T.C.

KIRIKKALE ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

ENDÜSTRİ MÜHENDİSLİĞİ ANABİLİM DALI

YÜKSEK LİSANS TEZİ

BİLGİ GÜVENLİĞİNİN SAĞLANMASINDA RİSK YÖNETİMİ: E-DEVLET KAPISI UYGULAMASI

ERHAN KUMAŞ

HAZİRAN 2009

Fen Bilimleri Enstitüsü Müdürünün Onayı.

Doç. Dr. Burak BİRGÖREN
Müdür

Bu tezin Yüksek Lisans tezi olarak Endüstri Mühendisliği Anabilim Dalı standartlarına uygun olduğunu onaylarım.

Doç. Dr. Burak BİRGÖREN
Anabilim Dalı Başkanı

Bu tezi okuduğumuzu ve Yüksek Lisans tezi olarak bütün gerekliliklerini yerine getirdiğini onaylarız.

Doç. Dr. Burak BİRGÖREN
Danışman

Jüri Üyeleri

Doç. Dr. Burak BİRGÖREN _____

Yrd. Doç. Dr. A. Kürşad TÜRKER _____

Yrd. Doç. Dr. Süleyman ERSÖZ _____

ÖZET

BİLGİ GÜVENLİĞİNİN SAĞLANMASINDA RİSK YÖNETİMİ: E-DEVLET KAPISI UYGULAMASI

KUMAŞ, Erhan

Kırıkkale Üniversitesi

Fen Bilimleri Enstitüsü

Endüstri Mühendisliği Anabilim Dalı, Yüksek Lisans Tezi

Danışman : Doç. Dr. Burak BİRGÖREN

Haziran 2009, 82 sayfa

E-Devlet Kapısı Projesi, Türkiye'nin devlet hizmetlerinin modernizasyonunu ve vatandaşların bu hizmetlere kolay ve rahat ulaşabilecekleri bir platformun kurulmasının hedeflendiği ön yüzünde vatandaşın tek noktadan devlet hizmetlerine ulaşabileceği, arka yüzünde ise kurumların birbirleri iletişim kurabilecekleri güvenli bir portal altyapısıdır. Bu noktada yönetilen bilginin güvenliğinin sağlanması, altyapı ile ilgili risklerin değerlendirilmesi ve yönetilmesi ile ilgili ulusal bir metodoloji ve yaklaşımın bulunmaması bu çalışmanın önemine vurgu yapmaktadır.

Bu tez çalışması, tamamlanmış risk analizi verileri için e-Devlet Kapısı Projesi çerçevesinde, ISO 27000 bilgi güvenliği standart ailesi ve diğer bilgi güvenliği, risk yönetimi model ve metodolojilerinin uygulamasını ele almaktadır. Bilimsel literatürün taranması, çalışmanın ilk adımını teşkil etmektedir. Ardından verilerin ISO 27000 bilgi güvenliği standartları ailesi ve diğer bilgi güvenliği, risk yönetimi model ve metodolojilerinden üretilen özgün modele uyumluluğunu test için kullanılan yöntemler incelenmektedir.

Anahtar Kelimeler: Bilgi Güvenliği, Risk Yönetimi, Risk Analizi, E-Devlet Kapısı Projesi.

ABSTRACT

RISK MANAGEMENT IN ENSURING INFORMATION SECURITY: E-GOVERNMENT GATEWAY CASE STUDY

KUMAS, Erhan

Kırıkkale University

Graduate School Of Natural and Applied Sciences

Deparment of Industrial Engineering, M. Sc. Thesis

Supervisor : Assoc. Prof. Dr. Burak BİRGÖREN

June 2009, 82 pages

E-Government project is a secure infrastructure with which modernization of Turkey is aimed. It is a platform where the citizens can easily reach the governmental services. At the same time public institutions can communicate with one another on the same platform. At this point, lack of a national methodology and an approach to maintaining the security of the information and evaluating and managing the risks of the substructure emphasize the importance of this study.

This thesis examines use of ISO 27000 information security management system standards group and other security models and methodologies' implementation progress. The first step is the survey of the

related scientific literature. Then, goodness-of-fit tests for ISO 27000 information security management system standards group and other security models and methodologies are analyzed.

Key Words: Information Security, Risk Management, Risk Analysis, E-Government Gateway Project.

TEŞEKKÜR

Tez konusunu bana öneren ve hazırlanması esnasında büyük bilgi birikimiyle yardımlarını esirgemeyen danışman hocam Sayın Doç. Dr. Burak BİRGÖREN'e, E-Devlet Projesi'nin değerli yöneticisi Sayın Dr. Ahmet KAPLAN'a, bugünlere gelmemde katkısı olan bütün hocalarıma, her türlü desteğinden dolayı sevgili eşime ve fedakarlıklarından dolayı aileme teşekkür etmeyi bir borç bilirim.

ÇİZELGELER DİZİNİ

ÇİZELGE

ŞEKİLLER DİZİNİ

ŞEKİL

İÇİNDEKİLER

1. GİRİŞ

Küreselleşme olgusunun gelişiminde önemli etkisi olan bilgi ve iletişim teknolojilerindeki yenilikler, ekonomik ve sosyal yaşamın her alanını ve toplumun tüm kesimlerini çeşitli yönlerden etkisi altına almakta; kamu yönetimi yaklaşımlarını, iş dünyasının iş yapma usullerini ve bireylerin yaşamlarını derinden etkilemekte, bir başka ifadeyle toplumsal bir dönüşüme neden olmaktadır. Yirmibirinci yüzyıla şimdiden damgasını vuran bu teknolojiler, yeni bir toplumsal dönüşüme yani "bilgi toplumu"na da zemin oluşturmaktadır(1).

Bilgi ve iletişim teknolojilerinde son yıllarda gözlenen gelişmeler, kamu yönetiminde yapısal bir dönüşüm ihtiyacını da gündeme getirmiştir. Kamu hizmetlerinin elektronik ortamda sunulması anlamına gelen e-devlet sayesinde halkın hizmete erişiminin daha hızlı ve daha ucuz olması beklenmektedir. Ancak, e-devlet olanaklarından azami ölçüde yararlanılması, kamu iş süreçlerinin vatandaşın bakış açısı ile yeniden tasarlanmasını ve kamu kurumlarının birlikte daha etkin ve verimli çalışabilirliğinin sağlanmasını gerektirmektedir. Bu çerçevede bu çalışmada, e-devletin gelişim süreci, etkin e-devlet hizmetinin anahtar unsurları olan entegrasyon ve paylaşım standartları ile, Türkiye'de 2005 yılından bu yana bu alanda yürütülmekte olan hazırlık çalışmaları ele alınmaktadır(2).

2000'li yıllardan itibaren sadece ülkemizde değil dünyada da bilgi toplumuna dönüşüm adına girişimlerin arttığı görülebilmektedir. Teknolojik

alanlardaki gelişmelere bağlı olarak sağlanan verimlilik artışları ve buna bağlı yeni ürün ve hizmetlerin hızla artması ulusal ve uluslar arası rekabetin kriterlerini de değiştirmeye başlamıştır.

Avrupa Birliğinin 2010 yılında dünyanın en rekabetçi ve dinamik bilgi tabanlı ekonomisi haline gelmesini amaçlayan Lizbon Stratejisi bu değişime uyum sağlamaya yönelik çabaların en kapsamlı örneklerinden biridir. Bu çerçevede hazırlanan eAvrupa 2002 Eylem Planı, yeni ve daha rafine hedefler içeren eAvrupa 2005 Eylem Planı ile devam etmiştir. 2005 yılında i2010 olarak güncellenen Lizbon Stratejisi; bilgi, yenilikçilik ve sosyal içerme başlıkları ile yeni hedeflere yönelmiştir. Türkiye'de bilgi toplumuna dönüşüm çalışmaları da bu gelişmelere paralel olarak 2000'li yılların başından itibaren yoğunluk kazanmaya başlamıştır. Türkiye, 2001 yılında AB'ye aday ülkeler için tasarlanan eAvrupa+ Girişimine taraf olmuştur(1).

Ülkemizde bu tarihe kadar kısmen de olsa kurumlar bünyesinde yürütülen münferit e-dönüşüm yada e-kurum çalışmaları, bir şemsiye altında toplanmış ve "e-Dönüşüm Türkiye Projesi" olarak yürütülmeye başlanmıştır. 2003/12 sayılı Başbakanlık Genelgesi ile amaçları, kurumsal yapısı ve uygulama esasları belirlenmiş olan e-Dönüşüm Türkiye Projesinin Kısa Dönem Eylem Planı 2003/48 sayılı Başbakanlık Genelgesi ile uygulamaya konulmuştur. Kısa Dönem Eylem Planının 40 numaralı "Kamu hizmetlerinin ortak platformda tek kapıdan (portal) sunumu ve sunulacak hizmetlerin geliştirilmesine yönelik stratejinin belirlenmesi" ve 41 numaralı "Kamu

hizmetlerinin geliştirilmesi ve ortak platformda sunumu için proje oluşturulması" eylemleri e-Devlet vizyonuna yönelik kilit adımlar arasındadır(3). Bu eylemler e-Devlet Kapısının kurulması ile gerçekleştirilmiş olacaktır. e-Devlet Kapısı teknik altyapısının kurulmasına yönelik iş ve işlemler ile bu amaçla tahsis edilmiş olan mali kaynaklarda dahil olmak üzere bütün hak ve sorumluluklar 20 Nisan 2006 tarih ve 2006/10316 sayılı Bakanlar kurulu kararnamesi çerçevesinde Türksat Uydu Haberleşme ve Kablo TV işletme Anonim Şirketi tarafından yürütülecektir(3).

Yukarıda da bahsedildiği üzere 2000'li yıllarda başlayarak yaşanan hızlı teknolojik gelişmeler, stratejik açılımlar ve internetin yaygınlaşmasının bir sonucu olarak bilgi güvenliği son yıllarda giderek önem kazanan bir konu haline gelmiştir. Bu durumun şu ana kadar olduğu gibi bundan sonra da önemini koruyan ve giderek artıran bir mevzu olması kaçınılmazdır. Kamu kurumları, özel sektör ve gerçek kişiler olarak bizleri oldukça yakında ilgilendiren bu konu, gereken önemin verilmeye başlandığı, ilgili önlemlerin alınmaya çalışıldığı bir döneme girmektedir. Ancak bilgi güvenliği sadece teknik ve teknolojik önlemlerle sağlanabilecek, olası risklerin ve tehlikelerin bertaraf edilebileceği bir alan değildir. "Gerek" şart olarak teknik ve teknolojik önlemler veya araçlar görülebilir ancak "yeter" şart kesinlikle "insan" olgusunu kapsayan tedbirler içermelidir; ancak böylelikle arzu edilen seviye yakalanabilir. Bilgi toplumu stratejisi içerisinde ve e-Dönüşüm Türkiye projesi çerçevesinde ulusal ve uluslararası kabul görmüş yol ve yöntemler, metod ve metodolojiler belirlenerek eyleme geçilmesi, uygulamaya yönelik adımlar atılması bilgi toplumuna dönüşümün ivme kazanmasını sağlayacaktır.

Bu çalışma içerisinde daha çok bilgi güvenliği ve risk yönetimi yaklaşımı çerçevesinde bilgiler verilecek olan e-Devlet Kapısı Projesi ile ilgili gelişmelerin paylaşımı yapılacaktır. E-Devlet Kapısının temelini çevrimiçi tek noktadan devlete erişim kavramı oluşturmaktadır. Bu kavram kamu hizmetleri kullanıcılarının (birey olarak vatandaşlar, özel şirketler ve sivil toplum örgütleri gibi kurumsal yapıların) kamu kesiminin fonksiyonel bölümlenmesine göre değil, kendi ihtiyaçlarına göre belirlenmiş "yaşam ve iş olaylarına" göre yapılandırılmış olarak hizmetlere erişebilmelerini içermektedir. Bu doğrultuda e-Devlet Kapısı, kamu kurumlarının fonksiyonlarının uyumunu sağlayacak, genişletilebilir, ölçeklenebilir ve kesintisiz olarak çevrimiçi çalışacak olan bir bilişim platformudur. Bu platformun güvenliğinin sağlanması da takdir edileceği üzere bütün ülke vatandaşlarına hitap eden bir altyapı olması nedeniyle oldukça önemlidir[(4)].

Bilgi güvenliği dünya genelinde benimsenmiş standartlara ya da modellere bağlı kalınarak yönetilmesi gereken bir süreçtir. Dünyada bilgi güvenliğinin yönetilmesi ile ilgili yapılan çalışmalar sonucunda 2009 yılında gelinen noktaya bakıldığında ISO–27001 standartlar ailesinin tüm dünya tarafından benimsendiği ve uygulamaya koymak için kurumlar tarafından çalışmalar yapıldığı görülmüştür. Ülkemizde bu konuda yapılan çalışmalar ve kurumların farkındalıkları yetersiz olduğundan bilgi güvenliği yönetimi konusunda büyük eksiklikler olduğu tespit edilmiştir. Çizelge 1.1 'de dünyada bilgi güvenliğinin sistemsel yaklaşımına verilen önem ve ülkemizin bu süreçteki yeri vurgulanmaktadır.

Çizelge 1.1. Ülkelere Göre ISO 27001 Sertifika Sayısı[5]

Japonya	2999*	Fransa	12	Umman	3
Hindistan	441	İzlanda	12	Peru	3
İngiltere	395	Pakistan	12	Portekiz	3
Tayvan	248	Filipinler	11	Vietnam	3
Çin	191	Singapur	11	Bangladeş	2
Almanya	124	Rusya	10	Kanada	2
Kore	89	Suudi Arabistan	10	İnsan Adası	2
ABD	86	Slovenya	9	Kazakistan	2
Çek Cumhuriyeti	71	İsveç	9	Morokko	2
Macaristan	64	Slovakya	6	Ukrayna	2
İtalya	59	Güney Afrika	6	Arjantin	1
Polonya	39	İsviçre	6	Ermenistan	1
İspanya	35	Bahreyn	5	Belçika	1
Hong Kong	31	Kolombiya	5	Kırgızistan	1
Avusturya	30	Gürcistan	5	Lübnan	1
Avusturalya	29	Endonezya	5	Litvanya	1
İrlanda	29	Kuveyt	5	Lüksemburg	1
Malezya	26	Bulgaristan	4	Makedonya	1
Brezilya	21	Gibraltar	4	Belarus	1
Tayland	21	Norveç	4	Moritanya	1
Meksika	20	Katar	4	Moldova	1
Birleşik Arap Emirlikleri	18	Sri Lanka	4	Yeni Zelanda	1
Türkiye	**18**	Şili	3	Uruguay	1
Yunanistan	15	Mısır	3	Yemen	1
Romanya	15	İran	3	**Genel Toplam**	**5314**
Hollanda	13	Macau	3		

Değerlendirmeye alınmış toplam 79 ülke içerisinde belge almış 18 özel ve kamu tüzel kişiliği ile dünya genelinde 24'üncü sırada olmamız bilgi güvenliğine verdiğimiz önem açısından manidardır.

Tez çalışması dört bölümden oluşmaktadır. Birinci bölümde öncelikle, güvenlik kavramının tanımı ve önemi açıklandıktan sonra, analizlerin temelini oluşturan güvenlik, risk yönetimi, risk analizi, e-devlet kapısı projesi ele alınmıştır. Detaylar ile ilgili bilgiler ilerleyen bölümlerde ayrıca aktarılmıştır.

İkinci bölüm'de, bilgi güvenliği kavramı, tehdit, açıklık, risk gibi kavramsal bilgiler verilmiş, güvenlik prensipleri, bilgi güvenliği ve risk yönetimi sistem yaklaşımı, risk yönetimi ve değerlendirme metodolojisi hakkında açıklamalar yapılmıştır. Ayrıca çalışmanın temelini oluşturan ISO 27000 bilgi güvenliği standart ailesinin e-devlet kapısı projesi çalışmalarındaki önem ve avantajlarından bahsedilmiş ve bu alanda yapılan çalışmalarda diğer modellere olan üstünlüklerine değinilmiştir. Risk analizi sürecinde yapılan çalışmalar detaylı olarak aktarılmış, literatür bağlamı sunulmuştur.

Üçüncü bölümde, uygulanan yöntem neticesinde elde edilen sonuçlar sunulmuş ve bunlarla ilgili değerlendirmeler yapılmıştır. Ayrıca geliştirilen yöntemle ortaya çıkan sonuçlar detaylı şekilde yorumlanmıştır.

Son bölümde ise çalışmada elde edilen bulguların yorumlanması, yaşanan sorunlar ve çeşitli karşılaştırmalar verilmiştir.

2. MATERYAL VE YÖNTEM

Bilgi; doğru karar vermede, geleceğe yönelik tahminlerde bulunmada, sağlıklı iletişimin gerçekleşmesinde, standart bir ürün/hizmet gerçekleştirmede, var olan problemlerin çözümlenmesinde ve olabilecek problemlere çözüm bulunmasında kullanılan bir araçtır[6]. Alvin Toffler gelecekte "cahil" olarak tanımlanacak kişilerin "okuma yazma bilmeyen" değil "bilgiye nasıl ulaşacaklarını bilmeyenler" olduklarını ifade etmiştir[7].

Bilginin organizasyonu, iletimi ve kullanılması, bilgi sistemlerinin doğmasına neden olmuştur. Günümüzde "Yönetim Bilgi Sistemleri" ve "Karar Destek Sistemleri" gibi sistemler her türlü organizasyonun bilgi akış ve yönetiminde yer almaktadır. Bilgi iletişim teknolojilerindeki gelişmelerin en önemli etkisi bilgi kavramı üzerinde olmuş ve bilgi ekonomik bir varlık olarak görülmeye başlamıştır. Organizasyonlarda bilgi yönetimi fonksiyonu bilgiden maksimum düzeyde katma değer yaratmayı sağlayacak süreç ve teknikleri içermektedir. Bu noktada üretilen bilginin, anlamlandırılması, saklanabilmesi ve güvenliğinin sağlanabilmesi önem arz etmektedir.

İkinci bölümde; bilgi güvenliği kavramı, bu süreçte karşılaşılan tehditler, açıklıklar, riskler, güvenlik prensipleri, sistemsel yaklaşımı, risk yönetimi ve değerlendirme metodolojisinin irdelenmesi söz konusu olacaktır.

2.1. Bilgi Güvenliği Kavramı

Bilgi güvenliği kavramı; bilginin gizliliği, bütünlüğü ve kullanılabilirliğinin korunmasıdır. Ek olarak, doğruluk, açıklanabilirlik, inkar edememe ve güvenilirlik gibi diğer özellikleri de kapsar. Bilgi güvenliği yönetim sistemi ise bilgi varlıklarını koruyan ve ilgili taraflara güven veren yeterli ve orantılı güvenlik kontrollerini sağlamak için tasarlanmış yapıdır[(8)].

1990'lı yıllarda yaşanan dünyadaki hızlı teknolojik gelişmelerin bir sonucu olarak bilgisayarlar, modern hayatın her alanına girmiş ve vazgeçilmez bir biçimde kullanılmaya başlanmıştır. Hayatımızın birçok alanında bilgisayar ve bilgisayar ağı teknolojileri "olmazsa olmaz" bir şekilde yer almaktadır. İletişim, para transferleri, kamu hizmetleri, askeri sistemler, elektronik bankacılık, savunma sistemleri, bu alanlardan sadece birkaçıdır. Teknolojideki bu gelişmeler, bilgisayar ağlarını ve sistemlerini, aynı zamanda, bir saldırı aracı haline, kullandığımız sistemleri de açık birer hedef haline getirmiştir[(9)].

