

## RİSK YÖNETİMİ VE ÜLKE UYGULAMALARINDA RİSK YÖNETİM MODELLERİ\*

### RISK MANAGEMENT AND RISK MANAGEMENT MODELS IN COUNTRY APPLICATIONS

Arş. Gör. Ruveyda KIZILBOĞA  
Nevşehir Üniversitesi

#### Özet

*Risk yönetimi, kurumların hedeflerine ulaşmasını engelleyici risklerin ve hedeflere ulaşımı kolaylaştırıcı fırsatların önceden fark edilerek yönetilmesini sağlayan dinamik ve disiplinli bir sistemdir. Özel sektör uygulamaları ile başlayan sistem kamu kurumları tarafından da benimsenmiştir. Risk yönetiminin temel amacı, özel sektörde kârı artırıcı uygulamaları desteklemek kamu kurumlarında ise fayda unsurunu geliştirmeye yardımcı olmaktır. Genelde amaç aynı, fakat sistemin kapsamı ülkeden ülkeye değişmektedir. Bu çalışmada farklı risk yönetim sistemlerine örnek olması amacıyla Avusturya/Yeni Zelanda, İngiltere, Kanada ve Amerika risk yönetim modelleri üzerinde durulmaktadır.*

**Anahtar Kelimeler:** Risk, Risk Yönetimi, Risk Yönetim Modelleri.

#### Abstract

*Risk management is a systematic and dynamic system that helps to be aware of before risk occurs and manage those risks which could prevent organization to realize its objectives and opportunities which are facilitate access to objectives. Implementation of the system has started in private sector and then adopted to the public sector. The aim of the system is to help to increase profit in private sector and develop benefits in the public sector. Generally, the goal is same but scope of the system differs from country to country. In this study, the focus was on Austria/New Zeland, The United Kingdom, Canada and America risk management systems in order to be an example for the different risk management systems.*

**Keywords:** Risk, Risk Management, Risk Management Models.

\* Bu makale “Kurumsal Risk Yönetimi Odaklı İç Denetim Sistemi ve İstanbul Büyükşehir Belediyesi için Bir Model Önerisi” isimli tezden üretilmiştir.

## 1. Giriř

Dünya her geen gün biraz daha risk üstlenerek büyümektedir. Afet, savař ve finansal çöküşler karřılařılan birçok riskli duruma verilebilecek örneklerdir. Bir riskin üstesinden gelindiğinde arkasından diğeri ortaya çıkmaktadır. Risklerin çeřidi ve miktarı artmakta ve çözüm üretme ihtiyacı bir zorunluluk olarak hem işletme sahiplerinin hem de kamu kurumlarının karřısına çıkmaktadır. Gerekli önlemlerin alınmaması beraberinde felaketleri getirmektedir. Kitlesele ve bazen beklenmedik kurumsal başarısızlıklar, özellikle muhasebe ve raporlamadaki, kurumsal yönetişimde risk yönetimin önemine dikkat çekmektedir (Walker, Shenkir ve Barton, 2002: 2).

Risk yönetim sisteminin önem kazanmasında büyük ve önemli kurumların yaşadığı ekonomik ve finansal çöküşlerin büyük etkisi olmuştur. Kurumlar yaşanan olumsuzluklardan kurtulabilmek ve hedeflerine ulaşabilmek için gelecekte ortaya çıkma olasılığı olan risklerin ve fırsatların önceden farkına varılarak yönetilmesi gerektiği gereğinin farkına varmıştır. Kurumların risk ve fırsatları yönetebilmesini saėlayan risk yönetim sisteminin temel amacı, kuruma deėer katmak, geliřtirmek ve kaynakların en etkin şekilde kullanılarak kurum hedeflerine ulaşılmasını saėlamaktır.

Ülke uygulamalarındaki risk yönetim sisteminin amacı aynı, ancak uygulama modeli ülkeden ülkeye farklılık göstermektedir. Ülke uygulamalarında en fazla dikkat çekenler ise Amerika, Kanada, Avustralya/Yeni Zelanda ve İngiltere risk yönetim modelleridir. Özellikle Avustralya ve Yeni Zelanda ve İngiltere risk yönetim modelleri ISO 31000 standartları dikkate alınarak geliřtirilmiştir. Modeller, temelde risk yönetiminin kurum apında etkili olması gerektiğini savunmakla birlikte esas, ilke ve süreçleri açısından birbirlerinden farklılaşmaktadırlar.

Bu alıřmada, risk yönetim sistemi ile ilgili genel bilgiler verildikten sonra ülke uygulamalarında risk yönetim modelleri incelenmektedir. Konu ile ilgili Türkiye’de yeterli kaynak olmaması nedeniyle yabancı kaynaklar taranmış ve kaynaklara çoėunlukla internet ortamında ulařılmıştır. alıřmanın hem Türk literatürüne hem de bundan sonra yapılacak arařtırmalarda arařtırmacılara katkı saėlayacağı düşünölmektedir.

## 2. Risk Yönetimi

Risk yönetim sisteminin anlaşılabilmesi için öncelikle risk kavramının açıklanması faydalı olacaktır. Risk, plan ve karar sonuçlarındaki belirsizliktir, kaçınılmazdır, stratejik hedeflerin bir fonksiyonudur (Burnaby ve Hass, 2009: 540) ve kurumun başarıya ulaşmasında bariyer rolü üstlenmektedir. İyi şeylerin oluşumunu saėlamak ya da kötü şeylerin oluşumunu engellemek amacıyla risklerin iyi yönetilmesi gerekmektedir (Reding, vd., 2009: 4-3).

Risk yönetimi ise kurumun hedeflerine ulaşmasını engelleyecek risklerin belirlenmesi, azaltılması ve başarıya ulaşılmasını saėlayacak fırsatların ortaya ıkarılarak kullanılması sürecidir (Reding, vd., 2009: 4-3).

İlk olarak sigortacılık sektöründe kullanılmaya başlanan risk yönetimi kavramının ortaya ıkmasında 1967’de Londra’da Edward Lloyd tarafından açılan kahve dükkânının zamanla gemicilikle ilgili bilgi alışverişinin yapıldığı bir yer ve kısa süre sonra denizcilik sigortasının merkezi haline gelmesi etkili olmuştur. Lloyd, oluşturduğu risk havuzları sayesinde risklerin kapsamını

geniřleterek sigortacılık sektörünün lideri konumuna gelmiřtir. Risk yönetimi kavramı uzun bir süre sigorta sektörü ile eř anlamlı kullanıldıktan sonra 1970'lerde Amerika'da iř dünyasında geniř kabul görmeye bařlamıřtır. Bretton Woods anlaşmasının sona ermesi ve 1973-1979 dönemi petrol krizi sonucunda risk oranlama ve deęerlendirme alanında danıřmanlık hizmeti talepleri bařlamıřtır. 1980'lerin ilk yarısı politik risklere aęırlık verilen bir süreçten 1980'lerin sonlarında politik riskler azalmıřtır (Non, 8).

1990'lı yıllar kurumların yönetmeleri gereken risk kapsamının geniřledięinin ve geniřlemeye devam ettięinin farkına varıldıęını dönemlerdir. Bu dönemden itibaren risk yönetimine verilen önem artmıř ve genellikle kurumun çökmesine neden olabilecek risklere odaklanılmaya bařlanmıřtır. Zamanla kapsamlı bir risk yönetim çerçevesi oluřturulması, iç denetimin risk yönetim uygulamaları ile bütünleřtirilmesi, kurum kültüründe risk farkındalıęının ve risk yönetiminde yönetim sorumluluęunun artırılması, kurumlarda risk yönetim ofisi oluřturulması ve kurumsal risk yönetim sisteminin kabulü gibi konularda ařama kaydedilmiřtir (Non, 10).

Risk yönetimi, riskleri deęerlendirmek ve riskin siyasi etkilerini tespit etmek için kullanılan bir yöntem olarak tanımlandıęında sistemin uygarlıęın bařlangıcından beri var olduęu söylenebilir. Ancak bilinçli bir uygulama olup olmadıęı kapsamında deęerlendirildięinde risk yönetimin 20. yüzyılın ortalarına kadar uzanan bir tarihe sahip olduęu ortaya çıkmaktadır (Non, 7).

