e-DEVLET KAPISI ve RİSK DEĞERLENDİRME METODOLOJİSİ

Erhan KUMAŞ
Türksat Uydu ve Kablo TV Operatörü İşletme A.Ş.,
Bilgi Teknolojileri Direktörlüğü
Konya Yolu 40. Km. Gölbaşı/ANKARA
ekumas@turksat.com.tr

ÖZET : 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 güvenliği sağlanması, altyapı ile ilgili risklerin değerlendirilmesi ve yönetilmesi ile ilgili ulusal bir metodoloji ve yaklaşımın bulunmaması bu yazının önemine vurgu yapmaktadır. Yazılım projelerinin problemlerinin yanısıra ortaya konulan teorik yaklaşıma uygulama eklenerek geliştirilmesi öngörülmektedir.

ANAHTAR KELİMELER: *Bilgi Güvenliği, e-Devlet Kapısı, Risk Yönetimi*

SUBJECT OF PAPER

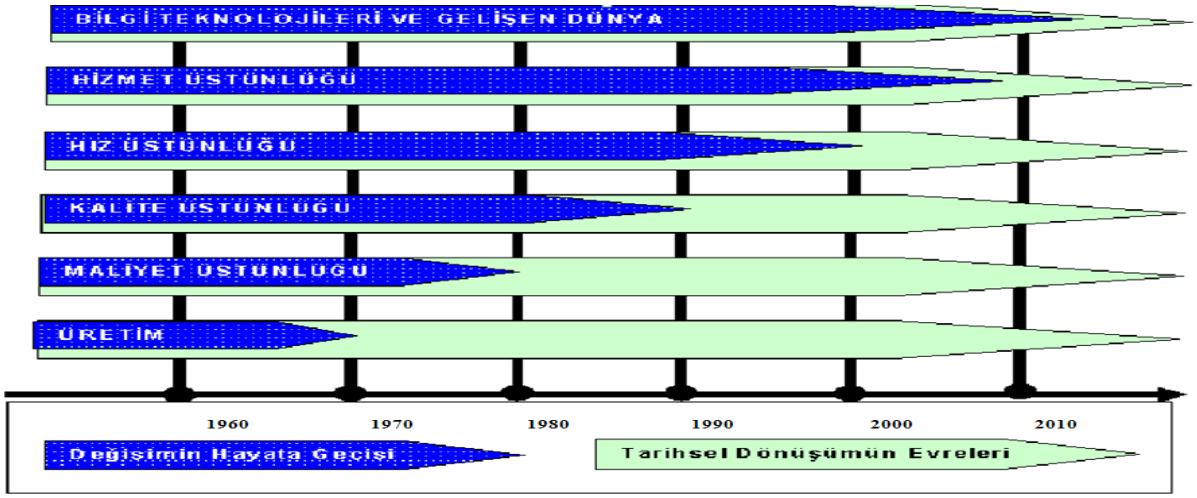
E-Government And Evaluatıng Rısk Methodology

ABSTRACT : 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, lacking a national methodology and an approach about maintaining the security of the information which is being conducted, evaluating and managing the risks of the substructure emphasizes the importance of this essay. It is foreseen that in addition to problematics of the software projects, the theoretical approach which is introduced should be developed with practice.

KEYWORDS : *Information Security, eGovernment Gateway, Risk Management*

1. GİRİŞ

Geçtiğimiz yarım asırda yaşanan sektörel değişime belirli periyotlarda hızlı bir göz atacak olursak; 1960_1970 yılları arasında "Üretim ve Maliyet Üstünlüğü", 1960-1980 yılları arasında "Kalite Üstünlüğü", 1980-1990 yılları arasında "Hız Üstünlüğü", 1990-2000 yılları arasında "Hizmet Üstünlüğü" ön plana çıkmaktadır.[1] Bu noktada bizim düşüncemizde 2000'li yıllarla beraber yaşanan hızlı teknolojik gelişmeler ve internetin yaygınlaşmasının bir sonucu olarak bilgi güvenliği, bilgi teknolojileri giderek önem kazanan bir konu haline gelmiştir. Şekil 1 Bilgi teknolojileri ve bilgi güvenliği gerek kamu kurumlarının, gerekse özel sektörün önümüzdeki dönemde öncelik listesinde giderek artan bir öneme sahip olacağı bilgi güvenliği alanına gereken önemi vermeye başlayacakları, ilgili önlemleri alma çabası içine girecekleri kuşkusuz görülmektedir. Ancak, bilgi teknolojileri ve bilgi güvenliğinin sadece teknolojik önlemlerle sağlanabileceği gibi genel bir yanılsamanın olduğu da gözlenmektedir.



