Bilgi ve Bilgi Teknolojilerine Ait Risklerin Yönetilmesinde Arayış, Yöntem ve Çözüm Önerileri

Dr. Ender Şahinaslan
Bilgi Teknolojileri Risk Yönetimi, Uyum ve Bilgi Güvenliği Yöneticisi, Bank Asya, İstanbul
e-posta: ender.sahinaslan@bankasya.com.tr

Özet: Bu çalışma, banka, sigorta, telekomünikasyon, üniversite, sağlık ve benzeri alanlarda kurumsal kimlik taşıyan firmalar için yönetilmesi gereken alanlardan biri olan bilgi ve bilgi teknolojileri risklerinin yönetilmesinde arayış, yöntem ve çözüm önerileri hakkında edinilen bilgi ve deneyimlerin paylaşılması için hazırlanmıştır.

Anahtar Sözcükler: Bilgi ve Bilgi Teknolojileri risk yönetimi, standartlar (ISO/IEC 27005, ISO/IEC 31000, RISK IT, COBIT vb), bilgi güvenliği yönetim sistemi, risk değerlendirme yöntemleri, risk yönetim uygulamaları, yasal uyum.

Quest, Method and Solutions for Information and Information Technology Risk Management

Abstract: This study concerning methods and solution suggestions for managing the risks of the quest for knowledge and information technologies which is one of the areas that should be managed for bank, insurance, telecommunications, university, health and other areas of corporate identity with one of the areas are prepared for the sharing of knowledge and experience acquired.

Keywords: Information technology risk management, standards(ISO/IEC 27005, ISO/IEC 31000, RISK IT, COBIT etc), information security management system, risk assessment methods, risk management practices, legal compliance.

1. Giriş

Bilgi teknolojileri alanında dünya çapında yaşanan hızlı gelişmeler, doğan fırsatlar bir yandan kurumları daha fazla kazanmaya teşvik ederken diğer taraftan o ana kadar bilinilen ya da bilinmeyen pek çok tehditleri de beraberinde getirebilmektedir. Bilgi ya da bilgi teknolojileri üzerinde yer alabilen açıklıkları kullanabilen bu tehditler risk denilen bu potansiyel tehdidin gerçekleşme ihtimalini önceden öngörmeye dayanır ve mutlaka kurumsal bir yaklaşımla ele alınarak yönetilmesi gerekir.

Bilgi ve bilgi teknolojilerinde kurumsal risk yönetimlerinin yapılması artık bir gereklilikten öte bir zorunluluk haline de dönüşebilmektedir. Kurumlar risk yönetimini gerçekleştirmeye karar verdikten sonra bunu nasıl, ne biçimde gerçekleştirileceğini, ne tür yöntem ve uygulamaların olduğunu, bu konuda uluslar arası bir standart olup olmadığı varsa standartların ne önerdiğini, yasal her hangi bir kural, yükümlülük ya da uyum gereklilikleri olup olmadığı gibi bir dizi araştırmaları yapma ihtiyacı doğmaktadır. Bu konuda yapılmış olan önceki benzer çalışma ve deneyimlere ayrı bir ihtiyaç duymaktadır.

Bu çalışma, bilgi ve bilgi teknolojileri risk yönetimine ilişkin gerçekleştirilen akademik çalışmalar ile kurumsal bir banka da edinilen uygulama deneyim sonuçları özetini benzer ihtiyaçları duyan tüm kurumsal firma ve/veya araştırıcılarla paylaşmayı hedeflemektedir.

2. Risk Yönetim Süreci

Risk yönetim sürecine ilişkin standartlarda yer alan tariflere baktığımızda;

- Bir kuruluşun riski kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetler bütününe[1],
- Bilgi sistemlerini etkileyebilecek olan güvenlik risklerinin, uygun bir maliyette tanımlanması, kontrol edilmesi ve en aza düşürülmesi veya ortadan kaldırılması sürecine denir[2].