### **3. Ülke Uygulamalarında Risk Yönetim Modelleri**

Birçok ülkede uygulanmakta olan farklı risk yönetim modelleri bulunmaktadır. Bunlardan en çok tercih edilenleri; Amerika kurumsal risk yönetim sistemi, Avustralya ve Yeni Zelanda, İngiltere ve Kanada risk yönetim sistemleridir. Kurumların tercih ettikleri risk yönetim modelini tespit etmek amacıyla Jacquetta Goy, Grant Purdy ve dięer arařtırmacıların katkılarıyla 2011 yılında bir anket çalıřması hazırlanmıřtır. Ankette 111 ülkeden 1823 katılımcı yer almıř, ancak kullanılan risk yönetim modelinin tespitine iliřkin soruya 1338 katılımcı cevap vermiřtir. Anket sonuçlarına göre kurumların % 36'sı ISO 31000 risk yönetim standartlarını, %18'i COSO kurumsal risk yönetim sistemini, %13'ü AS/NZS 4360 bütünleřik risk yönetim modelini ve % 4'ü BS ISO 31100 standartlarını kullanmaktadır. ISO 31000 standartları hem AS/NZS 4360 standartlarının 2009 yılında revize edilmesinde hem de İngiltere BS ISO 31100 standartlarının 2011 yılında oluřturulmasında temel referans kaynaęı olarak kullanılmıřtır (Goy, vd., 2012: 37). Ařaęıda bu sistemler hakkında açıklamalara yer verilmektedir.

#### **3.1. Avustralya ve Yeni Zelanda Risk Yönetim Modeli**

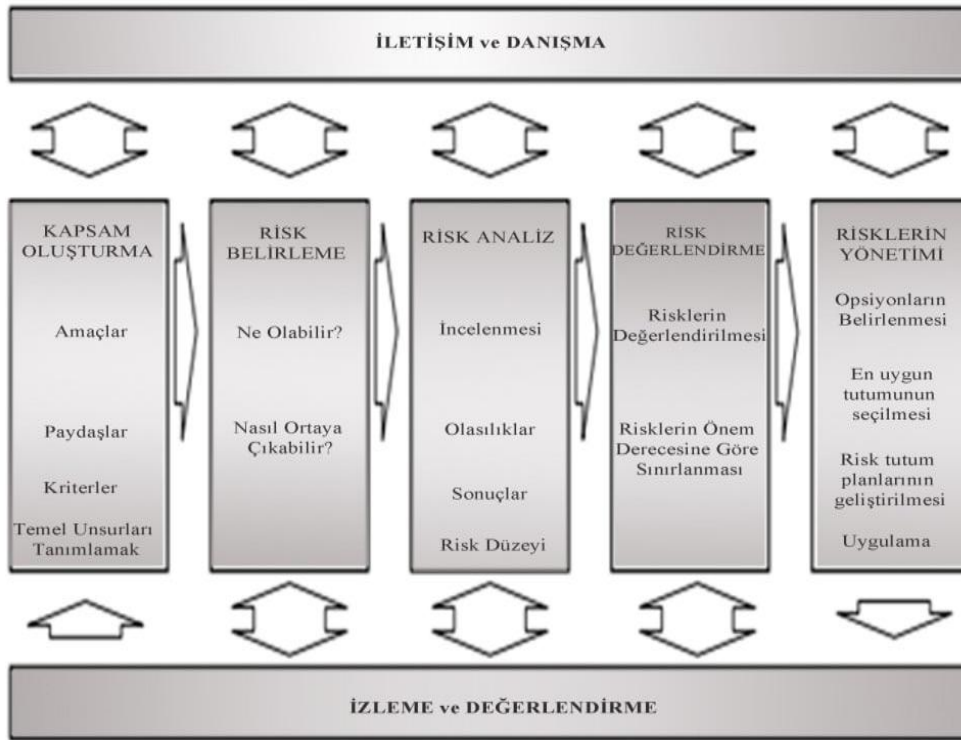
1995'de ortaya çıkan Avustralya ve Yeni Zelanda risk yönetim sistemi, risklerin yönetilmesi ve belgelendirilmesinde dünyanın ilk resmi ve çok güçlü standartlarına sahip bir uygulama modelidir (Inconsult, 2009: 1; Güneř ve Teker, 2010: 68). 2004 yılında yeniden yapılandırılan Avustralya ve Yeni Zelanda risk yönetim standartları "Risk Yönetim Esasları AS/NZS 4360:2004" olarak bilinmektedir. AS/NZS 4360 standartları, Avustralya ve Yeni Zelanda'daki kâr amaçlı ve kâr amacı olmayan grup temsilcilerinden oluřan bir ortak teknik komite tarafından geliřtirilmiř ve her çeřit kurumda kullanılabilir

řekilde tasarlanmıřtır. Yirmi sekiz sayfa uzunluęunda, anlaşılması ve uygulanması kolay ve esnek olan standartlar, kurumsal risk yönetim sisteminin uygulanması için dokuz adımlı bir program sunmaktadır (Arthur J. Gallagher Risk Management Services, 2009: 20). Standartlar, risklerin işlevsel risk yönetim grubu tarafından yönetileceęini ve bu grubun gerekli beceri ve tecrübeye sahip olduğunu ifade etmektedir (Güneş ve Teker, 2010: 68).

Standartlar, hem Sarbanes-Oxley uyumu gerektiren organizasyonlar için risk yönetim metodolojisi olarak hem de riskleri yönetmek için olasılık ve sonuç gibi geleneksel bir yöntem kullanmayı tercih eden organizasyonlar için iyi çalıştıęından kullanımı teşvik edilmektedir. AS/NZS 4360 standartları şirket veya sistemik riskler için teknik risklerden daha iyi çalışır; ancak tehdit risk modeli yapılı uygulamaları saęlayan metotları ele almaz. Ayrıca güvenlik incelemeleri için riskleri sınıflandırsa da web uygulamalarındaki tehditleri belirten yapısal metottaki eksiklięi onu dięer metotlardan daha az çekici kılmaktadır (<http://www.webguvenligi.org>, 2007).

AS/NZS 4360 risk yönetim standartları, risk yönetim sisteminin uygulanması ve geliřimi için yapılması gerekenlere açıklık getiren bir rehber nitelięi göstermektedir. Standartlara göre ilk olarak kurumun stratejik, kurumsal ve risk yönetim kapsamı oluşturulmalıdır. Kurumsal politika; risk yönetim hedeflerini kapsayıcı bir řekilde geliřtirilmeli, kurumsal ve bireysel sorumluluklara, uygulama ve deęerlendirme prosedürlerinin kapsamına açıklık getirmelidir. Risk yönetimi kurum kültürünün bir parçası olmalı ve bu kapsamda risk farkındalıęı ve iletiřim düzeyi artırılmalıdır. Bu amaçla eğitim programlarının organize edilmesi tavsiye edilmektedir. Üst yönetimin sistemi desteklemesi sistemin işlerlięi ve geliřimi için gerekli bir dięer ön adım olarak belirtilmektedir. Standartlara göre risk yönetimi, kurumun planlama ve yönetim süreçlerinin birer parçası haline getirilmelidir. Risk yönetimi ile ilgili kapsam oluşturulduktan sonra riskler tanımlanmalıdır. Daha sonra riskler meydana gelme olasılıkları, etkileri ve sonuçları dikkate alınarak deęerlendirilmeli ve öncelik sırasına konulmalıdır. Risklere yönelik uygulanacak politikalar tespit edilmelidir. Risk yönetim süreci izlenmeli ve deęerlendirilmelidir. Hem kurum içi hem de kurum dışı paydařlarla sonuçlar paylaşılmalı ve bütün süreçlerin yazılı doküman halinde saklanmasına özen gösterilmelidir. Risk yönetim sisteminde süreklilik saęlanarak sistemin uygulanması garanti altına alınmalıdır (Gaidow ve Boey, 2005: 8-9, 47).

AS/NZS 4360 risk yönetim süreci; kapsam oluřturma, risk belirleme, risk analizi, risk deęerlendirme, risk yönetimi, iletiřim ve danıřma, izleme ve deęerlendirme ařamalarından oluřmaktadır (Standards Austria/Standards New Zealand. 2009: 13). Avustralya ve Yeni Zelanda Risk Yönetim Standartları'ndaki risk yönetim süreçleri řekil 1'de gösterilmektedir.



