T.C.
ANKARA SOSYAL BİLİMLER ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

BİLGİ YÖNETİMİ VE GÜVENLİĞİ SİSTEMLERİNDE RİSK YÖNETİMİ UYGULAMA FARKINDALIĞI: ÜNİVERSİTELER ÜZERİNE BİR İNCELEME

Yüksek Lisans Tezi

Emine İPEK DİNÇER

Denetim ve Risk Yönetimi Ana Bilim Dalı
Tezli Yüksek Lisans Programı

Ağustos 2023

T.C.
ANKARA SOSYAL BİLİMLER ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

BİLGİ YÖNETİMİ VE GÜVENLİĞİ SİSTEMLERİNDE RİSK YÖNETİMİ UYGULAMA FARKINDALIĞI: ÜNİVERSİTELER ÜZERİNE BİR İNCELEME

Yüksek Lisans Tezi

Emine İPEK DİNÇER

Denetim ve Risk Yönetimi Ana Bilim Dalı
Tezli Yüksek Lisans Programı

Tez Danışmanı
Dr. Öğr. Üyesi Ali DURDU

Ağustos 2023

KABUL VE ONAY SAYFASI

TEŞEKKÜR

Tezimi hazırlamamda önerileriyle yol gösteren ve her zaman destek olan danışmanım Dr. Öğr. Üyesi Ali DURDU'ya teşekkürü borç bilirim.

Tez çalışmam boyunca bilgi, tecrübe ve desteğini esirgemeyen canım babam Mehmet İPEK'e, manevi desteklerini her zaman hissettiğim canım anneme, canım kardeşime ve bana her anımda destek olan sevgili eşime teşekkürlerimi sunarım.

İÇİNDEKİLER

ÖZET

Günümüzde artan rekabet ortamı ile birlikte başarılı olmak isteyen işletmeler hem bilgi hem de risk yönetimi konularına öncelik vermek istemektedirler. Gelişen teknoloji ile birlikte bilgi yönetimi ve risk yönetimi konularını ayrı düşünmek pek de mümkün olmayacaktır. Bilgi yönetimi ve risk yönetimini başarılı bir şekilde birlikte uygulayabilen işletmeler başarılı olmaktadır.

Artık işletmeler sermaye yatırımlarından çok teknolojik yatırımlara yönelmektedir. Teknoloji ile beraber daha iyi bir risk yönetimi sağlanabilir. İyi bir risk yönetimi için bilgi güvenliği ve bilgi varlıklarının korunması son derece önemlidir. Risklerin etkin bir şekilde yönetimi doğrudan bilginin yönetimi ile ilişkilidir. Bu doğrultuda bilgi tabanlı risk yönetimi işletmeler tarafından tercih sebebi olmuştur. Bilgi yönetim sistemleri ile risk yönetim sistemleri birbiri ile entegre edilmiş olmalıdır.

Risk yönetimi süreçlerinde bilgi kaynaklı varlıkların potansiyel risklerin belirlenmesi, risklerin değerlendirilmesi ve risklere verilecek cevapların belirlenmesi amaçlanır. Bilgi sistemlerinin güvenliği ile birlikte ortaya çıkacak risklerde azaltılmış olur. Bilgi güvenliği beraberinde başarılı bir risk yönetimi ile rekabet avantajı, şirket karlılığı, sürdürülebilirlik ve itibar kazanımı da sağlanır.

Bu çalışmada bilgi yönetimi ve risk yönetimi kavramları açıklanmış, bilgi yönetimi ve güvenliği sistemlerinde risk yönetiminin yeri ve önemi ortaya koyulmaya çalışılmış, anket katılımcılarının davranış ve farkındalığının incelenmesi amaçlanmıştır. Bu çalışmada yöntem olarak Türkiye'de faaliyet gösteren Üniversitelerde çalışan idari personele yönelik bir anket çalışması yapılmıştır. Anket çalışmasında hem demografik hem de katılımcıların konuya yaklaşım ve farkındalığını ortaya çıkaracak sorulara yer verilmiştir.

Anahtar Kelimeler: Bilgi, Bilgi Yönetimi, Bilgi Güvenliği, Risk, Risk Yönetimi, Bilgi Riski Yönetimi

ABSTRACT

Today, businesses that want to be successful with the increasing competitive environment want to give priority to both information and risk management. With the developing technology, it will not be possible to think separately about information management and risk management. Businesses that can successfully implement information management and risk management together are successful.

Businesses are now turning to technological investments rather than capital investments. Better risk management can be achieved with technology. Information security and protection of information assets are extremely important for good risk management. Effective management of risks is directly related to the management of information. In this direction, knowledge-based risk management has been preferred by businesses. Information management systems and risk management systems should be integrated with each other.

In risk management processes, it is aimed to determine the potential risks of information-based assets, to evaluate the risks and to determine the answers to the risks. The risks that may arise with the security of information systems are reduced. Along with information security, a successful risk management provides competitive advantage, company profitability, sustainability and reputation gain.

In this study, the concepts of information management and risk management were explained, the place and importance of risk management in information management and security systems was tried to be revealed, and it was aimed to examine the behavior and awareness of the survey participants. In this study, a survey was conducted for the administrative staff working in universities operating in Turkey as a method. In the survey study, both demographic questions and questions that will reveal the approach and awareness of the participants were included.

Keywords: Information, Information Management, Information Security, Risk, Risk Management, Knowledge Risk Management

KISALTMALAR

BRY: Bilgi Riski Yönetimi

BR: Bilgi Riski

BY: Bilgi Yönetimi

BGYS: Bilgi Güvenliği Yönetimi Sistemi

COSO: (Committee Of Sponsoring Organizations Of The Treadway Commission) Treadway Komisyonu Sponsor Kuruluşları Komitesi

ERM: Enterprise Risk Management (Kurumsal Risk Yönetimi)

IIA: The İnstitute Of İnternal Auditors (İç Denetçiler Enstitüsü)

ISO: (International Organization For Standardization) Uluslararası Standartlar Teşkilâtı,

IEC: (International Electrotechnical Commission) Uluslararası Elektroteknik Komisyonu

IRM: (Institute Of Risk Management) Risk Yönetim Enstitüsü

KRM: (Knowledge Rısk Management) Bilgi Risk Yönetimi

KRY: Kurumsal Risk Yönetimi

RY: Risk Yönetimi

TSE: Türk Standartları Enstitüsü

TUSİAD: Türk Sanayicileri ve İş İnsanları Derneği

ŞEKİL LİSTESİ

TABLO LİSTESİ

GRAFİK LİSTESİ

1. BÖLÜM: GİRİŞ

Bilgi Yönetimi ve Risk Yönetimi kavramları günümüzde eskiye göre daha da önem kazanmaktadır. Kurumların /İşletmelerin rekabet ortamına uyum sağlayabilmeleri ve ayakta kalabilmeleri için hem bilgiyi hem de karşılaştığı riskleri en iyi şekilde yönetebilmeleri gerekir.

Günümüzde başarılı olmak isteyen işletmeler sermaye ve fiziksel varlıklarını artırmaktan çok bilgi ve risk yönetimi konularına önem vererek beşerî yatırımlar yapmalıdırlar. Aynı zamanda teknolojik yatırımlara da öncelik verilmelidir. Teknoloji bu süreçte bir amaç değil araç olmalıdır. Bilgi güvenliği de teknoloji sayesinde sağlanmaktadır. Bilgi güvenliği beraberinde başarılı bir risk yönetimi ile işletmelere rekabet avantajı, şirket karlılığı, sürdürülebilirlik ve itibar kazanımı da sağlanır.

Risklerin çeşitliliği ve dinamikliği göz önünde bulundurulduğunda yöneticilerin işletmelerine katma değer sağlayabilmek için risk temelli yaklaşıma sahip ve bilgi teknolojileri destekli düşünce yapısında olmaları oldukça önemlidir.

Tezin birinci bölümünde araştırmanın amacı ve metodolojisi ile konuya ilişkin literatür taramasına yer verilmiştir. İkinci ve üçüncü bölümlerinde bilgi, bilgi yönetimi, bilgi güvenliği, risk, risk yönetimi kavramları detaylı şekilde anlatılmıştır. Tezin dördüncü bölümünde bilgi yönetimi ve risk yönetimi arasındaki ilişkiyi ortaya koyabilmek için bilgi riski yönetimi ve bilgi yönetimi anlayışında risk yönetimi konusuna değinilmiştir. Ayrıca bilgi yönetimi ve güvenliği sistemlerinde risk yönetimi uygulama farkındalığını incelemek üzere Türkiye'de bulunan Üniversitelerde çalışan idari personele yönelik anket çalışması yapılarak anket bulgularına yer verilmiştir. Tezin son bölümünde anket çalışmasının sonuçları, yorumlar ve bazı öneriler yer almaktadır.

1.1. Araştırmanın Amacı ve Metodolojisi

Yapılan araştırmada bilgi yönetimi ve risk yönetimi kavramları açıklanarak birbiri ile ilişkisini, bilgi yönetimi ve güvenliği sistemlerinde risk yönetimi uygulamasının rolü ve önemine ilişkin tutum ile farkındalığın belirlenmesi amaçlanmıştır.

Bu tezde nitel ve nicel araştırma yöntemleri kullanılmıştır. Nitel araştırma yöntemlerinden gözlem ve yazılı dokümanların incelenmesi kullanılmıştır. Nicel araştırma

yöntemi olarak anket tercih edilmiştir. Araştırmada veri toplama aracı olarak anket yöntemi kullanılmıştır. Bilgi Yönetimi Anlayışında Risk Yönetimi uygulamalarının analizini yapmak üzere Türkiye'de faaliyet gösteren Üniversitelere "Bilgi Yönetimi Anlayışında Risk Yönetimi Anketi" düzenlenmiştir. Anket internet üzerinden yayınlanmış ve ankete ait web adresi ile anketin doldurulması istenmiştir. Araştırma da kullanılan anket soruları bilgi ve risk yönetimi kuramlarından ve mevcut anket formlarından yararlanılarak oluşturulmuştur.

Anketin amacı; bilgi yönetimi ve güvenliği sistemlerinde risk yönetimi uygulaması arasındaki bağlantıyı, katılımcıların konuya davranış, yaklaşım, tutum ve farkındalıklarını ortaya koyabilmektir.

Anketin evrenini Türkiye'de faaliyet gösteren Üniversitelerde çalışan idari personeller oluşturmaktadır. 491 adet idari personel ankete katılım sağlamıştır. Anket 20 sorudan oluşmakta olup, soruların bir kısmı katılımcıların demografik özelliklerine yönelik olup diğerleri ise araştırmanın geneline yönelik tutum ve farkındalığı belirlemeyi amaçlamaktadır.

Araştırmada bazı kısıtlarla karşılaşılmıştır. Bunlardan biri anket çalışması Türkiye'de faaliyet gösteren Üniversitelerde çalışan idari personellere yönelik olmasına rağmen akademik personelin veya ilgisiz kişilerin ankete katılım sağladığı gözlemlenmiştir. Bir diğeri anketin Türkiye'de faaliyet gösteren tüm üniversitelere ulaşmamış olabilmesidir.

Anket yoluyla elde edilen bulgular SPSS İstatistik Programı ile değerlendirilerek analiz edilmiş bulgularla ilgili yorum ve sonuçlara dördüncü ve beşinci bölümde yer verilmiştir.

