T.C.

MARMARA ÜNİVERSİTESİ

BANKACILIK VE SİGORTACILIK ENSTİTÜSÜ

BANKACILIK ANABİLİM DALI

BİLGİ SİSTEMLERİNİN DENETİMİ VE TÜRK BANKACILIK SEKTÖRÜ UYGULAMASI

DOKTORA TEZİ

TEZ DANIŞMANI : DOÇ. DR. ERİŞAH ARICAN

ORKUN İÇTEN
970002

İSTANBUL, 2002

T.C.
MARMARA ÜNİVERSİTESİ
BANKACILIK VE SİGORTACILIK ENSTİTÜSÜ

Aşağıda belirtilen lisansüstü tez, Lisansüstü Öğretim Yönetmeliği hükümlerinde belirtilen esaslar çerçevesinde jüri önünde savunulmuş ve jüri tarafından başarılı bulunmuştur.

TEZ BAŞLIĞI : Bilgi Sistemlerinin Denetimi ve Türk Bankacılık Sektörü Uygulaması

TEZ TÜRÜ : Doktora

TEZİ HAZIRLAYAN : Orkun İÇTEN

ANABİLİM DALI : Bankacılık

SAVUNMA TARİHİ : 13.11.2002

JÜRİ ÜYELERİ :

GÖREVİ	**ADI SOYADI**	**İmza**
Danışman	Doç.Dr.Erişah ARICAN	
Üye	Prof.Dr. İlhan ULUDAĞ	
Üye	Prof.Dr. Niyazi BERK	
Üye	Doç.Dr.Zekai ÖZDEMİR	
Üye	Doç.Dr.Oral ERDOĞAN	

Marmara Üniversitesi Göztepe Kampüsü, Kuyubaşı Kayışdağı Cd. 81040 İSTANBUL / TÜRKİYE
Tel: + 90.418 20 88, + 90. 216.418 20 89 Faks: + 90.216.347 69 51

BİLGİ SİSTEMLERİNİN DENETİMİ VE TÜRK BANKACILIK SEKTÖRÜ UYGULAMASI

İ Ç İ N D E K İ L E R

ŞEKİLLER

T A B L O L A R

G İ R İ Ş

Çağımızdaki teknolojik ilerlemeler sayesinde bilgi sistemleri, organizasyonların fonksiyonlarını yerine getirmesinde vazgeçilemez bir araç haline gelmiştir. Bilgi sistemlerini başarıyla yöneten işletmeler, organizasyonlarının etkinliklerini ve verimliliklerini arttırarak diğer işletmelere göre önemli bir avantaj elde etmektedir. Ancak bilgi sistemlerinin organizasyonlardaki yaygın kullanımı beraberinde bir çok sorunu da beraberinde getirmiştir. Bu sorunlar bilgi sistemlerinin güvenliği, etkinlik ve verimliliği başlıklarında toplanabilir.

Son yıllarda yaşanan bilişim teknolojilerindeki ilerlemeler ve internetin tüm dünyada yaygınlaşması organizasyonların bilgi sistemleri güvenliği sorunuyla karşı karşıya kalmalarına neden olmuştur. Bu nedenle tüm işletmeler, bilgi sistemlerinin dizayn edilmesinde ve faaliyetlerini sürdürmesinde güvenliğe öncelik vermişlerdir.

Güvenliğin yanında bilgi sistemlerine ait kaynakların organizasyonun amaçlarına uygun ulaştırıcı nitelikte olması yani bilgi sistemlerinin etkinliğinin sağlanması ve kullanılan kaynaklarla bilgi sistemlerinden elde edilen çıktılar arasındaki ilişki yani verimliliğin elde edilmesi organizasyonların bilgi sistemleriyle ilgili yapılan çalışmaların başında yer almaktadır.

Bilgi sistemleri güvenliğinin, etkin ve verimliliğinin sağlanmasında düzenli kontrol çalışmalarının yanında denetim çalışmalarının sürdürülmesi organizasyonlara hizmet eden önemli bir araç olarak görev yapmaktadır. Geleneksel denetim disiplini altında son yıllarda ayrı bir disiplin haline gelen bilgi sistemleri denetimi, organizasyonlarının fonksiyonlarında bilgi sistemlerini yaygın olarak olarak kullanan işletmeler için vazgeçilmez bir unsur haline gelmiştir.

Ülkemizde ve dünyadaki tüm bankacılık sektöründe faaliyet gösteren bankalar için bilgi sistemleri vazgeçilmez bir unsur haline gelmiş ve bankalar neredeyse fonksiyonlarının tamamını bilgi sistemleri aracılığı ile yerine getirmeye başlamışlardır. Günümüzde internet bankacılığı bunun en güzel örneğidir. Bankaların ekonomideki önemli fonksiyonu ve bilgi sistemlerinin bankalar için önemi

düşünüldüğünde bilgi sistemlerinin denetiminin bankacılık sektöründeki önemi bir kat daha artmaktadır. Özellikle ülkemizde bilgi sistemlerinin güvenliği, etkin ve verimliliği ile ilgili kamusal herhangi bir düzenlemenin yapılmadığı düşünüldüğünde, ülkemizdeki bankaların bilgi sistemleri açısından önemli risk altında olduğu düşünülebilir.

Türk Bankacılık Sektörü'nün bilgi sistemleri açısından risk taşıdığı tezinden hareketle, bu doktora çalışmasında bilgi sistemleri denetimi ve Türk Bankacılık Sektörü uygulaması incelenmiştir.

Çalışmanın birinci bölümünde bilgi sistemlerine ait temel kavramlara yer verilerek, bu kavramların açıklamalarına yer verilmiştir.

Çalışmanın ikinci bölümünde ise bilgi sistemlerinin denetiminin teorik alt yapısı anlatırılırken, bilgi sistemlerinin güvenlik, etkinlik ve verimlilikle ilgili temel denetim uygulamaları açıklanırken, aynı zamanda bilgi sistemleri denetimi planlaması ve risk ölçümü, denetim dökümantasyonu ve denetim kanıtlarının hazırlanması aşamalarına da yer verilmiştir.

Çalışma sırasında bilgi sistemleri güvenliğinin, bilgi sistemleri etkinlik ve verimliliği açısından bankacılık sektörü açısından daha önemli bir risk kaynağı olması nedeniyle, çalışmanın üçüncü bölümünde bir risk ölçüm aracı olarak bilgi sistemleri güvenlik endeksi kurulmuş ve Türk Bankacılık Sektörü uygulamasına yer verilmiştir.

Güvenlik Endeksi Euripdis Loukis ve Diomidis Spinellis tarafından Yunan Kamu Sektörü'nde Bilgi Sistemleri Güvenliği konulu makalesinden modellenerek alınmıştır. Söz konusu güvenlik endeksinin kurulmasında bankacılık sektöründen seçilmiş bankalara anket formları gönderilerek, gelen cevaplar değerlendirilmiştir. Değerlendirme sonucunda Türk Bankacılık Sekörü'nün genel güvenlik endeksi ortaya çıkarılmış ve Türk Bankacılık Sektörü'nün güvenlik açısından zayıf yönleri tespit edilerek açıklanmıştır.

Çalışmanın son bölümü olan sonuç ve değerlendirme bölümünde ortaya çıkartılan güvenlik endeksi sonucunun yorumlaması yapılmış ve güvenlik konusunda Türk Bankacılık Sektörü'nün zaaflarıyla ilgili olarak yapılması gereken iyileştirici çalışmalar açıklanmıştır.

Bu çalışmanın baştan sona şekillenmesine ait aşamalarda özverili bir şekilde katkılarını ve emeğini esirgemeyen tez danışmanım ve hocam Sn.Erişah ARICAN'a, enstitümüzün bugüne gelmesinde sonsuz çaba sarfeden ve kendisinden her aşamada istifade ettiğim hocam Sn. İlhan ULUDAĞ'a ve lisanstan bu yana kendisinden çok istifade ettiğim ve feyz aldığım hocam Sn. Nazım EKREN'e sonsuz teşekkürlerimi sunarım

Orkun İÇTEN

İstanbul, 30.09.2002

BİLGİ SİSTEMLERİNİN DENETİMİ VE TÜRK BANKACILIK SEKTÖRÜ UYGULAMASI

1. BİLGİ SİSTEMLERİ DENETİMİNİN KAVRAMSAL ÇERÇEVESİ

1.1. Bilgi

Bir organizasyonun temel ve en önemli kaynağı olan bilgi, bir organizasyon içinde kararların alınması, olaylara ait kayıtların tutulması, geleceğe ait planların yapılması ve iletişim aktivitelerinde kullanılmaktadır. Bilgi, günümüzde onu yönetmek için istihdam edilen insan kaynaklarından ve bilginin saklanması ve ona katkıda bulunması için kullanılan bilgisayarlardan çok daha büyük bir önem arz etmektedir. Bir organizasyonda kullanılan bilgi, organizasyon büyürken genişleyerek büyümekte ve hatta organizasyonun büyümesinin önüne geçmektedir.

1999 yılında Reuters tarafından yapılan bir araştırmada, araştırmaya katılan işletme çalışanlarının,

a) %25'i bilginin en önemli varlıkları olduğunu,
b) %50'si bilginin markalarından ve ünvanlarından daha önemli olduğunu,
c) %40'ı bilginin binalarından ve nakit varlıklarından daha önemli olduğunu,
d) %50'si bilgilerinin en az 100.000 USD değerinde olduğunu,
e) %40'ı ise kaybolan bilgilerinin yerine getirilmesi için en az bir ay ilave olarak çalışmaları gerektiğini

belirtmişlerdir. [1]

[1] John Silltow, "Information Management (1)", ITAUDIT.ORG, March 15, 2001, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Bilgi kelimesinin kökenleri araştırıldığında temel olarak iki kavram göze çarpmaktadır. Bu kavramlar Data (Veri), ve Information'dır (Bilgi). Data kelimesi datum kelimesinin çoğuludur ve bu kelime dilimizde veri kelimesinin karşılığı olarak kullanılmaktadır. Data, genel olarak fiziki bir oluşun veya iş süreciyle ilgili ham gerçekler ve gözlemlerdir. Örneğin bir müşterinin banka hesabı açması, bu olayı tanımlayan bir çok veri meydana getirmektedir. Daha spesifik olarak veri, insan, yer ve olaylar gibi varlıkların özelliklerine ait objektif ölçümlerdir.[2]

Veri ve bilgi kelimeleri sıklıkla birbiri yerine kullanmaktadır. Bununla birlikte, veri'nin tamamlanmamış ve bilgi ürünlerine dönüştürülen hammadde olarak görülmesi daha anlamlı olacaktır.

Bilgi, spesifik kullanıcılar için anlamlı içeriğe dönüştürülmüş veri olarak tanımlanabilir. Bu nedenle veri, bilgiye dönüşürken artı değer ekleme sürecinde işlenmektedir. Bu sürece bilgi işlem süreci denilmektedir. Bu süreçte, veri organize edilmekte, çoğaltılmakta, değiştirilmekte, içeriği analiz edilmekte ve kullanıcılar için anlaşılır içeriğe dönüştürülmektedir. Bu nedenle bilgi, içeriği ile kullanıcılara değer sunan bilgi işlem sürecinden geçmiş veri olarak kabul edilmektedir. Aşağıdaki şekilde verinin bilgiye dönüşme süreci görülmektedir.

Şekil 1.1.
Veri ve Bilgi İlişkisi

Kaynak: James A. O'Brien, "Introduction to Information Systems", Eighth Edition, 1997, s.24

[2] A. S. Hornby, Christina Ruse, Oxford Student's Dictionary of Current English, Oxford University Press, Oxford, 1992

1.2. Bilgi Sistemleri

Sistem; birleştirilmiş bir bütün oluşturan birbiriyle ilgili elementler grubudur. Sistemler, insan topluluklarından, modern teknolojilere, biyoloji ve fizik bilim dallarına kadar bir çok yerde karşımıza çıkmaktadır.

Bu nedenle güneşin fiziki sisteminden ve gezegenlerden, insan vücudunun biyolojik sisteminden, petrol rafinerisinin teknolojik sisteminden ve organizasyonunun sosyo ekonomik sisteminden bahsetmek mümkündür. Bununla birlikte, aşağıda söz edilecek sistem tanımı, bilgi sistemini açıklayan daha uygun bir tanım sağlamaktadır.

Sistem, organize edilmiş dönüşüm süreci içinde girdi ve çıktı üretimi ile genel bir amaca doğru hep birlikte çalışan birbiriyle ilişkili elementler grubudur. Böyle bir sistem karşılıklı etkileşim içinde bulunan elementlerden veya fonksiyonlardan meydana gelmektedir.[3]

Sistem içinde,

a) Girdi
b) İşlem
c) Çıktı

olmak üzere üç temel kavram dikkati çekmektedir.

Girdi; İşleme tabi tutulmak amacıyla sisteme dahil edilen veya bunun için saklanan elementlerdir. Örneğin hammadde, veri ve insan eforu birer girdidir.

İşlem; Girdiyi çıktıya dönüştüren bir süreçtir. Örneğin üretim süreci, insanın solunum süreci birer işlemdir.

---

[3] James A. O'Brien, Introduction to Information Systems, Eighth Edition, 1997, p.18

Çıktı; Dönüşüm süreci tarafından meydana getirilen dönüşüm elementleridir. Örneğin üretilmiş ürünler, insan hizmetleri, yönetim bilgisi birer çıktıdır.

Sistem kavramına iki ek kavram ilave edildiğinde bilgi sistemlerinin açıklanması açısından daha faydalı olacaktır. Bu kavramlar;

a) Geri iletim(feedback)
b) Kontroldür.

Geri İletim; Bir sistemin performansı ile ilgili verilerdir. Örneğin, satış performansıyla ilgili veriler satış müdürü için bir geri beslemedir.

Kontrol; Bir sistemin amaçlanan sonuca doğru gidip gitmediği konusunda veriler elde etmek amacıyla yapılan gözlemler ve değerlendirmelerdir. Kontrol, bir sistemin tam ve doğru çıktıları ürettiğini garantilemek amacıyla sistemin girdi ve işlem elementleri için gerekli ayarlamaların yapılmasıdır. Örneğin bir satış müdürünün, satış performansıyla ilgili geri iletimleri değerlendirerek, yeni satış alanlarına yeni satış personellerini atarken yaptığı işlemler kontrol çalışmaları olarak değerlendirilebilir.[4]

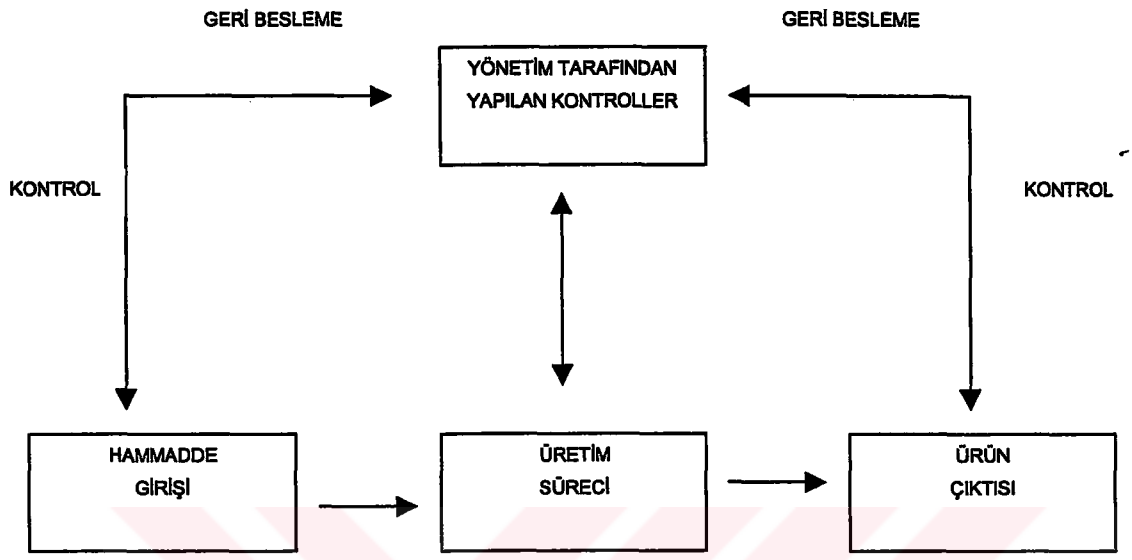
Geri besleme kontrol fonksiyonun ayrılmaz bir parçası olduğu için, genellikle kontrol kavramının bir parçası olarak algılanmaktadır. Geri besleme ve kontrol, girdilerin tam ve doğru çıktılara dönüştüğünü ortaya koyarak, sistemin amacına ulaşabilmesi konusunda bir organizasyona önemli katkılar sağlamaktadır.

Bir üretim sistemi, yukarıda sözü edilen sistem elementlerinin nasıl çalıştığını daha iyi ifade edebilecektir. Üretim sistemi hammaddeyi girdi olarak kabul ederken, tamamlanmış malları çıktı olarak üretmektedir. Bir bilgi sistemi ise girdi olarak veri'yi (data) kabul eder ve onları bilgi üretim sürecinden geçirdikten sonra bilgi'ye (information) dönüştürür. Bu bilgi sistemi için çıktıdır. Aşağıdaki şekil bir üretim sisteminin çalışma sistematiğini göstermektedir.

---

[4] Oktay Alpugan, M Hulusi Demir, Mete Oktav, Nurel Üner, İşletme Ekonomisi ve Yönetimi, Beta Yayınevi, İstanbul, 1995, s. 187

ŞEKİL 1.2.
Üretim Sistemi



Kaynak: James A. O'Brien, "Introduction to Information Systems", Eighth Edition, 1997, s.19

Yukarıdaki şekil bilgi sistemlerinin tam olarak anlaşılması için genel sistem karakteristikliklerini vurgulamaktadır. Bir sistem asla bir vakumun içinde var olmamakta ve diğer sistemleri de içeren bir çerçevede faaliyetlerini sürdürmektedir. Şayet söz konusu sistem daha geniş bir sistemin elementlerinden biriyse, bu sistem bir altsistemdir. Daha geniş sistem ise bu sistemin çevresidir. Aynı zamanda, sistem sınırı bir sistemi çevresinden ve diğer sistemlerden ayırmaktadır.

Bir çok sistem aynı çevreyi paylaşmaktadır. Bu sistemlerden bazıları diğer sistemlerle komşu olmakta ve aynı sınırı paylaşabilmektedir. Yukarıdaki şekil açık bir sistemi göstermektedir ve çevresindeki diğer sistemlerle karşılıklı iletişim halindedir. Bu sistem çevresiyle girdi ve çıktı alış verişinde bulunmaktadır.

Bilgi sistemi; bir organizasyonda bilginin toplanmasını, biçim değiştirmesini ve dağıtımını sağlayan iletişim ağı, yazılım, donanım ve insanların organize edilmiş bir kombinasyonudur. Bilgi sistemlerinin temel olarak beş ana bileşeni vardır.

a) İnsan
b) Bilgi
c) Yazılım
d) Donanım
e) İletişim Ağları

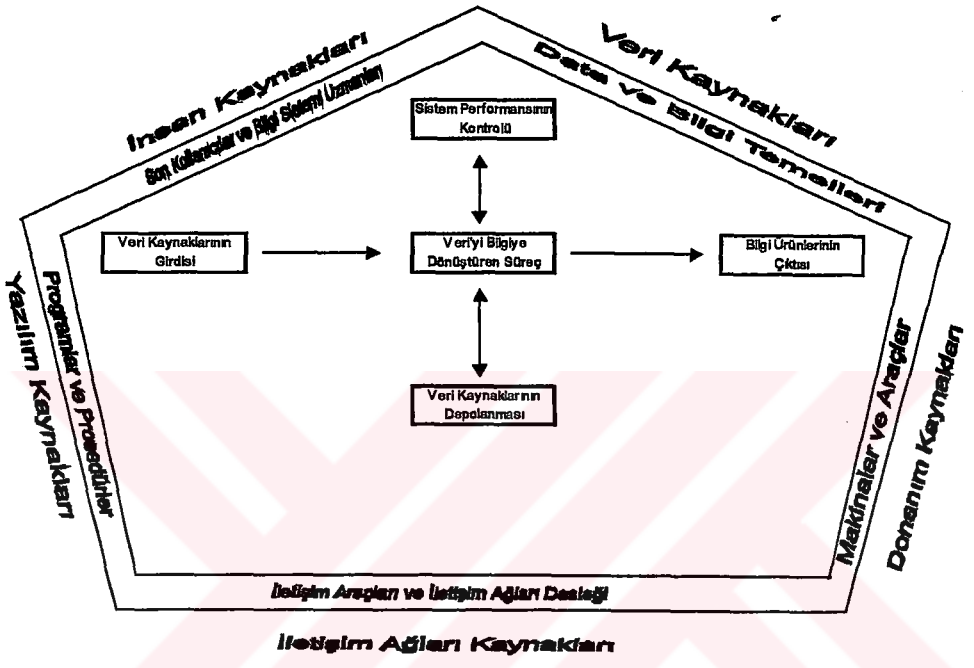
Günümüzde bilgi sistemleri basitten karmaşık donanımlı olanlara kadar çeşitli şekillerde karşımıza çıkmaktadır. Örneğin kalem ve kağıda dayanan bilgi sistemleri olduğu gibi konuşmaya dayalı bilgi sistemleri de mevcut bulunmaktadır. Ancak bu çalışmada bilgi sistemi denildiğinde, bilgi kaynaklarını bilgi ürünlerine dönüştürmede bilgisayar donanımları, bilgisayar yazılımları, iletişim ağları, bilgisayar tabanlı yönetim teknikleri ve bilgi teknolojilerini kullanan bilgisayar tabanlı bilgi sistemleri anlaşılmalıdır.

Günümüz organizasyonları içinde bilgi sistemleri temel olarak üç önemli işlevi yerine getirir. Bunlar;

a) İş operasyonlarının desteklenmesi,
b) Yönetimsel karar verme sürecinin desteklenmesi,
c) Stratejik rekabetsel avantajın desteklenmesi,

Bilgi sistemleri, iş sürecinin aksatılmadan kolaylıkla yürütülmesinin yanında, bilgilere kolay ulaşmada sağladığı avantajlar ve bu bilgilerin yorumlanabilir halde olmasıyla yönetimsel karar verme sürecinde ve stratejik anlamda rekabetsel avantaj sağlama konularında da organizasyonlara destek sağlamaktadır.

Şekil 1.3.
Bilgi Sistemi Modeli



Kaynak: James A. O'Brien, Introduction to Information Systems, Eighth Edition, 1997, p.21

Yukarıdaki şekil, bilgi sistemleri aktiviteleri ve temel elementleri ile ilgili genel yapıyı gösteren bir bilgi sistemi modelini göstermektedir. Bir bilgi sistemi, insan kaynaklarını (kullanıcılar ve bilgi sistemi uzmanları), donanımı (makinaları ve araçları), yazılımları (programları ve prosedürleri), veri'yi (veri ve bilgi tabanlarını) ve iletişim ağlarını (iletişim araçları ve iletişim ağı destekleri), veri kaynaklarını bilgi ürünlerine dönüştüren, girdi, işlem, çıktı, depolama ve kontrol aktivitelerini yerine getirmek için kullanılmaktadır.

1.2.1 Bilgi Sistemi Kaynakları

Yukarıda söz edilen bilgi sistemi modelinde, bilgi sistemlerinin temel olarak insan, donanım, yazılım, veri ve iletişim ağları olmak üzere beş ana kaynağı olduğu görülmektedir.[5]

1.2.1.1. İnsan

İnsan; tüm bilgi sistemlerinin operasyonları için en temel kaynaktır. İnsan kaynakları kavramı bilgi sistemleri kullanıcılarını ve bilgi işlem uzmanlarını kapsamaktadır. Kullanıcılar bilgi sistemlerini veya bilgiyi kullanan kişilerdir. Bunlar muhasebeciler, satış personeli, mühendisler, tüketiciler ve müdürler olabilmektedir.

Bilgi sistemi uzmanları; bilgi sistemlerini kuran ve işleten kişilerdir. Bunlar, sistem analistleri, programcılar, bilgisayar operatörleri, bilgi işlem yöneticileri, teknisyen ve diğer bilgi sistemi personelidir.

1.2.1.2. Donanım

Donanım; bilgi sürecinde kullanılan tüm fiziki araçları ve materyalleri kapsamaktadır. Bunlar sadece bilgisayar, hesap makinesi gibi makinalar değil aynı zamanda tüm veri araçları ve kayıt yapmaya yaran görünür cihazlardır. Örneğin kağıtlar ve manyetik diskler bu tür donanım kaynaklarıdır.

Bilgisayar sistemleri merkezi işlem üniteleri ve yüzeysel birbirine bağlı gereçlerden meydana gelmektedir. Örneğin geniş mainframe bilgisayar sistemleri, midrange bilgisayar sistemleri ve micro bilgisayar sistemleri, bilgisayar sistemleridir. Yazıcılar, mouse, keyboard, magnetik veya optikal diskler gibi araçlar bilgisayar donanımları arasındadır.

---

[5] James A. O'Brien, a.g.k., p.18.,

1.2.1.3. Yazılım

Yazılım kaynakları tüm bilgi işlem direktiflerini kapsamaktadır. Yazılım kaynakları, sadece bilgisayar donanımını yöneten ve programlar olarak anılan operasyonel direktifleri değil aynı zamanda çalışanlar tarafından ihtiyaç duyulan ve prosedür olarak anılan bilgi işlem direktiflerini de içermektedir.

Yazılım kaynaklarına en güzel örnekler sistem ve uygulama yazılımları ve prosedürleridir. Sistem yazılımları; Bir bilgisayar sisteminin operasyonlarını destekleyen ve kontrol eden programlardır. Uygulama yazılımları; kullanıcılar tarafından kullanılan spesifik bir amaca hizmet eden programlardır. Prosedürler; Bilgi sistemini kullanan kişiler için operasyonel direktiflerdir. Örneğin bir kağıt formun doldurulması veya bir programın kullanımıyla ilgili direktifler prosedürlere örnek olarak verilebilir.

1.2.1.4. Veri

Veri; bilgi sisteminin hammaddesi olmaktan çok daha fazla şeyi ifade etmektedir. Veri tanımı, yöneticiler ve bilgi sistemleri uzmanları tarafından genişletilmiştir. Onlar veri'nin değerli bir organizasyonel kaynağı meydana getirdiğini ifade etmektedir. Bu nedenle veri, bir organizasyondaki tüm kullanıcıların fayda elde etmesi için yönetilmesi gereken önemli bir kaynak olarak görülmelidir.

Veri değişik şekillerde olabilmektedir. Örneğin iş süreciyle ilgili ve diğer olay ve olgularla ilgili harf ve rakamları içeren nümerik veriler, yazılı iletişimi sağlayan cümle ve paragrafları içeren yazılı veriler, grafik ve şekilleri içeren imaj veriler ve insan ve diğer sesleri içeren sesli veriler bir organizasyon içinde karşımıza çıkabilmektedir.

Bilgi sistemlerinin veri kaynakları genel olarak aşağıdaki şekilde sınıflandırılabilmektedir.

a) Veri Tabanları; Süreçten geçmiş ve organize edilmiş verileri depolamakta ve saklamaktadır.

b) Bilgi Tabanları; Çeşitli konularla ilgili sonuç çıkarma kuralları ve gerçekleri olarak tutulan çeşitli bilgi formlarını ifade etmektedir. Örneğin, satış işlemleriyle ilgili veriler günlük, haftalık ve aylık olarak yönetime satış analiz raporu olarak sunulmak ve işlenmek üzere satış veri tabanında biriktirilmektedir. Bilgi tabanı ise spesifik bir konu üzerine kullanıcılara uzman araçlar veren ve uzman sistemler olarak anılan veri kaynaklarıdır.

1.2.1.5. İletişim Ağı

İletişim ağları; Modern organizasyonların ve onların bilgisayar tabanlı bilgi sistemlerinin operasyonları için vazgeçilmez bir konuma sahip bulunmaktadır. İletişim ağları, bilgisayarlardan, son kullanıcı terminallerinden, iletişim sağlayan cihazlardan ve iletişim yazılımları tarafından kontrol edilen diğer iletişim araçlarından meydana gelmektedir.

İletişim ağları kaynaklarının, iletişim araçları ve iletişim ağları destekleri olmak üzere iki ana unsuru bulunmaktadır.

a) İletişim araçları; Fiber optik kabloları, mikrodalga sistemleri ve uydu iletişim sistemlerini içermektedir.

b) İletişim ağları destekleri; Bir iletişim ağı kullanımlarını ve operasyonlarını destekleyen veri kaynaklarını, yazılımları, insanları ve donanımları içermektedir. Örneğin modemler, iletişim kontrolünü sağlayan internet erişim paketleri gibi programları iletişim ağları destekleridir.

1.2.2. Bilgi Sistemi Faaliyetleri

Tüm bilgi sistemlerinde temel olarak;

a) Girdi
b) İşlem
c) Çıktı
d) Depolama
e) Kontrol

aktiviteleri bulunmaktadır.[6]

1.2.2.1. Veri Girdi Aktiviteleri

İş ve diğer olaylar hakkındaki veriler, kaydetme ve düzenleme gibi veri giriş faaliyetleri ile veri işlem sürecine hazırlanmaktadır. Veri girdi aktivitelerinde kullanıcılar genel olarak işlemlerle ilgili bilgileri kağıt gibi fiziki araçlara kaydederek veya direkt olarak bilgisayara girmektedir. Bu aktivitelerde genellikle girilen veri'nin doğru olarak kaydedilip kaydedilmediğini belirlemek için çeşitli gözden geçirme çalışmaları da gerçekleştirilmektedir .

Veriler manyetik disk veya teyp gibi makine tarafından okunabilir ve aracılara transfer edilebilmektedir. Örneğin satış işlemlerine ait veri kağıt satış sipariş formu gibi kaynak dökümanlara kaydedilebilmektedir. Alternatif olarak satış personeli, satış verilerini bilgisayar klavyesini veya optik tarayıcı araçların kullanımıyla girebilmektedir.

[6] James A. O'Brien, a.g.k., p.25

1.2.2.2. Bilgi İşlem Aktiviteleri

Veri genel olarak hesaplama, karşılaştırma, sıralama, sınıflandırma ve özetleme gibi aktivitlerle düzenlenmektedir. Bu aktiviteler veri'yi organize eder, analiz eder, düzenler ve veri'yi kullanıcılar için bilgiye dönüştürmektedir. Bir bilgi sisteminde, depolanmış herhangi bir bilginin kalitesi, güncelleme ve düzeltme aktiviteleri ile devamlı olarak sağlanmalıdır.

Örneğin, bir satın alma işlemi hakkında alınan veri

a) Satış sonuçlarının toplamına eklenir,
b) Satış standart iskontoları ile karşılaştırılır,
c) Ürün tanıma numaraları esas alınarak sıraya dizilir,
d) Ürün kategorilerine göre sınıflandırılır,
e) Çeşitli ürün kategorileriyle ilgili bilgilerle satış müdürüne sunulur,
f) Son olarak satış kayıtlarının güncellenmesi için kullanılır.

1.2.2.3. Çıktı Aktiviteleri

Çeşitli formdaki bilgiler çıktı aktiviteleri ile kullanıcılar tarafından kullanılmak üzere çeşitli formlara dönüştürülmektedir. Bilgi sistemlerinin amacı sistem kullanıcıları için yeterli bilgi ürünleri üretmektir. Genel bilgi ürünleri, video görüntüleri, kağıt dökümanlar ve sesli mesajlardır. Tüm bunlar, mesajlar, formlar, raporlar, listeler, grafikler ve diğer ürünler sunmaktadır.

Bir organizasyonda çalışırken veya bir toplumda yaşarken bu ürünler tarafından sağlanan bilgiler düzenli olarak kullanılmaktadır. Örneğin, bir satış müdürü bir satış elemanının performansını kontrol etmek için video görüntülerini, telefon tarafından sağlanan sesli mesajları ve aylık satış sonuçlarının çıktılarını incelemektedir.

1.2.2.4. Veri ve Bilgi Depolama Aktiviteleri

Depolama bilgi sistemlerinin en temel fonksiyonudur. Depolama, veri ve bilgilerin daha sonra kullanılmak üzere biriktirildiği bilgi sistemi aktiviteleridir. Örneğin yazılı bir döküman kelimelere, cümlelere, paragraflara ve dökümanlara göre organize edilir. Depolanmış veri genellikle alanlara, kayıtlara, dosyalara ve veri tabanlarına göre organize edilir. Bu aktivite kullanıcıların ihtiyaç duyduğunda istenen bilgileri alarak kullanmasını sağlamaktadır.

1.2.2.5. Performans Kontrol Aktiviteleri

Bir bilgi sistemi girdi, çıktı, işlem ve depolama aktiviteleri ile ilgili geri beslemeler meydana getirmelidir. Bu geri besleme, sistemin daha önce belirlenen performans standartları ile uygun olup olmadığının belirlenmesi için izlenmeli ve değerlendirmelidir. Daha sonra yeterli sistem aktiviteleri, son kullanıcıları yeterli bilgi ürünleri üretilmesi için ayarlanmalıdır.

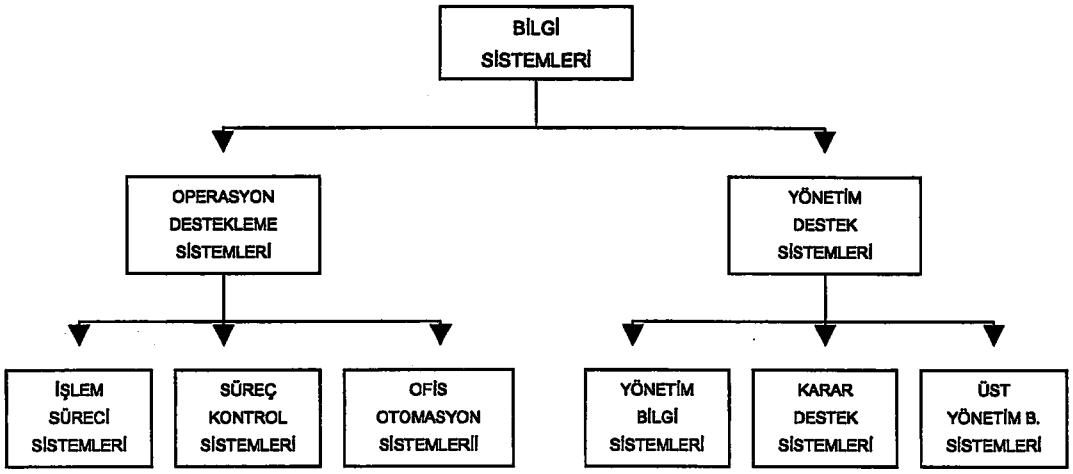
Örneğin bir satış müdürü satış tutarlarına ait alt toplamlarını genel toplama ilave olup olmadığını görmek için kontrol edebilir. Bu işlemle veri girişi ve işlem prosedürlerinin doğru olup olmadığı belirlenmelidir. Şayet yanlışlık varsa, yapılacak değişiklikler, bilgi sistemi tarafından işlenen ve depolanan tüm satış işlemlerinin doğru yapıldığını garantiler şekilde yapılmalıdır.

1.2.3. Bilgi Sistemlerinin Sınıflandırılması

Bilgi sistemleri değişik şekillerde sınıflandırılabilmektedir. Bu sınıflandırmaların en önde geleni bilgi sistemlerinin operasyon ve yönetim bilgi sistemleri olarak iki alt başlığa ayrılmasıdır. Bilgi sistemleri bu şekilde bir işin yönetim ve operasyondaki temel rollerine göre kategorize edilmektedir. Aşağıdaki şekil yönetim destekleme sistemleri ve operasyon destekleme sistemleri arasındaki ilişkiyi göstermektedir. Yönetim destek sistemleri, stratejik üst yönetim, orta kademe yönetimi ve operasyonel yöneticilerin karar verme ihtiyacını desteklemektedir. Operasyon destek sistemleri bir işin günlük bilgi işlem gerekliliklerini desteklemektedir.[7]

[7] James A. O'Brien, a.g.k., p.29

Şekil 1.4.
Bilgi Sistemlerinin Sınıflandırılması



Kaynak: James A. O'Brien, Introduction to Information Systems, Eighth Edition, 1997, p.29

Operasyon destekleme sistemleri, operasyonların gerçekleştirilmesinde kullanılır ve verilerin meydana getirmesinde önemli bir fonksiyonu meydana getirir. Böyle bir sistem dış ve iç kullanım için çeşitli bilgi ürünleri meydana getirmektedir. Operasyon destekleme sistemlerinin alt sistemleri aşağıdaki gibidir;

a) İşlem Süreci Sistemleri; Bu alt sistemde iş süreçlerinden gelen veri sonuçları kaydedilmekte ve işleme tabi tutulmaktadır. Bu sistemler işlemleri iki temel yöntemle gerçekleştirilmektedir. İlk grupta veriler periyodik olarak biriktirilmekte ve periyodik olarak işleme tabi tutulmaktadır. Gerçek zamanlı veya online işlemlerde ise veriler işlem yapılır yapılmaz derhal sürece tabi tutulmaktadır. Örneğin perakende satış merkezindeki satış noktaları merkezdeki bilgisayara elektronik olarak bağlıdır ve satış yapılır yapılmaz veriler aktarılabilir veya periyodik zamanlarda örneğin akşamları grup olarak aktarılarak işleme tabi tutulabilir.

b) Süreç Kontrol Sistemleri; Bu sistemler fiziki süreçleri gözlemlemekte ve kontrol etmektedir. Örneğin bir petrol rafinerisi bilgisayara bağlı elektronik algılayıcılar kullanmakta, kimyasal analiz süreci bu verileri sürekli olarak kontrol etmekte ve gerekli düzeltmeleri yapmaktadır.

c) Ofis Otomasyon Sistemleri; Bu sistemler ofis iletişimini ve üretkenliğini arttırmaktadır. Örneğin, bir işletme ofis iletişimi için elektronik mesajların alınması ve gönderilmesi için elektronik postayı ve elektronik toplantıların sağlanması için telekonferansı kullanabilmektedir.