Şekil 1: Yarım Asırlık Sektörel Değişim

Bu çalışmada bilişim güvenliği çerçevesinde ele alınan risk analizi ve risk değerlendirme çalışmalarının temel kavramları, en önemli bileşenleri ve e-devlet kapısı özelinde kısmi uygulamaları ele alınmaktadır. Konunun esas olarak çok boyutlu ve karmaşık bir süreç olmasından hareketle ve niş bir alan olması sebebiyle gerek kamu kurumları, gerekse özel sektör temsilcileri bu konuda ortak paydada buluşmada zorlanmaktadırlar.

2. E-DEVLET KAPISI, BİLGİ GÜVENLİĞİ VE RİSK YÖNETİMİ

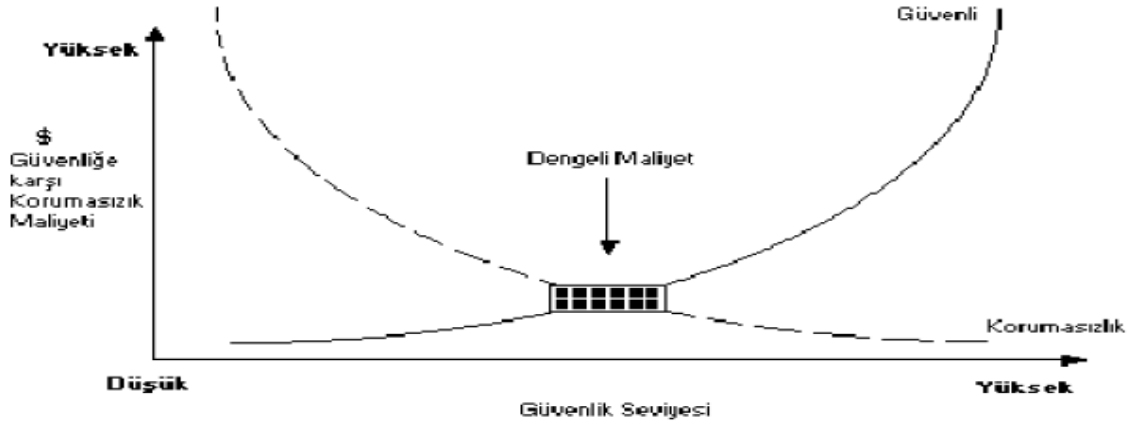
e-Devlet, kamu hizmetlerinin vatandaşlara, işletmelere, kamu kurumlarına ve diğer ülkelere bilgi ve iletişim teknolojileri yardımı ile etkin ve verimli bir şekilde sunmaktır. e-Devlet Kapısı Projesi, Türkiye'nin devlet hizmetlerinin modernizasyonunu ve vatandaşların bu hizmetlere kolay ve rahat ulaşabilecekleri bir platformun kurulmasını amaçlamaktadır. Gerek vatandaşların ve işletmelerin, gerekse kamu kurum ve kuruluşlarının aktif olarak kullanacağı bu platformun güvenli olması yadsınamaz bir gerçektir. Bu noktada e-Devlet kapısı projesi teknik şartnamesi[2] çerçevesinde teknik ve teknolojik açıdan gerekli tedbirler alındığı gibi bir de idari açıdan bu konuda uluslararası arenada kabul görmüş ve geçerliliği olan ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemi[3] kurulumu çalışmaları başlatılmıştır. Bahsi geçen standart incelendiğinde risk analizi çalışmalarının standardın önemli bir kısmını tuttuğu görülmektedir. E-Devlet Kapısı'nın güvenlik altyapısının kurulması ve işletilmesi çalışmaları çerçevesinde ortaya koyduğumuz ve kullandığımız metodoloji Tablo 1'deki gibidir.[7] Bu metodoloji içerisinde geçen iş paketleri adım adım açıklanarak çalışmamıza yön verilecektir.