1.2. Literatür Taraması

Literatürde bilgi yönetimi ve risk yönetimi konularında ayrı ayrı çalışmalar yer aldığı gibi bilgi riski yönetimi, bilgi sistemlerinde risk yönetimi gibi konulara değinen çalışmalarda bulunmaktadır. Bu çalışmalara bakacak olursak;

Bilgi yönetimi kavramı konusunda Barutçugil (2002) bilgi yönetimini kapsamlı şekilde anlattığı bir kitap yayınlamıştır. Güçlü ve Sotirofski (2006) bilgi yönetimi kapsamlı şekilde ele almıştır. Öğüt (2001) bilgi çağında yönetim konusunu incelemiştir. Canbazoğlu (2000) bilgi yönetiminde insan faktörüne değinmiştir. Davenport ve Prusak (2001) iş dünyasında bilgi yönetimi konusunu incelemiştir. Gülseçen (2014) ve Özgür (2012) genel olarak bilgi yönetimi konularına değinerek inceleme yapmışlardır. Fidancı (2017) bilgi yönetimi uygulamalarının farkındalığını belediyede çalışan personellere yönelik olarak incelemiştir. Kınık (2019) devlet üniversitelerindeki lisans öğrencileri ve akademik personelin bilgi yönetimi yeterliliklerini ve

farkındalıklarını ölçerek bilgi yönetiminin etkinliğini arttırmayı amaçlamıştır. Öztürk (2021) bilgi yönetiminin örgütsel performansa etkisini Türkiye'nin 500 büyük sanayi kuruluşunda anket çalışması yaparak incelemiştir.

Uzun ve Durna (2008) bilgi yönetimini rekabet unsuru olarak görmüşler ve bu yönde bir inceleme yapmışlardır. Sözbilir ve Yeşil (2016) bilgi yönetiminin rekabetçi avantaj üzerine etkisini sanayi işletmelerine yaptığı bir anket çalışması ile incelemiştir. Durdu ve İpek (2020) yine bilgi yönetiminin işletmelere yenilik ve rekabet üstünlüğü sağlamasını incelemişlerdir.

Canber ve Sağıroğlu (2006) bilgi güvenliği ve bilgi güvenliğinin süreçleri üzerine bir araştırma gerçekleştirmişlerdir. Bilgi kavramını açıklayarak, bilişim teknolojilerinin bilgi kavramı üzerindeki etkileri ile boyutlarını ortaya koymuşlar ve kazanımı zor olan bilginin saklanması ihtiyacından doğan bilgi güvenliği ile bilgi güvenliğini oluşturan ana unsurları incelemişlerdir. Özdemir (2019) kamu çalışanlarının bilgi güvenliği farkındalığını ortaya koyan bir çalışmaya yer vermiştir. Eren (2021) bilgi güvenliği yönetim sistemlerinin yükseköğretim kurumlarında sürdürülebilirliğinin sağlanıp sağlanmadığı konusunda inceleme yapmıştır. Ecek (2022) ise Zonguldak ilinde bulunan kamu kurumlarında çalışan personellerin bilgi güvenliği önlemlerine dair tutumlarını incelemiştir.

Marttın ve Pehlivan (2010) ISO 27001 bilgi güvenliği yönetim sisteminin bir kamu kuruluşu üzerinde incelemesini yapmıştır. Yılmaz (2014) ISO 27001 kapsamında bilgi güvenliği risk analizi yaparak bir inceleme yapmıştır. Çakır ve Tuygun (2019) ISO 27001 bilgi güvenliği yönetim sistemi standardının kamu kurumlarına uygulanabilirliğinin araştırabilmek için Ankara ilinde bulunan kamu kurum ve kuruluşlarına bir anket çalışması yapmıştır.

Risk Yönetimi kavramı konusunda Fıkırhoca (2003) bütünsel risk yönetimi konusunda, Kızılboğa (2012) geleneksel olarak uygulanan risk yönetiminden kurumsal olarak uygulanan risk yönetimine geçiş konusunda, Emhan (2009) risk yönetimi süreçleri ve teknikleri konusunda, Kızılboğa (2012) risk yönetimi modelleri konusunda inceleme yapmışlardır. Sobel (2015) denetçilere rehberlik edecek bir risk yönetim rehberi oluşturarak yayınlamıştır. Özer (2012) işletmelerin başarısının büyük ölçüde karşı karşıya kaldıkları riskleri yönetebilmek olduğunu düşünmüştür. Bu doğrultuda risk yönetimini rekabet ortamında var olabilme aracı olarak görmüş ve bu şekilde bir inceleme yapmıştır. Ahi (2020) özellikle 2008 krizi sonrası bankacılık sektöründe risk yönetimi konusunu ele alırken Güner (2020) aracı kurumlarda uyum ve risk yönetimi konusuna değinmiştir. Bay (2023) rekabet stratejilerinin işletme performansı üzerindeki etkisinde risk yönetimi uygulamalarının rolünü sanayi kuruluşları üzerine bir anket

çalışması yaparak incelemiştir. Rekabet stratejileri ve işletme performansı ölçekleri ile rekabet stratejileri ve risk yönetimi ölçekleri arasında ilişkiyi anlamlı ve pozitif yönlü bulmuştur.

COSO (2004-2017) Kurumsal risk yönetimi rehberi ile aslında kurumsal risk yönetiminin temellerini oluşturmuştur. Hazine ve Maliye Bakanlığı kamu iç denetim rehberi, TUSİAD (2008) kurumsal risk yönetimi konusunda kaynak olabilecek bir rehber yayınlamıştır, Akçakanat (2012) kurumsal risk yönetimi süreci konusuna değinmiştir. Derci ve Sarı (2007) Kurumsal risk yönetimini Sayıştay üzerine bir uygulama ile incelemiştir. Koç ve Çelik (2015) Kurumsal risk yönetimini bankacılık sektörü üzerine incelemiştir. Usman (2018) Kurumsal risk yönetiminde risk değerleme raporunun hazırlanması üzerine bir çalışma yapmıştır. Buca (2017) yenilenen COSO kurumsal risk yönetimi çerçevesini eski formatına kıyaslayarak incelemiştir. Bozdağ (2020) kurumsal risk yönetimini üniversiteler için bir örnek olay uygulaması çalışması yaparak kendi uygulamaları ve kapasiteleri kapsamında bu çalışmadan yararlanmak isteyen üniversitelere sunmuştur.

IRM (2010) kurumsal risk yönetimine ile ISO 31000 standardının yükümlülüklerini harmanlayarak derlemiştir. Altınbaş (2017) ISO 31000 risk yönetimi standardı ve bir portföy yönetim şirketi üzerine uygulamalı olarak araştırma yapmıştır. Uysal (2021) ISO 31000 standardının 2009 ve 2018 versiyonlarını karşılaştırarak COSO kurumsal risk yönetiminin 2017 versiyonuyla aralarındaki farklara ve benzerliklere değinmiştir Ağgül (2022) ISO 31000 risk yönetim standardını bir üretim işletmesi üzerine uygulamalı olarak incelemiştir.

Bilgi sistemlerinde güvenliğin sağlanabilmesi bilginin korunması, gizliliği ve bütünlüğün sağlanabilmesi ile doğrudan ilişkilidir. Gibson (1997) bir bilgi sisteminin tasarımının riske bağlı olduğunu savunarak, risk yönetimi için bilgi sistemleri konusunu ele almıştır. İren ve Can (2015) bilgi sistemlerinde risk yönetimi konusunu incelemişlerdir. Dimitrijevic (2014) risk yönetiminin bilgi sistemlerinin riskini de içermesi gerektiğini söyleyerek bilgi yönetimi alanında risk değerlemesini ele almıştır. Durdu (2021) bilgi sistemlerinde riskler ve risk yönetimi konusunu incelemiştir.

Massingham (2010) bilgi riski yönetimi konusunda bir çerçeve çizmiş ve örnek bir KRM modeli ile analiz yapmıştır. Neef (2005) şirketlerin bilgi ve risk kavramlarını bir arada kullanarak KRM (bilgi riski yönetimi) sistem ve tekniklerini uygulaması ve daha iyi bir bilgi yönetimi yoluyla kurumsal riski yönetme konularında inceleme yapmıştır. Alwahari ve diğerleri (2008) bilgi temelli risk yaklaşımı ile beraber bilgi yönetimi sürecinin proje riski yönetimindeki rolünü incelemişlerdir. Trkman ve Desouza (2012) bilgi yönetimiyle ilişkili

risklere atıfta bulunmak için bilgi riski yönetimi ifadesini kullanmışlar ve bilgi risklerini sınıflandırarak bu risklerin bilgi transferini nasıl etkilediğini incelemişlerdir. Rodriguez ve Edwards (2014) daha iyi bilgi yönetiminin daha iyi bir risk kontrolü ile ilişkili olduğunu düşünerek kurumsal risk yönetimi destekleyen bilgi yönetimi adıyla bir inceleme yapmışlardır. Mercier ve Laurent (2016) bilgi ve risk kavramlarını açıklayarak bilginin risk yönetimindeki rolünü analiz etmiştir. Durst ve Diğerleri (2019) bilgi riski yönetiminin örgütsel performansa nasıl etki ettiğini araştırmışlardır.

Ülkemizde yapılan çalışmalara bakıldığında bilgi ve risk yönetimi kavramlarına bir arada yer veren pek fazla kaynak bulunmamaktadır. Bu doğrultuda bu tezde yapılan incelemenin geliştirilerek literatüre katkı sağlayacağı düşünülmektedir.

2. BÖLÜM: BİLGİ KAVRAMI

Bilgi, yüzyıllardır felsefecilerin ve akademisyenlerin ilgisini çekmiştir. Bilgi kavramı, ilk olarak antik Yunan filozofu Plato tarafından gerçek inanışlar olarak tanımlanmış ve günümüze kadar bilgi kavramının pek çok tanımı yapılmıştır. 21'inci yüzyılda bilgi gerek bireyler gerekse kurumsal açısından oldukça önemli bir kavram haline dönüşmüştür.

Latin dilinde 'informatio' kökünden gelen bilgi kavramı şekil verme, biçim verme, bilgi veya haber verme eylemi olarak adlandırılmaktadır. Bunun yanı sıra en yaygın ifadesi ile bilgi, haber verme veya enformasyon anlamına gelmektedir. Selvi'ye göre (Balay, 2004).

Türk Dil Kurumu sözlüğünde bilgi 'İnsan aklının erebileceği olgu, gerçek ve ilkelerin tamamı, malumat' olarak tanımlanmıştır. Bilgi kavramı bakış açısı ve kullanım alanına göre birçok çeşitte anlamlara sahip olan karmaşık bir yapıya sahiptir. Bilgi çok karmaşık bir yapıda olduğundan ötürü farklı bağlamlarda veya farklı anlamlarda kullanılabilir. Selvi'ye göre (Balcılar, 2008). Bilgi; bilimsel, enformatik, açık, kapalı, teknolojik gibi sınıflandırmalara ayrılabilir. Bilginin sınıflandırılmasında en çok karşılaşılan sınıflandırılma tipleri bilimsel ve enformatik olarak karşımıza çıkar. Enformatik bilgi kodlanıp, saklanabilip ve aktarılabilirken; bilimsel bilgi aktarımı sağlanabilen bu bilgilerin deney yoluyla metotlanabilir ve kodlanabilir bir biçimde ortaya koyulmasıdır. Selvi'ye göre (Sümer,2007).

