GİRİŞİMCİLİKTE BİLGİ VE İLETİŞİM TEKNOLOJİLERİNİN OLUŞTURDUĞU OPERASYONEL RİSKİN YÖNETİMİ: FİNANSAL BAKIŞ AÇISI*

Esma YENİSARI
Araş. Gör., Çanakkale Onsekiz Mart Üniversitesi
Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü
esmay@comu.edu.tr

Bahadır KARASULU
Yrd. Doç. Dr., Çanakkale Onsekiz Mart Üniversitesi
Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü
bahadirkarasulu@comu.edu.tr

Bora UĞURLU
Öğr. Gör. Dr., Çanakkale Onsekiz Mart Üniversitesi
Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü
boraugurlu@comu.edu.tr

Geliş Tarihi: *10.07.2014*
Kabul Tarihi: *26.09.2014*

ÖZ

Girişimcilikte, sosyal ve finansal risklerin belirlenmesi ve buna uygun stratejinin oluşturulması önemlidir. Girişimci, ilgilendiği alanda var olan riskleri üstlenebilen, baskı altında karar verebilen ve etkin bir biçimde kaynak tahsislerini yapabilendir. Operasyonel risk; organizasyondaki çalışanlardan, sistem veya harici olaylardan kaynaklanmaktadır. Finansal kayıplar operasyonel risk olayı sonucunda oluşabilmektedir. Bilgi teknolojileri, finansal piyasalarda sıklıkla kullanılmaktadır. Sosyal ve güvenlik riskleri, doğal afetler, ve yetkisiz erişimler gibi nedenler de risk olaylarını doğurabilmektedir. Girişimcinin, rekabet ortamında sistem ve faaliyetle ilgili tehlikelerin farkında olması ve analiz araçlarını kullanarak operasyonel risk yönetimini yapılabilmesi gerekmektedir. Bu sayede; riskin kontrol edilebilmesi adına gerekli araç ve mekanizmalar kullanılabilmektedir. Çalışmamızda, girişimcilerin finans piyasalarında bilgi ve iletişim teknolojileri kaynaklı operasyonel riskleri yönetebilmesinde başvurabilecekleri çeşitli metodolojiler,

*Bu çalışmanın bir bölümü 34. Yöneylem Araştırması ve Endüstri Mühendisliği (YAEM 2014) Ulusal Kongresinde sözlü bildiri olarak sunulmuş ve özet metin olarak bildiri özetleri kitapçığında yer almıştır.

standartlar ve yazılımsal araçlar incelenmiştir. İncelemelere dayanılarak varılan sonuçlar, karşılaştırma, kıyaslama ve tartışma yoluyla sunulmaktadır.

Anahtar Kelimeler: Bilgi Teknolojileri, Finansal Riskler, Risk Yönetimi, Girişimcilik.

OPERATIONAL RISK MANAGEMENT IN ENTREPRENEURSHIP BASED ON INFORMATION AND COMMUNICATION TECHNOLOGIES: A FINANCIAL VIEW

ABSTRACT

In entrepreneurship, social and financial risk determination and appropriate strategy are very important. Entrepreneur can effectively allocate the resources, make decision under stress, and take responsibility of existing risks about related area. Operational risk arise due to employees in the organization, systems or external events. Financial losses can occur via operation risk event. Information technologies are mostly used in financial markets. Risk events are emerged by social and security risks, natural disasters, and unauthorized access. In competitive environment, entrepreneur should manage operational risks via using analyses tools, and be aware of threats of system and its operation. Therefore related tools and mechanism about risk control can be used. In our study, various methodologies, standards and software tools are reviewed. For management of operational risk in financial markets, entrepreneur can refer these that risks are based on information and communication technologies. The conclusions are presented by discussion, comparison and crosschecking.

Keywords: Information Technologies, Financial Risks, Risk Management, Entrepreneurship.

GİRİŞ

Finans piyasalarında önemli durumların organizasyonel sorunlara ve finansal kayıplara bunun yanı sıra itibar kaybına neden olabildiği; bu tarz kayıpların da temelde ölçülebilir ve kontrol edilebilir bazı kriterlere bağlı olduğu görülmektedir. Bir finansal krizin ortaya çıkmasında genellikle yönetimsel ve uzun vadeli sistematik hatalar başlıca nedenleri oluşturmaktadır. Risk, başarılması gereken amaçların üzerinde oluşan bir belirsizlik olayının ortaya çıkmasıdır. Bu açıdan risk çeşitli seviyelerde olmakta ve belirsizliğin getirmiş olduğu etkilere maruz kalmaktadır. Finans piyasalarındaki risk bu tarz anomalilerin farklı perspektiflerden değerlendirilmesine ihtiyaç duymaktadır. Risk; risk değerlendirme (assessment), risk azaltma (mitigation) ve risk raporlama ile incelenebilir. Operasyonel riskler (OR) sıklıkla personel, sistem, organizasyonel, yasal ve teknolojik riskler şeklinde ortaya çıkmaktadır. Operasyonel riskin tam bir tanımı üzerinde literatürde ortak bir karara

varılamamıştır. OR çeşitli bakış açılarıyla tanımlanabilir. Bunlardan bilgi sistemleri (information system, BS) bakış açısıyla sistemin çalışmasını etkileyen, beklenmedik kayıplara neden olan ve uygun olmayan süreçler, personel ve harici olaylar risk oluşumuna neden olmaktadır. Bunlara daha yakından bakılacak olursa beş ana kategoride değerlendirme yapılabilir. Organizasyon kategorisi; değişim yönetimi, proje yönetimi, şirket yönetimi ve iletişim, sorumluluklar gibi konuları içermektedir. Kural ve süreç kategorisinde yerleşim ve ödeme süreçlerindeki zafiyetler, müşterilerle görüşme veya ürünlerdeki hataların idare edilmesinde, harici düzenlemelere dayanan kurallarla uyumdan kaynaklanan risk oluşmaktadır. Teknoloji kategorisinde; donanım ve yazılım sorunlarında, telekomünikasyon ve bilgisayar ağları gibi bilişim alanında güvenlik ve organizasyon kapsamında ortaya çıkan riskler oluşmaktadır. Personel kategorisinde; işveren ve çalışanların hatalarından dolayı, çıkar çatışması veya diğer istenmeyen davranışlardan dolayı riskler ortaya çıkmaktadır. Harici kategoride; üçüncü taraf firmaların açmış olduğu davalar ve dolandırıcılıktan veya fiziksel güvenlik eksikliğinden dolayı çeşitli riskler ortaya çıkmaktadır (Doerig ve Chairman, 2003).

BS'leri ve Bilgi Teknolojileri (information technology, BT) gün geçtikçe önem kazanan ve finans piyasalarında neredeyse vazgeçilmez hale gelmektedir. Organizayonel ana çatılar, risk oluşumuna oldukça fazla yatkındırlar. BS/BT her organizasyonda ve her finans kuruluşunda risk değerlendirilmesinde önemli rol oynar. Bunun iki önemli nedeni bulunmaktadır. İlki, BS/BT organizasyon içerisindeki tüm farklı fonksiyonel alanları birleştirmekte böylece risk değerlendirme işlemlerinin yapılabilmesine olanak sunmaktadır. İkincisi, düşük kaliteli bilginin elde edilme ve kullanımı azaltıcı yönde oluşan risklerin yönetilmesini ve veri işleme konularında BT/BS kullanılmaktadır. Bu sayede iş süreçlerinin kalitesinin artırılmasında her bir sürecin çekirdek kısmını bilgi oluşturmaktadır. Bu bilginin işlenmesi oldukça önemlidir. Bu nedenle iş riski ve BT riski arasında fark bulunmamaktadır (Svatá ve Fleischmann, 2011). Finans piyasalarında bağımsız veya örtüşen birçok risk sınıfı bulunmaktadır. Burada dikkat edilecek konu riskin yönetilebilmesi için bu sınıfların doğru bir şekilde ayrıştırılarak belirlenebilmesidir. Doerig ve Chairman (2003) çalışmasına göre risk sınıfları; kredi riski, market riski, iş riski, sigortalama riski olarak verilebilir. Bu sınıflar daha üst sınıf olarak nitelendirilebilecek itibar riski, strateji riski ve operasyonel risk bulunmaktadır. Bunlar ilk dört risk ile kesişmektedir. BT riskinin iş riski ile eşdeğerde olmasından dolayı özellikle iş riski konusuna çalışmamızda odaklanılmıştır. Operasyonel risk yönetimi (ORY) bu tarz riskin tanımlanması, izlenilmesi, değerlendirilmesi, raporlanması ve kontrolü için gereken süreçleri, kuralları araç veya me-