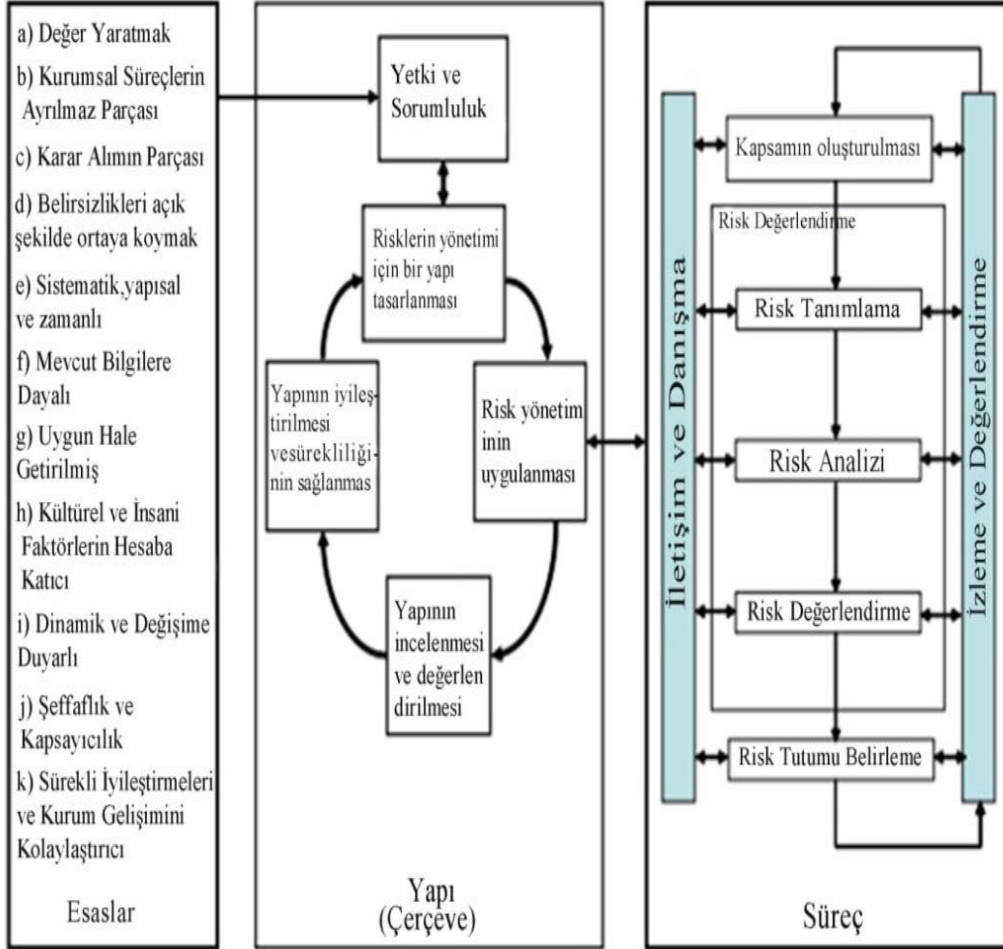
**Őekil 1:** Avustralya ve Yeni Zelanda Risk Yönetim Süreci  
**Kaynak:** Broadleaf Capital International Pty Ltd., 2007: 1.

AS/NZS 4360 risk yönetim standartları 2009 yılında “ISO 31000 Risk Yönetim İlke ve Esasları” dikkate alınarak revize edilmiş ve AS/NZS ISO 31000: 2009 adıyla yayımlanmıştır (Standards Australia/Standards New Zealand, 2009: ii).

ISO (The International Organization for Standardization), ulusal standart kuruluşlarının dünya çapında bir federasyonudur. Uluslararası standartlar genellikle ISO teknik komitelerince hazırlanmaktadır ve ISO 31000 risk yönetim standartları da bu teknik komitelerce hazırlanmıştır (Standards Policy and Strategy Committee, 2010: iv).

ISO 31000, uluslararası risk yönetim standartlarıdır ve işlevsel uygulama modeline yönelik bir rehber niteliği taşımaktadır. Standartlarda, ISO 31000’ne neden gerek duyulduğuna değinilmekte ve risk yönetim sisteminin ilke, esas, yapı ve süreçlerine ilişkin ayrıntılara yer verilmektedir. Ayrıca kurumsal risk yönetim uygulamasına yönelik tavsiyelerde bulunmaktadır (AIRMIC, ALARM, IRM, 2010b: 2,7). ISO 31000 risk yönetim standartları esas, çerçeve

ve sre olmak zere  blmden oluřmaktadır. ISO 31000'in esasları, yapı ve sreleri arasındaki iliřki Őekil 2'de gsterilmektedir.



**Őekil 2:** Risk Ynetim Esas, Yapı ve Sreleri Arasındaki İliřki

**Kaynak:** Standards Australia/Standards New Zealand, 2009: vi; Fionda, 2010: 14.

Őekil 2'de grldę zere ISO 31000 risk ynetim standartlarının belli unsurları bulunmaktadır. Bu unsurların ilk adımı risk ynetim sisteminin esas ya da kapsamının belirlenmesi oluřturmaktadır. Bunun iin kurumun i ve dıř evresinin tanımlanması, mevcut risk ynetim sisteminin zelliklerinin, eksiklerinin ve hatalarının belirlenmesi, risk ynetim sistemi ile ilgili kriterlerin tespit edilmesi ve sistemin kapsamının oluřturulması gerekmektedir. İkinici unsur olan sre ařamasında riskler tanımlanmalıdır (AIRMIC, ALARM, IRM, 2010a: 6).

ISO 31000'de risk; kısa, orta ya da uzun vadede kurumu hem olumlu hem de olumsuz etkileme olasılıęı olan stratejik, faaliyet ve kullanılan yol ve yntem kaynaklı bir olay ya da durum olarak tanımlanmaktadır. Stratejik riskler kurumun uzun dnemli hedeflerine ynelik risklerdir. Faaliyet riskleri kurumun rutin aktivitelerinden kaynaklanan risklerdir. Kullanılan yol ve yntem kaynaklı riskler ise kurumun deęiřimlere karřı verdięi mcadele srecinde

karşılařabileceđi riskler olarak tanımlanmaktadır. Risklerin tanımlanması ařamasında kurum; “ne tür risklerle karşılařılabilir, riskler ne zaman ve nerede ortaya ıkabilir, riskler nasıl ve neden oluşur” sorularını sormalıdır. Riskler tanımlandıktan sonra nicel, yarı nicel ya da nitel teknikler yardımıyla 3\*3, 4\*4 ya da 5\*5 matrisleri kullanılarak, olasılık ve sonuçları dikkate alınarak, önem sıralaması yapılması gerektiđine değinilmektedir (AIRMIC, ALARM, IRM, 2010b: 4-5). ISO 31000 spesifik bir risk sınıflandırma sistemi yerine her kurumun risklerine bađlı olarak uygun bir sistem geliřtirmesini önerir ve risk yönetim sürecinin başarılı bir řekilde uygulanması, desteklenmesi ve sürdürülmesi için gerekli alt yapıyı sunar (AIRMIC, ALARM, IRM, 2010a: 6).

Riskler tanımlandıktan sonra öncelikler belirlenerek kriterlere uygun olarak riskler değeriendirilir. Risklerin yönetilmesinin gerekli olup olmadığına karar verilir. Riskler yönetilirken artık riskler de dikkate alınır. Sürecin her adımının izlenmesi ve raporlanması, sonuçların değeriendirilmesi, risk yönetim sistemi ile ilgili genel değeriendirmelerin yapılabilmesi ve kurum performansının artırılabilmesi için önemli ve gerekli bir diđer adımdır (Pearson, 2007: 26).

