# Bilgi Güvenliğinin Kurumsal Bazda Uygulanması

Şeref SAĞIROĞLU, Eren ERSOY, Mustafa ALKAN

***Özet* - Kurum, kuruluş ve işletmelerin belirli güvenlik standartları çerçevesinde bilgi güvenliğini sağlayarak iç ve dış tehditler karşısında zarar görmeden veya en az zararla iş sürekliliklerini devam ettirebilmeleri için bilgi güvenliği standartlarını kendi kuruluşlarında uygulamaları artık neredeyse bir zorunluluk haline gelmiştir. Kurumların, bilgi sistemleri süreçlerini inceleyerek tehditleri ve riskleri belirlemesi ve bu riskleri kabul edilebilir bir seviyeye indirebilmesi için alınacak karşı önlemlerin tespit edilmesi gerekmektedir. Bu bildiride, bu yöntemlerin TS ISO/IEC 27001 Kurumsal Bilgi Güvenliği Standardı çerçevesinde bir kuruma nasıl uygulanabileceği konusunda birtakım ipuçları verilmeye çalışılmıştır.**

***Anahtar Kelimeler* : Kurumsal Bilgi Güvenliği, Risk Yönetimi, Uygulamalar**

*Abstract* - **It has become almost compulsory for institutions, organizations and enterprises to apply information security standards in their organizations so that they could ensure business continuity without any or minimum harm in case of internal and external threats. Organizations have to examine their information system processes to find out threats and risks and then countermeasures against these risks must be determined to be able to reduce the risks to an acceptable level. In this article, it is aimed to provide some clues on how these methods could be applied to organizations within the framework of TS ISO/IEC 27001 Information Security Management Systems standard.**

***Keywords* - Organizational Information Security, Risk Management, Applications**

## I. GİRİŞ

Kişiler, kurumlar ve kuruluşlar işlerini artık çok büyük oranda elektronik ortamlarda gerçekleştirmektedirler. Bunun sonucu olarak e-ticaret, e-kurum, e-devlet, e-imza, e-posta gibi kavramlar hızla klasik çalışma biçimlerinin yerini almaktadır. Bankacılık işlemlerini bankaya gitmeden evimizdeki veya iş yerimizdeki kişisel bilgisayarlarımızla ya da cep telefonlarımızla gerçekleştirebilmemiz, vergi ve ceza ödemeleri yapabilmemiz, pasaport başvurusunda bulunabilmemiz, seyahat rezervasyonları yapabilmemiz, on-line biletleri satın alabilmemiz,çalıntı cep telefonlarını sorgulayabilmemiz, tamirdeki veya bakımdaki cihazlarımızın işlemlerinin hangi aşamada olduğunu öğrenebilmemiz, mobil ortamlardan para transferi yapabilmemiz, artık günlük yaşantımızda bizlerin alışkanlık haline getirmeye başladığı davranışlardır. Bilgisayar kullanımındaki bu artışa paralel olarak bilgisayar sistemlerine ve ağlara da aynı oranda istenmeyen saldırıların olduğu ve gelecekte de olacağı açıktır. Özellikle 1998 yılından itibaren yeni bilgi sistemlerine ait bildirilen aylık güvenlik açıkları sayısı beş katına çıkmıştır [1].

Araştırma kuruluşu Gartner tarafından yapılan bir çalışmada, artan saldırı sayısı ve sürekli geliştirilen saldırı teknikleriyle baş edebilmek için, güvenlik yazılımları pazarının gittikçe büyüyeceği, hükümetlerin de desteğiyle 2009 yılına kadar pazardaki yıllık artış oranının %16,2 olacağı ve pazar payının 11,4 milyar ABD Dolarına ulaşacağı belirtilmektedir [2].

Bu tehlikeyi zamanında gören bazı kuruluşların ve BSI'ın (British Standards Institution) önderliğinde 1993 yılında başlatılan ilk bilgi güvenliği standardı çalışmalarında endüstri, devlet ve ticari sektörden gelen ortak bir güvenlik yapılanması isteği büyük rol oynamıştır. Bu isteğin asıl nedeni, kuruluşların birbirleriyle yaptıkları işlerin yürütülmesi sırasında karşılıklı olarak asgari düzeyde güvenlik seviyesini sağladıklarını birbirlerine göstermek ihtiyacını hissetmeleridir. Bu çalışmaya katılan kuruluşlar arasında British Standards Institution, British Telecommunications, British Security Industry Association, Marks and Spencer, Nationwide Building Society, Shell, Unilever, HSBC gibi yaklaşık 25 şirket bulunmaktadır [3].

Yapılan çalışmalar sonucunda, bu saldırılardan en az kayıpla kurtulabilmek ve riskleri en aza indirebilmek için belirli güvenlik standartlarının uygulanmasının gerekli olduğu ortaya çıkmıştır. İstenmeyen elektronik saldırılara karşı tek başına yazılım ve donanım önlemlerinin (virüs tarayıcılar, güvenlik duvarı v.b.) yeterli olmadığı, kurumlarda çalışan personelin güvenlik bilincinin artırılması ve en üst yöneticiden en alttaki personele kadar standart çerçevesinde belirlenmiş olan güvenlik prosedürlerine sıkı sıkıya tavizsiz bir şekilde uyulması gerektiği genel kabul görmüş bir yaklaşımdır.

Standart uyarınca, kurumların bilgi sistem süreçlerinin incelenerek tehditlerin ve risklerin belirlenmesi ve bu riskleri kabul edilebilir bir seviyeye indirebilmek için alınacak karşı önlemlerin tespit edilmesi gerekmektedir. Bu standardın adı TS ISO/IEC 27001 Kurumsal Bilgi Güvenliği (KBG) Standardı olarak bilinmektedir. Bu standart bir kuruma kurumsal bilgi güvenliğinin nasıl uygulanabileceği konusunda birtakım ipuçları vermek için hazırlanmış bir dokümandır. İlgili standart gereğince bazı kavramların anlaşılması, uygulamaların yapılması ve karar verme aşamalarına ışık tutmaktadır. Bu kavramlar ve risk tespit yöntemlerinin daha

Ş. SAĞIROĞLU, Bilgisayar Mühendisliği Bölümü, Mühendislik Mimarlık Fakültesi Gazi Üniversitesi, Ankara. ss@gazi.edu.tr
E. ERSOY, Telekomünikasyon Kurumu, Maltepe, Ankara, eersoy@tk.gov.tr
M.ALKAN,Telekomünikasyon Kurumu, Maltepe, Ankara, malkan@tk.gov.tr

ayrıntılı açıklamaları için ISO'nun yayınladığı kılavuzlardan yararlanılabilir [4].

