Bilgi Güvenliği Risk Yönetim Metodolojileri ve Uygulamaları Üzerine İnceleme

Ender Şahinaslan[1] Rembiye Kandemir[2] Arzu Kantürk[3]

[1,2]Bilgisayar Mühendisliği Bölümü, Trakya Üniversitesi, Edirne
[3]Bilgi Güvenliği Servisi, Bank Asya, İstanbul

[1]e-posta: ender@bankasya.com.tr [2] e-posta: rembiyeg@trakya.edu.tr
[3] e-posta: arzu.kanturk@bankasya.com.tr

Özetçe

Günümüz dünyasında teknolojik ilerlemelere paralel olarak, bilgi ve bilgi teknolojilerine ilişkin güvenlik riskleri de günden güne artmaktadır. Diğer taraftan *ISO 27001, ISO 27005*, *COBIT, PCI, SOX ve BASEL II* gibi uluslararası kabul görmüş standartlar-kurallar kurumlarda risk yönetimini zorunlu kılmaktadır.

Bilgi güvenliğin sağlanması noktasında, kurumların ilk olarak yapması gereken; bilgi güvenliği risklerinin belirlenmesi ve mevcut risklerin kurumun kabul edeceği bir seviyeye çekilmesi olmalıdır. Kurumlar, bilgi güvenliği risk değerlendirmesi yapmadan önce kendi ihtiyaçları doğrultusunda bir risk metodolojisi belirlemelidir.

Bu çalışma, günümüzde mevcut olan risk metodolojileri ve yazılımları hakkında yapılmış bir inceleme olup bu konuda bilgi vermeyi amaçlar. Çalışmanın ilk bölümünde risk yönetimi ve standartlarına ilişkin temel kavramların tanıtımı, ikinci bölümünde risk değerlendirme yaklaşımları ve yaygın kullanılan risk metodolojileri hakkında bilgi, üçüncü bölümde tanınmış belli başlı risk yönetim yazılımları hakkında bilgi, dördüncü bölümde ise bu uygulama yazılımlarının karşılaştırması yapılmıştır.

1. Giriş

Bilgi ve bilgi teknolojileri güvenliğine ilişkin riskleri yönetmek amacıyla her kurum kendi yapıları, kurumsal ve yasal bağlılıkları dikkate alan, bu alanda yer alan standartları destekleyen, aynı zamanda yönetimin onayladığı bir metodolojiyi benimsemeli ve buna uygun uygulamaları ya seçmeli ya da kendisi geliştirmelidir.

Risk metodolojisinin seçimi ya da geliştirilmesinde karar veren ya da bu alanda çalışan proje ekiplerince risk yönetimine ilişkin kavramlarının tam olarak anlaşılması ve aynı dilin kullanılmasında büyük yarar vardır.

Temel risk kavramı ve uluslararası kabul görmüş standart yada en iyi uygulamalar, bazı yasal düzenleyiciler tarafından belirlenen kuralların risk yönetiminden beklentilerine yönelik özet bilgiler bu bölümde açıklanmaya çalışılmıştır.

Risk kavramı; zarara ve kayba neden olacak bir olayın bilgi varlığı üzerinde gerçekleşme olasılığı olarak tarif edilebilir.

Risk yönetimi ise; var olan risklerin minimize edilmesi için oluşturulmuş prosesler bütünüdür. Risk yönetimi; risk analizi, risk değerlendirme, risk önleme, tehditlerin ve kontrollerin değerlendirilmesi olmak üzere dört ana süreçten oluşmaktadır.

ISO 27001, ISO 27005, COBIT, BASEL II gibi standartlar ve BDDK İlkeler Tebliği risk yönetimi üzerinde önemle durmaktadır;

ISO 27001, kuruma ait tüm bilgi varlıklarının değerlendirilmesi ve varlıklar üzerindeki tehditlerin ve açıklıkların göz önünde tutulup risk analizi yapılmasını gerekli kılar [1].

ISO 27005; bilgi güvenliği risk yönetim standardıdır. Bu standart kurumların ihtiyaçları doğrultusunda bir risk yönetim metodolojisi geliştirmesi gerektiğini ifade eder ve risk yönetim metodojilerine ilişkin örnekler verir [2].