Bilgi ve iletişim teknolojilerinin kullanıldığı sistemlere ve bu sistemler tarafından işlenen verilere yönelik güvenlik ihlalleri inanılmaz bir hızla artmaktadır. Bilgi ve iletişim teknolojilerinin kullanıldığı sistemlere olan bireysel ve toplumsal bağımlılığımız arttıkça bu sistemlerde meydana gelebilecek arıza ve saldırılara karşı duyarlılığımızın da o denli artması beklenmektedir. Bu duyarlılık arttıkça da bilgisayar sistemlerine ve ağlarına yönelik olarak gerçekleştirilecek olan saldırıların sonucunda; para, zaman, prestij ve değerli bilgi kaybı da artacaktır. Bilgi güvenliği konusunun, ilerleyen

yıllarda da bilgi ve iletişim teknolojileri sektöründe giderek artan bir öneme sahip olacağı bilinmektedir. Bilgi güvenliği kavramı ile birlikte ve tamamlayıcı nitelikte risk yönetiminin de projelerin, şirket ve kurumların karar verici noktasında bulunan yöneticilere dayanak noktası olması beklenmektedir. Bilgi güvenliğinin sağlanmasıyla değer odaklı karar verebilmeyi kolaylaştırıcı ve fayda-maliyet dengesini gözeterek yöneticilere katma değer sunabilen veriler sağlanabilmektedir(10).

İletişim ortamlarının yaygınlaşması ve kullanımının artması sonucunda elektronik ortamlarda bulunan bilgilerin her iki ayda neredeyse iki kat artmasından dolayı bilgi güvenliğinin sağlanması ihtiyacı kişisel veya kurumsal olarak en üst seviyelere çıkmıştır. Bunun önemli sebepleri iş veya günlük yaşamın bir parçası haline gelen elektronik uygulamaların artması, ihtiyaç duyulan bilgilerin ağ sistemleri üzerinde paylaşımı, bilgiye her noktadan erişilebilirlik, bu ortamlarda meydana gelen açıkların büyük tehdit oluşturması ve en önemlisi kişisel ve kurumsal kayıplarda meydana gelen artışlar olarak sıralanabilir. Ülkemizde konsolide e-hizmetlerin tek portaldan verilmeye başlanması konusunda yürütülen çalışmalarda sona gelinmiş ve Aralık 2008 tarihinde e-devlet kapısı www.turkiye.gov.tr adresi üzerinden kamuoyuna açılmıştır. Böylelikle her gün karşılaştığımız pasaport başvurusu, fatura ödemeleri, bilet kuyruğu, emekli maaşı kuyruğu, e-borcu yoktur belgesi ve daha birçok resmi ya da gayri resmi evrak alma, bilgi alma gibi faaliyetler artık entegre bir altyapı üzerinden sağlanabilecektir. Böylelikle önceden görece daha az karşılaştığımız e-hizmet yapısı artık daha fazla önümüze çıkacaktır. Bu durum elektronik ortamda yapılan güvenlik ihlâllerini hemen

hemen her gün karşımıza çıkaracaktır. Böyle bir durumdan elektronik ortamda hizmet veren kuruluşlar da hizmet alan kullanıcılar da etkilenebilecektir. Örneğin internet bankacılığı yapan kullanıcılar dolandırıldığı zaman; parasını kaybederken, o hizmeti sağlayan banka ise müşterilerinin gözünde güven kaybına uğrayarak ticari itibarını kaybetme tehlikesiyle karşı karşıya kalmaktadır. Bu çalışmaya konu olan e-devlet kapısı için bir örnek verilecek olursa; ülkemizin tüm sathına hizmet verecek olan bu altyapı üzerinden kamu kurumları, işletmeler ve tüm vatandaşlar işlerini yapabileceklerdir. Bu durumda e-devlet kapısı üzerinde işlem yapılırken ortaya çıkan bir güvenlik ihlali sadece ilgili vatandaşı değil, ilgili kamu kurumunu ve hatta bazen ülkenin imajını zedeleyebilecektir. Bu ve buna benzer tehditlerden etkilenmeyi en aza indirmek için kurumlara, kuruluşlara ve kullanıcılara düşen önemli görevler vardır. Kullanıcıların bilgi güvenliği konusunda bilinçli olmaları gerekirken, kurumların bilgi güvenliği konusunda kurumsal önlemler almaları ise mutlaka yapılması gereken görevler arasındadır[(9)].

2.2. Tehditler

E-Devlet Kapısı Projesi bünyesinde yapılan çalışmalar daha önce de bahsedildiği gibi ülke vatandaşlarının tamamının bireysel ve kurumsal güvenliğini ilgilendirdiği için yapılabilecek hataların oldukça önemli sonuçlar doğuracağı kesindir. Tehdit, bir sistemin veya kurumun zarar görmesine neden olan istenmeyen bir olayın arkasındaki gizli neden, olarak tanımlanabilir. Her tehdidin bir kaynağı ve bu kaynağın yararlandığı sistemdeki bir “güvenlik boşluğu” vardır. “Sistemi neye karşı korumalıyım?”

sorusuna verilecek cevap bir sisteme yönelik olan tehditleri belirlemekte yardımcı olacaktır. Tehditler, tehdit kaynağı açısından bakıldığında iki gruba ayrılarak incelenebilir:

- *İnsan Kaynaklı Tehditler;* Bu tür tehditleri de kendi içinde iki alt gruba ayırabiliriz:
    - Kötü Niyet Olmayan Davranışlar sonucu oluşanlar; bir kullanıcının sistemi bilinçsizce, yeterli eğitime sahip olmadan kullanması neticesinde sistem genelinde ortaya çıkması muhtemel sorunlardır.
    - Kötü Niyetli Davranışlar sonucu oluşanlar; sisteme zarar verme amacıyla ve sisteme yönelik olarak yapılan kötü niyetli davranışların neticesinde ortaya çıkması muhtemel sorunlardır. Bu tip tehditlerde, tehdit kaynağı sistemde bulunan açıklıklardan ve güvenlik boşluklarından faydalanmaktadır.
- *İnsan Kaynaklı Olmayan Tehditler;* bu tür tehditler genellikle önceden tespit edilemezler ve meydana gelmelerinin engellenmesi büyük olasılıkla zor olur. Deprem, yangın, su baskını, network altyapısının çökmesi gibi örnekler verilebilir.

Tehditin geliş yönüne göre de sınıflandırma yapılabilir. Buna göre iç tehditler, kurum içinden kuruma yönelik yapılabilecek saldırılar, dış tehditler ise kurum dışından kuruma yönelik olarak yapılabilecek saldırılar olarak tanımlanır.

2.3. Açıklıklar (Vulnerability)

Açıklıklar (Vulnerability), sistem üzerindeki yazılım ve donanımdan kaynaklanan, sistemin işletim kuralları ve/veya yönergelerindeki açık noktalar ve zayıf kalmış yönlerdir. Bir güvenlik boşluğu ya da açıklık sayesinde bir kişi, sistemdeki bilgisayarlara ya da bilgisayar ağı üzerindeki kaynaklara yetkisiz olarak erişebilir. Bir sunucu bilgisayar üzerinde çalışan bir hizmet (örneğin web sunucusu ya da e-posta alma/gönderme hizmeti), modem üzerinden içeri doğru sınırlandırılmamış arama hizmeti, bir güvenlik duvarı üzerinde açık unutulmuş bir erişim noktası (port), sunucu bilgisayarların bulunduğu odaya çıkışlarda denetim eksikliği ve sunucular üzerinde belli bir politikaya dayandırılmadan belirlenen parolalar, güvenlik boşluklarına örnek olarak verilebilirler. Yazılım ya da donanımdan kaynaklanan açıklıklar, program üreticisi ya da başka bir kaynak tarafından geliştirilen bir “yama program” yardımıyla kapatılmalı ve eldeki yazılım ve donanımların üreticilerinin yayınladığı yama listeleri sürekli olarak takip edilmelidir ve çıkan yamalar vakit geçirilmeden sisteme uygulanmalıdır.

2.4. Riskler

Bir tehdit kaynağının, bir sistemdeki güvenlik açıklıklarından yararlanarak sisteme yetkisiz erişimde bulunması olasılığı, bu tehdidin riski olarak ifade edilir. Tehdit kaynaklarının ya da güvenlik boşluklarının azaltılması, tehdide ait riskleri de aynı oranlarda azaltacaktır. Risklerin tespit edilmesi ve değerlendirilmesi çalışmaları içerisinde geniş bir alanı tutan risk analizi; sistem kaynaklarını etkileyebilecek belirsiz olayların belirlenmesi,

denetlenmesi, yok edilmesi ya da en aza indirgenmesini kapsayan süreç olarak tanımlandığı gibi, fayda-maliyet analizi, seçim, önceliklendirme, gerçekleştirim, sınama, önlemlerin güvenlik değerlendirmesi gibi komple güvenlik gözden geçirmesini de içerebilir[11].

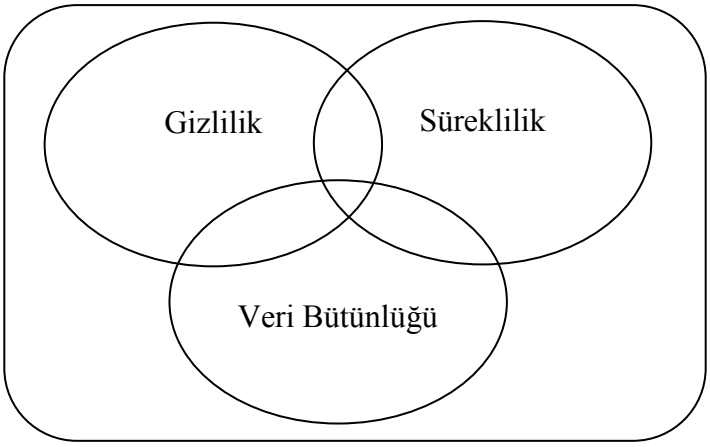
Çizelge 2.1'de e-Devlet Kapısı Projesi çerçevesinde yapılmış risk analizinden alınmış tehdit kaynağı – açıklık - risk ilişkisine örnekler verilmiştir.

Çizelge 2.1. Risk Analizi Çalışmasından Örnekler

Tehdit Kaynağı	Açıklık	Oluşabilecek Risk
Ekipman arızası nedeniyle bağlantının kesilmesi	*Ekipmanların yedekli çalışması sürekli olarak test edilmemektedir.*	*İnternet bağlantısının kesilmesi*
Doğal afetler nedeniyle bağlantının kesilmesi	*Telekom altyapısının doğal afetlere karşı korumasız olması*	*İnternet bağlantısının kesilmesi*
Yerel ağda yayılan bir solucanın ağı satüre etmesi nedeniyle bağlantının kesilmesi	*Anti-virüs yazılımlarının tanımadığı yeni virüslere karşı uçsistem koruması bulunmaması*	*Kurum Bağlantılarının kesilmesi*
Sistemin yada programın hatalı güncelleştirme nedeniyle kullanılamaz duruma gelmesi	*Güncelleştirmelerin öncesinde test yapılmaması*	*E-posta Sunucusu'nun tehlikeye girmesi*

2.5. Güvenlik Prensipleri

Bilgi güvenliğinin birçok alanı olmakla birlikte temelde üç prensipten bahsetmek gerekir diyebiliriz. Bu prensipler, ilerleyen bölümlerde standart ve metodolojilerden bahsederken detaylarına girilecek olan CobIT metodolojisi içerisinde verilen ve şekil 2.1.'de özetlenen; gizlilik, veri bütünlüğü ve süreklilik prensipleridir. Bu prensipler aynı zamanda ISO 27001:2005 bilgi güvenliği yönetim sistemi standardı çerçevesinde de kullanılmaktadır.



Şekil 2.1. Temel Güvenlik Prensipleri

2.5.1. Gizlilik (Confidentiality)

Bilginin yetkisiz kişiler, varlıklar ya da proseslere kullanılabilir yapılmama ya da açıklanmama özelliğidir[(11)]. Bilginin yetkisiz kişilerin eline geçmesinin engellenmesi de denilebilir. Gizlilik, hem kalıcı ortamlarda (disk, teyp, vb.) saklı bulunan veriler hem de ağ üzerinde bir göndericiden bir alıcıya gönderilen veriler için söz konusudur. Saldırganlar, yetkileri olmayan verilere birçok yolla erişebilirler: Parola dosyalarının çalınması, sosyal

mühendislik, bilgisayar başında çalışan bir kullanıcının, ona fark ettirmeden özel bir bilgisini ele geçirme (parolasını girerken gözetleme gibi). Bunun yanında trafik analizinin, yani hangi gönderici ile hangi alıcı arası haberleşmenin olduğunun belirlenmesine karşı alınan önlemler de gizlilik hizmeti çerçevesinde değerlendirilir.

2.5.2. Veri Bütünlüğü (Data Integrity)

Varlıkların doğruluğunu ve tamlığını koruma özelliğidir. Başka bir tabirle; veriyi göndericiden çıktığı haliyle alıcısına ulaştırmaktır. Bu durumda veri, haberleşme sırasında izlediği yollarda değiştirilmemiş, araya yeni veriler eklenmemiş, belli bir kısmı ya da tamamı tekrar edilmemiş ve sırası değiştirilmemiş şekilde alıcısına ulaşır. Bu hizmeti, geri dönüşümü olan ve olmayan şekilde verebiliriz. Şöyle ki; alıcıda iki tür bütünlük sınaması yapılabilir: bozulma sınaması ya da düzeltme sınaması. Bozulma sınaması ile verinin göndericiden alıcıya ulaştırılması sırasında değiştirilip değiştirilmediğinin sezilmesi hedeflenir. Düzeltme sınamasında ise, bozulma sınamasına ek olarak eğer veride değişiklik sezildiyse bunu göndericiden çıktığı haline döndürmek hedeflenir.

2.5.3. Süreklilik (Availability)

Bilgi ve iletişim sistemleri, kendilerinden beklenen işleri gerçekleştirirken, hedeflenen bir performans vardır. Bu performans sayesinde müşteri memnuniyeti artar, e-iş'e geçiş süreci hızlanır. Süreklilik hizmeti, bilgi ve iletişim teknolojileri sistemlerini, kurum içinden ve dışından gelebilecek

performans düşürücü tehditlere karşı korumayı hedefler. Bu durum e-Devlet Kapısı Projesi bünyesinde değerlendirildiğinde 7/24 kesintisiz hizmet sağlanması hedeflenmektedir. Süreklilik hizmeti sayesinde; kullanıcılar, erişim yetkileri dahilinde olan verilere, veri tazeliğini yitirmeden, zamanında ve güvenilir bir şekilde ulaşabilirler. Sistem sürekliliği, yalnızca kötü amaçlı bir "hacker"ın (Bilgisayar ve haberleşme teknolojileri konusunda bilgi sahibi olan, bilgisayar programlama alanında standardın üzerinde beceriye sahip bulunan ve böylece ileri düzeyde yazılımlar geliştiren kişi), sistem performansını düşürmeye yönelik bir saldırısı sonucu zedelenmez. Bilgisayar yazılımlarındaki hatalar, sistemin yanlış, bilinçsiz ve eğitimsiz personel tarafından kullanılması, ortam şartlarındaki değişimler (nem, ısı, deprem) gibi faktörler de sistem sürekliliğini etkileyebilir.

2.5.4. İzlenebilirlik (Accountibility)

Sistemde gerçekleşen olayları, daha sonra analiz edilmek üzere kayıt altına almaktır. Neredeyse tüm yönetim sistemlerinin "izlenebilirlik" özelinde amacı, faaliyetleri kayıt altına alarak, oluşabilecek vakalarda problemin 5N1K (Ne, Nerede, Nasıl, Ne zaman, Neden, Kim) prensibine göre sorgulanabilmesinin sağlanmasıdır. Bahsi geçen prensip ile ilgili tüm yönetim sistemlerinde gerçekleşmesi ve uygulamada görülmesi arzu edilen bir prensiptir. Burada olay dendiğinde, bilgisayar sistemi ya da ağı üzerinde olan herhangi bir faaliyeti anlayabiliriz. Bir sistemde olabilecek olaylara, kullanıcının parolasını yazarak sisteme girmesi, bir web sayfasına bağlanmak, e-posta almak, göndermek ya da msn ile mesaj yollamak gibi

örnekler verilebilir. Toplanan olay kayıtları üzerinde yapılacak analiz sonucunda, bilinen saldırı türlerinin görüntülerine rastlanırsa ya da istatistiksel teknikler veya yapay zeka teknikleri kullanılarak daha önce rastlanmayan ve saldırı olasılığı yüksek bir aktivite tespit edilirse alarm mesajları üretilerek sistem yöneticileri uyarılır. E-Devlet Kapısı projesi bünyesinde insan kaynaklı oluşabilecek ve/veya kullanıcı kaynaklı oluşabilecek hataların geçmişe doğru taranarak tespit edilmesi, vatandaşların projeye olan güveni açısından oldukça önemlidir. Aynı şekilde bu durumun devletin bilgi toplumuna geçişinde elektronik hizmetlerin kullanılmasını da doğrudan etkilemesi kaçınılmazdır.

2.5.5. Kimlik Doğrulama (Authentication)

E-Devlet kapısı özelinde değerlendirildiğinde değerli bir kaynağa, yalnızca ona erişmeye hakkı olanlara erişim yetkisi verilmesi gerekmektedir. Bu erişim yetkisinin denetimi sırasında kullanıcılardan iki tür bilgi istenecektir. Birinci bilgi herkesin bildiği kullanıcıya ait, kullanıcının T.C Kimlik Numarası gibi bir kimlik bilgisi, diğer bilgi ise kullanıcının yani vatandaşın şahsına ait sistemde belirleyeceği parola bilgisidir. Bahsi geçen bu iki bilgiyi vatandaş sisteme girdiğinde vatandaş bazlı tanımlama gerçekleştirilmiş olacaktır. Kimlik doğrulama bir kişinin tanımlama aşamasında üretilen kimliğe sahip kişi olduğunun tespit edilmesidir. Bu ispat bir parola, bir akıllı kartın kullanımı, tek seferlik parola (one-time password), bir sayısal imza bilgisi, biyometrik bir özelliğin belirlenmesi şeklinde karşımıza çıkabilmektedir. Giriş parolası en yaygın karşımıza çıkan kimlik doğrulama biçimidir. Kullanım kolaylığına

karşın, başkalarının eline geçmesi kolay olduğundan güvenlik boşluğu oluşturmaya aday bir yöntemdir. Bununla birlikte e-Devlet Kapısı Projesinde uygulayacağımız bu yöntem üzerinde uyulacak birkaç basit kural, vatandaşın parolasının başkalarının eline geçmesini engelleyebilecektir. Ağ güvenliği açısından kimlik doğrulama; alıcının, göndericinin iddia ettiği kişi olduğundan emin olmasıdır. Yani e-Devlet Kapısında elektronik kamu hizmeti almak isteyen kullanıcı ya da vatandaşın gerçekten sisteme giriş yapan kişinin kendisi olup olmadığının tespitine yarayan bir metodtur. Bunun yanında, bir bilgisayar programını kullanırken bir parola girmek de kimlik doğrulaması çerçevesinde değerlendirilebilir. Günümüzde kimlik doğrulaması, sadece bilgisayar ağları ve sistemleri için değil, fiziksel sistemler için de çok önemli bir hizmet haline gelmiştir. Akıllı karta ya da biyometrik teknolojilere dayalı kimlik doğrulama teknikleri de bulunmaktadır.