Bilgi tarih boyunca güç anlamına gelmiştir ve tüm toplumları ilgilendirmiştir. Bunun nedeni ise yaşantımızın kökünde olmasıdır. Bilgiyi elinde bulunduranlar güçlü olarak nitelendirilmektedir. Bilgiyi kullananlar rakiplerinin de önüne geçmektedir.

İçinde bulunulan bilgi çağında herkesin bilgi toplumuna erişme yolları araması ve bilgi kavramına herkesin önem vermesi çok doğaldır. Bilgiyle birlikte iç yaşantımız şekillenir, sosyalleşmemize ve kendimizi geliştirmemize yardımcı olur ve süreci hızlandırır.

2.1. Bilginin Oluşumu

Bilgiyi esas olarak örgütsel faaliyetlerin en temel girdisi şeklinde tanımlamak mümkündür. Bilgi kavramını tanımlarken bilgiyle ayrı düşünülemez veri ve enformasyon kavramlarına da bakmak gereklidir. Veri işlenmemiş ham gerçekler olarak tanımlanabilir.

Enformasyon ise verinin işlenmiş ve düzenlenmiş halidir. Enformasyon da yorumlanarak bilgiye dönüştürülür. Bu 3 kavram birbirinden ayrı düşünülemez (Abdullah ve Diğerleri, 2005).

Bilgi hiyerarşisi dört basamaklı piramit olarak aşağıda gösterilmiştir. (Şekil 2.1). Piramidin en altında, birbiriyle bağlantısı olmayan ve anlamsız veriler; ikinci basamakta veriler arasındaki ilişkiyi barındıran enformasyon; üçüncü basamakta, karar alınırken kullanılma potansiyeli olan düzenlenmiş enformasyonları içeren bilgi; en üst basamakta ise bilginin nerede kullanılacağını ve nasıl etkili olacağını bilen bilgelik bulunmaktadır (Cooper, 2010).

Şekil 2.1: Bilgi Piramidi

Veri

Bilgi piramidinin en altında yer alan veri işlemlerin işlenmemiş bir biçimde kayıtlarda tutulmasıdır. Veri, işlenmemiş ham gerçekler, özümsenemeyen ve yorumlanamayan gözlemler olarak tanımlanabilir. Verinin teknolojik ortamlarda saklanması gerekir ve bir anlam veya içerik ifade etmez (Barutçugil, 2002).

Tüm yapıların veriye ihtiyacı vardır. Yapının veriden enformasyon üretebilmesi adına ihtiyacı olan veri türünü ve sayısını belirlemelidir. Güçlü ve Sotirofski'ye göre (Awad ve Ghaziri, 2004)

Enformasyon

Bilgi piramidinin ikinci katında yer alan enformasyon, verilerin düzenlenmiş hali olarak tanımlanabilir. Güçlü & Sotirofski'ye göre (Barutçugil, 2002).

Enformasyon verilerin düzenlenmiş hali olup anlamlıdır ve bir amacı vardır. Konu ile ilgili ve belirli bir amaç için düzenlenmiştir. Enformasyon, taraflara yani yönetici ve çalışanlara e-posta, ağ bağlantıları veya internet ile iletilir. Güçlü ve Sotirofskiye göre (Awad ve Ghaziri,

2004). Enformasyon, bilgi oluşturmak için gerekli bir unsur olarak görülür. Verileri yorumlamak için bir bakış açısı kazandırır. Enformasyon, veriye biçimlendirerek bilgiye katkıda bulunur. Güçlü'ye göre (Nonaka, 2004). Enformasyon ve veri için kullanılan sorular; "kim-ne-nerede-ne zaman?" soruları iken bilgi için "neden?" ve "niçin?" sorulan sorulur. Güçlü ve Sotirofski'ye göre (Malhotra, 2000).

Bilgi

Bilgi piramidinin üçüncü katında yer alan bilgi, insan aklının düşünebileceği olgu, gerçek ve ilkelerin bütünüdür (Gülseçen, 2014). Bilgi, veri ve enformasyonun anlamlı bir şekilde biçimlendirilmiş halidir.

Bilgelik

Bilgi piramidinin en üstünde yer alan bilgelik yani akıl, bilginin nerede ve nasıl etkili bir şekilde kullanılacağını bilmektir (Gülseçen, 2014).

2.2. Bilgi Türleri

Literatürde bilginin çeşitli sınıflandırmaları yapılmaktadır. Bu çalışmada en çok kullanılan bilgi türlerine yer verilmiştir.

2.2.1. Örtük (Kapalı) Bilgi

Açıkça ifade edilmeyen ve ima yoluyla anlam çıkarılan bilgi olarak tanımlanabilir. Örtük bilgi kolaylıkla fark edilebilir, ifade edilebilir ve kişiseldir. Örtük bilginin açığa çıkarılması rekabet açısından önemlidir. Örtük bilgi bilişim teknolojileri ile açığa çıkarılabilir.

Kurumlarda örtük bilginin açığa çıkarılması çalışan tecrübesi ve sezgilerinden yararlanılarak yapılır.

Örtük bilginin kalitesini 2 önemli faktör belirler. Bunlardan birincisi bireysel tecrübe ve deneyimlerin kullanılması. İkincisi ise deneyim ve tecrübe kalitesinin iyi olmasıdır (Nonaka, 1994).

2.2.2. Açık Bilgi

Açık bilgi bir araya getirilmiş ve çoğunlukla metin, tablo, kitap vs. şeklinde sunulan bilgidir. Açık bilgi kurum içinde herkes tarafından kolayca anlaşılabildiğinden örtük bilgiye

göre daha hızlı iletilir ve düzenlenir. Açık bilgi yoruma açık ve objektiftir. Açık bilginin kodlanabilmesi, sistematik bir biçime ve biçimsel bir dile çevrilmesi kolaydır.

2.2.3. Stratejik Bilgi

Stratejik bilgi stratejik kararların alınmasında ve uygulanmasında kullanılan bir bilgi türüdür. Stratejik bilgi çoğunlukla işletme dışı kaynaklardan elde edilir. Rekabet üstünlüğünün tek ve güvenilir kaynağı olarak değerlendirilir (Karakaya, 2002).

2.2.4. Yöntemsel Bilgi

Yöntemsel bilgi bir şeyin nasıl yapılacağı ile ilgili bilgi türüdür. Bu bilgi türü kurumların misyonlarının, hedeflerinin ve temel ilkelerinin çalışanlar tarafından kolayca anlaşılmasına ve aktarılmasına olanak sağlar (Durna ve Demirel ,2008).

2.2.5. Örgütsel Bilgi

Açık ve örtülü bilgiden yararlanılarak örgütsel bilginin oluşumuna katkı sağlanır. İşletmelerin fiziksel oluşumunda örgütsel bilginin yeri çok önemlidir. Örgütsel bilginin sürecine bakacak olursak, bilginin üretimi ile başlar sonrasında bilginin benimsenmesi, bilginin dağılımı, bilginin gözden geçirilmesi ve son aşamada örgütsel bilgiye dönüşüm aşamaları seklinde olmaktadır (Bhatt,2000).

2.2.6. Öksüz Bilgi

Kurumlar sürekli değişen ve gelişmeye açık dinamik bir yapıya sahiptirler. Bu yüzden de yeni keşfedilen bilginin yanı sıra unutulan, kullanılmayan bilgiye de değer vermek gerekir. Öksüz bilgi organizasyonun içinde var olan bilgidir.

2.2.7. Bireysel Bilgi

Bireysel bilgi organizasyon içinde belli bir kişiye ait olan bilgidir. Bu bilgi kişinin zihnine yerleşmiş bilgilerinden ve tecrübelerinden oluşur. Bireysel bilgi kişiye özelleştirilmiş değerler bütünüdür (Ipe, 2003).

2.2.8. Kolektif Bilgi

Kolektif bilgi kişiye özel olmayan organizasyonlar içinde aktarılan ve paylaşılan bilgi olarak tanımlanmaktadır. Organizasyon içindeki bireysel bilgilerinin örgütsel bilgiye dönüştürülmesi ile ortaya çıkmaktadır.

2.3. Bilgi Yönetimi

Bilgi yönetimi birçok kaynakta farklı tanımlanmıştır. Yapılan bu tanımların bazılarına aşağıdaki tabloda yer verilmiştir.

Tablo 2.1: Bilgi Yönetimi Tanımları

Tanımlar
Bilgi yönetimi; en iyi kararın verilebilmesi için doğru kaynaktan doğru zamanda doğru bilginin toplanmasıdır.
Bilgi yönetimi; işletmelerin sahip oldukları beceri ve yetenekler ile tecrübeleri yoluyla elde ettikleri ortak akıl ve bilgileri tanımlamak ve sonrasında işlemektir.
Bilgi yönetimi; değer yaratmak için bilginin kullanılması, anlaşılması ve bulunması için sistematik yaklaşımların uygulanmasıdır.
Bilgi yönetimi; kurumların örgütsel performansını geliştirebilmek için bilginin yaratılması, bilginin ele geçirilmesi ve kullanılmasını içeren bir süreçtir.
Bilgi yönetimi; insan merkezli değerlerin yönetilebilmesi adına gerekli taktikler ve stratejiler ile ilişki eylemlerdir.
Bilgi yönetimi; stratejik bir motivasyonla çalışanların gelişimini kolaylaştırmak, bilgi ve verilerin yorumlanmasında çalışanların yeteneklerini kullanarak örgütsel hedeflerin başarılmasıdır.
Bilgi yönetimi; yöneticilerin örgütsel ve bireysel faydaları ortaya çıkarmak için bilgiyi elde etmesi, iletmesi ve kullanılmasını sağlamasıdır.
Bilgi yönetimi; günümüz dünyasında hızla artan belirsizlik ve karmaşıklık karşısında, firmaların yaşamını ve performansını artırma çabasıdır.
Bilgi yönetimi; örgüt arasında bilginin paylaşılması, yaygınlaştırılması ve kullanılmasını yöneten ve bilgiyi oluşturan ya da yerleştiren süreçlerdir.
Bilgi yönetimi; bilginin üretilmesini, düzenlenmesini, erişilmesini, yayılımını, derlenmesini, depolanmasını, yorumlanmasını ve kullanılmasını kapsamaktadır.

Genel olarak bilgi yönetimini, rekabet avantajı sağlayabilmek amacıyla bilgiyi oluşturarak, bilgiyi elde etme ve stratejik süreçlerde kullanmak şeklinde tanımlayabiliriz. Başka bir ifadeyle bilgi yönetimi; örgütlerin amaçlarına ulaşabilmesi için bilgiyi nasıl oluşturacakları, nasıl elde edip düzenleyerek kullanabilecekleri ve nasıl yönetilebileceklerini anlatan stratejik süreçler toplamı olarak tanımlanabilir (Özgener, 2002).

Wiig (1997) Bilgi yönetimini bilginin sistematik, açıkça ve kasıtlı olarak oluşturularak yenilenmesi ve bu şekilde uygulanması olarak tanımlamıştır.