kanizmaları belirli adımlara uygun olarak içermektedir. Doerig ve Chairman (2003) çalışmasında ORY'nin oluşturulması için dört basamaklı bir yapı ortaya koymuştur. Buna göre veri toplama; risklerin, önemli iş birimleri arasındaki ilişkinin, insan gücü kullanımının ve teknoloji kullanımının belirlenmesi için ilk adım olarak "belirleme" adımında yapılmaktadır. İkinci adım olarak risk takibinin ölçülebilir bir şekilde yapılması, raporlama mekanizmasının oluşturulması, otomatikleştirilmiş veri toplama ve teknoloji iş akışına dair yatırımın belirlenmesi "ölçütler ve takip" adımında gerçekleştirilmektedir. Üçüncü adım, modelleme yaklaşımın sürekli arındırılarak geliştirmenin iyileştirilmesi, OR verisinin oluşturulması, OR gruplarının büyük çoğunluğunun oluşturulmasıdır. Teknoloji geliştirme çabasının ortaya konması "ölçüm" adımında gerçekleştirilmektedir. Dördüncü adımda yönetim sürecinin içerisine OR verisinin entegre edilmesi, üst düzey yönetim ilişkisinin ortaya konması, ORY'e maruz kalmanın yönetilmesi, süreçlerdeki sınırlı teknoloji veya insan gücü isterlerine ait ilişkinin belirlenmesi "tümleştirilmiş yönetim" adımında yapılmaktadır. BT riskleri sınıflandırılacak olursa başlıca riskler arasında güvenlik riski, hazır bulunabilirlik riski (availability), performans riski, uyum riski (compliance risk) bulunmaktadır (Savić, 2008). Finans kurumuna karşı yapılacak herhangi bir saldırının oluşturacağı tehdidin büyüklüğünün değerlendirilmesi adına farklı disiplinlerden uzmanların ve verilerin bir araya getirilerek bir ortak zekâ oluşturulması, bu sayede güvenlik riskinin tanımlanması ve değerlendirilebilmesi mümkün olmaktadır. Günümüzde mobil platformların daha sık kullanılması bunların zafiyetlerinin çeşitli art niyetli kişilerce sızma girişimi veya finansal kayıp verdirme şeklinde özellikle bankacılık sektöründe etkili olmaktadır. Bu tarz sorunlarla baş edebilmek için güvenlik riskinin temel nedenlerinin neler olduğuna bakmak gerekir. Bilginin değiştirilmesi, bilgiye yetkisiz kişilerce erişilmesi, çalışma şartlarından memnun olmayan finans piyasası çalışanları, platform ve mesajlaşma tiplerindeki çeşitlilik bu nedenler arasında sayılabilir. Sosyal mühendislik, şirket içi iletişimdeki sorunlar, şirketin BT bölümündeki çalışanların siber güvenlik konusundaki dikkatsizlikleri özellikle harici dolandırıcılık, müşteri bilgilerine zarar verilmesi gibi konularda riski ortaya çıkartmaktadır. Risk sınıflarından olan kredi ve piyasa riskleri finans kurumunun dışından kaynaklanırken OR sınıfı temelde organizasyonun içerisinden kaynaklanmaktadır. Fakat harici nedenlerde bu riski artırıcı yönde etki etmektedir. Bu diğer riskler arasında aykırı olarak belirtilebilecek bir piyasa riski cinsi olan akışkanlık riski de bulunmaktadır. Finans piyasalarındaki para akışkanlığın artması ulusal finans kuruluşlarına yapılan saldırı sayısını da artırmaktadır. Özellikle Ortadoğu, Latin Amerika ve Asya Pasifik bölgesinde ekonomik olarak gelişmekte olan ülkelerin para akışları dolandırıcıların

BT tabanlı saldırılarında ön plana çıkmaktadır. Operasyonel verinin kullanımı veriye-hassas süreçlerin finans kurumlarınca güvenliğinin sağlanması ve taşınabilirliğin kontrolünün düzgün bir şekilde BS/BT kullanımı ile gerçekleştirilmesi gün geçtikçe önem kazanmaktadır. Bu bakış açısıyla veri seviyesi güvenliğine bağlı olarak büyük veri (big data) ile uğraşmak uzun yıllardan beri en önemli gündem maddelerinden birisi olmuştur. Günümüzde bulut bilişim (cloud computing) teknolojisinin gelişmesiyle yeni mimarilerin istenmeyen davranışların izlenilmesinde büyük hacimli verilerin daha güvenilir bir biçimde yönetilebilmesi gittikçe önem kazanmaktadır.

Mobil teknolojiler ve bulut bilişimin gün geçtikçe kullanımının artması finans piyasalarındaki kurumların veri çapı ile orantılı olarak ağ çaplarının da değerlendirmeleri gerektiğini, ağ çapı büyüdükçe taneselliğin (granularity) derecesinin artış göstererek, iletişim ve güvenlik konularında daha fazla kurallara yönelik iyileştirme ve süreç idaresine yatkın yaklaşımların ortaya konmasını gerektirmektedir. İş zekâsı (business intelligence) alanında çeşitli metodolojiler ve teknolojiler, yapısallaştırılmamış verinin elde edildiği kaynakları göz önüne alarak, veri içerisindeki anlamlı örüntülerin keşfedilmesi gerekiyorsa programa uygun olarak organize edilmesi ve buna dayanılarak çeşitli analitik iş başarımı ve planlama mekanizmalarını önermektedir. İş analitik'i yönetim bilimine oldukça yakın ve risk yönetimi için benzetim, istatistiksel ve makine öğrenmesine yatkın çeşitli metodolojiler ve teknikler sunmaktadır. Bu sayede, ilişkisel yönetim sistemleri ile büyük verinin büyük hacmi piyasalardaki risk doğuracak ana nedenler üzerinden OR olaylarının olabilirliğinin ve ana risk göstergelerinin (key risk indicators, ARG) belirlenerek değerlendirilmesinde kullanılabilir. Böylelikle, ORY metodolojileri olarak BS/BT alanında risk oluşumu, oluşan riske dair ölçüm ve ölçütler, altta yatan verinin hangi kategorilere uygun olabileceğine dair bir inceleme çalışmamızda yapılmıştır. Analitik, iş bilgi keşfini sağlayan ve en iyi kararda fikir kılmaya yardımcı nicel süreçleri inşa eden programdır. Analitik programları kendisine zemin olarak; veri madenciliğini, istatistik analizi, tahminlemeyi ve iş-süreç modellemesini almaktadır. Bu sayede uzmanlara karar destek açısından yardımcı olacak bir araç olarak kullanılabilmektedir. Başka bir ifade ile, analitikler verideki anlamlı örüntülerin keşfi ve aktarılmasıdır. Bunlar, kayıtlı bilgilerin değerli olduğu alanlarda bilgisayar programlama ve yöneylem araştırmaları kullanılarak başarımın ölçümlenmesinde kullanılabilmektedir. İş başarımı, iş karar yönetimi gibi alanları da kapsayacak şekilde eniyileme ve analiz yaklaşımıyla sağlanabilmektedir. Çoğunlukla yoğun hesaplama (büyük veri), yazılım ve algoritmalar kullanılmaktadır. İş analizi ve iş analitiklerinden farklı olarak iş zekâsı ana çatısı ve Web

analitikleri sayesinde, Web üzerinden gerçekleşen oturum-seviyesinde son kullanıcı etkileşimlerinin bulunduğu, özellikle sosyal medya gibi Web 2.0 teknolojilerinin yoğun olarak kullanıldığı, çeşitli mecralardan bilgi elde edilmesine dayalı BS'ler oluşturulabilmektedir. Bu yaklaşımın, girişimciye pazarlama stratejileri oluşturmasında yardımcı olacağı görülmektedir. Web analitik 3.0 (en güncel versiyon), betimsel ve tahminsel temeller göz önüne alınarak, Web analitik 1.0 ve 2.0'dan oluşturulmuştur. BS/BT açısından bakıldığında Web analitikleri, veri analistlerinin işlerini kolaylaştırmak için ortaya atılmış, sürekli geliştirilmekte olan, ölçüm ve ölçütlere dayalı bir teknolojiyi ifade etmektedir. Geleneksel veritabanı yönetim araçları ve veri işleme uygulamaları ile işlenilmesi oldukça zor olan veri setleri topluluğu şeklindeki oldukça büyük miktarda verinin kontrol edilmesi ve güvenliğinin sağlanması sıklıkla risk olayı oluşumuna neden olmaktadır. Bu açıdan günümüzde, Web analitik 3.0'ın ve büyük verinin oluşturmuş olduğu ortam sayesinde iş zekâsı, finans piyasaları için hem ilgi çekici hem de yönetimsel sorunların çözülebilmesinde dayanak olması nedeniyle, nihai çözüm için karar vericilere destek olmaktadır.

Bu çalışma üç bölümden oluşmaktadır. Birinci bölümde operasyonel risk yönetim metodolojilerine ve BT alanında karşılaşılan risklere değinilmektedir. Aynı bölümde literatür araştırması yapılarak uygulama örnekleri üzerinden OR ve bunun BT sektöründeki yansımalarına yer verilmiştir. İkinci bölümde konuyla ilgili çeşitli yazılımsal çözümler ele alınmaktadır. Üçüncü bölümde, örnek çalışmalar incelenerek karşılaştırma yoluyla bir tartışma yapılmıştır. İlgili bölümde çalışmamızda varılan sonuçlar sistematik bir biçimde verilmektedir.

1. OPERASYONEL RİSK YÖNETİM METODOLOJİLERİ

Risk değerlendirmesi temelde üç farklı bağlamda incelenebilir: olaylar, güvenlik konuları ve güvenlik değerlendirmesi. Olaylar, riskin yüksek seviyesini yansıtmakta ve acil eylemlere ihtiyaç duymaktadır. Bu tarz risk olayları çeşitli senaryo analizleri ile olabilirlikleri ve organizasyon üzerindeki etkileri açısından değerlendirilebilmektedirler. Bunun yanı sıra güvenlik konuları hangi eylemin risk sonrasında yapılacağının güçlü bir yoldan belirlenebilmesinde kullanılmaktadır. Güvenlik değerlendirmesi özellikle incelenen finans kuruluşuna ait planlama adımlarının değerlendirilmesinde aktiviteleri de içermektedir (ARMS working group, 2010). Çeşitli risk değerlendirme ana çatılarının tanımlayabildiği üç farklı boyut bulunmaktadır: BT'nin kapsam derinliği, risk yönetim kapsamının tamlığı, riske ve kontrole odaklanmış yaklaşımlar arasındaki dengenin seviyesidir (Svatá ve Fleischmann, 2011). Her