## II. Kurumsal Bilgi Güvenliği için Çalışma Alanı Belirleme ve Anket Çalışmaları

KBG'nin sağlanması için standartta genel olarak önerilen tüm maddelerin kurumun bütün işlerini kapsayacak şekilde birebir uygulanması gerekmeyebilir. TS ISO/IEC 27001 standardı ölçeklenebilir yapısından dolayı küçükten büyüğe doğru çeşitli büyüklükteki kurumlara uygulanabilmektedir. Bir kurumda uygulamaya hazırlık için ilk yapılması gereken husus, kurumda standardın uygulanacağı alanı belirlemektir. Bu alan belirlenirken en riskli ve tehditlere en açık sistemler ile ilgili çalışma alanlarının öncelikle dikkate alınması gerekmektedir. Daha düşük riskli iş alanları daha sonra standardın PUKÖ (Planla-Uygula-Kontrol et-Önlem al) yapısı içerisinde ele alınarak uygulamalara dahil edilebilir.

Bir kurumda hangi iş alanlarının risklere açık ve tehdit altında olduğu, bir riskin gerçekleşmesi halinde hangi iş süreçlerinin kesintiye uğrayabileceği ve hangi iş süreçlerinin kritik olduğunun belirlenmesi için tüm birimleri kapsayan bir anket çalışması yapılması en önemli hususlardan biridir. Bu çalışmada, anketlere ek olarak doğrudan iş süreçlerini uygulayan çalışanlarla yüz yüze görüşmeler yapmak süreç risklerinin tespitinde önemli rol oynamaktadır. Aksi takdirde sadece dağıtılan anketlerin dikkate alınması bir takım önemli risk faktörlerinin gözden kaçırılmasına neden olabilmektedir. Yapılan çalışmalar genellikle aşağıdaki sonuçları vermektedir [5].

- Süreç anketlerinde iş kesilmelerinin ana nedeni olarak, bilgisayar donanım-yazılım ve ağ sorunları gösterilmiştir.
- Kurumların uygulama süreçleri ağırlıklı olarak bilgi sistemlerini kullanmaktadır.
- Bilgi sistemlerinin çok büyük bir kısmı IT birimleri tarafından yönetilmektedir.
- En kritik varlıkların korunmasına en önce başlamak gerektiği ilkesinden yola çıkılarak, KBG'nin sağlanabilmesi için en önemli ve kritik varlıklar olan bilgi sistemlerine öncelik verilerek bu noktadan başlanması gerekmektedir. Genel eğilimin de bu yönde olduğunu belirtmekte fayda vardır.
- Bilgi güvenliği konusunda kurumsal kültürün oluşması ve eski alışkanlıkların terk edilmesini sağlamak çok kısa sürede tüm kurumda mümkün değildir.
- Kurumsal kültürün oluşturulması amacıyla ana bilgi sistemlerini yöneten, işleten ve sürekliliğini sağlayan bilgi teknolojileri (BT) birimlerinin pilot birim olarak seçilmesi uygun olmaktadır.

Bu çalışma çerçevesinde, KBG'ye geçiş için hazırlanan risk değerlendirme anket çalışmasına küçük bir örnek Çizelge 1'de verilmiştir. Bu soruların kurumların yapısına göre çeşitlilik ve derinlik kazanacağını belirtmekte fayda vardır.

Çizelge 1. Riskleri Hesaplamada Kullanılacak Olan Anket Sorularına Örnekler

| SORULAR | SEÇENEKLER |
|---|---|
| 1. Kullanılan bilgilerin gizlilik derecesi nedir ? | a) Çok gizli<br>b) Gizli<br>c) Açıklanabilir |
| 2. İş kesilmelerine karşı toleransınız nedir? | a) Hiç kesilmemeli<br>b) Maksimum 4 saat<br>c) Maksimum 24 saat<br>d) 24 saatten fazla |
| 3. Bilgi kaybında kolay geriye dönülebilir mi ? | a) Kolayca<br>b) Zaman alır, iş kaybı yaratır<br>c) Dönüş yapılamaz |
| 4. Süreçte kesilme olduğunda hangi süreçleri veya Kurumun hangi işini engeller? | Cevaplar serbest formda verilecektir |
| 5. Süreçte görevlendirilmiş personelin eğitim durumu nedir? | a) İyi eğitilmiş<br>b) Orta<br>c) Çok az bilgili |
| 6. Personelin yedeği var mıdır? | a)Var<br>b)Yok |
| 7. Süreç Kurum için ne derece önemlidir? | a) Çok önemli<br>b) Orta<br>c) Düşük |
| 8. Süreçler bilgisayar ağırlıklı mı işlemektedir? | a) Tümüyle<br>b) Kısmen<br>c) El ortamında yürütülmektedir |
| 9. Bilgiler yedekleniyor mu? | a) Evet<br>b) Hayır |
| 10. Bilgiye sadece süreçlerin yetkili personeli mi erişebiliyor ? | a) Evet<br>b) Tüm çalışanlar erişebiliyor |
| ..... | ..... |
| ..... | ..... |