3. *E-DEVLET KAPISI RİSK DEĞERLENDİRME METODOLOJİSİ*

Bilgi ve iletişim sistemlerine olan bireysel ve toplumsal bağımlılığımız ve sistemlerde meydana gelebilecek arıza ve saldırılara karşı duyarlılığımız arttıkça bu sistemlerde oluşabilecek arıza ve saldırılara karşı hassasiyetimiz de artmaktadır. Bilgi teknolojilerine ve bilgi ağlarına yönelik saldırılar ciddi miktarda para, zaman, prestij ve değerli bilgi kaybına neden olabilmektedir.

Risk değerlendirme 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 içerebilmektedir.

Şu ana kadar belirtilen süreçlerin bilgi güvenliği açısından değerlendirilmesinde fayda-maliyet analizi'nin Şekil 2'de her çalışmanın başlangıcında olduğu gibi işletmelerin veya kurumların bilgi güvenliği yatırımı'na ayıracakları bütçe ile yapılacak çalışmanın getirisinin önemi arasındaki ince çizgi vurgulanmaktadır.[4]



Şekil 2: Güvenliğe/Korumasızlık Bütçe Dengesi

Varlık Envanteri'nin Çıkarılması:

Sistemin bilgi varlıklarının tanımlanması adımına geçmeden önce yapılması gereken organizasyonun belirlenmesi, rol ve sorumluluk paylaşımı gibi kurumsal kimliğinizin yapıtaşlarının tanımlanmasıdır. Daha sonra ISO 27001:2005 ve ISO 17799:2005 standartları[5] çerçevesinde kurulacak bilgi güvenliği yönetim sistemi kapsamı belirlenmeli ve bu kapsama giren tüm bilgi varlıkları tanımlanmalı ve dokümante edilmelidir.

Tehditlerin Tanımlanması:

Burada yapılması gereken en önemli iş; potansiyel tehdit kaynaklarının tespit edilerek Şekil 3'de bir tehdit listesi oluşturulmalıdır. Sisteme zarar vermesi muhtemel bu tehditler;

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

şeklinde sınıflandırılabilir.

Tehdit Kaynağı	Motivasyonu Nedir?	Tehdit'in Ortaya Çıkardığı Eylemler
Hacker , Kaçık, Psikopat	• Meydan Okuma, • Kendini İspat Etme, • İsyan Etme	• **Sistemin hack'lenmesi,** • **Sisteme izinsiz girme,**
Teröristler	• **Yıkıcı ve bölücü eylem,** • **İstismar etme,** • **İntikam Alma**	• **Bombalama,** • **Bilgi Çalma,** • **Sisteme Saldırma,** • **Sistem ayarlarının bozulması**

Şekil 3: Tehdit Tanımlama Örnek Tablosu

Zayıflıkların Tanımlanması:

Sistemde olası zayıflıkların tespit edilmesi ve bunun istismar edilerek potansiyel bir tehdit kaynağı olup olmama durumunun tanımlanması ile ilgili Şekil 4'deki gibi bir liste çıkarılmalıdır. Sistem zayıflıklarının tanımlanması esnasında asıl kaynağın bulunması için sistem güvenlik test performansları ve sistemin güvenlik gereksinimlerine ait bir kontrol listesinin bulunması gerekmektedir.

Zayıflıklar	Tehdit Kaynağı	Tehdit'in Ortaya Çıkardığı Eylemler
İşten ayrılan personelin sistem ile ilgili ilişiğinin kesilmemesi	İşten Ayrılan personel	İşten ayrılan personelin sisteme ait önemli / patentli bilgileri çalması
Sistemin kurulumundan sorumlu tedarikçilerin sisteme yeni yamalar yaparken güvenlik açıklarını bilmeleri	Yetkisizi kişilerin eline geçmesi	Yetkisiz giriş yaparak hassas sistem dosyalarının çalınması

Şekil 4: Zayıflık Tanımlama Örnek Tablosu

Kontrol Analizleri:

Sistemin genel durumuna ait güvenlik kontrollerinin analizlerinin yapılıp yapılmadığını veya planlanıp planlanmadığını ve organizasyon ile ilgili tehditlerin olma olasılığının belirlendiği kısımdır.