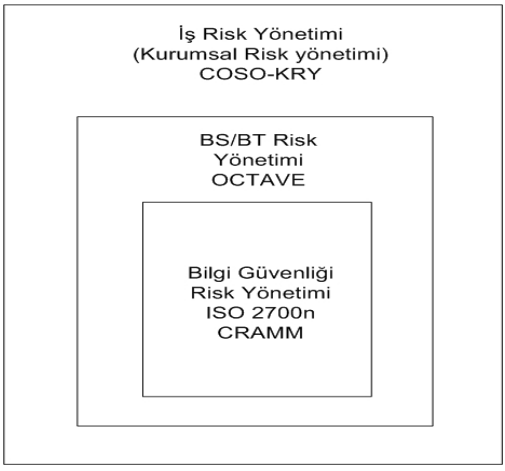
bir risk yönetimin ana çatısı BT alanını farklı ele almaktadır. Özellikle BT risk yönetimi için BT risk yönetimini dikkate almayan örnekler arasında COSO-KRY (Committee of Sponsoring Organizations of the Treadway Commission-Enterprise Risk Management), AS/NZS 4360 (Standards Australia/New Zealand 4360), ISO 31000 (International Standard Organization 31000) ve BASEL II bulunmaktadır. Bununla beraber bu ana çatılar finansal organizasyonlar için oldukça önemli standartlardır. Bu ana çatıların bir şekilde BT risk yönetimi ile entegre edilmesi gerekmektedir. Strateji riski bir finansal kuruluşun var olan tabanı ve onun seçenekleri ile ilgilenmekte ve bunları analiz etmeye çalışmaktadır. Strateji bu anlamıyla doğru şeyi doğru zamanda yapmaktır. Stratejiden daha çok gerçekleştirim OR'ye dönüşmektedir. Piyasalarda çeşitli kurum ve kişilerce yapılan oldukça göreceli değerlendirme kullanılmaktadır. İtibar riski çoğunlukla harici ve dâhili faktörlere bağlı olarak oluşmakta, uzunca bir süre üzerinden doğru şeyin doğru zamanda yapılması ile ortaya çıkmaktadır. İtibarın en iyi kanıtı başarının paylaşımı, gelir artışı, müşteri sayısının artışı ve kuruma olan ilgidir. İtibar ile ilişkili bu öğelerdeki en küçük bir değişiklik riski arttırmaktadır (Doerig ve Chairman, 2003). Finans piyasalarında OR için birçok farklı tür bulunmaktadır. Bu türlerin oluşturduğu OR olayları; dâhili dolandırıcılık (çalışanların yaptığı usulsüzlük), harici dolandırıcılık (çek kırdırma, hırsızlık ve bilgisayar korsanlığı gibi), iş yeri ile ilgili güvenlik ve diğer sorunlar (çalışanların sağlığının bozulması ve iş yeri kurallarının ihlali), müşteriler, ürünler ve iş uygulamaları (banka hesabı üzerinde yetkisiz işlemler yapılması), fiziksel zarar (deprem, yangın, sel vb.), sistem hataları (telekomünikasyon, yazılım vb.), çalıştırma, teslimat ve süreç hatalarıdır (veri giriş hatası, yetkisiz erişim vb.) (Chutia, 2013). ORY süreci genellikle finans kuruluşu için riskin tanımlanmasını, bu riskin ölçülmesini kapsamakta böylece etkin bir yoldan anapara planlaması ve yerinde programı izleme, riske maruz kalmayı izleme ve anapara ile ilgili devam eden temelde anapara ile ilgili isterleri ve riske maruz kalmayı azaltıcı ve kontrol edici adımları içermektedir. OR'nin tanımlanması için finans kuruluşu tüm sistemler, süreçler, aktiviteler, hizmetler ve ürünler için doğal olarak OR'yi tanımlamalı ve değerlendirmelidir. Etkin risk tanımlama için hem dâhili hem de harici faktörlerin göz önüne alınması gerekir. Dâhili faktörler arasında finans kuruluşunun yapısı, finans kuruluşunun aktivitelerinin doğası, insan kaynaklarının kalitesi ve organizasyonel değişikler arasında sayılabilir. Harici faktörler arasında endüstri ve teknolojideki değişimler sayılabilir. Öz riski değerlendirme, potansiyel olarak savunmasız olduğu alanları belirleyerek bunlara karşı gerekli aktivite ve operasyonların finansal kuruluşça yapılabilmesini içermektedir. Bu süreç dâhili olarak sürdürülmekte ve genellikle bir kontrol listesi şeklinde yapıl-

maktadır. Bu kontrol listesi OR ortamının güçlü ve zayıf yanlarını tanımlamaktadır. Risk haritalama sürecinde çeşitli iş birimleri organizasyonel fonksiyonlar ve süreç akışları risk türleri ile eşleştirilmektedir. Bu şekildeki çalışma ardıl yönetim eylemlerin gerçekleştirilmesine yardımcı olmaktadır.

Ölçütler veya istatistikler ARG'yi oluşturmaktadır. Finansal kuruluşun risk pozisyonu ARG ile gösterilmektedir. Oluşan hataların sıklığı, personelin rotasyon oranı ve ticari başarısızlıkların sayısı bu göstergeye eklenebilir. Bu göstergeler için en önemli olgu ölçüm ve ölçütlerdir. Bu sayede operasyonel riskin azaltılması ve kontrolü mümkün hale gelmektedir. Operasyonel zarar olaylarının izlenmesi için finans kuruluşları uygun göstergeleri belirlemek zorundadır. Böylece gelecekteki zararların oluşturacağı risk artışı için önceden tedbir alınabilir. Bu tarz göstergeler ileriye yönelik bir bakış açısı getirerek yeni ürün ve çalışanların etkisini de ortaya koymaktadır. Bu tarz izleme işlemleri periyodik bir süreç olarak yapılmaktadır (Chutia, 2013). Yönetilebilmenin daha kolay bir yoldan gerçekleştirilmesi adına finansal endüstri yöneticileri ve düzenleyicileri OR'nin ölçümüne daha fazla önem vermektedir. OR'nin ölçülebilir olması bir açıdan da yönetimin kontrol edilebilir olduğu anlamına gelir. Piyasa ve kredi riski gerçekleştirimine benzer olan ve ölçümü temel alan bir veri tabanı oluşturulmasına teknoloji ve harici riskler izin vermelidir. Ölçüm için iki farklı kategori bulunmaktadır. Bunlar nitel ve niceldir. Bu yolla ekonomik anapara kaybı, yönetim baskısı, etkinlik eniyilemesi gibi sebeplerle oluşan ve uzman girdileri, veri analizi, modelleme gibi metotlarla ortaya çıkan risk seviyesi değerlendirmesi yapılabilmektedir. Nitel ve nicel yaklaşımların kombinasyonu gelecek vaat eden ORY için bir yol açmaktadır. Bazı karmaşık modeller OR'yi bir miktar hesaplayabilmektedir. Risk kontrol göstergelerinin (risk control indicators, RKG) karmaşık modellerin kullanımına göre daha yararlı olduğu ORY ile ortaya çıkmaktadır. Risk ölçütleri (metrics) riskin nereden geldiğinin belirlenmesi konusunda bilgi sağlamaktadır. Bunlar, ARG'lerin göz önüne alınması ile riskin nereden kaynaklandığının belirlenmesine yardımcı olmaktadırlar. Bir ARG, riskin trendi ve seviyesini gösteren bir ölçüttür. Bir ölçüt, bir kuruluşun stratejik amaçları için hedeften ne kadar saptığını belirleyebilir. Ölçüt değerlerinin ölçülmesi ile risk ölçütleri, sonraki stratejik amacın uygun olup olmadığı hakkında bilgi verir. Bu açıdan finansal kuruluşların işlemlerini oldukça kolaylaştırmaktadır. Herhangi bir ölçüt bir amaç, bir yorum ve raporlama yapısına ihtiyaç duymaktadır. Bu sayede karar verme süreci işletilir, eğer az sayıda ölçüt varsa bu süreç oldukça zor işlemektedir (Scarlat, 2012). Çeşitli nedenlerden dolayı ölçütler kullanılmaktadır. Yatırımın getirisi (maliyet/kar analizi), seçimlerin değerlendirilmesi, alternatiflerin

karşılaştırılması, iyileştirilmelerin izlenmesi, problemlere erken uyarı verilmesi, tahmin yapılması, rekabete veya bir standarda karşı bir kıyaslama yapmak için ölçütler kullanılır (Amland, 1999). BT yönetişim ana çatısı (governance framework) ve standartları, BS ve BT altyapısından kaynaklanan farklı seviyelerdeki OR'lere cevap vermede sorun yaşamaktadır. ORY için çeşitli çalışmalarda BT eklentileri ve BT kontrol listeleri önerilmiştir. Çeşitli kurum ve kuruluşlar BT süreçlerinden kaynaklanan ORY ile ilişkili teknik dokümanlar ve eklentileri geçtiğimiz yıllar içerisinde yayınlamışlardır. Bunlar, çeşitli bilgi kontrol modelleri içermekte ve bunlar, zarar olay tipleri olarak tanımlanan OR kategorileri için eşleştirilmekte ve değerlendirilmektedir. İş riski yönetimi, aynı zamanda kurumsal risk yönetimi (enterprise risk management, KRY) olarak değerlendirilmektedir. Bunun kökeninde çeşitli kaynaklar bulunmaktadır: Kredi, stratejik, piyasa, rekabetçi ve operasyonel kaynak. Bu sayede küreselleşme, entegrasyon ve karmaşıklıkla ilgili olarak BT'ye dayalı oluşan önemli risk türleri ortaya çıkmaktadır: uyumluluk, finansal ve teknoloji riski. Her bir risk yönetimi çatısı, risk kategorizasyonu için farklı bir yaklaşım uygulamaktadır. Bu ana çatıların BT kapsamının derinliği için örnek olarak ISO 2700n ve CRAMM (Central Computing and Telecommunications Agency (CCTA) Risk Analysis and Management Method) verilebilir. Fakat bunlar iş risk yönetimini BT risk yönetimine ciddi olarak entegre etmeyi denememişlerdir. OCTAVE (Operationally Critical Threat and Vulnerability Evaluation) gerçek anlamda BT riskini organizasyonel riske eklemiştir. Şekil 1'de risk yönetiminin farklı kapsam seviyeleri görülmektedir.

Şekil 1. Risk Yönetimi İçin Farklı Kapsam Seviyeleri



Kaynak: Svatá ve Fleischmann (2011, s.44)

Elektronik bankacılık ve elektronik aktivitelerin iş operasyonlarının üzerindeki karmaşıklığı arttırması nedeniyle finans piyasalarında BT kullanımından dolayı risk gün geçtikçe artmaktadır. Yukarıda belirtilen ana çatılarla ve çeşitli eklentilerle BS/BT risk yönetimi ve güvenirlik risk yönetimi daha önemli hale gelmektedir. Takip eden bölümlerde risk oluşumu, riskin ölçümü ve buna ait ölçütler, veri kategorizasyonu, maliyet gibi konularda yapılan çalışmalara değinilmekte ve ORY yazılım ve ortamlarının detaylarından bahsedilmektedir.