## III. Risk Analizi Yaklaşımları, Değerlendirme ve Başarı Ölçümleri

Bilgi varlıklarının potansiyel tehditlere ne kadar açık olduğunun ölçüsü risk olarak tanımlanmıştır. Risklerin neler olduğunun tespiti, bilgi güvenliğini tehlikeye atabilecek olası tehditlerin değerlendirilmesi ve riskleri kabul edilebilir seviyeye düşürebilmek amacıyla yapılan çalışmalar, tanımlamalar, değerlendirmeler ve düzenli aralıklarla gözden geçirme işlemlerinin tümü risk yönetimi olarak tanımlanabilmektedir. Bu sayede risklerin doğru olarak yönetilmesi kolaylaşmakta ve yüksek seviyede bir güvenlik yaklaşımı sağlanabilmektedir. Bu çalışmada sunulduğu gibi bilgi güvenliği çalışmaları bir kurumda tepeden aşağıya veya aşağıdan tepeye doğru yapılabilir. Tepeden aşağı olan yaklaşımda; KBG çalışmalarının başlatılması, çalışmalara destek verilmesi ve uygun yapıların oluşturulması konusunda üst yönetimin konuyu benimsemesi ve bunun hiyerarşik olarak alt kademelere aktarılması konusunda gerekli kararlılığı göstermesi esastır. Aşağıdan tepeye doğru olan yaklaşımda ise; hiyerarşik olarak alttan üste doğru bir yapılanma takip edilir. Alt birimler gerekli çalışmaları yaparlar, gerektiği anda çalışmalara destek alınması ve çalışmaların aksamadan yürütülmesi için üst yönetimin bilgilendirilmesi esasına dayanır.

Risklerin analizini yapabilmek için kabul görmüş bazı kavramlar ve yaklaşımlar bulunmaktadır. Bileşen tabanlı risk

analizi, süreç tabanlı risk analizi, nicel yaklaşım, nitel yaklaşım, Delphie tekniği gibi risk değerlendirme ve başarı ve ölçümleri bunlara örnek olarak verilebilir.

Karşı önlemler alındıktan ve belli bir süre (önerilen en az 1 yıl) uygulandıktan sonra, önlemlerin ne kadar işe yaradığını ve arzu edilen risk seviyesine ulaşılıp ulaşılamadığını tespit edebilmek için literatürden yararlanılabilir [6].

## IV. Risk Analizi Yöntemlerinde Değerlendirme Örnekleri

Daha önceki bölümde de bahsedildiği gibi farklı risk değerlendirme yöntemleri mevcuttur. Bu yöntemlere örnekler aşağıda alt başlıklarda verilmiştir.

### *A. Nicel (Quantitative) Yaklaşım*

Var olan bir tehdidin varlıkları etkilemesinin derecesini ölçebilmek için 1'den 5'e kadar bir skala yapılabilir. (Örneğin: 1- Çok az zarar, 2- Önemsiz zarar, 3- Orta zarar, 4- Belli bölüme çok ciddi zarar, 5- Tüm sistemi durdurur). Tehdidin olma olasılığını ise yine benzer olarak 1'den 5'e kadar bir skalayla derecelendirebiliriz.
(Örneğin: 1- Çok az olasılık, 2- Az olasılık, 3- Orta olasılık, 4- Büyük olasılık, 5- Çok büyük olasılık). Nicel olarak riskleri değerlendirmede kullanılabilecek değerlendirme tablosuna bir örnek Çizelge 2'de verilmiştir.

Çizelge 2. Nicel olarak risk sınıflandırma örneği

| **R** | Çok az zarar (1) | Önemsiz zarar (2) | Orta Zarar (3) | Ciddi zarar (4) | Çok ciddi zarar (5) |
|---|---|---|---|---|---|
| Çok az olasılıkla (1) | 1 | 2 | 3 | 4 | 5 |
| Az olasılıkla (2) | 2 | 4 | 6 | 8 | 10 |
| Orta olasılıkla (3) | 3 | 6 | 9 | 12 | 15 |
| Büyük olasılıkla (4) | 4 | 8 | 12 | 16 | 20 |
| Çok Büyük olasılıkla (5) | 5 | 10 | 15 | 20 | 25 |

1-3: Düşük, 4-6: Orta, 7-12:Yüksek, 15-18:Kritik, 19-25:Çok Yüksek
Risk=R= Tehdidin gerçekleşme İhtimali * Tehdidin Etkisi

### *B. Nitel (Qualitative) Yaklaşım*

Çizelge 2'de verilen nicel olarak tehdidin olma olasılığı ve etki değerinin yanında aynı zamanda nitel olarak ta bunun nasıl verilebileceği Çizelge 3'de belirtilmiştir. Bu çizelgelerde VH=çok ciddi, H=ciddi, M=orta, L=düşük ve VL=çok az anlamına gelen kısaltmalar kullanılmıştır.

Çizelge 3. Nitel olarak risk sınıflandırma örneği

| **R** | Çok az zarar(VL) | Önemsiz zarar(L) | Orta Zarar(M) | Ciddi zarar(H) | Çok ciddi zarar(VH) |
|---|---|---|---|---|---|
| Çok az olasılıkla(VL) | Düşük | Düşük | Düşük | Orta | Orta |
| Az olasılıkla(L) | Düşük | Orta | Orta | Yüksek | Yüksek |
| Orta olasılıkla(M) | Düşük | Orta | Yüksek | Yüksek | Kritik |
| Büyük olasılıkla(H) | Orta | Yüksek | Yüksek | Kritik | Çok Yüksek |
| Çok Büyük olasılıkla(VH) | Orta | Yüksek | Kritik | Çok Yüksek | Çok Yüksek |

Risk=R= Tehdidin gerçekleşme İhtimali * Tehdidin Etkisi

## V. Varlık Belirleme Çalışmaları ve Yaşanabilecek Güçlükler

Bir kurumda standardın uygulanmasına hazırlık olarak süreç sorumluları ile yapılan anketlerin ve görüşmelerin ışığında, kurumun önemli varlıklarının neler olduğu ve bu varlıkların risklerinin neler olabileceği sorusuna cevap aranması önemlidir ve standardın şart koştuğu çalışmaların başında gelmektedir. Varlık belirleme çalışmaları çerçevesinde varlıkları; donanım, uygulama yazılımı, hizmet yazılımı ve bilgi varlıkları olmak üzere sınıflandırmak tehditlerin belirlenmesinde kolaylık sağlamaktadır. Varlık tespit çalışmaları, kurumun hangi iş alanları için standart uygulanacaksa o alanlardaki varlıkları kapsamalıdır. Kurum için korunması gereken önemli varlıklar tespit edildikten sonra, bu varlıkların kritiklik ve gizlilik dereceleri varlıkların önemine uygun bir şekilde atanmalıdır.