COBIT'e göre öncelikle kurumlar risk yönetim çerçevesini oluşturmalıdır.

Risk yönetim çerçevesi oluşturduktan sonra mevcut riskler tanımlanmalı ve tanımlanan risklere ilişkin aksiyon planları oluşturulmalı planların uygulanabilirliği ve sonuçları izlenmeli, değerlendirmelidir.

BASEL II riskleri, kredi riski, likitide riski ve operasyonel risk olmak üzere üçe ayırmıştır. Bilgi ve bilgi teknolojileri riskleri ***"operasyonel risk"*** başlığı altında toplanmaktadır. Operasyon risklere; itibar riski, insan riski, teknolojik risk, organizasyon risk, yasal riskler örnek olarak verilebilir.

Banka bilgi sistemleri yönetiminde esas alınacak ilişkin tebliğ; "Banka, bankacılık faaliyetlerinde bilgi teknolojilerini kullanıyor olmasından kaynaklanan riskleri ölçmek, izlemek, kontrol etmek ve raporlamak üzere gerekli önlemleri alır" şeklinde bir ifade kullanılmaktadır [3].

Tüm bu standartlar, yasal otoritelerin koymuş olduğu uyulması gereken çeşitli kurallar ve kurumsallığın gereklilikleri bize kurumlarda etkin bir risk yönetiminin gerçekleştirmesini önem ve gerekliliğini göstermektedir.

Kurumların kendi ihtiyaçlarına özgü risk metodojisi geliştirmesi veya mevcut kabul görmüş bir metodolojiyi benimseyerek bunu risk yönetim araçları ile otomatize hale getirmesi gerekmektedir.

2. Risk Yönetim Metodolojileri

Risk yönetim metodolojilerinin temelini teşkil eden risk değerlendirme yaklaşımlarından yaygın olarak nicel ya da nitel analiz yöntemlerinden biri veya her ikisi esas alınabilmektedir.

Nitel (qualitative) risk metodolojileri; çok yüksek, yüksek, orta, düşük, çok düşük gibi sözel ifadelere dayanır.

Nicel (quantitative) risk metodojileri ise; 0, 1, 2, 3, 4 gibi sayısal ifadelere dayanır.

Başlıca risk yönetim metodojileri şunlardır:

2.1. COBRA (*Consultative, Objective and Bi-functional Risk Analysis*)

Nitel analiz yöntemine dayanan, anket tabanlı olup İngiliz danışmanlık firması tarafından geliştirilmiştir. Metodu destekleyen uygulama da geliştirilmiş olup uygulama iki ana modülden oluşmaktadır; [4]

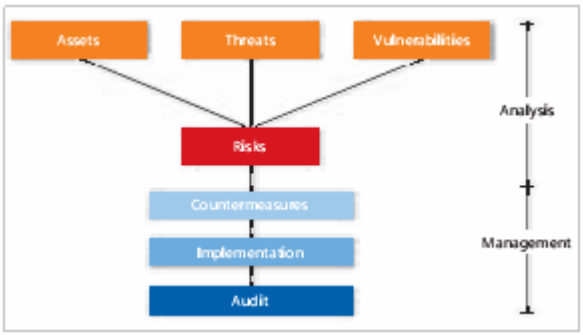
Risk Danışmanı: Standart sorulardan oluşur. Bu sorular kurum ile bilgi toplamak için kullanılır. Toplanan bilgiler risk analizinde kullanılır

Standartlara Uyum: Kurumun standartlara uyumunu ölçen sorular sorulur ve değerlendirilir.

2.2. 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].