Olasılıkların Belirlenmesi:

Olasılıklar belirlenirken; Tehdit kaynaklarının motivasyonlarının ve yeteneklerinin, sistemin doğal zayıflıklarının, mevcut kontrollerin etkinliğinin değerlendirilmesinin düşünülmesi gerekmektedir. Bununla ilgili Şekil 5'deki örnek çalışma değerlendirilmektedir.

Olasılık Tanımlama	
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 alınması oldukça kolay olan bir tehdit.

Şekil 5: Olasılık Tanımlama Örnek Tablosu

Sonuç itibarıyla olasılıkların belirlenmesi veya tanımlanması ile hedeflenen; olasılık dereceleri ve etki analizi tablolarının oluşturulmasıdır.

Etki Analizi:

Önem / Etki Tablosu	
Etki Büyüklüğü/Önemi	Etkinin Büyüklüğünün Tanımı
Yüksek	Sisteme ait maliyeti çok yüksek bir varlığın kaybedilmesi, Organizasyonun hayati öneme haiz bir görevini yapamaması, İnsanların ağır yaralanmasına veya ölümüne sebep olabilecek.
Orta	Sisteme ait maliyeti yüksek bir varlığın kaybedilmesi, Organizasyonda öneme haiz bir görevin yapılamaması, İnsanların ağır yaralanmasına sebep olabilecek.
Düşük	Sisteme ait maliyeti ihmal edilebilir bir varlığın kaybedilmesi, Organizasyonun herhangi bir görevini yapamaması.

Şekil 6: Önem / Etki Analizi Örnek Tablosu

Burada nitel veya nicel değerlendirmelerden hangisine karar verileceği önemli bir kıstastır. Her ikisinin de kendine göre avantaj ve dezavatajları bulunmaktadır. Şekil 6'da bu konuda örnek bir tablo oluşturulmuştur.

Nitel Etki Analizinin Avantajları;

- Risklerin önceliklendirilebilmesi,
- Tanımlanmış bölgelerdeki zayıflıklardaki gelişmelerin görülebilmesi.

Nitel Etki Analizinin Dezavantajları;

- Spesifik ölçümler ve etkilerin büyüklükleri hakkında sayısal veriler sunamaz,
- Fayda-maliyet analizi yapılamaz.

Nicel Etki Analizinin Avantajları;

- Etkilerin ölçülebilir büyüklükler vererek gösterir,
- Fayda-maliyet analizi bu verilere göre yapılabilir, tavsiye plan oluşturulabilir.

Nicel Etki Analizinin Dezavantajları;

- Ölçümlemeler sayısal oranlara göre yapılmaktadır, dolayısıyla sayılarla çıkan sonuç insanları yanıltabilir.

Risk Tanımlama:

Kurulacak olan sistemin risk düzeyleri belirlenmekte, ölçülebilir risk düzeyleri matrisi ve risk skalası oluşturulur. Tablo xxx'de gösterildiği gibi risk düzey matrisi içerisinde tehditlerin olasılığı ve bahsi geçen tehditin etkisinin ortaya konulması gerekmektedir.

a) Risk Düzey Matrisi Oluşturma: Şekil 7'de detaylı bir tablo oluşturulmuştur.