Çizelge 4'de donanımlar için kullanılabilecek bir örnek çizelge verilmiştir. Burada varlığın kritiklik ve gizlilik derecesi kriterlerinin neler olduğu açıklanmıştır. Bu sınıflandırma, diğer varlık türlerine de uygun bir şekilde uygulanabilmektedir ve seviyeler istenilen şekilde daha da detaylandırılabilmektedir.

Çizelge 4. Kurum Bilgi Sistemleri (Donanımlar) Kritiklik ve Gizlilik kriterleri

| **DONANIMLAR** | |
|---|---|
| **Kritiklik** | **Donanımın kritikliği üç seviyede belirlenir:** Yüksek, Orta, Düşük<br><br>Bu kriterler:<br>**Yüksek:** Bu donanımın devre dışı kalması tüm sistemi devre dışı bırakır. Sistem güvenliği tehlikeye girer. Sistem büyük oranda kullanılmaz hale gelir. Yüksek kritiklik derecesine sahip bir sistemin 1 saate kadar devre dışı kalması kabul edilebilir. Bu kritiklikteki donanımlar, **kırmızı** renk etiketle etiketlenmelidir.<br><br>**Orta:** Bu donanımın devre dışı kalması durumunda, sistem çalışmaya |

| | |
|---|---|
| | devam eder ancak sistemin bir bölümü zarar görmüş olabilir. Orta kritiklik derecesine sahip bir sistemin 24 saate kadar devre dışı kalması kabul edilebilir. Bu kritiklikteki donanımlar, **mavi** renk etiketle etiketlenmelidir.<br><br>**Düşük:** Bu donanımın devre dışı kalması durumunda sistem güvenliği etkilenmez. Sistem tüm işlevleri ile çalışır durumda olmaya devam eder. Düşük kritikliğe sahip bir donanımın 2 güne kadar devre dışı kalması kabul edilebilir. Bu kritiklikteki donanımlar, **yeşil** renk etiketle etiketlenmelidir. |
| **Gizlilik Derecesi** | Gizlilik derecesi iki seviyede belirlenir:<br><br>**Gizli:** Bu gizlilik derecesindeki bir donanıma ait erişim bilgilerinin ortaya çıkması durumunda, sisteme yetkisiz kişilerin erişmesi mümkün hale gelir. Sistem güvenliği tehlikeye girer.<br><br>**Tasnif Dışı:** Bu gizlilik derecesindeki bir donanıma ait erişim bilgilerinin ortaya çıkması durumunda, sistem güvenliği tehlikeye girmez ancak yalnızca bu donanıma yetkisiz kişilerin erişmesi mümkün hale gelir. |

Çizelge 5'de verilen donanıma ait bir örnek bilgi tablosu sunulmuştur. Varlıkların gizlilik ve kritiklik dereceleri sütunundaki bilgiler için kaynak tablo Çizelge 4'de verilen kriterlerdir.

ÇIZELGE 5. DONANIM VARLIKLARI ÇIZELGESI

| Özellik | Açıklama |
|---|---|
| **Donanımın Adı ve Tipi** | Veritabanı ve Uygulama Sunucusu |
| **Genel Tanıtım** | Üzerinde xxx projesi kapsamındaki yyy uygulamalarının bilgileri bulunmaktadır. Ayni zamanda xxx uygulamaları için de kullanılmaktadır. Bu donanımın çalışamaması sonucu şu gruplar doğrudan etkilenecektir:<br>• xxx projesini kullanan AAA Müdürlüğü uç kullanıcıları<br>• xxx uygulaması yapan uç kullanıcılar<br>• Diğer Bölgeler (xxx Projesi veritabanı tutarlılığı açısından)<br>• AAA Müdürlüğü (xxx sunucusu) |
| **Konum** | Ankara |
| **Üzerinde Çalışan Servisler ya da Uygulamalar** | İşletim Sistemi: xxx<br>Veritabanı : xxx<br>Uygulamalar: xxx |
| **Yedeği Var mı?** | Donanımsal anlamda yedeklenmemiştir. Raid, Mirroring veya Cluster yapısı yoktur. Bilgiler işletim sistemi komutlarıyla belirli zamanlarda kartuşlara yedeklenmektedir. Bu donanım bir UPS sistemine bağlıdır. |
| **Bağlantı Şekli (Fiber, Coax, UTP)** | UTP |
| **IP Adresi** | Xxx |
| **Erişim Bilgileri** | Bu donanımın yazılım ayarları değiştirilmek istendiğinde, IT birimi Sistem Destek Müh. tarafından yerinde konsol üzerinden veya uzaktan xxx ile erişilebiliyor. Erişim için şifre sorulmaktadır. |
| **Sorumlu Personel** | AAA Bölge Müdürü |
| **Yetkili Personel** | IT birimi Sistem Destek Müh. |
| **İşletim Sistemi ve Sürümü** | Bu donanım üzerinde çalışan işletim sistemi xxxx |
| **Erişim Yetkisine Sahip Kişiler** | IT birimi Sistem Destek Müh. |
| **Kritiklik Derecesi** | **Yüksek:** Bu donanımın devre dışı kalması tüm sistemi devre dışı bırakır. Sistem güvenliği tehlikeye girer. Sistem büyük oranda kullanılmaz hale gelir. Yüksek kritiklik derecesine sahip bir sistemin 1 saate kadar devre dışı kalması kabul edilebilir. xxx programları sürekli çalışır durumda olmalıdır. Bu kritiklikteki donanımlar, **kırmızı** renk etiketle etiketlenmelidir. |
| **Gizlilik Derecesi** | **Gizli:** Bu gizlilik derecesindeki bir donanıma ait erişim bilgilerinin ortaya çıkması durumunda, sisteme yetkisiz kişilerin erişmesi mümkün hale gelir. Sistem güvenliği tehlikeye girer. |
| **Maddi Değeri** | Sadece donanım olarak xxx $ |

Varlıkların değerlerini belirleme çalışmaları sırasında yaşanılabilecek güçlükler aşağıda sıralanmıştır. KBG politikaları bir kuruma uygulanmadan önce bu güçlüklerle karşılaşılacağı dikkate alınmalıdır.