2.5.6. Güvenilirlik (Reliability)

Sistemin beklenen davranışı ile elde edilen sonuçlar arasındaki tutarlılık durumudur. Başka bir ifade ile güvenilirlik, sistemden ne yapmasını bekliyorsak, sistemin de eksik ve fazla olmadan bunu yapması ve her çalıştırıldığında da aynı şekilde davranması olarak tanımlanabilir.

2.5.7. İnkar Edememe (Non-Repudiation)

Bu hizmet sayesinde, ne gönderici alıcıya bir mesajı gönderdiğini, ne de alıcı göndericiden bir mesajı aldığını inkâr edebilir. Bu hizmet, özellikle gerçek zamanlı işlem gerektiren finansal sistemlerde, banka sistemlerinde ve

e-Devlet kapısı üzerinden alınabilecek elektronik ödeme hizmetlerinde kullanım alanı bulabilecektir ve gönderici ile alıcı arasında ortaya çıkabilecek anlaşmazlıkların en aza indirilmesini sağlamaya yardımcı olmaktadır. Bu hizmetler, zaman içinde bilgisayar sistemlerine karşı ortaya çıkmış tehditler ve yaşanmış olaylar sonucunda ortaya konmuştur. Yani her bir hizmet, belli bir grup potansiyel tehdide karşı sistemi korumaya yöneliktir, denilebilir.

2.6. Sistemsel Yaklaşım

Yirmibirinci yüzyıla şimdiden damgasını vuran bilgi ve iletişim teknolojileri, yeni bir toplumsal dönüşüme yani "bilgi toplumu"na da zemin oluşturmaktadır. Bilgi toplumuna dönüşümdeki en önemli konu ise bilginin üretilmesi, üretilen bilginin yönetilebilmesi ve güvenliğinin sağlanabilmesi olarak değerlendirebiliriz. Bu noktada uzun vadeli projelerin desteklenmesi, ülkemizin bürokratik devletten elektronik devlete geçebilmesinin temel şartı olarak görülmektedir[12].

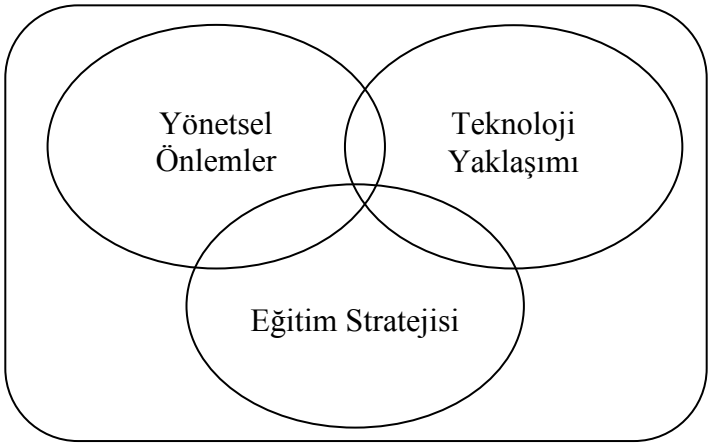
Bu dönüşüm sırasında; bilgi güvenliğinin sağlanmasında risk yönetimi sürecinde sistemsel yaklaşım; risklerin tanımlanması, tahmin edilmesi, değerlendirilmesi, bilgi teknolojileri varlıklarının ve bu varlıklara ait açıklıkların ve olası zafiyetlerin ortaya çıkarılması açısından çok önemlidir[13]. Başka bir noktadan konuya bakıldığında risk yönetimi; proje yönetimi ve e-dönüşüm gibi süreçlerin başarıyla sonuca ulaşmasında oldukça fayda sağlamaktadır. Projeyi veya süreci başarıya götürecek alternatif çözümlerin tespit edilmesinde, proje hedeflerine ulaşma olasılığını artırmada, başarı kriterlerini

belirlemede, karşılaşılabilecek sürprizleri ortadan kaldırmada, varsayımları tespit etmede, mükerrer iş yaparak maliyetlerin artmasını engellemede oldukça faydalı olduğu kabul görmüştür[14]. Küreselleşme olgusunun gelişiminde önemli etkisi olan bilgi ve iletişim teknolojilerindeki yenilikler, etkin risk yönetimi, ekonomik ve sosyal yaşamın her alanını ve toplumun tüm kesimlerini çeşitli yönlerden etkisi altına almakta; iş dünyasının iş yapma usullerini ve bireylerin yaşamlarını derinden etkilemekte, bir başka ifadeyle toplumsal bir dönüşüme neden olmaktadır. Türkiye'de profesyonel olarak kabul görmüş kişilerin deneyimini kullanarak bilgi güvenliği sürecinin değişik parçalarını tamamlayacak şekilde süreç içerisinde çapraz kontrol (cross-check) mekanizmasını da kullanarak sistemsel bir yaklaşım ile e-Devlet Kapısı Projesi'ne güvenlik şemsiyesi giydirilmesi öngörülmüştür.

2.6.1. Bilgi Güvenliği Proses Yaklaşımı

Bir kuruluş içerisinde, proseslerin tanımları, bunların etkileşimi ve yönetimleriyle birlikte proseslerin oluşturduğu bir sistem uygulaması "proses yaklaşımı" olarak tanımlanabilir. Güçlü bir güvenlik altyapısı kurabilmek için aşağıda bahsedilecek olan üç parçayı birbiri ile bütünleştirmek ve hepsini birlikte bütünsel bir proses yaklaşımıyla ele almak gerekir. Bu bahsedilen süreç alanlarının içinde, bilgi güvenliği teknolojilerinin dışında kalan farklı alanlar da bulunmaktadır. Bir kurumun, kurumsal bilgi güvenliğini sağlamak amacıyla, sadece bilişim teknolojilerini devreye sokarak başarıya ulaşma şansı oldukça azdır. Bu noktada insan faktörü oldukça öne çıkmaktadır. Zira istatistiklerde en fazla güvenlik problemlerinin kullanıcı hatalarından ya da

zafiyetlerinden kaynaklandığı ortaya koyulmuştur ki; e-Devlet Kapısı projesi bünyesinde yapılan risk analizinde de bu ortaya koyulmuştur. En fazla dikkat edilmesi gereken konulardan birisi olan eğitim konusunun altı çizilmiştir.



Şekil 2.2. Bilgi Güvenliği'nin Üç Temel Süreç Alanı

Bilgi güvenliğinin sağlanması amacıyla üç temel süreç alanı üzerinden hareket edilebilir; bu alanlar Şekil 2.2.'de gösterildiği gibi yönetsel önlemler, teknoloji açılımı ve eğitim stratejisi şeklinde ifade edilebilir. Bütün bunlara ek olarak, bu üç süreç alanından her biri, başarıya ulaşmak için diğer iki süreç alanının tam ve eksiksiz çalışıyor olmasına ihtiyaç duyar. Bu üç alan birbirileri ile ayrılmaz ve sıkı bağlara sahiptir. Birlikte çalışmalarından oluşacak sinerji, kuruma bilgi güvenliği yönünden tehdit oluşturacak tüm etkenlere karşı güçlü bir kalkan görevini üstlenecektir.

Yönetsel Önlemler, güvenlik yönetimi ile ilgili bir dizi kuralın ortaya koyulması ve uygulanması şeklinde özetlenebilir. Hemen her konuda olduğu gibi, bilgi güvenliğinin yönetiminde de başarı; iyi bir planlama ve üst düzey

politikaların doğru ve tutarlı bir şekilde belirlenmesi ile elde edilebilir. Bunun ardından, belirlenenlerin yazıya dökülmesi, yani prosedür, yönerge ve talimatlar gibi dokümanların oluşturulması gelmelidir.

Günümüzde basında ve haber bültenlerinde çok yüksek maddi kayıplara yol açan virüsleri, bilgisayar ağlarına yönelik saldırılardan zarar gören şirketleri konu alan haberler sıkça yer almaktadır. Bununla birlikte, bir sistem yöneticisinin ve güvenlik uzmanının uğraştığı işlerin, her zaman gazete haberlerinde çıkanlarla sınırlı olduğu düşünülmemelidir. Bunlar dışında, günlük ya da periyodik olarak gerçekleştirilecek bir takım işler vardır ki işte yönetsel önlemler, bu tür işleri kapsayan ve tanımlayan bir süreç alanıdır. Bu süreç alanını oluşturan;

- Risk Yönetimi
- Güvenlik Politikaları
- Standartlar ve Metodolojiler
- Denetim Süreci

gibi alt süreçler de bulunmaktadır. Bu konular ilerleyen bölümlerde detaylandırılacaktır. Yönetsel önlemlerle ortaya konulan kurumun güvenlik ihtiyaçlarının karşılanmasında, teknolojik uygulamalardan ve teknolojik açılımlardan da faydalanılır. Günümüzde bir bilgisayar ağına ya da tek başına bir bilgisayara yapılacak bir saldırının sonuçlanması saniyelerle ifade edilen çok kısa bir süre içinde oluşur. Bu tür saldırılara, ancak teknolojik bir takım önlemler ile karşı konulabilir.

2.6.2. Bilgi Güvenliği ve Teknoloji Açılımı

Bilgi güvenliğinin sağlanmasında kullanılan teknolojilerden bazıları aşağıdaki listede verilmiştir. Güvenlik uygulamalarının bütünü kesinlikle bunlarla sınırlı değildir. Burada en fazla kullanıldığı düşünülen ve en popüler olan teknolojilerden bahsedilmiştir. Bunlar;

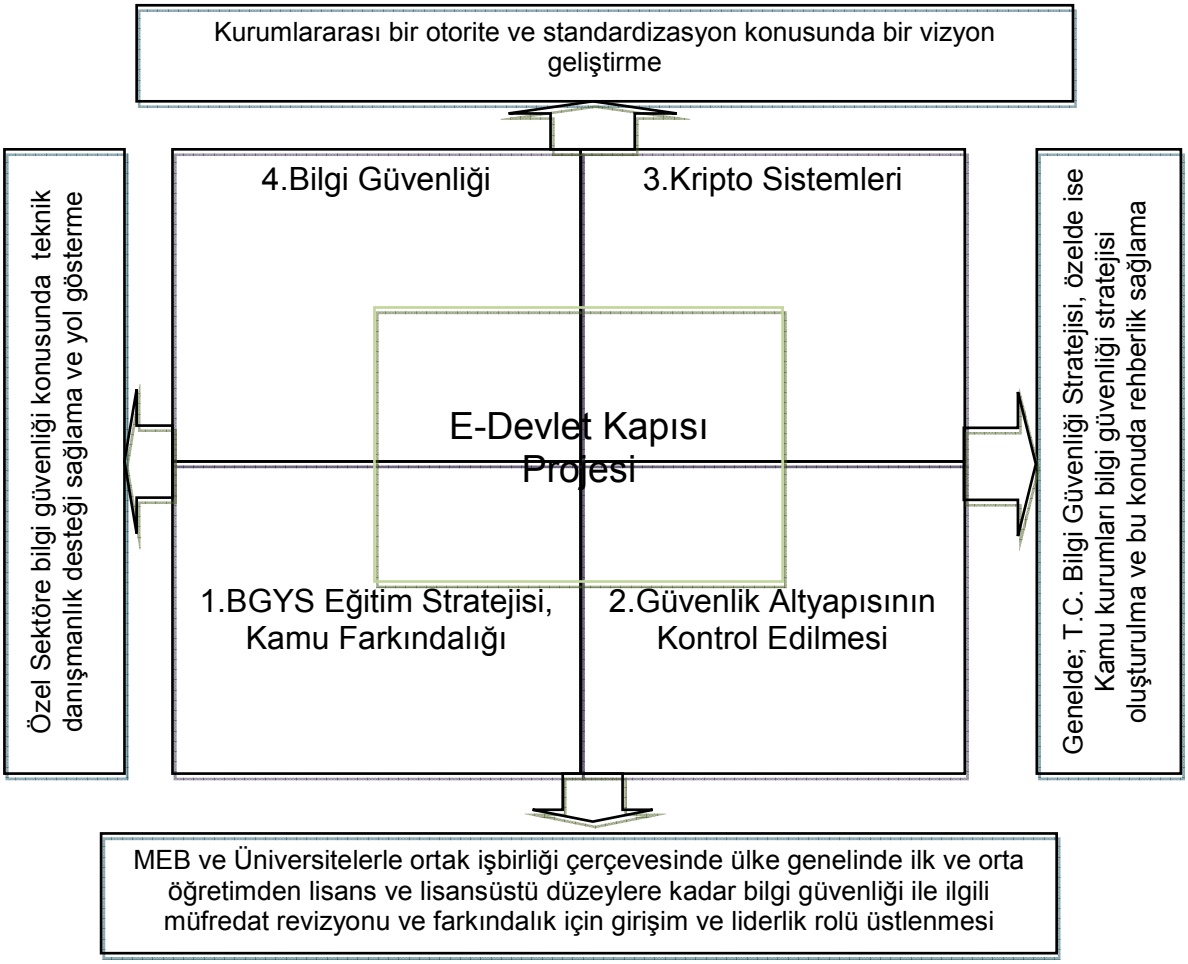
- Kriptografi
    - Simetrik ve Asimetrik Algoritmalar,
    - Özetleme Fonksiyonları,
    - Sayısal İmza ve PKI (Public Key Infrastructure) Altyapısı,
- Ağ Yönetimi ve Güvenlik Duvarları
- Yedekleme ve Felaket Kurtarma Merkezleri
- Erişim Denetimi
    - Tanımlama (Identification),
    - Kimlik Doğrulama (Authentication),
    - Yetkilendirme (Authorization),
- Saldırı Tespit ve Önleme Sistemleri
- Uygulama Güvenliği Yazılımları
- Penetrasyon Testleri, Olay Müdaheleleri, Ağ Analizleri

şeklinde sıralanabilir.

2.6.3. Eğitim Stratejisi

Bilgi ve iletişim teknolojilerinin aktif kullanıldığı günümüzde hem kamu kurumlarının uzun vadeli çalışmalarında, hem de birey olarak vatandaşların en alt seviyeden başlayarak, en üst düzey eğitim kurumlarına kadar bilgi

güvenliği bakış açısının yansıtılması gerekliliği ortaya çıkmaktadır. Kurumsal olarak bakış açısına ilaveten ülkemizin ilk ve orta öğretiminin eğitim müfredatına girdi sağlayarak, Milli Eğitim Bakanlığı ve Üniversitelerle ortak işbirliği çerçevesinde ülke genelinde ilk ve orta öğretimden lisans ve lisansüstü düzeylere kadar bilgi güvenliği ile ilgili müfredat revizyonu ve farkındalık için girişim ve liderlik rolü üstlenmek, uzun vadeli ülke eğitim stratejisi içerisinde yerini alması gereken kilit görevler olarak ortaya çıkmaktadır. Türkiye'nin Bilgi Güvenliği Stratejisi genelinde ve kamu kurumları bilgi güvenliği stratejilerinin oluşturulması özelinde rehberlik sağlama sorumluluğu alma girişimi öngörülmektedir. Bu noktada özel sektörün rekabet açısından ayakta kalmasına da destek olmak amacıyla yurtdışı örneklerinde olduğu gibi devletin vizyonunu ortaya koyabilecek ekiplerle özel sektöre bilgi güvenliği ve alt başlıkları konusunda teknik danışmanlık desteği ve yol gösterme, yönlendirme faaliyetleri yapılması, kamusal yapılanma çerçevesinde mutlaka yerini almalıdır[12]. E-Devlet Kapısı projesi özelinde yürütülmekte olan eğitim faaliyetlerinin ülkenin kamusal yapılanmasına katkı ve katma değer sağlaması gelecek nesillerin bilgi güvenliği temelinde nasıl yetişeceğini de ortaya koyacaktır.



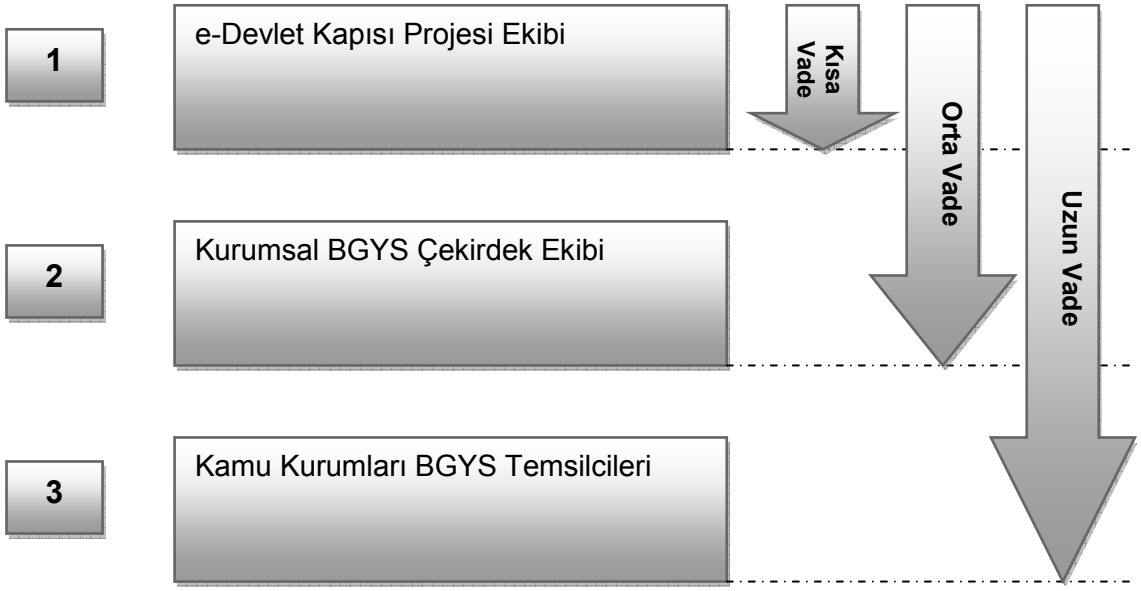
Şekil 2.3. Kurumlarüstü Bilgi Güvenliği Stratejisi

Şekil 2.3 ’te bahsi geçen dört ana bileşen aşağıda detaylandırılacaktır.

BGYS (Bilgi Güvenliği Yönetim Sistemi) eğitim stratejisi, proje ekibi ve kamu farkındalığının nasıl olması gerektiği ile ilgili olarak; bilgi güvenliği ve alt başlıkları konusunda gerek ve yeter şartı sağlayacak şekilde bir donanıma sahip olunabilmesinin en önemli adımının bir ekip kurmak olduğunun bilinmesi başlangıç açısından önemlidir. Bu noktada e-Devlet Kapısı projesi özelinde bilgi güvenliğinin sağlanmasında risk yönetimi kavramının uygulanması için oluşturulması gereken ekiplerle ilgili üç aşamalı yayılım

önerim Şekil 2.4 'teki gibidir. Bu öneri; e-devlet kapısı ekibi ve kamu kurumları ekipleri tarafından uygulanabilir.

