötesinde, başta yerel yönetim kademelerinde; su ve kanalizasyon idareleri, belediyeler ve ilgili diğer idarelerde; ulaşım, tüketim

ve kullanıma yönelik kullanıcı/yolcu/abonelerle ilgili kendine öz yazılım uygulamalarını kendi içerisinde barındırarak; görev, yetki, sorumluluk ve ürettiği hizmetin yapı ve özelliğiyle ilintili farklı işleyiş gösteren bilgi işlem yapılanması içerisinde olduğu görülmektedir. Her ne kadar kurumlar arasında hizmet, iş ve işleyişte yapısal farklılıklar bulunsa da genel olarak uygulamada bilgi işlem hizmet ve faaliyetlerinin güvenliği, etkin bir iç denetim için öncelikli olarak ele alınması gereken önemli bir konudur.

Kamu kuruluşlarının bilgi varlıklarının tehlike analizleri yapılarak, teknik, idari ve fiziksel açıklarının tespit edilmesiyle çok yönlü risk analizi çalışmaları gerçekleştirilerek bilgi varlıklarının envanteri ortaya çıkacak ve bilgi varlıklarının iş hedeflerine göre güvenlik derecelendirilmeleri yapılabilecektir. Sonuçta bundan kurum üst düzeyde fayda sağlayacaktır.

1- BİLGİ GÜVENLİĞİNİN TEMEL BİLEŞENLERİ VE VARLIK ENVANTERİ OLUŞTURMANIN ÖNEMİ[1]

Bilgi güvenliğinin temel bileşenleri "Gizlilik", "Bütünlük" ve "Kullanılabilirlik" kriterleridir. Bu kriterlere uygun doğrultuda bilgi varlığı ve güvenliği kavramları ile bilgi güvenliğinin nasıl test olunacağı ve iç denetimde riski yüksek görülen alanlarda, nasıl sorgulanacağı üzerinde durulması gereken önemli hususlardır. Bu süreçte varlık envanteri oluşturulması ve veri tabanı güvenliğiyle ilgili önemli hususlar da analize tabi tutulmuştur.

1.1 Bilgi Varlıkları;

Genel olarak bakıldığında; uygulamada verinin ancak yorumlandığı ve analize tabi tutulduğunda bilgiye dönüştüğü bilinmektedir. Bilgi kurum için önemli bir değer ifade eden soyut bir varlık olarak görülmelidir. Bilgiyi somutlaştıran temel ögeler; bilginin sahibi, tutulduğu ortam, bu ortamın fiziksel özellikleri, muhafaza edildiği teknik ortam ve bilginin çıktısı olarak değerlendirilebilir.

Bilgi diğer kurum varlıkları gibi korunması gereken bir varlık olarak ele alınmalıdır. Şöyle bir bakıldığında; bilgi bazen basılı bir doküman, bazen çalışan personelin zihninde yer eden, iletişimde, sürekli vurguladığı bir husus değil midir? Buradan yola çıkıldığında; bilgi kendisine ulaşabilen tarafından kullanılan, depolanan, değiştirilen, iletilen ve silinebilen yani bir bakıma günümüz teknolojisinde üzerinde çalışılabilen bir varlık olarak görülebilmelidir.

1.2. Bilgi Güvenliği;

Güvenlik açıklıklarının son yıllarda hızla artması, kurumların karşı önlem almasına ve yeni bilgi sistemi pozisyonları oluşturmalarına yol açmıştır. Kurumun güvenlikte daha kararlı bir noktaya ulaşabilmesi için sağlıklı bir "Bilgi Güvenliği Yönetim Sistemi"(BGYS) kurulması ve denetim altına alınması gerekmektedir. Bilgi işlem faaliyetlerinin kurumda devamlılığının sağlanabilmesinde olası risk ve zararların asgari düzeye çekilebilmesi, hizmette kalite, verimlilik ve etkililik işleyişini olumsuz etkileyebilecek geniş bir tehdit kümesi ve yelpazesine karşı idare için gizlilik teşkil eden bilginin her bakımdan korunabilmesine bilgi güvenliği denilmektedir.

Bilgi sistemlerinin giderek kurumlarda yaygınlaşmaya başlamasıyla ortaya çıkan, merkezi depolama, bilgiye ulaşabilme olanaklarının yaygınlaşması, işleme, izinsiz erişimler, bilinçli veya bilinçsiz hataların önemli sonuçlar doğurması, bilginin yetkisiz imhası, yetkisiz değiştirilmesi ve görülmesi olasılıklarının artması sorunları nedeniyle bilgi güvenliği kavramı gündeme gelmiştir. Kullanıcı sayısı ve bilgi teknolojisi ürünleri üretimi artışı, sistemlerin sürekli geliştirilip değiştirilmesi beraberinde güvenlik açıklarını ortaya çıkarmaktadır.

"Bilgi güvenliği bilgi işlem sistemleri hakkında yapılan her türlü denetimde ve özellikle iç denetimde risk teşkil eden bir süreç olarak sorgulanması gereken önemli bir alandır"

Bilgi güvenliği bilgi işlem sistemleri hakkında yapılan her türlü denetimde ve özellikle iç denetimde risk teşkil eden bir süreç olarak sorgulanması gereken önemli bir alandır.

1 Enocta Eğitim Platformu-Eğitim ders Notları

Bilgi güvenliğinin baş sorumlusu o kurumun üst düzey yöneticileri ile bilginin sahibi konumunda bulunan, bilgi sistemini kullanan ve bilgi sistemini yönetenlerdir.

Bilgi güvenliğinin en temel mekanizmaları; kullanılabilirlik ve bilgi güvenliği dengesi, bilgiyi iş sürecinde kullanan ve bilgi işleyen sistemleri yöneten kişilerin sorumluluğunda bulunan risk seviyesinin belirlenmesi, kurum birimlerinin bilgi güvenliğine sağlayacağı katkı ve üst yönetimin bilgi güvenliğini takip etmesi, yönlendirmesi ve faaliyetleri onaylamasıdır.

Bilgi Güvenliğinin temel bileşenleri "gizlilik", "bütünlük" ve "kullanılabilirlik" tir.