1. İlgili personele ulaşmak ve konuşmak için randevu almak zor olabilmektedir.
2. İlgili personel kullandığı donanımın ve yazılımın özelliklerini tam olarak bilememektedir.
3. Kullanıcılar arasında yüksek oranda koordinasyon eksikliği olabilmektedir.
4. Aynı serviste, aynı işi yapan birden fazla personel ile yapılan görüşmelerde, aynı konuda farklı cevaplar alınabilmektedir.
5. Personelin çalıştığı konuda eğitiminin genellikle yeterli olmadığı görülebilmektedir.
6. Envanter çalışmasının hiç yapılmamış veya yapılmaya çalışılsa bile yeterince sağlıklı olmadığı, güncellenmediği, angarya olarak görülebildiği izlenmektedir.
7. Varlıklarda sürekli güncellemeler, eklemeler, çıkarımlar ve yer değişiklikleri olabilmesi nedeniyle, izlemek için çok çaba ve dikkat gerekmektedir.

## VI. RISK ANALIZI ÇALIŞMALARI

Risk analizi aşamasında, daha önce yapılan anketler ve süreç sorumluları ile yapılan görüşmeler sonucu bilgi sistemleri bileşenleri ve süreçleri ile bilgi sistemlerini kullanan ana iş süreçleri dikkate alınarak bu işlemler yapılmalıdır. Bir bilgi sisteminde bulunabilecek ana iş süreçleri aşağıda örnek olarak sunulmuştur. Bunlar:

1. Doküman ve Arşiv Yönetim Sistemi Uygulamaları
2. Kurumsal Kaynak Planlama Uygulamaları
3. Muhasebe ve Finansman Uygulamaları
4. Tüketici Şikayetleri Sistemi
5. Merkezi işletim sistemleri yönetimi ve bakımı
6. Merkezi VTYS yönetimi ve bakımı
7. Web ve e-posta hizmetleri
8. Ağ ve bilgi güvenliği

olarak sıralanabilir.

Bu süreçlerin kullandığı bilgi sistemleri bileşenleri ve varlık-süreç risk bağımlılığı tabloları Çizelge 6 ve Çizelge 7'de verilmiştir. Bu tablolar oluşturulurken nicel ve nitel yöntemler için birer örnek verilmiştir. Analiz çalışması sırasında belirli risk kriterlerine ve iş sürekliliğini etkileme olasılıklarına karşı çeşitli düzeylerde risk atamaları yapılmıştır. Risk hesaplama formülü direkt olarak kullanılmamıştır. Bunun gerekçeleri ise hesaplama terimleri içinde literatürde verilen bir yıllık süre içinde bir tehdidin gerçekleşme sıklığı terimi sağlıklı olarak kurumların elinde genellikle hazır değildir. Bu tür istatistiksel verileri toplamak uzun süre alacağı ve kurumlarda hazır veri bulunmaması açısından matematiksel ifadeler başlangıçta efektif olarak kullanılamamaktadır. Ayrıca varlık değerleri ancak parasal olarak belirlenebilmektedir. Kurumların iş sürekliliğini kaybetmesi ve geri dönülemez kayıpların getireceği saygınlık ve iş kaybının da ölçülememesi diğer bir sebeptir. Bunun yerine, bileşen ve süreçleri yakından bilen personel, bu varlıkları tehdit edebilecek faktörleri uzun mesleki deneyimler sonucu daha kolaylıkla kestirebilmektedirler. Düzenlenen anketler çerçevesinde süreç sorumluları ile yapılan görüşmeler ışığında örnek olarak Çizelge 6 ve Çizelge 7 oluşturulmuştur. Çizelge 6'da kabul edilebilir risk seviyesi olarak düşük risk seviyesi (%26 - %35 bölgesi) seçilmiştir. Risklere karşı alınan önlemleri ölçmek için, belli bir süre sonra (önerilen en az 1 yıldır) yeniden nicel ve nitel değerlendirmeler yapılırsa riskteki düşüşlerin somut olarak kendiliğinden ortaya çıkacağı beklenmektedir.

KBG için yapılacak risk analiz çalışmaları sırasında yaşanılabilecek güçlükler aşağıda sıralanmıştır. Bu hususlara da dikkat edilmesinde büyük fayda olacaktır.

1. Çalışanlar risklere karşı fazla duyarlı olmayabilirler, çalışanların çoğu genellikle "bu zamana kadar bir şey olmadı, bundan sonra da olmaz" mantığına sahip olabilmektedirler.
2. Çoğu personel sorumluluk almaktan kaçınabilmektedir.
3. Daha önce yaşanan olaylar ve gerçekleşen riskler ayrıntılarıyla kayda geçirilmemektedir.
4. Yöneticilerin ve çalışanların oluşabilecek riskler ve doğabilecek olumsuz sonuçlar hakkında fazla fikirleri olmayabilmektedir.
5. Risk yüzdelerinin nasıl değerlendirileceği veya nitel değerlerin atanmasında baz alınacak metriklerin seçiminde güçlükler yaşanabilmektedir.
6. Birim sorumlularının riskleri tartışmaya ayırabilecekleri zamanları kısıtlı olabilmekte veya konuyu önemseme duyarlılıkları yeterince kuvvetli olmayabilmektedir.
7. Süreçlerin analizi daha karmaşıktır, süreçlerin adımlarını ve aralarındaki ilişkileri tespit edebilmek güç olabilmektedir, analiz çalışmalarının personel tarafından fazla önemsenmemesiyle karşılaşılabilir.
8. Personelin, süreçlerle ilişkili yeni prosedürlere uymak istememe eğilimi güçlü olabilmekte ve eski çalışma alışkanlıklarını koruma eğilimini gösterebilmektedirler.
9. Süreç-Varlık-Risk anlamında daha faydalı ve net görülebilir olması için hangi tabloların oluşturulması gerektiğine karar vermek zor olabilmektedir.
10. Risk hesaplama formüllerinin tümü varsayımlara ve istatistikî değerlere bağlı olması nedeniyle çok kesin bir değerlendirmenin yapılabilmesi hayli zordur, hatta çok kesinlik mümkün değildir.
11. Birimlerde personel değişikliğinin sık yaşanması dolayısıyla sürecin tanımına ait sıkıntılarla karşılaşılabilmektedir.