E-Devlet Kapısı projesi teknik şartnamesi çerçevesinde öngörülen ve gerek şart olarak sunulan projenin ISO 27001:2005 Bilgi Güvenliği Yönetim Sistemi şartlarına göre dizaynının, altyapı kurulumunun, sürdürülebilirliğinin önce e-Devlet Kapısı özelinde sonra kamu kurumları genelinde şöyle yapılması önerilmektedir;



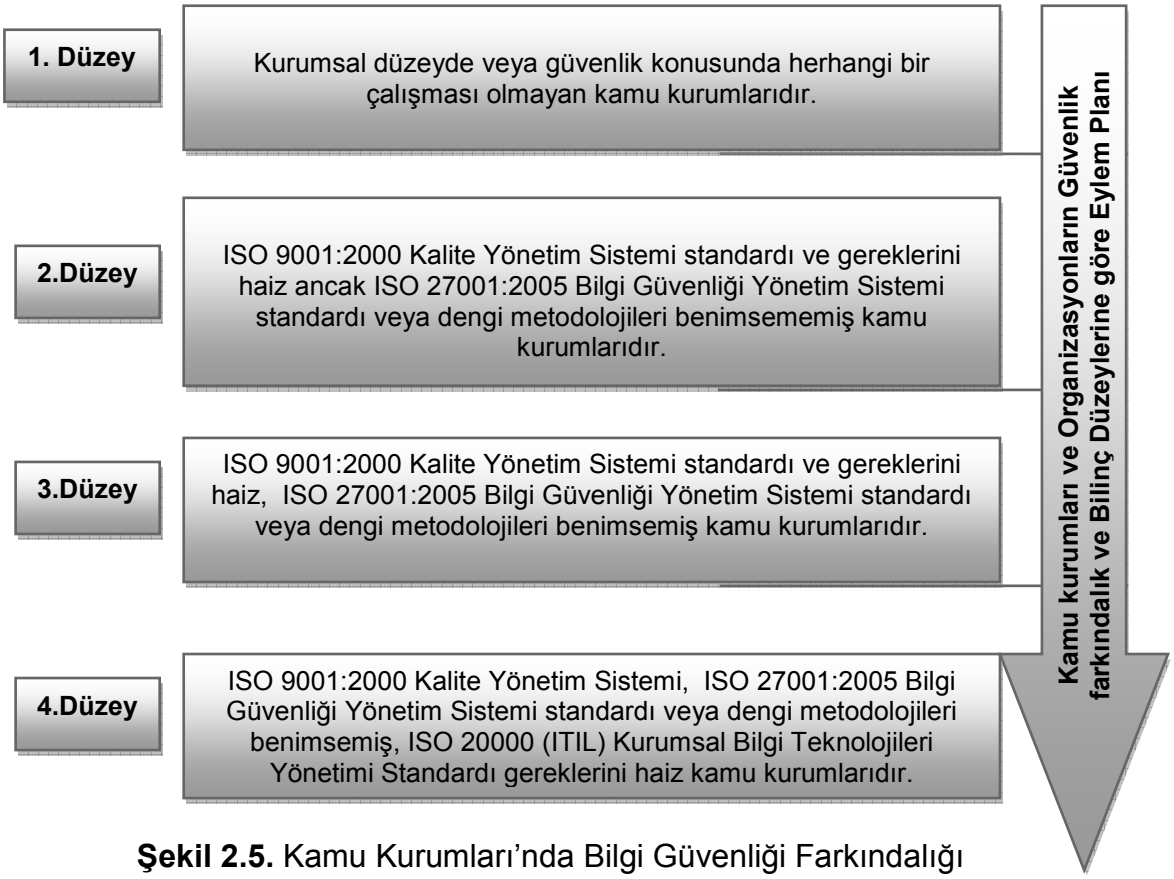
Şekil 2.4. BGYS Eğitim ve Farkındalık Stratejisi

1. E-Devlet Kapısı Projesi bünyesinde kurulmuş olan ekibe temel eğitim bakımından farkındalık anlamında bir eğitim aldırılması önemlidir. Bu farkındalığın bir adım ileriye götürerek bilinçlilik düzeyine çıkarılması gerekmektedir. Yapılması gereken; konuyla ilgili bilgi güvenliği ve risk yönetim ekibi, bilgi güvenliği ve risk

yönetimi lideri belirlemektir. Dünyada bilginin yönetilmesi ve güvenliği konusunda gidilen yöne gözatıldığında; ISO 9001:2000 (Kalite Yönetim Sistemi), ISO 27001:2005 (Bilgi Güvenliği Yönetim Sistemi), ISO/IEC 20000 (ITIL- Bilgi Teknolojileri Hizmet Yönetimi Sistemi) gibi standartların uygulanıyor olması küresel ölçekte, projelerin ya da kurumların ulaştıkları düzey açısından önemli bir göstergedir.

2. e-Devlet Kapısı Projesi özelinde Bilgi Güvenliği Yönetimi çalışmaları gereği belirli bir farkındalık ve bilinçlilik düzeyi sağlanması sonrasında projenin çerçevesini genişleterek kurumsal düzeyde yürütmek uygun olacaktır. Zira teknoloji çağı içerisinde çalışmalarına ve dönüşüm sürecine devam eden ülke olarak ürettiğimiz ürünlerden birinin "Bilgi" olduğunu düşünecek olursak mevcut kontrollerin yanısıra güvenliğinin uluslararası sertifikalarla taçlandırılması amaçlanmalıdır. O bakımdan Türkiye'nin kamu yapılanması içerisinde yapılandırılması hedeflenen "Bilgi Güvenliği Kurumu" na çok iş düşmektedir. Öncelikle orta seviye yöneticiler düzeyinde bir tanıtım toplantısı, sonrasında ise her kurumdan bir "temsilci" görevlendirilecek şekilde bilgi güvenliği ile ilgilenecek bir uzman atanması faydalı olacaktır. Bu noktada bilgi toplumu stratejisi ve eki eylem planı bünyesinde seksen sekiz numaralı eylem olan "Ulusal Bilgi Sistemleri Güvenlik Programı" çerçevesinde sürdürülmekte olan çalışmalarla paralellik sağlanması önem arz etmektedir.

3. Buraya kadar yapılacak güvenlik çalışmalarındaki asıl hedef, e-devlet kapısı projesi çerçevesinde yapılan çalışmalar gereği bilgi güvenliğinde yakalanması gereken hassasiyet yönetilirken, kamu kurumlarının da iç süreçleri ile ilgili var olan bilinç düzeylerinin bir üst seviyeye çıkarılmasıdır. Bu konuda e-Devlet Kapısı Projesi teknik şartnamesinde bulunan "Güvenlik Komisyonu/Grubu"nun yönlendirilmesinde kurumlara öncelikle bir farkındalık eğitimi, projenin güvenlik konusunda gidişatı ile ilgili bir bilgilendirme sağlandıktan sonra kurum temsilcilerini sinerji yaratarak hedefe yöneltebilecek bir strateji ortaya konulması hedeflenmektedir. Bu strateji çerçevesinde kurumların yönlendirilmesi ile ilgili olarak Şekil 2.5'te belirttiğimiz gibi bir seviyelendirmeye tabi tutulacaktır;

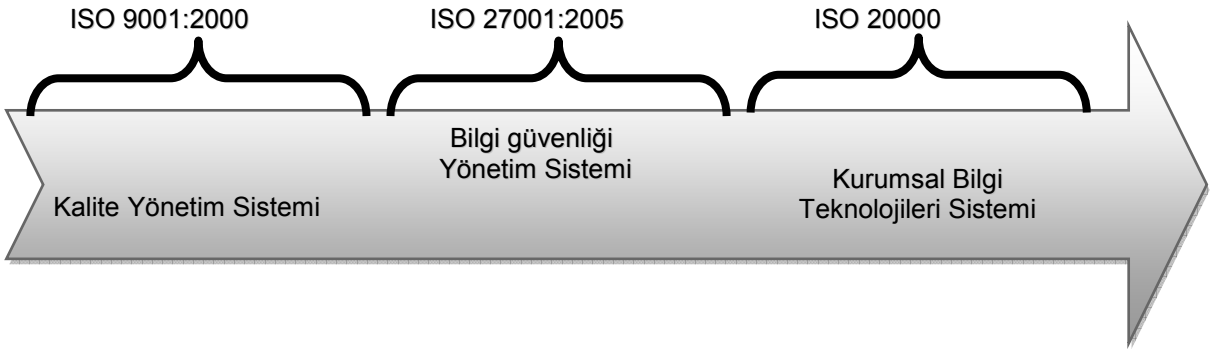


Şekil 2.5. Kamu Kurumları'nda Bilgi Güvenliği Farkındalığı

Bu seviyelendirme neticesinde hangi kamu kurumuna ne tür strateji ile yaklaşım gösterilmesi gerektiği tespit edilmiş olacaktır. Yukarıda belirtilen çalışmalarla ilgili olarak Şekil 2.5'te gösterilen her düzeye ait;

- Gerekli eğitimler,
- Gerekli kaynak yatırımları,
- Personel istihdamı ve niteliklerinin belirlenmesi,
- Yapılması gereken çalışmaların önceliklendirilmesi,
- Takip edilecek destek standartlar ve metodolojilerin belirlenmesi

gibi bazı işlemlerin bunlarla sınırlı kalmamak kaydıyla yapılması gerekmektedir.



Şekil 2.6. Bilgi Güvenliği Altyapısı Oluşma Süreci

Yukarıdaki Şekil 2.6'da gösterilen farkındalık ve yetkinlik süreci tamamlandığı taktirde bilgi güvenliği ve kurumsallaşma bakımından bir organizasyon % 80 olgunluğunu tamamlamıştır[15].

E-Devlet Kapısı Projesi organizasyonunda bulunan ve projenin tüm kamu kurumlarında benimsenmesi ve layıkıyla uygulanabilmesi amacıyla kurulması öngörülen alt komisyonlar bulunmaktadır. Bunlardan “Güvenlik Grubu” nun üstlendiği görev ve sorumluluk önem arz etmektedir. E-Devlet Kapısında güvenlik bütün platforma yayılacak bir katman olacaktır. Güvenlik Grubu, güvenlik katmanının tutarlı ve bütün platform için geçerli politikalarını, uygulama esaslarını belirler ve spesifik sistemlerden sorumlu personelle birlikte uygulamayı hedefler. Bu bağlamda kamu kurumlarından resmi yollar ile bildirilen kurum temsilcilerinin, bulundukları kurumların güvenlik liderleri olacak şekilde eğitilmeleri konusunda gerekli yönlendirmelerin yapılması gerekmektedir. Yapılacak olan yönlendirmeleri genel olarak sıralayacak olursak;

- Bilgi güvenliği ekibinin kurulması (Güvenlik lideri + Birimlerin temsilcileri)
- Bilgi güvenliği ekibinin eğitilmesi
- Kapsamın belirlenmesi
- Danışman seçimi veya önderlik etme
- Pilot bir birim seçilerek şablonların oluşturulması
- Dokümantasyon çalışmaları ve belgelendirme sürecinin tamamlanması

şeklindedir.

Yukarıda adım adım anlatılan kurumsal yönlendirme ve farkındalık yaratma çalışmalarına bireysel bazda kamu personellerinin kariyerlerini destekler tarzda bazı sertifikasyon hakları verilmesi sürece fayda

sağlayacaktır. Bu sertifikalar öncelikle Türkiye Cumhuriyeti sınırları içerisinde KPSS (Kamu Personeli Seçme Sınavı) sınavına ilave puan şeklinde (veya uluslararası anlaşmalar sayesinde daha geniş alanlarda tanınma şansına sahip olabilir) veya kurum içerisinde yükselmelerde kriter olarak geçerli olacak şekilde, kamu personelinin yetkinliklerini kanıtlamalarına fırsat verilmesi, sürece katkı sağlayacaktır.

Güvenlik altyapısının kontrol edilmesi ile ilgili olarak kamu kurumlarının güvenlik düzeyleri Şekil 2.4'te bahsedildiği gibi kurumların personelleri tarafından yapılacak ilk değerlendirmeler ile belirlenebilmelidir. Ancak buna ilaveten kurumların teknolojik güvenlik altyapısının yeterlilik düzeyi, kullandığı teknolojinin güvenlik zafiyeti gösterip göstermediği konuları da değerlendirilerek bir mevcut durum analizi yapılması önem arz etmektedir. Kurumun vatandaşlarına karşı yerine getirmekle yükümlü olduğu görev ve hizmetler ile vatandaşların devlete karşı olan hak ve yükümlülükleri karşılıklı olarak yerine getirirken olması gereken asgari güvenlik düzeyleri gözönünde bulundurularak olması gereken duruma ait bir öneri raporu ve aradaki farkı kapatmaya yönelik eylem planı sunulması ve bu plan üzerinden hareket edilmesi oldukça önemlidir.

Kripto sistemleri hakkında ise e-Devlet Kapısı projesinde, yukarıda detaylı olarak aktarılan iş süreçlerinde ve kamu kurumlarının bilgi güvenliği ve şifreleme açısından ortaya konulacak bir metodoloji çerçevesinde geliştirilecek algoritmalarla ülkemize katma değer sağlanması hedeflenmektedir. Kripto, köken olarak Yunanca gizli saklı anlamına gelen

kryptos sözcüğünden üretilmiştir. Bu sözcüğe yine Yunanca yazmak anlamına gelen *graphein* sözcüğünü eklediğimizde ise kriptografi türetilmektedir. Kriptografi ise; gizlilik, kimlik denetimi, bütünlük gibi bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemler bütünüdür(16). Her kurumun yaptığı iş kendisi için oldukça önemlidir. İzinsiz olarak açıklandığı takdirde kurumun güvenliğini, çıkarlarını ve diğer kurumlarla ilişkilerini olumsuz yönde etkileyebilecek, kurumun maddi manevi büyük zararına neden olabilecek nitelikte olağanüstü önem taşıyan bilgi varlıklarını çok gizli düzeyde değerlendirebiliriz. Aynı şekilde kullanılması güvenlik açısından önemli olmayan, kurumdaki veya kurum dışındaki her kişiye açık bilgi varlıklarını da yayınlanabilir düzeyde bilgiler diyebiliriz. Bu durumda çok gizli bilgilere sahip bir kurumdan, başka bir kuruma gönderilen bilgi ya da verinin paylaşım şekli ile yayınlanabilir düzeydeki bilgi ya da verinin paylaşım şekli aynı olamayacağı açıktır. Manuel ortamlarda kurumlar arası bilgi, belge ve veri paylaşımı düzenlenmiştir ve resmi yazının sol üst ve alt köşesine yazının içeriğinin önem düzeyine göre “çok gizli”, “gizli”, “kuruma özel” gibi ibareler ile paylaşılabilmektedir(17). Ancak bilgi ve iletişim dünyasında bu şekilde resmi evrağa kaşe ya da yazı ile bu tür ibareler koymak bilgi güvenliğinin özüne ters bir durum olup, sonuca olumlu katkısı olmayan çözümlerdir. İşte tam bu noktada bilgi ya da veri paylaşımında güvenlik düzeylerini tanımlamaya yönelik kripto sistemleri geçerli bir güçtür.

Bilgi, bir kurumun en önemli değerlerinden birisidir ve sürekli korunması gerekir. Bilgi güvenliği sistemi ile yetkili kullanıcıyı yetkisiz erişimlere, bilginin değiştirilmesine ve saldırılara karşı korumak, koruma

sırasında gerekli olan kontroller ve ölçümlerin tespiti, dokümantasyon oluşturulması ve karşı tedbirlerin alınmasının sağlanması hedeflenmektedir.

ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemi;

- Gizlilik (Confidentiality): "Yetkisiz kişilere, süreçlere ve benzeri vb. açıklanmaması ya da teslim edilmemesi gereken veri ya da programların özelliği…"
- Veri Bütünlüğü(Integrity): "Programların sistemin ve verilerin kötü niyetli olsun olmasın değiştirilmesi ve bozulmasına karşı korunması ya da korunmuş olması…"
- Süreklilik(Availability): "Bir sistem ya da özkaynağın gereksinildiğinde kullanıma elverişli olma derecesi…"[18]

şeklinde belirtilen üç ana konu üzerinde yükselen bir gerekler bütünüdür.

2.6.4. Risk Yönetimi

Risk; Fransızca "risque" kelimesinden dilimize geçmiştir, sözlük anlamı olarak zarara uğrama tehlikesi ve öngörülebilir tehlikeleri ifade eder. Risk, gelecekte oluşabilecek potansiyel problemlere, tehdit ve tehlikelere işaret eden, belirli bir zaman aralığında, hedeflenen bir sonuca ulaşamama, kayba ya da zarara uğrama olasılığı olarak da tanımlanabilir. Risk yönetimi ise, kurumun karşı karşıya bulunduğu risklerin tanımlanması, bu risklere değer biçilmesi, risklerin kabul edilebilir bir seviyenin altına indirilmesi ve sürekli bu seviyenin altında kalmalarını sağlayacak mekanizmaların devreye sokulmasıdır. Başka bir ifade ile risk yönetimi; bir kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetlerdir. Yüzde yüz güvenli bir çalışma ortamı kurmak imkansızdır. Her çalışma ortamında, bir takım güvenlik

boşlukları ve bunlara bağlı riskler mevcuttur. Yapılması gereken, karşı karşıya olunan riskleri, doğru bir şekilde yönetmektir. Sonuç itibarıyla; risk yönetiminde, riskin tamamıyla ortadan kaldırılması mümkün değildir. Bu konuyla ilgili ilerleyen kısımlarda detaylı olarak e-Devlet Kapısı Projesi bünyesinde nasıl bir metodoloji kullanıldığı ayrıntılarıyla açıklanacaktır.

2.6.5. Güvenlik Politikaları

Güvenlik Politikası, kurumda güvenliğin oynadığı rolün genel bir anlatımıdır. Güvenlik Politikası, üst yönetim, seçilmiş bir Kurul ya da bir Komite tarafından yazılabilir. Güvenlik Politikaları, bireylerden ve teknolojiden bağımsız hazırlanmalıdır. Kurumda uygulanacak güvenlik kontrolleri, ayrıntıya girilmeden kavramsal olarak tanımlanmalıdır. Güvenlik politikasının kuruma üç yararından bahsedilebilir:

1. Kurum çalışanlarını ve üçüncü tarafları yasal sorumluluktan kurtarmak,
2. Kuruma özel gizli bilgileri; hırsızlığa, suistimale, yetkisiz kişilerin eline geçmesine, ifşaya ve değiştirilmeye karşı korumak,
3. Kurumun bilgi işlem yeteneğini oluşturan kaynakların israfını ve boşa kullanımını engellemek.

Bir kurum için hiyerarşik olarak farklı düzeylerde güvenlik politikalarından bahsedilebilir:

- *Kurumsal Güvenlik Politikası*: Üst yönetim tarafından, kurumda bilgi güvenliği programının çerçeve çalışması ifade edilir. Bu tür bir politika, kurumun gelecekteki tüm güvenlik faaliyetlerini kapsaması ve yönlendirmesi açısından önem taşır. Politika içerisinde; programın

amaçları, verilecek sorumluluklar, güvenliğin stratejik/taktik açıdan önemi ve uygulamada yapılacak işler, genel hatları ile kavramsal olarak tarif edilir. Kurumsal Güvenlik Politikası içerisinde, ilgili kanunlara, yasal düzenlemelere ve diğer yönerge ve prensiplere başvurular yapılabilir. Üst yönetimin, bilişim güvenliği açısından kabul edilebilir bulduğu risk düzeyi de bu tür bir politikada yer alabilir.

- *Konuya Özel Güvenlik Politikası*: Üst yönetim, belli konularda çalışanlarını daha fazla bilgilendirmek, daha ayrıntılı bilgi vermek, bu konuyu kapsamlı bir şekilde ifade etmek istediğinde bu tür bir politika geliştirilebilir. Örneğin e-posta gönderme alma konusunda, üst yönetimin kararlarını, haklarını, yapıp-yapamayacaklarını bu tür bir politika içerisinde ifade etmek uygun olacaktır. Üst yönetimin, gerekli görüldüğünde çalışanların e-postalarını okuyabileceği, e-posta yoluyla gizlilik derecesine göre ne tür bilgilerin gönderilip alınabileceği gibi hususlar, e-posta özel politikası içerisinde ifade edilir.
- *Sisteme Özel Güvenlik Politikası:* Üst yönetimin, bilgisayarlar, bilgisayar ağları ve uygulamalar, kurumsal veriler hakkında aldığı ayrıntılı kararları içerir. Bu tür bir politika içerisinde, kullanılmasına izin verilen yazılımlar, veritabanlarının nasıl korunacağı, bilgisayarlara uygulanacak erişim - denetim kriterleri, güvenlikle ilgili yazılım ve donanımların nasıl kullanılacağı gibi konular açıklanabilir.