1.3 Bilgi Güvenliğinin Test Olunması;

Bilgi güvenliği denetimlerinde denetçiler çalışmalarında internet ortamında ya da literatürde var olan kontrol listelerini kullanmayı tercih etmektedirler. Fakat bu yönelim, yapılan testler hakkında bazı soru işaretlerinin oluşmasına sebep olmaktadır. Bunlar;

- Denetimlerde kullanılan kontrol listeleri yeterince detaylı mıdır? Farklı kontrol listeleri ile karşılaştırılarak sağlaması gerçekleştirilmiş midir?
- Kullanılan hazır kontrol listelerinde geçen maddeler net olarak anlaşılmış mıdır? Denetleme sonucunda oluşturulacak tavsiyelerin güvenliğe, performansa ve verilen servise olan etkileri net olarak bilinmekte midir?
- Kontrol listesi var olmayan BT varlıklarının denetimi ne şekilde gerçekleşmektedir?

1.4 Güvenlik Test Aşamalarında İç Denetçinin Sorgulaması Gereken Hususlar([2]);

Bilgi güvenliğinin test aşamaları aşağıda riski yüksek görülen alt süreçlerde ayrı ayrı analize tabi tutularak değerlendirilmiş ve denetimde nelere dikkat edilmesi gerektiği sorgulanmıştır.

1.4.1. Ağ Topolojisindeki Konum;

Topolojik konum ve erişim kontrolünde şu genel kurallar uygulanmalıdır;

1. Web, e-posta sunucu gibi kurumun verdiği servisler internet ve kurum ağından korunan "Yarı Güvenli Bölgede" yer almalıdır. Erişim sadece ilgili porta açılmalıdır.
2. Veritabanı gibi hassas veri taşıyan (BT) varlıklarına direk erişim engellenmelidir. Dolaylı erişim, salt uygulamaların koştuğu web platformları üzerinden sağlanmalıdır.
3. Yönetim merkezleri gibi bağlanılmaya ihtiyacı olmayan fakat diğer sunuculara bağlanma ihtiyacı olan varlıklara erişimler tümüyle kapatılmalıdır.
4. Kurum ağında ki bilgisayarlara ve sunuculara diğer ağlardan erişim engellenmelidir.
5. Kuruma ait sunuculardan hiçbirisi güvenlik duvarının önünde yer almamalıdır.

1.4.2. Güvensiz Kurulum Yöntemleri; Denetçi testini gerekleştirdiği varlıkta bu yazılımların kurulum yöntemini incelemeli, kullanım şartlarına uygun en güvenli kurulum moduna geçiş için önerilerde bulunmalıdır.

1.4.3. Varlık Yapılandırması; Bilgi teknolojileri varlıkları için özel çalışma gerektiren test adımları bu başlık altında yer alır. Internet ortamında ki varlık ve literatürdeki kabul görmüş kaynaklarla test yapılabilir.

1.4.4. İş Sürekliği ve Yedekleme Konuları; Saldırıya uğramış bir sistem için yapılması gereken en önemli şey sistemin tekrar çalıştırılmasıdır. Bu noktada alınan yedeklerin ve iş sürekliliği planının önemi ortaya çıkmaktadır. Yeterli bir iş sürekliliği planı olmayan kurumlar, saldırı karşısında oluşacak maddi zararın ve itibar kaybının artmasına engel olamazlar.

Denetçi, testi gerçekleştirilen "Bilgi Teknolojisi" (BT) varlığının yedeklenmesi konusunda: Yedekleme politikası var mı? Ya da politikaya uyuluyor mu? Düzenli aralıklarla geri dönüm (recovery) tatbikatları gerçekleştiriliyor mu? Yedek veriler doğru belirlenmiş mi ve sistemin geri döndürülebilmesi için yeterli mi? Yedek alma sıklığı ile verinin yedeklerden döndürülme süresi kabul edilebilir mi? Sorularını kendine sormalıdır.

1.4.5. Servisi Çalıştıran Kullanıcı; Yetkisiz komut çalıştırma ile sonuçlanabilecek saldırılar ilgili servisi çalıştıran kullanıcının yetkileri seviyesinde erişim hakkı kazanır. Bu sebeple servisler, sistem yöneticisi yetkilerine sahip (Microsoft tabanlı işletim sistem-

2 Tahsin Türköz, TÜBİTAK-UEKAE , BT Varlıklarının Güvenlik Testi Adımları…

lerinde *administrator, system*; Unix tabanlı işletim sistemlerinde *root, toor* vs.) kullanıcılar adına çalıştırılmamalı, bunun için yetkisi düşük yeni kullanıcılar oluşturulmalıdır. Sunucu üzerinde birden fazla servis çalışıyor ise her servis için farklı kullanıcı hesabı tercih edilmelidir.

1.4.6. Kullanıcı Hesapları ve Hakları; Kurulumla gelen varsayılan kullanıcı hesapları ve şifrelere dikkat edilmelidir. Uzun süre kullanılmayan hesaplar, kurumdan ayrılan personelin hesapları, gereğinden fazla yetki verilen hesaplar değerlendirilmesi gereken başlıklardır.

Kullanıcılara şifre politikası belirlenmeli ve bu politikaya uyma zorunluluğu getirilmeli, şifre politikalarının yeterliliği irdelenmelidir.

Sistemlere giriş sırasında kullanıcı bilgileri ve şifreler hakkında sunulan bilgiler de incelenmesi gereken bir diğer alt başlıktır. Örnek denetleme adımları şu şekilde belirlenebilir:

1*Son giriş yapan kullanıcının veya tüm kullanıcıların listesinin giriş ekranında bulunmaması.

2*Şifre hatası mesajının kullanıcı ismini varlığını bildirir içerikte olmaması.

1.4.7 Varlık Kayıt Tutma Yapılandırması; Kayıtla ilgili diğer konu, kayıt tutma hacminin ihtiyaçları karşılamasıdır. Mevzuata ya da kurum politikalarına göre belirlenen sürede kayıtlar tutulmalıdır. 5651 Sayılı Yasa erişim sağlayıcıların 6 ay - 2 yıl arası erişim kayıtlarını güvenli şekilde saklamasını şart koşmaktadır. [3]

1.4.8 Sürüm Bilgilerinin İfşası; Saldırganların bildiği açıklıklar ile erişilebilen servisleri ilişkilendirebilmeleri için kullandıkları en etkin yol, hedef sistemin parmak izini çıkarmaktır. Parmak izi genellikle sistemlerin karakteristik yapılarının incelenmesiyle ortaya çıkarılır. Üretilen hatalar, karşılama mesajları, ağ trafiğindeki ipuçları bu karakteristiğe örnektir.