Karşı önlemlerin geliştirilmesi aşamasında da güçlüklerle karşılaşılabileceği unutulmamalıdır. Tehditler ve risklere karşı kurumun bilgi sistemlerinin durumu ortaya çıktıktan sonra, bu zayıflıkların tehditlerden etkilenme olasılığını en aza indirmek için karşı önlemleri içeren prosedürler ve talimatlar geliştirilmelidir. Bu geliştirmeler sırasında yaşanabilecek güçlükler aşağıda sıralanmıştır.

1. Varlıklarda sürekli güncellemeler, eklemeler, çıkarımlar ve yer değişiklikleri olduğundan, izlemek için çok çaba ve dikkat gerekmektedir. Bileşenler için geliştirilmiş olan karşı önlemlerde bu nedenle sürekli güncelleme yapılmalıdır.
2. Standardın her bir maddesinin kurumlara birebir uygulanıp uygulanamayacağı konusunda karar vermekte güçlük çekilebilecek hususlar olabilmektedir. Her bir kurumun faaliyet alanı, büyüklüğü ve buna bağlı olarak alınması gereken önlemler standart değildir. İş alanlarının çok çeşitlilik gösterebilmesi açısından, alınacak karşı önlemlerin derinliği ve niteliği de her kurum için çeşitlilik göstermektedir.
3. Kurumlarda sağlıklı olarak uygulanamayacağı kanısına varılan ve daha önce yazılmış olan bazı prosedürlerin iptal edilmesi veya güncellenmesinin çok sıkı takip edilmesi için PUKÖ döngüsünün başlangıçta daha kısa aralıklarla uygulanması gerekmektedir. Bunun için standart uyarınca oluşturulması gereken "Bilgi Güvenliği Grubu"nun gözden geçirmeler için sağlıklı olarak toplanması sırasında katılım sorunları yaşanabilmektedir.

ÇIZELGE 6. NICEL YAKLAŞIMA GÖRE DONANIM RISK BELIRLEME TABLOSU

| **NİCEL YAKLAŞIM ÖRNEĞİ DONANIM RİSK BELİRLEME TABLOSU** | **Donanımlar** | | |
|---|---|---|---|
| **RİSK PUANLARI** (1: En Düşük Risk, 5:En Yüksek Risk) (max. 100 puan üzerinden) | | | |
| Riskler sıfıra indirilemez en düşük değer 1, En düşük risk puanı 20 olacaktır. | | | |
| **RİSK YÜZDELERİ** | | | |
| %20 - %25 Çok düşük risk, beyaz<br>%26 - %35 Düşük risk, yeşil<br>%36 - %50 Orta risk, pembe<br>%51- %65 Yüksek risk, turuncu<br>risk yüzdesi > 65 Çok yüksek risk, kırmızı | | | |
| **Risk Tanımları ve Değerleri** | **A** | **B** | **C** |
| **1-Fiziksel Konum** | | | |
| Kart Girişli Bölüm (1),<br>Anahtarlı Bölüm/ Sadece Görevli Girebilir (2),<br>Anahtarlı Bölüm/Diğer Personel Girebilir (3),<br>Anahtarsız Bölüm (4),<br>Serviste Açık Ortamda (5) | 3 | 3 | 3 |
| **2-UPS** | | | |
| Var (1) , Yok (5) | 1 | 1 | 1 |
| **3-Jeneratör** | | | |
| Var (1), Yok (5) | 5 | 1 | 1 |
| **4-Klima** | | | |
| Var (1), Yok (5) | 1 | 1 | 1 |
| **5-Kümeleme (Donanımsal/Yazılımsal)** | | | |
| Var (1) , Yok (5) | 5 | 5 | 5 |
| **6-RAID (Donanımsal/Yazılımsal)** | | | |
| Var (1) , Yok (5) | 5 | 1 | 1 |
| **7-Kritiklik (ref:Donanım Varlıkları Tablosu)** | | | |
| Yüksek (5), Orta (3), Düşük (1) | 5 | 5 | 5 |
| **8-Yedeklerin Saklandığı Ortam** | | | |
| Yanmaz Kasa (1),<br>Ayrı Binada/Özel Bölümde (2),<br>Ayrı Binada/Açık Bölümde (3),<br>Sistem Odası/Açıkta (4),<br>Serviste/Açıkta (5) | 4 | 4 | 4 |
| **9-TEMPEST** | | | |
| Var (1) , Yok (5) | 5 | 5 | 5 |
| **10-YANGIN** | | | |
| Alarm/Otomatik Söndürme Var (1), Manuel Söndürme/Yangın Tüpü (3), Önlem yok (5) | 5 | 1 | 1 |
| **11-Bakım Anlaşması** | | | |
| Var (1) , Yok (5) | 1 | 1 | 1 |
| **12-Patch(Yama) Takibi** | | | |
| SUS Sunucu ile Oto. (1),<br>Dönemsel/ Uyarı Geldikçe (3),<br>Takip edilmiyor (5) | 3 | 3 | 3 |
| **13-Root/Administrator Şifre Değişim Sıklığı** | | | |
| Her gün(1), Her hafta(2)<br>Her ay(3), Her 3 ay(4),<br>Gelişigüzel(5) | 4 | 4 | 4 |
| **14- Şifre Değişim Yöntemi** | | | |
| Çözülmesi zor şifre (1),<br>Gelişigüzel, çözülmesi kolay şifre (3),<br>Birden fazla kişinin bildiği, korunmayan şifre(5) | 3 | 3 | 3 |
| **15-Kolayca Yerine Koyulabilir mi?** | | | |
| Para ile satın alınabilir (1),<br>Satın alınabilir,çok pahalı (3),<br>Satın alınsa bile bilgiler/prestij kaybedilir (5) | 5 | 5 | 5 |
| **16-Güvenlik Duvarı** | | | |
| Firewall var mı?<br>Evet (1) / telnet,ftp,smtp, snmp,NAT, Virüs Koruma, Hayır (5) | 1 | 1 | 1 |
| **17-Bakım Firmalarının Erişimi** | | | |
| Sözleşme var (1)/yok(2), VPN'li giriş(3), VPN'siz(4), Root/admin ile(5) | 2 | 2 | 2 |
| **18-Üzerindeki Uygulamanın Kritiklik Seviyesi** | | | |
| (ref:Yazılım Varlıkları Tablosu-Donanım ile Üzerindeki Uygulama İlişkisi) Yüksek (5), Orta(3), Düşük (1) | 5 | 5 | 5 |
| **19- Donanımsal Yedek Varsa Bulunduğu Yer** | | | |
| Farklı şehirde (1)/ Aynı şehir, farklı semt (2)/ Aynı bina, farklı kat (3)/Aynı bina ve servis,farklı bölüm (4), Yok (5) | 5 | 5 | 5 |
| **20-Yetkili Personelin Niteliği (ref:Donanım Varlıkları Tablosu)** | | | |
| İleri Düzeyde Eğitimli (1),<br>Orta Düzeyde eğitimli (3),<br>Eğitimi yeterli değil (5) | 1 | 3 | 3 |
| **TOPLAM RİSK DEĞERİ** | 69 | 59 | 59 |
| **RİSK YÜZDESİ** | **0.69** | **0.59** | **0.59** |