Bir diđer unsur olan yapı ařamasında sistemin uygulanabilmesi için sistemin kapsamını içeren bir çerçeve oluşturulması istenmektedir. Risk yönetim sisteminin sürekliliđinin sağlanabilmesi için kurumdaki tüm yönetim sistemleri ile bađlantılı olması ve yönetimin güçlü desteđini alması gerektiđine değinilmektedir (Fionda, 2010: 16). AS/NZS 4360 ve AS/NZS ISO 31000 arasındaki temel farklılıklar řunlardır (Inconsult, 2009: 1):

i. ISO 31000 gerçek bir uluslararası risk yönetim standardıdır ve Kalite Yönetim Standardı ISO 9000 gibi iyi bilinen uluslararası standartların sahip olduđu özelliklere ve saygınlıđa sahiptir.

ii. ISO 31000’de kavram ve tanımlamalarda değışiklik yapılmıřtır. Bazı yeni tanımlar geliřtirilirken bazıları da ıkartılmıřtır.

iii. Risk yönetim ilkeleri, yapısı, kapsamı ve süreçleri arasındaki iliřki ISO 31000’de daha iyi açıklanmakta ve örneklendirilmektedir.

iv. ISO 31000’de risk yönetimini etkin kılmaya yardımcı olmak için dikkat edilmesi gereken on bir adet ilkeye yer verilmektedir.

v. ISO 31000 risk yönetimini geliřtirmek için gerekli beř niteliđi açıklamaktadır. Bunlar: sürekli iyileřtirme, riskler için tam sorumluluk, her türlü karar alımında risk yönetimin uygulanması, sürekli iletiřim ve kurumun yönetim yapısında tam entegrasyon’dur.

AS/NZS ISO 31000 standartlarının kuruma sağladıđı temel faydalar řunlardır (Standards New Zealand, 2010):

i. Risk yönetimin etkinleřtirilmesini sağlayarak hedeflere ulařılma olasılıđını artırır.

ii. Kurum apında risklerin ve tutumların belirlenmesine yönelik farkındalık yaratır.

iii. Fırsat ve tehditlerin belirlenmesinde geliřim sağlar.

iv. İlgili yasal ve uluslararası normlara uygunluk kazandırır.

v. Finansal raporlamayı, kurumsal yönetimi ve paydař güvenini geliřtirir.

vi. Karar verme ve planlama için güvenilir bir temel oluşturur.

vii. Kontrol sistemini geliřtirir.

- viii. Etkin risk tutumu belirlemede kaynak tahsisi ve kullanımı saęlar.
- ix. Faaliyetlerdeki etkinlięi ve verimlilięi artırır.
- x. Kayıpları önlemeyi ve olay yönetimini geliştirir ve kayıpları en aza indirir.
- xi. Kurumsal öğrenmeyi, esneklięi ve direnci artırır.

Hazırlanan risk yönetim raporları ile hem üst yönetime hem de yönetim kurulu ve denetim komitesine önemli risklerin standartlara uygun olarak yönetildięine dair bilgi saęlar (Pearson, 2007: 16).

### 3. 2. İngiltere Risk Yönetim Modeli

Şubat 2008’de İngiltere’de BS 31100 adıyla “Risk Yönetimi: Uygulama Kuralları” taslaęı yayımlanmış ve Haziran 2011’de “BS 31100: 2011 Risk Yönetimi- ISO 31000 için Uygulama İlke ve Esasları” (BS 31100: 2011 Risk Management. Code of Practice and Guidance for The Implementation of ISO 31000) adıyla British Standards Institution tarafından basılmıştır (Peace, 2012: 4; Hopkin, 2012: 57).

BS 31100, ISO 31000’ni destekleyici uygulama kodudur. BS 31100 risk yönetim hedeflerine ulařılması ve risklerin kurum apında yönetilmesi için risk yönetim esas, model, çereve ve süreçlerine rehberlik saęlayacak şekilde tasarlanmış sistematik ve etkili bir standartlar dizisidir (Hopkin, 2012: 64). Standartlar risk yönetim sisteminin, kurumun stratejisi kapsamında ve stratejinin uygulanmasında sürekli ve gelişen bir süreç olması gerektięine dikkat çekmektedir (FERMA, 2003: 3). BS 31100, uluslararası standartlarda olmayan risk yönetimi ile ilgili ek ilkelere de yer vermektedir (<http://www.continuitycompliance.org>). BS 31100 risk yönetim standartları ile ilgili ilkeler şunlardır (MANIGENT, 9):

- i. Risk yönetimi kuruma uygun yapılandırılmalıdır.
- ii. Risk yönetimi kurum kültüründe ve personel algısında yer edinmelidir.
- iii. Risk yönetimi sistematik ve yapısal olmalıdır.
- iv. Risk yönetimi için kurumda genel bir risk dili oluşturulmalıdır.
- v. Risk yönetimi en doęru bilgilere dayanmalıdır.
- vi. Risk yönetimi belirsizlikleri açık bir şekilde deęerlendirmelidir.
- vii. Risk yönetimi karar alım sürecinin bir parası olmalıdır.
- viii. Risk yönetimi şeffaf bir yapıda ve kapsamlı olmalıdır.
- ix. Risk yönetimi dinamik ve deęişimlere uyumlu olmalıdır.
- x. Risk yönetimi süreklilik özellięi taşınmalıdır.
- xi. Risk yönetim ilkeleri dönemsel olarak tekrar deęerlendirilmelidir.

Risk yönetim sisteminin yapısı kapsamında; görev ve baęlılık, risklerin yönetimi için bir içerik oluşturulması (risk yönetim stratejisinin, politikasının, kültürünün, risk iřtahının, risk profilinin ve risk kriterlerinin belirlenmesi; rol, sorumluluk ve yetkilerin yazılı hale getirilmesi; risk yönetim teknik ve araçlarının tespit edilmesi), risk yönetiminin uygulanması, izleme ve deęerlendirme süreci ve sistemdeki hata ya da eksikliklerin giderilmesi ve geliştirilmesi yer almaktadır (Ramsay, 2009: 9; MANIGENT, 10-11).

BS 31100 standartları riskleri inceleme, tanımlama, deęerlendirme, uygun tutumlar belirleme ve raporlama süreçlerinden oluşmaktadır (MANIGENT, 12).



Standartlar risk ynetimin ilke ve terminolojisini oluřturmakta ve kurum hedeflerine ulařma olasılıđını artırmak iin kurum apında etkili risk ynetim sisteminin anlařılması, geliřtirilmesi ve uygulanması iin bir temel sađlamaktadır. Standartlarda, iyi uygulama rnekleri ve tecrbelere dayalı olarak risk ynetim yapı, sre ve uygulamasına ynelik nerilere yer verilmektedir. Temel risk ynetim ilkeleri her kurum iin uygulanabilir niteliktedir; ancak uygulama tekniđi kurumun kapsamı, niteliđi, karmařıklıđı ve byklđne gre deđiřmektedir. Diđer standartlar kayıpları azaltmaya odaklanırken BS 31100 risklerin stlenilerek kurum iin nasıl deđere dnřtrlebileceđi zerine yođunlařmaktadır. BS 31100 standartlarının kullanılması risk ynetim stratejilerine ve kurum hedeflerine ulařıldıđına ve spesifik alan ya da faaliyetlerle ilgili risklerin gerekli tedbirler alınarak ynetildiđine dair gvence verir. Standartlar risk ynetim sisteminin kontroln ve paydařlara rapor sunulmasını sađlar (RIMS, 2011: 9; Ramsay, 2009: 4, 6).

### 3.3. Kanada Risk Ynetim Modeli

Kanada'da uygulanmakta olan "Btnleřik Risk Ynetim Sistemi" standartları Treasury Board Secretariat tarafından yayımlanmıřtır (The President of The Treasury Board, 2010).

Btnleřik risk ynetim sistemi, kurum apında risklerin anlařılmasını, ynetilmesini ve risklerle ilgili gerekli bilgi ve iletiřimin sađlanmasını amalayan sistematik ve sreklilik zelliđi tařıyan proaktif bir sretir (Robillard, 2001: 7). Sistem kurumun kurumsal stratejisine entegre edilmekte ve kurum risk ynetim kltrn biimlendirmektedir. Sistem, kurumun her seviyesindeki olası risklerin srekli deđerlendirilmesini ve daha sonra deđerlendirme sonularının bir araya getirilerek ncelikli dzenlemelerin ve geliřtirici kararların alınmasını gerekli kılmaktadır. Sistemde sadece risklerin azaltılmasına odaklanılmamakta aynı zamanda yenilik getirici faaliyetler desteklenerek kabul edilebilir en iyi sonu, maliyet ve risk oranlarına ulařılması hedeflenmektedir. Sistem risklerin ynetilmesinde daha btnsel bir yaklařımın adapte edilmesine iliřkin esasları belirlemiřtir ve kurumsal dzeyde dengenin sađlanması iin mcadele edilmesini teřvik etmektedir. Bylece hem alıřanlar hem de yneticiler tarafından risklerin yapısı daha iyi anlařılmakta ve daha sistematik bir risk ynetim modeli uygulanmaktadır. Sistem birbiri ile iliřkili drt unsurdan oluřmaktadır. Bunlar ařađıda yer almaktadır (The President of The Treasury Board, 2010):

- i. Kurumsal risk profili geliřtirilmesi:
  - Kurum riskleri evresel tarama ile tespit edilir.
  - Kurum mevcut risk ynetim yapısı deđerlendirilir.
  - Kurum risk profili tanımlanır.
- ii. Btnleřik risk ynetim fonksiyonu oluřturulması:
  - Risk ynetimine ynelik ynetim tebliđinin iletilmesi, anlařılması ve uygulanması.
  - Sistem, karar alım ve raporlama srecine entegre edilir.
  - đrenme planları ve aralar geliřtirilerek kapasite oluřturulur.
- iii. Btnleřik risk ynetim sisteminin uygulanması:
  - Kurumun her dzeyinde ortak bir risk ynetim sreci srekli uygulanır.