1.5 Varlık Envanteri Oluşturulmasının Önemi Ve Metodolojisi;

Bilgi Varlığının korunması için bilgi varlıklarının envanterinin oluşturulmasının yanı sıra güvenlik kriterleri olarak belirtilen gizlilik, bütünlük ve kullanılabilirlik değerlerinin tespit olunması gerekmektedir. Bilgi varlıklarının eksik tespiti halinde; bu değerlerin eksik ya da yanlış tespit edilmesi söz konusu olacaktır ki, böyle bir durumda başta risk analizi olmak üzere, uygulamada ve denetimin her aşamasında hatalara sebep olunacaktır. Bilgi varlıklarının tehlike risk analizlerinin yapılarak, teknik, idari ve fiziksel açıklarının tespit olunması gerek iç kontrol eylem planının kurumsal düzeyde uygulanabilirlik kazanması ve gerekse iç kontrolün bağımsız değişkeni iç denetimin etkin olabilmesi bakımından önem arz etmektedir.[4]

Varlık envanteri oluşturma kriterleri metodolojisine uygun bir sırada aşağıdadır.

- Önce varlık isimleri tespit olunmalıdır. Burada donanım varlıkları en somut varlıklar oldukları için tespiti en kolay olan varlıklardır. Dolayısıyla idarelerde kullanılan bilgisayarlar ve bağlı aygıtların (Yazıcı vs) donanım olarak taşınır kayıt sistemi içerisindeki yeri, sayısı, konumu ve fiziki olarak yeterliliği sorgulanmalıdır.
- Donanım varlıklarının bulunduğu liste sorgulanarak üzerlerindeki yazılım varlıkları tespit olunmalıdır. Bu tespitle; her bir yazılımın üzerinde kurulu olduğu donanım varlığı ile ilişkilendirilmesi liste ve kayıt düzeyinde yapılarak, çapraz kontrollerle test olunmalıdır.
- Sadece yazılımların işlediği bilgilerin dışında olabilecek diğer bilgi varlıkları da bu aşamada dikkate alınmalı, yazılı dokümanlarda bilgi varlığı olarak değerlendirilmelidir. Bu tür bilgi varlıklarının nerede saklandığı da yukarıdaki listede belirtilmelidir.
- Her bir varlığı daha somut olarak belirleyebilmek için seri no, sahibi, lisans bilgisi, kod no, vs gibi nitelendirici bilgiler kullanılarak varlık envanteri oluşturulmalıdır.

3 5651 Sayılı Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

4 Bülent GÜNGÖR, Bank Asya Yazılım Geliştirme Müdürü, Bilgi Güvenliği Danışmanlık Hizmetleri; http://www.innova.com.tr/solution-detail/Bilgi-Guvenligi-Danismanlik-Hizmetleri/

1.6 Veri Tabanı Kontrolü ve Şifre Güvenliğinin Sağlanması Hakkında;

Bir veri tabanı içerisindeki saklanan bilgilerin değeri ne kadar önemliyse veri tabanının güvenliği ve kontrolünün sağlanması da bir o kadar önemlidir. İdarelerde ilgili birimlerin kendi faaliyetleriyle ilgili veri tabanına ve kritik verilere erişiminde yetkilendirmenin önemi büyüktür. Bu konuda dikkat edilmesi gerekli konular aşağıda ayrı ayrı belirtilmiştir.

1.6.1 Yetkilendirilmiş Erişim; Buradaki yetkilendirmenin hangi konuda ve nasıl yapıldığı, yetkilendirilmeye dair yetkili makamdan onay alınarak yazılı görevlendirme yapılıp yapılmadığı, yetkilendirilmiş kişinin zaman içerisinde görev yeri değişikliği halinde yetkilendirmenin iptali ve yeniden yetkilendirmede bulunulup bulunulmadığı hususlarının risk teşkil eden hususlar olarak denetimde öncelikli olarak ele alınması gerektiği açıktır.

Kurumlarda yetkilendirilmiş personel listesinin sık sık gözden geçirilmesi, güncellenmesi ve yetkilendirilmiş personelin görev yeri değişikliğinden anında haberdar olunabilmesi için insan kaynakları departmanları ile koordineli hareket edilmesi mutlaka sağlanmalıdır.

1.6.2 Şifre Güvenliği; Veri tabanına erişimde şifre kullanımı önemli bir konudur. Bu şifreler karmaşık yapıda olmalı, belirli dönemlerde değiştirilmesi sağlanmalı ve en az 6 karakter uzunluğunda olmalıdır. Gerekli haller için şifre parametrelerinde yeni yeni tanımlamalar yapılıp yapılmadığı kontrol edilmelidir. (Hesap kilitlenmeden önce yanlış şifre deneme sayısı ve kullanıcının aynı şifreyi ne kadar deneyeceği sayısı, v.s.)

Şifre dosyaları ve şifrelere ilişkin riskler; ***** Zayıf Şifre politikaları, ****** Şifre Değişim Aralıkları, ******* Şifrelerin Tekrar Kullanımı, olarak tanımlanabilir.

1.6.3 Görev-Yetki ve Sorumlulukla ilgili Rollerin Belirlenmesi; Yetkisiz işlemlerin gerçekleştirilmemesini sağlayabilmek bakımından veri tabanı kullanıcılarının yetki ve sorumlulukları ve üstlendikleri idari rolleri ile ilgili görev tanımlarının açık ve net yazılı olarak ortaya konması sağlanmalı ve yapılacak denetimlerde bu durum kontrol edilmelidir.

1.6.4 Veri Tabanı Yönetim Sistemlerini Denetimi ve Ağ Güvenliğinin Sağlanması;

Veri tabanı yönetim sistemleri denetimi ve ağ güvenliğinin sağlanmasında emsal alınması bakımından *"Oracle Sistemi-Oracle Veri Tabanı"* geniş bir kullanıma sahip olan bir sistem ve veri tabanı olması bakımından aşağıda örnek olarak ele alınıp uygulama içerisindeki yaşanan sorunlara değinmek yerinde olacaktır.