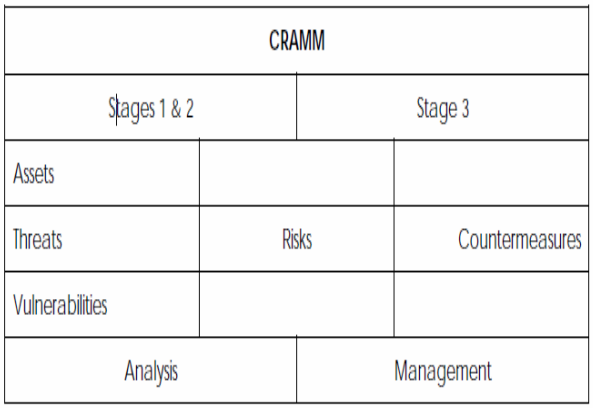
CRAMM metoduna ait genel şema Şekil 1'de verilmektedir



Şekil 1: CRAMM Metodu [6].

CRAMM metodu analiz ve yönetim olarak iki ana bölümde ele alınabilir. Risk analizi bölümünde bilgi varlığı, varlık üzerindeki açıklıklar(korumasızlıklar) ve tehditlerin bu açıklıkları kullanması sonucunda oluşabilecek risklerin analizini, yönetim bölümünde ise ölçümleme, uygulama ve denetim bölümlerinden oluşmaktadır.

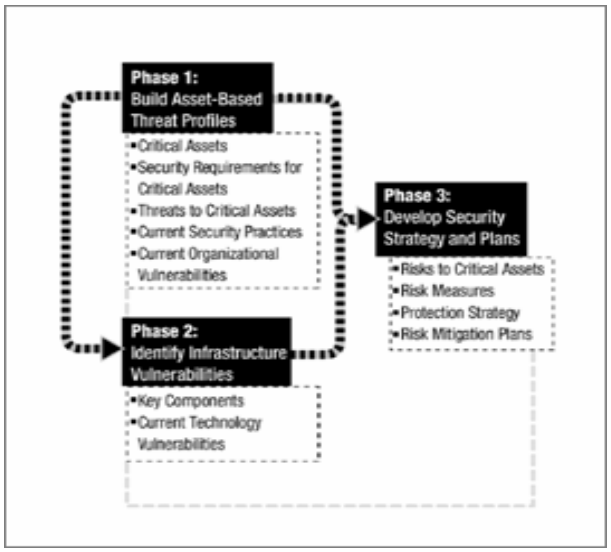
CRAMM yaşam döngüsü ele alında 3 aşamada gerçekleştirildiği görülmekte. Buna ait bilgiler Şekil-2'de yer almaktadır.



Şekil 2: CRAMM Yaşam Döngüsü [7]

2.3. OCTAVE

Risk tabanlı stratejik görüş sağlayan planlama tekniğidir. Octave, Cert, DoD, USAF tarafından bilgi güvenliği risk değerlendirme metodu olarak kurumlar için oluşturulmuştur. Octave, varlık tabanlı bilgi güvenliği risk değerlendirmesi yapamaktadır. Octave metodunun evreleri Şekil-3'de gösterilmektedir [8].

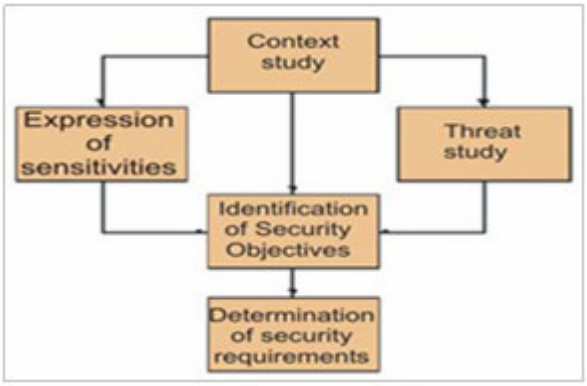


Şekil 3: OCTAVE Evreleri

2.4. EBIOS (In French-Expression des Besoins et Identification des Objectifs de Security)

Bu risk metodolojisi; DCSSI *(Direction Centrale de la Sécurité des Systèmes d'Information)* tarafından Fransa'da oluşturulmuştur.

EBIOS Method; Bilgi Güvenliği Sistemi ile ilgili riskleri ele alır ve değerlendirir. EBIOS metodunun genel şeması Şekil 4'te verilmektedir [9].



Şekil 4: EBIOS Method

2.5. ISAMM (Information Security Assessment & Monitoring Method)

ISAMM nitel yönteme dayanan risk analiz metodolojisidir.