1.1. Literatür Araştırması

Literatürde birçok çalışma BT kaynaklı riskin yönetilmesini kendine konu edinmiştir. Savić (2008) çalışmasına göre BT risk sınıflandırması dört ana gruptan oluşmaktadır. Bunlar güvenlik riski, hazır bulunabilirlik riski, başarım riski ve uyumluluk riskidir. Mobil ve elektronik ticaret hizmetlerinin her an elde edilebilir olması için iş sistemlerinin güvenilir, elde edilebilir ve yüksek başarımlı bir biçimde BT ilkelerine uyumlu olarak çalışması gerekmektedir. En çok sorun oluşturan durumların başında kullanıcıların yüksek teknolojiye karşı olan dirençleri ve tekrar eden yanlışlar yapabilmeleri bulunmaktadır. Bu durumlar, sistem ve süreçleri etkilemekte ve OR'nin artışıyla kalitenin düşüşü de yaşanmaktadır. Güvenlik duvarı ve ilgili güvenlik önemleri işin sürebilmesi için anahtar olgulardır. Çoğu sistem yedekleme yapmamaktadır. Bu durum değerlendirilirken yedeklemenin maliyet/kâr analizinin yapılması gerekmektedir. Çoğu zaman iş hattı süreçleri ile BT birbiri ile ayrılmış durumdadır. Yeni sistem ve süreçlerin risk kaynaklarını yok etmesi beklenirken yenilerini eklediği ve çoğu zaman da yeni problemlere yol açtığı görülmektedir. Finans kuruluşlarının bu açıdan güvenliği önemseyen bir kültüre sahip olması gerekir. Böylece geleceğe dönük risk tanımlama ve kestirim iş süreçlerine dâhil edilebilir. Finansal kuruluşun ağ yapısındaki kullanıcıların kurum içi ve dışı olmak üzere yoğun olarak kullandıkları elektronik posta (e-posta) içeriklerine üçüncü şahıslar tarafından erişilmesi, okunması ve/veya değiştirilmesi kurum içi iletişimi tehdit eden BT kaynaklı risklerin başında gelmektedir. E-posta parolalarının yeterince özenli seçilmemesi ve şifrelenmemesi bu riskin ortaya çıkmasına neden olmaktadır. Bunun yanı sıra kullanıcıların kurum içi cihazlara kurmuş oldukları üçüncü parti yazılımlar güvenlik açıklarını da beraberinde getirmektedir. Bu tür yazılımlar bilgisayar virüslerini de bünyelerinde barındırma olasılığına sahiptirler. Kullanıcıların herhangi bir kontrol mekanizmasından geçirmeden cihazlara kurmuş oldukları üçüncü parti yazılımlar kurum içi verilere izinsiz erişebilme, bu verileri değiştirebilme ve kurum dışarısında diğer

kişilerle paylaşabilme olasılığını da gündeme getirmektedir. Bunlardan korunmak ve riskin azaltılması adına güncel anti-virüs yazılımları, güncel İnternet tarayıcıları kullanılması gerekmekte, zor çözülebilen parola kullanmak ve bunu sıklıkla değiştirmek, sadece güvenli siteler üzerinden bilgi paylaşımında bulunmak ve güvenlik duvarı yazılımı üzerinden trafiğin izlenmesi gerekmektedir. Bunlar yetkisiz erişimin önlenmesi ve veri güvenliği adına önemli konulardır.

Herhangi bir doğal afet ve sistem hatası nedeniyle erişilemez olan uygulama bilgileri bulunduğu durumlarda hazır bulunabilirlik riski (availability risk) oluşmaktadır. Bunların ana kaynakları, donanım hataları, ağ kesintileri, veri merkezi hatalarıdır. Bu riskin etkileri arasında iptal edilmiş işlemler, kayıp satışlar, işin kritik süreçlerindeki kesinti ve gecikmeler bulunmaktadır. Başarım riskinin oluşmasının temel kaynakları arasında zayıf sistem mimarisi, ağ tıkanıklığı, etkin olmayan kod ve uygun olmayan kapasite bulunmaktadır. Bu nedenle, iş üretkenliği ve değeri azalmakta sistem uygulama ve personelin başarımı düşmektedir (Savić, 2008). Referans veri temel bilgi öğelerini içermektedir. Bunlar; müşterileri tanımlayan güvenlik ve işlemsel akışları belirten öğelerdir. Bu akışlar otomatikleştirilmiş finansal sistemler üzerinden yapılmaktadır. Ayrıca, güvenlikle ilgili istatistiksel bilgiler de içerilmektedir. Ticaret yapılan iş ortakları ve finansal enstrümanlar hakkında betimleyici bilgi içeren bir küme olarak referans veri tanımlanabilir. Bu tür veri, geniş aralıktaki bir özel iş fonksiyonuna bağlı bilgiyi ve bunun kullanım amacına sahiptir. Referans veri kategorileri; portföy yönetim bilgisi, yerleşim bölgesi ve ticaretle ilgili özel bilgilerin satışı, müşteri/karşı taraf tanımlayıcıları, şirket eylemleri ile ilgili bilgilerdir (Grody v.d., 2006). Referans veri sistemleri tüm işlemlerin merkezinde yer almakta, her bir işlem için temel öğeler hakkında kritik verileri tutmaktadır. Böylelikle, ticari uygulamalar ve çeşitli finansal yönetim uygulamaları için doğru ve geçerli veri, organizasyon üzerinden sağlamaktadır. Referans veririnin bulunabileceği üç farklı mekân bulunmaktadır. Bu mekânlarda risk yönetimi ve risk analizi de yapılmaktadır. Referans verinin yönetimi için farklı yaklaşımlar bulunmaktadır. Özellikle iş ortaklarının isterleri göz önüne alınarak dosdoğru yalın bir işlemle referans veri yönetimi iyileştirilmeye çalışılır. Risk yönetim ana çatılarından bazıları bu tarz referans veri yönetimini, finans kuruluşlarına stratejik yaklaşımlarda bulunabilmeleri için önermektedir. Referans veri standartlarına bakıldığında çok çeşitli standartların bulunduğu görülmektedir. Bu standartlar arasında en çok dikkati çeken ve finans piyasalarında sıklıkla kullanılan XML (Extensible Markup Language) dir. Böylece referans veri XML formatı kullanılarak geniş

çaptaki finansal firmalarda kullanılabilmektedir. Bunun haricinde XML'in finansal destek için FIXML şeması da bulunmaktadır.

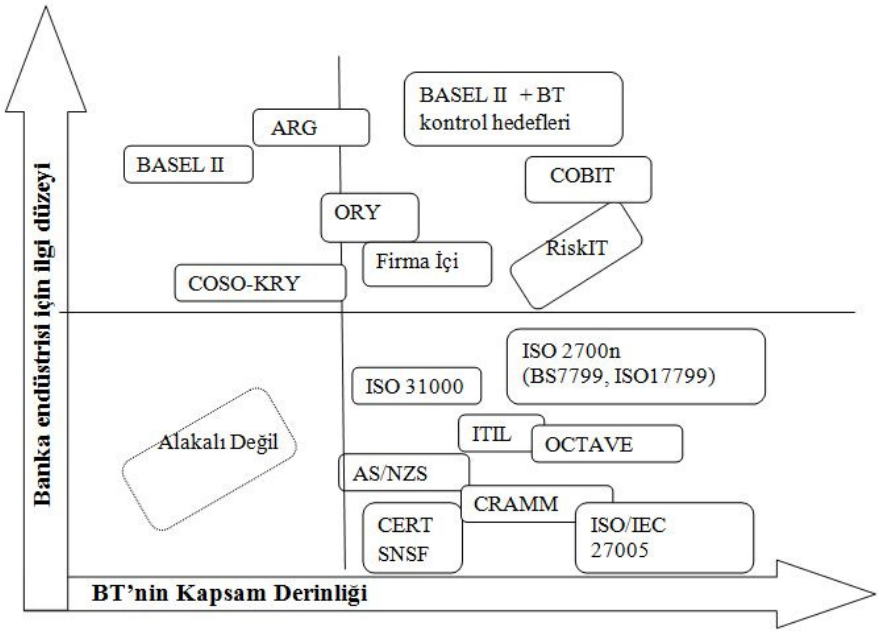
BASEL, 1974 yılında gelişmiş ülkelerin merkez bankalarının bir araya gelmesi ile oluşturmuş oldukları bir kuruluştur. Adını koordinatörlüğünü yapan ve kuruluşuna öncülük eden "Bank For International Settlements"ın İsviçre'nin Basel kentinde bulunmasından dolayı almıştır. BASEL bankaların muhtemel oluşabilecek kriz ve risk durumlarına karşı dayanıklılıklarını artırmak için belli bir standartlaşmaya gidilmesini hedeflemektedir. BASEL komitesi ilk olarak 1988 yılında BASEL I standart'ını yayımlamıştır. BASEL II referans veri yönetimine de çeşitli isterler üzerinden imkân sunmaktadır (Grody v.d., 2006). Önal (2007) çalışmasına göre, BASEL komitesi BASEL II ana çatısını tanımlayarak uluslararası bankacılık sisteminin kararlılığı ve güçlülüğü hakkında anapara yeterlilik düzenlemesinin yeteri tutarlılığı muhafaza edemediği durumlarda uluslararası faaliyet gösteren finans kuruluşları arasında bir düzenleme oluşturmaya çalışmıştır. BASEL II kullanılarak finans kuruluşlarının risklerinin yönetilmesi, ilk adım olarak kredi, piyasa, OR için toplam minimum anapara isterlerinin hesaplanılması önerilmiştir. Temel gösterge yaklaşımı (Basic Indicator Approach, TGY), standartlaştırılmış yaklaşım (Standardized Approach, SY), gelişmiş ölçüm yaklaşımı (Advanced Measurement Approach, GÖY) olarak isimlendirilen üç yaklaşım BASEL II tarafından önerilmiştir. BASEL ana çatısı kullanarak finans kuruluşları OR'in oluşturacağı kayıpları, OR tanımının kapsamında kalıp kalmadığını ve zarar olayının kredi riski gibi nedenlere bağlı olup olmadığını dâhili zarar verisinin finans kuruluşunun şu anki aktiviteleri, teknolojik süreçler ve risk yönetim prosedürleri ile bağlantılı olup olmadığını belirleyebilirler. Çoğunlukla kredi riskleri ile ilgilenen BASEL I standart'ının zaman içerisinde yetersiz kalması ile 1999 yılında BASEL II standartı yayımlanmıştır. BASEL II deki en önemli konular: oluşabilecek riskleri daha iyi ölçmek ve yönetmek, iç ve dış denetimi güçlendirmek, kamuya açıklanacak bilgiler ile şeffaflaşmaya gidilmesiyle piyasa disiplinini sağlamaktır. BASEL II, önceki sürümüne göre daha detaylı bir yapıya sahiptir. Bu nedenle bilgi işlem alanındaki alt yapılaşmaya ve bu alandaki çalışanların eğitimine de önem vermektedir (BDDK, 2014). Son olarak da BASEL III, 2000 yıllarının sonlarında meydana gelen küresel krizin ardından ortaya çıkan yüksek borçlanma, yetersiz likidite gibi konulara yeni bir bakış açısı getirerek bankacılık sektöründeki risk yönetiminin, denetimin ve finansal düzenlemelerin sağlamlaştırılması amacıyla 2010 yılında yayımlanan kapsamlı tedbirlerin bulunduğu bir uzlaşıdır. Önal (2007) çalışmasına göre, OR tanımı BT sistemlerindeki hata, bozulmalar ve herhangi bir sıkıntı yaratacak olaylar tanımı içerisinde bulunmaktadır. Ayrıca, BT