Bilgi ve bilgi teknolojileri üzerinde yer alan risklerin yönetilmesinde gerçekleştirilen bir dizi faaliyetleri; risk tanımının yapılması, değerlendirmesi, planlama, işleme, izleme ve risk sonlandırma süreç adımları olarak tanımlanabilir, temel bir risk yönetim süreci şekil-1'de gösterilmektedir.



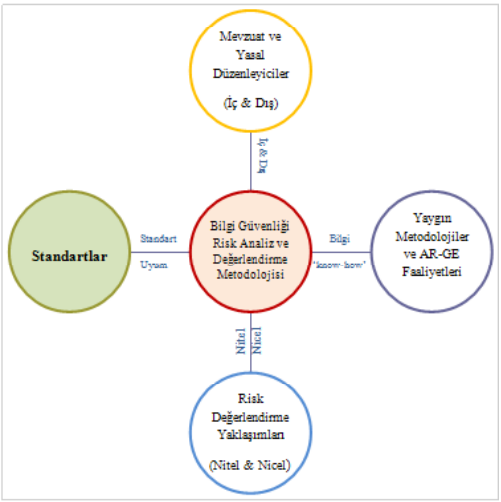
Şekil 1. Risk Yönetim Süreci [3]

Sağlıklı bir risk yönetimi yapmak için kurum risk yönetimine ait bu süreç aşamalarını işleterek riski doğuran tehditlere karşı kontrol ve önlemleri almak ve riskin mümkün olan kabul edilebilir seviyeye çekmesi ya da tamamen yok etmesi gerekir.

Risk yönetim sürecini işletmede; kurum beklentilerini, yasal ve standart yaklaşımlara uyum gibi unsurları dikkate alan bir risk değerlendirme yöntem seçimi, risk yönetiminin yapılacağı platform-uygulama seçimleri karar verilmesi gereken ana unsurlar arasında yer alır. İşte tam bu noktada bu unsurların arayışları, mevcut yöntem ve çözüm yollarının keşfi başlamaktadır.

3. Arayış ve Yöntemler

Genel bir risk yönetiminde özelde ise bilgi ve bilgi teknolojileri alanında yapılacak bir risk yönetimi için kurumsal bir firmanın karar vermesi gereken ilk unsur risk değerlendirme yöntemine karar vermektir. Bu yönde yapılacak bir arayış için çıkılan yolculuk da düşünülmesi gereken belli başlı alanlar Şekil-2'de gösterilmektedir.



Şekil 2. Risk Değerlendirme Yöntem Bileşenleri [4]

Risk değerlendirme yönteminde yer alması gereken temel unsurlar aşağıda belirtilmiştir.

- Standartlar (ISO/IEC 27005, ISO/IEC 31000, RISK IT, COBIT vb)
- İlgili kurum mevzuatlarına uyum gerekliliklerı (İç ve dış)
- Risk değerlendirme yaklaşımı; Nitel-nicel karma model
- Yaygın kullanılan metodolojiler ve bu alanda bilinen en iyi uygulama örneklerinin incelenmesi kurum için önemli avantaj doğurmaktadır.

3.1 Standartlar

Kurumsal bir kimliğe sahip ya da sahip olmak isteyen bir kurum için yapılan faaliyet kollarının her birinde varsa o alandaki ilgili uluslararası standartların belirlemiş olduğu kurallara asgari seviyede uyumlu olması önemli bir gösterge olarak kabul edilmektedir. Aynı zamanda bu uyumluluk artık gittikçe globalleşen bu çağda daha da önemli kılmaktadır.