- Risk ynetim sonuları karar verme ve ncelikli dzenlemelerin yapımında belirleyicidir.
- Ara ve yntemler uygulanır.
- Paydařlarla iletiřim ve mzakereler srdrlr.
- Srekli risk ynetim uygulamasının ğrenilmesini saėlama:
- Tecrbeye dayalı ğrenmeye, bilgi ve deneyimlerin paylařımına dayalı destekleyici bir alıřma ortamı kurulur.
- ğrenme planları oluřturulur.
- Risk ynetim sonuları yeniliėi, ğrenmeyi ve srekli geliřimi destekleyici řekilde deėerlendirilir.
- En iyi uygulama rnekleri ve tecrbeler paylařılır.

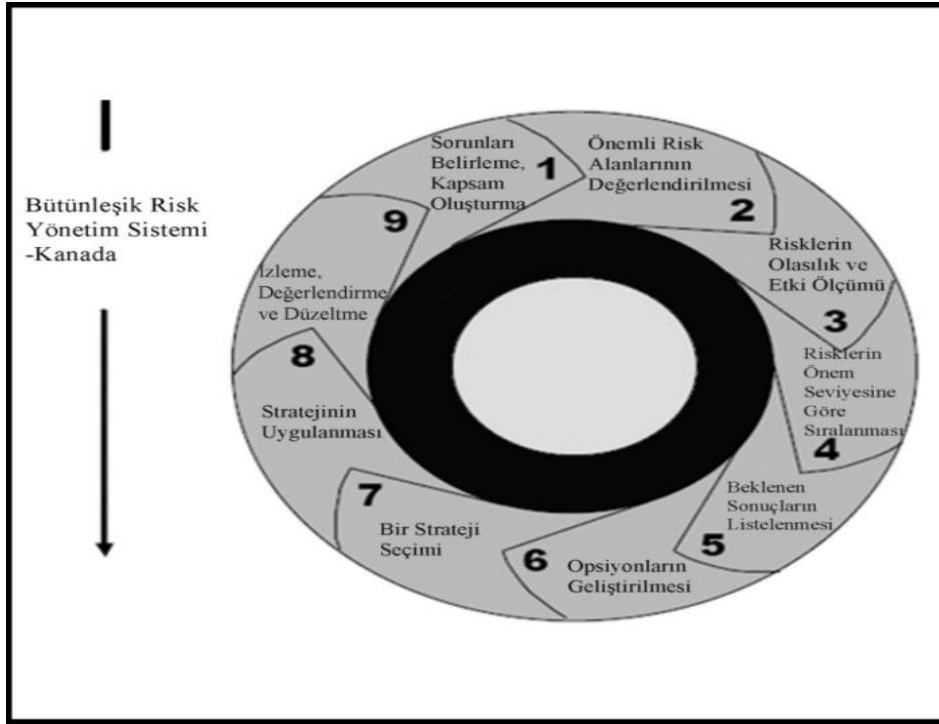
Btnleřik risk ynetim sistemi unsurlarının ilk adımı olan risk profilinin belirlenmesinde kurum faaliyet alanı ve hizmet trnn tespiti son derece nemlidir. Risk profilinin oluřturulmasıyla kurumun faaliyetlerine, hedeflerine ve kaynaklarına ynelik hem i hem de dıř kaynaklı risklerin ve fırsatların farkına varılması saėlanır. Dıř kaynaklı riskler politik, ekonomik, sosyal ve teknolojik olarak sınıflandırılmaktadır. İ kaynaklı riskler ise ynetim sistemi, etik deėerler, bireysel ve kurumsal risk kltr, risk tolerans seviyesi, risk ynetimi konusundaki uzmanlık dzeyi, kurumsal politikalar, prosedrler ve srelerdir. Kurumun mevcut risk ynetim kapasitesinin tespit edilmesi, eksikliklerin ve yapılan hataların anlařılmasını saėlayacaktır. Risk toleransının belirlenmesi ise risk profilinin oluřturulması ve risklerin ynetimi iin gerekli grlmektedir (The President of The Treasury Board, 2010).

İkinci unsur olan btnleřik risk ynetim fonksiyonunun oluřturulmasıyla, risklerin belirlenmesi ve ynetilmesini destekleyici, kurumsal risk ynetim altyapısının oluřturulması ve st ynetimin desteėinin saėlanması kast edilmektedir. Etkili bir risk ynetim sisteminin kurum hedefleriyle, stratejileriyle, hizmet uygulama biimleriyle ve kltryle iliřkilendirilmesi gerekmektedir (Robillard, 2001: 11).

Btnleřik risk ynetim sisteminin uygulanması risklerin kaynaėının belirlenmesi ile bařlayan bir sretir. Riskler belirlendikten sonra riskler etki ve olasılık deėerlendirmesi kapsamında ncelik sıralamasına konulmaktadır. Ortaya ıkma olasılıkları ve kurumu etkileme kapasitelerine gre ncelik sıralaması yapıldıktan sonra risklerin ynetilmesi iin tutumlar belirlenir. Tutumların uygulanma srecinin deėerlendirilmesi amacıyla izleme yapılır. İzleme sreci, risklerin ve tutumların istenen sonulara ulařılmasını destekleyip desteklemediėini belirlemekte ve gerekirse yeni tutumlar ve stratejiler oluřturulmasını saėlamaktadır (The President of The Treasury Board, 2010).

Btnleřik risk ynetim sisteminin son unsurunda risk ynetim sisteminin srekliliėinin saėlanabilmesi iin konu ile ilgili kurum ii ğrenmenin desteklenmesi gerektiėine vurgu yapılmaktadır. Bunun iin eėitim planlarının oluřturulması, risk ynetimi konusundaki iyi rneklerin ve tecrbelerin paylařılması nerilmektedir (Robillard, 2001: 21).

Kanada Btnleřik Risk Ynetim Sisteminin unsurları arasındaki iliřki řekil 3’de gsterilmektedir.



**Şekil 3:** Kanada Bütünlük Risk Yönetim Çerçevesi

**Kaynak:** Non, 23.

Şekil 3’de görüldüğü üzere bütünlük risk yönetim süreciyle ilgili faaliyetler dokuz adımdan oluşmaktadır. Öncelikle sorunların ve fırsatların belirlenmesi ve risk yönetimi ile ilgili kapsamın oluşturulması gerekmektedir. Risk yönetim sisteminde kullanılacak yöntem, uzman personel, araç ve gereçler de ilk adımda tespit edilmelidir. Daha sonraki adımlarda hedeflerle ilişkili faaliyetlere yönelik riskler belirlenir. Risk yönetim sürecine ilişkin beklentiler ya da hedefler tespit edilir ve planlamalar yapılır. Süreçler takip edilerek gerekli durumlarda strateji değişikliğine gidilir ve sistemden maksimum fayda sağlanması amacıyla süreçler izlenir ve değerlendirilir (Robillard, 2001: 16-17).

Bütünlük risk yönetim sisteminde Treasury Board Secretariat, üst yönetici, yöneticiler, danışmanlar, uzmanlar, iç denetçiler ve diğer tüm kurum çalışanlarının görev ve sorumlulukları olduğu belirtilmekte ve bunlara ilişkin ayrıntılı açıklamalara yer verilmektedir (The President of The Treasury Board, 2010).