süreçleri ve kontrolleri OR'yi oluşturan savunmasızlık, kayıp ve zararı oluşturan tehditleri başlatan unsurlardır. Gelecekteki OR'lerin belirlenmesine odaklanmanın yanı sıra problem ve hatalara odaklanmak yoluyla şu an da var olan durumların da tespiti mümkün hale gelmektedir. BASEL II'de tanımlı zarar olay tipleri OR kategorileri olarak da adlandırılmaktadır. BT kullanımı ile ilgili OR'lerin çeşitliliğinin artışı organizasyonlarda BT'ye olan bağımlılığın yaygınlaşmasını da beraberinde getirmiştir. BT tabanlı OR'lerin oluşmasında temel nedenler; virüs saldırıları, veriye yetkisiz erişim, alt sorunlar, sistem sorunları, çeşitli çakışmalar ve başarım problemleridir. Böyle risklerin etkin olarak önlenmesi için finans kuruluşlarının BT ile ilişkili potansiyel OR'leri değerlendirmesi, analiz etmesi ve tanımlaması gerekmektedir. Bu nedenle uygun BT yönetişim işlemi yapılmalı, bu yolla kontrol altına alınmış BT ana çatısı iş süreçlerine uygulanmalıdır. Böylece, BT yönetişimi bir organizasyona üç hayati amaca ulaşabilmesini sağlamaktadır: düzenleme ve yasal uyum, operasyonel mükemmeliyet ve risk eniyileme. Yukarıda bahsedilen bu tarz hayati amaçlar uygun endüstri standardı ana çatılarının oluşturulmasına yol açmıştır. Bu tarz ana çatılar bilgi kontrol modelleri kullanmaktadırlar. Bu yolla yetkinlik olgunluk toplulukları, kontrol listeleri, risk yönetim unsurları, çeşitli rehberler, şablonlar ve örnekler bir araya getirilerek bir uyum ve entegrasyon ortaya çıkmaktadır. Bilgi teknoloji yönetişim enstitüsü (Information Technology Governance Institute, BTYE), BASEL II için bilgi riskini ve OR'yi etkin bir biçimde yönetebilmesi için kontrol amaçları ismiyle bir doküman yayınlamıştır. Bu dokümana göre, bilgi risk yöneticileri, BT uygulayıcıları ve finansal hizmet uzmanları, OR ile ilişkili BT kontrol amaçları ve yönetim süreçlerinin bir ana çatı altında etkin bir şekilde kullanabilir hale gelmişlerdir. Diğer yandan, başkaca ana çatılar da BT kapsamını risk yönetimi için tümleştirmeyi denemişlerdir. Literatürde sık karşılaşılan bazı bilgi kontrol modelleri arasında COSO-KRY, ITIL, RiskIT, CRAMM, ISO 27001, CobiT, BS 7799 ve OCTAVE en ön plana çıkanlardır. Şekil 2'de uluslararası finans piyasalarında BT risk yönetimi için önerilen ana çatılar BT kapsam derinliği ve finans sektörü ile olan ilişkilerinin seviyesine göre gruplanmış şekilde gösterilmektedir.

COSO, 1985 yılında ABD'deki muhasebe ve denetim alanında çalışmalar yapan meslek örgütlerinin öncülüğünde kurulmuştur. 1987 yılında kamu ve özel sektörler için iç kontrol tavsiye ve değerlendirmelerinin yer aldığı bir rapor yayınlamışlardır. 1990'larda endüstri, devlet kurum ve kuruluşlarında risk yönetiminin kullanımı nedeniyle, bu yönetimin iyileştirilmesine olan ihtiyaç da oldukça artmıştır. Bu artan ihtiyaçları karşılamak adına 2001 yılında KRY adı altında bir ana çatı ge-

liştirilmiştir. Geliştirilen bu ana çatı, daha güçlü ve yaygın olarak bu ihtiyaçları göz önüne almaktadır.

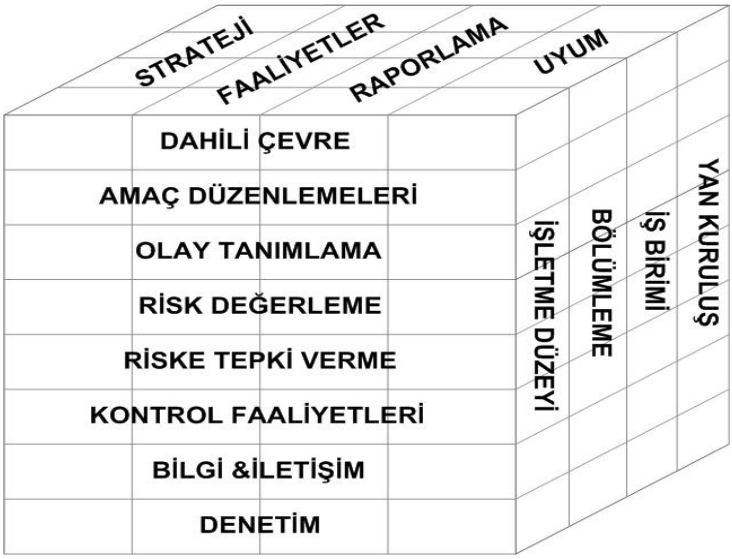
Şekil 2. Bilgi Teknolojileri Risk Yönetim Ana Çatıları



Kaynak: Svatáve Fleischmann (2011, s.46)

COSO-KRY dört amaç tarafından biçimlendirilen sekiz bileşenden oluşmaktadır. Bu amaçlar stratejik, faaliyetsel, raporlama ve uyumdur. Sunulan bu yapı oldukça geniş kapsamlı olup şirketlerin ve diğer organizasyonların risklerinin yönetimi için temel özellikleri içermektedir. Diğer sektörlere, endüstri kollarına da kolaylıkla uygulanabilir (McConnel, 2005). Şekil 3'te COSO-KRY'nin boyutları ve bileşenleri görülmektedir. Dâhili çevre risk yönetim felsefesini ve risk iştahını (risk appétit), bütünlüğü, etik değerleri ve çevreyi içermektedir. Amaç düzenlemeler, risk iştahı ile tutarlı olan işletmenin misyonu ile ilgili, seçilmiş amaçların desteklenmesi için amaçların ayarlamasını yapan bir sürecin bulunduğu bir yönetim şeklidir. Olay tanımlama, kurum amaçlarına ulaşmayı etkileyen dâhili ve harici olayları tanımlar. Risk değerlendirmesi, riskleri belirleyerek bir temel oluşturmakta, bu risklerin olabilirliğini ve etkilerini dikkate alarak risk analizi gerçekleştirmektedir.

Şekil 3: COSO Kurumsal Risk Yönetimi



Kaynak: McConnel (2005, s.6)

Riske tepki verme, bileşeni belirlenmiş risklere karşı önceden belirlenen tepkileri bünyesinde barındırır. Bu bileşen aynı zamanda risk toleransını ve risk iştahını dikkate alır. Kontrol faaliyetleri kuralları, prosedürlerin oluşturulması ve uygulanmasını içermektedir. Bilgi ve iletişim bileşeni, bilgiyi elde eder, tanımlar ve aktarılmasını sağlar. İzleme bileşeni, risk yönetim süreci hakkında bir takip gerçekleştirir ve gerekli olduğunda süreci düzenler. COSO, iş pratikleri, süreç yönetimi ve iş sorunları üzerine yoğunlaşmıştır. COSO, kontrol için yönetim sorumluluklarının ve etkin risk yönetim sürecinin oluşturulması için anahtar prensiplerin vurgulanmasına katkı sağlamaktadır. Bu sayede firmalar ve diğer kuruluşların kendi dâhili kontrol sistemlerinin iyileştirilmesi ve değerlendirilmesi için yardımcı olmaktadır. Böylelikle dâhili kontrol ortamı hakkında farkındalık yaratır. Olgunluk modeli oluşturmak adına ORY olgunluk modeli (ORM Maturity Model) COSO'nun üzerine entegre edilmiştir. Bu yolla organizasyonlar için oldukça iyi bir biçimde belgelendirilmiş inandırıcı ve kavramsal olarak doğru olan ORY sistemlerinin uyumluluk kalitesinin nesnel olarak ölçülmesini sağlayan bir mekanizma önerilmiştir. Olgunluk modeli BT endüstrisinde kullanılmakta ve en iyi uygulamalar karşısında ORY sisteminin gerçekleştirimindeki olgunluk seviyesini değerlendirmektedir. Bu mekanizma temelde yazılım mühendisliği değerlendirme ve ölçüm kriterlerinin göz önüne alınmasıyla COSO-KRY üzerine entegre edilmiştir.

Özer'in çalışmasında (2012) risk yönetiminin detaylarından bahsedilerek rekabet ortamında girişimciler için bir rehber oluşturulmaya çalışılmıştır. Bu kapsamda risk yönetim unsurlarına değinilerek özellikle yönetim kısmında insan, makine, çevre, ilgili görevler, prosedürler ve kontrollerden bahsetmiştir. Özellikle risk yönetim seviyelerindeki stratejik risk yönetiminde öncelikli ve muhtemel risklerle uğraşmak için belirli bir standart ve ORY yazılımsal aracına ihtiyaç duyulmaktadır. Bu bakış açısıyla sistem ve faaliyet ile ilgili tehlikelerin farkındalığı veya ilgili durumun sınanması için analiz araçlarının kullanımı, ayrıca risk değerlendirmesinde girişimcilere yardımcı olmak adına Özer'in de belirttiği hususlarda COSO-KRY'nin de kullanılabileceği ortaya çıkmaktadır. COSO-KRY'nin amaçları kapsamında bu öneri, faaliyetler ve raporlama açısından bir derinlemesine risk yönetimini gerçekleştirmek için yakın gelecekte tahmin edilen faaliyet planlarını, standart faaliyetlerin incelenmesini, buna ilişkin bakım ve eğitim yollarının, ilgili doğal afet ve zarar kontrolünün planlamalarını da içerebilmektedir. COSO-KRY, finansal piyasalarda çeşitli yazılımsal çözümlerde kullanılmaktadır (Blackline, 2014).