Bir bilgi sistemi, yöneticilerin etkin karar almasını desteklemek ve bunun için bilgi sağlanmasına odaklanıyorsa, bu bilgi sistemi yönetim destek sistemleri olarak kabul edilmektedir. Genel olarak karar alma sürecinin desteklenmesi ve bilgi sağlanması üst, orta ve alt kademe yöneticileri için yapılmaktadır. Kavramsal olarak, bilgi sistemlerinin değişik tipleri, değişik yönetimsel son kullanıcıların sorumluluklarını desteklemektedir. Yönetim Destek Sistemleri'nin alt sistemleri aşağıdaki gibidir;

a) Yönetim Bilgi Sistemleri; Yöneticilere raporlar ve dökümler formunda bilgi sağlamaktadır. Örneğin, satış yöneticileri satış durumlarını ve satış personelinin durumunu değerlendirmek için bilgisayarını ve haftalık satış raporlarını kullanmaktadır.

b) Karar Destek Sistemleri; Karar verme sürecinde yöneticilere direkt bilgisayar desteği sağlamaktadır. Örneğin reklam yöneticileri yeni ürünlerin tahmini satışlarıyla ilgili alternatif reklam bütçelerinin etkisini test etmek amacıyla olasılık analizi yapmak için tabloları kullanabilmektedir.

c) Üst Yönetim Bilgi Sistemleri; Üst ve orta kademe yöneticilere kolay kullanılabilir kritik bilgiler sağlamaktadır. Örneğin üst yönetim, rekabetsel ve organizasyonel performansın durumunu gösteren yazılı ve grafik çalışmalarına ulaşmalarını sağlayan terminalleri kullanabilmektedir.

Uygulamada bilgi sistemlerinin yukarıda bahsettiğimiz türdeki sınıflandırmaların birer karışımı günümüzde sıklıkla görülmektedir. Çoğu bilgi sistemi, hem karar alma sürecinin desteklenmesi hem de operasyonel işlemlerin yürütülmesi için tasarlanmaktadır.

1.3. Denetim

Denetim yeterli mesleki deneyime sahip ve bağımsız kişiler tarafından yürütülen, belirlenen kriterler ve nicel bilgiler arasındaki uyum derecesini belirlemek ve raporlamak amacı için spesifik bir ekonomik varlıkla ilgili nicel bilgilerle ilgili delil toplama ve değerlendirme sürecidir. [8]

Denetim çalışmaları ister bağımsız denetim birimleri tarafından yapılsın isterse şirketin iç denetim birimlerince yapılsın, temel olarak finansal ve finansal olmamak üzere iki ana başlıkta incelenmektedir. Finansal denetim çalışmaları, finansal raporlama sürecinin iki ana ürünü olan bilanço ve gelir tablosu üzerine odaklanmaktadır. Finansal olmayan denetim çalışmaları a) Operasyonel Denetim, b) Uygunluk Denetimi, c) Bilgi Sistemleri Denetimi, d) Performans Denetimi, e) Program Denetimi olmak üzere 5 ana bölüme ayrılmaktadır.[9]

a) Operasyonel Denetim; Bir işletmenin kaynaklarını ekonomik ve verimli olarak kullanıp kullanmadığının belirlenmesidir.

b) Uygunluk Denetimi; Bir organizasyonun kanunlara ve düzenlemelere uyup uymadığının belirlenmesidir.

c) Bilgi Sistemleri Denetimi; Elektronik bilgi işlem sistemlerinin ve bu sistemin meydana getirdiği bilginin doğruluğunun ve güvenliğinin tespit edilmesidir.

---

[8] Alvin A Arens, James K.Loebbecke, Auditing An Integrated Approach, New Jersey, Prentice-Hall International, Inc., 1991, pp.1-2

[9] S. Rao Vallabhaneni, Internal Audit Process, Florida, SRV Professional Publications, 1998, pp. 1-4

d) Performans Denetimi; Ekonomiklik ve verimlilik ve program denetimini kapsamaktadır. Ekonomiklik ve verimlilik denetiminde, bir organizasyonun kaynaklarının elde edilmesinde, kullanılmasında ve korunmasında ekonomiklik ve verimlilik ilkelerine uyulup uyulmadığının ortaya konulmasına çalışılmaktadır.

e) Program Denetimi; Bir amaca ulaşmak için oluşturulan programın, bu amaca ulaşma konusundaki yeterliliği ve yapılan çalışmaların program doğrultusunda gidip gitmediğinin ortaya konması için yapılan çalışmalardır.

1.4. Bilgi Sistemleri Denetimi

Bilgi sistemleri denetimi tek başına bir aktivite değildir. Daha ziyade iç ve dış denetim fonksiyonunun entegre bir bölümüdür. Bilgi sistemleri denetimi, bilgisayar tabanlı sistemlerin kullanıldığı ve bilgisayar ekipmanının yerleştirildiği uygulama sistemlerinin ve bilgisayar operasyonlarının görünümüyle ilgilidir. Bilgi sistemleri denetimlerinin amacı ve alanı bilgisayar sistemleri ve bilgi teknolojileri varlıkları üzerindeki kontrollerin yeterli olup olmadığının belirlenmesidir. [10]

Bilgi sistemleri denetimi finansal ve operasyonel denetim konularına önem vermektedir. Özellikle,

a) Bilgisayar operasyonlarının kontrol zayıflıklarının organizasyonun finansal ve operasyonel kayıtları üzerindeki etkisi,
b) Sistem bütünlüğü(güvenliği) ve güvenlik kontrolleri zayıflıklarının, uygulama sistemlerinin sahip olduğu bilginin ve sistemin kullanıcılar için kullanışlılığı üzerindeki etkisi,
c) Sistem hataları ve düzensizliklerinin (bilgisayar hırsızlığı, usulsüzlüğü, istismarı ve zimmete geçirme) mali tablolar üzerindeki etkisi,

ile ilgilenmektedir.

---

[10] Ron Weber, Information Systems Control and Audit, Prentice-Hall, Inc., New Jersey, 1998, p.10

Bilgi sistemleri denetiminden elde edilen sonuçlar bir işletmenin performansını etkileyen karar alma sürecindeki önemli paya sahip olan bilgi sisteminin yapısı ve güvenliği hakkında önemli katkılar sağlamaktadır. [11]

Bilgi sistemleri denetimi aynı zamanda bilginin nasıl elde edilip nerde kullanıldığı ve bu bilgi varlıklarının işletmenin daha verimli şekilde çalışması ve stratejik üstünlük kazanması için nasıl daha etkin değerlendirileceğini de anlaşılmasını sağlamaktadır.[12]

50 Yıl öncesinde bilgi işlem ihtiyaçlarının çoğu elle yerine getiriliyordu. Günümüzde bilgisayarlar, ekonomilerin kamu ve özel sektörlerinde ihtiyaç duyulan bilgi işlemlerinin çoğunu gerçekleştirmektedir. Sonuç olarak hayatımızın aksamadan devam etmesinin bilgi işlem sürecinin doğruluğuna bağlı olduğu görülmektedir. Bir çok kişi artan bilgi işlem yeteniğinin iyi bir şekilde kontrol edilmediğinden korkmaktadır.

Bilgisayarların kontrolsüz kullanımı toplum üzerinde yaygın bir etkiye sahip bulunmaktadır. Örneğin, doğru olmayan bilgi, ekonomideki kaynakların yanlış tahsisine neden olurken, yeterli olmayan sistem kontrolleri usulsüzlük ve sahtekarlıkların ortaya çıkmasına neden olmaktadır.

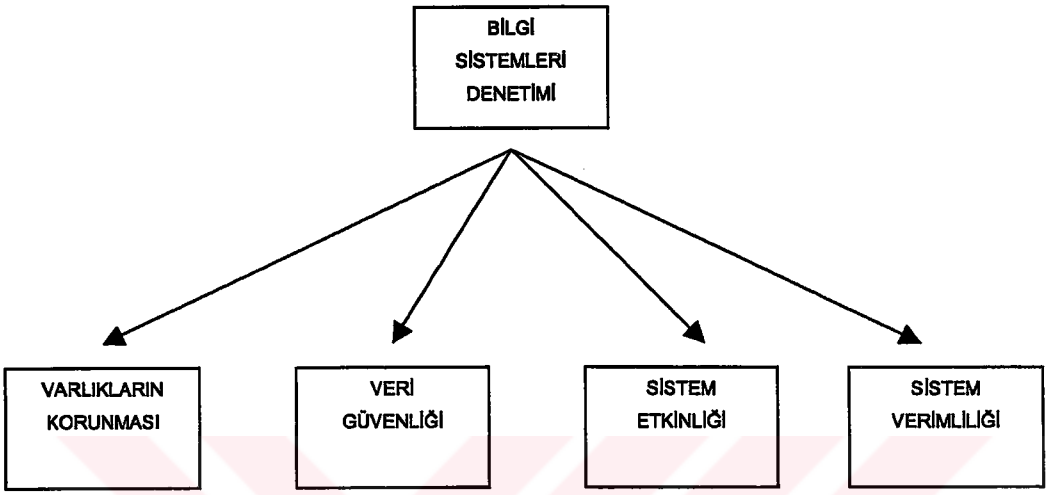
Bilgi Sistemleri Denetimi; Bir bilgisayar sisteminin varlıklarını koruyup korunmadığını, veri doğruluğunu devam ettirip ettirmediğini, organizasyonun amaçlarına etkin olarak ulaşıp ulaşmamasına izin verip vermediğini, kaynakların verimli bir şekilde kullanıp kullanılmadığı konusunda karar vermek için kanıt toplama ve değerlendirme sürecidir. Bazen bilgi sistemleri denetimi başka bir amaca sahip olabilmektedir yani organizasyonun bazı kurallara, düzenlemelere uyup uymadığını araştırabilmektedir. Aşağıda bilgi sistemleri denetiminin bir organizasyon üzerindeki fonksiyonları görülmektedir.

---

[11] C.P.R. Dubios, "The Information Audit" Library Management" Volume MCB University Press, 1995,pp.20-24

[12] G.D. Swash, "The Information Audit" Journal of Managerial Psychology, MCB University Press, 1997, pp. 312-318

Şekil 1.5.
Bilgi Sistemleri Denetiminin Bir Organizasyon Üzerindeki Fonksiyonları



Kaynak: Ron Weber, Information Systems Control and Audit, Prentice-Hall, Inc., New Jersey, 1998 p.11

1.4.1. Bilgi Sistemleri Denetiminin Fonksiyonları

1.4.1.1. Varlıkların Korunması

Bir organizasyonun bilgi sistemi varlıkları, donanım, yazılım, techizatlar, insan, bilgi, veri dosyaları, sistem dökümantasyonları ve diğer malzemelerdir. Diğer tüm varlıklar gibi, onlarında iç kontrol sistemiyle korunması gerekmektedir. Donanımlar, görünür ve bilinçli olarak zarara uğrayabilmektedir. Bir organizasyonun sahip olduğu donanım ve veri dosyalarının içeriği çalınabilmekte, yok olabilmekte ve malzemeler ve diğer dökümanlar yetkisiz bir şekilde kullanılabilmektedir. Bu varlıklar belirli bir alanda veya bir disk gibi belirli bir ortamda bulunabilmektedir. Bu nedenle varlıkların koruması, bir çok organizasyonun özel önem verdiği amaçlardan biri olmaktadır. [13]

---

[13] S. Rao Vallabhaneni, Management Control & Information Technology SRV Professional Publications, 1998, Illinois, p. 534

1.4.1.2. Veri Güvenliğinin Sağlanması

Veri güvenliği bilgi sistemleri denetiminde temel kavramlardan biridir. Şayet bir organizasyonda veri güvenirliliği sağlanmazsa, organizasyonun kendisini ve yaşadığı olayları doğru bir şekilde tanıtması mümkün olmayacaktır. Şayet veri güvenliği düşük ise, o organizasyon düşük rekabet avantajıyla da karşılaşabilmektedir.

Veri çeşitlerinin değerini üç temel faktör etkilemektedir;

a) Bireysel karar verme için bilgi çeşitlerinin bilgisel içeriğinin değeri. Bir veri çeşidinin bilgisel içeriği, bir fikri belirsizlik ortamında değiştirme gücüne bağlı olmaktadır

b) Veri çeşitlerinin karar vericiler arasında paylaşılması, bilginin paylaşıldığı bir ortamda verinin güvenliğinin devam ettirilmesi daha kritik bir öneme sahip olmaktadır.

c) Rakiplere bilgilerin kaptarılması, şayet veri türleri rakipler için değerli ise, işletmenin piyasadaki pozisyonunun kaybı demektir. Rakipler bu bilgileri kendi amaçları doğrultusunda kullanabilmektedir.

1.4.1.3. Sistem Etkinliğinin Sağlanması

Etkin bilgi sistemi amaçlarını başarabilen bir bilgi sistemidir. Etkinliğin değerlendirmesi kullanıcı ihtiyaçlarına ait beklentileri ifade etmektedir. Sistemin, kullanıcıların karar verme sürecindeki beklentileri doğrultusunda rapor sunup sunmadığınnı değerlendirilmesi için, kullanıcıların karakterleri ve karar verme çevresi bilinmelidir.

- Etkinlik denetimi genellikle çalışan bir bilgi sistemde gerçekleştirilmektedir. Yönetim, bilgi sisteminin amaçlarını başarıp başaramadığının görülmesi için bu tarz bir denetim çalışmasına ihtiyaç duymaktadır. Etkinlik denetimi aynı zamanda bir sistemin dizayn evresinde de yapılabilmektedir.

1.4.1.4. Sistem Verimliliğinin Arttırılması

Verimli bir bilgi sistemi amaçlarına ulaşmak için minimum kaynakları kullanan bilgi sistemidir. Bilgi sistemleri makina, zaman, yazılım ve işgücü gibi çeşitli kıt kaynaklardan faydalanmaktadır . Bir sistemin verimli olup olmadığının sorusuna verilecek cevap kısa ve kesin değildir. Herhangi özel bir sistemin vermliliği diğer sistemlerden ayrı olarak izole edilerek gözönünde tutulmamalıdır.

Yönetim verimliliğin iyileştirilebileceğine veya ekstra kaynak satın alınması gerektiğine karar vermelidir. Ekstra donanım ve yazılım bir maliyet konusu olduğundan, yönetim mevcut kapasitesinin tamamiyle kullanıp kullanmadığını veya mevcut bilgisayar kaynaklarındaki tahsisatın sıkışıklıklar neden olup olmadığını bilmek zorundadır. Yönetim bu verimlilikle ilgili yapılacak denetim çalışmalarıyla bu konuda bilgi elde edecektir.

1.4.2. Bilgi Sistemleri Denetiminin Amaçları

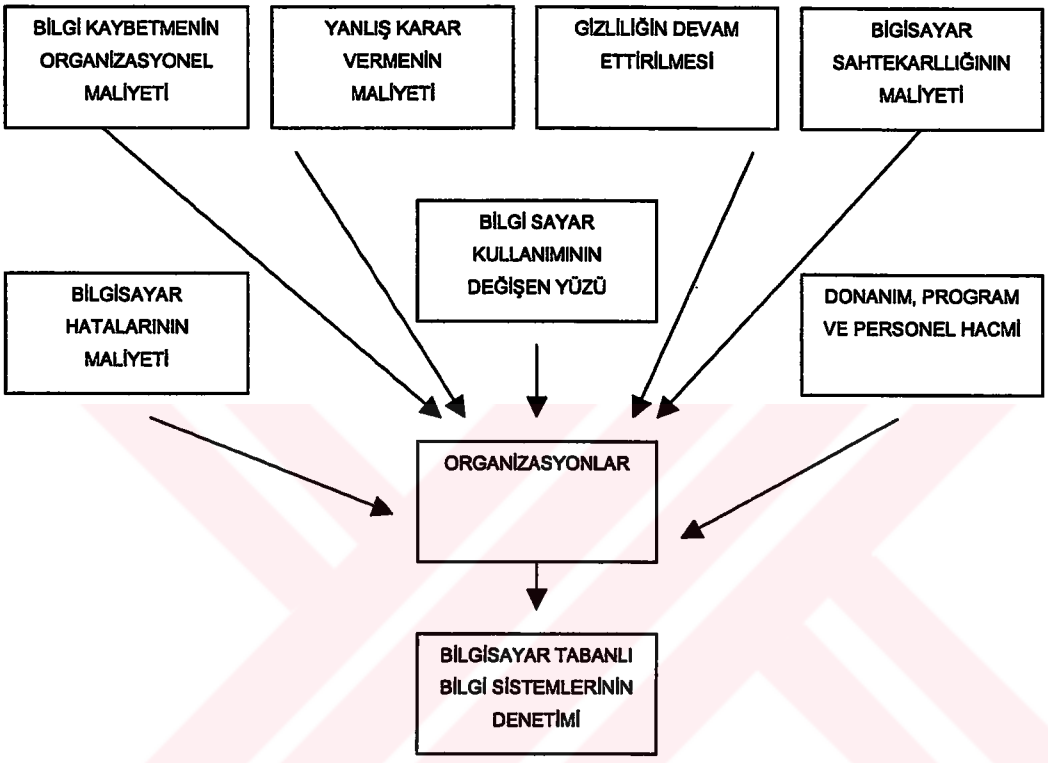
Bilgisayarlar yoğun olarak karar alma için bilgi sağlama ve veri işleme için kullanılmaktadır. Başlangıçta, yüksek operasyon maliyeti ve satın alma maliyetine katlanarak gücü yeten büyük organizasyonlar için mevcut olan bilgisayarlar, bilgisayar maliyetlerindeki hızlı düşüş ve mikro bilgisayarların yaygınlaşmasıyla orta ölçekli organizasyonların da veri işleme sürecinde bilgisayarlardan avantaj elde etmeye başlamasına neden olmuştur.

Karar verme süreci ve veri işleme sürecinde bilgisayarların geniş rol alması nedeniyle, bilgisayarların kontrol edilmesi oldukça büyük önem arz etmektedir. Aşağıdaki şekilde bilgisayar tabanlı sistemlerin için kontrolün gözden geçirilmesi için gerekli 7 temel neden gözükmektedir. [14]

[14] Ron Weber, a.g.k., p.17

Şekil 1.6.

Bir Organizasyonda Bilgisayar Kontrol ve Denetimini Etkileyen Faktörler



Kaynak: Ron Weber, Information Systems Control and Audit, Prentice-Hall, Inc., New Jersey, 1998 p.17

1.4.2.1. Bilgi Kaybı Maliyetlerinin Azaltılması

Bilgi bir organizasyonun devam eden operasyonları için önemli bir kaynak sağlamaktadır. Şayet bu kaynak yeterli ve doğru ise, organizasyon, değişen çevresine ayak uydurma ve hayatta kalma konusunda kabiliyet sahibi olacaktır. Şayet bu kaynak yeterli ve doğru değilse veya kaybedilme durumu söz konusu olursa, organizasyonun yaşam süresi kısalacak ve önemli kayıplara mağruz kalmasına neden olacaktır.

Örneğin bir bankanın kredileriyle ilgili dosyaların zarara uğraması, bankanın tahsilatları konusunda maddi sıkıntılara uğramasına neden olurken, bankanın borçlarıyla ilgili dosyaları kaybetmesi durumunda ise bankanın borçlarını zamanında ödememesine neden olacak ve bankanın kredibilitesinde azalmaya neden olacaktır.

Bütün kayıplar aslında bilgisayarlar üzerindeki kontrollerin ihmal edilmesinden kaynaklanmaktadır. Örneğin bilgisayar dosyalarından yeterli yedekleme işlemi yapılmayabilir. Sonuç olarak, bilgisayar programlarında meydana gelen hatalar, sabotajlar veya doğal afetler nedeniyle bir dosyanın kaybolması durumunda kaybolan dosyanın yeniden yerine getirilmesi mümkün olmayacak ve organizasyonun devam eden operasyonları zarar görecektir.

1.4.2.2. Hatalı Kararların Önlenmesi

Bir organizasyonda verilen kararların kalitesi bilgisayar tabanlı bilgi sistemlerinde var olan bilginin kalitesine bağlıdır. Zira yöneticiler yönetimsel ve operasyonel anlamda verdikleri kararlarda, muhtemelen yüksek derecede doğru bilgiye ihtiyaç duymaktadır. Bu tür kararlarda doğru olmayan bilgiler, maliyetli ve gerekli olmayan soruşturmalara neden olurken aynı zamanda alınan kararların başarısını da etkileyecektir. Başarısız olarak alınan kararlar ise işletmelerin finansal başarısızlığa uğrama riskini önemli derecede arttıracaktır. [15]

Yönetimin yanı sıra, doğru olmayan bilgi bir organizasyon üzerinde ilgiye sahip olan kişiler üzerinde de olumsuz etkiye sahiptir. Örneğin, bir bankanın ortaklarına doğru olmayan finansal bilgileri sunması durumunda, ortaklar mevcut yatırım kararlarını erteleyebileceklerdir.

Bir organizasyonda doğru olmayan bilginin sonuçları, bilginin kullanıldığı operasyonun tipine göre farklılık arz etmektedir. Örneğin, amortisman hesaplamalarında yapılacak hata düşük değerli bir varlığın amortisman hesaplamasında meydana gelebileceği gibi, bir bankanın müşterisine ödeyeceği faizin ve faiz oranının hatalı olması durumunda, banka, müşterilerine önemli ölçüde

[15] Niyazi Berk, Finansal Yönetim, Türkmen Kitabevi, İstanbul, 1995, ss. 413-419

fazla faiz ödemek durumunda kalabilecektir. Benzer bir şekilde hastalığın tedavisinde kullanılan bulguların hatalı tespit edilmesi, doktorların hastalarını yanlış tedavi etmelerine neden olacak ve bu hata ölümcül olabilecektir.

1.4.2.3. Bilgisayar Kötü Kullanımlarının Engellenmesi

Bir organizasyonda bilgi sistemleri denetiminin amaçlarının en önemlilerinden birisi de, bilgisayarların kötüye kullanımı veya bilgisayar suçlarıdır. Bilgisayarların kötüye kullanılması bir kurbanın bundan zarar gördüğü ve bilgisayar teknolojileriyle birleşen bir olaydır, bu olay bilinçli olarak yapılmaktadır ve tekrarlanması muhtemeldir.

Bilgisayarın kötü kullanımının bazı temel tipleri aşağıdaki gibidir;

Hacking; Bir kişinin bir bilgisayar sistemine okumak, değiştirmek, programları veya verileri silmek veya sistemi rahatsız etmek amacıyla yetkisiz olarak erişmesidir.

Virüsler; Virüsler kendilerini dosyalara, disketlerdeki sistem alanlarına ekleyen programlar veya veri ve programlara zarar veren veya bilgisayar operasyonlarını rahatsız eden dosyalardır. Bunlar iki amacı başarmak için oluşturulmaktadır.

a) Kendi kendilerini kopyalamak
b) Rahatsızlığa yol açacak şekilde ilgili yere ulaşmak

Yetkisiz Fiziki Erişim; Bir personelin bilgisayar tesislerine yetkisiz şekilde fiziki erişimidir. Sonuç olarak, bu yetkisiz erişimle donanımlara fiziki zarar verebilmekte veya program veya verilerin yetkisiz kopyalarını alabilmektedir.

Yetkilerin Kötüye Kullanılması; Bir personelin yetkilerini izin verilmeyen amaçlar için kullanmasıdır. Örneğin kendisine ulaşma konusunda yetki verilmiş bir kişi tarafından veri'nin izinsiz bir şekilde kopyasının çıkartılmasıdır.

Varlıkların Yok Edilmesi; Bilgi Sisteminin donanım, yazılım, veri, techizalatlar, dökümantasyonları ve diğer varlıkların yok edilmesidir.

Varlıkların Çalınması; Bilgi Sisteminin donanım, yazılım, veri, techizatlar ve diğer varlıklarının çalınmasıdır.

Varlıkların Değiştirilmesi; Bilgi Sisteminin donanım, yazılım, veri, teçhizatlar ve diğer varlıklar yetkisiz bir şekilde değiştirilmesidir.

Özele İzinsiz Giriş; Bir kişiye veya bir organizasyona ait olan veri özel alanına izinsiz girilmesidir.

Operasyonların Rahatsız Edilmesi; Günlük bilgi sistemi fonksiyonlarının geçici olarak aksatılmasıdır.

Varlıkların Yetkisiz Kullanımı; Donanım, yazılım, veri, dökümantasyon ve diğer varlıklar yetkisiz amaçlarla kullanılmasıdır. Örneğin bilgisayarların kişisel amaçlarla kullanılmasıdır.

Personele Fiziki Zarar; Personelin fiziki zararla karşılaşmasıdır.

1.4.2.4. Bilgi Sistemi Kaynaklarının Korunması

Bilgi sistemleri kaynakları içinde yer alan, bilgi, bilgisayar donanımı, yazılım ve personel bir organizasyon için kritik kaynaklardır. Bazı organizasyonlar donanıma milyon USD'lık yatırımlarda bulunmaktadır. Organizasyonlarda sigortalamaya rağmen, bazen kasdi bazen kasdi olmayan donanım kayıpları olmakta ve bu kayıplar önemli zararlara yol açmaktadır. Benzer bir şekilde yazılımlar da bir organizasyon için önemli bir kaynaklardır ve bu yazılımların zarar görmesi durumunda ise organizasyon operasyonlarını gerçekleştirememektedir. Personel de oldukça önemli bir kaynaktır. Zira iyi yetişmiş bilgisayar uzmanları bir çok ülkede az bulunan kaynaklar arasında gelmektedir.

1.4.2.5. Bilgisayar Hatalarının Önlenmesi

Bilgisayarlar günümüzde bir çok kritik fonksiyonu yerine getirmektedir. Hastahane yönetiminden, ameliyata, bankalardaki risk yönetimlerine kadar bir çok fonksiyon bilgisayarlar tarafından gerçekleştirilmektedir. Bilgi sistemlerinde hataların meydana gelmesi organizasyonlarda ve toplumumuzda tamir edilemez sorunların yaşanmasın neden olmaktadır.

1.4.2.6. Gizliliğin Sürdürülmesi

Bir çok veri vergileme, kredi, tıbbi, eğitimsel, istihdam gibi alanlarda kişisel amaçlarla toplanmaktadır. Bu veri'lerin ancak ilgili kişiler için ve ilgili yerlerde kullanılması oldukça önemlidir. Zira sır niteliğindeki bu verilerin istenen amaçlar dışında kullanılması bireylere, organizasyonlara ve topluma önemli zararlar vermektedir.

1.4.2.7. Bilgisayar Kullanımlarının Kontrol Altında Tutulması

Bilgi Sistemleri üzerine yapılan tartışmalar zaman zaman bilgisayar teknolojilerinin toplumumuzda nasıl kullanılması gerektiği üzerinde olmaktadır. Teknoloji onu kullanan kişilere göre olumlu ve olumsuz sonuçlar meydana getirmektedir.

Teknolojilerin özellikle bilgisayar teknolojilerinin bilinçsiz kişilerin eline geçmesi ve kötü amaçlar için kullanılması organizasyonlara ve topluma önemli zararlar vermektedir. Bu nedenle bilgisayar teknolojilerinin kullanımı bilgi sistemleri denetiminin önemli amaçlarından biri haline gelmiştir.

1.4.3. Bilgi Sistemleri Denetiminin Temelleri

Bilgi sistemleri denetimi sadece geleneksel denetimin bir uzantısı değildir. Bilgi sistemleri denetimi 4 temel disiplinden elde edilen bilgilerle şekillenir. Bu disiplinler aşağıdaki gibidir; [16]

a) Geleneksel Denetim
b) Bilgi Sistemleri Yönetimi

[16] Ron Weber, a.g.k., p.18

c) Davranış Bilimi
d) Bilgisayar Bilimi

1.4.3.1. Geleneksel Denetim

Geleneksel denetim, sahip olduğu iç kontrol tekniklerindeki deneyim ve bilgiyle, bilgi sistemleri denetimine katkıda bulunmaktadır. Bu bilgi ve deneyim, günümüzde bir bilgi sisteminin dizaynı ve çalışması hakkında önemli katkılara sahip olmaktadır.

Bilgi Sistemlerinde gerçekleştirilen kanıt toplama ve değerlendirme metodolijisi geleneksel denetim metodolijisine dayanmaktadır. Ayrıca, geleneksel denetim bilgi sistemleri denetimine bir kontrol felsefesi getirmektedir. Bu felsefe, bilgi sistemlerinin kritik bir düşünceyle değerlendirilmesini, bilgi sistemlerinin varlıkların korunmasındaki veri güvenliğinin sürdürülmesi ve bilgi sistemlerinin amaçlarına ulaşmasında etkinlik ve verimlilik konusundaki kabiliyetin sorgulanmasını içermektedir.

1.4.3.2. Bilgi Sistemleri Yönetimi

Bilgisayar tabanlı bilgi sistemlerinin ilk zamanlarında bazı önemli başarısızlıklar görülmüştür. Ancak uzun süren çalışma ve araştırmalar sonucunda, başarılı bilgi sistemi uygulamaları ortaya konmuştur.

Bilgi sistemleri alanında yapılan çalışma ve araştırmalarla bazı önemli avantajlar elde edilmiştir. Bilgi sistemlerinde dökümantasyon, standartlar, bütçeler ve sapma araştırmaları rahatlıkla başarılmaktadır. Bu başarılar varlık korumasını, veri güvenirliliğini, sistem etkinlik ve verimliliğini etkilemesinden dolayı, bilgi sistemlerinin denetimini etkilemektedir.

1.4.3.3. Davranış Bilimi

Bilgisayar sistemleri bazen, dizayn eden kişiler tarafından kişi davranışlarının doğru olarak değerlendirilmemesi nedeniyle başarısızlığa uğramaktadır. Denetim elemanlarının davranış problemlerine yol açacak durumları anlaması ve davranış bilimciler ve özellikle organizasyon teoristlerinin ortaya koyduğu organizasyonlardaki insan problemlerini bilmesi gerekmektedir.

Bilg sistemlerinde mevcut risklerin gerçekleştirilecek denetim çalışmalarıyla kontrol altında tutulması isteniyorsa, bilgi sistemleri denetim elemanları, çalışmalarında davranış bilimlerinden istifade etmek zorundadır.

1.4.3.4. Bilgisayar Bilimi

Bilgisayar bilimciler, aynı zamanda, varlıkların nasıl korunacağı, veri güvenliğinin nasıl sağlanacağı, sistem etkinlik ve verimliliğinin nasıl daha iyi başarılacağı ile yakından ilgilidir. Örneğin, bir yazılımın doğruluğunun arttırılması ve güvenli organizasyon sistemlerinin oluşturulması bunların arasındadır.

Günümüzde bilgisayar bilimi tarafından geliştirilen çalışmalar, denetim çalışmalarına hem fayda hem de problem katmaktadır. Örneğin başarılı sistem programcıları bir yolsuzluğun gizlenmesini isterse, bu yolsuzluğun denetçiler tarafından bulunması, denetçilerin yoğun bir şekilde bilgi sistemi teknolojileri hakkında bilgi elde etmeden başarılmasını imkansız hale getirmektedir. Bu nedenle bilgi sistemleri denetimi alanında yapılacak çalışmaların başarısı bilgisayar biliminden elde edilecek bilgilerle oldukça ilgilidir.

2. BİLGİ SİSTEMLERİNİN DENETİMİ

Bilgi sistemleri denetiminde yapılan çalışmaları temel olarak,

a) Denetim planlaması ve risk ölçümü,
b) Denetim uygulamasının gerçekleştirilmesi,
c) Denetim kanıtlarının toplanması,
d) Denetim dökümanlarının hazırlanması

başlıklarından oluşmaktadır. Aşağıda bu başlıklar hakkında detaylı bilgi verilecektir.

2.1. Denetim Planlaması ve Risk Ölçümü

Denetim çalışmalarına başlamadan önce denetmenler mutlaka denetim yapacakları organizasyonla ilgili denetim planlarını ve programlarını hazırlamalıdır. Denetim planlaması; Belirli bir zaman dönemi içinde gerçekleştirilecek denetim çalışmalarının tanımlanmasıdır. Böyle bir tanım,

a) Denetlenecek alanı
b) Planlama çalışma tipini
c) Çalışma alanını ve amaçlarını
d) Denetim bütçesi
e) Kaynak tahsisi
f) Raporlama tipini

içermelidir.[17]

[17] S. Rao Vallabhaneni, a.g.k. p. 31

Denetim programı ise denetim amaçlarının başarılmasını sağlamak için adımlar serisidir. Bilgi sistemleri denetmenleri, denetim alanı ve teknolojik yapıyla ilgili denetim amaçlarını dikkate alarak bir denetim planı geliştirmelidir. Denetmenler, gerektiği yerde organizasyonla olan stratejik, finansal veya operasyonel ilişkileri de dikkate almalı ve bilgi sistemlerini de içeren işletmenin genel stratejik planıyla ilgili bilgi almalıdır. [18] Denetmenler aynı zamanda bilgi sistemleri denetimi organizasyonunun bilgi mimarisi ve gelecek ve sıradaki teknoloji planını anlamalıdır.

Denetime başlamadan önce bilgi sistemleri denetiminin çalışması denetim amaçlarıyla örtüşen şekilde planlanmalıdır. Planlama sürecinin bir parçası olarak denetmenler organizasyon ve süreçlerle ilgili bilgi edinmelidir. Ayrıca organizasyonun operasyonları ve gereklilikleri hakkında bilgi sahibi olmak, denetmenlerin bilgi sistemleri kaynaklarının organizasyon için önemini anlamasına yardımcı olacaktır. Ayrıca denetmenler organizasyonun ticaret alanında mevcut olan iş, finans ve doğal riskler konusunda da bilgi sahibi olmalıdır.

Denetmenler bu bilgileri potansiyel problemleri, çalışmanın amaçlarını ve alanını ve yönetimin hareketleri konusunda dikkatli olması gereken alanları belirlemek için kullanmalıdır.

Denetmenler planlama sürecinde, denetim çalışmasının amaçlara ulaşması ve verimli olması için planlamanın denetim için nisbi önem derecesini ortaya koymalıdır.

Denetim planı oluşturulurken, organizasyon iç kontrol mekanizmasının etkinliği ve güvenirliliği denetmenler tarafından değerlendirilmelidir. İç kontrol; organizasyonun amaçlarına ulaşmak için, hoşa gitmeyen olayların engellendiği, tespit edildiği ve düzeltildiğine dair anlamlı güvence sağlamak amacıyla dizayn edilmiş politikalar, prosedürler uygulamalar ve organizasyonel yapılardır.

---

[18] Information Systems Audit and Control Foundation, "Auditing Guideline: Planning", (Çevirimiçi) http://www.isaca.org/standard/guide23.htm, 04 Temmuz 2002

Denetim planlamasında denetlenecek organizasyonla ilgili risk değerlemesi yapılması oldukça önemlidir. Zira denetim yönetimi açısından risk değerlemesi sayesinde, denetim kaynaklarının nasıl yönlendirileceği ve denetim ekibinin nasıl yönetileceği ortaya konulmakta ve denetim planlamasının başarısı artmaktadır.

Denetmenlerin seçebileceği birçok risk değerleme metodu vardır. Denetmenlerin değerlendirilmesine bağlı olarak düşük, orta ve yüksek derece olmak üzere basit bir sınıflandırma vardır. Aynı zamanda rakamsal risk ölçümde yapılabilir. Denetmen denetlenen organizasyonun detayı ve karmaşıklık derecisini de gözönünde bulundurmalıdır.