ISAMM'da risk değerlendirme evresi üç kısımdan meydana gelmektedir; [10,11]

- Kapsamlaştırma
- Tehdit ve açıklıkların değerlendirilmesi
- Riskin hesaplanması ve raporlanması

3. Risk Yönetim Yazılımları

Bu bölümde, risk metodolojileri hakkında ayrıntılı bir analiz yapabilmek amacıyla Art of Risk, Real ISMS, Callio, ISMart, Proteus, Risk Watch, ISMS-Rat uygulama yazılımlarının kullanmış olduğu risk yönetim metodolojileri incelenmiştir.

3.1 Art Of Risk

ISO 27001 tabanlı nicel metodu kullanan bir risk analizi yazılımıdır [12].

Başlıca üç modülden oluşur;

Bilgi Toplama Modülü: ISMS alanı, dokümanları ve dokümanların kayıt numaraları, risk politikaları ve kapsamları, risk değerlendirmeleri, varlıklar ve varlıkların gizlilik, bütünlük, erişilebilirlik ve diğer güvenlik özelliklerini tanımlar.

Risk Tanımlama ve Değerlendirme Modülü: Tanımlanan varlıklar için tehditler, açıklıklar ve risk değerleri ve hesaplamaların yapıldığı modüldür.

Risk Yönetimi Karar Modülü: Risk tedavi seçeneğinde tanımlanmış riskler için kontroller ve kontrol hedefleri oluşturur. Riskleri minimum seviyeye çekebilmek için seçilmiş kontrol amaçlarını, belirlenmiş kontrollerin ve uygulanabilirlik durumunun takip edildiği modüldür.

Kontrollerin Uygulanması: Seçilmiş kontrollerin uygulanması planlanır.

3.2 Real ISMS

ISO 27001 ve Cobit temelli internet tabanlı bir risk analiz yazılımıdır. Web sunucusu olarak ISS ve Apache'yi desteklemekte, veri tabanı olarak ise MS SQL, ORACLE ve POSTGRESS veri tabanlarını desteklemektedir.[13]

Real ISMS'nin başlıca modülleri şunlardır;

Yönetim: Bu modülden kullanıcıların tanımlanması, değer skalalarının belirlendiği bölümdür.

Raporlama: Grafiksel ve istatistiksel bilgilerin alınabildiği, kullanıcıların hareketlerinin izlendiği ve raporlamanın yapıldığı modüldür.

Risk Yönetimi: Bilgi varlıkların belirlendiği, varlıklara ait risklerin eklendiği ve risk hesabının yapıldığı modül olup yine kontroller de bu bölümde eklenebilmektedir.

Politika Yönetimi: BG politikalarına ilişkin bilgilerin yer aldığı modüldür. (Yayınlanan, revize edilen politikalar vs.)

İyileştirme: Aksiyon planlarının oluşturulduğu, olayların düzenlendiği ve raporlamanın yapıldığı modüldür.

Kütüphaneler: Organizasyona ait BG olaylarının yer aldığı, yeni olayların eklendiği, doküman şablonlarının bulunduğu,

Arama: Veri ya da eleman filtrelemesine göre aramaların yapıldığı modüldür.

3.3 ISMart

Biz Net, TSE ve ISO–17799 / 27001 standardına uygun olarak bilgi güvenliği yönetimi sistemi kurmak ve uygulamak isteyen kurumlar için geliştirilmiş, Linux, Unix, veya Windows üzerinde çalışabilen Java ile yazılmış web tabanlı bir programdır.

Programda öncelikler varlık, tehdit, risk kategorileri oluşturulur. Kategoriler birbiri ile ilişkilendirilir. Varlık kategorilerine varlıklar eklenir ve varlığa ilişkin tehditler girilir. Bu kapsamda risk değerlendirilmesi yapılır [14].

3.4 Callio

Secura 17799; şirketlere BS 7799/ISO 17799 bilgi güvenliği yönetimi standardını sağlayan web tabanlı bir yazılımdır. Nitel bir değerlendirmesi yapılır

Risk Tanımlama: Varlıklar açısından riskleri tanımlanır.