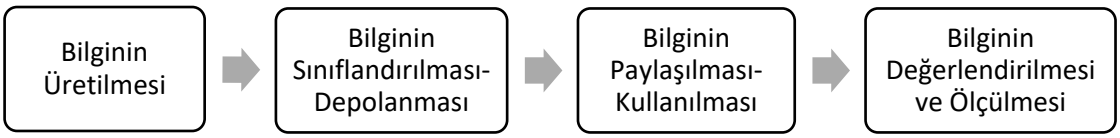
2.3.1. Bilgi Yönetimi Süreci

Bilgi, ortaya çıkmasından depolanmasına, ayırt edilmesinden değerlendirilmesine kadar pek çok süreçten geçer. Meydana gelen bu aşamalar bilgi yönetimi sürecini oluşturur.

Bilgi yönetimi süreci hakkında pek çok görüş bulunmaktadır Davenport ve Prusak (2001). Bilgi yönetim sürecini 4 aşamada değerlendirmiştir. Bunlar, bilginin oluşturulması, bilginin kodlanması, koordinasyon sağlanması ve son aşamada bilginin transfer edilmesini önermiştir (Güçlü ve Sotirofski, 2006). Bu yönetim sürecini Malhotra (2003) ise, 6 basamakta değerlendirmiştir. Bunlar, bilginin varlığından haberdar olmak, bilginin hedeflerini belirlemek, bilgiyi uygulamaya koymak, yaymak, iyileştirmek ve depolamaktır (Güçlü ve Sotirofski, 2006).

Temel olarak süreç bilginin üretilmesi (elde edilmesi), bilginin sınıflandırılması-depolanması, bilginin paylaşılması ve kullanılması son olarak da bilginin değerlendirilmesi ve ölçülmesi şeklinde tamamlanır.

Tüm bu aşamaların verimli ve etkili bir şekilde yönetilmesi örgütleri doğrudan etkileyecektir. Bilgi yönetimi sürecine Şekil 2.2'de yer verilmiştir.



Şekil 2.2: Bilgi Yönetimi Süreci

2.3.2. Bilgi Yönetiminin Önemi

Bilgi yönetimi örgütlerin bilgiden daha iyi yararlanmalarına, bilgiyi tanımlama süreçlerini oluşturmaya, bilgiyi depolamaya, araştırmaya ve bilginin transferini kolaylaştırmaya yardımcı olur. Bilgi yönetimi örgütlere değer katar ve rakiplerine karşı avantaj sağlar.

Bilgi yönetimi nerdeyse örgütteki herkesin katılımının olduğu bir süreçtir. Bu yüzden herkesin katkısını alarak oluşur.

Örgütlerin gelişen dünyaya ayak uydurabilmek ve ayakta kalabilmek için bilgiyi verimli kullanabilmeleri ve bilgi yönetimi süreçlerini çok iyi yönetmeleri gerekmektedir.

2.3.3. Bilgi Yönetiminin Amacı

Bilgi yönetiminin birçok amacı vardır. Bunlar; Bilgiyi korumak, bilginin ölçümünü sağlamak, bilginin büyüyüp yayılmasını sağlamak, örgütün farklı birimleri arasında iletişimi ve bilgi transferini sağlamak, bilginin doğru zamanda doğru kişilere ulaşmasını sağlamak, örgüt dışındaki bilgiyi anlamlandırabilmek, örgüt içerisinde yeni bilgi üretimini sağlayabilmek olarak sıralanabilir (Özgener, 2002).

2.3.4. Bilgi Yönetiminin İlkeleri

İşletmeler bilgi yönetimine ilişkin temel ilkelerini belirlemeli ve belirlediği ilkeler ışığında hareket etmelidir. Bu ilkeler şöyle sıralanabilir; (Barutçugil, 2002).

- Bilgi yönetimi uzun bir süreçtir. Bilgiye ulaşma sadece bir başlangıç olarak kabul edilir.
- Bilgi yönetimi devamlı yenilenen bir süreçtir asla bitmez.
- Bilgi yönetimi pahalıdır. Para ve emek yatırımına ihtiyaç duyar.
- İnsan ve teknolojinin ortak çözümleriyle etkili bir bilgi yönetimine ulaşılır.
- Bilgi yönetimi, bilgi çalışanları ve yöneticilerine ihtiyaç duyar.
- Bilgi yönetimi bilgi haritalarından ve bilgi piyasalarından faydalanır.
- Bilgiyi paylaşmak ve kullanmak genelde kendiliğinden ortaya çıkmaz.
- Bilgi yönetimi bilgi iş süreçlerinin iyileştirilmesine katkı sağlar.
- Bilgi yönetiminin başarılı olabilmesi için güven ve inanç gereklidir.

2.3.5. Bilgi Yönetimi Yararları

Etkili ve verimli bir bilgi yönetimi işletmelere birçok yarar sağlamaktadır. Bilgi yönetiminin yararları şöyle sıralanabilir; (Canbazoğlu, 2000);

- Bilgi kayıplarını önler: Tüm örgütün ulaşabileceği bir bellek oluşturarak bilgi kayıplarını önler ve korunmasını sağlar.
- Daha etkin kararlar alabilme imkânı ortaya çıkar: Bilginin tipini ve kalitesini belirleyerek bilgiye ulaşımı olanaklı kılar. Bunun sonucu olarak da kararlar daha kaliteli, verimli ve hızlı olarak işletme içine yayılır.
- Uyarlanabilirlik ve esneklik sağlar: İşletme içinde çalışanların daha az gözetim altında olmalarına, yenilikçi ve araştırmacı çözüm yollarına ulaşabilmelerine ve işlerine

odaklanmalarına olanak sağlar. Bu da işletme içinde bilginin daha geniş ağlara yayılımını sağlar.

- Rekabet avantajı sağlar: Günümüz rekabet ortamında işletmelerin ortama uyum sağlayarak bu rekabet ortamından avantajlı çıkmalarına olanak sağlar.
- İşletme varlığını geliştirmek: Bilgi sermayesine yasal korumanın eklenebilmesi için işletme yeteneklerini ve varlığını geliştirir. Doğrudan işletmenin Pazar payını ve değerini etkiler.
- Ürün iyileştirmesi sağlamak: İşletmenin ürün ve hizmetlerine bilgiyi eklemesine olanak sağlar. Bilginin kalitesine ve değerine bağlı olarak müşterinin algıladığı ürünün değeri de artar.
- Müşteri yönetimi sağlamak: İşletmelerin vereceği hizmetlere ve müşterilere odaklanmasını sağlar. Artan müşteri bilgileri sayesinde müşterilerin istek ve şikâyetlerine daha hızlı ve kolay çözüm bulunulabilir.
- İnsan sermayesine yatırımın değerini arttırmak: Bilgi yönetilmeye başlandıkça elde edilen bilgiler daha hızlı ve kolay paylaşılacak bununla birlikte iletilmesi kolaylaşacaktır. Bu doğrultuda çalışanların işe alım ve eğitim sürecinde yapılan yatırımların değerini artmış olacaktır.

2.4.Bilgi Güvenliği

Bilgi güvenliği bilgilerin saklanması ve korunması ve güvenli bir platform oluşturulması çabalarının tümü olarak ifade edilebilir. Bilgi güvenliği sağlayabilmek için çeşitli politikalar oluşturmak ve uygulayabilmek gerekir. Organizasyonlarda rekabet avantajı, karlılık, ticari itibar sağlayabilmek adına bilgi güvenliği oldukça önemlidir.

Bilgi güvenliğinden bilginin sahibi dahil bilgiyi kullanan ve bilgi sistemini yöneten herkes sorumludur.

Bilgi güvenliğini 3 temel unsur oluşturur. Bunlar gizlilik, bütünlük ve erişilebilirliktir.

a) Gizlilik

Bilginin yetkisi olmayan kişilerce erişiminin olmaması ve açığa çıkarılmasının engellenebilmesidir. Bilgiye sadece yetkisi olan kişiler erişebilir.

b) Bütünlük

Bilginin yetkisi olmayan kişilerce değiştirilmesi, silinmesi ya da herhangi bir zarar verilmesinin önüne geçilmesidir ve korunmasıdır. Bilgiyi sadece yetkisi olan kişiler değiştirebilir.

c) Erişilebilirlik

Bilginin yetkisi olan kişilerce ulaşılabilir ve ihtiyaç duyulduğu an ve yerde kullanıma hazır olmasıdır. Herhangi bir sorun ya da problem çıkması durumunda bilginin erişilebilir olması kullanılabilirlik özelliğinin bir gereğidir.

Güvenilirlik, inkâr edememe, kimliklendirme, kimlik sınaması, yetkilendirme, izlenebilirlik/kayıt tutma hesap verilebilirlik unsurları bilgi güvenliği yönetim sistemlerinin dikkat ettiği diğer destekleyici unsurlardır.

Şekil 2.3: Bilgi Güvenliği Unsurları

2.4.1. Bilgi Güvenliğinin Amacı

Bilgi güvenliğinin amacı bilgi sistemlerinin işleyişinin kesinti olmadan güvenilir ve kaliteli bir şekilde devamlılığını sağlamaktır. Böylece kurum varlıkları korunmuş ve yetkisi olmayan kişilerin erişimin kesilmesi sağlanmış olur.

Bilgi güvenliğinin sağlanması ile bilgi güvenliğinin alt yapısı kurulur ve sürdürülebilirlik gerçekleştirilmiş olur.

2.4.2. Bilgi Güvenliği Politikası

Bilgi güvenliği politikası kurumun hedeflerini ortaya koyabilen, yönetimi harekete geçirebilen ve hangi risklerin değerlendirileceği ile kapsamlarını ortaya koyan bir çerçeve sunmalıdır.

Bilgi güvenliği politikasına kurumda çalışanlar uyum sağlamalıdır. Bilgi güvenliği politikası doğrultusunda kurumun Bilgi Güvenliği Yönetim Sistemi oluşturularak bu doğrultuda dökümante edilme ve iyileştirme çalışmaları yapılır.

2.4.3. Bilgi Güvenliği Hedefleri

Bilgi Güvenliği hedeflerine aşağıda yer verilmiştir.

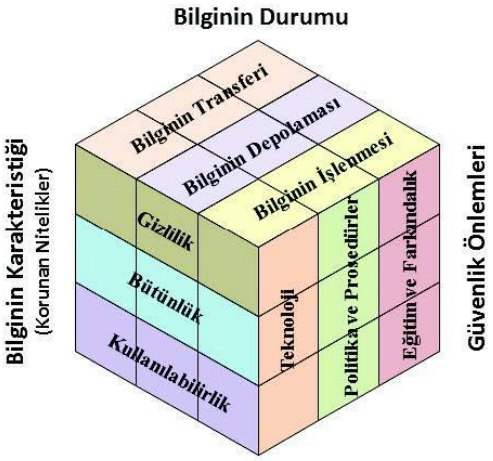
- Bilgi Güvenliği hedefleri bilgi güvenliği politikası ile uyumlu olmalıdır.
- Ölçülebilir olmalıdır.
- Risk değerlendirme ve risk işlemenin sonuçlarına önem vermelidir.
- Kuruluş içinde duyurulmalı ve uygun şekilde güncellenmelidir.

2.5.Bilgi Güvenliği Yönetim Sistemi

İletişimin kullanım alanlarının yaygınlaşması ve artmasıyla birlikte bilgi güvenliğinin sağlanması ihtiyacı da doğrudan artmaktadır. Güvenliğin sağlanması sadece teknik/bilişsel yöntemlerle olmamaktadır. Bu sebeple teknik yöntemler dışında kişileri, süreçleri ve teknik bilgi sistemlerini de içine alan bir yönetim ihtiyacı doğmuştur.