Uluslararası standartlar incelendiğinde ISO/IEC 9001, ISO/IEC 27001, ISO/IEC 27005, RISK IT, ISO/IEC 31000, AS/NZS 4360:2004, FISMA, NIST SP 800–53, PCI, PMI, CMMI, SPICE, ITIL, COBIT gibi standartlar mevcuttur. Bunların bir kısmı doğrudan bir risk yönetim standardı iken ISO/IEC 9001, PCI, CMMI, SPICE, PMI, ITIL, COBIT, HIPAA gibi bir takım standartlar ise kendisi bir risk yönetim standardı olmamakla birlikte risk yönetiminin ile de ilintilidir. Bilgi ve Bilgi Teknolojilerine yönelik risk yönetim standartları;

- ISO/IEC 27005: Bilgi Güvenliği Risk Yönetim Standardı
- RISK IT: bilgi teknolojileri risklerinin etkin yönetimine yönelik bir dizi ilkelerden oluşan ana çerçeve niteliğindedir.
- NIST SP 800–30: Bilgi Teknoloji için Risk Yönetim Rehberi

3.2 Mevzuat ve Yasal Uyum

Kurumlar kendi iç mevzuat ve yönetim tarafından onaylı politikalarına uyum gösterirken mevzuat gereği uyum sağlamak zorunda olduğu dış mevzuatlara da uyumlu olmak zorundadırlar. Bir banka için Bankacılık Düzenleme ve Denetleme Kurumu olan BDDK'nın koymuş olduğu yasal düzenlemelere uyum sağlarken üniversiteler ise Yüksek Öğrenim Kurumu(YÖK)'ün koymuş olduğu düzenlemeleri sağlamak zorundadır. Dolayısı ile kurumlar hangi sektörde faaliyet gösterirlerse göstersinler bir risk metodolojisine karar verirken yasal direktifleri de dikkate almak zorundadır.

3.3 Risk Analizi Ölçümleme Yöntemleri

Bilgi ve bilgi teknolojilerine ait risk yönetimi süreci içerisinde risklerin analiz ve değerlendirme aşamasında nitel ya da nicel risk analiz yöntemlerinden biri yada bu iki yöntemi birlikte kullanabilen karma yöntemden biri seçilerek gerçekleştirilir.

'Yüksek, orta, düşük, imkansız' gibi sözel ifadelerin kullanılarak gerçekleştirilmesine nitel(sözel) analiz, '3, 2, 1, 0' gibi sayısal ifadelerin kullanılmasıyla gerçekleştirilen analiz yöntemine ise nicel(sayısal) analiz yöntemi denir. Bir tehdit'in vuku bulma ihtimaline karar vermede kullanılan karar tablosu örneği Tablo 1'de verilmiştir.

Nicel	Nitel	Olasılık	Açıklama
0	İmkânsız	% 0	İmkânsız veya 10 yıl üzeri oluşabilir.
1	Düşük	%1–34	1-10 yılda bir kez oluşabilir
2	Orta	% 35–74	1-5 yıl içinde en az bir kez oluşabilir
3	Yüksek	% 75-100	0-12 ay içinde bir veya üzeri oluşabilir

Tablo 1: Tehdit Etki-Olasılık Karar Çizelgesi

Tüm bunların yanında daha çok akademik çalışmalarda kalmış pratik kullanımına sık rastlanmayan karar ağaçları, yapay zeka gibi çok veriye dayalı yöntemlere de rastlanmaktadır. Bilgi ve bilgi teknolojilerine ait benzer risklere ait çok sayıda geçmiş veri bulma pratikte pek mümkün olamamaktadır. Buna bilgi ve bilgi teknolojilerindeki tehditlerin teknolojik gelişmelere de paralel olarak çok değişkenlik göstermesi, mevcut bir tehdit'e ait riske konulacak bir sistemsel ya da yazılımsal önlemin benzer nitelikteki pek çok riski de önlüyor olabilmesi gösterilebilir.

3.4 Yaygın Kullanılan Metodolojiler

Yaygın kullanılan risk değerlendirme yaklaşımları incelendiğinde CRAMM, COBRA, EBIOS, ISAMM ve OCTAVE yaklaşımları karşımıza çıkmaktadır.

CRAMM (CCTA Risk Analysis and Management Method), 1987 yılında İngiliz hükümetine bağlı telekomünikasyon kurumu tarafından geliştirilen ve nitel yönteme dayanan risk analiz ve risk yönetim metodolojisidir[5].