Risk Değerlendirmesi: Risk hesaplama ve değerlendirmesi yapılır. Varlık envanteri oluşturulur ve değerlendirilir.

Risk tedavi: ISO 17799 Kontrolleri: Farklı senaryoları değerlendirmek (Risk Tedavi plan taslağı)

Risk İletişimi: Doküman Yönetimi, Bilinçlendirme Merkezi

Bilinçlendirme Merkezi Portalı: Farklı personel grupları için bilgi güvenliği belgeleri yayınlanır.

ISO 17799 Ön Teşhis: Anket, güvenlik durumu ile ilgili ilk karar, uyum raporları alınır. [15,16]

3.5 Proteus

Infogov (*Information governance limited*) Limited şirketi tarafından geliştirilmiş web tabanlı bir risk yönetim yazılımıdır. Proteus ile kurumlar COBIT, SOX, ISO 17799, PCI DSS gibi standartların kontrolleri uygulanabilir.

Nitel ve nicel risk analizini destekler. Her iki yöntemde de varlık yönetimi, tehditlerinin belirlenmesi, risk aksiyon planlarının oluşturulması ve olay yönetimi mevcuttur.

Riskler ile ilgili pdf, doc formatında raporlama yapılır ve dashboard'dan grafiksel bilgiler alınabilir.

ISO 27001, BS 25999, PCI DSS, Cobit, SOX gibi standartları destekler. [17]

3.6 Risk Watch

RiskWatch firması tarafından bilgi güvenliği risklerini analiz etmek için oluşturulmuş bir uygulamadır. Risk metodolojisi olarak nicel yaklaşımı benimsemiştir**.**

Bu uygulama bilgi sistemleri açıklıklarının değerlendirilmesi ve risk analizini içerir**.** Kurumların ihtiyacına göre şekillendirilebilir, yeni varlık, tehdit, açıklık kategorileri, soru kategorileri ve setleri oluşturulabilir.

ISO 17999 ve US-NIST 800–26 standartlarına ilişkin kontrolleri içerir. [18]

3.7 ISMS-Rat

ISMS- Rat client tabanlı basit bir risk analiz programıdır [19].

Uygulama veri tabanı olarak MS Access kullanmakta, standart yaklaşımı ISO 17799 ve ISO 27001 standardı bilgi güvenliği yönetim sistemini ve dolayısı ile risk yönetimini desteklemekte olup risk değerlendirme metodu olarak nitel analiz yaklaşım kullanılmıştır. Uygulama yazılım geliştirme platform bilgisine ise ulaşılamamıştır.

Varlık değerlendirme: Bilgi varlıklarının 'gizlilik', 'bütünlük', 'erişilebilirlik' nitelikleri bakımından ayrı ayrı ele alınır. Değerlendirme önceden tanımlanmış değer skalaları üzerinden gerçekleştirir.

Tehdit değerlendirme: Varlıkla ilişkili tehditler ve bunların gerçekleşme olasılık değerlerinin tanımlaması yapılarak tehditlerin değerlendirilmesi sağlanır.

Açıklık değerlendirme: Varlıkla ilgili varsa güvenlik zafiyetleri-açıklıkları tanımlanır.

Risk hesaplama: Standart yaklaşımları esas alan, bilgi varlık değeri, tehdit ve açıklık değerlerinin toplamından elde edilmektedir.

4. Uygulama Yazılımlarının Karşılaştırılması

Bilgi güvenliği risk yönetimine ait bilinen belli başlı uygulama 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 1'de gösterilmektedir.