Bilgi Güvenliği Yönetim Sistemi, bilginin gizliliğini, bütünlüğünü ve kullanabilirliğini sağlamak üzere planlanmış, sistemli dökümante edilmiş, üst yönetim tarafından kabul edilmiş, uluslararası güvenlik standartlarının temel alındığı faaliyet bütünü olarak tanımlanmaktadır. (Ersoy, 2012)

Bilgi Güvenliği Yönetim Sisteminden ilk kez BSI (British Standards Institute) tarafından yayınlanan standartta bahsedilmiştir. Ülkemizde ise Türk Standartları Enstitüsü (TSE) tarafından kabul edilerek ve ISO/IEC 27001:2005 versiyonuyla yayınlanmıştır. BGYS işletmelerin önemli /gizli bilgilerini yönetebilmek için kurulan sistematik bir yaklaşım olarak kabule dilebilir. Bu sistemin temel amacı da hassas bilginin korunabilmesidir.



Şekil 2.4: Bilgi Güvenliği Modeli

Kaynak: (McCumber, 1991)

2.5.1. Bilgi Güvenliği Yönetim Sistemi Kapsamı

Bilgi Güvenliği Yönetim Sisteminin kurulum aşamaları 11 başlık altında toplanmıştır. Bunlar;

1.Güvenlik Politikası

Bilgi güvenliğini artıracak kurallar ile yönetimin bu konudaki tavsiyelerine yer verilir. Üst yönetim tarafından onaylanmış bir bilgi güvenliği politikası oluşturulmalıdır.

2. Organizasyonel Güvenlik

Bu bölümde kurum içi ve dışı bilgi güvenliği organize edilmelidir. Bu sayede kurum içindeki bilgi güvenliği yönetimi kolaylaşır. Yönetim kurum içinde uygulanacak güvenlik tedbirlerini ve politikalarını aktif olarak takip etmeli, hedefler belirlemeli ve sorumluların atanmalarını sağlamalıdır.

3. Varlık Sınıflandırma ve Denetim

Kurumda yer alan tüm bilgi varlıklarının envanteri tutulmalı ve etkili bir şekilde korunması sağlanmalıdır.

4. Personel Güvenliği

Kurumun bilgi güvenliği politikası doğrultusunda kurum personeline düşecek görev ve sorumluluklar belirlenmeli, yeni işe alınacak personelinde işe alınmadan önce politikayı

anlamış olduğundan emin olunmalıdır. Bu sayede hata, hırsızlık, dolandırıcılık gibi riskler en aza indirgenmiş olur.

5. Fiziksel ve Çevresel Güvenlik

Bilgi güvenliğini sağlamak amacıyla bir fiziksel sınır güvenliği koyulmalıdır. Örneğin kart kontrolü ile giriş, duvar, nizamiye vb. Kurum içerisinde sadece yetkili personelin girişine izin verilecek kontrol mekanizmaları oluşturulmalıdır.

6.İletişim ve Operasyonel Yönetim

Bilgi işleme donanımlarının yeterli ve güvenli olduğunun kontrolü sağlanmalıdır. Bilgi işlem sistemlerinde yapılan değişiklikler belirli aralıklarla denetlenmeli ve kayıt altına alınmalıdır. Yedekleme politikası uyarınca yedekleme ve yedekleme işlemlerinin testleri düzenli yapılmalıdır.

7.Erişim Kontrolü

Bilgiye erişimin ihtiyaçları göz önünde bulundurularak erişim denetimi politikası oluşturulmalıdır. Erişim denetimi politikaları bütün kullanıcılar için açıkça belirtilmelidir.

8.Sistemlerin Geliştirilmesi ve Sürekliliği

Güvenliğin bilgi sistemlerinin içine dahil edilerek yeni sistemlerin geliştirilmesine ve mevcut sistemlerin iyileştirilmesine olanak sağlar.

9.Olay Yönetimi

Güvenlik olaylarının mümkün olduğunca en hızlı şekilde raporlamak, kurum çalışanlarının sistemlerdeki güvenlik zafiyetlerini ve tehditlerini bildirebileceği bir prosedür oluşturulmalıdır. Güvenlik ihlallerinin ne şekilde ele alınacağına yönelik tavsiyeler vermelidir.

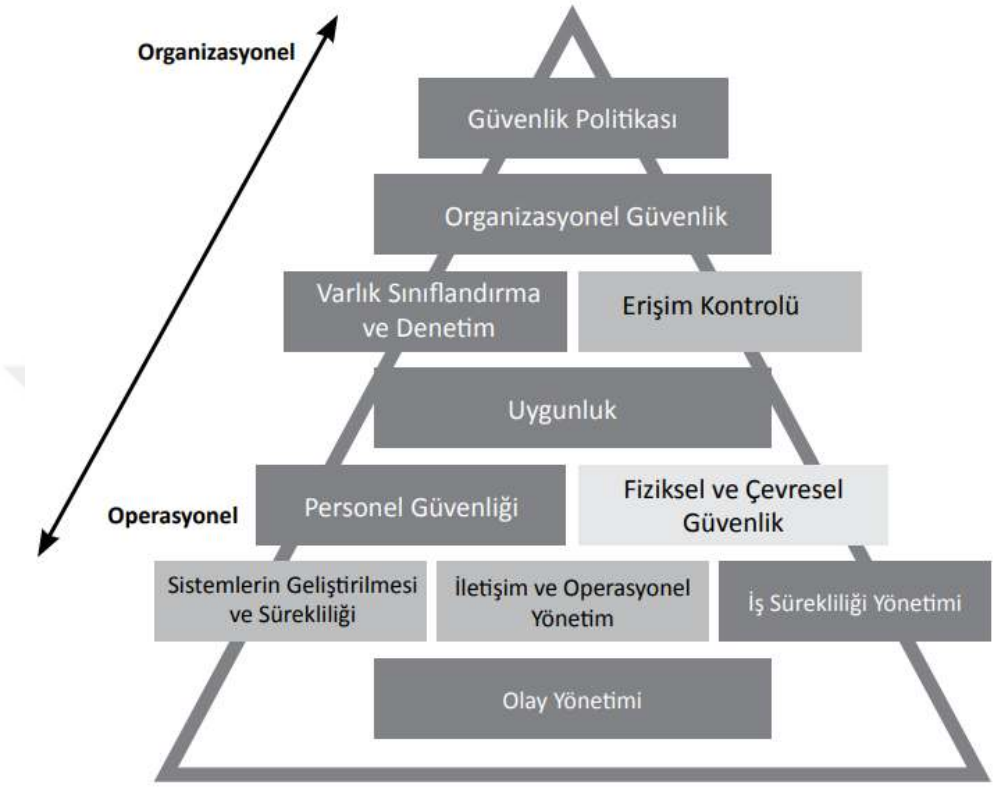
10.İş Sürekliliği Yönetimi

Kurumda bilgi güvenliği ihtiyaçlarına yer veren iş sürekliliği için süreçler oluşturulmalıdır. Kurumun esas işlemlerini arıza ve aksiliklerden korumaya yardımcı olur.

11.Uygunluk

Bilgi sistemlerindeki düzenleyici, yasal ve sözleşmeye bağlı gereksinimler ve yaklaşımlar açıkça belirtilmelidir. Bu gereksinimleri karşılamak amacıyla kontroller tanımlanmalıdır.

Aşağıdaki Şekil 2.5'te kurulum aşamalarına yer verilmiştir. Ana başlıkların her biri yönetimsel, teknik ve fiziksel ölçütler etrafında kurulmuş farklı konuları ele alır ve yukarıdan aşağıya doğru üretilir. Etkisi organizasyonel seviyeden operasyonel seviyeye doğru yorumlanır.



Şekil 2.5: BGYS Kontrolleri Şeması

Kaynak: (Marttin ve Pehlivan ,2010)

2.5.2. BGYS Süreçlerine Uygulanan PUKÖ Modeli

İşletmeler dökümante edilmiş bir BGYS'yi gerçekleştirmeli, iyileştirmeli ve takibini yapmalıdır. ISO 27001 standardının temelinde PUKÖ modeli (Planla-Uygula-Kontrol et-Önlem al) yer alır.

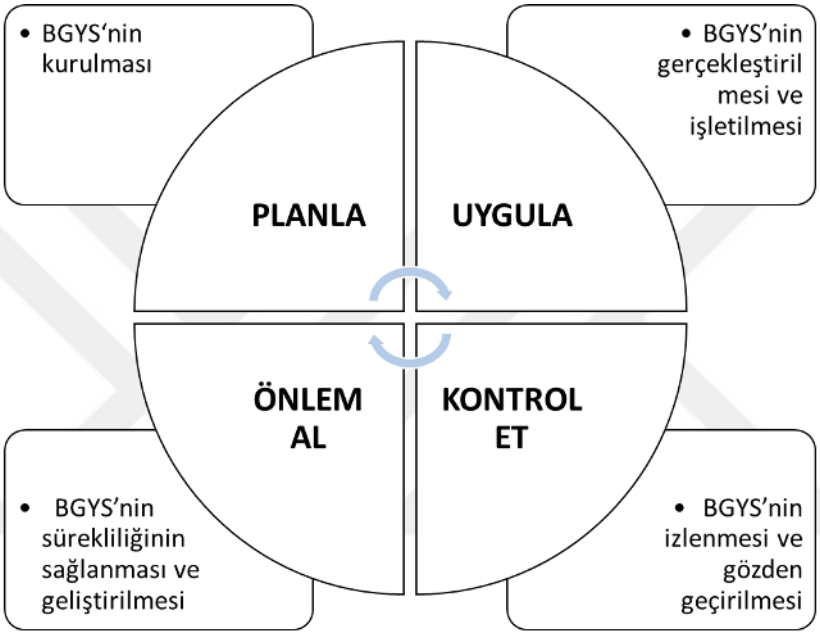
Planla: BGYS'de kullanılacak hedef, prosedür, süreç ve politikaların belirlenerek geliştirilmesi aşamasıdır.

Uygula: BGYS'nin tüm bu hedef, süreç, politika, prosedürleri uygulamasıyla birlikte gerçekleştirip işletilmesidir.

Kontrol et: BGYS ‘nin süreçleri, amaçları ve performansın gözden geçirilmesi, izlenmesi ve rapor edilmesidir.

Önlem al: Gözden geçirme sonuçları doğrultusunda düzenleyici ve önleyici aksiyonlar alınır.

BGYS sürekli devam eden bir gelişim süreci olarak nitelendirilebilir. Şekil 2.6’ da yer alan PUKÖ modelinde gösterildiği gibi sürekli durmaksızın devam eden bir döngüdür (Marttin ve Pehlivan, 2010).



Şekil 2.6: PUKÖ Modeli

2.5.3. Bilgi Güvenliği Yönetim Sisteminin Faydaları

BGYS’nin faydaları şöyle sıralanabilir;

- Dışarıdan gelen tehditlere karşı işletmeler korunmuş olacaktır. Yani bilgi varlıklarının gizliliği sağlanmış olur.
- Çalışanların daha bilinçli olması sağlanarak verimli ve uzun vadeli bir bilgi güvenliği sağlanmış olacaktır.
- Sistematik bir yaklaşım olduğu için işletmelerin değerini ve duyulan güveni artırır.
- Riskleri minimize ederek kontrol altında tutar.
- Gereksiz iş yükü ve israfı ortadan kaldırır asıl soruna odaklanılmasını sağlar.