Genel olarak ülkemizdeki yazılım ve donanım güvenliği çalışmaları incelendiğinde ortak görüş şu yöndedir; *"Oracle gelişmiş bir veritabanı yönetim sistemi olup ilişkisel özelliklidir. Diğer bütün ilişkisel veri tabanı sistemlerinde olduğu gibi bu sistemde de büyük ölçekli bir verinin çok kullanıcılı bir ortamda depolanması ve güvenli bir şekilde erişimi kontrol edilerek yönetilmektedir. Oracle veri tabanı da bir çok şifre hesabı içerir. Ve bu şifre hesaplarının şifreleri bilinir özelliklerde olabilir ve değiştirilmedikleri takdirde veri tabanına yetkisiz kişiler bağlanarak yetkisiz işlemler gerçekleştirebilirler. Oracle şifre parametrelerinin standardı düşüktür: Bu durum sisteme yetkisiz erişimde bulunulması riskini artırmaktadır. Tanımlanması gereken şifre parametrelerinin bu aşamada yeniden gözden geçirilmesi gerekmektedir."* Belirtilen bu tespitler uygulamada ve denetimde dikkate alınması gereken önemli hususlar olarak görülmelidir.

Yazılım ve donanım güvenliği çalışmaları kapsamında ağ güvenliğinin sağlanmasıyla ilgili olarak ortaya konan ve genel kabul gören tespit ve öneriler ile mevcut durumla ilgili görülen risk şöyle açıklanabilmektedir; *"Lokasyonlar arası bağlantılı mevcut ağ üzerinde transfer olunan her türlü verinin şifrelenerek transferi sağlanmalıdır. Aksi taktirde olası bir dinleme ve bilgi sızdırılması tehdidi ile karşı karşıya kalınması halinde gerekli önlem alınmamış ve ağ güvenliği kurum için oluşturulmamış olur. Ağ güvenliği sağlanmadıkça, mevcut ağ sistemine dışarıdan gelebilecek her türlü tehdit ve sızma sonucunda kriptolanmamış verinin yetkisiz kişiler tarafından görülüp kontrol edilebilme riski ortaya çıkacaktır. Sonuçta bu durumdan kamu kurumu her bakımdan zarar görebilecektir."*[5]

5 *TOBB Ekonomi ve Teknoloji Üniversitesi Sürekli Eğitim Araştırma ve Uygulama Merkezi, Bilgi Güvenliği Yönetim Sistemi Eğitim Notları.

Söz konusu tespit ve öneriler ile mevcut durum riski uygulamada ve denetimlerde dikkate alınması gereken önemli hususlar olarak mutlaka değerlendirilmelidir.

2-BİLİŞİM SİSTEMLERİNİN DOĞRUDAN DENETLENMESİNDE İZLENECEK YÖNTEM, USUL VE ESASLAR;

Bilişim sistemleri denetimi yürütülürken risk tabanlı denetim yaklaşımına uygun olarak;[6]

- Öncelikle incelenen bilişim sisteminden kaynaklanabilecek riskler belirlenir.
- Bu riskleri minimize edecek kontrol mekanizmaları belirlenir,
- Bu kontrol mekanizmalarının kurum tarafından oluşturulup oluşturulmadığı, oluşturulmuş ise etkin çalışıp çalışmadığı incelenir.
- İnceleme sonrası, iç kontrollerdeki zayıflıklar değerlendirilir,
- Elde edilen bulgular belli bir prosedüre göre raporlanır.

Bu çerçeve ile ilgili örnek sayılabilecek bir uygulama olarak; içeriğinde sistematik olarak bilişim sistemleri denetiminin planlanması sırasında denetçinin yapacağı işler ile kontrol alanı bazında "Sistem Kontrollerinin Değerlendirilmesi" ve raporlama süreçlerini barındıran, bilişimde dış denetim anlayışını yansıtan "Sayıştay Bilişim Sistemleri Denetim Rehberinin"[7] hazırlanmış olması, kamu kurum ve kuruluşlarının iç denetim uygulamalarında mevcut yapılarına uyarlanabilecek yeni bir denetim rehberi anlayışının geliştirilmesine yol açabilecektir.

Uygulamada bilgisayarlı denetim yaklaşımları ağırlıklı olarak

*Bilgisayar Sisteminin Denetlenmesi (Beyaz Kutu Modeli);

**Bilgisayar Destekli (Bilgisayar Yardımıyla) Denetim, olarak belirtilebilir.

Denetçinin yukarıda 2. şıkta belirtilen bilgisayar destekli denetim tekniğini uygulayabilmesi için, daha önceden eğitimini aldığı ve yapacağı denetim ile ilgili kurumunca satın alınmış ve piyasada genel kabul görmüş bazı özel denetim ve işletim programlarını yapacağı iç denetimde bizzat kullanabilmesi gerekmektedir. Kullanacağı bu bilgisayar programıyla denetleyeceği kurumun iş ve işlemleriyle ilgili mevcut bilgisayar sistemine gömülü olarak denetim yapabilecek; kurum programlarını, karmaşık hesap ve işlemlerini test edebilmesi, uygulanabilir işlemleri gözden geçirerek varsa açıkları tespit edebilmesi mümkün olabilecektir. Bu uygulama denetimde henüz yerleşik ve kabul görmüş düzeyde değildir.

Bilgisayar sisteminin denetlenmesi modelinin bakiye riski minimize edebilmesi, farklı denetim metotlarını da kendi içinde barındırarak gelişmeye açık olmasını gerekmektedir.[8]

***Bilişim Sisteminin Denetlenmesi (Beyaz Kutu Modeli);** "Beyaz Kutu" yaklaşımı da denilen bu yöntemde yazılım sistemi ve program akışının uygunluğunun denetimi söz konusu olacaktır. Uygulamada denetimin en çok karşı karşıya kaldığı yaklaşım budur. Bu yaklaşım denetçinin bilişimin temel konularına ve işleyişine iyice vakıf olmasını zorunlu kılmaktadır.

****Bilgisayar Yardımıyla Denetim;** Denetim işlemlerinin yerine getirilmesinde önceden başka amaçlar için hazırlanmış "İşletim Programlarından" ve denetim için hazırlanmış "Denetim Programlarından" yararlanılır. Denetçi gerek duyarsa bilgisayar firmalarınca hazırlanmış yardımcı programlardan yararlanabilir.

Günümüzde büyük işletmelerin iç kontrol oluşumlarının kontrollerini desteklemede bu tür özel bilgisayar programlarından yararlanılmaktadır. Kurum programlarının ve dosyalarının test edilmesinde iç kontrollerin önemli bir bölümü bilgisayar işletim ve denetim programları aracılığıyla sağlanmaktadır. Finansal ve muhasebeyle ilgili denetimin yanı sıra faaliyet ve yönetim denetiminde de bu tür programlardan yararlanılmaktadır.