### 3.4. Amerika Risk Yönetim Modeli

COSO, Amerika’daki beş büyük profesyonel finans kuruluşu (The American Association, The American Institute of Certified Public Accountants, The Financial Executives Institute, The Institute of Internal Auditors ve The Institute of Management Accountants) tarafından desteklenen gönüllü bir özel sektör kuruluşudur. Etkili dış denetim, kurumsal yönetim ve iş ahlakı ile finansal raporların kalitesini artırmaya odaklanmıştır (Arthur J. Gallagher Risk Management Services, 2009, 2009: 20-21).

COSO, daha nceden İ Kontrol –Bütünleřik erevesine (Internal Controls-Integrated Framework) duyulan ihtiyacın aynısının risk ynetimi iin de duyulduėunun farkına vardıktan sonra bir alıřma ierisine girmiřtir. COSO, orjinal kurumsal risk ynetim erevesini 1992 yılında oluřturmuř ve 2002 yılında gncelleyerek son halini vermiřtir (Arthur J. Gallagher Risk Management Services, 2009: 20-21). Kurumsal risk ynetim erevesi, COSO İ Kontrol-Bütünleřik erevesi ile uyumlu olacak řekilde hazırlanmıřtır. Bylece kurumların i kontrole ynelik yatırım yaparken risk ynetim sisteminin geliřimi iin de uygun ortam hazırlaması hedeflenmiřtir (Mattie ve Cassidy, 2008: 3).

COSO tarafından 2004 yılında yayımlanan “Kurumsal Risk Ynetim Bütünleřik ereve ve Uygulama Rehberi (Enterprise Risk Management-Integrated Framework and Related Application Guidance)” ve “Kurumsal Risk Ynetim Bütünleřik ereve ve Uygulama zeti (Enterprise Risk Management-Integrated Framework and Related Executive Summary Framework)” adlı kitaplar kurumsal risk ynetim sistemi ve unsurlarının anlařılması adına nem tařıyan birincil derece kaynaklardır. İyi ynetim uygulamalarının yanı sıra iyi risk ynetim uygulamalarını da ieren İ Denetimin Kurumsal Risk Ynetiminde Oynadıėı Rol (The Role of Internal Auditing in Enterprise-Wide Risk Management) isimli detaylı bir belge de IIA tarafından 2004 yılında hazırlanmıř ve 2009 Ocak ayında revize edilerek tekrar yayımlanmıřtır.

Yukarıda adı geen kaynaklar, yeni bir yaklařım olan kurumsal risk ynetim sisteminin kurulum ve uygulanma srecini ayrıntısıyla aıklamakta ve bu kapsamda ortak bir dil oluřturulması srecine hizmet etmektedir. Bu kaynaklar ayrıca řu anda kabul edilen kurumsal risk ynetim özm yollarını kurum iin kıyaslama aracı olarak deėerlendirmede ve kurumsal risk ynetim uygulaması iin doėru bir yol haritası izmede temel kaynak olma niteliėi tařımaktadırlar (Tonello, 2007: 5).

COSO'nun kurumsal risk ynetim erevesi tasarlamadaki amacı, kurumların uyguladıkları risk ynetim sreleriyle bu yeni sistemi karřılařtırabilmelerini saėlamaktır (COSO, 2005: 3).

Kurumsal risk ynetim sistemi, stratejilerin oluřturulması ve kurum apında uygulanması, kurumu etkileme olasılıėı olan olayların belirlenmesi, risklerin risk iřtahi kapsamında ynetilmesi ve kurum hedeflerine ulařılmasına ynelik makul gvence saėlayan kurum ynetim kurulu, ynetim ve diėer personeli tarafından etki edilen bir sretir (COSO, 2004: 16).

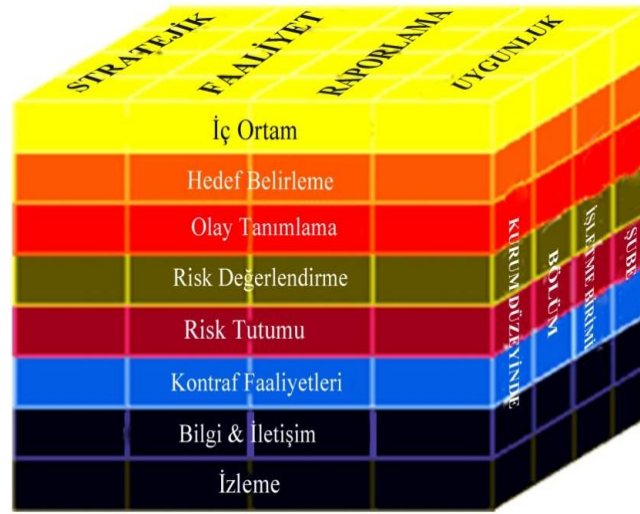
Kurumsal risk ynetim sistemi risklerin entegre edilmesinden daha fazlasını ifade etmektedir. Sistem riski “kurumun hedeflerine ulařmasını ya da stratejilerini bařarıyla uygulamasını olumsuz etkileyen herhangi bir eylem ya da faaliyet olarak” tanımlamaktadır (Walker, Shenkir ve Barton, 2002: 2). Kurumsal risk ynetim sistemi kapsamındaki temel faaliyetler řunlardır (IIA Position Paper: The Role of Internal Auditing in ERM, 2009: 3; PriceWaterHouseCoopers, 2008: 14; Maytjewicz, ve D'arcangelo, 5; Tonello, 2007: 10):

- i. Temel misyon ve program hedeflerini dzgn bir řekilde belirlemek ve kuruma bildirmek.
- ii. Kurum risk iřtahını belirlemek.
- iii. Risk ynetim erevesi dhil olmak zere uygun bir i ortam oluřturmak.
- iv. Kurum hedeflerine ulařılmasını engelleyici olası tehditleri tanımlamak ve risk evreni oluřturmak.
- v. Etki ve olasılık kapsamında riskleri deęerlendirmek.
- vi. Risk tutumlarına karar vermek ve uygulamak.
- vii. Kontrol ve dięer tepki faaliyetlerini yrtmek.
- viii. Kurumun her seviyesinde risklerle ilgili sreklilik temelinde bilgi alıřveriři saęlamak
- ix. Risk ynetim sre ve ıktılarının merkezi izleme ve koordinasyonunu saęlamak.
- x. Risklerin etkili ynetildięine dair gvence sunmak.
- xi. Baęımsız nesnel gvence ve danıřmanlık saęlamak.
- xii. Mevcut sistemlerle (i kontrol, dıř denetim, i denetim) kurumsal risk ynetim sistemini entegre etmek.

Kurumsal risk ynetimin bařlangı noktası kurum misyon ve vizyonunun belirlenmesidir. Ynetim misyon kapsamında stratejik hedefleri belirler, hedeflere ulařılmasını saęlayıcı stratejileri seer (INTOSAI, 2007: 10). Devamında hedeflere ulařmayı engelleyici riskler ve riskleri azaltıcı kontrol sistemleri ve sorumlular belirlenir. Hedeflere ulařılmasını etkileyecek olaylar dzenli olarak belirli aralıklarla gzden geirilir, riskler yeniden deęerlendirilir ve gerekli durumlarda yeni risk tutumları saptanır. Performans ve sonuların zamanında raporlanmasına dikkat edilir (PriceWaterHouseCoopers, 2008: 14; COSO, 2004: 39). Bu disiplinli ve sistematik yaklařım kurumun stratejik, faaliyet, uygunluk, mali vb. risklerini azaltmak amacıyla faaliyetleri planlar, yrtr ve kontrol eder (Razali, Yazid ve Tahir, 2011: 202).

Kurumsal risk ynetim unsurları; “i ortam, hedef belirleme, olay tanımlama, risk deęerlendirme, risk tutumu, kontrol faaliyetleri, bilgi-iletiřim ve izleme”dir (Staciokas ve Rupsys, 2005: 23). Unsurlar birbirleri ile iliřkilidir ve hepsi etkili kurumsal risk ynetim sistemini temsil etmektedir (Kinney, 2003: 141).