2.5.4. ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı

Bilgi varlıklarının yönetilmesini ve korunmasını sağlayan bilgi güvenliği yönetim sistemi için gereksinimlerin belirlendiği uluslararası düzeyde bilgi güvenliği yönetim standardıdır. Bu standart bilgi güvenliği yönetiminin daha verimli olması için tasarlanmıştır.

Ülkemizde bu standartlar Türk Standartları Enstitüsü tarafından yayımlanır. TSE, ISO/IEC 27001:2005 adıyla bu standardın hazırlanış amacını açıklamıştır. ISO 27001 standardı bir bilgi güvenliği yönetim sisteminin kurularak, uygulanması, işletilmesi, izlenmesi, gözden geçirilmesi, sürdürülebilirliğin sağlanması ve iyileştirilmesi adına bir model oluşturmak için geliştirilmiştir (Ersoy, 2012).

Ayrıca Resmî Gazete 'de yayımlanan yönetmelikler doğrultusunda bilişim sektörü, elektronik haberleşme sektörü, altyapı, e-fatura yetkisi almak isteyen birçok sektör ve alana ISO 27001 belgesi alma zorunluluğu getirilmiştir.

ISO 27001:2005 sonrası 2013 ve 2022 yıllarında güncellenmiştir. 2013 ve 2022 versiyonları ile daha verimli ve anlaşılır bir hale gelmiştir.

2.5.5. ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardının Faydaları

ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardının faydaları şöyle sıralanabilir;

-Güvenlik politikaları oluşturularak bilgi yönetimi sağlanır.

-Bilgi varlıklarının farkındalığını ve korunurluğunu sağlar.

- Bilgi varlıklarının etkin şekilde korunması zaman, para ve itibar kaybını önler.

- Kuruma rekabet avantajı ve prestij sağlar.

- Güvenlik risklerini en aza indirger.

-Güvenlik politikaları sayesinde suiistimal ve tehditleri önler.

-Tehdit ve riskler yönetilerek iş sürekliliği sağlanır.

- Bilgi güvenliği farkındalığı oluşturulmasına katkı sağlar.

-Hukuki ve yasal düzenlemelere uyum sayesinde kurumu olası yaptırımlara karşı korumuş olur.

3. BÖLÜM: RİSK KAVRAMI

Risk kavramı, herkesin anlamını çok iyi bildiği bir kavramdır. Gerçek kişiler ve örgütsel yapılar farkında olmadan ya da içgüdüsel olarak kaçınmaya veya yönetmeye çalıştığımız olası olumsuz olaylardır. Gerçek kişiler ya da örgütsel yapılar kişiye veya yapıya zarar verebilecek olaylardan kaçınmak veya zararları aza indirme çabası içindedirler. Risk hayatımızın her alanında karşımıza çıkan bir kavramdır. Riskin birçok tanımı bulunmakta olup herkesin üzerinde mutabık kaldığı bir tanım bulunmamaktadır. Sağlık, spor, ekonomi, teknoloji ve yaşamın her alanında risk kelimesi farklı anlamlara gelmektedir. Tüm bu farklılıklara rağmen risk tanımının ortak noktası meydana gelen bir olayın veya faaliyetin sonucuna ilişkin belirsizlikler olup bu belirsizliğin bir zarar veya kayba sebebiyet vermesidir. Daha doğrusu zarar ve kayıp ölçülebiliyorsa risk ölçülemiyorsa belirsizliktir (Özbek, 2012).

IIA yayınladığı Uluslararası İç Denetim Standartlarının ayrılmaz bir parçası olan ve standartları doğru bir şekilde anlamak ve uygulamak için kullanılan Terimler Sözlüğünde risk; "Amaçlara ulaşılması üzerinde etkisi olacak bir olayın meydana gelme ihtimalidir. Risk; söz konusu etki ve olasılık cinsinden hesaplanır." şeklinde tanımlanmıştır (Uluslararası İç Denetim Standartları,2008).

COSO ise riski "bir olay meydana gelirken onu kötü etkileyen olasılıklar toplamı" olarak tanımlayarak riskin, bir olayın gerçekleşmesini ve amaçlara ulaşılmasını olumsuz etkileme olasılığından bahsetmiştir (COSO, 2013).

Risk iki temel bileşenden oluşur. Birincisi bileşen istenilen sonuca ulaşamama veya istenilmeyen sonuca ulaşma olasılığı ikincisi bileşen ise istenilen sonuca ulaşamama veya istenilmeyen sonuca ulaşmanın etkisidir (Fıkırkoca; 2003).

3.1. Risk Kavramları

Risk Tanımlama

Risk tanımlama, kurumun amaçlarına ulaşmasını etkileyebilecek her türlü olay olarak ifade edilebilir (COSO,2004). Risk tanımlamasını doğru yapabilmek için kurumun /işletmenin geçmiş yıllar performansları göz önünde bulundurulmalıdır. Risklere neden olayların iç faktörlerden mi dış faktörlerden mi kaynaklandığını iyi analiz edebilmek gerekir. Risklerin ana

kaynağının anlaşılması risklerin etkili ve verimli yönetimi için ilk adım sayılabilir. Kaynağı bilinemeyen bir riski yönetmek oldukça zor olacaktır (Sobel,2015).

Risk tanımlamak için gerekli verilen kurumun içinden veya daha önce belirlenen kurum amaçlarından elde edilir.

Risk Tutumu

Risk tutumu genel olarak üç risk faktöründen etkilenir. Bunlar risk iştahı, risk toleransı ve risk eşiğidir. Risk tutumu risklerin önceliklendirilebilmesi için önemlidir. Organizasyonların ve paydaşların risk tutumlarını bilmesi gerekir. Risk tutumunu belirleyen ana faktör kurumun risk alma istekliliği sınırıdır. Risk alma istekliliği de kurumun riski arayan ve çözüme kavuşturmak isteyen bir yapıda mı yoksa riskten kaçan bir görüşe mi sahip olduğu ile ilişkilendirilebilir (Hillson, ve Murray-Webster,2007).

Risk İştahı

Hazine ve Maliye Bakanlığın yayınlamış olduğu Kamu İç Denetim Rehberinde ise "Bir kurumun misyonu, vizyonu ve ulaşmaya çalıştığı stratejik hedefleri doğrultusunda herhangi bir zaman diliminde, herhangi bir önlem almanın gerekliliğine karar vermeden önce kabul etmeye hazır olduğu risk düzeyidir." Şeklinde tanımlanmıştır. (Kamu İç Denetim Rehberi, 2014) Tanımdan da anlaşılacağı üzere risk iştahı örgütsel yapının kabul etmeye istekli olduğu risk seviyesidir.

İşletmeler için ise risk iştahı, "İşletmenin hedeflerini gerçekleştirmeye çalışırken almaya niyetli olduğu risk seviyesini göstermektedir. Burada göz önünde bulundurulması gereken risk iştahı yükseldikçe olası zarar hem de olası getiri yükselmektedir." (Özbek, 2012).

Risk Toleransı

İşletmeler için risk toleransı, işletmenin katlanabileceği risklerin veya zararlı sonuçların alt ve üst sınırlarını ifade etmektedir. Yani işletmenin amacın gerçekleşmesine yönelik olarak kabul edilebilecek risk miktarını ifade eder (Özbek, 2012).

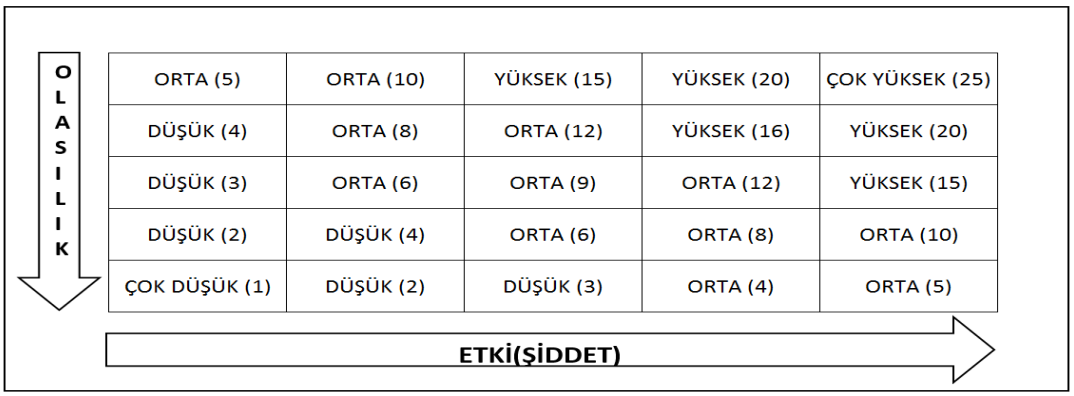
Risk Kütüğü

Örgütün risklerini, bu risklerin olasılık ve etkilerin düzeyleri, risk yetkilileri ve riskin kontrol faaliyetlerinin ve mevcut durum hakkında bilgilerin yer aldığı belge olarak tanımlanır (Derici ve diğerleri,2007).

Risk kütüğü içinde risk kategorisi, risk puanı, risk karşılama aksiyonları, aksiyon tanımı, aksiyon sorumlusu, risk sorumlusu, risk hakkında değerlendirme başlıklarını barındırabilir. Risk kütüğünün içeriği sabit ve değişmez yapıya sahip değildir. İhtiyaca göre geliştirilebilen dinamik bir yapıya sahiptir.

Risk Matrisi

Riskin gerçekleşme olasılığı ve gerçekleştikten sonra yaratacağı etki gibi iki değişkeni analiz etmek üzere kullanılan bir değerlendirme aracıdır. Risk değerlendirmesinde 5x5 (L tipi), 3x3, 10x10 gibi risk matrislerinden yararlanılır.



Şekil 3.1: L Tipi Risk Değerlendirme Matrisi

Olasılık puanı ile etki puanının çarpımıyla toplam risk puanı elde edilir. Toplam risk puanı risk derecesi olarak da adlandırılır.

Şekil 3.1.'de de görüldüğü üzere;

Risk derecesi 1 ise "Çok Düşük Risk" olarak değerlendirilir. Bu bölgede bulunan riskler için ek iyileştirme yapılmasına gerek yoktur.

Risk derecesi 2 ile 4 arasında ise "Düşük Risk" olarak değerlendirilir. Bu bölgedeki riskler kabullenilir ve takip edilmesi isteniliyorsa takip edilebilir.

Risk derecesi 5 ile 12 arasında ise "Orta Risk" olarak değerlendirilir. Bu bölgede olan ve ele alınması gereken risklere ilişkin öneriler risk yöneticisi tarafından oluşturulur ve risk yönetim komitesine sunulur. Yönetim komitesi ele alınması gereken risklere karar verir ve bu riskler için aksiyonlar belirlenir. Diğer riskler ise takip edilebilir.

Risk derecesi 13 ile 24 arasında ise "Yüksek Risk" olarak değerlendirilir. Bu bölgede bulunan tüm riskler ele alınarak aksiyonlar belirlenmelidir. Mutlaka iyileştirme yapılmalıdır. İyileştirme yapılırken geçici önlemler alınabilir.