Güvenlik politikalarını desteklemek üzere daha ayrıntılı bir takım dokümanlar oluşturulabilir.

2.6.6. Standartlar ve Metodolojiler

Bu bölüm, çalışma içerisinde yapılan analiz faaliyetlerinde ve uygulama sürecinde en fazla riayet edilen standart ve metodolojiler hakkında genel bilgilendirme sağlamaya yönelik olarak hazırlanmıştır. Bu noktada ISO (International Standard Organization) ve IEC (International Electrotechnical Commission) organizasyonları hakkında kısa bilgilendirmeden sonra en fazla başvurulan standart ve metodolojilerden üç tanesi üzerinde durulmaktadır.

ISO ve IEC; Uluslararası Standardlar Organizasyonu olan ISO[19] 1947 yılında kurulmuştur. Merkezi İsviçre Cenova'dır. Amacı, uluslararası ticareti kolaylaştırmak ve desteklemek için standardlar geliştirmektir. Uluslararası Elektroteknik Komisyonu olan IEC, 1906 yılında kurulmuştur. Merkezi İsviçre Cenova'dır. Amacı, her türlü elektroteknoloji için standardlar geliştirmektir.

ISO/IEC 27001:2005 - Bilişim Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler standardı, bir Bilgi Güvenliği Yönetim Sistemi'ni (BGYS) (ISMS – Information Security Management System) kurmak, geliştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model oluşturmak amacıyla hazırlanmıştır. ISO/IEC 27001, bilgi güvenlik yönetim standardıdır. Bir dizi bilgi güvenlik yönetim gereksinimlerini tanımlar. Gereksinim bir ihtiyaç, beklenti ya da zorunluluktur. Çok çeşitli türde gereksinimler vardır. Bunlar güvenlik gereksinimleri, sözleşmelere bağlı gereksinimler, yönetimsel gereksinimler, düzenleyici ya da yasal gereksinimleri içerir.

ISO/IEC 27001 standardının amacı, BGYS kurmak ve bakımını sürdürmektir. ISO/IEC 27001 standardı her türlü kuruluşa uygulanabilir. Kuruluşun ne yaptığı ya da büyüklüğü önemli değildir. Bu standart, kuruluşun bilgi güvenlik yönetim gereksinimleri ve gerekliliklerini karşılamaya yardımcı olur.

Bu standart ISO tarafından 14 Ekim 2005 tarihinde yayınlanmış ve ISO/IEC 27000 standart serisi altında yerini almıştır. Bilgi güvenliği yönetim sistemi ile ilgili belgelendirilebilen bir standarttır.

Türkiye'de ise, ISO tarafından kabul edilen, ISO/IEC 27001:2005 standardı esas alınarak, TSE Bilgi Teknolojileri ve İletişim İhtisas Grubu'nca hazırlanmış ve TSE Teknik Kurulu'nun 2 Mart 2006 tarihli toplantısında Türk Standardı olarak kabul edilerek, "TS ISO/IEC 27001 Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri - Gereksinimleri" adıyla yayınlanmıştır.

ISO/IEC 27000 standart serisi altında yer alan diğer bir standard; ISO/IEC 27002:2005 - Bilişim Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenlik Yönetimi için Uygulama Kılavuzudur. Bu standardın önceki adı ISO/IEC 17799:2005'dir. 1 Temmuz 2007 tarihinde, ISO tarafından yapılan teknik bir düzenlemeyle ISO/IEC 17799:2005 standardının adı, ISO/IEC 27002:2005 olarak değiştirilmiştir. Bu standard, bilgi güvenliği yönetimi sistemi (BGYS) oluşturmak için gereken 11 ana başlık altında yapılandırılmış 133 adet güvenlik kontrolü tanımlayan bir uygulama kılavuzudur.

CobiT; Türkçe karşılığı Bilgi ve İlgili Teknolojiler İçin Kontrol Amaçları olan **Control OBjectives for Information and related Technology** kelimelerinden üretilmiş bir kısaltmadır. ISACA (Information Systems Audit and Control Association) ve ITGI (IT Governance Institute) tarafından 1992 yılında geliştirilmiş, BT Yönetimi için en iyi uygulamalar kümesidir. CobiT; ISO teknik standartları, ISACA ve AB tarafından yayınlanan yönetim kanunları, COSO, AICPA (The American Institute of Certified Public Accounts) , GAO (The US General Accounting Office) tarafından yayınlanan profesyonel iç kontrol ve denetim standartları tarafından biçimlendirilmiştir. Bir şirkette teknolojinin kullanımından ve BT yönetişimi ile kontrol geliştirmekten türeyen faydayı en üst düzeye çıkarmaya yardım etmesi için yöneticilere, denetçilere ve BT kullanıcılarına genel olarak kabul görmüş ölçüler, göstergeler, süreçler ve en iyi uygulamalar sağlar. CobiT'in vizyonu; bilgi teknolojileri yönetişim (IT governance) modeli olmaktır. CobiT sadece bir denetim aracı değil, aynı zamanda bir yönetişim aracı olma amacını taşır. Bu nedenle yönetimden bilgi teknolojileri personeline kadar kurum içi ve dışında, kurumun varlığı ve sağlıklı faaliyet göstermesi konularında risk üstlenen çeşitli taraflara fayda sağlama amacını da yerine getirmeyi hedeflemektedir.

CobiT'in ilk sürümü 1996 yılında yayımlandı. Amacı; iş yöneticileri ve denetçilerinin günlük kullanımı için geçerli, güncel, uluslararası kabul görmüş BT amaçlarını araştırmak, geliştirmek ve teşvik etmekti. "Yönetim Rehberi", 1998'de yayınlanan 2. sürüme eklendi. 2000 yılında 3. sürüm yayınlandı. 2003 yılında bilgisayar bağlantılı versiyonu kullanılır duruma geldi. 2005

yılının aralık ayında 4. basım ilk olarak yayınlandı. 2007 yılının mayıs ayında, şu anda kullanılan 4.1 sürümü yayınlandı. Yayında olan bu versiyona ISACA'nın web sitesinden erişilebilmektedir[19]. 4.1 versiyonundaki temel değişiklikler;

- Olgunluk modeli için destek,
- Amaçların basitleştirilmiş tarifi,
- İş, BT Amaçları ve BT Süreçleri arasındaki çift yönlü ilişkileri ve süreçleri basamaklandırmak

şeklinde listelenebilir.

CobiT, dört etki alanında gruplanmış 34 bilgi teknolojisi sürecini ele alır. Bu dört grup;

- Planlama ve Organizasyon
- Tedarik ve Uygulama
- Teslimat ve Destek
- İzleme ve Değerlendirme

şeklindedir. Her bir sürecin 0-5 arası bir olgunluk seviyesi vardır. (0 yok, 5 optimize edilmiş) Bu ölçek, bir organizasyondaki sürecin olgunluk seviyesi, o sürecin hangi olgunluk seviyesinde olması gerektiği, hangi seviyenin en iyi uygulama olarak varsayıldığı ve diğer organizasyonların ne seviyede olduğu

gibi anahtar değerlendirmeler için kullanılır. Olgunluk seviyeleri Çizelge 2.2 ’de tarif edilmiştir.

Çizelge 2.2. Süreç Olgunluk Seviyeleri

0	**OLMAYAN**	TANIMLANMIŞ SÜREÇ BULUNMAMAKTADIR.
1	**Başlangıç**	Organize olmayan ve standartlaşmamış fakat kurumda farkındalığın mevcut olduğu ve adresleme ve standartlaştırma ihtiyacının tespit edildiği seviyedir.
2	**Tekrarlanan**	Bireye dayalı ve tekrarlanan işleri farklı kişilerin aynı şekilde yapabildiği seviyedir. Bu seviyede formal eğitim ve iletişim metodları belirlenmemiş fakat sorumluluk büyük oranda kişiye bağlı kılınmıştır.
3	**Tanımlı**	Prosedürler standartlaşmış ve dokümante edilmiş, eğitim aracılığı ile kurum içinde iletilmiştir. Ancak bu süreçleri izleyip izlememe kararı kişinin kendisine bırakılmıştır; bu nedenle yapılan işler arasında çeşitli farklılıklar mevcuttur. Prosedürlerin kendisi gelişmiş değildir; ancak mevcut uygulamaların biçimselleştirilmiş halidir.
4	**Yönetilen**	Prosedürlerle uyumu izlemek ve ölçmek, süreçlerin etkin çalışmadığının anlaşılması durumunda faaliyete geçmek mümkündür. Süreçler sürekli gelişmekte ve iyi uygulamaların tanımlanması sağlanmaktadır. Otomasyon ve araçlar kısıtlı veya parçalı bir biçimde kullanılabilmektedir.
5	**Optimize Edilmiş**	Süreçler en iyi uygulamalar seviyesine indirgenmiş, sürekli gelişim ve olgunluk modelleme konusunda diğer şirketlerin sonuçları ile çalışmaktadır. BT, iş akışlarının otomatize edilmesi, kalite ve etkinliğin artırılması ve kurumun çabuk adapte olabilmesi için entegre olmuştur.

ITIL; Information Technology Infrastructure Library sözcüklerinin kısaltılmışıdır ve BT Altyapı Kütüphanesi olarak adlandırılır. ITIL, BT Servislerini eksiksiz ve en iyi kalitede yönetmek üzere geliştirilmiş servis yönetim metodolojisidir[(20)].

ITIL, 1987'de İngiltere Ticaret Bakanlığı (OGC - Office of Government Commerce) tarafından geliştirilmiştir. İş süreç yaklaşımı sayesinde ITIL müşteri, tedarikçi, BT bölümü ve kullanıcıları arasında başarılı bir şekilde iletişim kurulmasını sağlamaktadır. "En iyi uygulamalar/deneyimler" üzerine yapılandırılmış olan ITIL BT Servis Yönetimi ve dağıtımı süreçleri ile dünyada yaygın olarak kullanılmakta ve kabul görmüş (de-facto) bir standart olarak benimsenmektedir. ITIL, Servis yönetimi ve sağlama süreçleri için en uygun başvuru kaynağıdır. Servis yönetimini en iyi şekilde sürdürmek için yol gösteren ve kullanıcılarına servis sağlama süreçlerini ayrıntılı şekilde gösteren bir kitap kümesi olmaktan çıkmış, dünyaca kabul gören yöntemler dizisine dönüşmüştür. ITIL yaklaşımının servis yönetimi süreçlerine nasıl uygulanacağı her organizasyon tarafından kendi kültürüne, yapısına ve teknolojisine göre belirlenmelidir.

Bilişim Teknolojileri servis yönetiminin en iyi uygulamalarının ve yönetim süreçlerinin tanımlandığı ve açıklandığı ITIL çalışmalarına dayanan standartlaştırma çalışmaları, Aralık 2005'te ISO tarafından uluslararası bir standart olarak ISO 20000 adı altında yayınlandı.

2.6.7. Denetim Süreci

Sistem bazlı yapılan çalışmalarda sonucun belirlenebilmesi adına bir takım kriterler üzerinden denetleme faaliyeti gerçekleştirilmektedir. E-Devlet Kapısı projesi çerçevesinde kurulmaya çalışılan sistemde baz alınan ISO 27001:2005 Bilgi Güvenliği Yönetim Sistemi standardı ile ilgili yapılan denetim sürecine değinilecektir. Dünyada ve ülkemizde kurumsal bilgi

güvenliği yönetim sistemlerinin sertifikalandırılmasında uyumluluğa esas teşkil eden standart, 2005 yılına kadar BS7799–2 standardı olurken bu yıldan sonra ISO/IEC 27001 standardı olarak değiştirilmiştir. 15 Ekim ile 15 Nisan 2006 tarihine kadar olan hazırlık dönemi sırasında, denetimler ve belgelendirme ISO/IEC 27001:2005 veya BS 7799–2:2002 standartlarına göre gerçekleştirilmiştir. Ancak, bu süre içerisinde yayınlanmış olan yeni bir BS 7799–2:2002 sertifikasının, 15 Nisan 2007 tarihine kadar ISO/IEC 27001:2005'e geçişi tamamlanmıştır. 15 Nisan 2006 tarihinden sonra bütün denetimler ve belgelendirmeler ISO/IEC 27001:2005 standardına göre gerçekleştirilmiştir. BS 7799'a göre belgelendirilmiş olan kuruluşların, 15 Nisan 2007 tarihine kadar yeni standarda geçişlerini tamamlamaları gerekmektedir. 23 Temmuz 2007 tarihi itibariyle BS7799–2 sertifikasyonu geçersiz olacaktır. Bu süreçte; BGYS belgeleri ve kayıtlarının geliştirilmesi, üretilen bu belge ve kayıtların kontrol edilmesi ve izlenebilirlik ilkelerine uygun olarak saklanması belgelendirmede önem arz etmektedir. Aynı zamanda ISO/IEC 27001:2005 standardına uygun olarak denetim yapabilen üçüncü taraf firmaların yetkilendirdiği baş denetçi (lead auditor) ünvanına sahip kişi ya da kişiler tarafından sistem denetlenir. Denetim neticesinde sistem sertifikası üç yıl geçerli olmak üzere ilgili kuruma verilir ve her yıl gözetim denetimi geçirilir, üçüncü yılın sonunda ise tekrar sertifika denetimi yapılır.

2.7. Risk Yönetimi ve Değerlendirme Süreci

Bir kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetler bütününe risk yönetimi denilmektedir(5). Bilgi ve iletişim sistemlerinde risk yönetimi teknikleri tüm bilgi

sistemine, ya da bu sistemi oluşturan ayrı sistem parçalarına, ya da servislere uygulanabilir. Risk yönetiminin amacı kurumun bilgi varlıkları için, uygun bir seviyede korumanın sağlanmasıdır. “E-Devlet Kapısı Projesi” çerçevesinde uygulamaya alınan risk değerlendirme sürecinin detayları ilerleyen bölümlerde detaylandırılmaktadır.

2.7.1. Risk Analizi

Risk analizi, ISO/IEC 27001:2005 standardında; kaynakları belirlemek ve riski tahmin etmek amacıyla bilginin sistematik kullanımı olarak tanımlanmaktadır. Tespit edilmiş veya edilecek olan riskler ile ilgili tehditlere ilişkin gerçekleşme olasılıkları ve tehditlerin gerçekleşmesi durumunda ortaya çıkabilecek olumsuz sonuçlara ilişkin düzeyler aşağıdaki skalalar baz alınarak belirlenir:

Çizelge 2.3. Olasılık Skalası

5	Neredeyse her seferinde gerçekleşir
4	Sıklıkla meydana gelebilir
3	Bazen meydana gelebilir
2	Meydana gelmesi çok olası değildir ama yine de olabilir
1	Çok nadiren ve yalnızca istisnai durumlarda meydana gelebilir

Çizelge 2.4. Potansiyel Sonuç Skalası

Feci	Organizasyonun bir çok kritik iş yada kalite amaçlarını, hizmet çıktılarını, proje ve diğer stratejik teşebbüslerini tehdit eden ciddi sonuçlar. Organizasyonun olanaklarını aşan veya çok sarsan maliyet ya da kaynak etkileri. Bir yada daha fazla temel varlığın tahrip olması. Bir ya da daha fazla çalışanın ölümü ve/veya birden fazla ve ciddi yaralanma ve/veya devamlı sakatlık. Ciddi şekilde zarar görmüş müşteri veya iş ortakları. Belirgin ve uzun dönem çevresel etki. İşlerin bir hafta durmasına eşdeğer iş aksaması.
Çok Önemli	Organizasyonun kilit iş ya da kalite amaçlarını, hizmet çıktılarını, proje ve diğer stratejik teşebbüslerini tehdit eden belirgin sonuçlar. İş birimi olanaklarını aşan maliyet ve kaynak etkileri. Bazı varlıkların zarar görmesi ve çalışmaz duruma

	gelmesi. Bazılarının devamlı sakatlıkla sonuçlandığı bir yada birden fazla ciddi yaralanma. Ortakların belirgin bir şekilde etkilenmesi. Muhalif politik ve medya raporları. Uzun dönem etkili çevresel sonuçlar. Birkaç işin 2-7 gün durduğu temel kesintiler. Hizmet ve çıktıların azaltılması ile sonuçlanan plansız iş gücü (çalışan) eksikliği.
Önemli	Organizasyonun iş ya da kalite amaçlarının, hizmet çıktılarının, proje ve diğer stratejik teşebbüslerinin bazı kilit yönleri için tehdit oluşturabilecek sonuçlar. Organizasyonun yerel çalışma gruplarının maliyet yada kaynak etkileri. Bir yada daha fazla temel varlığın zarar görmesi fakat hala çalışır durumda olması. 3 iş gününden daha fazla tedavi ve/veya yataklı tedavi ya da tıbbı ilgi gerektiren yaralanmalar. Müşteriler veya iş ortakları üzerinde bazı etkiler. Uzun dönem etkisi olmayan çevresel sonuçlar. Bir iş günü kapalı olmakla eşdeğer farkedilebilir kesinti. Operasyonları etkileyen plansız çalışan eksikliği.
Az Önemli	İlgili birim müdahalesi gerektiren fakat ilave kaynak ve yardım olmaksızın yönetilebilen sonuçlar. Bazı küçük yerel bütçe etkileri ya da organizasyonun iş yada kalite amaçlarında, servislerinde ve teşebbüslerinde küçük çaplı etkiler. Çok önemli olmayan varlıklarda hasar. Çok önemli olmayan 3 veya daha az iş günü tedavi gerektiren yaralanmalar. Müşteri ve iş ortaklarında ihmal edilebilir etkiler. Kamu hizmetlerinde kısa dönemli ve yönetilebilir kesinti. Çok önemli olmayan çevresel etki. Minimal kesinti. 2-8 saat iş durması. Sonuçlar normal iş eylemleri içerisinde yönetim çabası ile yönetilebilir. Var olan çalışanlar ile telafi edilebilen plansız çalışan eksikliği.
Önemsiz	Rutin prosedürler ile yönetilebilen düşük seviye sonuçlar. Organizasyon, iş ve kalite amaçları, hizmet çıktıları ya da diğer teşebbüslere ihmal edilebilir etkiler. Varlıklar üzerinde önemsiz etkiler. Olay yerinde ilkyardım ile tedavi edilebilecek yaralanmalar. Kamu hizmetlerinde küçük kesinti olması veya hiç olmaması. Ölçülebilir çevresel etki yaratmaması. Normal iş akışı içerisinde yönetilebilir. 2 saatten az hizmet aksaması. Normal seviyede plansız işgücü eksilmesi.

Yukarıdaki skalalar yardımıyla tehditlerin gerçekleşme olasılıkları ve potansiyel sonuçları belirlendikten sonra olasılık ve sonuç değerleri ışığında aşağıdaki matris kullanılarak risk hesaplamaları yapılır.