Tüm risk ölçüm metodları, risk değerlendirme sürecindeki bazı noktalarda sübjektif değerlendirmelere güvenmektedir. Denetmen bu alanlardaki sübjektif kararını vererek değerlendirmesini yapmalıdır. Denetmen sadece tek bir risk değerleme modelini kullanmamalıdır. Ayrıca denetmen periyodik olarak risk değerleme modelini gözden geçirerek değerlendirmelidir, zira her koşula uyan risk değerlendirme modeli mevcut değildir.

Genel olarak bakıldığında bilgi sistemlerine ait risk üç ana başlıktan kaynaklanmaktadır. Söz konusu risk kaynakları,

a) Sistem hassiyeti
b) Sistem güveni
c) Sistem karmaşıklığı

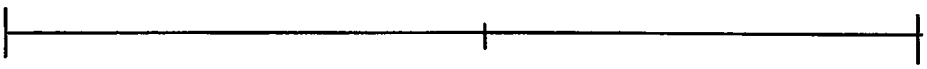
olarak sıralanabilir. [19]

[19] Alan Oliphant, "Taking the Helicopter View of Information Risks", 5 July-15, 2002 (Çevirimiçi) http://www.theiia.org/itaudit

Bu başlıklardan risk derecesinin belirlenmesinde, başlıkların alt detaylarının da belirli kriterlerle değerlendirilmesi sonucunda elde edilecek sayısal verinin değerlendirilmesi kullanılmaktadır. Yukarıda belirtilen başlıklar ve onların alt detayları risk derecesine göre,

Yüksek Risk Derecesi = 3
Orta Risk Derecesi = 2
Düşük Risk Derecesi = 1

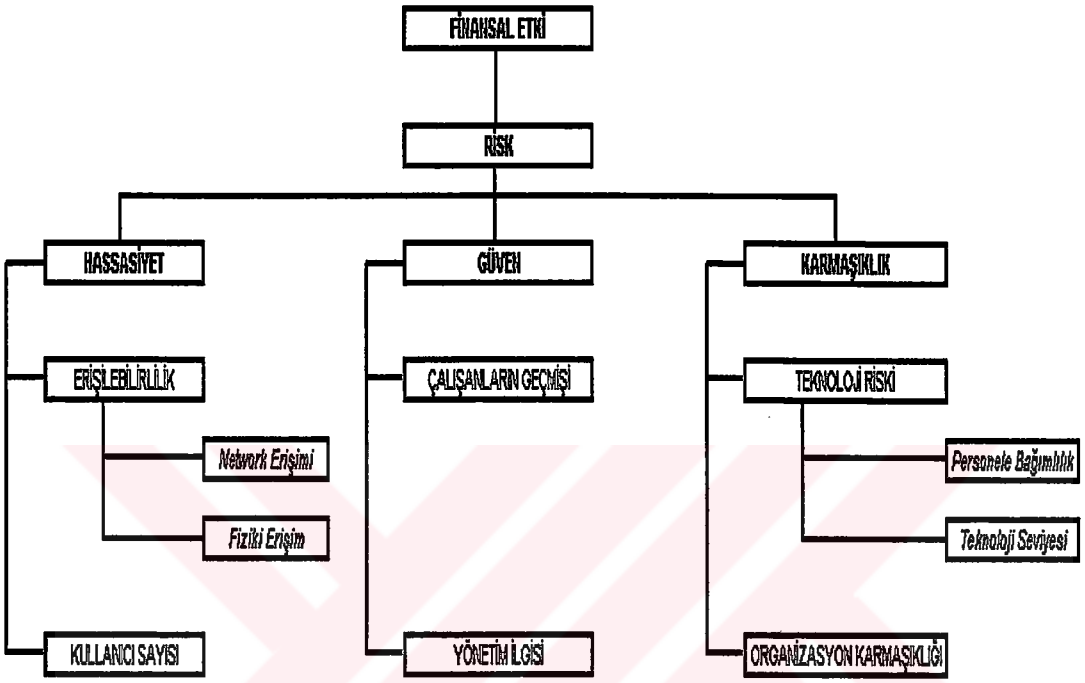
puanlanır. Puanlama sonucunda sistem hassasiyeti, güveni ve karmaşıklığının puanları toplamı bilgi sistemlerinin risk derecesini verecektir.



Düşük Risk	Orta Risk	Yüksek Risk
3 Puan	6 Puan	9 Puan

Değerlendirmenin sonucunda 9 puan alan bir bilgi sistemi yüksek bir riske sahip iken 3 puan alan bir bilgi sistemi düşük riske sahip olmaktadır. Aşağıdaki şekil risk değerleme modelinin genel görünümünü ve bilgi sistemlerinde riski meydana getiren sistem hassasiyeti, sistem güveni ve sistem karmaşıklığının alt başlıklarını vermektedir.

Şekil 2.1.
Risk Değerleme Modeli



Kaynak : Alan Oliphant, "An Introduction to Computer Auditing- Part Deux, No:7", ITAUDIT.ORG, January 15, 2000, (Çevirimiçi) http://www.itaudit.org/forum/newitauditor/f302na.htm,

2.1.1. Sistem Hassasiyeti

Bilgi sistemi hassasiyeti, bilgi sistemi varlıklarına ve sisteme erişen yetkili kullanıcı sayısının erişim durumunun bir fonksiyonu olarak belirlenmektedir. Sistemin erişebilirliği, organizasyon tarafından uygulanan fiziki erişim kısıtlamaları ve organizasyon bilgi sisteminin dış network'lerle iletişimine bağlı olarak değerlendirilmektedir.

Tablo 2.1.

Fiziki Erişebilirlilik

RİSK DERECESİ	TANIMLAMA
YÜKSEK	Bilgi Sistemi ekipmanına ve diğer bilgi kaynaklarına, binaya giren herkes rahatlıkla ulaşabilmektedir.
ORTA	Bilgi Sistemi ekipmanı ve diğer bilgi kaynakları, binaya girenlerin normal olarak erişemeyeceği yerde bulunmaktadır.
DÜŞÜK	Bilgi Sistemi ekipmanı ve diğer bilgi kaynakları, yetkisiz kişilerin girişinin engellendiği yerde bulunmaktadır.

Yukardaki tabloda görülen fiziki erişime ait durum tespitiyle birlikte fiziki erişebilirliğe ait risk ortaya çıkacaktır. Örneğin denetim yapılan organizasyonun terminal ekipmanı ve diğer bilgi kaynaklarının binaya girenlerin normal olarak erişemeyeceği yerde bulunduğunu düşünelim, bu durumda risk derecesi orta olarak belirlenecektir.

Tablo 2.2.

Network Erişimi

RİSK DERECESİ	TANIMLAMA
YÜKSEK	Bilgi sistemi, bir kamusal network ağına fiziki olarak bağlıdır. Bu duruma bilgi sisteminin bağlı olduğu internet ve kamu telefon hattı örnek olarak verilebilir.
ORTA	Bilgi sistemi tamamen organizasyon tarafından yönetilen ve sınırlı erişimi olan bir network'e bağlıdır. Örneğin kiralık hat
DÜŞÜK	Bilgi sisteminin herhangi bir dış network'e fiziki anlamda bağlantısı yoktur.

Yukarıdaki tabloda görülen network erişimine ait durum tespitiyle network erişimine ait risk derecesini ortaya çıkarılmaktadır. Örneğin organizasyonun internete ve kamusal olarak kullanılan bir telefon hattına bağlı olduğunu düşünelim, bu durumda network erişim riski yüksek olarak belirlenecektir.

Bir sistemin genel erişilebilirliği fiziki erişilebilirlik ve network erişiminin bir fonksiyonudur. Bununla ilgili genel tablo aşağıdaki gibidir.

Tablo 2.3.

Fiziki Erişim ve Network Erişiminin Karşılaştırılması

FİZİKSEL ERİŞİM	NETWORK ERİŞİM SEVİYESİ		
	YÜKSEK	ORTA	DÜŞÜK
YÜKSEK	YÜKSEK	YÜKSEK	ORTA
ORTA	YÜKSEK	ORTA	DÜŞÜK
DÜŞÜK	ORTA	DÜŞÜK	DÜŞÜK

Yukarıdaki tabloda görülen organizasyonun fiziki ve network erişim durumunun karşılaştırılması sonucunda organizasyonun erişebilirlilik risk derecesi ortaya çıkacaktır. Örneğimizi hatırlayacak olursak

Fiziki Erişim Sonucu : Orta

Network Erişim Sonucu : Yüksek

Erişebilirlilik Risk Sonucu : Yüksek

olarak gerçekleşecektir.

Sistem hassasiyetinin belirlenmesi için bilgi sistemi yetkili kullanıcı sayısının risk derecesinin, erişilebilirlilik risk sonucu ile toplu olarak değerlendirilmesi gerekmektedir.

Tablo 2.4.

Kullanıcı Sayısı

RİSK DERECESİ	TANIMLAMA
YÜKSEK	Çoğunluk
ORTA	Birkaç kullanıcı
DÜŞÜK	Oldukça sınırlı sayıda kullanıcı

Yukarıdaki tabloda görülen organizasyondaki yetkili kişilerin bilgi sistemini kullanım sayısının belirlenmesiyle kullanıcı sayısı risk derecesi ortaya çıkacaktır. Örneğin organizasyon çalışanlarının çoğunluğunun yetkili olarak bilgi sistemlerine erişerek kullandıklarını düşünelim. Bu durumda risk derecesi yüksek olarak gerçekleşecektir.

Tablo 2.5.

Kullanıcı Sayısı ve Erişebilirlilik Derecesi Karşılaştırılması

KULLANICI SAYISI	ERİŞİLEBİLİRLİLİK		
	YÜKSEK	ORTA	DÜŞÜK
YÜKSEK	YÜKSEK	YÜKSEK	ORTA
ORTA	YÜKSEK	ORTA	DÜŞÜK
DÜŞÜK	ORTA	DÜŞÜK	DÜŞÜK

Kullanıcı sayısı ve erişebilirlilik risk dereceleri karşılaştırılarak organizasyon hassasiyeti risk derecesi belirlenecektir. Örneğimizde

Erişebilirlilik Risk Sonucu : Yüksek

Kullanıcı Sayısı Risk Sonucu : Yüksek

Sistem Hassasiyeti Risk Sonucu : Yüksek

olarak gerçekleşecektir.

2.1.2. Sistem Karmaşıklığı

Bilgi sisteminin karmaşık olması, işlem modüllerinin, kullanıcı departman sayılarının ve teknoloji riskinin bir fonksiyonu olarak karşımıza çıkmaktadır. Teknoloji riski, bilgi teknolojileri personeline olan bağımlılık ve teknoloji seviyesinin karşılaştırılması sonucunda bulunmaktadır.

Bilgi teknolojileri personeline bağımlılık riski, bilgi sistemini bilen personelin ve dökümantasyon riskinin bir fonksiyonu olarak belirlenmektedir.

Tablo 2.6.

Personel Bilgisi

RİSK DERECESİ	TANIMLAMA
YÜKSEK	Teknoloji ve sistem fonksiyon bilgisine sahip sadece bir personel mevcuttur.
ORTA	2 veya 3 personel teknoloji veya sistem fonksiyon bilgisine sahiptir.
DÜŞÜK	3'ün üzerinde personel teknoloji ve sistem fonksiyonu konusunda bilgiye sahiptir.

Yukarıdaki tabloda görülen personel bilgisine ait risk derecesi, sistem bilgisine sahip personel sayısı ile belirlenmektedir. Örneğin organizasyonda 3'ün üzerinde personelin teknoloji ve sistem fonksiyonu konusunda bilgiye sahip olduğunu düşünelim, bu durumda risk seviyesi düşük olarak belirlenecektir.

Tablo 2.7.

Dökümantasyon

RİSK DERECESİ	TANIMLAMA
YÜKSEK	Hiç döküman yok.
ORTA	Dökümanlar güncel değil.
DÜŞÜK	Güncel dökümanlar mevcut.

Yukarıdaki tabloda görülen dökümantasyona ait risk, bilgi sistemine ait dökümanların durumuyla belirlenmektedir. Örneğin organizasyondaki bilgi sistemleri dökümanlarının mevcut olduğunu ancak güncel olmadığını düşünelim bu durumda risk seviyesi orta olarak gerçekleşecektir.

Tablo 2.8.

Personel Bilgisi Riski ve Dökümantasyon Riski Karşılaştırması

PERSONEL BİLGİSİ	DÖKÜMANTASYON SEVİYESİ		
	YÜKSEK	ORTA	DÜŞÜK
YÜKSEK	YÜKSEK	YÜKSEK	ORTA
ORTA	YÜKSEK	ORTA	DÜŞÜK
DÜŞÜK	ORTA	DÜŞÜK	DÜŞÜK

Yukarıdaki tablodan personel bilgisi riski ve dökümantasyon riski karşılaştırması sonucunda bilgi sistemleri personeline bağımlılık riski ortaya çıkacaktır. Örneğimizdeki sonuçlar karşılaştırıldığında,

Personel Bilgisi Riski Sonucu : Düşük

Dökümantasyon Riski Sonucu : Orta

Personele Bağımlılık Riski Sonucu : Düşük

olarak gerçekleşecektir.

Teknoloji riskinin belirlenmesi için, teknoloji seviyesi riski ile bilgi sistemleri personeli bağımlılık riski ile birlikte değerlendirmesi gerekmektedir. Teknoloji seviyesi riski bilgi sisteminin ne kadar süreyle organizasyonda kullanıldığı ile ilgilidir.

Tablo 2.9.

Teknoloji Seviyesi

RİSK DERECESİ	TANIMLAMA
YÜKSEK	Bilgi sistemi teknolojileri bir yıldan az ve 20 yıldan uzun süredir kullanılmaktadır.
ORTA	Bilgi sistemi teknolojileri 1 ile 4 yıl arasında kullanılmaktadır.
DÜŞÜK	Bilgi sistemi teknolojileri 4 yıldan uzun süredir kullanılmaktadır.

Yukarıdaki tabloda görülen teknoloji seviyesi risk derecesi bilgi sisteminin ne kadar süreyle organizasyonda kullanıldığının belirlenmesi ile ortaya çıkmaktadır. Örneğin organizasyondaki bilgi sisteminin 4 yıldan uzun süredir kullanıldığı düşünüşülürse risk derecesi düşük olarak gerçekleşecektir.

Tablo 2.10.

Teknoloji Seviyesi Riski ve Bilgi Sistemleri Personeline Bağımlılık Karşılaştırması

TEKNOLOJİ SEVİYESİ	BİLGİ SİSTEMLERİ PERSONELİNE BAĞIMLILIK		
	YÜKSEK	ORTA	DÜŞÜK
YÜKSEK	YÜKSEK	YÜKSEK	ORTA
ORTA	YÜKSEK	ORTA	DÜŞÜK
DÜŞÜK	ORTA	DÜŞÜK	DÜŞÜK

Yukarıdaki tabloda teknoloji riskinin belirlenmesi için teknoloji seviyesi riski ile bilgi sistemleri personeline olan bağımlılık riski karşılaştırması yapılmaktadır. Örneğimizdeki sonuçlar hatırlanacak olursa,

Personele Bağımlılık Riski Sonucu : Düşük

Teknoloji Seviyesi Riski Sonucu : Düşük

Teknoloji Riski Sonucu : Düşük

olarak gerçekleşecektir.

Organizasyonel karmaşıklık riski, organizasyonel etkilenme riski ve sistem dizaynı karmaşıklığı riskinin bir fonksiyonu olarak belirlenmektedir.

Tablo 2.11.

Organizasyonel Etkilenme

RİSK DERECESİ	TANIMLAMA
YÜKSEK	Başarısızlık tüm organizasyonu etkileyebilir.
ORTA	Başarısızlık bazı departmanları etkileyebilir.
DÜŞÜK	Başarısızlık sadece bir kullanıcıyı ve bir departmanı etkilemektedir.

Yukarıdaki tablo bilgi sistemleri bilgi sistemlerindeki bir başarısızlığın, organizasyonu etkileme riskinin belirlenmesi amacıyla kullanılmaktadır. Örneğin organizasyonun bilgi sistemindeki başarısızlığının tüm organizasyonu etkilediğini düşünelim bu durumda risk derecesi yüksek olarak ölçülecektir.

Tablo 2.12.

Sistem Dizaynı Karmaşıklığı

RİSK DERECESİ	TANIMLAMA
YÜKSEK	Sistem birbiriyle etkileşim halinde olan birden çok fonksiyonu yerine getirmektedir.
ORTA	Sistem birbiriyle bağlantılı olmayan bir çok fonksiyonu yerine getirmektedir.
DÜŞÜK	Sistem sadece bir tek performansı yerine getirmektedir.

Yukarıdaki tablo bilgi sistemleri karmaşıklığına ait risk derecesinin belirlenmesi için kullanılmaktadır. Örneğin organizasyonun bilgi sisteminin birden çok fonksiyonu yerine getirdiğini düşünelim risk derecesi yüksek olacaktır.

Tablo 2.13.

Organizasyonel Etkilenme Riski ve Sistem Dizaynı Karmaşıklığı Karşılaştırması

ORGANİZASYONEL ETKİLENME	SİSTEM DİZAYNI KARMAŞIKLIĞI		
	YÜKSEK	ORTA	DÜŞÜK
YÜKSEK	YÜKSEK	YÜKSEK	ORTA
ORTA	YÜKSEK	ORTA	DÜŞÜK
DÜŞÜK	ORTA	DÜŞÜK	DÜŞÜK

Yukarıdaki tabloda organizasyonel karmaşıklık risk derecesinin belirlenmesi için organizasyonel etkilenme ve sistem dizaynı karmaşıklığı riskleri karşılaştırılmaktadır. Örneğimizdeki sonuçlar hatırlanırsa,

Organizasyonel Etkilenmesi Riski Sonucu : Yüksek

Sistem Dizaynı Karmaşıklığı Riski Sonucu : Yüksek

Organizasyonel Karmaşıklık Riski Sonucu : Yüksek

olarak şekillenecektir.

Tablo 2.14.

Genel Karmaşıklık

ORGANİZASYONEL KARMAŞIKLIK RİSKİ	TEKNOLOJİ RİSKİ		
	YÜKSEK	ORTA	DÜŞÜK
YÜKSEK	YÜKSEK	YÜKSEK	ORTA
ORTA	YÜKSEK	ORTA	DÜŞÜK
DÜŞÜK	ORTA	DÜŞÜK	DÜŞÜK

Yukaridaki tabloda organizasyona ait genel karmaşıklık riskinin belirlenmesi için organizasyonel karmaşıkık ve teknoloji riski karşılaştırılmaktadır. Örneğimizdeki sonuçlar hatırlanacak olursa,

Organizasyonel Karmaşıklık Riski Sonucu : Yüksek

Teknoloji Riski Sonucu : Düşük

Sistem Karmaşıklığı Riski Sonucu : Orta

olarak şekillenecektir.

2.1.3. Sistem Güveni

Güven riski organizasyonda görev alan insan faktörleriyle ilgilenmektedir. Sistem güvenliğine ait risk organizasyonda çalışanlara ve yöneticilere olan güvenin belirlenmesiyle elde edilmektedir.

Tablo 2.15.

Çalışanların Geçmişinin Araştırılması

RİSK DERECESİ	TANIMLAMA
YÜKSEK	Daha önceki çalışmasına ilişkin hiç bir kontrol yapılmamıştır.
ORTA	İstihdam gerçekleştirilmeden önce çalışan kalifikasyonu ve referanslar kontrol edilmemiştir.
DÜŞÜK	Normal geçmiş kontrollerine ek olarak, kredi referansları ve suç kayıtlarıda kontrol edilmiştir.

Yukarıdaki tablo çalışanlara olan güvenin risk derecesinin ölçülmesi amacıyla çalışanların geçmişine ait kontrol çalışmalarının yapılıp yapılmadığının belirlenmesi için kullanılmaktadır. Örneğin organizasyon çalışanlarının istihdam edilmeden önce referanslarının kontrol edilmediğini düşünelim bu durumda risk derecesi orta olarak gerçekleşecektir.

Tablo 2.16.

Bilgi Sistemleri Güvenliği ve Yönetim İlgisi

RİSK DERECESİ	TANIMLAMA
YÜKSEK	Yönetim geçmişte yaşanan bilgi sistemi güvenlik başarısızlığı ile yakından ilgilidir.
ORTA	Yönetim bilgi sistemleri güvenlik başarısızlığı ile ilgilidir ancak başarısızlığa ait kesin kanıt yoktur.
DÜŞÜK	Yönetimin ilgisi yoktur.

Yukarıdaki tablo organizasyon yönetimine ait güvenin ölçülmesi amacıyla bilgi sistemlerindeki güvenlik başarısızlıkları ile yönetimin ilgisi araştırılmaktadır. Örneğin organizasyonda bilgi güvenliği ihlallerine dair yönetimin hiç bir ilgisinin olmadığını düşünelim bu durumda yöneticilerle ilgili güven riski düşük olarak gerçekleşecektir.

Tablo 2.17.

Çalışanlara Güven Riski ve Yönetime Güven Riskinin Karşılaştırılması

ÇALIŞANLARA GÜVEN RİSKİ	YÖNETİME GÜVEN RİSKİ		
	YÜKSEK	ORTA	DÜŞÜK
YÜKSEK	YÜKSEK	YÜKSEK	ORTA
ORTA	YÜKSEK	ORTA	DÜŞÜK
DÜŞÜK	ORTA	DÜŞÜK	DÜŞÜK

Yukarıdaki tabloda genel genel güven riskinin belirlenmesi amacıyla çalışanlara ve yönetime olan güven riskleri karşılaştırılmaktadır. Örneğimizdeki sonuçlar hatırlanırsa

Çalışanlara Güven Riski Sonucu : Orta

Yönetime Güven Riski Sonucu : Düşük

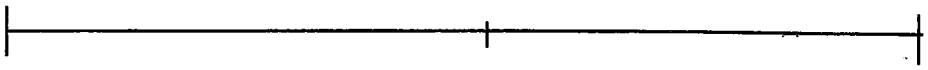
Sistem Güven Riski Sonucu : Düşük

olarak gerçekleşecektir.

2.1.4. Risk Ölçüm Sonucunun Belirlenmesi

Risk ölçümüne ait sorular cevaplandırılıp her bölüme ait risk durumları belirlendikten sonra sıra bu risk ölçüm sonucunun belirlenmesi için bu sonuçların toplanmasına ve risk seviyesinin tespit edilmesine gelmiştir.

Hatırlanacağı gibi risk ölçüm modelinde genel risk; Sistem Hassasiyeti, Sistem Karmaşıklığı ve Sistem Güveni'ne ait sonuçların toplanmasıyla belirlenmektedeydi ve çıkan sonuç aşağıdaki ölçümle karşılaştırılarak risk derecesi belirleniyordu.



Düşük Risk	Orta Risk	Yüksek Risk
3 Puan	6 Puan	9 Puan

Örneğimizdeki sonuçlar hatırlanacak olur ise

Sistem Hassasiyeti Risk Sonucu	:	Yüksek	=	3 Puan
Sistem Karmaşıklığı Riski Sonucu	:	Orta	=	2 Puan
Sistem Güveni Riski Sonucu	:	Düşük	=	1 Puan

Toplam Risk Sonucu	:	6 Puan
Genel Risk Seviyesi	:	Orta

olarak gerçekleşecektir.

Denetimin yöneten kişi genel risk seviyesini belirledikten sonra, söz konusu denetimin başarıyla gerçekleştirilmesi için kaynakların nasıl tahsis edileceğini belirlemesi gerekmektedir.

Denetim çalışmasında risk seviyesi belirlenip, kaynak tahsisi yapılırken mutlaka mevcut risk düzeyinin organizasyon için finansal etkilerinin de belirlenmesi gerekmektedir.

Bu amaçla bilgi sisteminde meydana gelebilecek güvenlik başarısızlıklarının meydana getireceği finansal sonuçlarla ilgili olarak, kontrol altında olan organizasyon varlıklarının değeri dikkate alınmalıdır. Buna ek olarak, başarısızlık nedeniyle meydana gelecek olan organizasyonun şöhretindeki kayıbın değeri ve yasal cezalar da hesaba katılmalıdır.

2.2. Denetim Uygulamasının Gerçekleştirilmesi

Bilgi sistemleri denetim uygulamaları, denetim çalışmalarından elde edilecek sonuçlar gözönünde bulundurulduğunda,

a) Güvenlik denetimi,
b) Etkinlik ve verimlilik denetimi

olmak üzere iki alt başlıkta incelenebilir.

2.2.1. Güvenlik Denetimi

Güvenlik, aslında tüm denetim çalışmalarının özünü ve nihai amacını oluşturmaktadır. Bilgi sistemlerinde güvenlik denetimi,

a) Fiziki Varlık Güvenliği
b) Bilgi Güvenliği

olmak üzere iki alt başlıktan oluşmaktadır.

2.2.1.1. Fiziki Varlık Güvenliği

Bir organizasyonda bilgi sistemlerine yapılan yatırımların önemli miktarlara ulaşması ve bilgi sistemleri tarafından gerçekleştirilen operasyonların bir organizasyonun devamlılığı ve başarısı açısından son derece önemli olması nedeniyle, tüm bilgi sistemi elemanları onları zarar uğratacak veya yok edecek fiziki tehditlere karşı korunmalı ve bu korunmayı sağlayacak kontrol çalışmaları yürütülmelidir.

Bilgi sistemi fiziki varlıklarının güvenliğinin sağlanmasındaki tüm önlemler bir organizasyonun tüm katmanlarında organize edilmeli ve bir merkezden koordine edilmelidir. Bilgi sistemlerinin fiziki varlık güvenliğine ilişkin denetimler,

a) Bilgisayar donanımların yerleşimi,
b) Fiziki erişim,
c) Yangınlar,
d) Sel baskınları,

e) Güç kayıpları, havalandırma bozuklukları ve radyasyon

başlıkları dikkate alınarak gerçekleştirilmektedir. [20]

2.2.1.1.1. Bilgisayar Donanımlarının Yerleşimi

Tüm bilgisayar sistemleri donanımları bir binada maksimum güvenliği sağlayacak şekilde yerleştirilmelidir. Merkezi bilgisayar donanımının yerleşimi, onlara zarar verecek kişilerden korunmak amacıyla, haritalarla ve işaretlerle kesinlikle belirtilmemeli ve mümkün olduğunca saklanmalıdır.

Bilgisayar merkezleri benzin ve gaz depoları, düzenli olarak su baskınlarının olduğu yerler ve havalimanlarının yakınında olmamalıdır. Benzin ve gaz depolarında meydana gelebilecek patlamalar, bilgisayar ekipmanlarına ve binalara zarar verebilecektir. Su baskınlarının tehlikesi detaylı anlatılmasına gerek olmayacak şekilde açıktır. Havalimanlarında meydana gelen sarsıntı ve titreşim bilgisayar ekipmanlarına önemli zararlar verebilecektir. Ayrıca havalimanları, radarlardan ve hava trafik kontrolü ekipmanlarından elektromanyetik radyasyon yayılan yerlerdir ve bu radyasyon bilgisayar donanımlarında ve operasyonlarında zarar meydana getirecektir. Şayet seçtiğimiz alan havalimanlarına yakın olmak zorunda ise, donanımlar bu radyasyondan korunacak şekilde ilgili araçlarla kaplanmalıdır.

Binanın içine dışarıdan girişi sınırlandırmak için dış sınırı belirleyen çitleme işlemi gerçekleştirilmelidir. Bu çitleme sistemi bilgisayar merkezlerinin sınırlarını belli edecektir. Bilgisayar merkezinin bulunduğu mekanların dış duvarları dayanıklı bir şekilde inşa edilmeli ve dışarıdaki kazai veya kasıtlı patlamalara dayanıklı şekilde dizayn edilmelidir.

Ayrıca bilgisayar odaları ve diğer önemli hizmetler dış duvarların hemen yanında bulunmamalıdır. Çünkü patlama ilk önce dış duvarlara zarar vereceğinden

---

[20] Alan Oliphant, "An Introduction to Computer Auditing- Part Deux, No:7'", ITAUDIT.ORG, January 15, 2000, (Çevirimiçi) http://www.itaudit.org/forum/newitauditor/f302na.htm

bilgisayarların böyle bir patlama nedeniyle hasar görmesi yüksek bir ihtimal olarak karşımıza çıkacaktır.[21]

Duvarlar tırmanmayı güçleştirecek ve bu şekilde yetkisiz ulaşımı engelleyecek şekilde düz olmalıdır. Çatılar hassas noktalardır ve bu alanlar nadiren korunmaktadır. Çatılar herhangi bir cismin delip geçmesine dayanacak şekilde güçlü inşa edilmelidir. Bu cisimler kazaen uçaktan düşebileceği gibi kasıtlı olarak da çatılara atılabilecektir.

Bilgisayarların bulunduğu binaların dış duvarlarında minimum seviyede kapı ve pencereler olmalıdır. Bu sayede binaya giriş noktaları azalacaktır. Bu durum organizasyona giriş kontrolünün etkin bir şekilde yapılmasını sağlayacaktır. Pencereler izinsiz giriş için önemli bir risk unsurudur. Ayrıca pencereden atılan cisimler bilgisayar ekipmanlarına zarar verecektir. Tüm pencereler yetkisiz girişleri engelleyecek şekilde korunmalıdır.

Tüm kapılara uygun kilitler takılmalıdır. Anahtar kartlar vasıtasıyla elektronik olarak kontrol edilen kapıların olması kontrol açısından daha iyi olacaktır. Kartlar ile yetkili personelin anahtar kullanımları elektronik ortamda belirtilmelidir. Bu bilgiler denetmenlere çalışmaları sırasında kimin ne zaman bilgisayar odasını kullandığını görmesine ve anlamasına yardımcı olacaktır. Bu tarz kilitler yüksek hassasiyet taşıyan ve sınırlı erişim istenen bilgisayar odalarında mutlaka kullanılmalıdır. Kapılar bir kerede yanlız personelin geçeceği şekilde dizayn edilmelidir. Zira zaman zaman yetkisiz kişiler yetkili kişilerle aynı anda geçebilmektedir.

Bilgisayar donanımları bir organizasyon içinde fiziksel olarak diğer departmanlardan ayrılmalıdır. Bilgisayar cihazlarının fiziki ayrımı kasıtlı ve kasıtsız güvenlik ihlallerine karşı koruyacaktır. Çok katlı binalarda sel baskınından ve dış izinsiz girişlerden korkuluyorsa, bilgisayar cihazları yukarıdaki katlarda tutulmalıdır. Sel baskını olabilecek yerlerde bilgisayar donanımları kesinlikle bodrum katlarda korunmamalıdır. Çimento duvarlar ve katlar toz önleyiciler ile doldurulmalıdır. Toz şayet serinletici pencereler ve benzerleri araçlar bilgisayar ekipmanlarına önemli zarar verebilecektir.

---

[21] Alan Oliphant, a.g.k.

Bu durum bilgisayarların bozulmasına neden olan kısa elektrik kesintilerine yol açacaktır.

Yangın çıkışını ve yayılmasını engelleyecek binanın dizaynında bazı önlemler alınmalıdır. Genel bir yol gösterici olarak aşağıdaki önlemler alınmalıdır.

Bilgisayar operatörleti için uygun bir çalışma alanı sağlanmalıdır. Işık, ısı, gürültü ve benzerleri dikkate alınmalıdır. Operatötlerin çalışma ortamındaki mutlulukları sağlanmalıdır. Mutlu operatörler bilgisayar ekipmanlarının bakımına daha fazla önem verir ve daha yoğun bir şekilde bakımlarıyla ilgilenirler.

Sigara içmek, yemek ve içmek bilgisayar odasında ve bilgisayarların yanında yasaklanmalıdır. Bu önlem hassas bilgisayar ekipmanına zararlar veren yemek ve sıvı dökülmesine karşı koruyucu tedbir getirecektir.

Tüm bilgisayarların ve ilgili ekipmanın temizlenmesi, yer değiştirmesi ve korunması uzman kişiler tarafından yapılmalıdır. Bilinçsiz kişiler tarafından gerçekleştirilecek taşınma ve temizleme bilgisayar donanımları üzerinde kalıcı hasarlara neden olabilecektir.

2.2.1.1.2. Fiziki Erişim Kontrolü

Bilgisayar merkezi fiziki güvenliği sağlayacak şekilde dizayn edildiğinde, erişim kontrolü kavramı etkin hale getirilebilecektir. Uygulanan erişim kontrol koruma seviyesi değerlendirilirken ve incelerken aşağıdaki prensipler gözönünde tutulmalıdır.

Bilgisayar ekipmanının olduğu binaya giriş için sadece yetkili personele izin verilmelidir. Bilgisayar operasyonları merkezi veya teyp veya disk gibi daha hassas ekipmanlara erişim daha da sınırlandırılmalı ve girişler sadece günlük işlemlerin gerçekleştirilmesi ve ekipmanların doğru çalışmasının sağlanması için yapılmalıdır:

Günümüzde operatörlerin bilgisayar ekipmanlarından ayrı bir yerde çalışma eğilimi mevcuttur. Operatörler sadece sistem konsülüne ve yazıcılara ihtiyaç duyacağından ayrı yerde çalışma, bilgisayar donanımları üzerindeki fiziki zarar riskini azaltacaktır.

Bazı kayıt sistemleri formları merkezi bilgisayar alanına giriş kayıdı ve sınırlandırılması için kullanılmalıdır. Böyle bir sistem değişik hassasiyet alanlarına değişik erişim haklarına izin verir. Düzenli çalışan personel organizasyonu kayıt sisteminin kullanılmasıyla kontrol edilmeli ve kabul edilmelidir.

Güvenli alana giren personeller mutlaka tanımlanmalıdır. Yetkili personeller, personelin anahtar kayıtlarıyla tanımlanabilmektedir. Bu ziyaretçileri tanımlamak kadar kolay değildir. Ziyaretçiler minimum seviyede tutulmalı ve bilgisayar tesislerini gösterecek turlar mümkün olduğunca az yapılmalıdır. Şayet ziyaretçiler gerekli ise, bu ziyaretçilere ziyaret süresince eşlik edilmeli, onların tanınmasının sağlayan rozetler takılmalıdır. Eşlik edilmeyen tüm ziyaretçilere dikkat edilmeli ve tüm personel eşlik edilmeyen ziyaretçilerin tehlikesi konusunda eğitilmelidir. Bilgisayar merkezi çalışanları için sadece bir giriş ve çıkış kapısı sağlanmalıdır. Diğer tüm kapılar kapalı olmalıdır, diğer kapılar alarmlar gibi yeterli güvenlik araçlarıyla donatılmalıdır. [22]

Bilgisayar merkezindeki girdi ve çıktı yapılan araçlarına fiziki erişim sınırlandırılmalıdır. Gerek çalışanlara gerekse ziyaretçilere ait tüm paketler, çantalar, el çantaları, bilgisayar alanlarında ve benzer hassas alanlarda yasaklanmalıdır. Bu önlem bilgisayar merkezlerindeki medya araçlarında tutulan bilgilerin yetkisiz kişiler tarafından bazı araçlara kopyalanarak alınmasını engelleyecektir.

Binadaki tüm alanlar her zaman gözlem altında tutulmalıdır. Yeterli ışık tertibatı binanın tüm gece aydınlatılmasını sağlayacak şekilde kurulmalıdır. Kameralar güvenlik elemanlarının izinsiz girişleri gözlemleyebilmeleri için kullanılmalıdır. Tüm kapılar titizlikle gözlemlenmeli ve özellikle yangın çıkışlarına özel önem verilmelidir. Kapılar izinsiz giriş alarmları ile donatılmalıdır. Aynı zamanda kapılara izinsiz giriş için yaklaşımları tespit edecek dedektörlerin yerleştirilmesi faydalı olacaktır.

[22] Alan Oliphant, a.g.k.

2.2.1.1.3. Yangınlar

Bir bilgi sistemini tehdit eden temel tehditlerden birisi de bir saldırı sonucunda veya kaza sonucu çıkan yangınlardır. Tüm bilgisayar donanımının yangına karşı korunduğunun ve bu korumanın sürdürüldüğünün denetmenler tarafından tespit edilmesi gerekmektedir.

Yangının etkileri;

a) Donanımın doğru yerleştirilmesi,
b) Yangın tespit edicileri,
c) Yangın söndürücüleri,

sayesinde minimize edilebilmektedir. [23]

Temel kural olarak beton ve çelik iyi yanmamaktadır, ancak plastik, ağaç ve benzeri maddeler yoğun bir yangına sebep verebilmektedir. İnşaat yapısıyla ilgili olarak bu durumun mutlaka denetmenler tarafından kontrol edilmesi gerekmektedir. İnşaat maddelerinin çoğunun yüzeyin altında olduğu unutulmamalıdır.