**Ferruh Mavituna, Netsparker Geliştirme Sorumlusu, Web Uygulamalarındaki Açıklıklar ve Korunma Yolları,

6 Özcan Rıza YILDIZ-Bilişim Sistemleri Denetimi ve Sayıştay, Sayı: 65 (Özel)

7 Davut ÖZKUL, "Bilişim Sistemi Kavramı ve Bilişim Sistemlerinin Denetimi",Sayıştay Dergisi, Sayı: 44-45, Ocak-Haziran 2002.

8 *Mehmet Kara, TÜBİTAK-UEKAE, Türkiye'de Yazılım/Donanım Güvenliği Değerlendirme Çalışmaları
*Enocta Eğitim Platformu notları

Ülkemizde kamu sektöründe bu iş için özel olarak oluşturulmuş yaygın bir "Denetim Programı" kullanımı söz konusu olmamakla birlikte yer yer bazı kurumlardaki hizmetle ilgili mevcut yazılımların işleyişi ve varlığından yararlanılarak denetimi kolaylaştırıcı veri analizi çalışmaları yapılmaktadır. Mevcut yazılımlar daha çok muhasebe ve finansman ağırlıklıdır. Ancak söz konusu mevcut yazılımları dışarıdan test edecek özel amaçlı farklı denetim programlarının kullanılması kamusal alanda henüz yaygın bir yerleşik düzen kazanmamıştır. [9]

Sayıştay ile Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) arasında bilişim sistemleri denetimi, eğitimi, rehber ve yazılım geliştirilmesi ile ilgili konularda işbirliği yapılmasına ilişkin Haziran 2007 de bir protokol imzalanmıştır.[10] Buna göre, Sayıştay'ın kamu kurumlarında yürüteceği bilişim sistemleri denetimlerinde, 1995 yılından itibaren çalışmalarını bilgi güvenliği alanında yoğunlaştırmış ve bilgi güvenliği alanında Türkiye'deki en yetkin ve tecrübe sahibi kurum olan TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) ile işbirliği yapılması öngörülmüştür. Bu işbirliği ile bir yandan Sayıştay'ın bilişim sistemlerine yönelik denetim işlerinin kalite güvencesini arttırması hedeflenmiş fakat bu işbirliğin bilgisayar destekli denetim tekniği kullanma anlayışını içermediği görülmüştür. Nitekim Sayıştay'ın bazı kurumların bilişim sistemleriyle ilgili raporlarında işaret ettiği bulgular, kamuda bilgisayar destekli denetim teknolojisinin kurulmasının öngörülmesinin ötesinde henüz tam yer etmediği, bununla birlikte günümüzde mevcut bilişim sistemlerinin işleyişinde bile hala aksamalar yaşandığını ortaya koymaktadır.

Denetimde güvenilir sonuçlara ulaşabilmek için, dış denetimin iç kontrol-bilişim sistemi-iç denetim düzleminde gerekli tüm bilgiyi edinme ve çözümlemeye ihtiyacı olduğu genel olarak kabul gören bir anlayış olarak gelişme göstermektedir [11]

"Denetimde güvenilir sonuçlara ulaşabilmek için, dış denetimin iç kontrol-bilişim sistemi-iç denetim düzleminde gerekli tüm bilgiyi edinme ve çözümlemeye ihtiyacı olduğu genel olarak kabul gören bir anlayış olarak gelişme göstermektedir"

2.1 Uygulamada Bilişim Sistem Denetimi;

Kamuda yerleşik muhasebe ve finansman programlarının doğruluğu ve işleyişi değişik metotlarla test olunmalıdır. Muhasebe finansal konuların denetiminde doğrulama testleri yapılmalıdır. Doğrulama testlerinde mevcut program kapsamındaki işlemlerin hesaplama ve kayıt doğruluğu farklı işlem kategorilerinde de örnekleme yoluyla kontrol edilmelidir. Bu kontroller genellikle mevcut ekipmanlar yardımıyla manuel olarak yapılabilmektedir.

Bilişim sistem denetimi sırasında kontroller genel ve uygulama kontrolleri olmak üzere iki sınıfta toparlanabilir. Genel Kontroller; organizasyonun yapısı ve işleyişi ile ilgili kontrollerdir. Örneğin donanım kontrolleri, sistem geliştirme kontrolleri vs. gibi. Uygulama kontrolleri ise; girdi, bilgi işleme ve çıktıların bire bir yapılan kontrollerdir.

Bilişim sistemlerindeki açıklara karşı her türlü önlemin alınabilmesi bakımından kurum içi bilişim güvenliğini denetlemek amaçlı açıklık tarama yazılımları kullanılmalıdır.

2.1.1. Direk Test/Veri Tutarlılığı; Genellikle örnekler belirlendikten sonra testler denetçi tarafından manuel olarak yapılır. Örnekleme rastlantısal, aralıklı ve farklı işlem kategorileri üzerinde yoğunlaşma şek-

9 Abdulkadir Poşul, TUBİTAK-UEKAE, Bilgi Güvenliği Standartları.

10 Sayıştay Haber Bülteni, Haziran 2007, Yıl:11 Sayı:127, Bölüm 3. ; "Sayıştay ile Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) arasında, bilişim sistemleri denetimi, eğitimi, rehber ve yazılım geliştirilmesi ile ilgili konularda işbirliği yapılmasına ilişkin bir protokol haziran 2007 de imzalanmıştır. Sayıştay ve TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü(UEKAE),kamu kurumlarının bilişim sistemlerinin denetimlerinin iş birliği ile gerçekleştirilmesi konusunda anlaşmaya varmışlardır. İki kurum arasında imzalanan çerçeve protokolle, Sayıştay, kamu kurum ve kuruluşlarının bilişim sistemlerinin denetimi görevini TÜBİTAK UEKAE' den alacağı danışmanlık ve eğitim hizmetleri desteğinde gerçekleştirecektir."