Çizelge 2.5. Risk Düzeyi Matrisi

		Potansiyel Sonuç Düzeyi				
		Önemsiz(1)	**Az önemli (2)**	**Önemli(3)**	**Çok önemli (4)**	**Feci(5)**
Olasılık	**5**	Orta (O)	Yüksek (Y)	Yüksek (Y)	Çok Yüksek (ÇY)	Çok Yüksek (ÇY)
	4	Orta (O)	Orta (O)	Yüksek (Y)	Yüksek (Y)	Çok Yüksek (ÇY)
	3	Düşük (D)	Orta (O)	Yüksek (Y)	Yüksek (Y)	Yüksek (Y)
	2	Düşük (D)	Düşük (D)	Orta (O)	Orta (O)	Yüksek (Y)
	1	Düşük (D)	Düşük (D)	Orta (O)	Orta (O)	Yüksek (Y)

Risk İşleme Stratejisinde riskler; risk kabulü, maliyet-etkinlik değerlendirmesi, önceliklendirme ve iyileştirmelerin gerçekleştirilmesi gibi alt stratejiler doğrultusunda ele alınır. Bu noktada ilk olarak risk kabulü'nün nasıl yapılacağı konusu üzerinde durulacaktır. Kabul edilebilir risk düzeyleri Çizelge 2.5.'deki belirtilen (düşük, orta, yüksek, çok yüksek) seviyelerden belirlenir. Belirleme işlemi üst yönetimin katılım ve iradesi doğrultusunda gerçekleşir.

- *Risk Kabulü;*

  Kabul edilebilir risk düzeyi ..... tür. Bu düzey ve altındaki riskler için herhangi bir iyileştirme planlanmaz.

  Risk düzeyi .....ve daha yüksek olan riskler için başka hiçbir kritere bakılmaksızın gereken iyileştirmeler yapılır veya ilgili varlığa ilişkin operasyonlar durdurulur. Bu iki seçenekten hangisinin gerçekleştirileceğine ..... karar verir.

  Maliyet-etkinlik değerlendirmesi sonucunda, iyileştirme maliyetinin olası zarardan yüksek olduğu durumlarda, risk kabul edilebilir risk olarak tanımlanır.

  Bu noktada bahsi geçen düzey belirleme süreci e-devlet kapısı projesi için tamamen projenin ülke, kurumlar, işletmeler ve vatandaşlar açısından önemine binaen tercih edilmektedir.

- *Maliyet-Etkinlik Değerlendirmesi;*

  Kabul edilebilir risk olarak tanımlanan riskler dışında kalan tüm riskler için iyileştirmelerin maliyet-etkinlik değerlendirmesi yapılır. Bu değerlendirme iyileştirmenin maliyeti ile tehdidin gerçekleşmesi durumunda oluşacak kayıp ile kıyaslanarak gerçekleştirilir. Maliyet-

etkinlik değerlemesi, çizelge 2.6.'da verilen skala baz alınarak gerçekleştirilir. Çizelge 3.2'de Risk Kabulü ile ilgili sütunda belirtilmiş olan planlanmış kontrollerin hayata geçirilebilmesi için ne kadar yatırım yapılması gerektiği ile yapılan bu yatırımın maliyetinin sistem etkinliği değerlendirilir. Bu değerlendirme proje içerisinden bir uzman tarafından yapılmalıdır.

Çizelge 2.6. Maliyet-Etkinlik Düzeyi Matrisi

1	İyileştirme maliyetinin, olası zarar düzeyinden çok daha yüksek olduğu durumlarda
2	İyileştirme maliyetinin, olası zarar düzeyinden fazla olduğu durumlarda
3	İyileştirme maliyetinin, olası zarar düzeyine aşağı yukarı denk olduğu durumlarda
4	İyileştirme maliyetinin, olası zarar düzeyinden düşük olduğu durumlarda
5	İyileştirme maliyetinin, olası zarar düzeyinden çok düşük olduğu durumlarda

- Önceliklendirme; İyileştirmelerin önceliği sırasıyla maliyet-etkinlik değeri, mevcut risk ve hedeflenen risk düzeyleri değerlerine göre belirlenir.

Bu yapılan risk analizi çalışmaları neticesinde ortaya çıkan riskler Bölüm 3.3'deki risk analizi çizelgesinde görülebilmektedir.

2.7.2. Varlık Envanteri ve Sınıflandırması

Kuruluş için değeri olan herhangi bir şeye varlık denilebilmektedir. Varlık envanterine, etkin varlık korumasının gerçekleştiğini temin etmeye yardımcı olması amacıyla; ayrıca sağlık ve güvenlik, sigorta ve mali (varlık yönetimi) nedenler gibi diğer ticari amaçlar için gereksinim duyulmaktadır. Varlıkların

envanterinin toplanması süreci, risk yönetiminin önemli bir parçasıdır. Varlık envanteri çalışmalarında aşağıdaki hususlar göz önünde bulundurulmalıdır:

a. Varlık envanteri, her bilgi sistemiyle bağlantılı olan önemli bilgi varlıklarını içerecek şekilde, ilgili Yönetim birimlerince hazırlanmalı, korunmalı ve bu envanter periyodik olarak ve değişiklikler oldukça güncellenmelidir. Bu çalışmada; her bir varlık açıkça tanımlanmalı, varlık sahipleri belirlenmeli, varlıkların güvenlik sınıflandırmaları yapılmalı, varlığın mevcut bulunduğu yer (bu kayıp ve hasarlar giderilmeye çalışıldığında önemlidir) belirtilmelidir.
b. Bilişim sistemleriyle ilgili varlıklar aşağıdaki şekilde kategorize edilebilir:
    - Bilgi Varlıkları: Veritabanları ve veri dosyaları, sistem belgeleri, kullanıcı el kitapları, eğitim malzemeleri materyalleri, işlemsel ve destek uygulamaları, devamlılık (süreklilik) planları, yedek anlaşmaları, arşivlenmiş bilgiler vb.
    - Yazılım Varlıkları: Uygulama yazılımları, sistem yazılımları, geliştirme araçları ve yazılımları vb.
    - Fiziksel Varlıklar: Bilgisayar ekipmanları (kasa, ekranlar, diz üstü bilgisayarlar, modemler), iletişim ekipmanları (yönlendirici, telefon, faks), manyetik kayıt ortamları (teyp, kartuş, disket, disk, CD), diğer teknik ekipmanlar (güç kaynakları, adaptör, havalandırma üniteleri), mobilya, yerleşim düzeni;
    - Servisler: Bilgi işleme (bilgisayar) ve iletişim (haberleşme) hizmetleri, genel hizmetler (ısıtma, aydınlatma, elektrik, havalandırma).

Bilgi varlığı; korunma gereksiniminin, önceliklerinin ve derecesinin belirlenmesi için sınıflandırılmalıdır. Varlık sınıflandırmasında aşağıdaki konular göz önünde bulundurulmalıdır:

- Varlık sınıflandırması ihtiyaç, önem ve koruma için ayrılacak kaynak gereksinimini yansıtmalıdır,
- Bazı bilgi varlıkları, ilave korunma seviyesine veya özel olarak ele alınmaya gerek duyabilir,
- Bilgi varlıkları sınıflandırma sistemi, uygun koruma seviyesi tanımlanması için kullanılabilmelidir,
- Bilgi varlıklarının zaman içerisinde sınıflandırma derecesi değişebilir.

Bu çerçevede aktarılan varlık envanteri ve sınıflandırma yapısı ile ilgili "yüksek", "orta", "düşük" şeklinde benimsenmiş sınıflandırma örneği e-devlet kapısı projesi çerçevesinde uygulanan ve Bölüm 3.1'deki e-Devlet Kapısı Projesi Varlık Envanteri çizelgesinde görülebilmektedir.

2.7.3. Tehdit Tanımlama

Spesifik bir zayıflık, sistem adına olumsuz bir kazaya sebep olacak tetikleyici bir davranış, potansiyel bir tehdit kaynağıdır. Burada yapılması gereken en önemli iş; potansiyel tehdit kaynaklarının tespit edilerek bir tehdit listesi oluşturulmasıdır. Sisteme zarar vermesi muhtemel bu tehditler;

- Doğal (Sel baskınları, Depremler v.s.),
- Çevresel (Binaya ait borulardan birinin patlaması ve sistem odasındaki bilgisayarlara zarar vermesi v.s.),
- İnsan (Çalışan personel kasıtlı olarak sisteme zarar verebilir, kötü niyetli kişiler sisteme zarar verebilir veya personel istemeden / bilmeden sisteme zarar verebilir)

şeklinde olabilmektedir. Bu çerçevede tehdit tanımlamalarının yapılması ile ilgili benimsenmiş model örneği e-devlet kapısı projesi çerçevesinde uygulanmış ve Bölüm 3.3'deki risk analizi çizelgesinde görülebilmektedir.

2.7.4. Zayıflıkların/Zafiyetlerin Tanımlanması

Hedef; sistemde olası zayıflıkların/zafiyetlerin tespit edilmesi ve bunun istismar edilerek potansiyel bir tehdit kaynağı olup olmama durumunun tanımlanması ile ilgili bir liste çıkarmaktır. Çıkarılmış olan bu liste risk analizi sürecinde karşılaşılacak olan etkenlerin tanımlanmasında, fayda maliyet analizinin yapılması aşamalarında ciddi bir katma değer sağlayacaktır. Zayıflık ve zafiyet tanımlamalarının yapılması ile ilgili benimsenmiş yöntem; e-devlet kapısı projesi çerçevesinde uygulanmış ve Bölüm 3.3'deki risk analizi çizelgesinde görülebilmektedir.

2.7.5. Tehdit Olasılıklarının Belirlenmesi

Olasılıklar belirlenirken tehdit kaynaklarının motivasyonlarının ve yeteneklerinin, sistemin doğal zayıflıklarının, mevcut kontrollerin etkinliğinin değerlendirilmesinin düşünülmesi gerekmektedir.

Çizelge 2.7. Olasılık Düzey Matrisi

OLASILIK TANIMLAMA	
Olasılık Düzeyi	***Olasılığın Tanımı***
Yüksek	Tehdit kaynağının motivasyonu ve yetenekleri oldukça kuvvetli ve kontrol altına alınması oldukça düşük bir tehdit.
Orta	Tehdit kaynağının motivasyonu ve yetenekleri kuvvetli ancak kontrol altına alınması mümkün bir tehdit.
Düşük	Tehdit kaynağının motivasyonu ve yetenekleri yeterli olmayan veya önemsiz etkiye sahip ve kontrol altına oldukça kolay alınan bir tehdit.

Yukarıda belirtilen Çizelge 2.7'de olasılık düzeyleri ile ilgili örnek tanımlama kriter tanımı ve olasılık düzeyi matrisinden söz edilmektedir. Olasılık tanımlama süreci ile ilgili e-devlet kapısı projesi özelinde tercih edilen yöntem Bölüm 3.3 'deki risk analizi çizelgesinde görülebilmektedir.

2.7.6. Etki Analizi

Burada etki analizi yapılırken nitel değerlendirme mi yoksa nicel değerlendirme mi yapılacağına iyi karar verilmelidir. Her ikisinin de kendine göre avantaj ve dezavatajları bulunmaktadır. Nitel etki analizinin avantajları; risklerin önceliklendirilebilmesi, tanımlanmış bölgelerdeki zayıflıklardaki gelişmelerin görülebilmesi iken dezavantajları; spesifik ölçümler ve etkilerin büyüklükleri hakkında sayısal veriler sunamaması ve fayda-maliyet analizine

veri sağlayamamasıdır. Benzer şekilde nicel etki analizinin avantajları; etkilerin ölçülebilir büyüklükler vererek gösterme, fayda-maliyet analizine veri sağlayabilme ve tavsiye plan oluşturulabilme iken dezavantajları; ölçümlemelerin sayısal oranlara göre yapılması nedeniyle sayılarla çıkan sonucun karar vericileri yanıltabilir olmasıdır. Fayda-maliyet analizinin uygulamaya alınabilmesi için ihtiyaç duyulan kaynakların tahsis edilmesi gerekmektedir. Olası kontrollerin belirlenmesi, organizasyona ait bu işlemin fizibilitesi ve etkinliğinin ortaya konulması gerekmektedir. Bir fayda maliyet analizinde dikkat edilmesi gereken unsur, analize girdi teşkil eden kriterlerin yukarıda bahsedildiği gibi nicel veya nitel olabilmesidir. Riskin etki düzeyinin durumuna göre, riski azaltmaya yönelik uygulanacak herhangi bir kontrol mekanizmasının çalıştırılmasının maliyeti ile hiç bir şey yapılmadığı durumda riskin gerçekleşmesiyle ortaya çıkacak zararın organizasyona ya da projeye maliyeti değerlendirilir. Bu noktada e-devlet kapısı projesi çerçevesinde yapılan fayda - maliyet analizine girdi teşkil edebilmesi amacıyla nicel etki analizi uygulanmıştır. E-devlet kapısı projesi özelinde tercih edilen yöntem Bölüm 3.3'deki risk analizi çizelgesinde görülebilmektedir.

2.7.7. Mevcut ve Hedeflenen Kontrollerin Tanımlanması

Varlıkların, tehdit, zafiyet gibi nesnel tanımlamaların yapılması, sonuç ve olasılık kriterleri neticesinde ortaya çıkan risk düzeyi ile birlikte ana sistemin ayakta kalabilmesi için kurum ya da kuruluşun hali hazırda yaptığı kontrollerin sonuca ne kadar etkisi olduğunu tespit etmek açısından önemlidir. Bu noktada ortaya çıkan etkinin yeterli bulunmaması durumunda mevcut riskin azaltılması ya da ortadan kaldırılması amacıyla yeni kontroller

tanımlanması gerekmektedir. Belirlenecek kontrollerin fayda-maliyet dengesinin iyi kurgulanması bu süreçte etkin rol oynamaktadır. E-Devlet kapısı projesi özelinde tercih edilen yöntem Bölüm 3.3'deki risk analizi çizelgesinde görülebilmektedir.

2.7.8. Risklerin Azaltılma Süreci

Risk yönetimi sürecinde, yukarıdaki adımların tespit edilmesi ile birlikte bir değerlendirme raporu üretilir. Raporun üretilmesi ile birlikte yapılacak en önemli faaliyet risklerin azaltılması veya etkisiz hale getirilmesi için yapılacak çalışmalardır.

Çizelge 2.8. Risk Azaltma Süreci

RİSK AZALTMA SÜRECİ		
Girdiler	***Risk Azaltma Aktiviteleri***	***Çıktılar***
• Risk değerlendirme raporunda bulunan risk seviyeleri	1. Adım: Aktiviteleri Önceliklendir	• Aktivitelerin yüksek ile düşük arasında önceliklendirilmesi
• Risk Değerlendirme Raporu	2. Adım: Tavsiye Edilen Kontrol Seçenekleri • Fizibilite • Etkinlik	• Olası Kontroller Listesi
	3. Adım: Fayda & Maliyet Analizi • Uygulama Etkileri, • Uygulanmama Etkileri, • Birleştirilmiş Maliyetleri	• Fayda Maliyet Analizi Raporu sonucuna göre kontrolün uygulanabilirliğinin ortaya konulması
	4. Adım: Kontrol Çeşidi Seçimi	• Kontrollerin seçilmesi
	5. Adım: Sorumlulukların Atanması	• Sorumlu Personel Listesi
	6. Adım: • Riskler ve Seviyeleri, • Önceliklendirilmiş Aktiviteler, • Tavsiye Kontroller, • Hedeflenen Başlama ve Bitiş Tarihi • Gereksinimlerin Devamlılığının Sağlanması	• Uygulama Planı
	7. Adım: Uygulanacak Kontrollerin Seçimi	• Kalan Riskler

Yukarıda verilen Çizelge 2.8'de risk azaltma sürecinde nasıl hareket edilmesi gerektiği hakkında bilgi verilmektedir. E-Devlet kapısı projesi özelinde tercih edilen yöntem Bölüm 3.4'deki önceliklendirilmiş riskler ve planlanan kontroller çizelgesinde görülebilmektedir.

3. ARAŞTIRMA BULGULARI

3.1. E-Devlet Kapısı Projesi Varlık Envanteri

E-Devlet Kapısı Projesi çerçevesinde yapılan risk değerlendirme faaliyetleri içerisinde ilk çalışma ürünü olarak varlık envanteri karşımıza çıkmaktadır. Çizelge 3.1'de görüleceği üzere ülkemize katma değeri yüksek, ve bilgi toplumuna dönüşüm sürecinde bilgiyi yönetebilmemizi ve devlet kurumları ile iletişimimizi güçlendirecek olan e-devlet kapısı platformunun varlık envanteri bulunmaktadır. Envanter incelendiğinde yetmiş yedi ayrı varlık tespit edilmiş ve proje içerisindeki sahibi, proje açısından kıymeti/değeri, konumu gibi bilgileri içeren bir envanter çıkarılmıştır.

Çizelge 3.1. E-Devlet Kapısı Projesi Varlık Envanteri

E-Devlet Kapısı Projesi Varlık Envanteri							
No	Varlık Adı	Adedi	Sahibi	Kıymeti	İş Süreçlerinde Kullanımı	Konumu	Notlar
1	İnternet Bağlantısı	1	Bilgi İşlem	Yüksek		Gölbaşı	
2	Kurum Bağlantıları	Proje bitiminde hedeflenen doğrudan bağlantı sayısı	Ağ ve İletişim	Yüksek		Ulus	
3	Kapı Yerel Ağ Altyapısı	Yerel ağ switch adedi?	Ağ ve İletişim	Yüksek		Gölbaşı	
4	E-posta Sunucusu	2	Sistem Yönetim	Yüksek		Gölbaşı	
5	LDAP Sunucusu	2	Sistem Yönetim	Yüksek		Gölbaşı	
6	DNS Sunucusu	3	Sistem Yönetim	Yüksek		Gölbaşı	
7	NTP Sunucusu	3	Sistem Yönetim	Yüksek		Gölbaşı	
8	Radius Sunucusu	2	Sistem Yönetim	Yüksek		Gölbaşı	
9	Web Sunucusu	2	Sistem Yönetim	Yüksek		Gölbaşı	
10	Portal Sunucusu	2	Sistem Yönetim	Yüksek		Gölbaşı	
11	Kimlik Doğrulama Sunucusu	2	Sistem Yönetim	Yüksek		Gölbaşı	

Çizelge 3.1. e-Devlet Kapısı Projesi Varlık Envanteri **(devam)**

e-Devlet Kapısı Projesi Varlık Envanteri							
No	Varlık Adı	Adedi	Sahibi	Kıymeti	İş Süreçlerinde Kullanımı	Konumu	Notlar
12	Sistem Yönetim Sunucusu	10+	Sistem Yönetim	Yüksek		Gölbaşı	
13	Ağ Yönetim Sunucusu	10+	Sistem Yönetim	Yüksek		Gölbaşı	
14	Güvenlik Yönetim Sunucusu	10+	Sistem Yönetim	Yüksek		Gölbaşı	
15	SQL Server Veritabanı Sunucusu	6	Sistem Yönetim	Yüksek		Gölbaşı	
16	Yedekleme Sunucusu	2	Sistem Yönetim	Yüksek		Gölbaşı	
17	Veri Madenciliği Sunucusu	1	Sistem Yönetim	Yüksek		Gölbaşı	
18	Disk Sistemi	1	Sistem Yönetim	Yüksek		Gölbaşı	
19	Teypler	100+	Sistem Yönetim	Yüksek		Gölbaşı	
20	Teyp Kütüphanesi	1	Sistem Yönetim	Yüksek		Gölbaşı	
21	Teknik Ekip Dizüstü Bilgisayarları	100	Bilgi İşlem	Yüksek		Gölbaşı	
22	Teknik Ekip Avuçiçi Bilgisayarları	50	Bilgi İşlem	Yüksek		Gölbaşı	
23	Akıllı Kartlar	500	Sistem Yönetim	Orta		Gölbaşı	
24	Şifre Basım Yazıcısı	1	Operasyon	Yüksek		Gölbaşı	
25	Lazer Yazıcı	3	Operasyon	Yüksek		Gölbaşı ve Balgat	
26	Yük Testi Sistemi	1	Kalite/Test	Düşük		Gölbaşı	
27	Projeksiyon Cihazı	2	Bilgi İşlem	Orta		Gölbaşı ve Balgat	
28	Kapı Sistem Odası	1	Operasyon	Yüksek		Gölbaşı	
29	Toplantı Odaları	2	Operasyon	Orta		Gölbaşı ve Balgat	
30	İzleme Monitörü	4	Operasyon	Orta		Gölbaşı	
31	Evrak Arşivi	1	Operasyon	Yüksek		Gölbaşı ve Balgat	
32	Malzeme Deposu	1	Operasyon	Düşük		Gölbaşı	
33	Kapı Çalışma Ofisi	2	Operasyon	Yüksek		Gölbaşı ve Balgat	
34	Kapı Test Odası	1	Kalite/Test	Orta		Gölbaşı	
35	Taşınabilir Sabit Diskler	100	Bilgi İşlem	Yüksek		Değişken	
36	USB Flash Diskler	100	Bilgi İşlem	Yüksek		Değişken	
37	Sözleşmeler ve Protokoller	20+	Bilişim Hukuku	Yüksek		Gölbaşı	