Tehdit Olasılığı	**Tehdit Etkisi**		
	Düşük (10)	Orta (50)	**Yüksek (100)**
Yüksek (1.0)	Düşük (0.1 x 10 = 1)	Orta	**Yüksek**
Orta (0.5)	Düşük	Orta	**Orta**
Düşük (0.1)	**Düşük**	**Düşük**	**Düşük**

Şekil 7: Risk Düzey Matrisi Örnek Tablosu

b) Risk skalası :
   - 50 < Yüksek < 100
   - 10 < Orta < 50
   - 1 < Düşük < 10

   olarak tanımlanabilir.

c) Risk Düzeylerinin Tanımlaması:

Risk Skalası Tanımlama Tablosu	
Risk Düzeyi	**Risk Tanımı**
Yüksek	**Tespit edilen risk yüksek ise; ölçümleme yapılabiliyorsa yapılır veya hemen yeni bir eylem planı hazırlanarak uygulamaya alınır.**
Orta	**Tespit edilen risk orta ise; Uygun bir periyod belirlenerek yeni bir plan oluşturulması beklenir.**
Düşük	**Tespit edilen risk düşük ise; sistemde onay makamı bu durum için riskin kabul edilebilirliğine karar verir.**

Şekil 8: Risk Skalası Tanımlama Örnek Tablosu

Bu bölümde beklenen; "Risk Skalası Tanımlama Tablosunun" oluşturulmasıdır.

4. SONUÇ

Günümüz dünyasında kişiler, kurumlar ve hatta ülkeler için özellikle parasal değeri olan veya menfaat sağlanabilecek her türlü kıymetli bilginin dost olmayan kişi, kurum veya ülkelerin eline geçmesi son derece tehlikeli olabilmektedir. E-Devlet kapısı gibi sadece vatandaşların değil aynı zamanda tüm kamu kurum ve kuruluşlarının, işletmelerin kullanacağı bir sitemin gerek altyapı, gerekse idari açıdan uluslararası geçerliliği olan model, metodoloji veya standartlara uygun olarak işletilmesi gerekliliği görülmektedir. Sırf bu yasal olmayan müdahaleler için eğitilmiş ve ayrılmış kaynakların bulunması ve kişi veya kurumların planlarını ellerine geçirdikleri bu bilgileri üstünlük sağlayacak şekilde kullanabilmeleri ağ güvenliğinin ve sonuçta ortaya çıkan bilgi ve kişisel hakların korunmasının, ne kadar önemli olduğunu ortaya koymak için yeterlidir.

Bilgi ve iletişim teknolojileri dünyasının yeni trendi olarak görülen; insan, teknoloji ve süreç üçlemesi sektörün göremediği noktalardan birisidir. Güvenli bilgisayar ortamlarının oluşturulması için eksiksiz bir teknoloji birikimi gerekir. Ancak teknoloji tek başına bu ortamlardaki tehditlerin çözümü için yeterli olamaz. İyi tasarlanmış ürünler, oturmuş ve etkili süreçler ve bilgili, iyi eğitimli operasyon ekipleri olmaksızın üst düzey güvenlik sistemleri ortaya koymak olası değildir.

5. TEŞEKKÜR

Bu çalışmayı hazırlamama yardımcı olan Dr. Ahmet KAPLAN, Mustafa CANLI, Ömer KILIÇ ve tüm e-devlet kapısı projesi çalışanlarına teşekkürlerimi sunarım.

6. KAYNAKLAR

1. Kavrakoğlu, İ., Toplam Kalite Yönetimi, Kalder Yayınları, İstanbul, 1996.

2. e-Devlet Kapısı Projesi Teknik Şartnamesi.