***Tablo 1**: Risk Yönetim Yazılımları*

Kriter-Nitelik		Art Of Risk	Anet Track	Callio Secura	COBRA	CRAMM	FIHOS	GRC	GSTOOL	ISAMM	ISMART	ISMS RAT	OCTAVE	PROTEUS	Real BMis	Risk Watch	Secure Aware
Uygulama Türü	BGYS	+	+	+							+	+			+		+
	Risk Yönetimi				+	+	+	+	+	+			+	+		+	
Standart Yaklaşımı	BS 7799			+		+											
	ISO 17799	+		+	+		+				+	+				+	+
	ISO 27001	+	+	+		+		+		+	+	+		+	+		+
	ISO 13335-						+										
	BS 25999							+						+			
	SOX							+						+		+	
	COBIT							+						+	+	+	
	ITIL							+									
	HIPPA					+											
	Risk IT							+									
	PCI DSS							+		+				+	+		
	NIST 800-26													+		+	
	Basel II									+							
	GLBA					+											
Kendi Metodolojisi	Diğer (*)				+	+	+		*				+				*
Risk Değerlendirme Yaklaşımı	Nitel Analiz	+	+	+	+	+	+	+	+		+	+	+	+	+		+
	Nicel Analiz					+				+				+	+	+	
Yazılım Platformu	Php		+														
	XML						+										
	Java						+	+			+						
	Ulaşılamadı	+		+	+	+			+	+		+	+	+	+	+	+
Veri Tabanı	SQL Server			+					+						+		
	MS Access	+										+	+				
	My SQL			+										+			
	ORACLE							+							+		
	Ulaşılamadı		+		+	+	+			+	+					+	+
Araştırma Kaynağı	Demo	+	+	+				+			+	+					+
	İnternet	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

Uygulamaların bir kısmı sadece "risk yönetimi" yaparken diğerleri risk yönetimini de içerisinden barındıran bir Bilgi Güvenliği Yönetim Sistemi (BGYS)'ni işletmek amaçlı geliştirildiği görülmektedir.

Standart yaklaşımlar bakımından incelendiğinde GSTOOL(IT Baseline Protection Manuel) ve kendi metodolojisini kullanan OCTAVE hariç hepsi bir şekilde bilgi güvenliği standardı olan (BS7799, ISO 17799, 27001, 27005) standartlarını referans aldığı, kartlara ilişkin standart olan PCI DSS, İş sürekliliğine yönelik BSI 25999, BT yönetişimi'ne ilişkin COBIT ve diğer NIST 800–26, SOX, Basel II, HIPPA, Risk IT ve ITIL gibi bilinen pek çok standardı destekleyen uygulamalardan oluştuğu görülmektedir.

Risk değerlendirme yaklaşımı bakımından incelendiğinde yazılımların çoğu nitel analiz yöntemini esas aldığı, nicel analiz yaklaşımın ise çok nadir kullanıldığı, CRAMM, PROTEUS ve Real ISMS uygulamalının ise hem nitel hem de nicel yaklaşımı kullanıldığı gözlemlenmiştir.

Araştırma esnasında yazılım platformu ve veri tabanı bilgisi gibi teknik bilgiler kısmen elde edilebilmiştir. İncelemeler sonrasında, uygulama platformlarının genellikle web tabanlı (Real ISMS, ISMART, GRC, Callio vb) olarak geliştirildiği, Art of Risk, ISMS Rat gibi uygulamalar ise istemci tabanlı (C/S) olarak geliştirildiği görülmektedir. Günümüz kullanıcı talepleri ve internet teknolojilerinin gelişimi, taşınabilirlik, kolay erişilebilirlik ve kurulum ve bakımda sağladığı avantajlar bakımından internet tabanlı uygulamaları öne çıkarmakta. Buna karşın farklı bölgelerde dağıtık yapıda olmayan, küçük işletmeler için güvenlik riski/maliyeti daha düşük olan C/S olarak geliştirilen ürünler tercih edilebilir.

Uygulamanın kullandığı yada desteklediği veri tabanları incelendiğinde uygulamaların yarıya yakınında bilgiye ulaşılamadı. Elde edilebilende ise MS Access, My SQL, SQL Server ve ORACLE veri tabanlarının kullanılabildiği görüldü.

5. Sonuç

Bilgi ve bilgi teknolojisinden kaynaklanan risklerin yönetiminde; günümüz iş dünyası gereksinimleri, yasal düzenlemeler, teknolojik gelişmeler ve artan rekabet koşulları, kurumsal risk yönetimini zorunlu kılmaktadır. Diğer taraftan kurumsallaşmayı hedefleyen şirketler artık kurumsallığın bir gereksinimi olarak yaptığı işlerde ilgili standartları da dikkate almak zorundadır.