11 Adem Yaman, Kamu İç Kontrol Sisteminin Başarı Faktörleri, Mali Hukuk Dergisi 138. Sayısı, Kasım/Aralık 2008

liyle gerçekleştirilebilir. Veri girdi, işleme, depolama ve çıktısı bir bütünsellik içerisinde tutarlılık göstermelidir. (Aslında bu yöntem bilgisayar destekli denetim uygulamaları kapsamında farklı özel denetim programlarının sisteme gömülü hale getirilmesiyle o kurumun bilgisayar sistemi içerisinde ki yazılımlarının izlenebilmesi ve denetlenebilmesini test etmede başarıyla uygulanabilecektir.)

2.1.2. Uygunluk Testi; Hizmete dayalı program/yazılım uygulamalarının işleyişinde iç yapıda yapılan gözlemler ile müşteri ve vatandaş memnuniyeti dikkate alınarak karşılaşılan hata ve sorunlara göre programın güncellenmesi, tadilatı ve hataların giderilmesi sağlanabilir.

Uygunluk testi ile sistem denetiminin doğruluğu test olunurken akabinde yapılacak uygunluk denetimi sırasında da verilerin kontrol edilebilir olması bir bakıma garanti altına alınmaktadır. Denetçi bu çalışmaları yürütürken;

- Uygunluk oranında kontrol toplamları arasında mutabakat çalışmaları yapmalıdır.
- Çıktıların makul olup olmadığını incelemelidir.
- Program değişiklik kontrollerinin sisteme, programa ve/veya veri dosyalarına erişim kontrolünü gerçekleştirmeli; bilginin nasıl depolandığı, kurum politikasına ve yasalara uygunluğunu kontrol etmelidir.
- Telif hakları ve lisans kontrollerinin uygunluğuna bakmalıdır.

2.1.3. Denetçinin Dikkat Etmesi Gereken Diğer Konular;

- Bilgisayarın kullanım imkanlarının değerlendirilmesi ve olası makine hatalarının tespiti,
- Yeri geldiğinde koordineli çalışma potansiyelinin denetim sırasında hayata geçirilmesi, ilgili yazılım uzmanından yaratılan yazılım hakkında gerektiğinde yararlanma.
- Akış ve küme diyagramlarının analizi ve okunmasının doğru yapılabilmesi.
- Programlama metotları, değiştirme yöntem ve program koruma hakkında bilgilenme.
- Test yöntemleri hakkında bilgi sahibi olmak ve bilgi taşıyıcıların işleyişini bilmek.

Sistem denetimi sırasında delil ve kanıt teşkil edebilecek çıktıların bulguya dönüştürülebilir bir halde kayda ve değerlendirmeye tabi tutulması, üzerinde durulması gerekli konulardır.

2.2. Sistem Denetimde İş Sürekliliği Esası;

İş sürekliliğini bir yönetim süreci olarak algılarsak bu sürecin hizmette kalite, etkililik ve verimlilik sağlanabilmesi bakımından hiçbir şekilde sekteye uğramaması gerekmektedir.[12] Sistem denetimi yapılırken, iş sürekliliğiyle ilgili etki ve risk belirleme analiz çalışmaları yapılarak bu çalışmanın yarattığı çıktılara göre güvenlik ve kurtarma senaryoları, stratejileri geliştirilmelidir. İş sürekliliği geleceğe dönük güvenceli planları da kendi içinde geliştirerek barındırmalıdır. Bu planlar zaman içerisinde geliştirilmeli, test olunmalı ve bakımları sağlanmalıdır. Yetkili personelin takım görev anlayışı, görev, yetki ve sorumlulukları ile üstlendikleri rollerin iş sürekliliğine olumlu ya da olumsuz etkileri sorgulanmalıdır.

2.3. Sistem Denetiminde Fiziksel Güvenlik;

Veri merkezlerinde donanım, merkezin büyüklüğü ve yönetim araçları sistem denetiminin özünü teşkil etmektedir.

Donanımların türünün (bilgisayar, ağ yazıcısı, uygulama sunucusu, web sunucusu vs) ve donanımların sağlandığı donanım tedarikçilerinin belirlenmesi, donanımların ne kadarının kiralık olduğunun sorgulanarak kiralama sözleşmelerinin incelenmesi önemlidir.

Diğer önemli bir konu ise; donanımların yaşı ve kullanılabilirlik durumudur. İdarece belirlenmiş yatırım ve stratejik planlar doğrultusunda donanım yenileme kural ve prosedürlerinin önceden öngörülerek oluşturulup oluşturulmadığı sorgulanmalıdır.

2.3.1. Veri Merkezleri ve Tesislerin Fiziksel Güvenliği Hakkında;

- Kapasite durumu ve merkezin kapsadığı alan,
- Yedekleme ve geri yükleme ekipmanlarının varlığı ve işleyişi.

12 Altay Onur, Risklere Hazırlıklı Olmak İçin "İş Sürekliliği Yönetimi", http://ahsetr.blogspot.com/2011/03/risklere-hazirlikli-olmak-icin-is.html

- Kesintisiz güç kaynakları ve klimaların varlığı, çevresel zararlara karşı (doğal afet) koruma tedbirlerinin alınıp alınmadığı,
- Bina ve tesisin yapı kalitesi, sistemi kaldırabilecek bir yapı ömrüne sahip olup olmaması,

Veri merkezleri ve tesislerin fiziksel güvenliğinde dikkat edilmesi gereken hususlardır.

2.3.2. Fiziksel Güvenlikle İlgili İncelenebilecek Diğer Önemli Konular

- Donanım, ekipman sağlayıcılarıyla ve bina sahibiyle yapılmış kira sözleşmelerinin varlığı,
- Telekomünikasyon şirketleri ile yapılmış hizmet sözleşmeleri,
- Alt yapı, ağ, donanım ve servislerin bakım ve servis sözleşmeleri,
- Kurulum bakım ve değişiklik kontrolleri,
- Tedarikçilerin sorumlulukları ve sahip olma maliyetleri ile sistem yazılım güvenliği,

Denetim sırasında riskli görülen alanlar olarak analize tabi tutulup sorgulanmalıdır.

2.3.3. Sözleşmeler ve Uygunluk; Veri koruma, güvenlik, mahremiyet ile ilgili

Sözleşmeler den mutlaka incelemeye tabi tutulması gerekenler;

- Yazılım lisansları, sınırlayıcı düzenlemeler (Şifreleme Algoritmaları)
- Ülkelere göre değişik avantaj durumlarının idare yararına analizi, (Örneğin vergi avantajı)
- Fikri Mülkiyet hakları,
- Düzenli olarak iç kontrolde uygunluk kontrollerinin yapılıp yapılmadığının takibi,
- Yasalar ve düzenleyicilerle ilgili gelişmelerin takibi, hakkındaki konulardır.