Bilgi Teknolojisi Altyapı Kütüphanesi (Information Technology Infrastructure Library, ITIL), iş sorunları üzerine yoğunlaşmakta, böylece kaza, problem, hazır bulunabilirlik ve değişim yönetimi ile ilgili özel alanlar hakkında içeriğe sahiptir. ITIL, iş sorunlarının sürüm yönetimi, değişim yönetimi, problem yönetimi, kaza yönetimi, elde edilebilirlik yönetimi, kapasite yönetimi, alt yapı yönetimi için kapsamlı kontrol amaçlarına sahip olacak şekilde iş sorunları ile ilgili OR'leri kapsamaktadır. Böylece donanım, yazılım, telekomünikasyon ve araçların devre dışı kalmasını önleyebilir. Bunun yanı sıra herhangi bir güvenlikle ilgili kontrol amacını da içermemektedir. En büyük katkısı, BT yönetişimi ile ilgili OR'lerin değerlendirilmesinde kullanımı, bu sayede iş sorunlarını göz önüne alan bir organizasyonun risk iştahını kapsayabilmektedir (Önal, 2007). Çoğu finansal kuruluşu KRY yaklaşımı için bazı ana çatıları kullanarak BT risk yönetimine ayrı bir süreç olarak yaklaşmakta ve raporlamaktadır. RiskIT ana çatısı içerdiği süreç modeli ile BT risk yönetimini BT ile ilişkili sorumlulukları tanımlandığı rollerle beraber model üzerinde KRY sistemlerine entegre etmektedir. Bu sayede risk yönetişim alanı olarak tanımlanan ek süreç adımları ile tümleşik bir risk yönetim ana çatısı ortaya çıkmaktadır. Bu açıdan RiskIT aktivite seviyeleri, süreç ve alan üzerinden çeşitli ölçütler ve amaçlar içerecek şekilde bir yapı oluşturmaktadır (Svatá ve Fleischmann, 2011). Risk Analiz ve Yönetim Metodu (CCTA Risk Analysis and Management Method, CRAMM), Merkezi İletişim ve Telekomünikasyon Ajansı (Central Communication and

Telecommunication Agency, CCTA) tarafından önerilmiştir. CRAMM İngiliz hükümeti tarafından risk analiz metodu olarak biçimlendirilmiştir. Bu metodu destekleyen aynı isimli bir araç bulunmaktadır. Bu aracı kullanmadan yöntemi kullanmak oldukça güçtür. CRAMM metodu ve ilgili araç, İngiliz hükümeti organizasyonlarının en iyi uygulamaları temel alınarak oluşturulmuştur. Böylelikle İngiltere'nin dışında birçok ülkede de bu metot ve araç kullanılmaktadır. Özellikle devlet kurumları ve endüstri kuruluşları gibi büyük organizasyonlara uygundur (Svatá ve Fleischmann, 2011).

İlgili Teknoloji ve Bilgi için Kontrol Amaçları (Control Objectives for Information and Related Technology, CobiT), BT hizmetlerinin teslimatı ve desteklenmesi için tasarlanmış kontrol amaçlarına sahip ve BT yönetişim ana çatısı şeklinde tanımlanmıştır. Bu ana çatı, iş yeri uygulamaları süreç yönetimi gibi olgulara odaklanmıştır. CobiT kendi alanında BT yapısının değerlendirilmesi ve izlenmesi, BT hizmetlerinin desteklenmesi ve teslimatı, BT sistemlerinin ve teknolojilerinin gerçekleştirilmesi ve elde edilmesi, BT aktivitelerinin organizasyonu ve planlanması için kapsamlı kontrol amaçları içermektedir. Bu kontrol amaçları süreç yönetimi iş pratikleri ile ilgili OR'leri kapsar. Bu sayede BT süreçlerinin genel biçimde yürütülmesi, süreç yönetiminin devam eden iyileştirilmesi, iş ve çalışan uygulamaları ve BT'nin teslimat değeri elde edilebilir. CobiT bunların haricinde güvenlik ile ilgili kontrol amaçlarına ait detay içermemektedir. Dâhili ve harici dolandırıcılıkla ilgili OR'leri de içermemektedir. CobiT için fiziksel güvenlik bakış açısıyla genel kontrol amaçları detaylandırılmamıştır. BT yönetişimin bir parçası olarak iş sorunları ile ilgili OR'lerin CobiT tarafından değerlendirilmiş olması bu ana çatının bir katkısıdır (Önal, 2007).

BS 7799 ve ISO 27001 standartları aynı kapsamda bulunan güvenlik standartlarıdır ve ISO 27001, BS 7799 kullanılarak üretilmiştir. Buradaki BS terimi İngiliz standardı anlamına gelmektedir. Bunun uluslararası versiyonu da ISO standardı ile gösterilmektedir. Dâhili ve harici dolandırıcılık ve fiziksel varlıklara zarar verme gibi nüfuz etme seviyeleri bu standartlarla OR ile ilişkili olarak göz önüne alınmaktadır. Böylece kullanıcı hesabının yönetimi, fiziksel güvenlik, ağ güvenliği ve sistem geliştirme bakımı açısından ele alınmaktadır. Güvenlik için mantıksal açıdan kapsamlı kontrol amaçlarını ortaya koyan ana çatılar oluşturulmuştur. Bu sayede yetkisiz aktiviteler ve yetkisiz erişimlerden dâhili ve harici kaynaklar korunabilmektedir. Organizasyonlar açısından iş yeri güvenliği ile ilgili OR'lerin değerlendirilmesine bu ana çatılar büyük katkı sağlamaktadır (Önal, 2007).

Operasyonel Kritik Tehdit, Varlık, Zafiyet Değerlendirmesi (Operational Critical Threat, Asset and Vulnerabilitiy Evaluation, OCTAVE), risk tabanlı bilgi güvenliği stratejisi, değerlendirmesi ve planlanması için araçlar, teknikler, yöntemlerin bir takımdır. OCTAVE'ın üç temel metodu bulunmaktadır. Orijinal OCTAVE metodu temel bilgi gövdesini oluşturmaktadır. OCTAVE-S, küçük organizasyonlar için ve OCTAVE-Allegro ise bilgi güvenliği değerlendirme ve sigorta için bir akış hattı yaklaşımıdır. OCTAVE metotları risk-ilesürülen ve uygulama tabanlı bilgi güvenliği değerlendirmesi için standart bir yaklaşım önermektedir. Bu metotlar teknoloji kullanımı ile ilgili risk yönetimine dair temel ilkeleri de sağlamaktadır (Svatá ve Fleischmann, 2011). Solvency II, Avrupa Birliği tarafından önerilen anapara yeterlilik isterlerini inceleyen bir yapıdır. Yeni bir düzenleyici ana çatı olarak Avrupadaki sigortacılık endüstrisine Avrupa Birliği'nce önerilmiştir. 2012 yılı itibariyle kullanıma giren Solvency II, sigortacılık sektöründeki firmalar için risk yönetim pratikleri ve anapara seviyelerine ilişkin standartları düzenlemektedir. Bu sayede, BASEL I ana çatısına benzer olarak risk tipleri ve risk hassasiyetleri ile ilgili olarak büyüyen sigorta firmaları için yeni risk tiplerinin varlığının veya tanımlamasının yapılabilmesi için önerilmiştir (Stokkers, 2013). Solvency II; Avrupalı sigorta firmalarının BASEL II'ye benzer olarak karşılaşılan sorunlar için düzenleme yapan bir ana çatı olarak OR'lerin kullanılması yoluyla anapara isterlerinin ödeme gücünü belirleyebilmektedir (Bauer, 2012). Amerikan hükümeti tarafından, 2000'li yılların başlarında operasyonel kayıpların finansal piyasalardaki etkilerinin düzenlenebilmesi adına, Amerikan borsasında listelenen tüm firmalar için zorunlu tutulan, Sarbenes Oxley Act (SOX) ismi verilen bir standart önerilmiştir. SOX, finansal piyasalarda denetleme uzmanlarının katkısıyla finansal raporlamanın halkın güvenliği gözetilerek yapılmasını şart koşmaktadır. SOX'un benzeri olarak Avrupa Parlamentosu EUROSOX standardını önermiştir (Bauer, 2012).

Çalışmamızda yapılan literatür araştırmasında günümüzde de var olan ve sıklıkla kullanılan çeşitli ORY metodolojileri incelenmiş ve bunlar arasından ön plana çıkanlar alt yapı, amaç ve finans piyasalarında uygulanabilirlik açısından değerlendirilmiştir. Bu değerlendirmeler ve uygulamalar hakkında karşılaştırma tabanlı bir tartışmaya çalışmamızın üçüncü bölümünde yer verilmektedir.