COSO, kurumsal risk ynetim unsurlarını  boyutlu kp ile aıklamaktadır (Bkz. řekil 5). Hedefler dikey olarak, unsurlar da yatay olarak kp zerinde gsterilmektedir. Kurum ve birimler de  boyutlu kp zerinde yer almaktadır. Hedeflerle unsurlar arasında doęrudan baęlantı bulunmaktadır. Unsurlar kurumun ulařmak iin aba gsterdięi hedeflerin gerekleřtirilmesinde neyin gerekli olduęunu ortaya koymaktadır (COSO 2004: 23).



**Şekil 4:** Kurumsal Risk Yönetim Sisteminin Unsurları

**Kaynak:** Reding, vd., 2009: 4-5.

Hedef belirleme, kurumun misyon ve vizyonu ile ilişkili ve bunları destekleyici hedeflerin oluşturulması sürecidir. Kurumsal risk yönetim sistemi aşağıda belirtilen dört alanda kurum hedeflerine ulaşılmasını amaçlamaktadır. Bunlar (COSO, 2004: 36-38):

- i. Stratejik hedefler: Kurum misyonu ile uyumlu ve destekleyici yüksek seviyede hedeflerdir.
- ii. Faaliyet hedefleri: Kaynakların etkin ve verimli kullanımını teşvik edici hedeflerdir.
- iii. Raporlama Hedefleri: Hem iç hem de dış raporlamaların güvenilirliğine odaklanılmaktadır.
- iv. Uygunluk Hedefleri: Yasa ve düzenlemelere uygunluk sağlanmasına yönelik hedeflerdir.

Bu sınıflandırma kurumsal risk yönetimin ayrı; fakat eşit derecede önemli yönlerine odaklanılmasını desteklemektedir. Ayrıca farklı kurumsal ihtiyaçlara ve üst düzey yönetim üyelerinin farklı sorumluluklarına ışık tutmaktadır.

Olay tanımlama, kurumun hedeflerine ulaşılmasını olumsuz etkileyen ya da olumlu anlamda destekleyen iç ve dış kaynaklı olayların tanımlanmasıdır (Reding, vd., 2009: 4-7). Risk değerlendirme, risklerin tanımlanarak, analiz edilmesi ve öncelik sırasına konulmasıdır (INTOSAI, 2004: 22). Risk tutumu belirleme sürecinde her riske yönelik bir tutum belirlenir ve riskin etki ve olasılığının en alt düzeye indirilmesi hedeflenir (Olson ve Wu, 2010: 47). Kontrol faaliyetleri risk yönetim süreçlerinin uygun işlemesine yardımcı olmak amacıyla geliştirilen politika ve prosedürlerdir. Denetim yıllık kontrollerle sınırlı olmadığı için belli periyotlarla yapılacak denetimlerle sistemin etkinliği sorgulanır ve sorunlar büyümeden önüne geçilmesini sağlayıcı tedbirler alınmasını sağlar (Mattie ve Cassidy, 2008: 5). Bilgi ve iletişim süreci, sistemin iyi bir şekilde işleyebilmesi için önemli bir unsurdur. Bilgi akışı kurumun riskleri tanımlama, değerlendirme ve yönetmesine yetecek istikrar ve yeterlilikte olmalıdır (Reding, vd., 2009: 4-9,10). Risklerin yönetilebilmesi için önem arz eden hem iç hem de dış kaynaklı bilgi akışının, yöneticilerin uygun

kararlar alabilmesi iin yeterli kalitede olması gerekmektedir. Sistem izlenerek eksik ve hataların tespiti saėlanır ve kalıcı zmler retilir.

#### 4. Sonu

Risk ynetimi, kurumun hedeflerine ulařmasını engelleyecek risklerin ve fırsatların belirlenerek, deėerlendirilmesi ve ynetilmesi srecidir. Bu kapsamda uygulanmakta olan ve bu alıřmada da incelenen Avusturya/Yeni Zelanda, İngiltere, Kanada ve Amerika gibi lkelerde farklı risk ynetim modelleri kullanılmaktadır.

Avustralya/Yeni Zelanda risk ynetim sistemi, risklerin ynetilmesi ve belgelendirilmesinde dnyanın ilk resmi ve ok gl standartlarına sahip bir uygulama modelidir. Standartlar, risklerin ynetilmesine ynelik farkındalıėı artırır, mevzuata uygunluėu saėlar, kontrol sisteminin etkinliėini artırıcı tedbirler alır, raporlamaları dikkate alarak karar alınmasını saėlar, kaynakların etkin ve verimli kullanılmasına ynelik tedbirler geliřtirir.

İngiltere’de uygulanmakta olan risk ynetim standartları, risk ynetiminin kurumun stratejileri kapsamında ve stratejilerin uygulanmasında yrtlen srekli ve geliřen bir sre olması gerektiėine dikkat ekmektedir. Standartlar, kurum hedeflerine ulařma olasılıėını artırmak iin kurum apında etkili risk ynetim sisteminin anlařılması, geliřtirilmesi ve uygulanması iin bir temel saėlamaktadır. Standartlar, kurum hedeflerine ulařılacaėına ve spesifik alan ya da faaliyetlerle ilgili risklerin gerekli tedbirler alınarak ynetildiėine dair gvence verir.

Kanada’da uygulanmakta olan btnleřik risk ynetim sistemi, kurumsal stratejilere entegre edilerek kurumun risk ynetim kltrn biimlendirmektedir. Sistem, her alandaki risklerin srekli deėerlendirilmesini ve deėerlendirme sonularının bir araya getirilerek ncelikli dzenlemelerin ve geliřtirici kararların alınmasını gerekli kılmaktadır. Sistemde sadece risklerin azaltılmasına odaklanılmamakta aynı zamanda yenilik getirici faaliyetler desteklenerek kabul edilebilir en iyi sonu, maliyet ve risk oranlarına ulařılması hedeflenmektedir.

Amerika’da uygulanmakta olan kurumsal risk ynetim sistemi, stratejilerin oluřturulması ve kurum apında uygulanması, kurumu etkileme olasılıėı olan olayların belirlenmesi, risklerin risk iřtahu kapsamında ynetilmesi ve kurum hedeflerine ulařılmasına ynelik makul gvence saėlayan kurum ynetim kurulu, ynetim ve diėer personeli tarafından etki edilen bir sretir. Riskler kurum btnnde etki ve olasılık zellikleri dikkate alınarak deėerlendirilmekte ve ncelik sıralaması yapılarak ynetilmektedir. Bu uygulama kurumun en nemli riskten bařlayarak riskleri ynetmesini saėlar ve riskler arasındaki iliřkinin farkına varılmasına imkn sunar.

Risk ynetim modelleri, temelde aynı hedefe hizmet etmekle beraber uygulamada farklılıklarla karřılařılmaktadır. Hangi lke modeli tercih edilirse edilsin, sistemin uygulanma srecinde karřılařılan sorunlar ve saėladıėı faydalar dikkate alınmalıdır. Risk ynetim sisteminin, kurumun hedeflerine ulařma bařarisını artırmasına ve kuruma deėer katarak geliřim srecini desteklemesine nem verilmelidir.