1:Çok Düşük Risk, 2:Düşük Risk, 3:Orta Risk, 4:Yüksek Risk, 5:Çok Yüksek Risk

ÇIZELGE 7. SÜREÇ-VARLIK İLIŞKISI ANLAMINDA TOPLAM RISK

| **Bilgi Sistemleri Süreç Adı** | **İlgili Donanım ve Riski** | **İlgili Uyg. Yazılımı ve Riski** | **Süreç Topl. Riski** |
|---|---|---|---|
| X Uygulama Süreci | D1**(ÇYR)** | Y1 Yazılımı **(ÇYR)** | **ÇYR** |
| | D2**(ÇYR)** | Konsol Yazılımı**(ÇYR)** | |
| | D3**(ÇYR)** | Y2**(ÇYR)** | |
| | D4**(ÇYR)** | Y3**(ÇYR)** | |
| | D5**ÇYR)** | Y4**(ÇYR)** | |
| | D6**(ÇYR)** | Y5**(ÇYR)** | |
| | D7**(DR)** | - | |
| | Yönlendiriciler**(ÇYR)** | - | |
| | Modemler**(YR)** | - | |
| | Anahtarlar**(YR)** | - | |
| Muh. ve Finansman Süreci | D4**(ÇYR)** | Y3 **(ÇYR)** | **ÇYR** |
| Personel Takip/Bordro Süreci | D4**(ÇYR)** | Y5**(ÇYR)** | **ÇYR** |
| | Yönlendiriciler**(ÇYR)** | - | |
| | Modemler**(YR)** | - | |
| | Anahtarlar**(YR)** | - | |
| Tüketici Şikayetleri Süreci | D6**(ÇYR)** | Y6**(YR)** | **YR** |
| | D6**(ÇYR)** | Y8 **(ÇYR)** | |
| | Web Sunucu**(YR)** | - | |

ÇDR: Çok Düşük Risk, DR: Düşük Risk, OR: Orta Risk, YR: Yüksek Risk, ÇYR: Çok Yüksek Risk,
D: Donanımlar, Y: Yazılımlar

## VII. KURUMUN GÜVENLIK DÜZEYININ STANDARDIN MADDELERINE GÖRE KONTROLÜ

Bir kurum kendi içerisinde standardı uygulamadan önce, standardın şart koştuğu ana ve detay maddelerle kurumda mevcut olan yapı ve uygulamaların ne kadar örtüştüğünü belirleyebilmektedir. Bunun için örnek kontrol listesini kullanarak kurumun ne durumda olduğunun fotoğrafının ortaya konulması, güvenlik açısından kurumun hangi seviyede olduğunu somut olarak göstermesi bakımından önemli bir çalışmadır [7]. Çizelge 8'de bu denetim listesi için "Varlıkların Envanteri" adlı standart maddesini içeren bir değerlendirme örneği verilmektedir. Çizelge 8'den de görülebileceği gibi, kurumun envanter çalışması seviyesi standardın istediği şekilde değildir ve dolayısıyla burada örnek verilen kurum standartla uyumsuz bir yapı içerisindedir. Denetim listesinde bulunan her madde titizlikle takip edilirse bu kurumun standartla uyum derecesi ortaya çıkarılabilir.

ÇIZELGE 8. KBG ÇIZELGESI ÖRNEĞI (VARLIK SINIFLANDIRILMASI VE DENETIMI)

| **A Kurumu - Bilgi Güvenliği Yönetimi TS ISO/IEC 2700 Denetim Listesi** | | | | | |
|---|---|---|---|---|---|
| Referans | | Denetim Alanı, Amaçlar ve Soru | | Sonuçlar | |
| Kontrol Listesi | Standart 27001 | Bölüm | Denetim Sorusu | Bulgular | Uyum |
| Varlık Sınıflandırması ve Denetimi | | | | | |
| 3.1 | 5.1 | **Varlıklar İçin Sorumluluk** | | | |
| 3.1.1 | 5.1.1 | Varlıkların Envanteri | Her bir bilgi sistemi ile ilişkili önemli varlıkların kayıt veya envanterleri var mı? Her bilgi varlığının güvenlik sınıfı, yeri ve sahibi var mı? | Envanterler çok sağlıksız bir şekilde ve eksik tutulmakta<br>Hayır | Uyumsuz |

Bunun sonucu olarak, standardın ana maddelerini içeren bir ISO/IEC 27001 Standardına Uygunluk Düzeyi Çizelgesi hazırlanarak, kurumun güvenlik standardına uygunluk derecesinin toplam görüntüsü belirlenmelidir.