Kablolar bilgisayar ekipmanlarının vazgeçilmez unsurlarıdır. Kablolar plastik malzemesiyle kaplandığı için yangın açısından tehlike meydana getirmektedir. Bu nedenle tüm kablo kanallarının yangına karşı korunduğu izlenmeli ve belirlenmesi gerekmektedir.

Bilgisayar odaları genellikle binalarda dağınık yerlerde tutulurlar. Bu nedenle olası bir yangın durumunda bilgisayar donanımları kolayca çıkartılmaz ve zarar görür. Bir yangın durumunda boşaltma, tahliye rotasının belirtilmesi ve bu rotanın ışıklarla donatılması söz konusu donanımların zarar görme olasılığını azaltacaktır.

Aynı zamanda periyodik olarak yangın tahliye alıştırmalarının yapılması faydalı olacaktır. Bu alıştırmalar sayesinde insanlar yangın başladığında durup yangın direktiflerini okumak zorunda kalmayacak ve zaman kaybetmeyeceklerdir.

---

[23] Alan Oliphant, a.g.k.

Bilgisayar odalarında, yanıcı maddelerin bulundurulmaması gerekmektedir. Zira bir çok organizasyonda bilgisayar donanımını temizleyici araçlar ve çözücüler bilgisayar odasında tutulmamalıdır.

Tüm binayı ateş geçirmez maddelerle ve cihazlarla donatmak ekonomik koşullar nedeniyle mümkün olmamaktadır. Bu nedenle yangın dedektörleri önemli bir görev üstlenmektedir. Yangın dedektörleri bilgisayar merkezinin tüm alanına yerleştirilmeli ve yangın dedektörleri ısıyı, dumanı tespit edebilmelidir. Tüm dedektörler 24 saat boyunca veri iletimi ile bir merkezden izlenmelidir. Bu merkez şayet tespit edilen yangın varsa derhal itfaiyeye haber veren iletişime sahip olmalıdır. Bu ekipmanların düzenli olarak çalışıp çalışmadığı da kontrol edilmelidir.

Bir binada yangın çıkması veya tespit edilmesi durumunda, yangının itfaiye yetişene kadar yayılmaması ve diğer cihazlara zarar vermemesi için yangın söndürücülerin kullanılması gerekmektedir. Yangın söndürücülerin düzenli olarak bakımları yapılmalı ve bu araçların kullanımı için personele eğitim verilmelidir.

Binanın duvarları, çatısı, iç donanımları, mobilyaları, klima ve elektrik kanal hatları yanmaz malzemelerden yapılmalıdır. Bu yangının yayılmasını engelleyecektir. Bilgisayar odası binanın diğer bölümlerinden yanmaz malzemelerle yangına en az iki saat dayanacak şekilde ayrılmalıdır. Bu önlem bilgisayar cihazlarının dışında yangın çıkması durumunda, bilgisayar cihazlarının zarar görmeden müdahale edilmesi için zaman verecektir.

Ayrı bir teyp, disk depolama kasası, ateş iletmeyen duvarlar, otomatik olarak kapanan yangın kapısı, alarmlar ve otomatik yangın söndürme cihazı ile korunmalıdır. Bu durum yedekleme malzemelerinin bilgisayar odasında başlayan bir yangından korunmasını sağlayacaktır.

Bilgisayar ekipmanı ihtiva eden tüm ortamlar düzenli olarak temizlenmelidir. Toz, kir ve çöp ve atık birikmesi, küçük bir yangının büyümesine yol açacaktır.

2.2.1.1.4 Su Baskınları

Yangınlara karşı önlemler alınırken, bu sefer iç veya dış kaynaklı olarak zarar su baskınından meydana gelebilir. Bilgisayar merkezleri su altında kalabilecek alçak yerlerde kurulmamalıdır. Bilgisayar merkezlerinin bodrum katında veya diğer suyun ulaşabileceği yerlerde kurulmaması gerekmektedir. Bilgisayar merkezine giriş yer seviyesinden yukarıda olmalıdır. Zira su baskını meydana gelirse suyun merkeze girişi böylece güç olacaktır. Dış duvarlarda suyun kolayca girmesini sağlayan çatlak yerlerin olmamasına özen gösterilmelidir. Tüm kablo kanalları su geçirmeyecek malzemelerle kaplanmalıdır.[24]

Kanalizasyon ve su kanalları şayet su baskını meydana gelirse suyun kolayca boşaltılabilmesini sağlayacak şekilde açık tutulmalıdır. Ancak su baskınlarının bazen bu yollarla geleceği de unutulmamalıdır.

Su borularının bilgisayar odasından geçmesine izin verilmemelidir. Patlak iç borular bilgisayar odası su baskınlarının en önemli nedenlerinden birisidir. Şayet yangına su serpen sistemler varsa, bu sistemlerin kuru olduğuna ve ancak yangın durumu olduğunda harekete geçeceklerinden emin olunmalıdır.

Tavanlardaki muhtemel potansiyel sızıntı ve çatlaklar araştırılmalı ve önlemler alınmalıdır.

2.2.1.1.5. Güç Kayıpları, Havalandırma Bozuklukları ve Radyasyon

Elektrik olmadan bilgi sistemlerinin çalıştırılması mümkün değildir. Dünyadaki hiç bir yerde elektrik gücün her gün her dakika geleceği garanti edilemez ve her organizasyon zaman zaman bilgisayar sistemlerinin ihtiyaç duyduğu gücü elde edemeyebilmektedir.

Bilgi sistemlerinin sürekli çalışması için elektrik kesintilerine karşı güç kaynaklarının kullanılması gerekmektedir. Aksi taktirde bilgi sistemi işlemleri yapılamayacaktır.

---

[24] Alan Oliphant, a.g.k.

Bu nedenle güç kaynakları korunmalı ve tüm dönüştürücü ekipman güvenli alanlarda tutulmalıdır. Bunların kurcalanması ve oynanması engellenmelidir. Cihazların sürekli ve düzenli voltaj ve akışa sahip olduğundan emin olunmalıdır. Şayet ana cihazlar bozulursa, elektrik üreticileri yedekte olmalıdır. Kesintisiz güç kaynağı tüm bilgisayar donanımları için gereklidir. Ayrıca jeneratörlerin en azından haftada birkez çalışıp çalışmadığı test edilmelidir. [25]

Havalandırma; Bilgisayar donanımları ciddi miktarda ısı meydana getirirler bu nedenle iklimlendiriciler bu ısıyı ortadan kaldırmak için kullanılmalıdır. Şayet bu yapılmazsa bilgisayarlar etkin çalışmalarını durdurma eğilimine sahip olacaktır. Bu nedenle havalandırma çalışmaları yeterli şekilde gerçekleştirilmelidir.

Radyasyon; Bilgisayar ekipmanı elektromanyetik radyasyon için oldukça duyarlıdır. Tüm bilgisayarlar elektromanyetik radyasyondan sakındırılmalıdır. Bilgisayar odası TV, radyo gibi cihazlardan olabildiğince korunmalıdır ve tecrit edilmelidir.

2.2.1.2. Bilgi Güvenliği Denetimi

Güvenlik denetiminin ikinci alt başlığı olan bilgi güvenliği denetiminin amacı bilginin yetkisiz kişilerin eline geçmeden, doğru ve bütünlüğünü koruyacak şekilde ve zamanında talep edilen bilginin talep eden kişilere ulaşmasını sağlayacak yapıya ait kontroller sisteminin bir organizasyonda kurulup kurulmadığının belirlenmesidir.

Temel olarak bakıldığında bilgi güvenliği denetimi,

a) Girdi,
b) İşlem,
c) Çıktı,
d) İletişim ve Erişim,
e) Veri Tabanı ve Veri Yönetimi,
f) Üst Yönetim.

başlıklarına ait kontrol sisteminin denetlenmesinden ibarettir.

---

[25] Alan Oliphant, a.g.k.

2.2.1.2.1. Veri Girişi

Veri girişi bilgi sistemleri içinde yer alan bir alt sistemdir. Bu alt sistem, bilgi sistemindeki veri'nin, bilgiye dönüşme süreci için bilgi sistemine girilmesi fonksiyonunu yerine getirmektedir. Veri girişi bir bilgi sistemindeki en fazla düzenli olarak insan müdahalesinin olduğu aşamadır.

Veri giriş alt sistemi düzenli insan müdahalesinin olması nedeniyle, hataların ve aldatmaya yönelik işlemlerinde en fazla çıkma olasılığı olan bölümdür. Bu nedenle veri girişi kontrollerinin yeterliliği ve güvenliği üzerinde yapılacak denetim çalışmaları özel bir önem taşımaktadır. Zira bu aşamada meydana gelecek olan hatalı bir veri girişi yanlış ve işe yaramaz bilgilerin meydana gelmesine neden olarak bilgi sisteminin etkinliğini olumsuz etkileyecektir.

Veri girişine ait gerçekleştirilecek denetim çalışmaları aşağıdaki

a) Veri giriş yöntemi
b) Veri giriş ekranlarının yapılandırılması
c) Veri girişinde işlem hızı ve cevap verme çabukluğu
d) Veri girişinde kullanıcıya sağlanacak yardımlar
e) Veri girişinde kodlama sistemi
f) Veri girişinde yığın kontrolü
g) Veri girişinin onaylanması, hataların tespiti ve raporlanması

başlıklardan oluşmaktadır.

Günümüzde veri'ler bilgi sistemine çeşitli yöntemlerle girilebilmektedir. Bu yöntemlerden en önemlisi veri'nin kullanıcı tarafından bilgi sistemine direkt olarak girilmesidir. Örneğin bankalardaki banko elemanları bilgi sistemine işlemleri direkt olarak girmektedir. Diğer bir önemli yöntem ise veri girişinde kaynak dökümanlarının kullanılmasıdır. Kaynak dökümanları olayın gerçekleşmesiyle veri girişinin yapılması arasında zaman geçmesi durumunda kullanılmaktadır.

Kaynak dökümanlarındaki en önemli konu ise elde edilmek istenen verinin nasıl toplanacağı, nasıl biriktirileceği ve evrakların nasıl saklanacağı gözönünde bulundurularak kaynak dökümanının bu şartları sağlayacak şekilde dizayn edilmesidir. Kaynak dökümanlarının en önemli faydası veri girişindeki hata oranını azaltmaları ve veri giriş hızını arttırmalarıdır. [26]

Veri girişinde diğer önemli bir yöntem ise dokunmatik ekranlar ve sesler gibi ortamlarla kullanıcının veri girişini yapması yöntemidir. Ayrıca bazı araçlarla daha önceden girilmiş verilerin kullanılması da veri girişinde mümkün olmaktadır. Örneğin bir plastik kartın arkasına manyetik olarak hesap sahibinin hesap numarası kaydedilmiş olması ve bunun POS cihazları tarafından okunması bu tür bir veri girişine örnek olarak verilebilir.

Günümüzde veri girişi sırasında sıklıkla yukarıda belirtilen veri giriş yöntemlerinin bir kombinasyonu karşımıza çıkmaktadır. Örneğin banka müşterileri ATM kullandıklarında makina bilgiyi plastik karttan okumaktadır. Bu önceden kaydedilmiş bir bilgidir. Ancak daha sonra banka müşterisi kendisine ait bilgileri sisteme direkt olarak kendisi girmektedir.

Veri giriş yöntemleri kendilerine ait bazı güçlü ve zayıf yönler taşımaktadır. Denetmenler,

a) Veri girişinde insan müdahalesinin artmasının hataları arttıracağını,
b) Olayın meydana gelmesiyle verinin sisteme girilmesi arasındaki zaman farkının hataların ve suistimallerin artmasına neden olacağının,
c) Veri girişinde araçların kullanılması hataların azalmasını sağlayacağını.

gözönünde bulundurarak organizasyonları için hangi veri giriş yönteminin daha uygun olacağına karar vererek mevcut durumlarını sorgulamaları ve bununla ilgili kontrolleri gözden geçirmeleri gerekmektedir.

---

[26] Donald A. Watne, Peter B.B. Turney, Auditing EDP Systems, Prantice Hall, Inc., New Jersey, Second Edition, 1990, p. 313

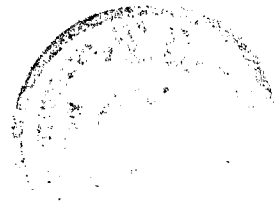
Veri girişi konusundaki diğer bir önemli konu ise bilgi sistemlerindeki veri giriş ekranlarının doğru olarak yapılandırılmasıdır. Zira doğru olarak yapılandırılmış ekran dizaynı verilerin sisteme daha etkin ve verimli şekilde girilmesini sağlayacaktır. Bu nedenle denetmenler bilgi sistemine veri girişi sırasında ekranın kullanıcı kolaylığını sağlayacak şekilde ve kullanıcının ilgili bölümleri karıştırmadan veriyi doğru alanları girmesine yardım edecek şekilde dizayn edilip edilmediklerini değerlendirmelidir.

Veri girişi sırasında kullanıcılar girdikleri verilere ait sistemin en çabuk şekilde cevap vermesini ve girdikleri karakterlerin ekranda çabuk bir şekilde görünmesini isterler. Bu durumun aksi olması durumunda kullanıcılar veri girişine ait hızlarını ve ilgililerini kaybeder ve bu durum hatalı veri girişlerinin olmasına neden olur. Bu nedenle denetçiler veri giriş sisteminin cevap verme süresinin uzunluğunu ve karakterlerin görünme çabukluğu konusunda inceleme yapmalı ve konuyla ilgili peridyodik kontrolleri test etmelidir.

Veri girişi sırasında, sisteme veri girişi yapan kişiye sistemin yol göstermesi ve veri girişinde nasıl ilerlemesi gerektiği konusundaki yardımlar veri girişinin doğruluğunu ve hızını arttıracaktır.

Veri girişi sırasında zaman zaman kodlar kullanılmaktadır. Kodların temel amacı uzun metinlerle açıklanması gereken veri grublarının daha kolay bir şekilde belirlenebilmesidir. Veri girişi yapılması sırasında kodların kullanılmasıyla ilgili sorunlarla karşılaşılmaktadır. Bu nedenle seçilen kodların hatalı yazımını engelleyecek şekilde kod mimarisinin kullanılması da kontrol edilmesi gereken başlıklar arasında yer almaktadır.

Sisteme veri girişi yapıldıktan sonra verilerin mümkün olduğunca çabuk bir şekilde onaylanmalı ve şayet hatalar varsa düzeltilmelidir. Bilgi sistemlerindeki veri onay ve hata düzeltme süreci denetmenler tarafından kontrol edilerek sistemin işleyişi belirlenmelidir. Ayrıca veri girişinden sonra hata raporları üretilmeli ve gerekli ikazlar bu konuda sorumlu olan kişilere ulaştırılmalıdır. Söz konusu hata raporlama süreci de denetmenler tarafından kontrolü gereken başlıklar arasında yer almakktadır.



Veri giriş aktivitelerinin doğruluğunu kontrol etmede en etkili yöntem yığınların gözden geçirilerek işlem doğruluklarının tespit edilmesidir. Bu şekilde sisteme girilen verilerin gruplandırılması sonucunda oluşan yığınlardan elde edilen sonuçlar verilerin kaynağını oluşturan işlemlerle kontrol edilerek doğruluğu belirlenmiş olur. Denetmenler bilgi sistemleriyle ilgili yığın kontrollerinin etkinliğini belirlemelidirler.

2.2.1.2.2. Erişim

Erişim sistemi bir bilgi sisteminin kendi alt sistemi ve sistemlerle arasındaki bilginin güvenli ve hızlı bir şekilde taşınması ve bilgisayar sisteminin kendisiyle bilgisayar sistemi kullanıcıları arasında iletişim noktası kurma fonksiyonunu yerine getirmektedir. Erişim sisteminin temel amacı bilgisayar sistemiyle ancak izin verilen ve yetkilendirilmiş kullanıcıların etkileşime girmesidir.

Erişim sistemi bir bilgi sisteminin alt sistemdir. Bir iletişim sistemi merkezi işlemci ile disket sürücüsü arasındaki kablo hattı kadar basit olabileceği gibi karmaşık iletişim ağları gibi detaylı olabilir.

Günümüzde bilgi sistemleri etkinlik, verimlilik ve güvenliğinin sağlanmasında erişim sisteminin önemli bir payı vardır. Bankacılık sektörünün ülkemizde ve dünyada göstermiş olduğu elektronik bankacılıktaki ilerlemeler iletişim ağlarının önemini bir kez daha gözönüne sermektedir. [27]

Erişim alt sistemine ait gerçekleştirilecek denetim çalışmaları

a) İletişim bozuklukları
b) Donanımlardaki arızalar
c) Yıkıcı tehditler

olmak üzere iki alt başlıktan oluşmaktadır.

---

[27] Alan Fuhrman, "Your E-Banking Future", Strategic Finance, April, 2002, (Çevirimiçi) http://www.strategicfinancemag.com/2002/04g.htm

Erişim alt sisteminde çeşitli sorunlar gündeme gelebilmektedir. Bu sorunlardan ilki iletişim bozuklukları nedeniyle gönderilen ve alınan veri arasında farklılık meydana gelmesidir.

İletişim bozukluğu ilk olarak veri iletimindeki işaret zayıflıklarından meydana gelebilir. Genellikle bu durumlar için analog işaretlerde kuvvetlendiriciler, dijital işaretlerde ise tekrarlayıcılar kullanılmaktadır. İkinci olarak iletişim bozuklukları gecikmelerden dolayı ortaya çıkmaktadır. Bu durum genellikle kablo ve tellerle yapılan iletişim sürecinde meydana gelir. Farklı işaret sıklığı, farklı dalgalarla hareket edeceğinden, farklı sıklık içeriğine sahip işaretler farklı gecikmeler meydana getireceğinden dolayı iletişim bozukluğu meydana gelecektir. Uzaydan ve havadan yapılan iletişimde gecikmeler söz konusu olmamaktadır. Üçüncü olarak, gürültüler iletişim bozukluğu meydana getirirler.

Gürültüler geçiş sağlayan iletişim aracıların performansını azaltan tesadüfü işaretlerdir. Gürültü, bir iletişim aracı üzerinden veri aktarımı çoğaltıkça artmaktadır. Örneğin, şayet kamusal telefon değişim ağı veri aktarımı için kullanılırsa, artan trafik gürültü meydana getireceğinden hat hataları artmaya başlar. Tüm iletişim bozukluğuna neden olan bu nedenlerle ilgili, bilgi sistemi görevlileri gerekli önlemleri almalı ve gerekli kontrol mekanizmasını kurmalıdırlar.

Erişim alt sisteminde meydana gelen sorunlardan bir diğeri de iletişim alt sisteminin öğelerini meydana getiren

a) İletişim aracıları örneğin mikro dalgalar ve kablolar
b) Donanımlar örneğin modemler, portlar ve güçlendiriciler
c) Yazılımlar örneğin veri sıkıştırma ve havuzlama yazılımları'nda

meydana gelen arıza ve bozulmalar nedeniyle aktarılmak istenen verilerin istendiği gibi aktarılamamasıdır. Bu nedenle denetmenler bu iletişim alt sistemi öğelerine ait gerekli kontrol süreçlerini izleyerek yeterliliği konusunda yorum yapmalıdırlar.

İletişim alt sisteminde meydana gelen sorunlardan diğeri birisi de yıkıcı saldırılardır. Bu saldırıların amacı bilgisayar suçlarının işlenmesidir. Bilgisayar suçları, bir suçun işlenmesi için bilgisayarın bir araç olarak kullanılmasıdır veya bilgisayar donanımlarının çalınması gibi bilgisayara karşı suç işlenmesidir. [28] Internet ortamındaki iş kapasitesinin artmasıyla birlikte, bilgi sistemlerine yapılan saldırılar artmıştır. 1994'den yılından 1999'a kadar internet kaynaklı saldırılar 4 kat artmıştır. [29]

Bilgisayar suçları elektronik ticaret ortamında oldukça yaygın olan bir risktir. Bilgisayar suçları sadece organizasyonların dışından organizasyonun ağ bağlantılarını kullanan kişiler tarafından gerçekleştirilmemekte aynı zamanda organizasyonun içinde yer alan organizasyon üyeleri tarafından da gerçekleştirilebilmektedir. [30] Günümüzde bilgi sistemlerine izinsiz giriş yapan hackerler bilgi sistemleri güvenliği açısından önemli bir tehdittir. Hacker'lar her hangi bir kişinin veya organizasyonun bilgisayarına veya bilgisayar sistemine izinsiz olarak giren kişilerdir. Bu kişiler zaman zaman suç işlemek amacının dışında sadece eğlence olsun diye bu tür eğlemlerini gerçekleştirebilmektedirler.[31]

Günümüzde güvenlik elektronik ticaret açısından vazgeçilmez bir unsur haline gelmiştir. Özellikle bankalar gibi elektronik ticaret ve işlem anlamında ileri seviyedeki organizasyonlar için bilgi sistemleri güvenliği olmazsa olmaz unsurlar haline gelmiş ve bu güvenlikle ilgili düzenlemeler kamusal anlamda çalışmalar ve kontroller yapılmasına neden olmuştur. Özellikle internet bilgi sistemleri için risk arttıran önemli bir unsur haline gelmiştir. [32]

---

[28] James D. Willson, Steven J. Root, Internal Audit Manual, Warren, Gorham & Lamont, Inc. 1989, p. 25-2

[29] Bruce Hunter, "Information Security: Raising Awareness", ITAUDIT.ORG, September 15, 2000, (Çevirimiçi) http://www.itaudit.org/index_search.htm

[30] Denys Martin, "Risk Assessment When Auditing E-commerce Activities", ITAUDIT.ORG, February 1, 2000, (Çevirimiçi) http://www.itaudit.org/index_search.htm

[31] Chuck Jones, "Internet Security Software", ITAUDIT.ORG, April 1, 2001, (Çevirimiçi) http://www.itaudit.org/index_search.htm

[32] David C. Hall, "The Internet: It's Full of Holes", ITAUDIT.ORG, April 1, 2001, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Bir organizasyonla ilgilenen hemen hemen herkes bilgi sistemleri güvenliği ile yakından ilgilenmek zorundadır. Örneğin bir elektronik ticaret müşterisi kullandığı elektronik ticaret servisinin güvenlik derecesini bilmek zorundadır. Organizasyonun hisselerine sahip ortak ise, ortağı olduğu organizasyonun gerçekleştirdiği elektronik ticaretten kaynaklanan risklerin tam olarak yönetilip yönetilmediğini bilmek zorundadır, çünkü organizasyon bu tür riskleri tam olarak yönetmez ise önemli maddi zararlara uğranacak ve organizasyon zarar edecektir. Organizas çalışanı ise kendilerine ait kişiselliklerin korunduğunu ve bunun başkaları tarafından ihlal edilmeyeceğini bilmek zorundadır. [33]

Son yıllarda bilgisayar suçlarının yaygın bir şekilde yaygınlaşmasının nedenleri aşağıdaki gibidir; [34]

a) Bilgisayarlara daha önce hiç olmadığı kadar çok çalışanın erişmesi,
b) Her geçen gün çok daha fazla kişinin bilgisayar kullanımıyla ilgili eğitim alması,
c) Evlerdeki bilgisayar kullanım potansiyelinin tahmin edilemeyecek kadar çok hızlı bir şekilde artması,
d) Bilgisayar güvenliğini koruma tekniklerinin teknolojilik ilerlemelerle aynı hızla geliştirilmemesi,
e) Uygulama programlarını kullanan personelin güvenlik konuları hakkında bilinçli olmaması ve standart kontrol prosedürlerine yabancı olması,
f) Uygulama programlarını kullanan personele fazla özgürlük tanınması ve çok az kontrol edilmesi,
g) Klasik denetim çalışmalarının yeterli olmaması ve önceden bu suçların belirlenmesini sağlayacak işaretlerin takip edilmemesi

Bilgisayar suçlarının kategorileri aşağıdaki gibi sıralanabilir;

a) Bilgisayarların bir fonun zimmete geçirilmesi için kullanılması veya bir varlığın çalınması amacıyla kullanılması,

---

[33] Barry Horowitz, "Developing a Measurement System for E-business Security", ITAUDIT.ORG, July 1, 2000, (Çevirimiçi) http://www.itaudit.org/index_search.htm

[34] James D. Willson, Steven J. Root, a.g.k. s. 25-3

b) Bilgisayarın sahtekarlık için kullanılması örneğin sahte çek basılması eylemi;
c) Yetkisiz olarak bilgisayar kullanılması,
d) Yetkisiz olarak bir bilgisayara veya network ağına erişilmesi,
e) Bilginin veya yazılımın ortadan kaldırılması veya değiştirilmesi
f) Yazılım, donanım veya bilginin çalınması

Günümüzde bilgisayar suçlarının organizasyonların hızlı büyümesi, yeterli olmayan denetim çalışmaları ve yeterli olmayan kontrol çalışmaları nedeniyle beslendiği ve daha güçlendiği belirlenmiştir. Bilgisayar suçlarının işlenmesinde genel olarak kullanılan tekniklerden bazıları aşağıdaki gibidir;[35]

Veri Aldatımı (Data diddling); Bu en basit, en güvenli ve en yaygın bilgisayarla ilgili suçtur. Verinin bilgisayara girilirken veya daha önce değiştirilmesidir. Verinin bilgisayara girişi, kontrolü, taşınması ile ilgili erişime sahip olan herkes tarafından bu yöntem gerçekleştirilebilmektedir.

Truva Atı (Trojan Horse); Bu yöntem bir bilgisayar programı çalışırken bilgisayarın yetkisiz bir şekilde fonksiyonlar yerine getirmesidir. Bu en yaygın ama tespit edilmesi en zor yöntemdir. Şayet bilgisayarda Truva Atı'ndan şüpheleniliyorsa ilk olarak operasyon programının kontrol kopyası alınarak program çalışırken yapılanların aynı olup olmadığı belirlenmelidir. İkinci olarak ise farklı bir operasyon sistemini kullanarak bireysel uygulama sistemi tekrar çalıştırılır ve uygulamanın çalışması ve çalışmaması durumundaki operasyon sistemi sonuçları karşılaştırılmalıdır.

Mantık Bombası (Logic Bomb); Bir bilgisayar sistemine sokulan uygun ve periyodik zamanda aktif hale gelen talimatlar bütünüdür. Örneğin, talimatlar bir bilgisayara Truva Atı olarak sokulur, talimatlar ilgili günü bilgisayarın tarih ve saatini referans alarak özel bir güne erişilip erişilmediğini belirlemek için test eder. O özel güne erişildiğinde, talimatlar aktif hale gelir ve operasyon sistemi çöker.

Salam Tekniği (Salami Technique); Bu teknik ise büyük bir kaynaktan kimsenin fark etmeyeceği kadar küçük rakamların çalınması veya başka yere transfer edilmesidir.

---

[35] James D. Willson, Steven J. Root, a.g.k., p.25-6

Örneğin bir vadesiz hesaptan mesela 100.000 USD'lik bir hesaptan 0,15 USD gibi bir rakamın başka bir hesaba aktarılmasında hesap sahibi ve banka yetkilileri şüphelenmeye bilir ve önemsemeye bilirler. Ancak bu işlemin binlerce hesaptan yapıldığı düşünüldüğünde önemli zararlara neden olacaktır.

Yukarıda açıklanan bilgiler ışığında bilgisayar suçlarının önemli bir kısmının erişim kontrolündeki zaaflardan kaynaklandığı açıktır. Bu nedenle yıkıcı tehditlere karşı alınacak önlemlerin bilgi sistemlerine erişiminden başlaması alınacak önlemelerin etkinliğini önemli derece arttıracaktır.

Erişim sisteminde yıkıcı tehditlere karşı alınacak ilk tedbir şifrelemedir. Şifreleme gerek organizasyonun içinde gerekse organizasyonun dışında internet aracılığı ile bilgi sistemlerine girişin yetkili kişiler tarafından yapılmasına ilişkin önemli bir kontrol aracıdır. Etkin bir şifreleme çalışmasında dikkat edilecek unsurlar aşağıdaki gibidir; [36]

a) Doğru şifreleme politikası izlenmelidir. Yani şifreler şifre kırıcılar tarafından kolay bir şekilde kırılmayacak tarzda olmalı rakam ve harflerin bir karşımı olmalı ve kesinlikle şifre sahiplerinin kişisel bilgilierini içermemelidir,
b) Şifreler düzenli olarak değiştirilmelidir,
c) Değişen kullanıcılara ait eski şifreler kesinlikle kullanılmamalıdır,
d) Mümkün ise şifrelerin yanında sisteme giriş için kişinin kimlik bilgileri sorulmalıdır.

Şifreler önemli koruyu tedbilerden biridir. Ancak bu şifrelerin korunması ve ifşa edilmemesi gerekmektedir. Şifreler kullanıcılara özenle ulaştırılmalı ve ulaştırma sırasında başka kişilerin öğrenmesinin mümkün olmayacağı yöntem seçilmelidir, [37]

---

[36] Brion Moss, "Security Policy Checklist", 1997, (Çevirimiçi) http://queeg.com/~brion/security.html

[37] Told Feinman, David Goldman, Ricky Wong and Neil Cooper, "Security Basics: A White Paper", ITAUDIT.ORG, September 15, 2000, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Yukarıda görüldüğü gibi yıkıcı tehditlerin önemli bir kısmı bilgi sistemine yetkisiz olarak sokulan programlardan (virüslerden) gelmektedir. Bu nedenle söz konusu virüslere karşı aşağıdaki tedbirler alınmalıdır;

a) Mutlaka bir virüs tarayıcı programlar kullanılmalıdır,
b) Kullanılan virüs tarayıcı programlar düzenli olarak güncellenmelidir,
c) Gelen elektronik postalardaki dökümanların bilgisayarlara aktarılmasında mulaka virüs taraması yapılmalıdır,
d) Personele gönderilenin ve amacının belirtilmediği maillerin açılmaması ve dikkatli olunması konusunda personel ikaz edilmelidir,
e) Network ağına bağlı bilgisayarlara internet ortamından yüklenecek programlara izin verilmemeli veriliyor ise mutlaka kontrol edilmelidir,
f) Network ağına bağlı bilgisayarlara flopy ve cd üzerinden program yüklenmesine izin verilmemeli veriliyor ise mutlaka kontrol edilmelidir,
g) Bir organizasyondaki kişisel internet bağlantıları mutlaka kontrol edilmelidir.

İletişim sistemin gönderilen ve alınan verilerin yetkisiz kişilerin eline geçmesini engelleyen önemli araçlardan birisi de kriptolama yöntemidir. Bu yöntem şayet sisteme izinsiz giriş varsa, erişilen verinin kullanılmayacak durumda olmasını sağlayacaktır. Kriptolama elektronik ticaret için vazgeçilmez bir unsurdur.[38]

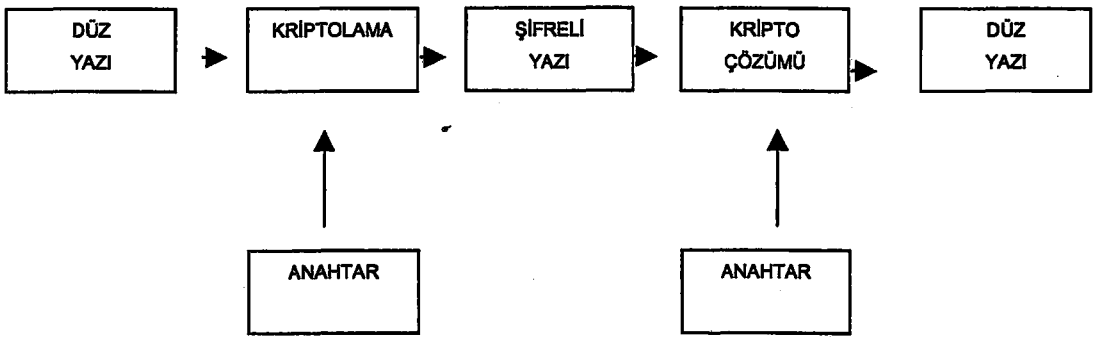
Kriptolama verinin yetkisiz değişimini engelleyen ve verinin güvenliğini koruyan önemli bir tekniktir. Bu teknik sayesinde veri anlaması gereken kişiler dışındaki kişilerin anlamayacak şekile getirilir. Kriptolama yöntemi sayesinde kişiler dijital imzalarına kavuşmuş olurlar. Kriptolama ve dijital imzalar usulsüzlüklerin, veri bütünlüğü ve bilgi kaybını önlemek için mutlaka kullanılmalıdır. Özellikle günümüzde gerçekleştirilen elektronik posta yolula mesaj iletiminin güvenliği açısından kriptolama hassas bir konuma sahiptir.[39]

---

[38] John W. Yu, "Cryptography-A Must for E-Commerce", ITAUDIT.ORG, January 15, 1999, (Çevirimiçi) http://www.itaudit.org/index_search.htm

[39] Chris Hare, "Digital Signatures: Electronic Handwriting", ITAUDIT.ORG, June15, 2001, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Şekil 2.2.
Kriptolama Sistemi



Kaynak: Alan Oliphant, "Confidentiality and the Internal Auditor", ITAUDIT.ORG, December 1, 1998, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Denetim perspektifinden, kripto sistemlerinin en önemli görünüşü, kriptografik anahtarlarının yönetilme tarzıdır. Kriptografik anahtar yönetimi üç fonksiyonu yerine getirmelidir.

a) Anahtarlar nasıl meydana getirilecektir,
b) Bu anahtarlar kullanıcılara nasıl dağıtılacaktır,
c) Anahtarlar kriptografik araçlardan nasıl yüklenecektir.

Erişim alt sisteminde, sisteme izinsiz girişlerin engellenmesi ve bilgi güvenliğinin sağlanması açısından ateş duvarları (firewall) önemli bir fonksiyonu yerine getirmektedir. Firewall'lar erişim alt sisteminde bilgi sistemine giriş ve çıkışları kontrol ederek yetkisiz erişimler için bir siper fonksiyonunu yerine getirir. Bu nedenle erişim alt sistemine ait denetim çalışmalarında Firewall'ların kullanılıp kullanılmadığı belirlenmelidir. Ancak ateş duvarının kullanılmasının yanında bu ateş duvarının organizasyonun güvenlik politikasıyla ve organizasyonun yapısına uygun olarak dizayn edilip edilmediği de belirlenmelidir. [40]

[40] Sandy Lindsedt, "Firewall Audit", ITAUDIT.ORG, June 15, 1999, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Erişim alt sisteminde bilgi sistemlerine girişi kontrol eden önemli bir araç da kişisel kimlik numaraları (PINs)'dır, kişisel kimlik numaraları sayesinde bilgi sistemi kullanıcıyı tanımakta ve sistemin içine almaktadır. Kişisel kimlik numaralarının uygulanmasında aşağıdaki konulara hassasiyet gösterilmelidir.

a) PIN'lerin meydana getirilmesi
b) PIN'lerin ilanı ve kullanıcılara teslimi
c) PIN geçerliliğinin terminal araçlarına yüklenmesi (örneğin ATM makinaları)
d) İletişim hatları üzerinden PIN'lerin geçişi iletilmesi
e) PIN'lerin depolanması ve yok edilmesi

Erişim alt sisteminde bilgi sistemlerine girişi kontrol diğer bir araçta plastik kartlardır. Plastik kartlar sayesinde bilgi sistemine giriş yetki açısından önemli bir sınırlandırmaya tabi tutulmuş olur. Plastik kartlarla ilgili çalışmaların başarılı olması için aşağıdaki konulara hassasiyet gösterilmesi gerekmektedir.

1) Kartın kullanıcı tarafından uygulanması
2) Kartın hazırlanması ve basılması
3) Kartın kullanılması
4) Kartın iadesi ve yok edilmesi

Erişim sisteminde bilgi sistemine bağlı olan bilgisayarların network ağı üzerindeki yerini gösteren network topolojilerin mutlaka belirlenmesi gerekmektedir. Erişimle ilgili olarak yapılacak denetim çalışmalarında departmanlarda yer alan bilgisayarların bu topolojiyle örtüşüp örtüşmediği kontrol edilmelidir. [41]

Denetmenler tüm bu süreçlere ait gereki prosedürleri inceleyerek bunlar üzerindeki kontrol mekanizmalarını belirlemelidir.

[41] Brion Moss, a.g.k.

2.2.1.2.3. İşlem

Bilgi sistemindeki işlem alt sistemi, verilerin hesaplanması sınıflandırılması ve özetlenmesi fonksiyonlarını yerine getirirler. Bu alt sistem,

a) Merkezi İşlemci
b) Gerçek Hafıza
c) Operasyon Sistemi
d) Uygulama Programları'ndan

meydana gelmektedir.