2. OPERASYONEL RİSK YÖNETİM YAZILIM VE ORTAMLARI

Risk yönetimine ait yukarıda bahsedilen çeşitli standartlar mevcuttur. Bu standartların finansal kurumların iş süreçlerinde karşılaşılan OR'lerin etkin bir biçimde yönetilebilmesi adına geliştirilmiş olan çeşitli yazılımsal araçları da bulunmaktadır. Araştırmamız kapsamında; ISO 27001 (ISO 17799, BS 7799), CobiT, CRAMM, OCTAVE standartlarından herhangi birini veya daha fazlasını kullanan ve literatürde yer alan çeşitli yazılımlar incelenmiştir. Bu yazılımlar arasında; Otomatikleştirilmiş Risk Yönetim Sistemi (Automated Risk Management System, ARMS), Kıyaslama Değerlendirme Aracı (BEnchmark Assessment TOol, BEATO), CobiT araçları, CRAMM araçları, Güvenlik hedeflerinin belirlenmesi ve ihtiyaçların tanımlanması (Expression of Needs and Identification of Security Objectives, EBIOS). Bilgi Güvenliği Yönetim Sistemleri (Information Security Management Systems, ISMS), ISO/IEC 17799:2005. Modulo Risk yöneticisi (Modulo Risk Manager), OCTAVE, Risk Watch, Açık kaynak kodu isterlerinin yönetim aracı (Open Source Requirements Management Tool, OSRMT) bulunmaktadır (Abie ve Borking, 2012), (McDonald v.d., 2013), (Şahinarslan v.d., 2010). Bunlara yakından bakacak olursak, ARMS; ISO 1779, ISO 27001 uluslararası standartları bünyesinde barındıran yönetişime şekil vermenin hızlı ve kolay bir yolu olarak önerilmiştir. BEATO, güvenlik değerlendirmesine dayalı hem bir araç hem de bir yöntemdir. Kontrollerin niteliğini ve yetenek olgunluk modelini kullanan uyumlulukların derecesini de belirler. ISO standartlarına bağlı olarak BEATO aynı zamanda uyumluluk değerlendirmesi olarak da kullanılabilir. CobiT, genellikle kabul edilmiş ölçekleri, göstergeleri, süreçleri ve en iyi uygulamaları sağlayan temel bilgi güvenliği yönetişim modelidir. CobiT, organizasyonlar BT faaliyetleri için bir uygulama ve açık kural geliştirilmesini sağlar. Bu araçlar uyum düzenlemelerini vurgulamaktadır (Abie ve Borking, 2012). EBIOS, risk değerlendirmesi için önerilmiş olan kapsamlı bir tekniktir. Fransız hükümeti tarafından geliştirilmiştir. EBIOS, Fransa'da hem özel sektörde hem de kamuda kullanılmaktadır. Büyük çapta BT güvenlik standartlarını içermekte ve beş aşamadan oluşmaktadır. Bu sayede BS'lerdeki genel iş süreçlerinin ve tehdit analizinin en iyi şekilde yapılabilmesini sağlar. EBIOS, klasik BS risk değerlendirme için önerilmesinden dolayı çeşitli özel durumlara da uyarlanması gerekmektedir (McDonald v.d., 2013). CRAMM, İngiliz hükümeti tarafından geliştirilen bir risk analiz yöntemidir. Risk analizi metodu aşamaları; risk tanımlanması, analizi ve değerlendirmesini kapsar. Bu aşamalar CRAMM araçları ile gerçekleştirilirler. CRAMM araçlarına sıradan ve uzman kullanıcılar

ilgili web sitelerinden ulaşılabilir (CRAMM Toolkit Expert, 2014), (CRAMM Toolkit Express, 2014).

ISMS, ISO standartlarına uygun olarak çeşitli bilgi güvenlik yönetim kurallarını içermektedir. Kendi mekanizması bilgi güvenlik risklerini minimize edecek şekilde bilgi hazır bulunabilirliği ve tümleştirme gizliliğinin sağlanması için sistemlere ve süreçlere kullanabilecekleri çeşitli ölçüt ve inceleme, gerçekleştirim, tasarım imkânları sunar. Risk değerlendirme fazı sayesinde çeşitli tehditleri tanımlamak mümkün olmaktadır. Bu yolla ISMS'nin ilgili aracı sayesinde risk tanımlama desteği sağlanmaktadır (ISMS Tools, 2014). ISO/IEC 17799:2005 modeli, ISO bilgi teknolojileri ve güvenlik tekniklerini içermektedir. İsterleri, İngiliz Standartlar Enstitüsü tarafından belirlenen BS 7799-2 oluşumuna dayanmaktadır. ISMS, bilgi güvenliği yönetimi ile ilişkili kurallar bütününü kapsar. Tasarım, gerçekleştirim, değerlendirme, ölçüm ve bakım işlemlerini içermektedir. Risk yönetim metodu aşamaları üç aşamada oluşmaktadır. Bunlar; risk değerlendirmesi, risk sorununu çözme, risk kabulüdür. Bu standartta birçok araç bulunmaktadır. ISO 27001/ISO 27002 araçları, ISMS araçları, BT yönetişimi için CobiT, ITIL ve ISO 27001 tabanlı araçlar bu kapsamda örnek olarak verilebilir (Abie ve Borking, 2012). Modulo Risk Yöneticisi; yönetişim, risk yönetimi ve uyumluluk için etkili çözüm setlerini bünyesinde barındırır. Modulo BT ve kurumsal risk yönetim modülü; envanter, analiz, değerlendirme ve tehdit risklerini CobiT, ISO 31000 gibi temel çatıları kullanarak otomatikleştirmektedir. Bu yapının fonksiyonellikleri arasında kural yönetimi, BT ve kurumsal yönetim, uyum yönetimi, olay ve akış yönetimi yer almaktadır (Abie ve Borking, 2012), (Modula, 2014). OCTAVE, stratejik değerlendirme ve planlama, risk tabanlı bilgi güvenliği için metotlar ve teknikler ve araçların dâhil olduğu bir takımdır. Bu takım kullanılarak OCTAVE-S ve OCTAVE-Allegro ismi verilen iki farklı yaklaşım sayesinde bilgi güvenlik riski için bağlam-ile-sürülen (context-driven) sistematik ve kapsamlı bir değerlendirmeye tabi tutulabilmektedir (Abie ve Borking, 2012).

Tablo 1. Standartlar ve ORY Yazılımsal Araçları.

	CRAMM	COSO - KRY	CobiT	ISO 17799 (ISO 27001, BS 7799)	OCTAVE
ARMS				+	
BEATO				+	
Blackline COSO Jumpstart Solution Financial Close Suite		+			
CobiT Tools			+		
CRAMM Tools	+				
EBIOS Tools				+	
ISMS Tools				+	
ISO/IEC 17799-2005				+	
MODULO Risk Manager			+		
OCTAVE Toolkit					+
OSRMT				+	
Risk Watch				+	

Risk Watch, bilgi güvenliği risklerini analiz etmek için oluşturulan ve BS'lerdeki açıkların ve risklerin analiz edilerek değerlendirmesinde kullanılan bir yazılımdır. Kontrol için ISO 17799 standartına uygun temeller içermektedir (Şahinarslan v.d., 2010), (Elky, 2007), (Risk Watch, 2014).

OSRMT, kurumlardaki güvenliğin risk analizi için geliştirilmiş açık kaynak kodlu bir yazılımdır. ISO 17799 standart'ını temel alarak model tabanlı risk değerlendirme metodolojisini uygulamaktadır. Analiz sonuçlarının tekrar kullanımı ve yönetimin kolaylaştırılması gibi imkânlar sunmaktadır. Böylece bir yönetim aracı olarak test, gerçekleşti-

rim ve tasarım için gerekli özellikleri bir arada sunabilmektedir (Abie ve Borking, 2012), (OSMRT, 2014). Tablo 1'de BT kaynaklı OR'lerin yönetilmesine dair literatürde sık kullanılan çeşitli yazılımsal araçlar görülmektedir.

Literatür incelemesi sonucunda en sık kullanılan standartlar olarak ISO 17799 ve CobiT standartlarının olduğu Tablo 1'de görülmektedir. Riskin seviyesini, sistematik ve güçlü bir yoldan sunmak adına çeşitli çalışmalarda ilgili yazılımsal araçlar kullanılmaktadır. Tablo1'de standartlar ve ORY yazılımsal araçları arasındaki ilişki de görülmektedir. Bunun yanı sıra OCTAVE kendi metodolojisini kullandığı için tüm bunlardan farklı bir yerde durmaktadır.

SONUÇ VE TARTIŞMA

BS/BT risk oluşumuna yatkın bir yapı sergilemektedir. Bu nedenle ORY için dikkate alınacak detaylı araştırmaların öncelikli dayanak noktasını, finansal kurum ve kuruluşların bilgi işlem yapılanmalarında, karmaşık ve büyük iş süreçleri dâhilinde BT'ye ne kadar önem verdikleri oluşturmaktadır. Buna göre; risk tahminleri parametrik olarak, risk analizi ile ortaya çıkan sorunlara karşı alınacak önlemlere karar vermeyi kolaylaştırmaktadır. OR'lerin oluşturacağı zararları en aza indirgemek için risk yönetimini çeşitli açılardan değerlendirmek gerekmektedir. Bu sayede girişimcilik alanındaki faaliyet gösteren yöneticilerin içgüdü ve deneyimlerinin çeşitli risk gruplarının daha somut yönetilebilmesinde kullanılabilmesi gündeme gelmektedir. Mikro ve makro riskler bireyden topluma ve toplumdan ülke geneline kadar geniş bir kitleyi etkilediği gibi bu kitle içerisindeki girişimcileri de doğrudan veya dolaylı olarak etkileyebilmektedir. Finansal piyasaların etkilenmesine neden olacak şekilde bilgi teknolojilerinden kaynaklanan OR'nin yönetilebilmesi bu açıdan önem kazanmaktadır.

BT sağladığı avantajların yanı sıra oldukça fazla sorunu da beraberinde getirmektedir. Bu sorunlar arasında güvenlik riski; yetkisiz erişim sonucunda veri güvenliğinin yitirilmesi, e-postalara üçüncü şahıslar tarafından erişilmesi ve okunması olarak nitelendirilebilir. Sosyal patlama, şiddet olayları, terörizm ve çıkar amaçlı çete hareketleri gibi unsurlar Özer'in çalışmasında (2012) sosyal riskler kapsamında incelenmiştir. Ayrıca deprem, sel gibi doğal afetler de doğal riskler olarak gruplandırılmıştır. Sosyal risklerin yönetiminde ana amaç krizlere önlem almaktır. Bu açıdan, bu tarz sosyal ve doğal risklerle uğraşabilmek adına girişimcinin risk yönetimini etkili olarak başarıyla uygulayabilmesi gerekmektedir. Sosyal girişimciler, sosyal yenilikçiliğe (innovasyon) bağlı risklerin etkilerini azaltmaya dayanan ve önceden

riskleri sigortalamayı önerecek yapıları düzenli bir biçimde kullanabilmelidirler.

Dâhili ve harici olaylar için OR, çeşitli düzenleme (regülasyon) ana çatılarına göre farklılaşabilir. Bu ana çatılar ile uyumluluğun yönetişim açısından değerlendirilmesinde; kuralların, süreçlerin ve prosedürlerin ORY için geliştirilmesi, iş sürekliliği planlarının oluşturulması, farkındalık ve sürdürülebilirliğin tesis edilmesi önemli yer tutmaktadır. Bu ana çatılar sıklıkla OR'leri tanımlama, değerlendirme, izleme ve kontrol etme yoluyla azaltmayı sağlamaktadır. Çalışmamızda toplam yedi adet bilimsel yayın ve bunun yanı sıra çeşitli firma dokümanı ve web siteleri incelenmiştir. Endüstrinin yönelimini belirlemek adına Amerika ve Avrupa standartları göz önüne alınarak ilgili alanda düzenlemenin hangi temellerde yapılabildiği ve hangi ana çatıların kullanıldığı yapılan inceleme ile ortaya konulmuştur.