Çizelge 9'da Uygunluk Düzeyi Çizelgesi için bir örnek verilmektedir. Bu örnekte görüldüğü gibi, kurum bir an önce standardı uygulayarak güvenlik düzeyini acilen yukarı seviyelere çekmek zorundadır. Bu tür somut tespitler, kurum üst yönetiminin de konuyu ve işin aciliyetini algılayabilmeleri açısından büyük önem taşımaktadır.

ÇIZELGE 9. KURUMUN STANDARDA UYGUNLUK DÜZEYI ÇIZELGESI

| **- Kurum Bilgi Sistemleri - ISO/IEC 27001 Standardına Uygunluk Düzeyi Çizelgesi** | | | | | |
|---|---|---|---|---|---|
| Ana Maddeler | Çok İyi | İyi | Kritik | Zayıf | Çok Zayıf |
| Güvenlik Politikası | | | | | **X** |
| Örgütsel Güvenlik | | | | | **X** |
| Varlık Sınıflandırması ve Denetimi | | | | | **X** |
| Personel Güvenliği | | | | | **X** |
| Fiziksel ve Çevresel Güvenlik | | | | **X** | |
| İletişim ve İşletim Yönetimi | | | **X** | | |
| Erişim Denetimi | | | **X** | | |
| Sistem Geliştirilmesi ve Sürekliliğinin Sağlanması | | | **X** | | |
| İş Sürekliliği Yönetimi | | | | | **X** |
| Uyum | | | | | **X** |

## VIII. SONUÇ VE DEĞERLENDIRMELER

Bu çalışmada sunulan nicel/nitel risk belirleme yaklaşımları ve süreç-varlık ilişkisi örneklerinde açıkça görüldüğü gibi, kurumlar için örnekleri sunulan bilgi sistemleri genelde yüksek risk altındadır. Nicel ve nitel değerlendirmelerin birbirine çok yakın olması da doğruluğun sağlanması açısından önemli bir gösterge olmaktadır. Değerlendirmelerde kullanılan risk kriterleri çizelgelerde bilgi olarak yer almaktadır. Bu çalışmalar sonucunda oldukça somut olarak belirlenen yüksek risk seviyesi bir kurum için iş süreçlerinde kesintilere, büyük iş kayıplarına, geri dönülemeyecek bilgi kayıplarına, büyük prestij ve müşteri kaybına ve bazen de büyük maddi kayıplara sebebiyet verebilecektir. Bu çalışmada sunulan veriler ışığında böyle bir sonuç elde eden bir kurumun en kısa sürede "Bilgi Güvenliği Yönetim Sistemi"ni oluşturması gerektiği ortadadır.

Bu çalışmada sunulan hususlara ilave olarak;

- Güvenliğin bir süreç olduğu, sürekli bir takip ve iyileştirme gerektirdiği
- İnsan faktörünün çok önemli olduğu
- Güvenliğin sadece donanım ve yazılımlarla sağlanamayacağının farkında olunması eğitim ve bilgilendirmenin öneminin her zaman hatırda tutulmasının gerektiği,
- Yüksek seviyede bilgi güvenliğinin sağlanmasında teknoloji (yazılım-donanım), eğitim ve insan faktörünün her zaman birbirini destekleyen unsurlar olduğu,
- Standartların uygulanması ve denetlenmesi,
- Güncel açıklar sürekli olarak takip edilmeli ve sistemde bu tür açıkların bulunup bulunmadığı denetlenmeli,
- Sızma testlerinin belirli periyotlarda tekrar yapılması ve tespit edilen zafiyetlerin kısa sürede giderilmesi

gerekmektedir.

Uygulama açısından değerlendirildiğinde, kurumsal bilgi güvenliği standartlarının bir kuruma uygulanması, istenilmeyen ve beklenilmeyen pek çok problemi de beraberinde getirebilecektir. Kurumsal bilgi güvenliğini uygulamak isteyen kurum ve kuruluşların, önünde uzun ve zaman alıcı bir süreç olduğu, başlangıçta planlarken bunun dikkate alınması, kurum bilişim kültürünün yaygın ve yeterli olmamasının uygulamayı zorlaştıracağı, eğer bu iş için yeterli eleman görevlendirilmemiş ise ve bu işlerin mevcut iş süreçleriyle birlikte götürülmeye çalışılmasının beklenilmeyen sıkıntılara yol açabileceği de hatırda bulundurulmalıdır.

## KAYNAKLAR

[1] J. Wack, M. Tracy, M. Souppaya, "Guideline on Network Security Testing", p.2-1, NIST, Special Publication 800-42

[2] Gartner Araştırma Kuruluşu, Forecast: Security Software, Worldwide, 2005-2009 (Executive Summary – Norma Schroder) (30.3.2005)

[3] http://www.gartner.com/research/focus_areas/asset_48267.jsp

[4] http://www.infosecurenet.com

[5] ISO/IEC Guide 73:2002, Risk Management, Vocabulary, Guidelines for use in standards

[6] E. Ersoy, "Kurumsal Bilgi Güvenliği Standartları, Kurumsal Analiz ve Telekomünikasyon Kurumu "Bilgi Güvenliği Politikasının Oluşturulması" Uzmanlık Tezi, Ankara, Haziran 2005.

[7] www.cccure.com

[8] V.Thiagarajan, "Information Security Management BS 7799.2:2002 – Audit Check List for SANS", SANS Institute, USA.