Denetmenler genellikle yukarıda belirtilen elementlere güven duyduklarından işlem denetimlerine çok fazla ağırlık vermemişlerdir. Ancak denetmenler bu bileşenlerle ilgili ortaya çıkabilecek sorunları bilmeli ve buna uygun olarak gerçekleştirilen kontrolleri denetlemelidir.

Merkezi işlemciler bir bilgisayar sisteminde en güvenilen elementler arasında yer almaktadır. Ancak merkezi işlemciler zaman zaman dizayn hatalarından, üretim bozukluklarından, aşırı çalışma ve elektromanyetik araya girme ve radyasyon gibi sebeplerle fonksiyonlarını yerine getiremeyebilirler. Denetmenler bu açılardan merkezi işlemciyi ve ilgili kontrolleri gözden geçirmelidir.

Operasyon sistemi bir bilgisayar sisteminde kaynakların kullanılmasını ve paylaşılmasına izin veren yazılım ve donanımlardan meydana gelmektedir. Operasyon sistemiyle ilgili en önemli konu, operasyon sisteminin ne olursa olsun durmaması, çalışmalarının bozulmaması ve aksamamasıdır. Bu bozulmaya kullanıcılardan kaynaklandığı gibi çevresel faktörlerden kaynaklanabilir. Aynı zamanda operasyon sisteminin kendi alt modülleri arasındaki sorunlar nedeniyle de operasyon sistemi zarar görebilir.

Uygulama yazılımları bilgi sistemindeki spesifik verileri hesaplamakta, sınıflandırımakta, sıralamakta ve özetlemektedir. Uygulama yazılımlarına ilişkin olarak denetmenlerin ilk dikkat edecekleri husus kullanılan yazılımların lisanslı ve yasal kullanım hakkına uygun olarak kullanılıp kullanılmadığının belirlenmesidir. Her yazılımın mutlaka bir lisansı olmalıdır. Ayrıca lisans şartlarına uygun organizasyonda kullanılmalıdır. Yazılım programlarına ilişkin olarak lisans sözleşmelerinde yer alan destek hizmetlerinin yeterince yerine getirilip getirilmediği de belirlenmelidir. [42]

Yazılımların hangi versiyonlarının kullanıldığı ve mevcut versiyonun diğer programlarla etkileşiminin nasıl sonuçlandığı ve mevcut versiyonun yazılım değişen şartlara göre fonksiyonelliğinin korunup korunmadığı da analiz edilmelidir.

Yazılımlarla ilgili diğer önemli bir nokta ise kullanılan yazılımların organizasyonun bilgi sistemleri politikasına uygun olup olmadığı ve bu yazılımlarla işletmenin misyon ve vizyonuna ulaşılıp ulaşılmayacağı ve kullanıcı ihtiyaçlarına cevap verip vermediğidir. Bu konuda gözlemlerin yanında kullanıcılarla görüşerek konuyla ilgili bilgi alınabilir.

2.2.1.2.4. Veri Tabanı ve Veri Kaynakları Yönetimi

Bilgi sistemlerinin alt sistemi olan Veri Tabanı, bir bilgi sistemindeki verilerin tanımlanması, meydana getirilmesi, değiştirilmesi ve silinmesi fonksiyonlarını yerine getirmektedir.

Veri tabanıyla ilgili en önemli denetim konusu erişimle ilgili olarak yapılan kontrol çalışmalarıdır. Bu kontrol çalışmalarında veri tabanına erişimler sınırlandırılmalıdır.

---

[42] John Silltow, "Software Management (9)", ITAUDIT.ORG, October 15, 2000, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Veri tabanında erişime ilişkin sınırlandırmaları

a) Genel Erişim Sınırlandırmaları
b) Yetkiye Bağlı Erişim Sınırlandırmaları

olmak üzere iki başlık altında ele alınabilir.

Genel erişim sınırlandırması bilgi sistemlerindeki bilginin yetkili kılınmamış kişilerin dışındaki hiç kimse tarafından erişilmemesidir. Yetkiye bağlı erişim sınırlandırması ise veri tabanındaki bilgiye, bilginin içeriğine bağlı olarak kişisel sınırlandırmalardır. Daha detaylı bir ifade ile veri tabanını kullanan her kişinin her bilgiye erişmemesidir. Örneğin bankalardaki belirli bir bakiye miktarının üzerindeki müşterilere ait hesap bilgilerinin bazı çalışanlara kapatılması buna bir örnektir.

Veri tabanı yönetiminin temel hedeflerinden birisi de, veri tabanı kullanıcılarına aynı veri kaynaklarından sorunsuz olarak veri dağıtmaktır. Ancak veri tabanı yönetiminde verinin aynı anda farklı kullanıcılara dağıtılması bazen sorunlar meydana getirmektedir.

Bu problemlerden en önemlisi verilerin ortak kullanılması nedeniyle ortaya çıkan ölü kilit durumudur. Bu durum iki farklı departman programlarını aynı veri tabanını kullanırken, bir programın kendi içindeki sürecini tamamlayarak veri tabanına bilgi aktarmadan önce başka bir departmanın programının veri tabanında bilgi alması ve işletmenin yanlış bilgiden dolayı zarar uğramasıdır. Örneğin bir işletmenin satın alma departmanı kullandığı programları mal alımı için veri tabanına baktığında girişi yapar ancak satış departmanı henüz veri tabanında bu veriyi görmediği için mal satışına onay verilmez ve işletme zarara uğrar.

Veri tabanıyla ilgili diğer bir konu da veri tabanındaki bilgilerin düzenli olarak yedeklenmesidir (back up). Bu sürecin aksamadan ve çok düzenli olarak yürütülmesi gerekmektedir. Olumsuz bir durumda işletme verilerini kaybeder ve önemli maddi zararlarla karşı karşıya kalır. Aynı zamanda manyetik band, video band ve teyp kasedi gibi depolama araçlarının düzenli arşivlemesinin yapılması, etiketlenmesi ve kazai silinmelere karşı silinemez konuma getirilmesi gerekmektedir.

Organizasyonlarda yedeklemelerin kimin tarafından gerçekleştirileceği, ne kadar sıklıkla bunun gerçekleştirileceği ve alınan yedeklerin güvenliğinin nasıl sağlandığı gerçekleştirilecek denetim çalışmalarındaki önemli konu başlıklarıdır.

Veri tabanı, farklı amaçlarla farklı kullanıcılar tarafından kullanılan ve paylaşılan verilerin toplandığı bir birimdir. Veri tabanı mutlaka bir ağ üzerindeki iletişimi desteklemelidir. Bir ağ sisteminde ana birim (server)'daki verilere client'lar direkt olarak ulaşmamalıdır. Veri tabanı mutlaka bu konuda fonksiyonel olmalıdır.

Günümüzde tüm organizasyonlar verininin kendileri için önemli bir kaynak olduğunu ve başarılı bir şekilde yönetilmesi gerektiğini kabul eder. Bu nedenle organizasyonların sahip oldukları verilerin merkezi olarak planlanması ve kontrolü büyük bir önem arz etmektedir. Veri yöneticisi verinin yönetimi, planlaması, tanımlanması ve veri mimarisinden sorumlu olan kişilerdir.[43]

Temel olarak verinin daha iyi yönetilmesi için 4 amaç elde edilmelidir.

a) Kullanıcılar veriyi paylaşabilmelidir,
b) İhtiyaç olduğunda kullanıcılar veriye kolayca ulaşabilmelidir,
c) Değişen kullanıcı ihtiyaçlarına göre veriyi kolayca değiştirmek mümkün olmalıdır,
d) Verinin bütünlüğü(doğruluğu) korunmalıdır.

Bu dört amaca ulaşmak için hem teknik hem de yönetimsel çözümler gerekmektedir. Teknik çözümler veri tabanı yönetimi ve veri saklama sistemleri tarafından sağlanmaktadır. Bu sistemler organizasyona paylaşılan veri tabanının bütünlüğünü tanımlamaya, kurmaya, devam ettirmeye, korunmaya izin vermektedir. Yönetimsel çözümler ise veri tabanı yönetim rollerinin ve veri yönetim stratejisinin ortaya konulmasıdır.

[43] John W. Yu, "Auditing Database Systems", ITAUDIT.ORG, September 15, 2000, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Veri tabanı yönetiminin temel işlevi paylaşılan veri çevresinde problem ortaya çıktığında tasarımlar yapmaktır. Ek olarak aşağıdaki fonksiyonları da yerine getirmektedir.

a) Verinin tanımlanması ve meydana getirilmesi,
b) Veri tabanının kullanıcılara hazır hale getirilmesi,
c) Kullanıcıların bilgilendirilmesi ve hizmet edilmesi,
d) Veri tabanının bütünlüğünün sürdürülmesi,
e) Performans ve operasyonların işlenmesi.

Denetmenler veri yöneticilerinin ve veri tabanı yöneticilerinin rollerini iyi bir şekilde anlamalıdırlar. Şayet bu roller tam olarak yerine getirilmez ise veri tabanının kalitesini ciddi derecede olumsuz etkileyecektir. Görevler denetçilere kontrol gücü ve zayıflığı ile ilgili önemli bilgiler sunmaktadır.

Veri yöneticisi ve veri tabanı yöneticisi tasarım görevlerini tam olarak etkin olarak gerçekleştirmek istiyorlarsa, bu kişiler organizasyonel hiyeraşide kullanıcıların kendilerini özgür algılayacakları şekilde yerleştirmeleridirler.

Denetmenler bir organizasyonun veri biritirme sistemi kullanımı ve bunun üzerindeki kontrolü çok iyi şekilde değerlendirmelidir. Şayet bu tam olarak kullanılırsa, veri biriktirme sistemi veri ve uygulama sistemi güvenliğini arttırmaktadır.

2.2.1.2.5. Çıktı

Bilgi sistemlerinin alt sistemi olan çıktı sistemi kullanıcılara sağlanacak verinin içeriğini belirleme fonksiyonunu gerçekleştirmektedir. Bir çıktı alt sisteminin temel bileşenleri kullanıcılara sağlanan verinin zamanını, formatını ve içeriğini belirleyen yazılımlar ve insan kaynaklarıdır. Kullanıcılara veri sunmak amacıyla yazıcı gibi çeşitli donanım araçları kullanılmaktadır.

Günümüzde bir çok çıktı yazılı olarak alınmakla birlikte, zaman zaman sadece ekranda görüntü şekilde olabilmektedir. Veri tabanı teknolojileri, iletişim teknolojileri ve raporlama yazılımlarındaki ilerlemeler sayesinde kullanıcılar herhangi bir aracıya ihtiyaç duymadan çıktılarına rahatlıkla ulaşabilmektedir.

Çıktılarla ilgili ilk konu, gerekli, doğru çıktıların zamanında elde edilip kullanıcılara ulaştırılıp ulaştırılmadığıdır. Şayet kullanıcılar kendileri için gerekli olan çıktıları zamanında ve doğru olarak alamıyorlarsa ve bununla ilgili sorunlarla karşılaşıyorlarsa bilgi sistemindeki çıktı alt sistemi fonksiyonlarını yerine getirmiyor demektir. Örneğin bir bankada bir müşteriye ait hesap ekstrelerinin başka bir müşteriye gönderilmesi önemli bir sorunu gündeme getirmektedir.

Bilgi sisteminde pek tabi ki çıktıların kimler tarafından kullanılacağı önceden belirlenmeli ve bu konuda mutlaka yetki sınırlandırılması yapılmalıdır. Zira işletmenin ancak belirli kişilere açacağı bilgilerin başkalarının eline geçmesi durumunda zarar göreceği muhakkaktır. Ayrıca çıktı alt sistemi öyle kurulmalıdır ki, bu sistemi kullananlar mantiki sorgulamalar ve çıkarımlar yaparak gizli bilgileri tespit edememelidirler.

2.2.1.2.8. Üst Yönetim

Bir organizasyonda bilgi sistemlerinin güvenliğinin sağlanmasında üst yönetime önemli görevler düşmektedir. Herşeyden önce üst yönetim bilgi güvenliği ve kontrolü ile ilgili çalışmaları koordine eden ve organizasyonun amacına ulaşması için yapılması gereken bilgi sistemleri planlamalarını yapan en üst birimdir. Bu nedenle üst yönetimin bilgi sistemleriyle ilgili güvenlik ve yatırımı içeren planlama çalışmalarındaki başarısızlığı organizasyonun başarısını olumsuz olarak etkileyecektir. Üst yönetim planladığı ve organizasyonundaki mevcut bilgi sistemini güvenlik ve kontrol uygulamaları açısından değerlendirebilmek için gerekli çatıyı kurmalıdır. [44]

Son yıllarda bilgi sistemleri güvenliğinin sağlanmasında üst yönetime önemli bir rol verilmektedir. Organizasyonlar sağlam oldukları güvenli bilgiler sayesinde diğer organizasyonlarla sağlam ilişkiler kurar aynı zamanda diğer organizasyonlarında kendileriyle güvenli ve sürekli ilişki kurmalarını sağlayacaktır. Daha fazla güvenlik

[44] IT Governance Institute, "The COBIT Framework Executive Summary", July, 2000, (Çevirimiçi) http://www.isaca.org

daha iyi iş demektir.[45] Üst yönetimden beklenen, bilgi sistemleri risklerinin tam olarak tanımlandığı, anlaşıldığı ve etkin olarak yönetildiği bir kontrol sisteminin kurulmasıdır. Aslında bilgi sistemleri güvenliği bilgi teknolojileri ile ilgili herkesin sorumluluğundadır. Bu sorumluluk bilgi sistemleri risk yönetimi konusunda vereceği direktiflerle üst yönetimden başlamaktadır. Yönetim kontrol sistemi bir organizasyondaki devam eden tehditlerin meydana geldiği alanların sürekli izlenmesini sağlayacak şekilde yapılandırılmalıdır. [46]

Denetmenler üst yönetimi dört temel fonksiyonu gerçekleştirme açısından değerlendirebilir.

Üst yönetimin ilk fonksiyonu planlamadır. Bu fonksiyon organizasyonun amaçlarını gerçekleştirecek ve başarıyla çalışmalarını sürdürecek bilgi sistemleri ve bilgi sistemleriyle ilgili yatırımların planlamasının yapılmasıdır.

İkinci fonksiyonu bu amaçların başarılması için kaynakların bir araya getirilmesi, tahsisatı ve koordinasyonunu içeren organizasyon çalışmalarıdır. Bilgi sistemleri için gerekli donanım, yazılım ve insan kaynaklarının bir araya getirilerek yönetilmesi ve bunları bir hedefe doğru koordinasyonu, organizasonun başarısını sağlarken hedeflere ulaşmasına yardımcı olacaktır.

Üçüncü olarak, üst yönetim liderlik fonksiyonunu yerine getirmelidir. Bu fonksiyon personelin motivasyonunu sağlama ve personele yol gösterimini içermektedir. Bilgi Sistemleri donanımlarını ve yazılımlarını kullanan ve onlara yön veren temel kaynak insandır. Bu önemli kaynağın yönetimindeki başarısızlık tüm bilgi sistemini de olumsuz etkileyecektir.

---

[45] Charles H. Legrand, Willis J Ozier, "Information Security Management Elements : A Call to Action" ITAUDIT.ORG, March 1, 2000, (Çevirimiçi) http://www.itaudit.org/index_search.htm

[46] Charles H. Legrand, Willis J Ozier, "Information Security Management and Assurannce : A Call to Action" ITAUDIT.ORG, January 15, 2000, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Dördüncü fonksiyon ise kontrol etmedir. Bu planlanan bilgi sistemleri performansıyla gerçek performans arasındaki farkın tespit edilmesidir. Üst yönetim uzun dönem stratejik planı ve kısa dönem operasyonel planı olmak üzere iki tür bilgi sistemleri planını hazırlamalıdır. Planlama çalışmasında risklerin değerlendirilerek bu risklere karşı güvenlik planlarının olması ve bunları sonuçlarının değerlendirilmesi de önemli bir kontrol fonksiyonudur.

Bilgi sistemleri planlaması gereksinimleri var olan bilgi sistemlerinin önemine bağlı olarak değişecektir. Bir bilgi sistemleri yönetim komitesi, bilgi sistemleri planlaması ile ilgili en fazla sorumluluğu almalıdır. Bilgi sistemleri yönetimi komitesinin fonksiyonları ve formatı organizasyonun başarısında bilgi sistemlerinin kritik önemine bağlı olarak değişmektedir.

Yönetim denetiminde önemli bir konu da bilgi güvenliği politikası ve bilgi güvenliğine ilişkin yapılacak denetimlerdir. Bilgi güvenliği politikası bilgi güvenliğinin sağlanması için yönetimin direktiflerini ve desteklerini içermektedir. Yönetim anlamında güvenlik politikasının ve güvenliğe ilişkin prosedürlerin mutlaka olması gerekmektedir. [47]

Üst yönetimin mutlaka bilgi sistemleriyle ilgili riskler nedeniyle ortaya çıkan zararların telafi edilmesi, yaraların sarılması ve daha büyük kayıpların engellenmesi amacıyla felaket ve iyileştirme planlarına sahip olması gerekmektedir. Bu tarz bir planın olmaması durumunda organizasyon açılan risk kapılarını kapayamayacak ve daha büyük zararların meydana gelmesine neden olacaktır. [48]

---

[47] Dick Price, "A New Standart in Information Information Security Management" ITAUDIT.ORG, May 15, 1999, (Çevirimiçi) http://www.itaudit.org/index_search.htm

[48] Alan Oliphant, "Managing Information Security" ITAUDIT.ORG, March 1, 1999, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Denetim raporlarının denetimin konusuyla ilgilenen tüm organizasyon yöneticilerine dağıtılması, denetim organizasyonun başındaki yöneticinin veya onun görev verdiği bir denetim ekibinden bir kişinin sorumluluğunda gerçekleştirilmelidir.

Denetim sonuçlarını içeren rapor mutlaka denetim organizasyonun başındaki kişi tarafından okunmalı, onaylanmalı ve imzalanmalıdır. Şayet denetim çalışmaları sırasında, organizasyon içindeki yetkililer tarafından usulsüzlük yapılarak suç işlendiği ortaya çıkartılmış ise denetim raporu ilk olarak mutlaka organizasyonun murakıplarına iletilmelidir.

2.2.2. Etkinlik ve Verimlilik Denetimi

2.2.2.1. Bilgi Sistemleri Etkinliği

Bilgi sistemleri ile ilgili diğer bir denetim başlığı, bilgi sistemlerinin etkinliği ile ilgili gerçekleştirilen denetimlerdir. Bu denetim ve çalışmalarının amacı bilgi sistemlerinin kuruluşunda belirlenen amaçlarına ne derecede ulaştığının yani bilgi sistemi etkinliğinin tespit edilmesidir. Etkinlik, gösterilen çabaların amaca ulaştırıcı nitelikte olması biçiminde olması olarak tanımlanabilir. [49]

Bilgi sistemleri etkinliğini tespit eden denetim çalışmaları sayesinde bilgi sisteminin kuruluşunda belirlenen amaç ve hedeflerine ulaşma başarısı ölçülürken şayet amaç ve hedeflere ulaşılamıyorsa, sistem üzerinde ne tür değişiklerin yapılması gerektiği belirlenmektedir. [50]

2.2.2.1.1. Etkinlik Değerlendirme Sürecinin Genel Görünümü

Bilgi sistemleri etkinliğinin değerlendirme sürecinde aşağıdaki aşamaların gözönünde bulundurulması gerekmektedir.

a) Bilgi sistemi amaçları kesin, net ve açık bir şekilde belirlenmelidir. Bilgi sistemini kullanan farklı gruplar bilgi sisteminden farklı beklentiler içinde

[49] Oktay Alpugan, M Hulusi Demir, Mete Oktav, Nurel Üner, a.g.k. s. 23

[50] Ron Weber, a.g.k., p. 892

olabilirler. Bu nedenle bilgi sistemi kuruluşunda kullanıcılar için belirlenen amaçları kapsamlı bir şekilde ortaya çıkartılmalıdır.

b) Amaçların gerçekleştirilme başarısının değerlendirilmesi için gerekli kriterler ortaya konmalıdır. Bu kriterler bilgi sistemi ve bilgi sistemi kullanıcıları üzerinde yapılacak gözlemler ve görüşmelerle ortaya çıkartılabilir.

c) Belirlenen kriterlerle ilgili verilerin hangi kaynaklardan elde edileceği belirlenmelidir. Yanlış kaynaklardan alınan veriler, kriterler doğru olsa da başarılı etkinlik ölçümüne engel olacaktır.

d) Sistem çalıştırılmadan önceki durumun belirlenmesi gerekmektedir. Bu bilgiler yazılı olarak bulunabileceği gibi kullanıcılarla yapılacak görüşmelerle de ortaya çıkartılabilir. Örneğin önceki sistemde yaşanan sorunlar, işlem hızı, çalışma koşullarını kolaylaştırma becerileri hakkında yazılı bilgiler mevcut değilse önceki sistemin kullanıcıları bu konuda bilgi verebilirler. Şayet organizasyon daha önce bilgi sistemine sahip olmaması durumunda önceki sisteme ait durum belirlemesi yapılamayacaktır. Bu durumda bilgi sisteminin kuruluşu sırasında belirlenen amaçları ve mevcut sistem hakkında elde edilen veriler etkinliğin değerlendirilmesinde belirleyici olacaktır.

e) Belirlenen ölçütler ve veri kaynakları gözönünde tutularak işleyen sistemden bilgi toplanmalıdır. Bilgi toplama noktasında dikkat edilmesi gereken önemli bir konu şayet yeni uygulamaya geçildi ise veri toplanması için ne kadarlık bir süre geçmesi gerektiği konusunda karar verilmelidir. Bu konuda sistem uzmanlarıyla yapılacak görüşmelerle sistemin oturma süresi hakkında detaylı bilgi alınmalıdır.

f) Doğru veri kaynaklarından alınan veriler sistem öncesi verilerle karşılaştırılmalı yani sistem etkinliği hakkında değerlendirme yapılmalıdır.

2.2.2.1.2. Bilgi Sistemi Etkinlik Modeli

Bilgi sistemi etkinliğinin tanımı ve bilgi sistemi etkinliğinin güvenilir ve geçerli kritlerlerinin belirlenmesine ilişkin çalışmalar, bilgi sistemi araştırmacıları tarafından yıllardır yapılmaktadır. Bu çalışmalara bakıldığında aşağıdaki birbiriyle ilişkili faktörlerin bilgi sistemi etkinliğini önemli ölçüde etkilediği görülmektedir.[51]

[51] Ron Weber, a.g.k., p. 894

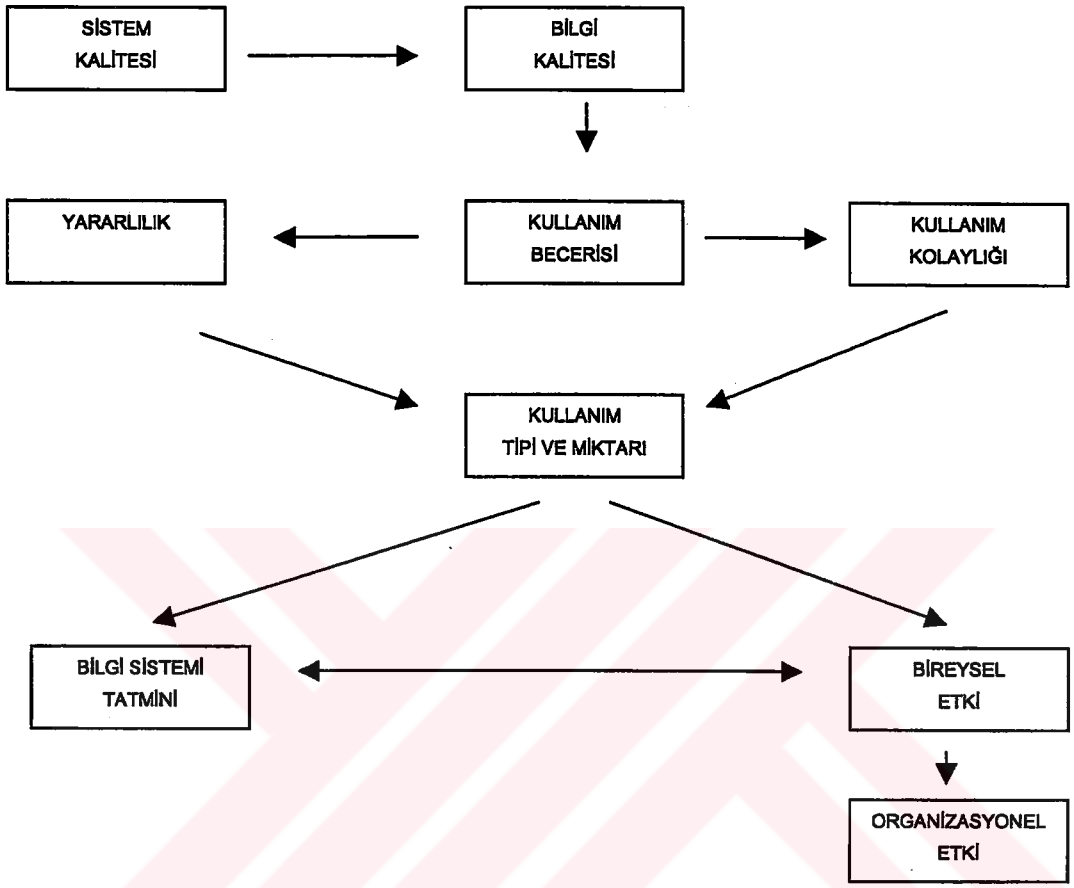
a) Sistem kalitesi
b) Bilgi kalitesi
c) Kullanım becerisi
d) Yararlılık
e) Kullanım kolaylığı
f) Kullanım tipi ve miktarı
g) Bilgi sistemi tatmini
h) Organizasyonel etki

Bilgi sistemi etkinliğini belirleyen faktörlerin başında sistem ve bilgi kalitesi gelmektedir. Sistem ve bilgi kalitesi, sistem kullanıcılarının kullanım becerilerini arttırmakta ve kullanım becerisindeki artış kullanıcıların sistemi daha yararlı ve kullanımı daha kolay olarak algılamalarına neden olmaktadır. Sistem kullanıcılarının sistemi yararlı ve kullanışı kolay olarak algılamaları, onların sistemi ne miktarda ve ne tipte kullandıklarını belirlemektedir.

Bilgi sisteminin nasıl kullanıldığı, kullanıcıların organizasyondaki performanslarını ve dolayısıyla organizasyonun tüm performansını etkilemektedir. Aynı zamanda sistemin kullanım şekli, bilgi sistemindeki tatmini belirlemektedir. Zira geniş kapsamlı kullanıcılar bilgi sisteminden daha fazla tatmin olacaklardır. Yukarıda söz edilen faktörler bilgi sistemi etkinliğinin ölçülmesinde önemli birer kıstas iken aynı zamanda etkin olmayan bilgi sistemlerinin niçin etkin olmadığı konusunda açıklamalar da sunmaktadır.

Şekil 2.3.

Bilgi Sistemi Etkinlik Modeli



Kaynak: Ron Weber, Information Systems Control and Audit, Prentice-Hall, Inc., New Jersey, 1998 p. 894

2.2.2.1.3. Sistem Kalitesinin Değerlendirilmesi

Bir bilgi sisteminin donanım ve yazılıma ait karakteristiği, kullanıcıların sistemin yararlılığı ve kullanım kolaylığı konusundaki düşüncelerini önemli ölçüde etkilemektedir. Aşağıdaki faktörler kullanıcıların sistem hakkındaki düşüncelerini belirlemektedir. [52]

[52] Ron Weber, a.g.k., p. 895

1- Yanıt süresi
2- Dönüşüm süresi
3- Sistemin güvenirliliği
4- Sistemde etkileşimin kolaylığı
5- Sistem tarafından sağlanan fonksiyonelliğin yararlılığı
6- Öğrenme kolaylığı
7- Yardım becerisi ve dökümantasyon kalitesi
8- Diğer sistemlerle etkileşim kapsamı

Yukarıdaki faktörlerden bazıları donanım etkinliği ile ilgilidir. Örneğin, bir sistemin yanıt süresi veya dönüşüm süresi, şayet sistemi destekleyen donanım platformu konfigürasyonu zayıf ve yeterli kaynaklara sahip değilse, kullanıcılar için tatmin edici olmayacaktır.

Bu faktörlerin bazıları ise yazılım etkinliği ile ilgilidir. Yazılım etkinliğinin belirlenmesinde aşağıdaki 4 önemli faktörün değerlendirilmesi gerekmektedir.

1- Tamir sıklığı; Programın tamir sıklığı, program mantığının kalitesini açıklayan önemli bir göstergedir. Tamir çalışmalarının mantiki hataların düzeltilmesi için sürdürüldüğü düşünülürse, yoğun tamir çalışmaları yetersiz dizayn, kodlama ve test teknolojileri anlamına gelmektedir.
2- Adabte edici bakım sıklığı; Adabte edici bakım çalışmaları, değişim gerekliliklerine uygun olarak bir programı değiştirmek amacıyla sürdürülmektedir. Adapte edici bakım çalışmalarının ortaya çıkmasının iki temel nedeni vardır. İlk olarak, program dizayn edicileri, doğru olmayan detaylar formüle etmişlerdir ve sonucunda detaylar ve program mantığı değiştirilmesi gerekmiştir. Aslında doğru olmayan detaylar, detayların geliştirilmesinde kullanılan yaklaşımların gözden geçirilmesi gerektiğini de işaret etmektedir. İkinci olarak kullanıcı gereksinimleri değişebilmekte ve sonucunda, yeni kullanıcı gereksinimlerine uygun olması için programın değiştirilmesi gerekmektedir. Bu tür yapılan değişiklikler programın esnek olmadığını göstermektedir.

3- Mükemmelleştirici bakım sıklığı; Mükemmelleştirici bakım çalışmaları program çalışmasının daha verimli olması için program kaynak tüketiminin iyileştirilmesi için gerçekleştirilmektedir. Bu tür bakım çalışmalarının fazlalığı, programın zayıf bir şekilde dizayn edildiğini göstermektedir.

Program değiştirme ve tamir bakımından sorumlu olan dizayn ediciler ve programcılar ve çalışmaya devam eden programlardan sorumlu olan operatörler, bir bilgi sistemini desteklemek için kullanılan yazılım teknolojisinin yeterliliği konusunda denetim elemanlarına bilgi verebileceklerdir. Dizayn ediciler ve programcılar, programların genel kalitesi üzerine değerlendirme yapabileceklerdir.

2.2.2.1.4. Bilgi Kalitesinin Değerlendirilmesi

Bir bilgi sistemi tarafından üretilen bilginin kalitesi, kullanıcının bilgi sistemi kullanım kolaylığı ve yararlılığı hakkındaki düşünceleri üzerinde önemli bir etkiye sahiptir. Bilgi kalitesinin özelliklerinin bazıları aşağıdaki gibidir; [53]

1- Gerçeklilik,
2- Doğruluk,
3- Bütünlük,
4- Teklik,
5- Zamanlılık,
6- İlgililik,
7- Anlaşırlılık,
8- Kesinlik,
9- Kısalık (Özlük),
10- Bilgilendiricilik,

Bir sistem tarafından üretilen bilginin kalitesi denetim elemanları tarafından değerlendirildiğinde, bilginin kullanıcıların görevlerini yerine getirmede ne derecede katkıda bulunduğunu belirleyebilecektir.

[53] Ron Weber, a.g.k., p. 897

Bilgi, gerçek dünyada meydana gelen olguların sunumunu ve tanıtımını sağlamaktadır. Bilgi kalitesi konusunda farklı kullanıcıların farklı düşünceleri mevcut olması muhtemeldir. Bu farklılık kişilerin dünyayı anlamada kullandığı modelden kaynaklanmaktadır. Bu algılama ve algılama modeli kişilere göre farklılık göstermektedir. Şayet bilgi sistemi kişinin dünya kavramına göre şekilleniyorsa, bir kullanıcı diğer kullanıcıya göre bilgi kalitesini yüksek algılamayabilecektir. Bu nedenle denetmenler, bilgi kalitesinin özelliklerinin objektif olmadığını ve bilgi kalitesi hakkında kullanıcılar tarafından verilen ratinglerin dünyayı nasıl algıladıkları ile yakından ilgili olduğunu unutmamalıdır.

2.2.2.1.5. Yararlılığın Değerlendirilmesi

Yararlılık; Organizasyonel bağlamda kullanıcıların bir bilgi sistemini kullanarak işlemlerdeki performanslarını arttırma olasılığıdır. Yararlılık, kullanıcıların o bilgi sistemini kullanarak fayda elde edip etmedikleriyle yakından ilgilidir. Şayet kullanıcıların bu konuda görüşleri olumlu ise, büyük olasılıkla sistemi daha sık ve etkin bir şekilde kullanacaklardır. Şayet görüşleri olumlu değilse büyük olasılıkla sistemi kullanmayacaklar veya kullanmak istemeyeceklerdir.

Bilgi sistemindeki yararlılığın tespiti ile ilgili bir çok kriter kullanılır. Aşağıdaki bu kriterlere bazı örnekler görülmektedir. [54]

1- Kullanıcılar bilgi sisteminin onları işleriyle ilgili görevlerini daha çabuk yapmasına yardımcı olduğunu düşünmektedir,
2- Kullanıcılar bilgi sisteminin onların iş performanslarını arttırdığını düşünmektedir,
3- Kullanıcılar bilgi sisteminin onların işlerindeki etkinliklerini arttırdığını düşünmektedir,
4- Kullanıcılar bilgi sisteminin onların üretkenliğini arttırdığını düşünmektedir,
5- Kullanıcılar bilgi sisteminin onların işleriyle ilgili görevlerini yapmayı kolaylaştırdığını düşünmektedir,
6- Kullanıcılar bilgi sisteminin onların işlerinde faydalı olduğunu düşünmektedir.

[54] Ron Weber, a.g.k., p. 898

Denetmenler bilgi sistemiyle ilgili bu düşünceleri anket formlarıyla veya görüşmelerle elde edebilirler.

2.2.2.1.6. Kullanım Kolaylığının Değerlendirilmesi

Kullanım kolaylığı, kullanıcıların çalışmalarını sürdürürken serbestlik derecesi olarak tanımlanabilmektedir. Bilgi sistemindeki kullanım kolaylığının tespiti ile ilgili bir çok kriter kullanılır. Aşağıdaki bu kriterlere bazı örnekler görülmektedir. [55]

1- Kullanıcılar bilgi sisteminin operasyonlarının öğrenilmesinin kolay olduğunu düşünmektedir,
2- Kullanıcılar yapmak istedikleri şeyler için bilgi sisteminin kullanılmasının kolay olduğunu düşünmektedir,
3- Kullanıcılar bilgi sistemiyle anlaşılabilir ve açık bir yolla etkileşime girdiklerini düşünmektedir,
4- Kullanıcılar bilgi sistemiyle etkileşiminin esnek olduğunu düşünmektedir,
5- Kullanıcılar bilgi sistemiyle daha becerikli ve daha çabuk olduklarını düşünmektedir,
6- Kullanıcılar bilgi sistemi kullanımının kolay olduğunu düşünmektedir.

Denetmenler bilgi sisteminin kullanım kolaylığı ile ilgili bu düşünceleri anket formları ve görüşmelerle elde edebilirler.

2.2.2.1.7. Kullanım Becerisinin Değerlendirilmesi

Bilgisayar kullanım becerisi bir kişinin bilgisayar kullanım kabiliyeti konusundaki genel fikri olarak ifade edilebilir. Kullanım becerisi geçmişle ilgili değil kişinin gelecekte nasıl kullanacağına ait kişisel algılamadır. Ancak kişinin geçmişteki bilgisayar kullanımı gelecekteki bilgisayar kullanımı konusundaki algılamasını etkilemektedir. Kişisel bilgisayar kullanım becerisi kolay anlaşılır işlerle ilgili değil daha genel ve kompleks işlerle ilgili becerileri ifade etmektedir. Yani kişiler sadece bir işin yapılmasıyla ilgili becerilerinin yanında daha geniş kapsamlı işlerde de beceri sahibi olmaları gerekecektir.

Bir çok araştırmacı kişisel bilgisayar kullanım becerisiin bir bilgi sisteminin etkinliği üzerinde önemli bir etkiye sahip olduğuna inanmaktadır. Zira bu beceri kişinin bilgi sisteminin yararlılığı ve kullanım kolaylığı konusundaki algılamalarını etkilemektedir.