COBRA (Consultative, Objective and Bifunctional Risk Analysis), nitel analiz yöntemine dayanan, anket tabanlı olup İngiliz danışmanlık firması tarafından geliştirilmiştir[6].

CORAS(Construct a platform for Risk Analysis of Security Critical Systems), nitel risk analizi yöntemini kullanır. Temel amacı risk analizi için yöntemler, nesneye dayalı modelleme için yarı biçimsel yöntemlerle güvenliğin kritik olduğu sistemlerde kesin, belirgin ve etkin bir risk analizi sağlayan araçları sınayan bir çerçeve geliştirmektir[7].

EBIOS metodu; bilgi güvenliği sistemi ile ilgili riskleri ele alma ve değerlendirmede nitel risk değerlendirme yaklaşımı benimsenmiştir.

ISAMM (Information Security Assessment & Monitoring Method) nitel yönteme dayanan risk analiz metodolojisidir[8].

OCTAVE metodu nitel risk değerlendirme yaklaşımı benimsemiştir. Varlık tabanlı bilgi güvenliği risk değerlendirmesi yapmaktadır[9].

Bu alanda yaygın kullanılan metodoloji ve uygulamalara ilişkin yapılan araştırma sonuçları ABGS 2010 sempozyumunda "Bilgi Güvenliği Risk Yönetim Metodolojileri ve Uygulamaları Üzerine İnceleme" adlı çalışmada sunulmuştur[10].

3.5 Uygulama Yazılımları

Bilgi ve bilgi teknolojileri risklerinin yönetimi amacıyla geliştirilen pek çok uygulama geliştirilmiştir. Yayın olarak kullanılan uygulamalar olarak Art of Risk, Real ISMS, Callio, ISMart, Proteus, Risk Watch, ISMS-Rat uygulamalarını örnek olarak verebilir.

Kriter-Nitelik		Art Of Risk	Real Tools	Callio Secura	COBRA	CRAMM	EBIOS	GRC	ISAMM	ISMART	ISMS-RAT	OCTAVE	Proteus	Risk Watch	Safran Modul
Uygulama Türü	BGYS	+	+	+							+	+		+	+
	Risk Yönetimi				+	+	+	+	+				+	+	
Standart Yaklaşım	BS 7799			+		+									
	ISO 17799	+		+	+		+				+	+			+
	ISO 27001	+	+	+		+		+		+	+	+		+	+
	ISO 13335						+								
	BS 25999							+					+		
	SOX							+					+		+
	COBIT							+					+	+	
	ITIL							+							
	MEHARI					+									
	Risk IT							+							
	PCI DSS							+		+			+	+	
	NIST 800-26												+		+
	Basel II									+					
	OLIRA					+									
Kendi Metodolojisi	Diğer (*)				+	+	+		*				+		*
Risk Değerlendirme Yaklaşımı	Nitel Analiz	+	+	+	+	+	+	+		+	+	+	+	+	+
	Nicel Analiz					+				+			+	+	
Yazılım Platformu	Php		+												
	Net						+								
	Java						+	+		+					
	Uygulamalı	+		+	+	+			+	+		+	+	+	+
Veri Tabanı	SQL Server			+					-				+		
	MS Access	-										-			
	My SQL			+									+		
	ORACLE							+						+	
	Uygulamalı		+		+	+				+	+				+
Araştırma Kaynağı	Demo	+	+	+			+				+	+		+	+
	Internet	+	+	+	+	+	+	+	+	+	+	+	+	+	+

Tablo 1: Risk Yönetim Yazılımları

Mayıs-Ekim 2009 tarihleri arasında kapsamlı bir şekilde araştırılmıştır. İnceleme, ilgili uygulamaların demo yazılımlarının elde edilmesi ve/veya internet ortamında yer alan bilgilerin taranması yoluyla elde edilmiştir. İncelenen risk yönetim yazılımlarının uygulama türü, standart yaklaşımları, risk metodolojisi, yazılım geliştirme platformu ve çalıştığı veri tabanı bakımından karşılaştırma özeti Tablo 2'de gösterilmektedir[10].