3- OUTSOURCİNG/DIŞ KAYNAK KULLANIMI YOLUYLA BİLGİ TEKNOLOJİSİ TEMİNİ VE SİSTEM DENETİMİ

Outsourcing "Dış kaynak kullanımı" olarak tanımlayabileceğimiz bir kavramdır. İş yönetiminde, belli iş alanlarında uzmanlaşmış firmalara iş aktarımı yapılarak, aktarımı yapan firmanın asıl işine odaklanmasını sağlayan bir yöntemdir.[13] Outsourcing/Dış kaynak kullanımı kamusal alanda idarenin hizmet ve faaliyetlerini sürdürülebilir düzeyde kesintisiz yürütebilmesi için ihtiyaç duyduğu bilgisayar teknolojilerinin belirli bir süre boyunca teknik şartname ve sözleşme hükümlerine göre, verilen taahhütler doğrultusunda, idareyle işbirliği ve koordinasyon içerisinde kullanılabilmesine olanak sağlayacak şekilde temin olunmasıdır.

Bilgi Güvenliği Standartları kapsamında; [14]

- Hızla değişen teknolojiyle temellendirilmiş bilgisayarların, uygulamaların ve ağ yapılarının yüksek tehdit altında bulunmaları.
- Yeni teknolojik sistemlerin sürekli saldırıya maruz kalmaları ve açıkların keşfedilmesi.
- Kurumların düşük maliyetli ve yüksek verimli sistemlere duydukları ihtiyaç.
- Yasal ve düzenleyici zorunlulukların "Bilgi Güvenliği" adına getirdikleri yükümlülükler.
- Kurum ve organizasyonların, kaynak, beceri ve uzmanlık bakımından "Bilgi Güvenliğini"

sağlamadaki yetersizlikleri, güvenceli Outsourcing/Dış kaynak kullanımı.

3.1 Outsourcing Dış kaynak Kullanımının Kuruma Sağlayacağı Faydalar;

- Kurumsal ana faaliyet alanında konuya odaklanma olanağı sağlar,
- Dağınık verilerin tek merkezde toplanmasını sağlar,
- İstenilen bilgiye kısa zamanda ulaşılabilmesi olanağını sunar,
- Gizliliğin korunması sağlar,
- Kaynakların etkin kullanımı, zamandan tasarruf, verimlilik artışı sağlaması[15]
- İşin uzman tarafından yapılması gibi önemli bir avantaj yaratır,

13 Outsourcing´in avantajları, editör sunumu, http://www.kobifinans.com.tr/tr/bilgi_merkezi/020606/349

14 Abdulkadir Poşul, TUBİTAK-UEKAE, Bilgi Güvenliği Standartları

15 Atila KARAHAN, Dış kaynak Kullanımının verimlilik üzerine Etkisi, Balıkesir Üniversitesi Sosyal Bilimler Enstitüsü Dergisi Sayı 21 Haziran 2009.

3.2 Denetimde Outsourcing/Dış Kaynak Kullanımı Uygulamasıyla İlgili Dikkat Edilecek Bazı Hususlar;

Outsourcing/Dış kaynak kullanımı uygulamasında idareye bilişim hizmeti taahhüdünde bulunan firma gerektiğinde konusunda ihtisas sahibi alt yüklenici firmalarla yazılım uygulamaları ve tasarımları konusunda çalışabileceğini ve hangi konuda hangi uzman ve yetkili alt yüklenici firma ile çalışacağını sözleşmede ortaya koymak durumundadır. Bu firmaların yeterli etkinlikte, alanında ihtisas sahibi firmalar olması gerekmektedir.

Taahhütte bulunan firmanın bilgi işlem hizmetleri için idarenin kullanımına vereceği donanımlar varsa bunların sayısı ve taşınır kayıt listesi ve kullanıcıları, varlık envanterindeki yeri, bakım ve servis hizmetlerinin sağlanması vs hususlar mutlaka sorgulanmalıdır.

Diğer önemli bir konu hizmet taahhüdünde bulunan firmanın idare bünyesinde idarenin bilgi işlem departmanı çalışanlarıyla birlikte koordineli olarak görev yapacak personelinin (Proje Yöneticisi Bilgisayar Mühendisi, Yazılım Uzmanı, Sistem Destek Uzmanı, Desktop Destek Uzmanı vs) yetkinlikleri, benzeri bir işte yaptıkları çalışmalara dair belge ve dokümanı içeren kişisel dosyalarının idareye sunulmasıdır. Bu aşamada idare bilgi işlem departmanında da eş değer yetkinlikte teknik personelin istihdam olunması kontrol yetkisinin ehil ellerce idare yararına kullanılabilmesi bakımından çok önemlidir.

Sözleşme ve teknik şartnamede öngörülen yazılım hizmetlerinin işlerlik kazandırılabilmesi için idare personeli olan kullanıcısına eğitim verilmesi yönünde yükümlülüğün firmasınca yerine getirip getirilmediği izlenmelidir.

3.3. Outsourcing/Dış Kaynak Kullanımı Yoluyla Hizmet Satın Alınmasında Gizlilik Sözleşmesi Düzenlenmesinin Önemi;

Hizmet İşleri Genel Şartnamesinde gizliliğe dair genel bir hükmü olsa da, ilgili madde hükmünün Tip Şartname hükmü olması ayrıca özel bir düzenlemeyi zorunlu kılmaktadır.

Kurumsal bilgi yönetim sistemi kapsamında bilgi işlem hizmet ve faaliyetleriyle ilgili yapılacak her türlü çalışma dolayısıyla kurumun yüklenici firmaya işle ilgili vereceği gizli bilgiler ile yüklenici tarafından herhangi bir şekilde öğrenilecek gizli bilgilerin ve/veya yükleniciden alınacak olan gizli bilgilerin gizlilik sözleşmesi kapsamında belirtilen şartlar ve taahhütler altında gizli tutulabilmesi bakımından "Gizlilik Sözleşmesi "nin[16] hizmet satın alınan firma ile ilgili kamu kurumu arasında düzenlenmesi yerinde olacaktır.