Tablo 2'de literatürdeki çeşitli çalışmalarda temel alınan ORY metodolojilerinin dayandığı uluslararası kabul görmüş düzenleme standartları ile çalışma kapsamında incelenen yayınlar arasındaki ilişki görülmektedir.

Tablo 2'deki çalışmalarda BASEL I ve BASEL II en çok kullanılan standartlar olmuştur. Bunun ardından COSO ve SOX standartları çalışmalarda sıklıkla kullanılan standartlar olarak Tablo 2'de görülmektedir. BASEL standart'ının daha sık kullanılmasındaki temel nedeni BASEL'deki risk çeşitlerinin kredi riski, likidite riski ve OR olarak üçe ayrılmış olması, bu sayede BT tabanlı riskleri OR başlığı altında toplayabilmesidir. Bu açıdan finansal kurumlara BT tabanlı risk yönetimi yoluyla riskleri minimize edebilmek adına çeşitli yol ve yöntemler sunmaktadır. Özer'in (2012) belirttiği hususlar göz önüne alındığında ise çalışmamız doğrultusunda COSO-KRY'nin kullanımının finansal bakış açısıyla girişimciler için önerilebileceği ortaya çıkmaktadır.

Tablo 2. Yayınlarda Temel Alınan Standartlar

	Svata (2001)	McConnel (2005)	Grody (2006)	Elky (2007)	Önal (2007)	Savic (2008)	Bauver (2012)	Stokkers (2013)
AS/NZS 4360	+							
BASEL I/II	+		+		+	+	+	+
BS 7799					+			
CRAMM	+							
COSO	+	+						
CobiT					+			
ISO 27001					+			
ISO 31000	+							
ITIL					+			
RiskIT	+							
Risk Watch				+				
SOX						+	+	
OCTAVE	+							

Çalışmamız sonucunda, BT tabanlı risk yönetimi hakkında; standartlar, risk olayları, ana çatılar, yönetişim kuralları ve süreçler konusunda bir değerlendirme yapılmıştır. ORY için olgunluk modeli oluşturma yaklaşımını deneyen COSO-KRY ve CobiT gibi ana çatılarda uyum kalitesi için bir mekanizmanın varlığı gündeme getirilmekte, böylece sistemin gerçekleştirimi için önceki benzer durumlarda elde edilen bir karşılaştırma ORY yapılmasında kullanılabilmektedir. Olgunluk modelleri, etkin ölçüm ve karar vermeyi de kolaylaştırmaktadır. COSO, CobiT, BS 7799, ISO 27001 ve ITIL gibi standartlar; finansal işlemlerin belirli bir harmoni içerisinde BT sistem ve temel teknolojileri ile çalışabilmesine yardımcı olmaktadır. Günümüzde siber suçların (cybercrime) gösterdiği artış ve BT sistemlerinin artan karmaşıklığı yukarıda bahsedilen harmoniyi bozmakta ve finans kurumlarındaki çeşitli operasyonel ve organizasyonel faaliyetlerdeki riskin seviyesini değiştirmektedir. ORY oldukça yeni ve karmaşık bir araştırma alanı olarak, var olan sınırlandırmaları ve çatışma durumlarını da beraberinde getirmektedir.

Birçok OR modeli, dâhili zarar verisinin hazır bulunabilirliğini temel almaktadır. Bu modeller arasında; uç değer teorisi, zarar dağılım yaklaşımı veya Bayesçi çıkarsama yaklaşımının genişletilmiş hali bulunmaktadır. Operasyonel BT riskleri özel amaçlı bir tabanda tanımlanabilmekte, bu sayede özel bir OR kategorisine uygun olmasına gerek kalmadan zarar verisi toplanabilmektedir. BT tabanlı OR değerlendirme süreci, dâhili veya harici zarar verisinin yokluğunda tekrarlanan bir iş haline gelmektedir. BT tabanlı OR için karar frekansı ve zarar şiddet dağılımına bakıldığında, yıllık zarar dağılımının yapılandırılabildiği görülmektedir. Belirli bir BT tabanlı OR'in finansal etkisinin ölçüsü olarak yıllık zarar dağılımından elde edilen düzenleyici anaparaya ait biçimin risk değeri (Value at Risk, VaR) oldukça yüksektir. Belirsizlik, OR modellemesinde önemli bir yer tutmaktadır. BT tabanlı OR'in değerlendirilmesinde hangi model veya model kombinasyonlarının kullanılacağına veri hazır bulunabilirliği yön vermektedir. Yazılım açısından OR'ler, sıklıkla zararlı yazılımlar (malware) ve siber suçlar nedeniyle oluşmakta ve OR değerlendirmesine etki etmektedir. Taneselliğin ve VaR ölçülerinin, OR değerlendirmesinde büyük etkisi bulunmaktadır (Stokkers, 2013). OR'lerin bankacılık endüstrisine sigortacılık endüstrisinden daha çok etkisi bulunmaktadır. Bunun temel nedeni, bankaların daha dinamik bir ödeme sistemine sahip olmaları ve piyasa değer azalışlarından daha az etkilenmeleridir (Bauer, 2012).

KAYNAKÇA

Abie, H. & Borking, J. (2012). Risk Analysis Methods and Practices: Privacy Risk Analysis Methodology, Norsk Regnesentral, DART/05/2012, Note, 37 sayfa.

Amland, S. (1999). Risk Based Testing And Metrics: Risk Analysis Fundamentals and Metrics for software testing including a Financial Application case study, 5th International Conference EuroSTAR '99, 8 - 12 Kasım, (ss. 1-20). Barselona, İspanya.

ARMS Working Group, (2010). The ARMS Methodology for Operational Risk Assessment in Aviation Organisations, v4.1, Skybrary refernce for aviation safety knowledge, Mart 2010, Çevrimiçi: "http://www.skybrary.aero/ bookshelf/books/1141.pdf"

Bankacılık Düzenleme ve Denetleme Kurumu - Web sitesi, (2014), Çevrimiçi: " www.bddk.org.tr".

Bauer, S. (2012). A Literature Review on Operational IT Risk and Regulations of Institutions in the Financial Service Sector, In proc. of 2012 International Conference on Information Resource Management (Conf-IRM 2012), (ss. 1-14), 21-23 Mayıs 2012, Viyana, Avusturya.

Blackline (2014), COSO Jumpstart Solution, Blackline Financial Close Suite, Task Management Module. Çevrimiçi: "www.blackline.com/products/financial-close-suite".

Chutia, R. (2013). Operational Risk Management in Banking Sector: An Overview, *Indian Journal of Applied Research*, 3(1), 6-8.

CRAMM Toolkit Expert- Web sitesi, (2014), Çevrimiçi: "www.cramm.com/overview/expert.htm"

CRAMM Toolkit Express - Web sitesi, (2014), Çevrimiçi: "www.cramm.com/overview/express. htm"

Doerig, H. & Chairman, V. (2003). *Operational Risks In Financial Services: An Old Challenge in a New Environment*, Partly adjusted, Credit Suisse Group, Teknik Rapor, 136 sayfa.

Elky, S., (2007). *An Introduction to Information System Risk Management, Sans Institute Infosec Reading Room Whitepaper, Sans Institute.* Çevrimiçi:" http://www.sans.org/reading-room/whitepapers/auditing/introduction-information-system-risk-management".

Grody, A. D., Harmantzis, F. C. & Kaple, G. J. (2006),Operational Risk And Reference Data: Exploring Costs, Capital Requirements And Risk Mitigation, *Journal of Operational Risk*, 1(3), 1-57. Çevrimiçi: "http://ssrn.com/abstract=849224".

ISMS Tools – Free Demo – ISO27001/ISO 27001 Information Security site - Web sitesi, (2014), Çevrimiçi: "www.27001.com/ISMSFreeDemo.aspx"

McConnel, P. (2005). Measuring Operational Risk Management Systems Under Basel II, Continuity Central, Sydney: Risk Trading Technology, Çevrimiçi: "http://www.continuitycentral.com/feature0197.htm".

McDonald, J., Oulha, N., Puccetti, A., Hecker, A. & Planchon, F. (2013). Application of EBIOS for the risk assessment of ICT use in electrical distribution sub-stations, In Proc. of 2013 IEEE GrenoblePowerTech Conf. (POWERTECH), (ss.1-6), 16-20 Haziran 2013. DOI: 10.1109/PTC.2013.6652221

Modulo – Web sitesi. (2014). Çevrimiçi: "www.modulo.com".

OSMRT (Open Source Requirement Management Tool) – Web sitesi. (2014). Çevrimiçi: "http://sourceforge.net/projects/osmrt".

Önal, M. Z. (2007). An Aggregated Information Technology Checklist For Operational Risk Management, *BDDK Bankacılık ve Finansal Piyasalar*, 1(2), 49-75. ISSN: 1307-5705. Çevrimiçi: "www.bddk.org.t/bddkdergisi/".

Özer, M. A. (2012). Rekabet Ortamında Girişimciler İçin Varolabilme Reçetesi: Risk Yönetimi. *Girişimcilik ve Kalkınma Dergisi*, 7(1), 143-162.

Risk Watch – Web sitesi. (2014). Çevrimiçi: "http://rm-inv.enisa.europa.eu/tools/t_riskwatch.html".

Savić, A. (2008). Managing It-Related Operational Risks, *Economic Annals, Communications*, 53(176), 88-109.

Scarlat, E. (2012). Indicators And Metrics Used In The Enterprise Risk Management (ERM), *Journal of Economic Computation And Economic Cybernetics Studies And Research,* 46(4), 5-19.

Stokkers, M. (2013). Quantifying Operational IT Risk: Improving Achmea IM&IT's Risk Management, Yüksek Lisans tezi, University of Twente, Hollanda, 54 sayfa.

Svatá, V. & Fleischmann, M.(2011). Is/It Risk Management In Banking Industry, *Acta Oeconomica Pragensia*, 19(3), 42-60.

Şahinaslan, E., Kandemir, R. & Kantürk, A. (2010). Bilgi Güvenliği Risk Yönetim Metodolojileri ve Uygulamaları Üzerine İnceleme, III. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu, (ss.1-5), 05-06 Şubat 2010, Ankara.