## Kaynaka

- Aırmıc, Alarm, İrm. (2010a). Kurumsal Risk Yönetimine Yapısal Bakıř Aısı ve ISO 31000 Yüklümlükleri. [http://www.theirm.org/documents/SARM\\_ERM\\_000.pdf](http://www.theirm.org/documents/SARM_ERM_000.pdf). [08.03.2012].
- Aırmıc, Alarm, İrm. (2010b). A Structured Approach to Enterprise Risk Management and the Requirements of ISO 31000. [http://www.theirm.org/documents/SARM\\_FINAL.pdf](http://www.theirm.org/documents/SARM_FINAL.pdf). [28.04.2011].
- Arthur J. Gallagher Risk Management Services, Inc. (2009). Road to Implementation ERM for Colleges and Universities. [http://www.ajgrms.com/portal/server.pt/gateway/PTARGS\\_0\\_28406\\_570\\_311\\_0\\_0\\_18/ERM%20TT%20Report%20Final%209-23-09.pdf](http://www.ajgrms.com/portal/server.pt/gateway/PTARGS_0_28406_570_311_0_0_18/ERM%20TT%20Report%20Final%209-23-09.pdf). [29.05.2011].
- Broadleaf Capital International Pty Ltd. (2007). The Australian and New Zealand Standard on Risk Management, AS/NZS 4360: 2004. [http://www.ucop.edu/riskmgt/erm/documents/asnzs4360\\_2004\\_tut\\_notes.pdf](http://www.ucop.edu/riskmgt/erm/documents/asnzs4360_2004_tut_notes.pdf). [14.08.2011].
- Burnaby, P. ve S. Hass. (2009). Ten steps to enterprise-wide risk management. Corporate Governance, C: 9. S: 5. 539-550.
- COSO. (2004). Enterprise Risk Management-Integrated Framework- Executive Summary Framework. Eylül.
- COSO. (2005). ERM&Implications for Internal Auditors. Corporate Governance and Sarbenes-Oxley Hulb Bulletins. Temmuz. C: 7. S: 6. 1-9.
- FERMA. (2003). Risk Yönetim Standardı. <http://www.ferma.eu/wp-content/uploads/2011/11/a-risk-management-standard-turkish-version.pdf>. [11.03.2012].
- Fionda, S. (2010). The Changing Faces of Risk Management: The Evolution of a Concept. <http://irmforum.files.wordpress.com/2010/12/irmf03thechangingfacesofriskmanagement.pdf>. [10.02.2011].
- Gaidow, S. ve S. Boey. (2005). Australian Defence Risk Management Framework: A Comparative Study. Australia: DSTO Systems. Sciences Laboratory.
- Güneř, ř. ve S. Teker. (2010). Türk Enerji Sektöründe Kurumsal Risk Yönetimi Farkındalıđı. Dođuř Üniversitesi Dergisi, C: 11. S: 1. 64-76.
- Goy, J., G. Purdy, A. Schanfield, J. Lark, J. Talbot, J. D. Plessis, J. DeRose, P. Croke ve A. Dali. (2012). Global ISO 31000 Survey 2011 Result&Analysis. [http://www.iso31000survey.com/Global\\_Survey\\_ISO\\_31000\\_English.pdf](http://www.iso31000survey.com/Global_Survey_ISO_31000_English.pdf). [10.09.2012].
- Hopkin, P. (2012). Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management. Second Edition. Great Britain and United States: Kogan Page Ltd.
- IIA Position Paper: The Role of Internal Auditing in Enterprise-wide Risk Management.* (2009). The Institute of Internal Auditors. [IPPF PP Role of IA in ERM 01.09\[1\].pdf](http://www.iaa.org.uk/PPF_PP_Role_of_IA_in_ERM_01.09[1].pdf). [10.09.2011].



- InConsult. (2009). *Risk Management Update ISO 31000 Overview and Implications for Managers*.  
<http://www.inconsult.com.au/Articles/ISO%2031000%20Overview.pdf>.  
[06.02.2012].
- Intosai. (2004). Guidelines for Internal Control Standards for The Public Sector. 1-71.  
<http://intosai.connexcc-hosting.net/blueline/upload/1guicspubsece.pdf>. [22.05.2011].
- Intosai. (2007). Guidelines for Internal Control Standards for the Public Sector- Further Information on Entity Risk Management. 1-39.  
[http://www.issai.org/media\(577,1033\)/INTOSAI\\_GOV\\_9130\\_E.pdf](http://www.issai.org/media(577,1033)/INTOSAI_GOV_9130_E.pdf).  
[22.05.2011].
- Kinney, W. R. (2003). *The Research Opportunities in Internal Audit. Auditing Risk Assessment and Risk Management Process*. Bölüm 5. Altamonte Springs, FL: The Institute of Internal Auditors.
- Manigent. *What is BS 31100*.  
<http://docsfiles.com/view.php?view=http://manigent.com/storage/downloads/What%20is%20BS31100.pdf&keyword=bs%2031100&count=>.  
[11.09.2012].
- Mattie, J.A. ve D.L. Cassidy. (2008). *Achieving goals, protecting reputation: Enterprise Risk Management for Educational Institutions*.  
<http://www.universityofcalifornia.edu/regents/regmeet/july08/a7a.pdf>  
[11.09.2011].
- Maytjewicz, G. ve J. D'arcangelo. *ERM-Based Auditing*.  
[http://www.gapent.com/media/inthenews/Article-Internal\\_Auditing-ND.pdf](http://www.gapent.com/media/inthenews/Article-Internal_Auditing-ND.pdf). 1-12. [03.11.2010].
- Non, A.J. *Are We Ready for Enterprise Wide Risk Management?*. 1-37.  
<http://www.picpa.com.ph/getmedia/114f621e-84bc-45ff-b43a-961532bb55eb/erm.aspx>. [12.09.2011].
- Olson, D.L. ve D. Wu. (2010). *Enterprise Risk Management Models*. Berlin: Springer –Verlag Berlin Heidelberg.
- Pearson, DDR. (2007). *Managing Risk Across the Public Sector: Toward Good Practice*. Basan: Victorian Auditor-General's Directors: 1-8.  
[http://download.audit.vic.gov.au/files/Managing\\_risk\\_report.pdf](http://download.audit.vic.gov.au/files/Managing_risk_report.pdf) [Eriřim Tarihi: 10.09.2011].
- PriceWaterHouseCoopers. (2008). *A Practical Guide to Risk Assessment*.  
[http://www.pwc.com/en\\_US/us/issues/enterprise-risk-management/assets/risk\\_assessment\\_guide.pdf](http://www.pwc.com/en_US/us/issues/enterprise-risk-management/assets/risk_assessment_guide.pdf) [02.09.2011].
- Ramsay, C. (2009). *Workshop on British Standard Code of Practice for Risk Management BS 31100:2008*.  
<http://www.theirm.org/events/documents/CameronRamsay-BS31100-IRM-23Apr09.pdf> [08.03.2012].
- Razali, A.R., A.S. Yazid ve I.M. Tahir. (2011). The Determinants of Enterprise Risk Management Practices in Malaysian Public Listed Companies. *Journal of Social and Development Sciences*. Haziran. C: 1. S: 5. 202-207.
- Reding, F.K., P.J. Sobel, L. U. Anderson, M.J. Head, S. Ramamoorti, M. Salamasick ve C. Riddle. (2009). *Internal Auditing: Assurance & Consulting Services*, 2. Baskı, The IIA Research Foundation.

- RIMS. (2011). *An Overview of Widely Used Risk Management Standards and Guidelines*.  
<http://www.rims.org/resources/ERM/Documents/RIMS%20Executive%20Report%20on%20Widely%20Used%20Standards%20and%20Guidelines%20March%202010.pdf> [12.04.2012].
- Robillard, L. (2001). *Integrated Risk Management Framework*. <http://www.tbs-ct.gc.ca>. [14.01.2011].
- Staciokas, R. ve R. Rupsys. (2005). *Application of Internal Audit in Enterprise Risk Management*. Engineering Economics. ISSN 1392-2785. S: 2. 20-25.
- Standards Australia/Standards New Zealand. (2009). *AS/NZS ISO 31000:2009 Risk Management-Principles and Guidelines*. <http://sherq.org/31000.pdf> [06.03.2012].
- Standards New Zealand. (2010). *New Risk Management Standard*. <http://translate.google.com.tr/translate?hl=tr&sl=en&tl=tr&u=http%3A%2F%2Fwww.standards.co.nz%2Ftouchstone%2FIssue12%2FBusiness%2FNew%2BRisk%2Bmanagement%2BStandard%2Bavailable%2Bnow%2Bseminars%2Bplanned%2Bfor%2Bearly%2B2010.htm&anno=2>. [04.03.2011].
- Standards Policy and Strategy Committee. (2010). *British Standard Risk Management-Principles and Guidelines BS ISO 31000:2009*. Oxford Brookes Athens. <http://graelaws.files.wordpress.com/2011/01/risk-bsi-2010.pdf>. [05.04.2011].
- The President of The Treasury Board. (2004). *Integrated Risk Management-Implementation Guide*. <http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12254&section=text#sec3.3>.ca [07.02.2011].
- Tonello, M. (2007). *Emerging Governance Practices in Enterprise Risk Management, The Conference Board, Inc.* Research Report R-1398-07-WG, 1-99. [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=963221](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=963221) [01.02.2010].
- Walker, P. L., W.G. Shenkir ve T..L. Barton, (2002). *Enterprise Risk Management*. The Institute of Internal Auditors Research Foundation. <http://www.webguvenligi.org/wp-content/uploads/2007/08/Threat%20Risk%20ModelingTRK.pdf>
- <http://www.continuitycompliance.org/risk-management-bs-iso-31000-vs-bs-31100/>