Uygulamaların ağırlıklı olarak internet tabanlı olduğu, kısıtlı elde edilen verilere göre veri tabanı olarak MS Access, SQL Server, My SQL ve ORACLE veri tabanlarının kullanıldığına rastlanmıştır. Risk değerlendirme yaklaşımı olarak nitel yöntem ağırlıklı olarak kullanılmıştır.

4. Sonuç ve Öneriler

Bilgi teknolojilerinin sunduğu çeşitli avantajlarla git gide küreselleşen dünyada var olma yolunda bayrak açmaya hazırlanan, uzun soluklu bir yolculuğu göze alan kurumlar için değerli olan bilgi ve bilgi teknolojilerine ait tehditlerin öngörülmesi, risklerin belirlenmesi ve yönetilmesi artık bir gereklikten çıkıp zorunluluk haline gelmiştir. Bu zorunluluk içten gelen bir

zorunluluk olduğu kadar artık yasal bir zorunluluk olarak da karşımıza çıkabilmektedir.

Kurumlar risk yönetim ve yöntemlerini belirlemek için yola çıktığında bunlara ilişkin bir standart, yasal uyum gerekliği, risk yönetimi yöntem ve uygulaması olup olmadığı gibi cevap verilmesi gereken pek çok sorularla karşı karşıya kalabilmektedir.

Bu çalışma, bu alanda ihtiyaç duyulabilecek pek çok soruya yanıt niteliğindedir. Akademik bir çalışma olmasının yanında kurumsal bir bankada edinilen deneyim ve araştırma sonuçlarının bir özeti olarak ihtiyaç duyan tüm kurum ve araştırmacılarla paylaşılması açısından önemlidir.

Bilgi ve bilgi teknolojilerine ait risklerin yönetilmesinde kurumlar ihtiyaç ve beklentilerini belirledikten sonra mevcut yöntem ve uygulamalardan birini seçebilecekleri gibi kendi yöntem ve uygulamalarını da geliştirebilirler.

5. Kaynaklar

[1] TS ISO/IEC Guide 73, "Risk Yönetimi- Terim ve Tarifler", **Türk Standartları Enstitüsü**, Ankara, 2005

[2] TS ISO/IEC 17799, "Bilgi Teknolojisi – Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri", **Türk Standartları Enstitüsü**, Ankara, Kasım 2002

[3] Şahinaslan, E. "Standartlara Dayalı Bilgi Güvenliği Risk Analiz ve Ölçümleme Metodolojisinin Bankacılık Sektörüne Özgü Modellenmesi ve Uygulama Yazılımının Geliştirilmesi", **Doktora Tezi**, Trakya Üniversitesi, Edirne, 2010

[4] Sahinaslan, E., Kandemir, R., Sahinaslan, Ö., "Examinations Results of International Standard Approaches in Developing Information Security Risk Analyses and Assessment Method", **ISCSE 2010**, Izmir, Turkey, June, 2010

[5] http://en.wikipedia.org/wiki/CRAMM, Ekim 2009

[6] http://www.riskworld.net/benefits.htm , Ekim 2009

[7] Braber, F., Hogganvik, I., Lund, M.S., Stolen, K., Vraalsen, F., "Model-based security analysis in seven steps - A guided tour to the CORAS method", v 25, S:101-107, 2007

[8] http://rm-inv.enisa.europa.eu/methods_tools/m_isamm.html , Ekim 2009

[9] OCTAVE. (2001, December). OCTAVE Criteria V.2.pdf, P:7.

[10] Şahinaslan, E., Kandemir, R., Kantürk, A., "Bilgi Güvenliği Risk Yönetim Metodolojileri ve Uygulamaları Üzerine İnceleme", **ABGS 2010 – Ağ ve Bilgi Güvenliği Sempozyumu 2010**, EMO, Ankara, Şubat, 2010.