Böylece, tarafların birbirlerinden, çalışanlarından yardımcılarından ve ilgili diğer üçüncü taraflardan yazılı veya sözlü edindikleri, gizli olduğu açıkça ifade edilen veya edilmeyen işle ve taraflarla ilgili ticari olup olmadığına bakılmaksızın her türlü gizli bilginin; güvenliği, bütünlüğü, erişebilirliği daha fazla güvence altına alınabilecektir.

Sonuç:

Kamu kurum ve kuruluşlarının bilgi işlem sistemlerinde güvenli bir yapı oluşturmaları mevcut iç kontrol sisteminin daha etkin bir işlerlik kazanabilmesi bakımından temel bir algı olarak kabul edilmelidir. Bu bağlamda;

I-Kurumun bilgi güvenliğini zedeleyici dışarıdan gelebilecek her türlü eylemlere karşı kurum içinde bir bilgi güvenliği anlayışının geliştirilmesi ihtiyacı kaçınılmazdır. Bu bağlamda kurumlarda bilgi güvenliği yönetim stratejileri geliştirilerek bilgi varlıklarının güvenliğine yönelik tedbirler alınmalı, bilgi varlıkları envanteri oluşturulmalıdır.

II-Devlet Planlama Teşkilatı tarafından geniş katılımla hazırlanan 2006-2010 yıllarını kapsayan ve eylem planlarıyla desteklenen Türkiye Bilgi Toplumu Stratejisinde kamusal alanda bilgi güvenliği yönetim sistemlerinin oluşturulması ve geliştirilmesi amaçlarına katkıda bulunulmasının hedeflendiği görülmektedir. Söz konusu bu bilgi güvenliği yönetim sistemlerinin oluşturulması kapsamında; kamu kurum ve kuruluşlarında ki farklı hizmet çeşitliliği gözetilerek, dış denetimin yanı sıra iç kontrol ve iç denetim anlayışına da giderek yer verilmesi gerekmektedir. Mevzuati alt

16 Gizlilik Sözleşmesi Örneği; "Bilişim Grup Gizlilik sözleşmesi", http://www.bilisimgrup.com/index.php?option=content&task=view&id=192&Itemid=0

yapısı ve standardı belirlenmiş olan bilgisayar destekli denetim tekniklerinin geliştirilerek yaygınlaştırılmasına yönelik temel politikaların oluşturulması kamu yararına olacaktır.

III-Kurum ve organizasyonların düşük maliyetli ve yüksek verimli bilişim teknolojisi sistemlerine duydukları ihtiyaç karşısında dış kaynak kullanımıyla bilişim hizmetleri ya da bilgisayar teknolojileri temin ederek bilgi varlıklarının güvence altına alınması kamu kurum ve kuruluşlarınca bir yöntem olarak kabul görmelidir. Bu yöntem sayesinde iç denetimin bir bütünsellik içerisinde hizmet temin olunan teknolojik sistem üzerinden idari uygulamaları kontrol ve test etme yükümlülüğü, bilgi varlıkları sisteminin idari bütünlük içinde ki sağlıklı ve güvenli işleyişine katkı sağlayacaktır.

IV-Kamu iç kontrol eylem planında sistematik olarak yapılması öngörülen kontrollere ilişkin verilerin kurumların kendi bilgi sistemlerinde yapılacak yeni düzenlemelerle otomasyona dayalı yeni bir kontrol anlayışıyla geliştirilerek sürdürülmesi daha güvenli olacaktır.

Kaynakça:

Enocta Eğitim Platformu – Bilgisayar Destekli Denetim Eğitim Ders Notları.

Tahsin Türköz, TÜBİTAK-UEKAE , BT Varlıklarının Güvenlik Testi Adımları.

5651 Nolu İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun.

Bülent Güngör, Bank Asya Yazılım Geliştirme Uzmanı/Müdürü, Bilgi Güvenliği Danışmanlık Hizmetleri Hakkında. http://www.innova.com.tr/solution-detail/Bilgi-Guvenligi-Danismanlik-Hizmetleri/(Erişim Tarihi15.08.2011

*****TOBB Ekonomi ve Teknoloji Üniversitesi Sürekli Eğitim Araştırma ve Uygulama Merkezi, Bilgi Güvenliği Yönetim Sistemi Eğitim Notları.

******Ferruh Mavituna, Netsparker Geliştirme Sorumlusu, Web Uygulamalarındaki Açıklıklar ve Korunma Yolları,

Özcan Rıza Yıldız-Bilişim Sistemleri Denetimi ve Sayıştay, Sayıştay Dergisi, Sayı: 65

Davut Özkul, "Bilişim Sistemi Kavramı ve Bilişim Sistemlerinin Denetimi",Sayıştay Dergisi, Sayı: 44-45, Ocak-Haziran 2002.

Mehmet Kara, TÜBİTAK-UEKAE, Türkiye'de Yazılım/Donanım Güvenliği Değerlendirme Çalışmaları.

Abdulkadir Poşul, TUBİTAK-UEKAE, Bilgi Güvenliği Standartları.

Sayıştay Haber Bülteni, Haziran 2007, Yıl:11 Sayı:127, Bölüm 3. ; "Sayıştay ile Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK- UEKAE) arasında protokol imzalanması hakkında"

Adem Yaman, Kamu İç Kontrol Sisteminin Başarı Faktörleri, Mali Hukuk Dergisi 138. Sayısı, Kasım/Aralık 2008

Altay Onur, Risklere Hazırlıklı Olmak İçin "İş Sürekliliği Yönetimi". http://ahsetr.blogspot.com/2011/03/risklere-hazirlikli-olmak-icin-is.html (Erişim Tarihi15.08.2011)

Outsourcing´in Avantajları, Editör Sunumu, http://www.kobifinans.com.tr/tr/bilgi_merkezi/020606/349 (Erişim Tarihi, 22. 08. 2011)

Abdulkadir Poşul, TUBİTAK-UEKAE, Bilgi Güvenliği Standartları

Atila KARAHAN**,** Dış kaynak Kullanımının Verimlilik Üzerine Etkisi, Balıkesir

Üniversitesi Sosyal Bilimler Enstitüsü Dergisi Sayı 21 Haziran 2009.

Gizlilik Sözleşmesi Örneği; "Bilişim Grup Gizlilik sözleşmesi", http://www.bilisimgrup.com/index.php?option=content&task=view&id=192&Itemid=0 (Erişim Tarihi, 22.08.2011)