Çizelge 3.1. e-Devlet Kapısı Projesi Varlık Envanteri **(devam)**

e-Devlet Kapısı Projesi Varlık Envanteri							
No	Varlık Adı	Adedi	Sahibi	Kıymeti	İş Süreçlerinde Kullanımı	Konumu	Notlar
38	Toplantı Tutanakları	50+	İlgili Birimler	Orta		Gölbaşı ve Balgat	
39	İç Yazışmalar	50+	İlgili Birimler	Orta		Gölbaşı	
40	Diğer Belgeler	100+	Operasyon	Orta		Gölbaşı ve Balgat	
41	Kapı İdari Personeli	10+	Asım Balcı ve Ahmet Kaplan	Yüksek		Gölbaşı ve Balgat	
42	Kapı Teknik Personeli	20+	Asım Balcı ve Ahmet Kaplan	Yüksek		Gölbaşı ve Balgat	
43	Kapı İdari Yöneticileri	4+	Asım Balcı ve Ahmet Kaplan	Yüksek		Gölbaşı ve Balgat	
44	Vatandaş Verileri	70M+	Türksat	Yüksek		Gölbaşı	şifreler de vatandaş verisi olarak ele alınmıştır.
45	İşletme Verileri	1M+	Türksat	Yüksek		Gölbaşı	
46	Kurum Verileri	190+	Türksat	Yüksek		Gölbaşı	
47	Log Sunucusu	3	Operasyon	Yüksek		Gölbaşı	
48	Şifre Zarfları	70M+	Operasyon	Yüksek		Gölbaşı	
49	İnternet Bağlantısı	1	Bilgi İşlem	Yüksek		Ulus	
50	Kapı Yerel Ağ Altyapısı	Yerel ağ switch adedi	Ağ ve İletişim	Yüksek		Ulus	
51	E-posta Sunucusu	1	Sistem Yönetim	Yüksek		Ulus	
52	LDAP Sunucusu	1	Sistem Yönetim	Yüksek		Ulus	
53	DNS Sunucusu	1	Sistem Yönetim	Yüksek		Ulus	
54	NTP Sunucusu	1	Sistem Yönetim	Yüksek		Ulus	
55	Radius Sunucusu	1	Sistem Yönetim	Yüksek		Ulus	
56	Web Sunucusu	2	Sistem Yönetim	Yüksek		Ulus	
57	Portal Sunucusu	1	Sistem Yönetim	Yüksek		Ulus	
58	Oracle Veritabanı Sunucusu	1	Sistem Yönetim	Yüksek		Ulus	
59	PKI ve Akıllı Kart Yönetim Sunucusu	1	Sistem Yönetim	Yüksek		Ulus	
60	Sistem Yönetim Sunucusu	5+	Sistem Yönetim	Yüksek		Ulus	
61	Ağ Yönetim Sunucusu	5+	Sistem Yönetim	Yüksek		Ulus	
62	Güvenlik Yönetim Sunucusu	5+	Sistem Yönetim	Yüksek		Ulus	

Çizelge 3.1. e-Devlet Kapısı Projesi Varlık Envanteri **(devam)**

e-Devlet Kapısı Projesi Varlık Envanteri							
No	Varlık Adı	Adedi	Sahibi	Kıymeti	İş Süreçlerinde Kullanımı	Konumu	Notlar
63	SQL Server Veritabanı Sunucusu	3	Sistem Yönetim	Yüksek		Ulus	
64	Yedekleme Sunucusu	1	Sistem Yönetim	Yüksek		Ulus	
65	Veri Madenciliği Sunucusu	1	Sistem Yönetim	Yüksek		Ulus	
66	Disk Sistemi	1	Sistem Yönetim	Yüksek		Ulus	
67	Teypler	100+	Sistem Yönetim	Yüksek		Ulus	
68	Teyp Kütüphanesi	1	Sistem Yönetim	Yüksek		Ulus	
69	Lazer Yazıcı	3	Operasyon	Yüksek		Ulus	
70	FKM Sistem Odası	1	Operasyon	Yüksek		Ulus	
71	Toplantı Odaları	2	Operasyon	Orta		Ulus	
72	İzleme Monitörü	4	Operasyon	Orta		Ulus	
73	Kimlik Doğrulama Verileri	70M+	Türksat	Yüksek		Ulus	
74	FKM Çalışma Ofisi	2	Operasyon	Yüksek		Ulus	
75	Vatandaş Verileri	70M+	Türksat	Yüksek		Ulus	
76	İşletme Verileri	1M+	Türksat	Yüksek		Ulus	
77	Kurum Verileri	190+	Türksat	Yüksek		Ulus	

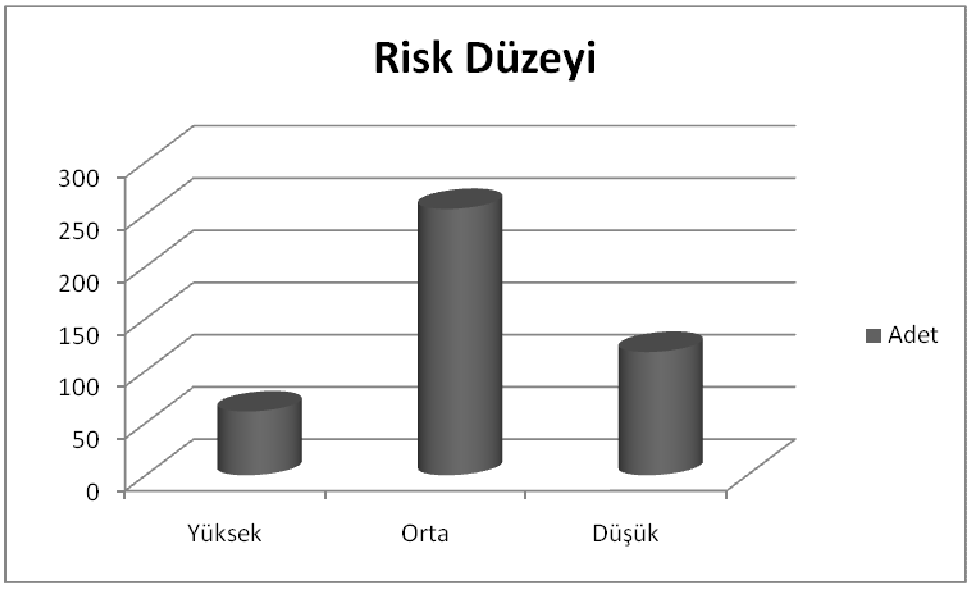
Çizelge 3.1 incelendiğinde e-devlet kapısı projesi bünyesinde yapılan varlık envanteri çalışmasında üç seviye (yüksek, orta, düşük) şeklinde kıymetlendirilme yapılmış; yetmiş yedi varlıktan altmış beş tanesinin yüksek, on tanesinin orta ve iki tanesinin de düşük düzeyde kıymete sahip olduğu tespit edilmiştir. %85'i yüksek düzeyde kıymete sahip olan bu envanter, Türkiye'nin bilgi toplumu yolunda önemli bir projesi olan; e-devlet kapısı projesinin önem katsayısının yüksek olması itibarıyla mevcut risk seviyesi oldukça manidardır. Bu durum aşağıda Şekil 3.1'de görülebilmektedir

Şekil 3.1. Adet ve Varlık Önem Düzeyi İlişkisi

3.2. E-Devlet Kapısı Projesi Risk Düzeyleri Matrisi

Yapılan risk değerlendirme çalışmalarında tespit edilmiş varlık envanteri içerisindeki ögelerin olasılık ve potansiyel sonuç düzeylerinin nasıl tespit edileceğine dair Bölüm 2'de Çizelge 2.5'te aktarılmış olan risk düzeyi matrisi üretilmiştir. Bu matris ışığında tespit edilmiş yetmiş yedi varlık ile ilgili ortaya çıkarılmış zafiyetler, tehditler değerlendirilmiş ve potansiyel sonuç skalasına göre Bölüm 3.3'teki risk analizi tablosu üretilmiştir.

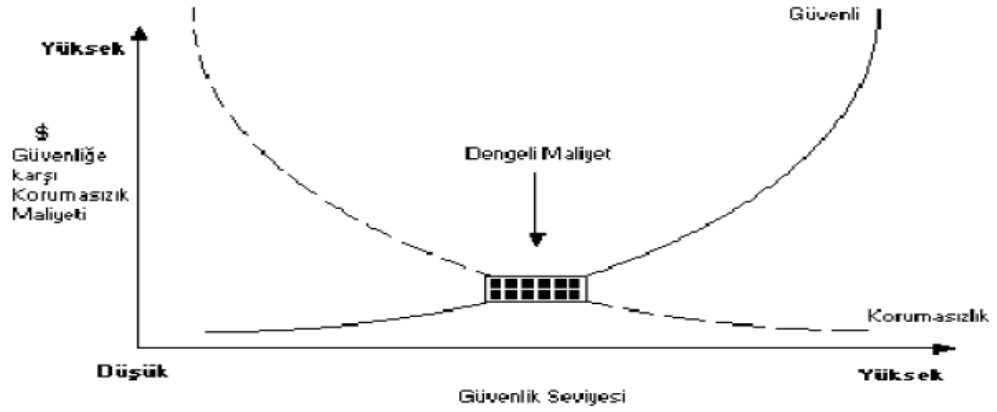
Risk analizi Çizelge 2.4 ve Çizelge 2.5'teki kriterler ışığında irdelendiğinde tespit edilmiş olan toplam dörtyüz otuz dört riskten altmış bir tanesi "yüksek", iki yüz elli beş tanesi "orta" ve yüz onsekiz tanesi "düşük" riks düzeyinde çıkmıştır. Bu durum Şekil 3.2 'de görülebilmektedir.



Şekil 3.2. Adet ve Risk Düzeyi İlişkisi

3.3. E-Devlet Kapısı Projesi Risk Analizi Tablosu

Risk analizi proje yönetimi çalışmaları içerisinde önemli bir yer tutmaktadır. Bu durum özellikle yazılım projeleri irdelendiğinde daha da netleşmektedir. Risk analizi ile proje başarı performans'ı arasında doğrudan bir bağ bulunmaktadır[21]. Birçok bilimsel çalışma göstermiştir ki; iyi bir risk analizi çalışması, proje varlıklarının tespit edilmesi, risk olasılığı ve projeye olan etkisi, risk önem düzeyi ve fayda-maliyet dengesinin korunması gibi kriterleri kapsamalıdır. Aynı şekilde Şekil 3.3'te görüleceği üzere yapılan risk analizi neticesinde ortaya çıkan durumun fayda-maliyet dengesi gözetildiğinde güvenliğe karşı korumasızlık maliyeti ile güvenlik seviyesi arasında ters bir orantı görülebilmektedir.



Şekil 3.3. Güvenlik ve Korumasızlık Bütçe Dengesi[28]

E-Devlet Kapısı Projesi özelinde yapmış olduğumuz risk analizi çalışması Çizelge 3.2 ’de görülebilmektedir. Bu çalışma çerçevesinde toplam dörtyüz otuz dört adet risk tespit edilmiştir. Tespit edilen bu risk’ler değerlendirmelere tabi tutulmuş, proje yönetimi ekibi ile yapılan toplantılar sonucunda hangi risklerin kabul edileceği, hangi risklerin iyileştirmelere tabi tutulacağı kararlaştırılmıştır. Bu durum ile ilgili Bölüm 3.4’de detaylı bilgi görülebilmektedir.

3.4. E-Devlet Kapısı Projesi Önceliklendirilmiş Risk Tablosu

E-Devlet Kapısı Projesi çerçevesinde elde edilen risk analizi tablosu Çizelge 3.2'de verilmişti. Bu çizelge üzerinden hareketle yapılan önceliklendirmede, kabul edilen riskler yani iyileştirmenin mümkün olmadığı riskler ve ele alınarak yeniden işlenecek riskler şeklinde bir çalışma yapılmıştır. Bu çalışmanın neticesinde de risk işleme önceliklerinin görülebileceği bir tablo üretilmiştir.

Kabul Edilen Riskler*;* Başka bir ifade ile iyileştirmenin mümkün olmadığı riskler Çizelge 3.3 'te görülmektedir.

Çizelge 3.3. Kabul Edilen Riskler

Sonuç	Risk Satırı
Kabul Edilen Riskler	29-35-36-37-39-40-42-51-54-55-56-63-64-65-72-73-74-81-82-83-89-90-91-97-98-99-109-110-121-122-134-135-144-145-155-156-165-166-177-178-188-189-197-199-202-209-210-212-213-221-229-230-231-232-240-246-247-250-253-255-256-257-258-259-260-264-267-269-270-271-272-273-274-278-288-293-294-295-296-297-298-299-304-305-306-307-308-309-310-315-316-317-318-319-320-321-326-327-335-336-339-344-345-346-349-350-351-352-353-354-355-356-357-358-359-360-361-362-363-364-365-366-367-368-369-370-371-372-373-374-375-376-377-378-379-380-381-382-383-384-385-386-387-388-389-390-391-392-393-394-395-396-397-398-399-400-401-402-403-404-405-406-407-408-409-410-411-412-413-414-415-416-417-418-419-420-421-422-423-424-425-426-427-428-429-432-433-434

Kabul edilen risklerin bir bölümü maliyet etkinliğinden bağımsız olarak proje bünyesinde yapılabilecek tüm iyileştirmelere rağmen ortadan kaldırılamayan, azaltılamayan ya da transfer edilemeyen risklerdir.

Kabul edilen risklerin başka bir tarafı ise maliyet etkin olmaması nedeniyle iyileştirmelerin yapılamadığı risklerdir. Bu türden riskler bir sonraki periyotta gerçekleştirilecek risk analizinde tekrar ve öncelikli olarak gözden geçirilecek, değişen koşullar doğrultusunda iyileştirme imkanları araştırılacaktır.

Ele Alınacak Riskler*;* Ele alınması hedeflenen riskler ve ilgili kontrollere ilişkin hedeflenen iyileştirmeler Çizelge 3.4'te verilmektedir. Riskler sırası ile hedeflenen risk düzeyi (azalan), kontrol maliyet etkinliği (azalan) ve mevcut risk düzeyi (azalan) sırası ile verilmiştir. Bir sonraki aşamada da bu risklerin giderilmesi için önceliklendirilmiş iyileştirme planı yer almaktadır.

Çizelge 3.4. Ele Alınacak Riskler

Sonuç	Risk Satırı
Ele Alınacak Riskler	78-103-30-14-28-80-106-38-3-4-5-17-18-19-76-85-101-102-104-105-107-108-111-112-113-114-115-116-117-118-119-120-239-11-13-25-27-31-32-41-43-44-45-46-47-57-58-59-60-61-66-67-68-69-70-75-77-84-86-95-100-123-124-125-126-127-136-137-138-139-140-146-147-148-149-157-158-159-167-168-169-170-179-180-181-182-190-191-193-198-205-206-207-217-220-224-225-226-236-243-244-245-262-265-266-276-279-280-281-282-283-284-285-286-289-290-300-328-329-331-92-93-94-192-200-201-203-204-216-218-219-222-223-235-237-238-241-242-311-322-324-330-337-430-431-6-20-1-2-7-8-9-10-15-16-21-22-23-24-79-87-88-227-248-12-26-33-34-48-49-50-52-53-62-71-96-128-129-130-131-132-133-141-142-143-150-151-152-153-154-160-161-162-163-164-171-172-173-174-175-176-183-184-185-186-187-194-195-196-208-211-214-228-233-234-249-251-261-263-268-275-277-287-291-292-301-303-332-333-334-340-341-342-343-347-348-254-302-312-313-314-323-325-338-252-215

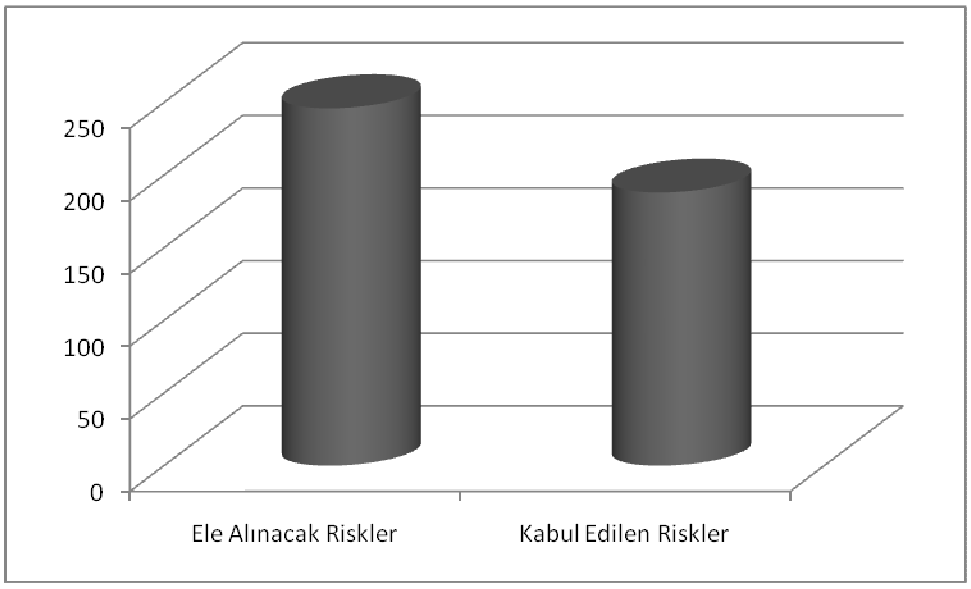
Belirlenen iyileştirici kontrollerin bir bölümü birden fazla riskin giderilmesine katkı sağlayacak niteliktedir. Bu açıdan bakıldığında planlanan kontrollerin önceliklendirilmiş bir listesi Çizelge 3.5'deki gibidir:

Çizelge 3.5. Önceliklendirilmiş Riskler ve Planlanan Kontroller

Sıra No	Planlanan Kontrol	İlgili Riskler
1	İşlem kaydı tutulması	104,105,107,108, 115, 119, 120, 95, 127, 79, 87, 48, 52, 53, 128, 129, 130, 131, 132, 141, 142, 143, 150, 151, 152, 153, 154, 160, 161, 162, 163, 164, 171, 172, 173, 174, 175, 176, 183, 184, 186, 187, 194, 196, 334, 47, 61, 70, 332,
2	Merkezi kayıt sunucusu kullanımı	104,105,107,108, 115, 119, 120, 95, 127, 79, 87, 48, 52, 53, 128, 129, 130, 131, 132, 141, 142, 143, 150, 151, 152, 153, 154, 160, 161, 162, 163, 164, 171, 172, 173, 174, 175, 176, 183, 184, 186, 187, 194, 196, 334, 47, 61, 70, 332,
3	Değişiklik kontrol prosedürü	4,5,18,19,76,85,101,102, 112, 113, 31,32, 44, 45, 58, 59, 67, 68, 77, 86, 124, 125 137, 138, 147, 148, 158, 159, 168, 169, 180, 181, 191, 329, 93, 94, 192, 200, 201, 218, 219, 237, 238, 330, 430, 431,
4	Güçlü kimlik doğrulaması	78, 103, 114, 117, 118, 11, 25, 60, 69, 126, 139, 140, 149, 170, 182, 193, 331, 290, 314, 323, 325, 292, 301, 303, 312, 185, 195, 333,
5	Etkin güncelleme yönetimi	78, 103, 38, 114, 117, 118, 11, 25, 60, 69, 126, 139, 140, 149, 170, 182, 193, 331, 13, 27, 46, 185, 195, 333,
6	Bütünlük denetimi yazılımı ile kontrol	14,28,80,106, 104,105,107,108, 117, 118, 115, 119, 120, 95, 127, 79, 87, 48, 52, 53, 128, 129, 130, 131, 132, 141, 142, 143, 150, 151, 152, 153, 154, 160, 161, 162, 163, 164, 171, 172, 173, 174, 175, 176, 183, 184, 186, 187, 194, 196, 334, 88, 12, 26, 49, 50, 62, 71, 96, 185, 195, 333, 332,
7	Periyodik yedekli çalışma testi	30,3,17
8	Zafiyet veritabanlarının düzenli incelenmesi	38, 13, 27, 46,
9	Acil durum müdahale planlaması	38, 13, 27, 46,
10	Kabinetlerin kilitli tutulması	111,43,57,66,75,84,100,123, 136,146,157,167,179, 190, 328, 92,
11	Görev kritik PC'ler ve Laptop'lar için imaj alınması	200,201,203, 204, 216, 218, 219, 222, 223, 195, 205, 206, 207, 220, 224, 225, 266,
12	Görev kritik avuçiçi sistemler için imaj alınması	235, 237, 238, 241, 242, 239, 243, 244, 245,
13	Bağlantı yedeklemesi	6,20,1, 8,9, 10, 15, 22, 23, 24, 2, 7, 16, 21
14	Servis sağlayıcının DoS koruması	2, 16
15	Uçsistem güvenliği ve NAC	7, 21, 34, 211, 214, 228, 233, 234, 249, 251, 252, 215,
16	Disk şifrelemesi	208, 261, 263, 268, 275, 277, 227, 248, 254,
17	Şifrelenmiş yedekleme	340, 341, 342, 343, 347, 348,
18	Sözleşmelerin bilgisayar dosyası olarak saklanması	281, 282, 283, 284, 285, 286,
19	Veri yedeklemesi	314, 323, 325, 292, 301, 303, 312,
20	Disklerin başka kullanıcılar ile paylaşılmaması	262, 265, 266, 276, 279, 280,
21	Temiz masa politikası uygulaması	289, 300, 311, 322,
22	Arşiv sorumlusu atanması ve fiziksel erişim kontrolü	313, 302, 287, 291, 324,

23	Yedekleme prosedürü oluşturulması	337
24	Kablo kanallarının güvenliğinin sağlanması	33
25	E-posta limitlerinin tanımlanması	41
26	Bilgisayarların yalnızca Türksat uzmanları nezaretinde/tarafından kullanılması	217, 236,
27	Yedeklerin FKM'ne gönderilmesi	338
28	PKI yönetimi için ikili kontrol	133

Şu ana kadar yapılan değerlendirme ve analizler neticesinde e-devlet kapısı projesi bünyesinde tespit edilen 434 adet risk'ten 188 tanesi kabul edilmiş risk'tir. Yani proje yönetim ekibi ile yapılan toplantılarda projenin genelini zor durumda bırakmayacak, projenin devamlılığına engel teşkil etmeyecek ve değerlendirmeye alındığı takdirde sonucun maliyeti'nin faydasından büyük olduğu risklerdir.



Şekil 3.4. Kabul Edilen ve Ele Alınacak Riskler

Geriye kalan 246 risk ise ele alınmaya değer, projenin genelini tehlikeye atabilecek düzeyde ve proje yönetimi ekibi ile değerlendirildiğinde sonucun maliyeti, faydasından büyük olsa da değerlendirme zorunluluğu olan risklerdir. Bu durum Şekil 3.4'te özetlenmiştir.

4. TARTIŞMA VE SONUÇ

Bilgi ve iletişim teknolojilerinin gelişimi ile küreselleşmenin durdurulamayan hızı arasında, birbirini tetikleyen, biri diğerinin hem sonucu ama aynı zamanda nedeni olarak da okunabilecek karşılıklı bir ilişki vardır. Bugün gerek kuramcılar gerekse konu ile ilgili olan kurum ve kuruluşlar söz konusu karşılıklı ilişkinin beraberinde getirdiği sorunlara yönelik çözüm önerileri geliştirme veya sunduğu kolaylıklar, güç ve fırsatlar konusunda pay sahibi olma yolunda çeşitli teknik ve metodolojiler geliştirmeye çalışmaktadır[23].

Bu çalışma, günümüz küresel dünyasında bilgi ve iletişim teknolojilerinin her geçen gün artan önemini kavrayan; ülke kalkınmasını ve toplumsal refahı hedeflerken, söz konusu teknolojilerin yaygınlaştırılması ve etkin kullanımıyla hem kamu yönetimi kurumları, hem vatandaşlar hem de işletmeler açısından faydalarına odaklanan; 2006–2010 Bilgi Toplumu Stratejisi eki Eylem Planı'nın, ve e-Dönüşüm Türkiye Projesi'nin geliştirilmesine yönelik bilgi güvenliği ve risk yönetimi anlamında bir model niteliğindedir. Temel referans metni 2006–2010 Bilgi Toplumu Stratejisi ve e-Dönüşüm Türkiye Projesi olan bu çalışma[1]; gerek Türkiye'nin dönüşüm politikaları açısından gerekse bilgi toplumu uzanımında söz konusu e-devlet kapısı projesi'nin oturtulmaya çalışıldığı teorik zemine ilişkin bilgi verme amacı taşımaktadır.

10 Haziran 2004 tarihli, e-Dönüşüm Türkiye İcra Kurulu kararı ile kabul edilen Bilgi Toplumuna Dönüşüm Politika Belgesi'nde Türkiye'nin bilgi toplumuna dönüşümdeki vizyonu; ***bilim ve teknoloji üretiminde odak noktası haline gelmiş, bilgi ve teknolojiyi etkin bir araç olarak kullanan, bilgiye dayalı karar alma süreçleriyle daha fazla değer üreten, küresel rekabette başarılı ve refah düzeyi yüksek bir ülke olmak*** ifadeleri ile ortaya konulmuştur(24).

Bilgi güvenliği konusunda daha önceden alınmış eğitimler, bilgi güvenliğinin sağlanmasında risk yönetimi konusunda katılım sağlanan ulusal ve uluslar arası seminerler, bilgi güvenliğiyle ilgili uluslar arası alanda sahip olunan sertifikalar, e-devlet kavramı ile ilgili çeşitli üniversitelerde verilen seminerler, 5 yıllık sektörel çalışmalardan elde edilen bilgi birikimi ve deneyimler ile yapılan pratik uygulamalara dayanılarak kurumsal anlamda risklerin yönetilmesinde yapılması gerekenler, alınması gereken önlemler, atılması gereken adımlarla e-devlet kapısı projesi özelinde bilgi güvenliğinin sağlanmasında risk yönetiminin nasıl sağlanacağı üzerinde durulmuştur.

Bu tez çalışması çerçevesinde bilgi güvenliğinin sağlanması sürecinde risk yönetiminin yapılabilmesi için; şirket içi ve dışı tehditlerin tespit edilmesini sağlamak, gerekli tedbirleri almak ve alınmasını sağlamak, bu süreçte kapsam, ilke, politika, standartları tespit etmek, geliştirmek ve onaylamak gerekmektedir. Aynı şekilde; proje bünyesindeki bilgilerin gizlilik, bütünlük ve erişilebilirlik ilkelerine uygun olmasını sağlayacak şekilde gerekli tedbirleri almak ve bunları kontrol altında tutmak gerekmektedir. Risk yönetimi bakış açısı içerisinde kurumsal bir model geliştirmek ve bu modele uygun risk

analizi ve risk değerlendirmesi yapmak ve yapılmasını sağlamak, üretilmiş çıktılara göre yönetsel beceri geliştirmek, üst yönetimin karar alma mekanizmalarına güvenilir girdi sağlayabilmek oldukça önemlidir[25].

İnternet teknolojileri üzerinden temin edilen raporlama içerikleri, biri diğerinin müşterisini çalmaya çalışan bankalar, VISA raporlarına yansımış kredi kartı işlemleri artan vatandaşlar, uydu yayını ya da kablolu yayın hizmeti veren şirketlerin birbirinin akıllı kart teknolojilerini kopyalamaya çalışması veya hukuki zemini tam olarak oturtulamamış "siber alem"in kontrol altına alınması gibi bilgi ve iletişim teknolojileri ile ister istemez ilgilenmek zorunda olan biz vatandaşları her gün bekleyen ya da karşılaştığımız sorunlardan ötürü bilgi güvenliği önem arz etmektedir[26].

Devlet kurumlarına ait hizmetlerin e-devlet kapısı altyapısı üzerinden sunulması, kamu elektronik hizmetleri ve bu elektronik hizmetlerin sunumundaki etkinlik, ülkemizin ekonomik ve sosyal yaşamı üzerinde ve bilgi toplumuna dönüşüm sürecinde büyük etkiye sahiptir. Bu açıdan, bilgi toplumuna dönüşüm sürecinde kamu hizmetlerinin, vatandaşlar ve iş dünyasının ihtiyaç ve beklentilerine uygun olarak, bilgi ve iletişim teknolojilerinin de yardımıyla etkin, hızlı, kaliteli, sürekli, güvenilir, şeffaf ve bütünleşik şekilde sunumu önem arz etmektedir. Bu dönüşüm sürecinin bir unsuru olan e-devlet olgusu, sadece hizmetlerin elektronik kanallara taşınması anlamına gelmemekte; bunun yanı sıra verimli iş süreçlerine, kurumlar arası işbirliği yeteneğine, ortak vizyona ve en önemlisi bilgi güvenliğini önceleyen, bilgiye dayalı kamu yönetimi anlayışını ifade etmelidir.

Her geçen gün e-toplum olma yolunda hızla ilerleyen ve e-devletleşme çalışmalarını sürdüren ülkemizde, maalesef bilgi güvenliğinin öneminin kamu veya özel sektör tarafından kavranmadığı veya yüksek seviyede bir farkındalığın oluşmadığı bu çalışma sonucunda tespit edilen en önemli bulgulardan birisidir. Ülkemizde bilgi güvenliği konusunda yapılan araştırmalar incelendiğinde bilgi güvenliğinin sağlanmasında dünya standartlarının altında kaldığımız görülmektedir. Bunun için ülkemizde bilgi güvenliği konusunda daha çok araştırma ve geliştirme çalışmalarına ihtiyaç duyulmaktadır.

Tez içerisinde bilgi güvenliği kavramının literatür içerisinde nasıl yer bulduğu, bilginin üretilmesi kadar saklanmasının da önemli olduğuna yer verilmiştir. Bu üretim ve saklama sürecinde karşılaşılabilecek olası açıklıklar, zafiyetler, tehditler ve risklerin neler olabileceği konusuna değinilmiştir. Sistem yaklaşımı içerisinde değerlendirilen bilgi güvenliği ve risk yönetimi süreci ile ilgili öneriler sıralanmış ve karşılaşılabilecek zorluklar hakkında bilgiler sunulmuştur. Türkiye şartlarında bilgi güvenliği kavramı ile ilgili durum değerlendirilmesi yapılırken, özel olarak irdelenen e-devlet kapısı projesi ile ilgili eksiklikler ve gözlemler tariflenmiştir. Uluslar arası platformlarda kabul görmüş ve uygulama alanı bulmuş model ve metodolojilerden bahsedilmiştir. Türkiye kamu yapısına, özel sektörün çalışma dinamiklerine uygun bir metodoloji türetilmeye çalışılmıştır. Üretilen bu metodolojinin e-devlet kapısı projesi özelinde nasıl çalıştığı aktarılmıştır.

E-Devlet kapısı projesi bünyesinde yapılan risk değerlendirme ve risk analizi çalışmaları esnasında tespit edilen önemli noktalar, dikkat edilmesi gereken bulgular ve alınması gereken tedbirler ile ilgili detaylı veriler elde edilmiş ve paylaşılmıştır. Risk yönetimi bakış açısı içerisinde yürütülmüş olan bu süreçte; varlık envanterinin nasıl oluşturulması gerektiğinden, risk düzeyleri matrisinin üretilmesine, analizi yapılmış risklerin ortaya konulmasından, önceliklendirilmiş risklerin tariflenmesine varan geniş yelpazede konu işlenmiştir. Çizelge 1.1'de görselleştirildiği üzere Türkiye olarak bilgi güvenliği konusunda dünya ülkelerine nazaran oldukça gerilerde olduğumuz göz önünde bulundurulacak olursa; yapılan gerçek uygulamanın ve değerlendirmelerin önemi bir kez daha anlaşılmış olacaktır.

Bu çalışma ile bilgi güvenliği ve risk yönetimi kavramlarının uygulama sahasındaki karşılığı olarak literatür içerisinde rahatlıkla faydalanılabilecek bir Türkiye uygulaması sunulmuştur. Ulusal bilgilerin güvenliği, Türkiye'de sağlık, eğitim, silahlı kuvvetler, ulaştırma, hukuk, teknoloji ve diğer birçok alanda hizmet veren kurum ve kuruluşların bilgilerinin güvenliğinin sağlanmasına bağlıdır. Bu bağlamda kurumların bilgi güvenliği sadece kurumların kendisi için değil ulusal güvenliğimiz için de gereklidir. Tez içerisinde vurgulanan önemli noktalardan birisi de devletimizin eğitim çalışmalarına bakış açısı ile bilgi güvenliği kavramının nasıl ve hangi zeminlerde örtüştürülebileceği tartışmasıdır. Önerimiz; bilgi güvenliğinin devletimizin hem kurumsal yapılanması içerisinde, hem de eğitim stratejileri belirlenirken hak ettiği öneme uygun değerlendirilmesidir.

Bilgi güvenliğinin sağlanmasına yönelik risk analizi ve risk değerlendirme kavramlarını kapsayan risk yönetimi süreci ile ilgili kurumsallaşmasını sağlayamamış firmalardan, özel sektörün lider firmalarına, kamu kurum ve kuruluşlarından, kurulması planlanan özerk bilgi güvenliği kurumuna kadar bir çok yerde kullanılabilecek yazılımlar geliştirilebilir. Ortaya konulmuş olunan metodolojinin bir yazılım ile desteklenerek kullanıcılara katma değer sağlaması beklenen faydayı artıracaktır.

5. KAYNAKLAR

1. Bilgi Toplum Stratejisi ve Eki Eylem Planı, http://mevzuat.dpt.gov.tr/ypk/2006/38.htm, Devlet Planlama Teşkilatı, Ankara, 2006, [Erişim tarihi: 12.12.2008].

2. E. Kumaş, M. Acar, Kamu Hizmetlerinin Sunumunda Dönüm Noktası: e-Devlet, e-Dönüşüm ve Entegrasyon Standartları, 17. İstatistik Araştırmalar Sempozyumu Bildiriler Kitabı, 1-18, TÜİK, Ankara, 2008.

3. Bakanlar Kurulu Kararı, 2006/10316 sayılı Bakanlar kurulu kararnamesi, Resmi Gazete, 20 Nisan 2006.

4. E-Devlet Kapısı Projesi Teknik Şartnamesi, Türksat Uydu Haberleşme ve İşletme A.Ş., Ankara, 2007.

5. Number of Certificates Per Country, http://www.iso27001certificates.com/, [Erişim tarihi: 16.05.2009].

6. D.Atılgan, Bilgi Yönetiminin Gelişimi, Ulusal e-Devlet Konferansı, www.edevletkonferansi.org/sunum/dogan_atilgan.ppt , 2008. [Erişim tarihi: 16.06.2009].

7. A.Toffler, The Third Wave, Bantam Books, NewYork, 1980.

8. TS ISO/IEC 27001:2005, Bilgi Teknolojisi-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-Gereksinimleri, Türk Standartları Enstitüsü, Ankara, 2005.

9. Bilişim Güvenliği Kitapçığı, Pro-G ve Oracle, http://www.pro-g.com.tr/whitepapers/bilisim-guvenligi-v1.pdf, 2003, [Erişim tarihi:14.05.2009].

10. G.H.Eduljee, Trends in Risk Assessment and Risk Management, The Science of the Total Environment, 13-23, 2000.

11. E. Kumaş, e-Devlet Kapısı ve Risk Değerlendirme Metodolojisi, Türkiye'de İnternet Konferansı – İnet-tr Bildiriler Kitabı, 174-180, Ankara, 2007.

12. E. Kumaş, Kurumlar Üstü Bilgi Güvenliği Stratejisi, Uluslar Arası Katılımlı Bilgi Güvenliği ve Kriptoloji Sempozyumu Bildiriler Kitabı, 102-107, Ankara, 2007.

13. M.Gerber, R. Von Solms, Management of Risk in the Information Age, Computer & Security, Vol - 24, 16-30, 2005.

14. P.L.Bannerman, Risk And Risk Management in Software Projects: A Reassessment, The journal of systems and software, Vol – 81, 2118-2133, 2008.

15. İ. Kaplan, Bilgi Güvenliği ve Kurumsallaşma Sunumu, Bilgi Güvenliği Günleri Semineri, TSE, Dr.kaplan@de.ibm.com, 2007.

16. S. Akleylek, C. Çimen, E. Akyıldız., Şifrelerin Matematiği: Kriptografi, ODTÜ Yayıncılık, 2007.

17. Resmi Yazışma Kuralları, 1994/40 Sayılı Başbakanlık Genelgesi, Başbakanlık Personel ve Prensipler Genel Müdürlüğü, Ankara, www.rega.gov.tr, 2003, [Erişim tarihi: 13.05.2009].

18. B. Sankur, Bilişim Sözlüğü, Pusula Yayıncılık, Ankara, 2008.

19. COBIT, Control Objectives for Information and Related Technology, Version 4.1, IT Governance Institute, IL 60008 USA, 2005.

20. ITIL, Information Technology Infrastructure Library, http://www.itil.co.uk , [Erişim tarihi: 14.09.2009].

21. W. Han, S. Huang, An Empirical Analysis of Risk Components and Performance on Sofware Projects, The Journal of Systems and Software, Vol – 80, 42-50, 2006.

22. G. Durmuş, Risk Analizi, Tapu ve Kadastro Genel Müdürlüğü, Ankara, 2003.

23. H. Taşdelen, M. Heybet, A. Sezen, Bilgi Toplumunda e-Ulaştırma Dünya Örnekleri, T.C. Ulaştırma Bakanlığı, 2008.

24. Bilgi Toplumu Politika Belgesi, Devlet Planlama Teşkilatı, www.bilgitoplumu.gov.tr, Ankara, 2006. [Erişim tarihi: 14.09.2009].

25. Y. Vural, Kurumsal Bilgi Güvenliği ve Sızma (Penetrasyon) Testleri, Yüksek Lisans Tezi, Gazi Üniversitesi, Ankara, 2007.

26. R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, Cambridge, 2001.