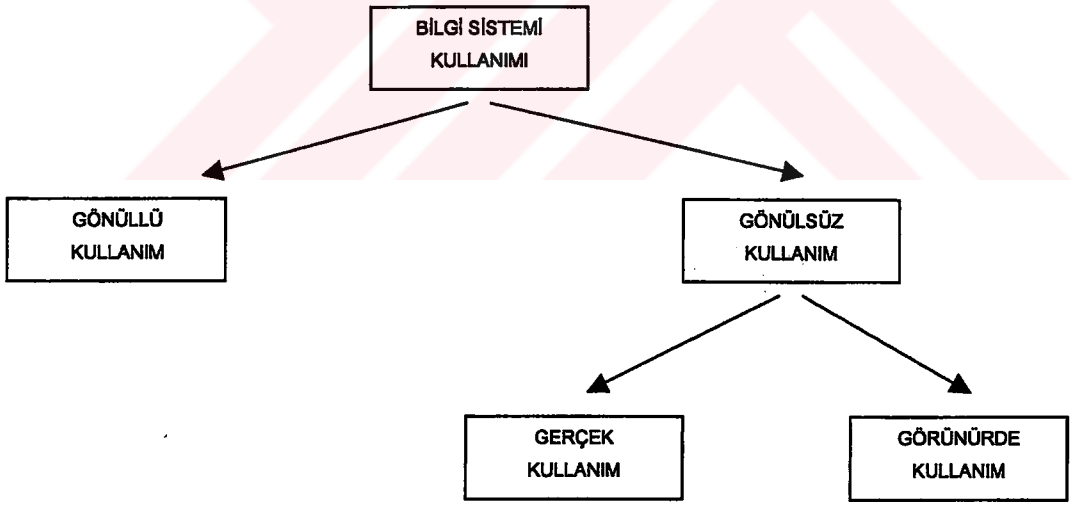
Bilgisayar kullanım becerisininin ölçümünde bazı ölçüm enstrümanlarına ihtiyaç duyulmaktadır. Bu amaçla anketler kullanılabilir.

2.2.2.1.8. Bilgi Sistemi Kullanımının Değerlendirilmesi

Kullanıcılar bilgi sistemini faydalı ve kullanımda kolay olarak algılıyorlarsa, bu kişiler bilgi sistemi hakkın olumlu düşüncelere sahip olacaklardır. Bu olumlu düşünceler sistem kullanışına karşı olumlu yaklaşımlara dönüşecektir

Şekil 2.4.

Bilgi Sistemi Kullanım Türleri



Kaynak: Ron Weber, Information Systems Control and Audit, Prentice-Hall, Inc., New Jersey, 1998 p. 900

[55] Ron Weber, a.g.k., p. 898

Bilgi sistemi kullanımının sıklığı ve şekli kadar, kullanımın gönüllümü, gönülsüz mü olduğu belirlenmelidir. Zira kullanıcılar, bilgi sistemi tarafından sağlanan çıktıların kullanılması için yönetim tarafından zorlanabilmektedir.

Sistem kullanımı gönüllü ise, sistemin ne sıklıkla kullanımınının talep edildiğinin görülmesi için sistem gözlemlenmelidir. Şayet kullanım gönülsüz ise, bu kullanımın gerçek olup olmadığı belirlenmelidir. Kullanımın gerçek olup olmadığı değerlendirilirken çeşitli kanıtlar değerlendirilebilmektedir. Örneğin, sistem çıktılarının gerçekten görevin yapılması için alınıp alınmadığı üzerine kanıt toplanabilecektir. Ayrıca görüşme ve anketler çalışanların gerçek kullanımını ölçmek için kullanılabilecektir.[56]

Bilgi sisteminin ne kadar kullanıldığına dair bilgi edinilmesi amacıyla kullanım sıklığı ve miktarı ölçüt olarak kullanılabilmektedir. Kullanım miktarı değişik veriler ışığında ölçülebilir. Aşağıda bu ölçüme ışık tutabilecek bazı kriterler görülmektedir.

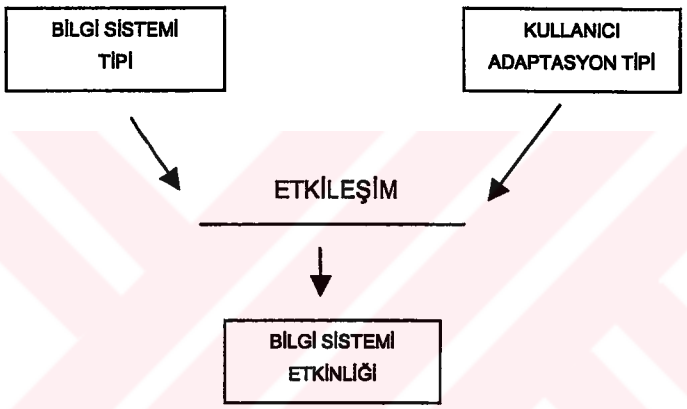
1- Sisteme bağlanma süresi,
2- Bilgi alma sayısı,
3- Sistemde talep edilen fonksiyon sayısı,
4- Database'deki erişilen kayıt sayısı,
5- Oluşturulan rapor sayısı,
6- Sistem kullanımı için boşaltma ölçüsü,

Yukarıdaki kriterler dikkatli kullanılmalıdır zira nicelik açısından fazla olabilmekte ancak nitelik açısından problem taşıyabilmektedir. Örneğin sistem bağlantı süresi yüksek olurken, sistem bağlantı süresince atıl olabilmekte veya kullanıcılar sistemin kullanımında yeterli beceriye sahip olmayabilmektedir. Sonuç olarak ihtiyaç duyulan çıktıların üretilmesi için aşırı kaynak kullanılır.

[56] Ron Weber, a.g.k., p. 900

Bilgi sisteminin kullanım şekli sistem etkinliği konusunda önemli ip uçları vermektedir. Kullanıcılar bilgi sistemini basit işlemler için kullanabilecekleri gibi daha karmaşık daha detaylı çalışmaların yapılması amacıyla da kullanabilirler. Bilgi sisteminin daha karmaşık çalışmalar için kullanılanılması bilgi sistemi etkinliğindeki artışı göstermektedir.

Şekil 2.5.
Bilgi Sistemi Tipi ve Kullanıcı Adaptasyonu



Kaynak: Ron Weber, Information Systems Control and Audit, Prentice-Hall, Inc., New Jersey, 1998 p. 902

Bilgi sistemi etkinliğininin değerlendirilmesinde, bilgi sisteminin kimin tarafından kullandığınının belirlenmesi gerekmektedir. Çünkü kullanımın kaynağı bilgi sistemi etkinliğini belirleme açısından oldukça önemlidir. Bilgi sistemini kullanan kişiler zaman zaman direkt etkileşime girmek yerine bazı aracıları kullanmaktadır. Bu durumun çoğalması halinde kullanıcı sistemle yakından bilgisi olan kişilere sürekli ihtiyaç duyacaktır.

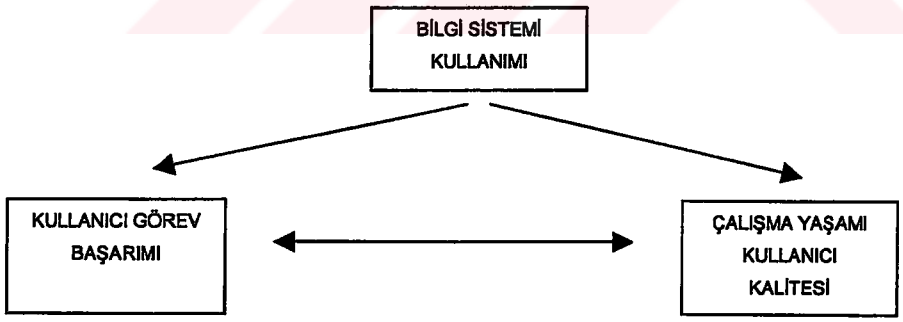
Bu durum kullanıcıların sisteme tam entegre olup olmadıkları konusunda önemli bir bilgi sağlayacaktır. Zira kullanıcılar sistemle sıklıkla etkileşime girmiyorlarsa ve sistemi kullanmak uzmanlık gerektiriyorsa, kullanıcıların sisteme aracı kullanmadan etkileşime girip girmediklerini tespit edilmelidir. Çünkü onların sistemdeki uzmanlık konusundaki eksikliği, sistemin nasıl çalıştığı konusunda bilgi sahibi olmaları için zaman harcamaları anlamına gelmektedir. Ayrıca bu durum sistemi tam olarak kullanmamalarına neden olacaktır. Çünkü sistemin fonksiyonlarının anlaşılması konusunda eksiklikleri vardır. [57]

2.2.2.1.9. Bireysel Etkinin Değerlendirilmesi

Bir bilgi sisteminin kullanıcılar üzerindeki etkisi çeşitli şekillerde değerlendirilebilir. Sistemin etkinliğini değerlendirilirken gözönünde bulundurulması gereken etkilerin iki temel tipi, görev iş başarım etkilesi ve çalışma yaşamı kalitesi etkisidir.

Şekil 2.6.

Bilgi Sistemi Kullanımı, Görev Başarımı ve Çalışma Yaşamı Kalitesi Arasındaki Etkileşim



Kaynak: Ron Weber, Information Systems Control and Audit, Prentice-Hall, Inc., New Jersey, 1998 p. 903

[57] Ron Weber, a.g.k., p. 902

Şayet sistem, kullanıcıların iş başarısını iyileştiriyorsa aynı zamanda onların çalışma yaşamları kalitesini de iyileştiriyor olabilecektir. Örneğin kullanıcılar işleri ile daha çok tatmin olabileceklerdir. Benzer bir şekilde şayet bir sistem kullanıcıların çalışma yaşamı kalitesini iyileştiriyorsa, aynı zamanda onların iş başarısını iyileştirebileceklerdir. Örneğin, şayet bir sistem, kullanıcıların işleri üzerindeki kabiliyetiyle ilgili daha geniş imkanlara sahip olmalarını sağlıyorsa, bu sistem onların görev başarmalarını iyileştirebilecektir. Diğer bir deyişle, bir sistem birinin üzerinde olumsuz bir etki meydana getiriyorsa, diğerini de olumsuz şekilde etkileyecektir. [58]

Etkin bir bilgi sistemi kullanıcıların iş başarılarını etkileyecektir. Aşağıda sistem kullanıcılarının iş başarmalarının iyileştirildiğine dair genel ölçütler yer almaktadır.

1- Karar doğruluğu,
2- Karar verme süresi,
3- Karar güveni,
4- Kararın etkinliği,
5- Meydana getirilen ürün ve hizmetin kalitesi,
6- Meydana getirilen ürün ve hizmetin tüketici tatmini,
7- Görevi tamamlama zamanı.

Bir bilgi sisteminin etkin olup olmadığının belirlenmesi için iş başarısının özel ölçütlerinin tanımlanmasına ihtiyaç duyulmaktadır. Ancak görev başarma için performans kriterleri uygulamalara göre farklılık arz etmektedir.

Bu durumun daha iyi anlaşılması için aşağıdaki iki sistem gözönünde bulundurulabilir. Örneğin üretim kontrol sistemi ve satış sistemi, üretim sistemi için aşağıdaki kriterler kullanılabilecektir.

1- Çıktı ünitelerinin miktarı,
2- Hatalı ürünlerin sayısı,
3- Hurda ürünlerin miktarı,
4- Atık ürünlerin sayısı,
5- Kullanılmayan atıl zaman miktarı.

---

[58] Ron Weber, a.g.k., p. 902

Satış sistemi için aşağıdaki iş başarma kriterleri kullanılabilir;

1- Satışların dolar bazında hacmi,
2- Tüketici tatmin ratingindeki değişiklikler,
3- Şüpheli alacakların miktarı,
4- Malların tüketicilere ulaştırma ortalama süresi,
5- Yeni kazanılan tüketici sayısı,
6- Eski müşterilere yapılan satış miktarı.

İş başarısının değerlendirilmesinde seçilecek kriterlerin ne çok global ne de çok detaylı olmaması gerekmektedir.

Bir bilgi sistemi, çalışanlarının iş başarısını etkilemesinin yanında, çalışanlarının çalışma yaşamı kalitesini etkileyebilir. Bu etkiye önem verilmelidir, çünkü insanların çalışma yaşamları kalitesi ve onların fiziki ve zihinsel sağlıkları arasında önemli bir ilişki mevcuttur. Örneğin araştırmacılar çalışma karakteristikleri ve bazı hastalıklar arasında (örneğin ülser, kalp hastalıkları gibi) ilişki olduğu ortaya konulmuştur.

Aşağıda çalışma yaşamı kalitesine katkıda bulunan faktörler görülmektedir.

1- Yeterli ve adil tazminat; Çalışmadan alınan gelir sosyal standartlarla uyuşmalı ve diğer işlerden alınmış gelirlerle tutarlı ilişkiye sahip olmalıdır,
2- Güvenli ve sağlıklı çalışma şartları; Fiziki çalışma koşulları hastalık ve incinme (yaralanma) risklerini minimum seviyeye indirmeli ve çalışma saatleri konusunda sınırlandırma olmalıdır,
3- İnsan kapasitesini kullanma ve geliştirme konusunda imkan; İşler çalışanlara planlama ve uygulama konusunda yetki vermelidir. Çalışanlar çalışmalarının sonucunda bilgi almalıdır,
4- Sürekli büyüme ve güven imkanı; Yeni becerilerin hazırlanması konusunda imkanlar olmalıdır. İstihdam ve gelir güvenliği var olmalıdır,
5- Çalışma organizasyonunda sosyal entegrasyon; çalışma alanında personel arasında açıklık ve toplum olma hisse desteklenmelidir,
6- Çalışma organizasyonunda oluşum; çalışma alanı kişisel özelliği korunmalı, serbest konuşmayı sağlamalı, eşit muameleyi sağlamalıdır,

7- Dengelenmiş çalışma rolü ve toplam yaşam aralığı; Çalışma toplam yaşam aralığı ile entegre edilmelidir. Örneğin çalışma aile yaşantısı üzerinde gereksiz taleplerde bulunmamalıdır,
8- Çalışma yaşamının sosyal bağı; Çalışanlar çalışma alanını sosyal bir sorumluluk olarak görmelidir.

Şayet bir bilgi sisteminin çalışma yaşamı kalitesi üzerindeki etkisini değerlendirmek için bu faktörler kullanılmak istenirse, iki problemle karşılaşılacaktır. İlk olarak, farklı kullanıcıların çalışma yaşam kalitesi konusunda farklı algılamaları mevcuttur. Örneğin, bazı kullanıcılar çalışma yaşamı kalitesini verimlilik açısından alırken bazıları fiziki koşulları ve ücret açısından algılayacaklardır.

İkinci olarak, çalışma yaşam kalitesinin değerlendirilmesinde geçerli ve güvenilir ölçüm araçlarının bulunması genellikle zordur. Zira farklı ortamlarda bulunan çalışanlar farklı tatmin dereceleri ve beklentilere sahiptirler. Bu nedenle kriterler bir çalışandan diğerine göre farklılık gösterebilecektir. [59]

2.2.2.1.10. Bilgi Sistemi Tatmininin Değerlendirilmesi

Bilgi sistemi tatmini, bir bilgi sistemi başarısını etkileyen faktörlerin belirlenmesinde kullanılmaktadır. Etkin olan bir sistemin kullanıcılarının tatmin olacağı öngörülmektedir. Bilgi sistemi tatmini bilgi sistemi kullanım doğası ve miktarından etkilenecektir. Şayet kullanıcılar sistem hakkında olumlu görüşlere sahiplerse, kullanıcılar iş başarılarının artması için bilgi sistemini kullanma konusunda daha fazla motive olacaklardır. Aynı zamanda, kullanıcıların görevlerini tamamlama ve çalışma yaşamı kalitesi bir bilgi sistemindeki tatminlerini etkilemektedir. [60]

[59] Ron Weber, a.g.k., p. 904

[60] Ron Weber, a.g.k., p. 907

Bilgi sistemi etkinliğinin değerlendirmede, bilgi sistemi tatminini ölçmek için çeşitli enstrümanlar geliştirilmiştir. Aşağıda bu enstrümanlara örnekler görülmektedir.

1- Bilgi sistemi çalışanları ile ilişkiler,
2- Sistem değişim ihtiyaçları süreci,
3- Bilginin zaman hattı,
4- Kullanıcılar için sağlanan bilgi sistemi eğitim seviyesi,
5- Çıktının ilgisi (diğer konularla faaliyeterle),
6- Çıktı miktarı,
7- Sağlanan dökümantasyon kalitesi,
8- Bilgi sisteminin bağımlılığ,

Bir bilgi sistemi kullanıcılarına, bu maddelere göre ne derecede tatmin oldukları sorularak sonuçlar değerlendirilmelidir. Değerlendirme sürecinde kullanılan enstrümanların spesifik sistemelere uyarlanıp uyarlamadığını gözönünde tutulmalıdır. Örneğin muhasebe sistemi için geliştirilen enstrüman karar destekleme sistemleri için kullanılmamalıdır.

2.2.2.1.11. Organizasyonel Etkinin Değerlendirilmesi

Bir bilgi sistemi onu kullanan kişiler üzerinde olumlu etkiye sahipse, bu bilgi sistemi, o kişilerin ait olduğu organizasyonlar üzerinde olumlu etkiye sahip olacaktır. Kişiler ve organizasyonlar üzerindeki etkilerin arasındaki ilişki doğrusal değildir. Kişiler işlerini gerçekleştirmede daha verimli olabileceklerdir.

Aşağıdaki bölümlerde, bilgi sisteminin bir organizasyon üzerindeki potansiyel etkisi iki açıdan ele alınacaktır. İlk olarak, organizasyonun genel etkinliği, ikinci olarak ise ekonomik etkinlik açısından ele alınacaktır.[61]

Yüksek kaliteli bir bilgi sisteminin amaçları ne olmalıdır. İlk olarak bir bilgi sisteminin genel amacı hizmet ettiği organizasyonun etkinliğini arttırmak olmalıdır. Bilgi sistemleri bir organizasyonun amaçlarına yardımcı olmak amacıyla geliştirilirmelidir.

---

[61] Ron Weber, a.g.k., p. 908

Bu nedenle, bir sistemin etkin olup olmadığının değerlendirilmesi organizasyonel amaçlar için değerlendirilmelidir.

Bir organizasyonun amaçları konusunda çok az fikir birliği vardır. Amaçların başarılmasının ölçülmesinde kullanılmak için çeşitli tiplerde göstergeler elde edilmiştir. Bu göstergeler büyüme, dönüşüm, olma, iş tatmini, istikrar, esneklik normlarını içermektedir.

Bilgi sisteminin organizasyon üzerindeki etkisi değerlendirilirken, bilgi sisteminin amaçlarıyla ilgili geniş ilgi ve bilgiye sahip olunmalıdır. Şayet bu yapılmaz ise etkinlik değerlendirmesi başarısız olacaktır.

Etkinliğin özel bir çeşidi de ekonomik etkinliktir. Bu etkinlik değerlendirilmesinde bir bilgi sisteminin bir organizasyonun karlılığına katkıda bulunup bulunmadığı ile ilgillenilmektedir.

Bir bilgi sistemindeki yatırımların etkisi değerlendirilirken üç sorunun cevaplandırılması beklenmelidir.[62]

1- Bilgi teknolojilerindeki yatırım bir organizasyondaki verimliliği arttırdı mı?,
2- Bilgi teknolojilerindeki yatırım bir organizasyondaki karlılığı arttırdı mı?,
3- Bilgi teknolojilerindeki yatırım tüketiciler için değer meydana getirdi mi?,

Bilgi sisteminin ekonomik etkinliğinin değerlendirilmesi için yukarıdaki sorular açıklanmalıdır. Bir bilgi sisteminin ekonomik etkinliğinin değerlendirilirken aşağıdaki 4 adım gerçekleştirilmek zorundadır.

Bilgi Sistemi Faydalarının Tanımlanması; Bir bilgi sisteminin uygulanmasından elde edilen faydalar görünür veya görünmez olabilir. Örneğin sistem üretim maliyetlerini düşürür (görünür fayda) çalışanların moralini yükseltebilir.(görünmeyen fayda) Görünen ve görünmeyen faydaları ortaya çıkartırlırken, kullanıcı tipleri gözönünde bulundurulmalıdır.

[62] Ron Weber, a.g.k., p. 910

Bilgi Sistemi Maliyetlerinin Tanımlanması; İki türlü maliyet bilgi sistemi maliyetini arttırmaktadır. Bunlar uygulama maliyetleri ve operasyonel maliyetlerdir. Uygulama maliyetleri satın alınan yazılım ve donanım maliyetleri, sistem geliştirme için katlanılan işgücü maliyetleri gibi maliyetleri kapsamaktadır. Operasyonel maliyetler ise bilgisayar zamanı ve donanımlarının harcamaları, sistem sürdürme maliyetleri gibi maliyetleri içermektedir.

Fayda gibi maliyetler de görünür veya görünmez olabilir. Örneğin yeni donanım alınması görünür bir maliyettir, sistem ile karşılıklı etkileşimleri nedeniyle kullanıcıların üzerinde biriken artan stresin maliyetleri görünmeyen maliyetlerdir.

Bilgi Sistemi Fayda ve Maliyetlerinin Değerlendirilmesi; Fayda ve maliyetlerin tanımlanmasından sonra değerlendirilmelidir. Bazı durumlarda fayda ve maliyetlerin değerlendirilmesi kolaydır. Örneğin hizmet sağlama ve bir mal satın almanın maliyetlerinin azaltılması veya bir sistemin operasyonel maliyeti dışarıda başka firma aracılığı ile işlemleri gerçekleştiren faturalarda açıkça ortaya çıkabilir. Bazı durumlarda, fayda ve maliyetlerin değerlendirilmesi güç olabilir.

Bilgi sistemi kullanıcılarına sistem fayda ve maliyetlerinin değerlendirilmesinde yardımcı olması konusunda güvenilmelidir. Şayet kullanıcılar direkt olarak fayda ve maliyetleri tahmin edemiyorlarsa, değerleme konusunda onlara yardımcı olacak teknikler kullanılabilir. İlk olarak fayda ve maliyetler küçük parçalara bölünmelidir. Böylece küçük parçalar daha kolay değerlendirilebilir.

İkinci olarak, piyasa durumu gözönünde bulundurularak çalışılmalı ve kullanıcılara dışarıdan bu fayda ve maliyetler elde etmek için ne kadar ödemeye istekli olduğunu sormalıdır.

Üçüncü olarak, fayda ve maliyetlerin listesi sunulara bunları değerlerine göre sıralanması istemelidir.

Dördüncü olarak, kullanıcılardan bu sıralama sonrası fayda ve maliyetlerini tahmin etmeleri istemelidir. İlk önce görünür fayda ve maliyetler değerlendirilmeli ardından görünmeyenler değerlendirilmelidir.

2.2.2.2. Bilgi Sistemleri Verimliliği

Bilgi sistemlerinin verimliliği, bilgi sistemleri denetimine ilişkin önenmli bir başlıktır. Zira verimli çalışmayan bir bilgi sistemi organizasyon içindeki fonksiyonunu tam olarak yerine getirmemiş olacak ve bilgi sistemleri açısından bir risk meydana getirecektir. Verimlilik, çıktı ile çıktının üretiminde kullanılan girdiler arasında ilişki kuran bir kavramdır. En basit tanımı ile verimlilik, elde edilen faydanın, kullanılan kaynaklara oranıdır.[63]

Bilgi sistemleri verimliliğine ilişkin yapılacak denetim sayesinde elde edilecek sonuçlarla mevcut operasyonel sistemin performansının daha da yükseltilip yükseltilemeyeceği belirlenirken aynı zamanda mevcut sisteme alternatif sistemlerin satın alınması, kiralanması ve geliştirilmesi anlamında da yönetime destek sağlayacaktır.

Temel olarak bilgi sistemleri verimlilik denetimi aşağıdaki başlıklardan oluşmaktadır;

a) Değerlendirme amaçlarının belirlenmesi,
b) Performans krititerlerinin belirlenmesi,
c) İş yükleme modelinin kurulması,
d) Deney yapılması,
e) Sonuçların analiz edilmesi,
f) Önerilerde bulunulması.

2.2.2.2.1. Değerlendirme Amaçlarının Belirlenmesi

Denetmenler bilgi sistemi verimliliği denetimine başlamadan önce bu çalışmanın amaçlarını açık olarak belirlemelidirler. Bu amaçlar değerlendirme çalışmalarının sınırlarını da çizecektir. Aynı zamanda verimlilik değerlendirmesi için gerekli olan performans göstergelerinin ve gerekli olan performans modelinin belirlenmesinde yardımcı olacaktır.

---

[63] Oktay Alpugan, M Hulusi Demir, Mete Oktav, Nurel Üner, a.g.k. s.13

Bu denetim çalışmasında amaç online kayıt etme sisteminin performansını iyileştirmek gibi global olabileceği gibi bir işlemcinin faydasını arttırmak gibi spesifik de olabilir.

2.2.2.2.2. Performans Kriterlerinin Belirlenmesi

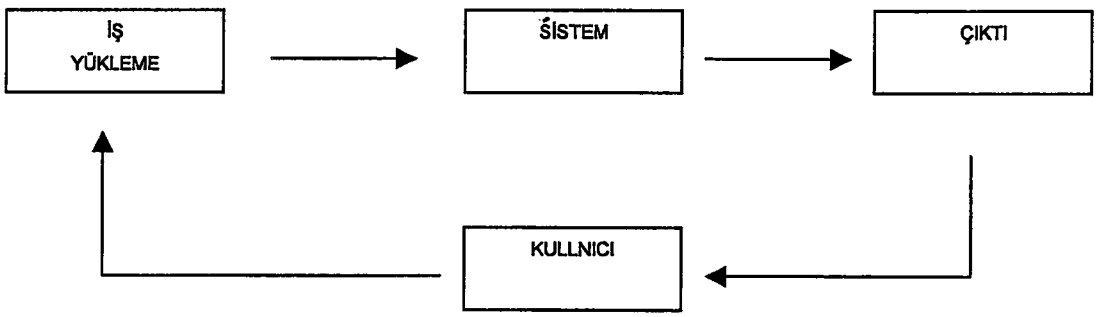
Performans göstergeleri bir sistemdeki verimliliğin seviyesi için bir temel sağlamaktadır. Değerlendirme çalışması için hangi performans göstergelerinin seçileceği, çalışmanın amaçlarına bağlı olarak değişecektir. Örneğin amaç bir interaktif sistemin çıktı süresini iyileştirmek ise, performans kriteri açık olarak karşılık verme zamanı olacaktır.

2.2.2.2.3. İş Yükleme ve Sistem Modelinin Kurulması

Bir sistemin performansı, sistemin yerine getirmek zorunda olduğu iş yüklemenin bir fonksiyonudur. Sistem verimliliği ölçülürken, denetmenler gerçek iş yükleme sistemini gösteren bir iş yükleme modeli kurmalıdır. Şayet değerlendirilecek sistem henüz dizayn aşamasında ise, yapay sistem iş yükleme modeli kurulmalıdır. Aşağıda bir bilgisayar sisteminin yapısal modeli görülmektedir.

Şekil 2.7.

Bir Bilgisayar Sisteminin Yapısal Modeli



Kaynak: Ron Weber, Information Systems Control and Audit, Prentice-Hall, Inc., New Jersey, 1998 p.931

Ayrıca sistem modeli kurulur. Bu sistem modeli konfigurasyonla ilgilidir.

2.2.2.2.4. Deneyin Yapılması

İş yükleme ve sistem modeli kurulduktan sonra, denetmenler performans göstergelerinin değerlerini belirlemek için deney yapabilirler. Söz konusu deneylere ilişkin analiz iş yükleme ve sistem modeliyle ilgili olarak daha yoğun bir şekilde gerçekleştirilebilir.

2.2.2.2.5. Sonuçların Analiz Edilmesi

Verimlilik analiz edilirken, denetmenler performans göstergeleri değerleri ile iş yükleme ve sistem karakteristikleri arasındaki kesin ilişkileri ileri sürmelidir. Denetmenler ileri sürdükleri bu ilişkileri parametreleri değiştirdiklerinde nasıl kurdukları hipotezlere uygun olarak değiştiğini ortaya koymalıdırlar.

2.2.2.2.6. Önerilerde Bulunulması

Denetmenler deneyler ve analiz çalışmalarından sonra sistemin daha verimli hale gelmesi için önerilerde bulunmalıdırlar. Bu önerilerini yukarıda bahsedilen hipotezlere bağlı olarak yapmalıdırlar. Ayrıca söz konusu değişiklikle elde edilecek faydanın katlanılacak maliyetten daha yüksek bir getiri sağlayacağı da anlatılmalıdır.

2.3. Denetim Kanıtlarının Toplanması ve Örnekleme

Bilgi sistemleri denetim çalışması planlandığında, bilgi sistemleri denetmeni toplanması gereken denetim kanıtları tiplerini hesaba katmalıdır. Denetim kanıtları denetim amaçlarına ulaşmak için kullanılır ve herbirinin farklı güven seviyesi mevcuttur.

Bu kanıtların nitelikleri ve bağımsızlığı dikkate alınmalıdır. Denetlenen organizasyonda elde edilen veriler organizasyonun dışından elde edilen üçüncü kişilerden sağlanan verilere göre daha az güvenilirdir. Fiziki denetim kanıtları tasvirlere göre daha güvenilirdir.[64]

Denetim kanıtlarının çeşitleri aşağıdaki gibidir;

a) Fiziki maddelerin varlığı ve gözlenen süreçler,
b) Dökümantal denetim kanıtları,
c) Tasvirler,
d) Analizler,

Fiziki maddelerin varlığı ve gözlenen süreçler, aktivitelerin, varlıkların ve bilgi sistemleri fonksiyonlarının gözlemlerini de içerebilir. Örneğin operasyondaki bir bilgisayar odası güvenlik sistemi.

Dökümantal denetim kanıtı, medya araçları ve kayıtlara kaydedilen dökümental denetim kanıtı aşağıdakileri içerebilir,

a) Sistem geliştirme dökümanları,
b) Aktivite ve kontrol kütükleri,
c) Faturalar,
d) Program listeleri,
e) İşlemlerin kayıtları

Tasvirler aşağıdaki gibi olabilir,

a) Yazılı politikalar ve prosedürler,
b) Sistem iş akış şemaları,
c) Yazılı ve sözlü beyanlar,

---

[64] Information Systems Audit and Control Foundation, "Auditing Guideline:Audit Evidence Requirement", (Çevirimiçi) http://www.isaca.org/standard/guide6.htm

Analizlerle ilgili olarak yapılan karşılaştırmalar, simülasyonlar, hesaplamalar ve çıkarımla denetim kanıtı olarak kullanılabilir. Bunlara örnek olarak,

a) Diğer organizasyonlara ve geçmiş periyodlara göre bilgi sistemleri performansının karşılaştırılması,
b) Kullanıcılar, işlemler ve uygulamalar arasındaki hata oranları karşılaştırmaları

Denetmen bu denetim kanıtlarından hangilerini seçmesi gerektiğini yapılan denetimin amacına ulaşmada en fazla katkıyı sağlayacak, en güvenilir olası uygun zaman içinde olmak koşuluyla kendisi uygun kombinasyonu kurmalıdır.

Denetim kanıtı, denetmenin bulgularını ve çıkarımlarını destekleyecek şekilde yeterli, güvenilir, ilgili ve kullanılabilir olmalıdır. Şayet, denetmenin değerlendirmesinde, elde edilen denetim kanıtı bu kriterlere uymuyorsa, denetmen ilave denetim kanıtları elde etmelidir. Örneğin, bir program listesi, mevcut program listesinin üretim sürecinde kullanıldığına dair başka bir kanıt bulunmadıkça kanıt olmayacaktır.[65]

Denetim kanıtı toplamak için kullanılan prosedürler denetlenen bilgi sistemine bağlı olarak değişmektedir. Denetmenler, denetim amacına en uygun olan prosedürü seçmelidir. Aşağıdaki prosedürler veri toplamada kullanılabilir,

a) İstihbarat,
b) Gözlem,
c) Teftiş,
d) Teyitleme-Doğrulama
e) Tekrar hesaplama,
f) İzleme

[65] Information Systems Audit and Control Foundation, "Audit Evidence Requirement", (Çevirimiçi) http://www.isaca.org/standard/guide6.htm

Bu prosedürler hem elle yapılan prosedürlerde hem de bilgisayar yardımlı denetim tekniklerinde kullanılabilir.

Denetmenler genellikle pratik olmadığından ve fayda maliyet analizi açısından dolayı mevcut tüm bilgileri kontrol etmezler. Bunun yerine örnekleme yönteminin kullanılmasıyla sonuca ulaşmaya çalışırlar.

Denetim örneklemesi bir grubun belirli bir karakteristiği ile ilgili denetim kanıtı elde etmek için gruptaki elemanların %100'ünden daha az kalemi üzerinde denetim prosedürlerinin uygulanmasıdır.[66]

İki türlü örnekleme yöntemi kullanılmaktadır,

a) İstatistiki örnekleme,
b) İstatistiki olmayan örnekleme

İstatistiki örnekleme; Grupla ilgili olarak bir çıkarıma ulaşmak için bir gruptan bir örneği seçmek ve değerlendirmek için olasılık kanunlarını kullanan denetim örneklemesidir. Bu örneklemede istatistiki örnek rastlantısal olarak seçilir ve sonuçların ölçülmesi için istatistiki hesaplamalar kullanılır. İstatistiki örnekleme yöntemi denetim problemlerine kesin bir yaklaşım sağlarken, denetim altındaki grup ve örnek sonuçları arasında direkt bir ilişkiyi hesap etmektedir.

İstatistiki olmayan örnekleme; denetmenlerin sonuçları belirtmek için istatistiki hesaplamaları kullanmayan denetim örneklemesi yöntemidir. Bu örnekleme yöntemi istatistiki metoda uymayan özel problemlere daha esnek bir yaklaşım sağlamaktadır.

[66] Jack C. Robertson, Auditing, Irwin, 1996, Texas, Eight Edition, p. 242

2.4. Denetim Dökümanlarının Hazırlanması

Bilgi sistemleri denetim dökümantasyonu gerçekleştirilen denetim çalışmasının kayıdı ve bilgi sistemleri denetiminin bulgularını ve çıkarımlarını destekleyen denetim kanıtlarıdır.[67]

Dökümantasyon minimum seviyede aşağıdaki belgeleri ve çalışmaları içermelidir,

a) Denetim alanı ve amaçlarının hazırlanması ve planlanması,
b) Denetim programı,
c) Gerçekleştirilen adımlar ve toplanan denetim kanıtları,
d) Denetim bulguları, çıkarımlar ve tavsiyeler,
e) Denetim çalışmasının bir sonucu olarak yayınlanan herhangi bir rapor,
f) Denetimi idare edenin görüşü ve değerlendirmesi

Dökümantasyon profesyonel standartlar, kamu düzenlemeleri ve kanun tarafından gerekli olan denetim bilgilerini içermelidir. Dökümantasyon açık, tam ve anlaşılabilir olmalıdır. Denetim bulgularını ve çıkarımlarını destekleyen dökümantasyonun yeterli süre saklanması ve korunmasını sağlayan politikalar ve prosedürler etkin olmalıdır. Dökümantasyonlar güvenli şekilde saklanıp korunabileceği ve istendiğinde çıkartılablecek ortamlarda saklanmalıdır. Bu konudaki yasal zorunluluklar unutulmamalıdır. Denetim dökümantasyonları arasında denetim raporunun özel bir önemi vardır. Denetim çalışmalarının sonucunda, denetmenlerin bilgi sistemleriyle ilgili bulgu ve yorumlarının yer aldığı denetim raporu yayınlanmalıdır. Söz konusu raporda yer alan yorumlar ve kanaatler yeterli ve gerçek kanıtlarla mutlaka desteklenmelidir. Şayet bazı denetim alt başlıklarıyla ilgili yeterli denetim kanıtlarının toplanamadığına inanılıyorsa, bu durumun denetim raporunda mutlaka açıklanması gerekmektedir.[68]

---

[67] Information Systems Audit and Control Foundation, "IS Auditing Guideline: Audit Documentation", (Çevirimiçi) http://www.isaca.org/standard/guide12.htm

[68] S. Rao Vallabhaneni, Internal Audit Skills, SRV Professional Publications, 1998, Illinoi, pp. 191-201

3. BİLGİ SİSTEMLERİ GÜVENLİK ENDEKSİ VE BANKACILIK SEKTÖRÜ UYGULAMASI

3.1. Bilgi Sistemlerinin Bankacılık Sektöründeki Önemi

Gerçekleştirdikleri finansal aracılık hizmetleriyle atıl fonların harekete geçirilmesini sağlayan bankacılık sektörü, gösterdiği performansla ülke ekonomisine önemli katkılar sağlamakta ve ülkemizde gerekse diğer ülkelerde ekonomik istikrarın sağlanmasında bankacılık sektörü kilit bir rol üstlenmektedir. Zira son yıllarda yaşanan ekonomik krizlerde istikrar politikalarının hayata geçirilmesinde bankacılık sektöründeki yapılanmanın gözden geçirilerek düzenlenmesinden gerek ülkemizde gerekse diğer ülkelerde özel bir önem verilmiştir.[69]

Günümüzde gelişmiş iletişim teknolojileri, bankacılık sektöründeki gelişmiş ürün yelpazesinin sadece bölgesel ve ülkesel değil aynı zamanda tüm dünyaya sunulmasını da sağlamaktadır. Finansal piyasalardaki yaşanan entegrasyon, bankacılık sektöründeki bir krizin tüm dünyadaki global bir krize dönüşmesine neden olmaktadır. Bu nedenle günümüzde bankacılık sektöründe risk yönetimi daha önce hiç olmadığı kadar bankalar için büyük bir önem arz etmektedir.