Risk derecesi 25 ise "Çok Yüksek Risk" olarak değerlendirilir. Bu bölgede bulunan riskler için acilen önlem alınmalı ve denetim altında tutulmalıdır.

Risk Puanı/Skoru

Risk matrisinde bulunan olasılık değeri etki değeri ile çarpılarak her bir olayın risk puanı/skoru bulunur.

Risk Değerlendirmesi

Kurumun amaçlarının meydana gelmesini önleyen riskleri tespit ve analiz ederek alınabilecek önlemleri belirlemek ve uygulamaya koymak olarak tanımlanabilir. Riskler nitel veya nicel analizlerle değerlendirilir. Olayların ortaya çıkabilecek etkilerinin ve olasılıklarının veriye dayalı metotlar dışında yani sözel olarak açıklanması nitel analiz olarak adlandırılır. Olayların ortaya çıkabilecek etkilerinin ve olasılıklarının veriye dayalı yani matematiksel olarak açıklanması nicel analiz olarak adlandırılır.

Yapısal Risk (Doğal Risk)

Kurumlarda yer alan mevcutta yapılan kontroller ve tedbirler dışında kurumların mevcut yapısından veya yürütülen faaliyetin kendi doğasından kaynaklanan risktir (Kamu İç Denetim Rehberi, 2013).

Yapısal risk, herhangi bir sürecin doğasında bulunan ve bu riskin ortadan kaldırılması için herhangi bir kontrol faaliyetinin bulunmaması halinde söz konusu riskin meydana getirebileceği zararı ifade etmektedir (Özbek, 2012).

Artık Risk (Kalan Risk)

Terimler Sözlüğünde artık risk, "Yönetimin, olumsuz bir olayın etki ve ihtimalini azaltmak amacıyla, riski karşılamaya yönelik kontrol faaliyetleri de dahil, aldığı tedbirlerden sonra kalan risktir." şeklinde tanımlanmıştır (Uluslararası İç Denetim Standartları, 2008).

Örgütsel yapı tarafından alınması gereken tüm önlemler alınmasına rağmen söz konusu riskin gerçekleşmesi halinde oluşacak riske artık risk denir (Özbek, 2012).

Risk çok yönlü anlamı olan bir kavramdır. Algı ve tutumlar sonucu şekillenerek farklı durumlarda farklı sonuçlar ifade edebilmektedir (Fone ve Young, 2005).

3 unsur riski oluşturmaktadır. Bu unsurlar senaryo, olayın meydana gelme olasılığı ve olayın meydana geldiği zamandaki etkisi (Vose, 2008).

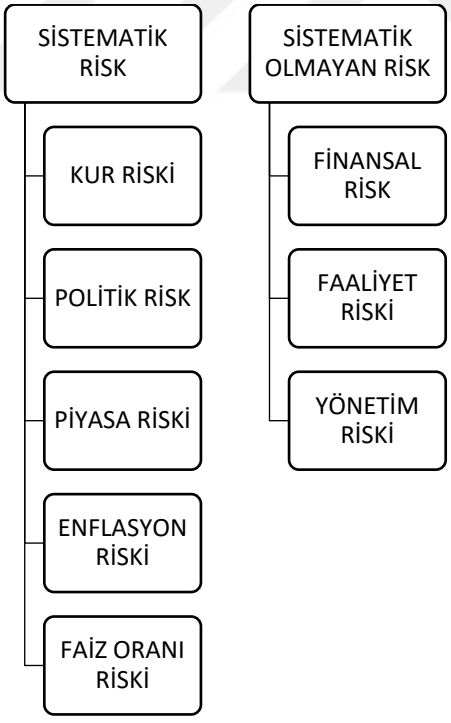
İşletmelerde bu riskleri en aza indirebilmek için çabalamaktadırlar. Bunun için de bir risk yönetimi politikası uygulamak zorundadırlar. İşletmelerde hedeflerine ulaşabilmek için bu riski yönetme ihtiyacı içindedirler.

3.2. Risk Türleri

Riskler farklı bakış açıları ile farklı gruplarda sınıflandırılmıştır. Bazı kaynaklar riskleri sistematik ve sistematik olmayan riskler olarak ayırırken bazıları finansal riskler, operasyonel riskler, stratejik riskler ve dış çevre riskleri olmak üzere dört ana başlık altında toplamıştır. Dört ana başlık altında yapılan bu sınıflandırma en çok tercih edilen sınıflandırma olmuştur (TUSİAD,2008).

Öncelikle sistematik ve sistematik olmayan risklere bakacak olursak;

Sistematik ve sistematik olmayan riskler birleşerek toplam riski oluşturur. Risk kaynaklarının sınıflandırması Şekil 3.2.'de gösterilmektedir.



Şekil 3.2: Risk Kaynaklarının Sınıflandırması

3.2.1. Sistematik Riskler

Çeşitlendirilemeyen ve piyasada işlem gören tüm ekonomik faaliyetlerin etkilendiği risktir. Sistematik risk ekonomide yer alan herkesi etkileyen politik, ekonomik ve doğal çevre

şartlarından meydana gelen risklerdir. Kişinin tek başına önleyemediği risk olarak da adlandırılır (Aksoy ve Tanrıöven,2007).

Sistematik riske çeşitlendirilemeyen risk de denir. Sistematik risk piyasa riski, politik risk enflasyon riski, faiz oranı ve kur riskinden oluşur. Sistematik riski oluşturan bu risklere aşağıda detaylı olarak yer verilmiştir.

a) Piyasa Riski

Genel olarak piyasalarda fiyat /değer değişikliklerinin, hisse senedi, emtia ve finansal araçların fiyatlarında meydana gelen değişikliklerin yarattığı risk olarak karşımıza çıkar. Bu risk pazar riski olarak da adlandırılır.

Başka bir deyişle, ekonomik sebeplerden dolayı hisse senetlerinin beklenen getirilerinin gerçekleşen getirilerinden az olması durumu olarak da ifade edilir (Sayılgan, 2003).

b) Politik Risk

Ülkelerde meydana gelen siyasi bunalımlar ve ekonomik krizler birer belirsizlik unsurlarıdır ve bu yüzden yatırım kararlarını etkilerler (Usta,2005). Yatırımcıların ülkenin geleceği hakkında beklentilerinin iyi ya da kötü olması piyasa riskini etkiler.

c) Enflasyon Riski

Enflasyon riski fiyatların yükselmesiyle ortaya çıkan ve satın alma gücünü azaltarak ortaya çıkan risktir. Bu riskin diğer bir adı da satın alma gücü riskidir.

d) Faiz Oranı Riski

Piyasa faiz oranında meydana gelen değişimlerle meydana gelen sabit gelirli menkul kıymetlerin fiyatındaki dalgalanmalar olarak tanımlanabilir (Taner ve Akkaya,2009).

e) Kur Riski

Döviz kurlarında meydana gelen beklenmeyen değişikliklerin ulusal para cinsini etkilemesidir (Holland,1993). Daha çok bu riskten uluslararası işlem yapan şirketler etkilenir.

3.2.2. Sistematik Olmayan Riskler

Çeşitlendirilebilen ve belli bir sektöre veya kişilere ait risklerdir. Sistematik olmayan riskler daha çok şirketlerin kendi içinden kaynaklanan risklerdir. Sistematik olmayan riskler çeşitlendirilemeyen riskler olarak da adlandırılır. Bunun nedeni kişinin farklı yatırım araçlarına yönelmesiyle yani portföyünü çeşitlendirerek bu riski azaltma olasılığının olmasıdır (Büberkökü,2018).

Sistematik olmayan riskler tek bir firmaya veya şirkete özgü risklerdir ve bir tek onları etkilerler. Finansal risk, faaliyet riski ve yönetim riski sistematik olmayan riski oluşturur.

Sistematik olmayan riski oluşturan bu risklere aşağıda detaylı olarak yer verilmiştir.

a) Finansal Risk

İşletmenin finansal sorumluluklarını yerine getirememesi riskidir. İşletmenin gelirlerinin azalmasıyla borçlarını ödeyememesi, çevresel koşullara ayak uyduramamasıyla ortaya çıkar.

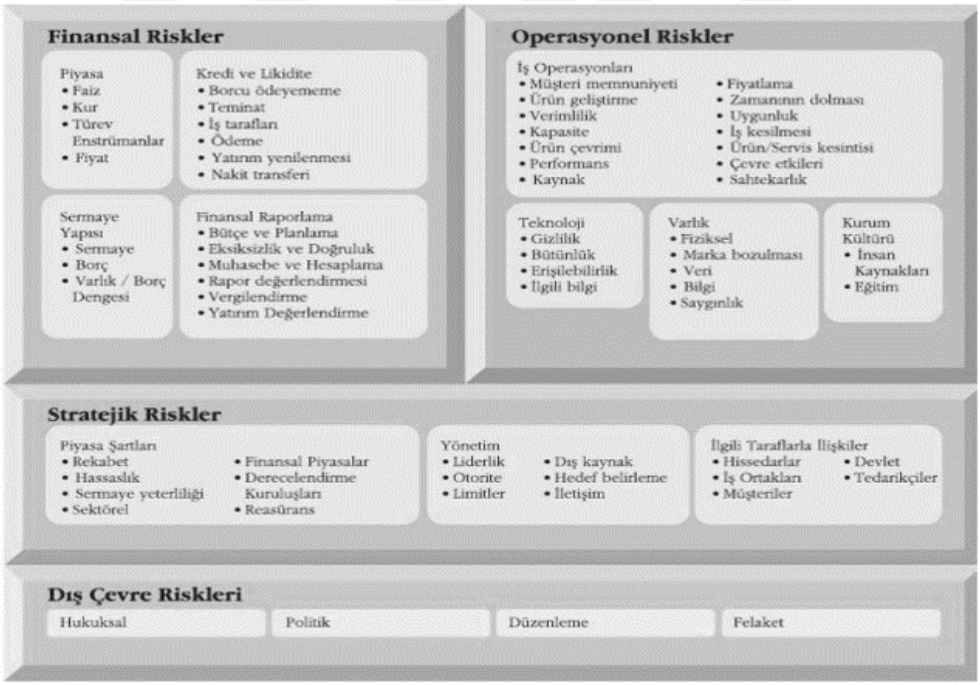
b) Faaliyet Riski

İşletmelerin iş ve endüstri kolundaki fiyat değişikliklerinden kaynaklanan risklerdir. İş ve endüstri riski olarak da adlandırılır.

c) Yönetim Riski

İşletmelerin yönetim kararları, yönetim anlayışı ve uygulanma gücüne bağlı olarak değişebilen risklerdir.

TUSİAD tarafından yapılan ve riskleri dört grupta değerlendiren risk sınıflandırmasına Şekil 3.3.'de yer verilmiştir.



Şekil 3.3: Risk Türleri

Kaynak: (TUSİAD,2008)

Finansal Riskler

Bu riskler örgütsel yapıların mali yapısı ile ilgili yani finansal duruşu ve tercihleri sonucunda oluşan risklerdir. Finansal riskler içerisinde;

- Piyasa
- Kredi ve likidite
- Sermaye yapısı
- Finansal raporlama riskleri yer almaktadır.