Gerçekleşecek bir bilgi güvenlik riskinin kuruma maliyetini önceden tam olarak kestirebilmek zor olsa da bu riskleri kabul edilmiş bir risk metodolojisini kullanarak önceden kestirebilmek ve yönetebilmek mümkündür.

Kurumlar madden ve manen varlıklarını etkin bir şekilde devam ettirebilmek için, kendi ihtiyaçları doğrultusunda bir risk yönetim metodolojisi belirlemeli ya da var olan risk metodolojilerinden birini seçmelidir. Seçilen metot kurumda etkin bir şekilde uygulanmalı, periyodik olarak izlenmeli ve alınan risk iyileştirme kararları doğrultusunda giderilmeli ya da kurumun kabul edebileceği bir seviyeye indirgenerek revize edilmelidir.

Bu çalışma, risk yönetim metodolojileri yapmak isteyen kurum ya da kuruluşlara mevcut belli başlı risk metodolojileri hakkında bilgilendirilmesine yönelik inceleme sonuçlarının paylaşımından oluşmaktadır.

Bu çalışmada incelenen uygulama yazılımların pek çoğu aynı zamanda bilinen bir standardı da referans almaktadır. İnceleme sonuçlarına göre en yaygın, bilinen ve aynı zamanda bilgi güvenliği yönetim sistemi(ISO 27001)'ni de destekleyen uygulamalara; Art Of Risk, Real ISMS ve ISMart'ı tercih edilebilecek örnek uygulamalar olarak verebilir. Bununla birlikte her kurum kendi ihtiyacı doğrultusunda ihtiyaçlarına cevap verecek uygulama yazılımını kullanmalı ya da kendi ihtiyacı doğrultusunda uygun yazılımını geliştirmelidir.

Araştırma sonuçları anlamlandırılırken araştırmanın zaman dilimi, uygulamalara sınırlı erişim hakkı olan kullanıcı ya da 'demo' programlarının kullanılması veya diğer internet kaynakları aracılığıyla elde edilen bilgilerin değerlendirilmesi sonucunda elde edildiği göz önünde tutulmalıdır.

6. Kaynakça

[1] ISO 27001 Information Security Management System

[2] ISO 27005 Information Technology Risk Management

[3] BDDK İlkeler Tebliği, *Eylül 2007*

[4] Cobra, http://www.riskworld.net/benefits.htm, *Ekim 2009*

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

[6]Cramm,http://www.cramm.com/files/datasheets/CRAMM%20(Datasheet).pdf, *Ekim 2009*

[6] Cramm, http://www.cramm.com/overview/ *Mayıs 2009*

[7] Cramm Management Guide, Page:10, *April 1996*

[8] Octave Criteria V.2.pdf, Syf.7, *December 2001*

[9] Ebios, http://en.wikipedia.org/wiki/EBIOS, *Ekim 2009*

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

[11]Isamm,http://www.bankingfinance.nl/42828/DossierTelindusBelgacom.pdf, *Kasım 2009*

[12]Art Of Risk, http://www.aexis.de/index.php?site=static&staticID=4 , *Ekim 2009*

[13] RealISMS, *Haziran 2009*

http://www.realismssoftware.com/

[14] ISMart, http://www.biznet.com.tr/ismart_faq.htm, *Ekim 2009*

[15]Callio,http://www.callio.com/PDF/Calio_Secura17799.pdf, *Ekim 2009*

[16] Callio, http://www.callio.com/bs7799/id,301, *Mart 2009*

[17]Proteus,http://rm-inv.enisa.europa.eu/methods_tools/t_proteus.html, *Ekim 2009*

[18]RiskWatch,http://rminv.enisa.europa.eu/methods_tools/t_riskwatch.html, *Ekim 2009*

[19] ISMS-RAT, *Ekim 2009* http://www.brothersoft.com/isms-rat-74927.html

[20]ENISA,http://rm-inv.enisa.europa.eu/rm_ra_methods.html, *Ekim 2009*