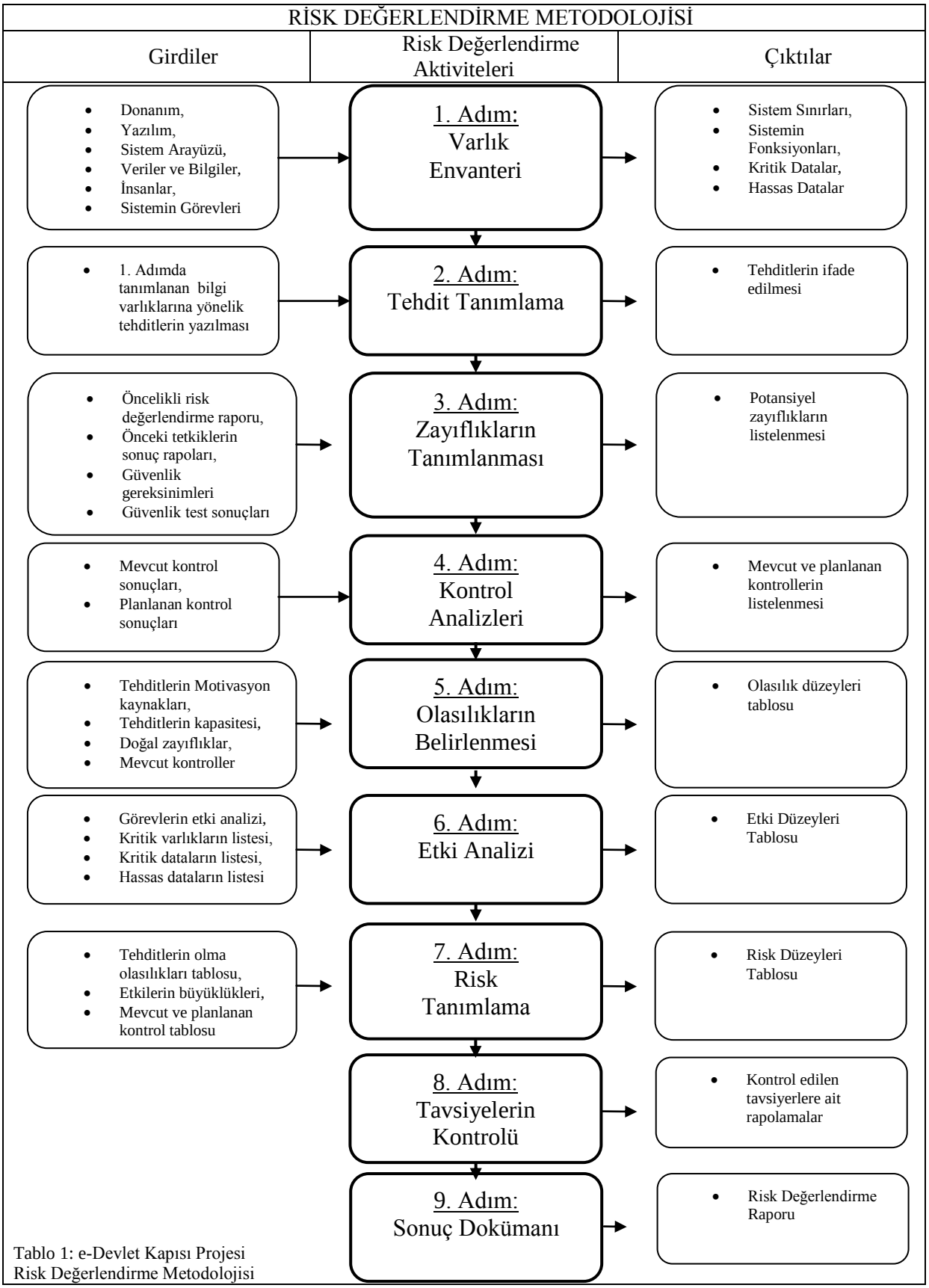
3. Türk Standartları Enstitüsü, "Bilgi Teknolojisi-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler", TS ISO / IEC 27001, Mart 2006.

4. DURMUŞ, G., "Risk Analizi", gdurmus@yahoo.com, Gursoy.Durmus@tikle.com

5. Türk Standartları Enstitüsü, "Bilgi Teknolojisi- Bilgi Güvenliği Yönetimi için Uygulama Prensibi", TS ISO / IEC 17799, 2000.

6. Türkiye Bilişim Derneği, TBD Kamu-BİB, "Bilişim Sistemleri Güvenliği El Kitabı Sürüm 1.0", Türkiye Bilişim Derneği Yayınları, Mayıs 2006.

7. Stoneburner, G., Goguen, A., Feringa, A., "Risk Management Guide For Information Technology Systems", NIST Special Publication 800-30, Computer Security Division Information Technology Laboratory Gaithersburg, MD 20899-8930, July 2002.



Tablo 1: e-Devlet Kapısı Projesi Risk Değerlendirme Metodolojisi