Bankacılık sektöründe başarılı ürün ve hizmet sunumu başarılı bir banka yönetiminin elde edilmesiyle gerçekleştirilmektedir. Genel olarak bakıldığında bilgi sistemleri bankacılık sektöründeki başarılı yönetim açısından vazgeçilemez bir araç haline dönüşmüştür. Bilgi sistemleri bankalardaki yönetime

a) Operasyonların Gerçekleştirilmesi,
b) Risk Yönetimi

alanlarında önemli katkılar sağlamaktadır.

---

[69] Erişah Arıcan, Gelişmekte Olan Ülkelerde İstikrar Politikaları ve Türkiye, Der'in Yayınları, İstanbul, 2002, s. 139

3.1.1. Operasyonların Gerçekleştirilmesi

Bankalar fon toplayan ve topladıkları fonları yatırıma dönüştüren kuruluşlardır. Bu kurumların aktiviteleri sadece mudilerden fon toplama, hesap açımı, kredi kullandırma ve faiz hesaplamadan ibaret değildir. Özellikle iletişim ve internet teknolojilerindeki ilerlemeler bireysel bankacılık hizmetlerinde de önemli gelişmelerin elde edilmesine neden olmuştur. [70]

Bu çalışmaların tüm aşamalarında bilgi sistemleri kullanılmaktadır. Bilgi sistemleri sayesinde bankacılık sektöründeki operasyonlarda hız ve doğruluk sağlanırken aynı zamanda hizmetlerin kalitesi de artmaktadır. Verilen hizmetlerin iletişim teknolojileri sayesinde telefon, elektronik ortam ve internet aracılığı ile yapılması nedeniyle aynı zamanda güven kavramını da gündeme getirmektedir.

3.1.2. Risk Yönetimi

Finans sisteminin günümüzde globalleşmesi, hukuki serbestleşme ve uluslararası rekabet kaynaklı olarak piyasalardaki dalgalanmanın artması nedeniyle hangi ülkeden kaynaklandığına bağlı olmadan ekonomik krizler diğer ülkeleri de etkisi altına almaktadır. Aynı zamanda ülke içinde başlayan finansal piyasalardaki bir sorun diğerlerine yansırken ülke içinde ekonomik bir krize dönüşmektedir.

Risk bankalar ve finansal kuruluşlar için hep ilgi odağı olmuştur. Bankalar risk alan, risk değiştiren ve bu riski ürün ve hizmete dönüştüren kuruluşlardır. Bankalar tam anlamıyla risk makineleridir. Riski en temel anlamıyla beklenen bir sonuç ile gerçekleşen sonuç arasındaki sapma olarak tanımlayabiliriz.

Başarılı bir banka yönetimi için risk yönetimi ihmal edilmemesi gereken bir aktivitedir. Günümüze kadar finans konusundaki yasal düzenlemelerdeki eksiklikler nedeniyle, bankalardaki risk yönetimi sıradan bir faaliyet olarak düşünülerek, bağımsız departman veya bölüm tarafından yönetilen faiz oranı, likidite ve kredi riski

---

[70] İlhan Uludağ, Erişah Arıcan, Finansal Hizmetler Ekonomisi, Beta Yayınevi, İstanbul, 1999, s. 122

şeklinde uygulanmaktaydı. Oysa bankalar hem ürün geliştirme bakımından hem de müşteriyle olan ilişkilerinden dolayı çok fazla risk altında bulunmaktadır.

Bankalardaki başarılı bir risk yönetimi için de, bankalarda yer alan bilgi sisteminin yeterli seviyede olması gerekmektedir. Nitekim 4389 sayılı Bankalar Kanunu gereğince 01.09.2000 tarihinde göreve başlayan Bankacılık Düzenleme ve Denetleme Kurulu (BDDK)'nun Bankalarîn İç Denetim ve Risk Yönetim Sistemleri Hakkındaki Yönetmeliği'nin 14. ve 15. maddelerinde açık olarak belirtildiği gibi güvenilir bilgi erişim sistemlerinin tesisi ve bilgi işlem teknolojisinin kontrolü konularının yeterliliği üzerinde durarak risklerin günlük bazda takibini etkin bir biçimde yapabilmesi için yeterli bir bilgi işlem desteği zorunlu tutulmuştur. [71]

Denetmenler gelecek bin yılda risk yönetim uzmanları olacaklardır. Gerçekte mevut olan risklerin tanımlanması organizasyonlar için kullanışlı ve yararlı olurken, potansiyel risklerin tanımlanması ve bunlardan kaçınılma yolların belirlenmesi ise organizasyonlar son derece önemli çalışmalardan biri olacaktır. Bu açıdan da denetmenlerin organizasyonlardaki önemi her geçen gün artmaya devam edecektir. [72]

Bilgi sistemleri'nin bankaların yönetimindeki önemli katkılarının yanında, bilgi sistemlerinin bizzat kendisinin önemli bir risk kaynağı olması nedeniyle bankalar için önem arz etmektedir. Zira bilgi sistemlerinde meydana gelebilecek hatalar ve güven zaafları bankaların ciddi derecede maddi kayıplara uğramasına neden olacaktır.

---

[71] Emre Alkin, A. Tuğrul Savaş, Vedat Akman, Bankalarda Risk Yönetimine Giriş, İstanbul, 2001, s. 142

[72] Will Ozier, "Information Risk Analysis, Assessment and Management", ITAUDIT.ORG, February 1, 2000, (Çevirimiçi) http://www.itaudit.org/index_search.htm

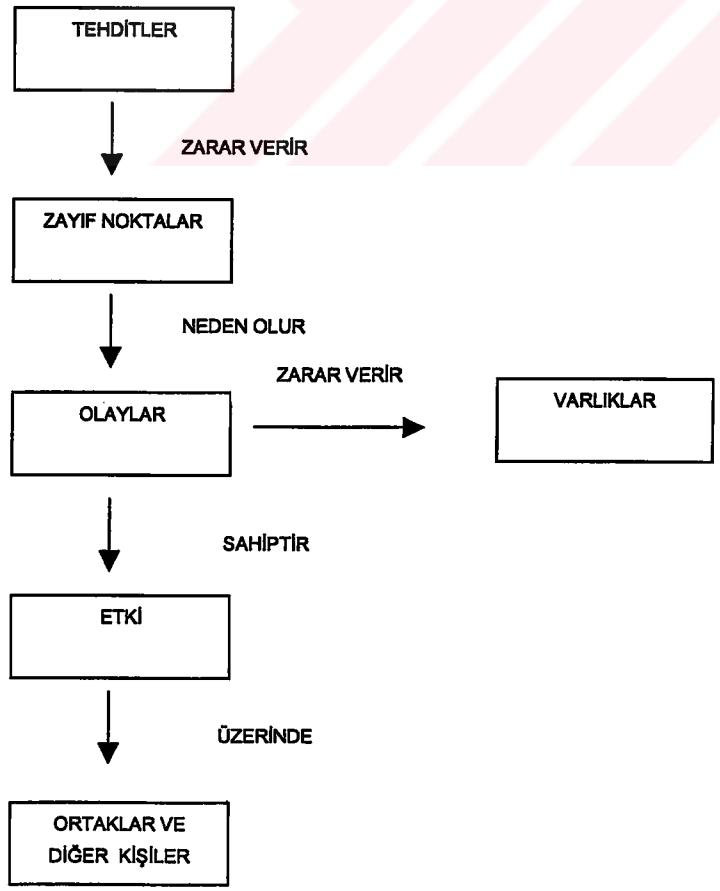
3.2. Bankacılık Sektörü Bilgi Sistemleri Güvenliği Endeksi Modeli

Tüm ülkelerde olduğu gibi ülkemizde de Bankacılık Sektöründe faaliyet gösteren bankalar, ölçeği ne olursa olsun hemen hemen tüm işlemlerde bilgisayar tabanlı bilgi sistemlerini kullanmaktadır. Bu durum bilgi sistemleri kaynaklı riskleri de beraberinde getirmiştir.

Bu risklerin banka bazlı olarak ölçülmesi ve genel bankacılık sektöründeki risk durumunun analiz edilmesi, bankacılık sektörünün uğraması muhtemel tehditlerin bilinmesi ve bu tehditler için önlem alınması açısından bankacılık sektörünün performansı üzerinde gerçekten önemli bir etkiye sahiptir. Aşağıdaki şekilde mevcut tehditlerin bankacılık sektöründe nasıl bir sonuç meydana getirebileceği görülmektedir.

Şekil 3.1.

Güvenlikle İlişkili Tehditlerin Bankalar Üzerindeki Etkisi



Yukarıdaki şekilde de görülebileceği gibi mevcut tehditler, bankaların zayıf yönlerini suistimal ederek ve onları zorlayarak güvenlik sorunları meydana getiren olaylar meydana getirmektedir. Söz konusu bu olaylar, organizasyonların varlıklarına zarar vermekte ve bu durum bankaların ortaklarını ve bankayla ilgilenen devlet ve müşterileri de olumsuz etkilemektedir. Bu olumsuz etkilenme sadece bankacılık sektörüyle sınırlı kalmamakta ve tüm ülke ekonomisiyle ilgili önemli sorunlarında meydana gelmesine neden olmaktadır.

Genel olarak bakıldığında, bir bilgi sistemlerinin karşı karşıya olduğu tehditler, aşağıdaki gibi sınıflandırılabilir.

a) Güvenirliliğin ve Kişiselliğin Kaybedilmesi; Bilgi sistemlerindeki verilere yeterli olmayan erişim kontrolleri, programlama hataları ve taklitlerin kullanılması nedeniyle verilere ilişkin güvenirlilik ve kişisellik kaybedilebilmektedir. Aynı zamanda yetkili kullanıcılar erişim hakkı olmayan üçüncü kişilere bilgileri açabilmektedir. Bu tip bir tehdit organizasyona ait verilerin intranet aracılığı ile kullanıcılara dağıtılması durumunda daha çok gündeme gelmektedir. Gönderilen veriler yetkisiz erişimlerle elde edilebilmektedir. Kullanıcılardaki verilerin güvenli olmayan operasyon programlarında olması, ve internet'den elde edilen programlarda kullanılması durumunda suistimale oldukça açık bir ortam sağlanmaktadır.
b) Bilgi Bütünlüğünün Kaybedilmesi; Uygulama ve operasyon seviyesinde bilgi sistemlerindeki zayıflıklar, veri bütünlüğünün bozulmasına neden olabilmektedir. Yetkisiz iletişim ağına sızmalarda, iletişimdeki verilerin bütünlüğünün bozulmasına neden olmaktadır. Ayrıca kullanıcılardaki verilerin internetten elde edilen yazılımlar kullanılması durumunda bütünlüğünün bozulma olasılığı artmaktadır.

c) Orjinalliğin Kaybedilmesi; Tehdit ajanları sahte birimler veya bir ana birim üzerinde sahte dökümanlar meydana getirebilirler. Taşınmakta olan veriler için tehdit ajanları bilginin kaynağını sahte hale dönüştürebilirler. Bir ana birime bilgi gönderen kullanıcılar kendi haraketlerini doğru olarak gösteremeyebilir ve dökümanı oluşturan kişiler dökümanların gerçek yazarları olmaması gereken kişilere ulaşabilirler. Bu durum genellikle web tabanlı online işlemlerin kullanılmasıyla ortaya çıkmaktadır.
d) Fiziki Varlıkların Kaybedilmesi; Çevresel faktörler nedeniyle ortaya çıkan doğal afetler, hırsızlık ve kazai zarar vermeler nedeniyle fiziki varlıkların kaybedilmesi söz konusu olabilmektedir.

Organizasyonlar korunması gereken sistemlerini açıkça anlamadan ve tehditlerle karşı karşıya olan varlıkların belirlemeden, ciddi ve verimli bir güvenlik politikası ve planı oluşturamazlar. Risk analizinin amacı, uygun güvenlik politikasını seçmek ve uyarlamak için bilgi sistemlerinin ve onun varlıklarının karşı karşıya olduğu riskleri tanımlamak ve değerlendirmektir.

Risklerin analizi 4 aşamalı olarak gerçekleştirilir.

a) Varlıkların tanımlanması ve değerlendirilmesi
b) Tehditlerin tanımlanması ve değerlendirilmesi
c) Zayıflıkların değerlendirilmesi
d) Risk değerlemesi

Varlıklar bir bilgi sisteminin değer üreten varlıklarıdır. Meydana gelen güvenlik sorunları, varlıkları ve varlıkların sahibi olan organizasyonu ve onun ortakları ve üçüncü kişileri dolaylı olarak etkileyecektir. Varlıklar olası bozulmaları ve yok olmaları durumundaki etkiye göre değerlendirilmelidir. Tehditler tek başlarına değil aynı zamanda güvenlik sorunlarına neden olacak zayıf noktalarla birlikte değerlendirilmelidir.

Risk analizinin devamı olarak, organizasyonun zayıf noktalarını referans alarak bir güvenlik planı geliştirilmelidir. Güvenlik planı güvenliğin nasıl gerçekleştirileceğini gösteren bir güvenlik politikası ile uygulanmalıdır. Güvenlik politikası organizasyonel kaynakların uygun kullanımını, hesapları talep eden ve devam ettiren bireylerin gereksinimlerini, organizasyon ağına yabancı bağlantıların kabul edilebilir bağlantısını, bilginin yetkisiz erişim, ifşa, suistimal ve kayıplara karşı korunma yolları, iletişim ağına yeni araçların eklenmesi ve ayrılacalıklı sistem hesaplarının kullanım kurallarını içeren yöntemleri içermelidir.

Güvenlik politikası yeterli güvenlik seviyesinin sağlanıp sağlanmadığı konusunda gözden geçirilmelidir. Ayrıca güvenlik politikası güvenlik sorunlarının, doğal felaketlerin ve çalışanlarla ilgili tehditlere ilişkin duyumların sağlayan güvenlik uygulamalarına ilişkin yeterli ve uygun prosedürleri de içermelidir. Böyle bir politika donanımlarla ilgili olarak fiziki saldırılara karşı gelecek şekilde çevresel kontrolleri ve alarm sistemlerini de içermelidir. Yazılım şifreleri, ateş duvarları, yedekleme çalışmaları ve kriptolama da yazılım seviyesinde meydana gelebilecek fiziki zararlara karşı tedbir olarak güvenlik politikasında yer almalıdır.

Bilgi sistemlerinde güvenlik sadece tek boyutlu değildir. Yani sadece teknoloji ile ilgili bir konu değildir. Güvenlik teknoloji ile birlikte insanların ve iş süreçlerininde göz önünde bulundurulması gereken bir konudur. [73]

Aynı zamanda bilgi sistemleri denetim prosedürleri yayınlanmalıdır. Personele bilgi sistemleri güvenliği ile ilgili olarak gerekli eğitimler verilmelidir. Tam zamanlı bir bilgi sistemleri güvenlik yetkilisi, bu tür tehditlere karşı alınacak önlemleri koordine ederek izleyebilir ve bu tedbirlerin uygulanmasını güçlü hale getirebilecektir.

---

[73] John W. Lindquist, "Information Security Management, Engineering and Assurance" ITAUDIT.ORG, May 15, 2001, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Bilgi sistemleri açısından risk; bir organizasyonun kendisi ve amaçları üzerinde istenmeyen ve beklenmeyen etkilere neden olan olaylar nedeni ile zararların ve kayıpların meydana gelme olasılığıdır. [74] Bilgi sistemleri açısından riskin meydana gelmesi karşımıza tehditler, zayıf noktalar ve etkiler olmak üzere üç kavram çıkmaktadır.

Denetmenler bilgi sistemlerine yönelik usulsüzlüklere karşı koruyucu kalkan durumundadır. Zira denetmenler gerekli kontrol eksiklikleri ve riskleri belirleyerek bilgi sistemlerine yapılacak saldırılara karşı bir siper niteliğindedir. [75]

Denetmenlerin amacı bilgi sistemlerindeki kayıplara neden olacak riskler nedeniyle ortaya çıkacak zararları engellemek için yapılan kontrol çalışmalarını değerlendirmek bu kontrol çalışmalarının etkinliği noktasında yorumlar yapmaktır. [76]

Tehditler iç ve dış kaynaklı olarak organizasyonun zayıf noktalarını etkileyerek olumsuz etkilere neden olacak olaylar ve aktivitelerdir.

Zayıf noktalar; bir organizasyonun bilgi sisteminde tehditlerle karşılaşma olasılığı olan güçlü olmayan yerlerdir.

Etkiler; ise tehditlerin organizasyonun bilgi sistemlerindeki zayıf noktaları zorlaması sonucunda meydana gelen kısa ve uzun dönemli organizasyonel olumsuz sonuçlardır.

Yukarıda verilen risk tanımı ve açıklamalar doğrultusunda, risk aşağıdaki şekilde formüle edilebilir.

---

[74] Thomas R Horton, Charles H. Legrand, William H. Murray, Willis J Ozier and B. Parker, "Managing Information Security Risks" ITAUDIT.ORG, August 15, 2000, (Çevirimiçi) http://www.itaudit.org/index_search.htm

[75] Charler H. Le Grand "Auditors on Guard Against Fraud" ITAUDIT.ORG, August 15, 2000, (Çevirimiçi) http://www.itaudit.org/index_search.htm

[76] J.P. Pathak, "IT Audit Approach, Internal Controls, and Audit Decisions of an IT Auditor", ITAUDIT.ORG, June 1, 2000, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Risk = Tehditler + Zayıf Noktalar + Etkiler

Riskin meydana gelme durumu şu şekilde açıklanabilmektedir; Riskin olabilmesi için ilk olarak tehdit olmalıdır. Tehdit sadece riskin meydana gelmesi için bir neden değildir. Tehditle birlikte o alanda mutlaka zayıf noktalarda olmalıdır. Şayet tehdit var ancak bilgi sistemi o noktada oldukça sağlam ise herhangi bir riskten söz edilmesi mümkün olmamaktadır. Tehdit ve zayıf noktaların yanında gerçek etkilerin olması gerekmektedir. [77]

Bu açıdan bakıldığında mevcut tehditlerini analiz ederek bilen, bu analiz sonucunda zayıf yönlerin değerlendiren, gerekli güvenlik tedbirlerini alan ve mevcut tehditlerin olumsuz sonuçlar meydana getirmesine mani olan bankalar, bilgi sistemleri açısından daha güvenilir durumda olacaktır. [78]

Bankalar ve bilgi sistemini kullanan tüm organizasyonlar için bilgi sistemlerinin etkinlik ve verimlilik probleminden ziyade bilgi sistemlerinin güvenlik problemi daha büyük bir önem arz etmektedir. Zira etkinlik ve verimlilik problemi bir organizasyonun belki daha az kar etmesini sağlayacak iken, bilgi sistemleri güvenliğinde meydana gelen aksamalar ve ihlaller, organizasyonun telafi edilemez maddi kayıplara uğramasına neden olacak ve faaliyet gösterdiği sektörde tüm prestijini ve pazar payını kaybetmesine neden olacaktır.

---

[77] Gary Hinson, "A Practical Model for Risk Assessment and Prioritization", ITAUDIT.ORG, April 1, 2000, (Çevirimiçi) http://www.itaudit.org/index_search.htm

[78] Will Ozier, "A Framework for an Automated Risk Assessment Tool", ITAUDIT.ORG, August 15, 1999, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Bu durum tamamen bir güven merkezi olan bankalar için düşünüldüğünde sonuçların çok daha ağır olacağının tahmin edilmesi güç olmayacaktır. Bu nedenle ülkemizdeki bankacılık sektörünün bilgi sistemleri güvenliği açısından risk oluşturduğu tezinden hareketle, bankalarımızdaki bilgi sistemleri güvenliğinin incelenmesinde en iyi yöntemin bir endeksleme çalışması olacağı düşünülmüş ve bankalarımıza ait bilgi sistemleri güvenliği endeksi kurularak sonuçları incelenmiştir.

Yukarıda söz edilen risk ölçüm yöntemi bağlamında Bankacılık Sektöründeki Bilgi Sistemleri Güvenlik Derecesi ölçülmesi için sektörde faaliyet gösteren bankalar seçilmiş ve bunlara bilgi sistemleri güvenliğine ilişkin anket soruları gönderilmiştir. Bankaların seçilmesinde Türkiye merkezli olarak kurulan yerli ve yabancı ticari bankalar ve özel finans kurumları tercih edilmiş ve anketleme çalışması bu bankalar üzerinde anketleme çalışması gerçekleştirilmiştir. Türkiye merkezli olarak kurulan yerli ve yabancı ticari bankalar ve özel finans kurumlarının sayısı 33'dür. [79]

Anket formu sonucu alınan banka sayısı 14'dür. Bu sayısı yukarıda belirtilen sayıya oranla %45,5'lik bir oranı vermektedir ki, bu oranın Türk Bankacılık Sektörü Bilgi Sistemleri Güvenliği Endeksi kurulabilmesi açısından örneklemenin gerçekleştirilmesi için yeterli sonuç olduğu söylenebilir.

Bilgi Sistemleri Güvenlik Endeksi'nde kullanılacak olan sorular University of Aegean öğretim üyelerinden Euripidis Loukis ve Diomidis Spinellis tarafından hazırlanan "Yunan Kamu Sektöründe Bilgi Sistemleri Güvenliği" isimli makaleden model olarak alınmıştır. Bu anket soruları iki kısımdan oluşmaktadır.

[79] Bankalar Birliği Resmi Web Sitesi, (Çevirimiçi) http://www.tbb.org.tr, 02 Eylül 2002

Anket sorularının birinci kısmında bilgi sistemleri güvenliği kriterlerine ilişkin sorular yer almaktadır.[80] Bu sorular

a) Analiz kriterleri
b) Organizasyonel kriterler
c) Teknik kriterler
d) İnsan kaynaklarına ait kriterler

olmak üzere dört ana başlıktan oluşmaktadır.

Analiz kriterleri, bankaların güvenlik ihlallerinden dolayı meydana gelebilecek olan risklerin ve bilgi sistemlerinde elektronik olarak arşivlenen bilgilerin güvenliğine ait risk analiz çalışmalarının değerlendirilmesi amacıyla ankette yer alan sorulardır.

Organizasyonel kriterler bölümünde bankaların bilgi sistemleri güvenliğine ilişkin prosedürlerinin, planlarının, politikalarının ve organizasyonel yapılanmasına ilişkin çalışmaların değerlendirilmesi amacıyla ankette yer verilen suallerdir.

Teknik kriterler bölümünde bankaların bilgi sistemleri güvenliğine ilişkin fiziki erişim kontrollerinin ve yetkisiz olarak elektronik ortamdaki erişimleri engelleyecek teknik tedbilerin alınıp alınmadığının belirlenmesi amacıyla sorulan sorulardır.

İnsan kaynaklarına ilişkin kriterler ise bilgi sistemleri güvenliğine yönelik olarak, bankaların insan kaynaklarının nasıl yapılandırıldığının ve insan kaynaklarına bilgi sistemleri güvenliği konusunda yeterli eğitimlerin verilip verilmediğinin değerlendirilmesi amacıyla ankette yer alan suallerdir.

Anket sorularının ikinci kısmında ise anketin birinci bölümünde yer alan sorulara verilen cevaplarla organizasyonel ve teknik bağlantıların kurulabileceği faktörlere ilişkin sorular yer almaktadır. Bu sorular

---

[80] Euripdis Loukis, Diomidis Spinellis, " Information Systems Security in the Greek public sector" Information Management and Computer Security Journal, MCB University Press, 2001, pp. 21-31

a) Dahili Kullanım Faktörleri
b) Dahili Bilgi Sistemleri Bölümü Faktörleri
c) Dış Faktörler

olmak üzere üç ana başlıktan oluşmaktadır.

Dahili kullanım faktörleri bankaların bilgi sistemlerini kullanıcı sayılarının ve bankanın bilgi sistemleri tarafından desteklenen fonksiyonlarının durumunun belirlenmesini sağlayan faktörlerdir.

Dahili bilgi sistemleri bölümü faktörleri, bankaların bilgi sistemleri organizasyonunda çalışan kişilerin ve bilgi sistemleri organizasyonunun bankalardaki hiyeraşik yapısının durumunu belirleyen faktörlerdir.

Dış faktörler ise bankaların sahip olduğu bilgi sistemlerine dışardan yapılan ihlallerin takip edilip edilmediği ve bilgi sistemlerine dışarıyla olan bağlantılarını belirleyen faktörlerdir.

Anket formunun birinci bölümünde toplam olarak 14 soru yer almış ve bilgi sistemleri güvenlik kriterlerine ait tüm soruların cevapları evet-hayır seçenekleri olarak verilmiştir. Bu sorularda verilen her evet cevabı değerlendirilmede 1 puan alırken, verilen her hayır cevabı 0 puan olarak değerlendirilmiştir. Evet cevabına ait puanlar toplanarak sonucunda elde edilen sayısal veri toplam kriter sayısına bölünerek genel güvenlik endeksi bulunurken aynı zamanda değişik kriter gruplarına ait güvenlik endeksleri de hesap edilmiştir.

Anket formunun ikinci bölümünde yer alan organizasyonel ve teknik faktörlere ait bölümde toplam olarak 7 soru yer almış ve bu sorulara verilen cevaplar daha özellikli olarak düşünülmüş ve 2-3 cevap şıkkından oluşturulmuştur. Bu sorulara verilen cevaplar Bilgi Sistemleri Güvenlik Kriterleriyle ilgili sorulara verilen cevaplarla organizasyonel ve teknik ilişkilerin sağlanması amacıyla kullanılmıştır. Organizasyonel ve teknik faktörlerdeki dağılımın, bilgi sistemleri güvenlik endeksi ile etkileşimi ölçülmüştür.

Güvenlik endeksinin bulunmasında aşağıdaki formüller kullanılmıştır,

Kriter Bazında

$$\text{Güvenlik Endeksi} = 1 - \frac{\text{Olumlu Sonuçlar Toplamı}}{\text{Ankete Katılan Banka Sayısı}} * 100$$

Banka Bazında

$$\text{Güvenlik Endeksi} = 1 - \frac{\text{Olumlu Sonuçlar Toplamı}}{\text{Toplam Soru Sayısı}} * 100$$

Genel Güvenlik Endeksi

$$\text{Güvenlik Endeksi} = 1 - \frac{\text{Kriter Bazında Güvenlik Endeksleri Top.}}{\text{Toplam Kriter Sayısı}} * 100$$

veya

Genel Güvenlik Endeksi

$$\text{Güvenlik Endeksi} = 1 - \frac{\text{Banka Bazında Güvenlik Endeksleri Top.}}{\text{Ankete Katılan Toplam Banka Sayısı}} * 100$$

Yukarıdaki formüllere örnek verilmesi gerekirse,

Banka bazında güvenlik endeksi,

$$\text{X Bankası Güvenlik Endeksi} = 1 - \frac{8}{14} * 100$$

X Bankası Güvenlik Endeksi = (1 – (0,57)) * 100)

X Bankası Güvenlik Endeksi = 42,8

X Bankasının yanında Y ve Z bankalarınında ankete katıldığını ve banka bazında aşağıdaki sonuçlara ulaşıldığını düşünelim

Y Bankası Güvenlik Endeksi = 28,6

Z Bankası Güvenlik Endeksi = 0,0

Bu durumda X, Y ve Z Bankaları Güvenlik Endeksi aşağıdaki gibi olacaktır,

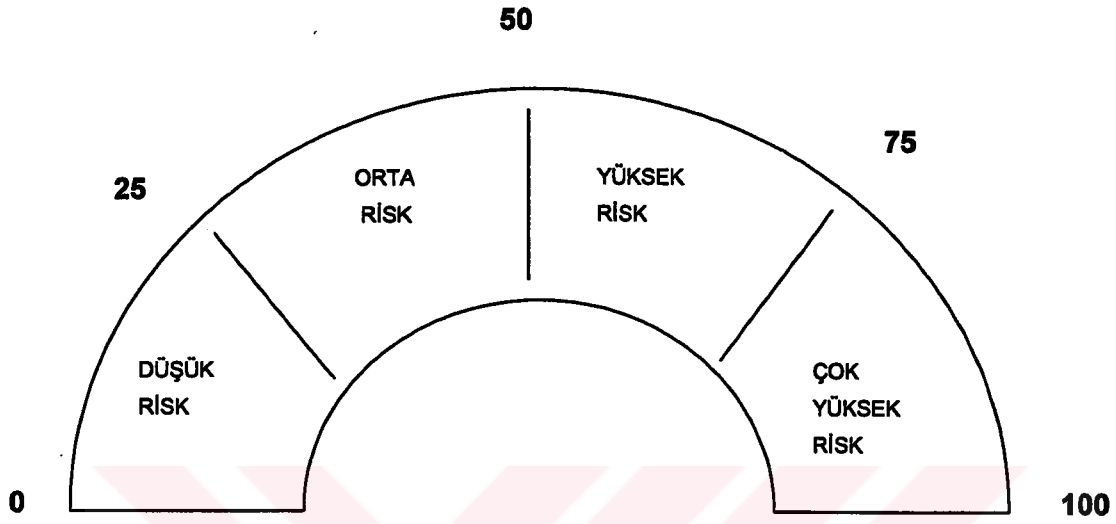
$$= \frac{42,8 + 28,6 + 0}{3} = 23,8$$

Yukarıda belirtilen örnekler ankete katılan toplam 14 banka için uygulanarak gerek kriter bazında gerekse banka bazında endeks değerlerine ulaşılmıştır. Ankete katılan bankaların güvenlik endekslerine ait sonuçların verilmesi doğru olmayacağından dolayı kriter bazında endeksler açıklanmış ve kriter bazındaki endeks değerlerinden hareket edilerek Güvenlik Endeksine ulaşılmıştır.

Güvenlik Endeksi sonucunda elde edilen değer aşağıdaki şekilde yer alan değerleme ölçütleriyle yorumlanmıştır.. Endeks değerleri 0-25 arasında olanlar düşük risk seviyesinde, 26-50 arasında olanlar orta risk seviyesinde, 51-75 arasında olanlar yüksek risk seviyesinde ve 76-100 arasında olanlar ise çok yüksek risk seviyesinde olarak açıklanmıştır. [81]

[81] Nils-Gören Olve, Jan Roy ve Magnus Wetter, "Performance Drivers", John Wiley & Sons, England, 2000 p. 240

Şekil 3.2.
Güvenlik Endeksi Risk Değerleme Ölçütleri



Kaynak : Nils-Gören Olve, Jan Roy ve Magnus Wetter, "Performance Drivers", John Wiley & Sons, West Sussex, 2000, s. 240

Anket sorularının tamamı ilgili bölümlerle birlikte aşağıdaki gibidir.

BİLGİ SİSTEMLERİ GÜVENLİĞİ ENDEKSİ

ANKET SORULARI

BİLGİ SİSTEMLERİ GÜVENLİĞİ KRİTERLERİ

ANALİZ KRİTERLERİ

K1 : Güvenlik ihlallerinden meydana gelecek olan riskler analiz ediliyor mu?

a) Evet
b) Hayır

K2 : Bilgi Sistemlerinde Elektronik Olarak Depolanan Verinin Güvenliği Analiz Ediliyor mu?

a) Evet
b) Hayır

ORGANİZASYONEL KRİTELER

K3 : Veri Güvenliği İhlali Sonrası Düzeltme Prosedürleri Mevcut mu?

a) Evet
b) Hayır

K4 : Yazılı ve Onaylanmış Bilgi Sistemleri Güvenliği Planı Mevcut mu?

a) Evet
b) Hayır

K5 : Yazılı ve Onaylanmış Spesifik Roller ve Prosedürlerle Bilgi Sistemleri Güvenliği Politikası Mevcut mu ?

a) Evet
b) Hayır

K6 : Hem Fiziki Hem de Mantıki Seviyede Güvenlik Alanları Mevcut mu ?

a) Evet
b) Hayır

K 7 : Kopyalama İşlemlerine ait Prosedürler Mevcut mu?

a) Evet
b) Hayır

K 8 : Bilgi Sistemleri İç Denetimine Ait Prosedürler Mevcut mu?

a) Evet
b) Hayır

TEKNİK KRİTERLER

K9 : Fiziki Erişim Kontrolleri Uygulanıyor mu?

a) Evet
b) Hayır

K10 : Operasyonel Ateş Duvarı (Firewall) Sistemi Uygulanıyor mu?

a) Evet
b) Hayır

İNSAN KAYNAKLARI KRİTERLERİ

K11 : Tam Zamanlı Bilgi Sistemleri Güvenliği Yetkilisi Mevcut mu?

a) Evet
b) Hayır

K12 : Tam Zamanlı Bilgi Ağı (Network) Yöneticisi Mevcut mu?

a) Evet
b) Hayır

K13 : Bilgi Sistemleri Güvenliği Yetkilisi ve Bilgi Ağı Yöneticisine Yeterli Eğitim Veriliyor mu?

a) Evet
b) Hayır

K14 : Bilgi Sistemleri Kullanıcılarına Bilgi Sistemlerinin Doğru ve Güvenli Kullanımı ile İlgili Yeterli Eğitim Veriliyor mu?

a) Evet
b) Hayır

ORGANİZASYONEL VE TEKNOLOJİK FAKTÖRLER

DAHİLİ KULLANIM FAKTÖRLERİ

F1 : Bilgi Sistemleri Kullanıcılarının Sayısı

a) 0-100
b) 101-400
c) 400-

F2 : Bilgi Sistemleri Tarafından Desteklenen Organizasyonun Fonksiyonlarının Sayısı

a) Tüm Fonksiyonlar
b) Fonksiyonların Çoğu
c) Fonksiyonların Küçük Bir Bölümü

DAHİLİ BİLGİ TEKONOLOJİSİ UNİTESİ FAKTÖRLERİ

F3 : Bilgi Sistemleri Organizasyonunda Bilgi Teknolojilerinden Sorumlu Olan Personel Sayısı

a) 0-10

b) 11-40

c) 40-

F4 : Bilgi Sistemleri Organizasyonunun Hiyeraşik Seviyesi

a) Direktörlük

b) Departman

DIŞ FAKTÖRLER

F5 : Elektronik Bilgi Güvenliği İhlalleri Sıklığını Biliyor musunuz?

a) Evet

b) Hayır

F6 : Bilgi Sistemlerine Dış Kullanıcılar Tarafından Erişim Yapılıyor mu?

a) Evet

b) Hayır

F7 : Bilgi Sistemlerinden Internete Bağlantı Yapılıyor mu? (Bir bilgisayar bile olsa)

a) Evet

b) Hayır

3.3. Türk Bankacılık Sektörü Bilgi Sistemleri Güvenlik Endeksi Sonuçları

Bankalardan alınan anket formlarının alınmasıyla birlikte sonuçlar değerlendirilmiş ve aşağıdaki sonuçlara ulaşılmıştır.

Tablo 3.1.

Analiz Kriterleri ve Endeks Değerleri

ANALİZ KRİTERLERİ	OLUMLU CEVAP %	ENDEKS DEĞERLERİ
K1: Güvenlik ihlallerinden meydana gelecek olan riskler analiz ediliyor mu?	93,3	6,7
K2: Bilgi sistemlerinde elektronik olarak yedeklenen verilerin güvenliği analiz ediliyor mu?	100,0	0,0

Analiz kriterleri ile ilgili sonuçlara bakıldığında ankete cevap veren bankaların %93,3'ü güvenlik ihallerinden meydana gelecek olan risklerin ve %100'ü bilgi sistemlerinde elektronik ortamda yedeklenen verilerin güvenliği konusunda analiz çalışmalarının yapıldığını belirtmişlerdir. Bu sonuca göre analiz kriterleri başlığı altında güvenlik endeksi 3,4 olarak sonuçlanmıştır.

Tablo 3.2.

Organizasyonel Kriterler ve Endeks Değerleri

ORGANİZASYONEL KRİTERLER	OLUMLU CEVAP %	ENDEKS DEĞERLERİ
K3: Veri güvenliği ihlalleri sonrası düzeltme prosedürleri mevcut mu?	80,0	20,0
K4: Yazılı ve onaylanmış bilgi sistemleri güvenliği planı mevcut mu?	46,7	53,3

K5: Yazılı ve onaylanmış spesifik roller ve prosedürlerle bilgi sistemleri politikası mevcut mu?	46,7	53,3
K6: Hem fiziki hem de mantıki seviyede güvenlik alanları mevcut mu?	100,0	0,0
K7: Yedekleme işlemlerine ait prosedürler mevcut mu?	93,9	6,1
K8: Bilgi sistemleri iç denetimine ait prosedürler mevcut mu?	60,0	40,0

Organizasyonel kriterlerle ilgili sonuçlara bakıldığında ankete katılan bankaların %100'ü hem fiziki hem de mantıki seviyede güvenlik alanlarının mevcut olduğunu belirtmişlerdir. Bankaların %80,0'i veri güvenliği sonrasında düzeltme işlemlerine ait prosedürlerin mevcut olduğunu belirtmişlerdir.

Bankaların %93,9'u ise yedekleme işlemlerine ait prosedürlerin mevcut olduğunu ifade ederken, bankaların ancak %46,7'si üst yönetim tarafından onaylanarak yayınlanmış bilgi sistemleri güvenliği planı ve bilgi sistemleri politikasının mevcut olduğunu belirtmişlerdir. Bu oranlar ise tüm anket sonuçları arasındaki en düşük sonuçlardır. Tüm organizasyonel kriterler başlığı altında güvenlik endeksi 37,9 olarak sonuçlanmıştır.

Tablo 3.3.

Teknik Kriterler ve Endeks Değerleri

TEKNİK KRİTERLER	OLUMLU CEVAP %	ENDEKS DEĞERLERİ
K9: Fiziki erişim kontrolleri uygulanıyor mu?	100,0	0,0
K10: Operasyonel ateş duvarı (firewall) sistemi uygulanıyor mu?	100,0	0,0

Teknik kriterlerle ilgili sonuçlara bakıldığında ankete katılan bankaların %100'ü bilgi sistemi varlıklarına ilişkin fiziki erişim kontrollerinin ve bilgi sistemlerine elektronik ortamda yetkisiz erişimi engelleyen operasyonel ateş duvarı sisteminin uygulandığını belirtmişlerdir. Tüm teknik kriterler düşünüldüğünde, teknik analiz kriterleri başlığı altında güvenlik endeksi 0,0 olarak sonuçlanmıştır.

Tablo 3.4.

İnsan Kaynakları Kriterleri ve Endeks Değerleri

İNSAN KAYNAKLARI KRİTERLERİ	OLUMLU CEVAP %	ENDEKS DEĞERLERİ
K11: Tam zamanlı bilgi sistemleri güvenliği yetkilisi mevcut mu?	73,3	26,7
K12: Tam zamanlı bilgi ağı (network) yöneticisi mevcut mu?	86,7	13,3
K13: Bilgi sistemleri güvenliği yetkilisi ve bilgi ağı yöneticisine yeterli eğitim veriliyor mu?	66,7	33,3
K14: Bilgi sistemleri kullanıcılarına bilgi sistemlerinin doğru ve güvenli kullanımı ile ilgili yeterli eğitim veriliyor mu?	60,0	40,0

İnsan kaynakları kriterleri sonuçlarına bakıldığında ankete katılan bankaların %86,7'si tam zamanlı bilgi ağı (network) yetkilisinin ve %72,7'si ise tam zamanlı bilgi sistemleri güvenliği yetkilisinin mevcut olduğunu belirtmişlerdir. Bankaların %60'ı ise bilgi stemleri kullanıcılarına bilgi sistemlerinin doğru ve güvenli kullanımı ile ilgili yeterli eğitimin verildiğini belirtmiştir.

Ankete katılan bankaların %66,7'si ise bilgi sistemi güvenliği yetkilisi ve bilgi ağı yöneticisine yeterli eğitimin verildiğini ifade etmişlerdir. Tüm insan kaynakları kriterleri başlığı altında güvenlik endeksi 28,3 olarak sonuçlanmıştır.

Aşağıdaki şekilde Tüm Bilgi Sistemleri Güvenlik Kriterleri ve Güvenlik Endekleri görülmektedir.

Tablo 3.5.

Tüm Kriterler ve Endeks Değerleri

KRİTERLER GENEL SONUÇLARI	OLUMLU CEVAP %	ENDEKS DEĞERLERİ	RİSK SEVİYESİ
K1: Güvenlik ihlallerinden meydana gelecek olan riskler analiz ediliyor mu?	93,3	6,7	DÜŞÜK RİSK
K2: Bilgi sistemlerinde elektronik olarak yedeklenen verilerin güvenliği analiz ediliyor mu?	100,0	0,0	DÜŞÜK RİSK
K3: Veri güvenliği ihlalleri sonrası düzeltme prosedürleri mevcut mu?	80,0	20,0	DÜŞÜK RİSK
K4: Yazılı ve onaylanmış bilgi sistemleri güvenliği planı mevcut mu?	46,7	53,3	YÜKSEK RİSK
K5: Yazılı ve onaylanmış spesifik roller ve prosedürlerle bilgi sistemleri politikası mevcut mu?	46,7	53,3	YÜKSEK RİSK
K6: Hem fiziki hem de mantıki seviyede güvenlik alanları mevcut mu?	100,0	0,0	DÜŞÜK RİSK

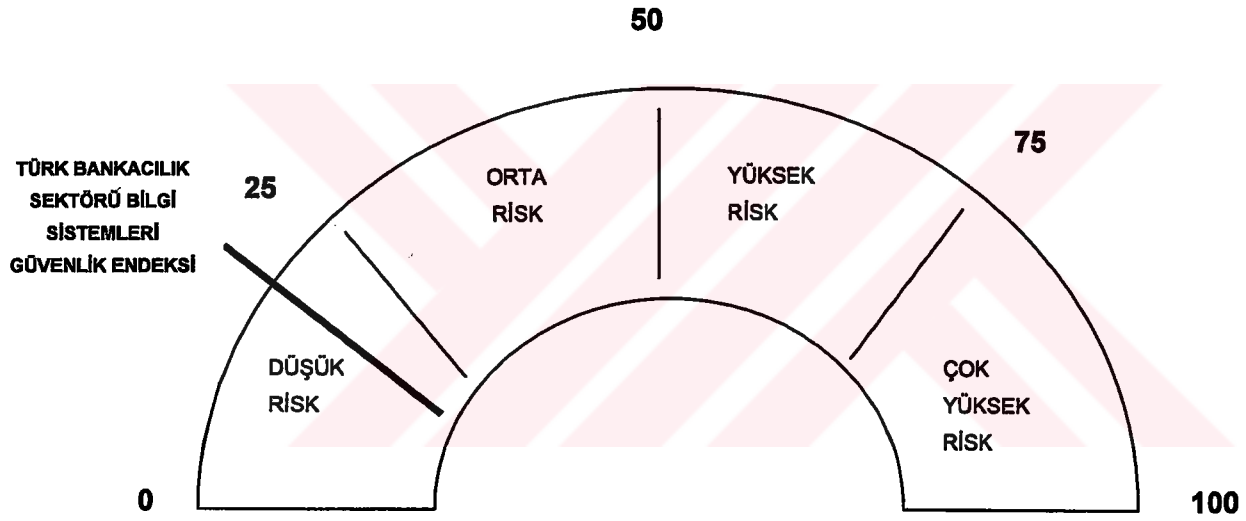
K7: Yedekleme işlemlerine ait prosedürler mevcut mu?	93,9	6,1	DÜŞÜK RİSK
K8: Bilgi sistemleri iç denetimine ait prosedürler mevcut mu?	60,0	40,0	ORTA RİSK
K9: Fiziki erişim kontrolleri uygulanıyor mu?	100,0	0,0	DÜŞÜK RİSK
K10: Operasyonel ateş duvarı (firewall) sistemi uygulanıyor mu?	100,0	0,0	DÜŞÜK RİSK
K11: Tam zamanlı bilgi sistemleri güvenliği yetkilisi mevcut mu?	73,3	26,7	ORTA RİSK
K12: Tam zamanlı bilgi ağı (network) yöneticisi mevcut mu?	86,7	13,3	DÜŞÜK RİSK
K13: Bilgi sistemleri güvenliği yetkilisi ve bilgi ağı yöneticisine yeterli eğitim veriliyor mu?	66,7	33,3	ORTA RİSK
K14: Bilgi sistemleri kullanıcılarına bilgi sistemlerinin doğru ve güvenli kullanımı ile ilgili yeterli eğitim veriliyor mu?	60,0	40,0	ORTA RİSK

Yukarıdaki kriter bazında güvenlik endeksleri sonucunda elde edişen genel güvenlik endeksi aşağıdaki gibi şekillenmiştir.,

Türk Bankacılık Sektörü Bilgi Sistemleri Güvenlik Endeksi	**=**	***21,0***
Güvenlik Riski Seviyesi	**=**	***DÜŞÜK RİSK SEVİYESİ***

Şekil 3.3.

Türk Bankacılık Sektörü Güvenlik Endeksi Risk Seviyesi



Türk Bankacılık Sektörü Bilgi Sistemleri Güvenlik Endeksi 21,0 değeri ile düşük risk seviyesinde kalmıştır. Bu olumlu görülen sonuca rağmen ankete katılan tüm bankaların ve anketteki tüm kriterlere ait endekslerin aynı değerlere sahip olmadığı ve aynı performansa sahip olmadığı görülmüştür. Nitekim aşağıdaki tabloda da görülebileceği gibi ankete katılan bankaların % 6,7'si yüksek risk seviyesinde yer alırken, %33,3'ü ise orta risk seviyesinde bulunmakadır.

Tablo 3.6.

Endeks Değerlerinin Banka Sayları Arasındaki Dağılımı

Banka Sayısı	%	Endeks Aralığı	Risk Seviyesi
0	0,0	76-100	Çok Yüksek Risk
1	6,7	50-75	Yüksek Risk
5	33,3	26-50	Orta Risk
9	60,0	0-25	Düşük Risk

Bunun yanında güvenlik endeksi kriterlerinin tümü düşük risk seviyesinde değildir. Nitekim aşağıdaki tablodan da görülebileceği gibi kriterlerin önemli bir kısmı orta ve yüksek risk seviyesinde bulunmaktadır. Bu risk seviyelerinde bulunan kriterler ise bankaların bilgi sistemleri açısından zayıf olduğu alanları vermektedir.

Tablo 3.7.

Türk Bankacılık Sektörü'nün Bilgi Sistemleri Güvenliği Açısından Zayıf Olduğu Alanlar

KRİTERLER	ENDEKSLER	RİSK SEVİYESİ
K4: Yazılı ve onaylanmış bilgi sistemleri güvenliği planı mevcut mu?	53,3	YÜKSEK RİSK
K5: Yazılı ve onaylanmış spesifik roller ve prosedürlerle bilgi sistemleri politikası mevcut mu?	53,3	YÜKSEK RİSK
K8: Bilgi sistemleri iç denetimine ait prosedürler mevcut mu?	40,0	ORTA RİSK
K11: Tam zamanlı bilgi sistemleri güvenliği yetkilisi mevcut mu?	26,7	ORTA RİSK
K13: Bilgi sistemleri güvenliği yetkilisi ve bilgi ağı yöneticisine yeterli eğitim veriliyor mu?	33,3	ORTA RİSK
K14: Bilgi sistemleri kullanıcılarına bilgi sistemlerinin doğru ve güvenli kullanımı ile ilgili yeterli eğitim veriliyor mu?	40,0	ORTA RİSK

Bankalardan alınan anket formlarında yer alan faktörel sorulara verilen cevaplar değerlendirilmiş ve aşağıdaki sonuçlara ulaşılmıştır.

Tablo 3.8.

Bilgi Sistemleri Kullanıcılarının Sayısı ve Endeks Değerleri

BİLGİ SİSTEMLERİ KULLANICILARININ SAYISI	FAKTÖRLERİN % DAĞILIMI	FAKTÖRE BAĞLI GÜVENLİK ENDEKSİ
0-100	0,0	0,0
101-400	6,7	14,3
400-	93,3	21,4

Ankete katılan bankaların %93,3'ü kendilerinde mevcut olan bilgi sistemi kullanıcı sayısının 400 ve 400'den fazla olduğunu ve bankaların %6,7'si ise kullanıcı sayılarının 101-400 arasında olduğunu belirtmiştir. Kullanıcı sayısı faktöründeki dağılıma bağlı olarak yapılan güvenlik endeksinde, kullanıcı sayısı artan bankalarda güvenlik endeksinin daha yüksek bir değer aldığı görülmektedir.

Tablo 3.9.

Bilgi Sistemleri Tarafından Desteklenen Organizasyon Fonksiyonları ve Endeks Değerleri

BİLGİ SİSTEMLERİ TARAFINDAN DESTEKLENEN ORGANİZASYON FONKSİYONLARININ SAYISI	FAKTÖRLERİN % DAĞILIMI	FAKTÖRE BAĞLI GÜVENLİK ENDEKSİ
Tüm fonksiyonlar	53,3	12,5
Fonksiyonların çoğu	46,7	30,6
Fonksiyonların küçük bir bölümü	0,0	0,0

Ankete katılan bankaların %53,3'ü tüm fonksiyonlarının bilgi sistemleri tarafından desteklendiğini belirtirken, bankaların %36,4'u ise fonksiyonlarının çoğunun bilgi sistemleri tarafından desteklendiğini ifade etmiştir. Bu durum ise bilgi sistemlerinin bankacılık sektöründeki önemini daha iyi ortaya koymaktadır.

Bilgi sistemleri tarafından desteklenen fonksiyonların sayısı faktörüne bağlı olarak yapılan güvenlik endeksinde, fonksiyon sayısı artan bankaların daha düşük bir güvenlik endeksine sahip olduğu görülmektedir. Nitekim tüm fonksiyonları bilgi sistemleri tarafından desteklenen bankaların güvenlik endeksi 12,5 iken, fonksiyonların çoğunu destekleyen bilgi sistemlerine sahip bankaların güvenlik endeksi ise 30,6'dır. Bu bankacılık sektörü açısından olumlu bir resim çizmektedir.

Tablo 3.10.
Bilgi Teknolojilerinden Sorumlu Olan Personel Sayısı ve Endeks Değerleri

BİLGİ SİSTEMLERİ ORGANİZASYONUNDA BİLGİ TEKNOLOJİLERİNDEN SORUMLU OLAN PERSONEL SAYISI	FAKTÖRLERİN % DAĞILIMI	FAKTÖRE BAĞLI GÜVENLİK ENDEKSİ
0-10	6,7	14,3
11-40	60,0	32,5
40-	33,3	1,4

Bankaların bilgi teknolojilerinden sorumlu olan personel sayılarına bakıldığında 0-10 arasında personele sahip bankalar %6,7 iken, 11-40 arasında personele sahip bankalar %60,0 ve 40 ve üzerinde personele sahip bankalar ise %33,3'dür.

Bilgi teknolojilerinden sorumlu personel sayıları faktörüne bağlı olarak güvenlik endeksi personel sayısı ile doğru orantılı olarak düşmektedir. Nitekim 0-10 arasında bilgi teknolojilerinden sorumlu olan personele sahip bankaların güvenlik endeksi 14,3 iken 40 ve üstü personele sahip bankaların güvenlik endeksi 1,4 olarak gerçekleşmiştir.

Tablo 3.11.

Bilgi Sistemleri Organizasyonunun Hiyeraşik Seviyesi ve Endeks Değerleri

BİLGİ SİSTEMLERİ ORGANİZASYONUNUN HİYARAŞİK SEVİYESİ	FAKTÖRLERİN % DAĞILIMI	FAKTÖRE BAĞLI GÜVENLİK ENDEKSİ
Direktörlük	20,0	35,7
Departman	80,0	17,3

Bankaların %80,0'i bilgi sistemleri organizasyonun kendilerinde departman bazında olduğunu belirtirken, %20,0'si ise direktörlük bazında olduğunu belirtmiştir. Faktör bazında güvenlik endeksine bakıldığında departman bazında güvenlik endeksi 17,3 olurken direktörlükte ise endeks 35,7 olarak gerçekleşmiştir.

Tablo 3.12.

Elektronik Bilgi Güvenliği İhlalleri ve Endeks Değerleri

ELEKTRONİK BİLGİ GÜVENLİĞİ İHLALLERİ SIKLIĞI BİLİNİYOR MU?	FAKTÖRLERİN % DAĞILIMI	FAKTÖRE BAĞLI GÜVENLİK ENDEKSİ
Evet	66,7	17,1
Hayır	33,3	28,6

Bankaların %66,7'si bilgi sistemlerindeki güvenlik ihlalleri sıklığını bildiğini ifade ederken, bankaların %33,3'ü bilgi sistemlerindeki güvenlik ihlallerinin sıklığını bilmediklerini belirtmişlerdir. Faktöre bağlı güvenlik endeksine bakıldığında güvenlik ihlalleri hakkında bilgi sahibi olan bankaların güvenlik endeksinin 17,1 olurken, bilgi sistemi güvenlik ihlallerini bilmeyenlerin daha yüksek güvenlik endeksine sahip olarak 28,6 olduğu tespit edilmiştir.

Tablo 3.13.

Bilgi Sistemlerine Dış Kullanıcılar Tarafından Yapılan Erişim ve Endeks Değerleri

BİLGİ SİSTEMLERİNE DIŞ KULLANICILAR TARAFINDAN ERİŞİM YAPILIYOR MU?	FAKTÖRLERİN % DAĞILIMI	FAKTÖRE BAĞLI GÜVENLİK ENDEKSİ
Evet	100,0	21,0
Hayır	0,0	0,0

Bankaların %100'ünün bilgi sistemlerine dış kullanıcılar tarafından erişim yapıldığının belirtildiği görülmüştür. Bu durum bankacılık sektöründeki internet bankacılığının ne kadar ilerlediğinin ve bilgi sistemleri güvenliğinin ne kadar önem arz ettiğinin bir göstergesidir. Tüm bankalar evet cevabı verdiği için faktöre bağlı olan güvenlik endeksi doğal olarak genel güvenlik endeksi ile eşit olacaktır.

Tablo 3.14.

İnternet Erişimi ve Endeks Değerleri

BİLGİ SİSTEMLERİNDEN İNTERNETE ERİŞİM YAPILIYOR MU?	FAKTÖRLERİN % DAĞILIMI	FAKTÖRE BAĞLI GÜVENLİK ENDEKSİ
Evet	100,0	21,0
Hayır	0,0	0,0

Bankaların %100'ünün bilgi sistemlerinden internete erişim yapıldığının belirtildiği görülmüştür. Bu durum bankacılık sektöründeki bilgi sistemleri güvenliğinin ne kadar önem arz ettiğinin bir göstergesidir. Zira güvenlik açısından internet oldukça riskli bir alandır. Tüm bankalar evet cevabı verdiği için faktöre bağlı olan güvenlik endeksi doğal olarak genel güvenlik endeksi ile eşit olacaktır.

Ankete katılan bankalarla ilgili dikkati çeken önemli konulardan birisi de, bankaların %100'ünün bilgi sistemlerine elektronik ortamda erişimin ve internet bağlantısının mevcut olduğunu belirtmesine rağmen, bankaların %33'ünün bilgi sistemleri ihlallerinin sıklığı konusunda bilgi sahibi olmamaları oldukça düşündürücüdür.

SONUÇ VE DEĞERLENDİRME

Çağımızdaki organizasyonların fonksiyonlarını yerine getirmesinde vazgeçilmez bir araç haline gelen bilgi sistemleri, organizasyonlar için bir çok sorunu da beraberinde getirmiştir. Bilgi sistemlerinin etkin ve verimli kullanılması ve bilgi sistemlerinin güvenliğinin sağlanması, bilgi sistemlerine ilişkin en önemli sorunların başında gelmektedir. Bilgi sistemlerine ait bu sorunların tespit edilmesinde ve sorunlara ait çözüm üretilmesinde bilgi sistemlerine ait denetim çalışmaları en önemli yönetimsel işlevler arasında karşımıza çıkmaktadır.

Bilgi sistemleri denetimi geleneksel denetim çalışmalarının esasları dahilinde hareket eden ancak yanında bilgi sistemleri yönetimi, davranış bilimleri ve bilgisayar biliminden destek alan bir denetim aktivitesidir. En genel tanımı ile bilgi sistemleri denetimi; bir bilgi sistemi içindeki varlıkların korunup korunmadığını, bilgi güvenliğinin sağlanıp sağlanmadığını, bilgi sistemlerinin kuruluşundaki amaçlara ulaıp ulaşmadığını yani etkinliğini ve bilgi sistemlerinin organizasyon kaynaklarını verimli bir şekilde kullanıp kullanmadığını ortaya çıkarmak için gerçekleştirilen kanıt toplama ve değerlendirme sürecidir.

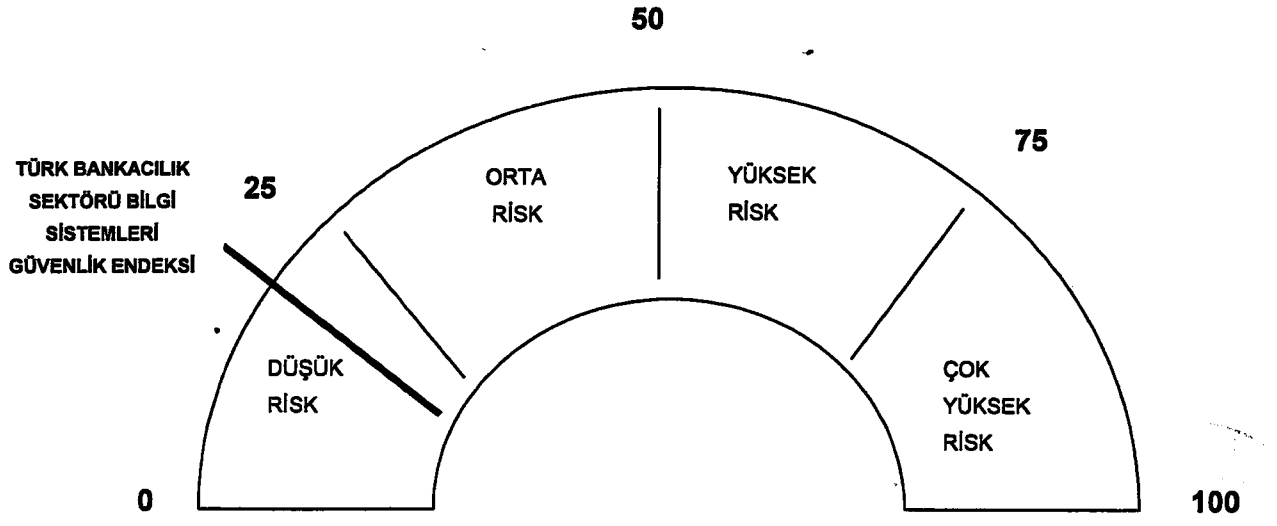
Bilgi sistemeleri denetimini başarıyla gerçekleştiren organizasyonlar bilgi sistemlerine ilişkin riskleri daha iyi analiz edebilmekte ve bilgi sistemlerine ait sorunlarına daha kolay çözüm üretebilmektedir. Bilgi sistemleri denetimi dünyada ve ülkemizde hemen hemen tüm fonksiyonlarını bilgi sistemlerinin aracılığı ile gerçekleştiren bankalar için bir kat daha önem kazanmaktadır. Özellikle bankaların gerek kendi aralarında gerekse müşteriyle gerçekleştirdikleri elektronik bilgi akışı ve operasyonlarında internet teknolojilerinden yararlandıkları düşünülürse, bankaların ne kadar önemli bir risk altında olduğu ve bilgi sistemleri denetiminin ne büyük bir önem arz ettiği görülebilir.

Bankalar ve bilgi sistemini kullanan tüm organizasyonlar için bilgi sistemlerinin etkinlik ve verimlilik probleminden ziyade bilgi sistemlerinin güvenlik problemi daha büyük bir önem arz etmektedir. Zira etkinlik ve verimlilik problemi bir organizasyonun belki daha az kar etmesini sağlayacak iken, bilgi sistemleri güvenliğinde meydana gelen aksamalar ve ihlaller, organizasyonun telafi edilemez maddi kayıplara uğramasına neden olacak ve faaliyet gösterdiği sektörde tüm prestijini ve pazar payını kaybetmesine neden olacaktır.

Bu durum tamamen bir güven merkezi olan bankalar için düşünüldüğünde sonuçların çok daha ağır olacağının tahmin edilmesi güç olmayacaktır. Bu nedenle ülkemizdeki bankacılık sektörünün bilgi sistemleri güvenliği açısından risk oluşturduğu tezinden hareketle, bankalarımızdaki bilgi sistemleri güvenliğinin incelenmesinde en iyi yöntemin bir endeksleme çalışması olacağı düşünülmüş ve bankalarımıza ait bilgi sistemleri güvenliği endeksi kurularak sonuçları incelenmiştir.

Bilgi sistemleri güvenliğine ait endeksleme çalışmasında University of Aegean öğretim üyelerinden Euripidis Loukis ve Diomidis Spinellis tarafından gerçekleştirilen Yunan Kamu Sektöründe Bilgi Sistemleri Güvenliği isimli incelemede kullanılan Anket soruları kullanılmıştır.

Ankete toplam olarak 15 banka katılmış ve anket sorularına verilen cevapların değerlendirilmesi neticesinde Türk Bankacılık Sektörü'nün Güvenlik Endeksi'nin 21,0 ile düşük risk seviyesinde olduğu tespit edilmiştir.



Türk Bankacılık Sektörü Bilgi Sistemleri Güvenlik Endeksi	**=**	***21,0***
Güvenlik Riski Seviyesi	**=**	***DÜŞÜK RİSK SEVİYESİ***

Türk Bankacılık Sektörü'nün Bilgi Sistemleri Güvenliğinin düşük risk seviyesine sahip olmasına rağmen ankete katılan tüm bankalar için aynı yorumu yapmak mümkün değildir. Nitekim aşağıdaki tabloda da görülebileceği gibi ankete katılan bankaların %40'ı yüksek ve orta risk seviyesinde bulunmaktadır.

Banka Sayısı	%	Endeks Aralığı	Risk Seviyesi
0	0,0	76-100	Çok Yüksek Risk
1	6,7	50-75	Yüksek Risk
5	33,3	26-50	Orta Risk
9	60,0	0-25	Düşük Risk

Türk Bankacılık Sektörü'nün Bilgi Sistemleri Güvenliğinin düşük risk seviyesine sahip olmasına rağmen, anket formunda yer alan tüm kriterlerin bilgi sistemleri güvenliği açısından düşük risk düzeyinde olduğu söylenemez, söz konusu güvenlik endeksini oluşturan tüm kriterler ve faktörel değişkenler incelendiğinde 25,0 endeks değerlerinin yani düşük risk seviyesi eşiğinin üstünde olan kriterlerin Türk Bankacılık Sektörü'nün Güvenlik açısından iyi olduğu alanlar olarak değerlendirilirken, bu seviyenin altında yer alan güvenlik kriterler ise Türk Bankacılık Sektörünün Güvenlik açısından zayıf olduğu alanlar olarak değerlendirilmiştir.

Aşağıdaki tabloda anket formunda yer alan, yüksek ve orta risk seviyesinde olan bilgi sistemleri güvenlik kriterleri görülebilmektedir;

KRİTERLER	ENDEKSLER	RİSK SEVİYESİ
K4: Yazılı ve onaylanmış bilgi sistemleri güvenliği planı mevcut mu?	53,3	YÜKSEK RİSK
K5: Yazılı ve onaylanmış spesifik roller ve prosedürlerle bilgi sistemleri politikası mevcut mu?	53,3	YÜKSEK RİSK
K8: Bilgi sistemleri iç denetimine ait prosedürler mevcut mu?	40,0	ORTA RİSK
K11: Tam zamanlı bilgi sistemleri güvenliği yetkilisi mevcut mu?	26,7	ORTA RİSK
K13: Bilgi sistemleri güvenliği yetkilisi ve bilgi ağı yöneticisine yeterli eğitim veriliyor mu?	33,3	ORTA RİSK
K14: Bilgi sistemleri kullanıcılarına bilgi sistemlerinin doğru ve güvenli kullanımı ile ilgili yeterli eğitim veriliyor mu?	40,0	ORTA RİSK

Türk Bankacılık Sektörü'nün Bilgi Sistemleri Güvenliği'ne ilişkin bu zayıf noktalar ışığında daha iyi bir bilgi sistemi güvenliği için aşağıdaki noktalara dikkat edilmesi ve geliştirilmesi gerekmektedir,

a) Bilgi sistemleri güvenliği ile ilgili üst yönetim tarafından tüm organizasyon tarafından uyulması gereken güvenlik politikaları ve güvenlik planları oluşturulmalı ve politikalar ve planlara uyulması konusunda üst yönetim tarafından hassasiyet gösterilmelidir,

b) Bilgi sistemi kullanıcılarına ve bilgi sistemi sorumlularına, bilgi sistemleri güvenliğine ait gerekli periyodik eğitimler verilmelidir,

c) Bilgi sistemleri güvenliğine ilişkin organizasyonel yapılanma kurularak gerekli insan kaynakları istihdamı sağlanmalıdır,

d) Bilgi sistemleri iç denetimine önem verilerek gerekli denetim prosedürleri oluşturulmalıdır.

Yukarıdaki konulara önem verilerek gerekli düzenlemelerin yapılması durumun Türk Bankacılık Sektörü'nün Bilgi Sistemleri Güvenliği açısından daha sağlam bir yapıya kavuşacağına inanılmaktadır. Bilgi sistemleri denetimi ve bilgi sistemleri güvenliği konusunda giriş niteliğinde olan bu çalışmanın, bu alanda araştırma yapmak isteyen tüm araştırmacılara destek olarak yol göstereceği umulmaktadır.

K A Y N A K Ç A

Alkin, E., Savaş, A. T., Akman, V., Bankalarda Risk Yönetimine Giriş, İstanbul, 2000,

Alpugan, O., Demir, M. H., Oktav, M., Üner N., İşletme Ekonomisi ve Yönetimi, Beta Yayınevi, İstanbul, 1995,

Arens, A. A., Loebbecke, J. K., Auditing An Integrated Approach, Prentice-Hall International, Inc., New Jersey, 1991

Arıcan, E., "Gelişmekte Olan Ülkelerde İstikrar Politikaları ve Türkiye", Der'in Yayınları, İstanbul, 2002

Bankacılık Düzenleme ve Denetleme Kurulu, Bankaların İç Denetim ve Risk Yönetim Sistemleri Hakkındaki Yönetmeliği

Bankalar Birliği'nin Resmi Web Sitesi (Çevirimiçi) http://www.tbb.org.tr,

Berk, N., Finansal Yönetim, Türkmen Kitabevi, İstanbul, 1995

Dubios, C.P.R., "The Information Audit" Library Management Volume MCB University Press, England, 1995, pp.20-24

Feinman, T., Goldman, D., Wong, R., Cooper, N., "Security Basics: A White Paper", ITAUDIT.ORG, September 15, 2000, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Fuhrman, A., "Your E-Banking Future", Strategic Finance, April, 2002, (Çevirimiçi) http://www.strategicfinancemag.com/2002/04g.htm

Hall, David C., "The Internet: It's Full of Holes", ITAUDIT.ORG, April 1, 2001, (Çevirimiçi) http://www.itaudit.org/index_search.htm,

Hare, C., "Digital Signatures: Electronic Handwriting", ITAUDIT.ORG, June15, 2001, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Hinson, G., "A Practical Model for Risk Assessment and Prioritization", ITAUDIT.ORG, April 1, 2000, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Hornby, A. S., Ruse, C., Oxford Student's Dictionary of Current English, Oxford University Press, Oxford, 1992

Horowitz, B., "Developing a Measurement System for E-business Security", ITAUDIT.ORG, July 1, 2000, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Horton, T. R., Legrand, C. H., Murray, W. H., Ozier, W. J., Parker B., "Managing Information Security Risks" ITAUDIT.ORG, August 15, 2000, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Hunter, B., "Information Security: Raising Awareness", ITAUDIT.ORG, September 15, 2000, (Çevirimiçi) http://www.itaudit.org/index_search.htm,

Information Systems Audit and Control Foundation, " IS Auditing Guideline: Planning.Document",(Çevirimiçi) http://www.isaca.org/standard/guide23.htm

Information Systems Audit and Control Foundation, "IS Auditing Guideline: Audit Documentation", (Çevirimiçi) http://www.isaca.org/standard/guide23.htm

IT Governance Institute, "The COBIT Framework Executive Summary" July, 2000, (Çevirimiçi) http://www.isaca.org

Jones, C., "Internet Security Software", ITAUDIT.ORG, April 1, 2001, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Le Grand, C.H., "Auditors on Guard Against Fraud" ITAUDIT.ORG, August 15, 2000, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Legrand, C. H., Ozier, W. J., "Information Security Management Elements : A Call to Action" ITAUDIT.ORG, March 1, 2000, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Legrand, C. H., Ozier, W. J., "Information Security Management and Assurannce : A Call to Action" ITAUDIT.ORG, January 15, 2000, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Lindquist, J. W., "Information Security Management, Engineering and Assurance" ITAUDIT.ORG, May 15, 2001, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Lindsedt, S., "Firewall Audit", ITAUDIT.ORG, June 15, 1999, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Loukis, E., Spinellis, D., "Information Systems Security in the Greek public sector" Information Management and Computer Security Journal, MCB University Press, England, 2001, pp. 21-31

Martin, D., "Risk Assessment When Auditing E-commerce Activities", ITAUDIT.ORG, February 1, 2000, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Moss, B., "Security Policy Checklist", 1997, (Çevirimiçi) http://queeg.com/~brion/security.html

O'Brien, J. A., "Introduction to Information Systems", Eighth Edition, USA, 1997

Oliphant, A., "Confidentiality and the Internal Auditor", ITAUDIT.ORG, December 1, 1998, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Oliphant ,A., "Taking the Helicopter View of Information Risks", 5 July 15, 2002 (Çevirimiçi) http://www.theiia.org/itaudit

Oliphant, A., "An Introduction to Computer Auditing- Part Deűx, No:7", ITAUDIT.ORG, January 15, 2000, (Çevirimiçi) http://www.itaudit.org/forum/newitauditor/f302na.htm

Oliphant, A., "Managing Information Security" ITAUDIT.ORG, March 1, 1999, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Olve, N.-G., Roy, J., Wetter, M., "Performance Drivers", John Wiley & Sons, West Sussex, England, 2000

Ozier, W., "A Framework for an Automated Risk Assessment Tool", ITAUDIT.ORG, August 15, 1999, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Ozier, W., "Information Risk Analysis, Assessment and Management", ITAUDIT.ORG, February 1, 2000, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Pathak, J.P., "IT Audit Approach, Internal Controls, and Audit Decisions of an IT Auditor", ITAUDIT.ORG, June 1, 2000, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Price, D., "A New Standart in Information Information Security Management" ITAUDIT.ORG, May 15, 1999, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Robertson, J. C., "Auditing", Irwin, Texas, 1996

Silltow, J., "Information Management (1)", ITAUDIT.ORG, March 15, 2001, (Çevirimiçi) http://www.itaudit.org/index_search.htm,

Silltow, J., "Software Management (9)", ITAUDIT.ORG, October 15, 2000, (Çevirimiçi) http://www.itaudit.org/index_search.htm

Swash, G.D., "The Information Audit" Journal of Managerial Psychology, MCB University Press, England, 1997, pp. 312-318

Uludağ, İ., Arıcan, E., Finansal Hizmetler Ekonomisi, Beta Yayınevi, İstanbul, 1999

Vallabhaneni, S. R., Internal Audit Process,SRV Professional Publications, Florida, 1998

Vallabhaneni, S. R., Management Control & Information Technology, SRV Professional Publications, Illinois, 1998

Vallabhaneni, S. Rao, Internal Audit Skills, SRV Professional Publications, Illinois, 1998,

Watne, D. A., Turney, P. B.B., Auditing EDP Systems, Prantice Hall, Inc., Second Edition, New Jersey, 1990

Weber, R., Information Systems Control and Audit, Prentice-Hall, Inc., New Jersey, 1998

Willson, J. D., Root, S. J., Internal Audit Manual, Warren, Gorham & Lamont, Inc., USA, 1989

Yu, J. W., "Cryptography-A Must for E-Commerce", ITAUDIT.ORG, January 15, 1999, (Çevirimiçi) http://www.itaudit.org/index_search.htm