Operasyonel Riskler

Örgütsel yapının temel faaliyetlerini yerine getirmesini engelleyen risklerdir. Bir başka deyişle çalışanların ve yöneticilerin günlük iş akışları esnasında karşılaşabilecekleri risklerdir. Operasyonel riskler içerisinde;

- İş operasyonları
- Teknoloji
- Varlık
- Kurum kültürü başlıkları yer almaktadır.

Operasyonel riskler kendi içerisinde rekabet, sözleşme ve fiziksel risk olarak bölümlendirilebilir (Grıffıths,2005).

Rekabet Riski

Rakiplere karşı rekabet üstünlüğü sağlamak amacıyla yapılan işlerde başarısızlığa uğrama ihtimalinin bulunması riskidir.

Sözleşme Riski

Karşı tarafa malları veya hizmetleri zamanında, istenilen maliyette ya da özellikte teslim edememe sonucu ortaya çıkabilecek risktir.

Fiziksel Risk

Kaza, yangın veya güvenlik sebebiyle ortaya çıkabilecek risklerdir. Meydana gelecek zararları, tedbirlerdeki eksiklikleri ve fiziksel riskleri barındırır.

Stratejik Riskler

Örgütsel yapının ileriye yönelik olarak belirlemiş olduğu amaç ve hedeflerine ulaşmasını engelleyebilecek iç ve dış belirsizliklerin oluşturduğu risklerdir. Stratejik risklerin içinde;

- Piyasa şartları
- Yönetim
- İlgili taraflarla ilişkiler başlıklarına yer verilmiştir.

Stratejik riskler aşağıdaki gibi bölümlendirilebilir (Grıffıths,2005).

Politik Risk

Hükümet politikalarının gereğini yapma zorunluluğu ya da uygulamanın başarısızlıkla sonuçlanması riskidir.

Ekonomik Risk

Enflasyon, faiz oranı gibi ekonomik göstergeler üzerinde ortaya çıkan değişimler sonucu başarısızlığa uğrama ihtimalinin olması riskidir.

Sosyal Risk

Sosyal, demografik değişimlerin etkilerine yanıt verebilmede başarısızlığa uğrama ihtimalinin olması riskidir.

Müşteri Riski

Müşterilerin istek ve ihtiyaçlarını karşılamada başarısız olma ihtimali olarak tanımlanabilir.

Dış Çevre Riskleri

Örgütsel yapının faaliyetlerinden bağımsız olarak ortaya çıkan ancak örgütsel yapıyı etkileyen risklerdir. Örgütsel yapının kontrol edemediği risklerdir. Dış çevre riskleri içerisinde;

- Hukuksal
- Politik
- Düzenleme
- Felaket başlıkları yer almaktadır.

3.3.Risk Yönetimi

Risk Yönetimi örgütsel yapıların amaçlarına ulaşmak üzere makul bir güvence sağlamak amacıyla potansiyel durumları ve olayları belirleme, değerlendirme, yönetme ve kontrol süreci olarak tanımlanmaktadır (Özbek, 2012).

Uluslararası İç Denetim Standartlarının ayrılmaz bir parçası olan Terimler Sözlüğünde Risk Yönetimi "Kurumun amaçlarını gerçekleştirmek üzere makul bir güvence sağlamak amacıyla potansiyel olay ve durumları belirlemek, değerlendirmek, yönetmek ve kontrol etme sürecidir." Şeklinde tanımlanmıştır (IIA Uluslararası İç Denetim Standartları,2008).

Son yıllarda işletmelerde risk yönetiminin yeri konusunda çok kapsamlı değişiklikler gözlemlenmiştir. Ayrıca işletmeler için risk yönetimi çok önemli bir hal almıştır. Günümüzün başarılı işletmeleri belirsiz ortamlardan kaçmak için riskleri tehdit yerine fırsat olarak algılamışlardır. Buna göre de geleneksel yöntemlerle uygulanan risk yönetimi var olan koşullarda yetersiz kaldığı görülmektedir. İşletmeler operasyonel ve stratejik riskler gibi farklı risk türlerine önem vererek bu riskleri yönetmeye çalışmaktadırlar. Bir işletme var olan risklerini yönetmek için 2 farklı yol izleyebilir. Birinci yol var olan risklerini teker teker ele alıp yönetmek; ikinci yol ise bütün riskleri sistemin bir parçası olduğunu görerek, bu riskleri risk yönetimi ilkeleri çerçevesinde yönetmektir. İkinci yola genel olarak "Kurumsal Risk Yönetimi" adı verilir. İşletmeler etkin bir risk yönetimi sürecine, yapısına ve uygulamalarına sahip olurlarsa risk yönetiminden istedikleri faydaları elde etmeleri daha kolay olacaktır (Akçakanat,2012).

Globalleşmeye bağlı olarak ulusal ve uluslararası düzeyde gelişen yeni teknolojilerin ortaya çıkması ile birlikte riskler farklılaşmış, artmış ve risklerin yönetimi zorunlu hale gelmiştir. Piyasalar birbirlerini çok fazla etkilediği için bir piyasadan diğer piyasaya riskin geçişi de kolaylaşmıştır. Özellikle finans sektörünün gelişiminin artmasıyla birlikte bu sektörde yaşanan riskler ve krizlerde artmıştır. Şirketlerin durumlarının kötüye gitmesi daha modern bir risk yönetim çıkmasını zorunlu hale getirmiştir (Koç ve Çelik,2015).

Risk yönetiminin önemi kurumlar tarafından kabul edilen bir gerçektir. Aslında tüm finansal ve finansal olmayan şirketler için kâr marjlarının çok düştüğü bir ortamda kar sürekliliği sağlamanın tek yolunun risklerin belirlenip bu risklerin yönetilmesinden geçtiği ifade edilmektedir (Koç ve Çelik,2015).

Birçok görüşe göre disiplinli ve verimli bir şekilde uygulanmaya çalışılan kurumsal risk yönetim sistemi, kurumların başarısızlığını önleyip önemli risklere önem verilmesini sağlamakta ve daha da önemlisi kurumu rekabet açısından öne geçirdiği düşünülmektedir. Ayrıca kurumlar üzerinde pozitif bir imaj oluşturarak ve yaşamını sürdürme yeteneğini artırarak kurumlara katkı sağlamakta, bunun yanında ürünlerin toplam kalitesini ve üretilen hizmetleri ve pozitif yönde etkilemektedir (Aksoy, 2005: Kızılboğa,2012).

COSO' ya göre kurumsal risk yönetim anlayışında kâr amacı güden bir şirket de olsa kâr amacı gütmeyen bir şirket te olsa bir kurumun temel amacı paydaşlarına değer katmaktır. Risk yönetim süreci yalnızca kuruma değer katmak ve bu değeri korumak üzerine kurulmamıştır hatta bu değeri geliştirip ilerletmesi de gereklidir.

Aslında çoğu risk yönetimi yönteminde, risklerin tamamen yok edilmesi ve kurumun risksiz bir sürece sahip olması mümkün değildir. Ama kurumsal risk yönetimi ile sürekli değişen piyasalarda meydana gelen riskleri daha doğru ve etkin bir şekilde yönetme şansı oluşturulması mümkündür (Koç ve Çelik,2015).

Günümüzde yaşanan yoğun rekabet ortamında işletmeler karşı karşıya kaldıkları riskleri yönetebilmelerini başarı olarak nitelendirirler. Bu süreci başarıyla tamamlayan işletmeler, yönetim ve finans yapılarındaki gereken düzenlemeleri yaparak, oluşabilecek yeni şartlara ve olaylara göre hareket etmektedirler. Bu sürecin en önemli yapıtaşı olan risk yönetimi, işletmelerin bu riskleri yönetirken daha dikkatli davranmalarına ve gereksiz kayıpların önüne geçmelerini sağlayacaktır (Özer,2012).

3.3.1. Risk Yönetiminin Amacı

Risk yönetiminin ana amacı ileride kuruma/şirkete zararlı olabilecek olasılıkları ve olasılıkların meydana gelmesi durumunda ortaya çıkabilecek olumlu olmayan sonuçları en aza indirgeyebilmek, süreci kontrol ederek asıl hedefe ulaşılması için süreçleri en iyi şekilde koordine etmektir.

Risk yönetimine ihtiyaç duyulma nedeni bir nevi risk yönetiminin amacını yansıtmaktadır. Operasyonlarda süreklilik sağlamak, kayıpların yol açtığı maliyetleri yönetilebilir seviyede tutmak, faaliyetlerde istikrarı sağlanmak, sürdürülebilirliği sağlamak, ulusal ve uluslararası yasal düzenlemelere uyumu sağlamak da risk yönetiminin amaçları arasında sayılabilir (Pehlivanlı,2010).

Etkili ve verimli bir şekilde uygulanan risk yönetimi kurumun daha çok önem verdiği risklere yoğunlaşılmasını kolaylaştırır ve bu sayede kuruma rekabet avantajı sağlamaktadır (Beasley ve diğerleri, 2009). Kurumun piyasadaki yerini koruyarak uzun süreli yaşam sürmesiyle birlikte pozitif imaj oluşturmasını sağlar. Bu da kurumu her yönüyle olumlu olarak etkiler.

Risk yönetiminin kuruma sağlayacağı faydalar şöyle sıralanabilir (IIA,2009);

1. Yönetimin riskleri anlayarak, tanımlaması ve önlem almasına katkı sağlar.
2. Risklere önem sırasına göre odaklanan bir anlayış belirlenir.
3. Olumsuz durumlarla karşılaşılabilme olasılığını minimuma indirir.
4. Hedeflere daha çabuk ve kolay ulaşılmasını sağlar.
5. Başarıya ulaşabilmek amacıyla değişikliklerde insiyatif alma sorumluluğunu arttırır.
6. Kurum içi verimliliği artırır ve kurumsal imajı güçlendirir.
7. Kurum içi risklerin belirlenmesini ve paylaşılmasını sağlar.

3.3.2. Risk Yönetimi Gelişim Süreci

Risk başlarda tehlike olarak algılanırken zamanla belirsizliğe dönüşmüştür. Son zamanlarda ise fırsat olarak görülmektedir. Risk yönetimi uygulamaları öncelikle bankacılık, sigortacılık ve finans sektöründe görülmeye başlanmıştır. Piyasalarda dalgalanmalar ve değişiklikler, teknolojik gelişmeler, işlem hacimlerindeki büyümeler vb. durumlar risk yönetiminin önemini arttırmıştır.

Risk yönetimi ilk önce işlem odaklı olan geleneksel yöntemlerle yapılmış. Daha sonra bütünsel olarak bakılarak ileri düzey yöntemlere geçilmiş. Hâlihazırda strateji odaklı olan kurumsal yöntemlere geçilmiştir.

Şekil 3.4: Geleneksel Risk Yönetiminden Kurumsal Risk Yönetimine Geçiş

İlk zamanlarda uygulanan ve geleneksel risk yönetimi adını alan kavramda riskin olumsuz etkilerinden kurtulmaya odaklanılırdı. Klasik mali yönetim anlayışı olarak da bilinen bu sistemde, riskler kötü algılanarak kurum, mal ve finans varlıklarını risklerden korumaya odaklanmakta ve riskleri sözleşme ya da sigortalama yoluyla transfer etmenin yolları araştırılmaktadır (Arthur,2009).

Hatalar ortadan çıkmadan önlem almak ve sonrası sürecini de iyi şekilde yönetebilmek için bir sisteme ihtiyaç hasıl olmuştur. Bu ihtiyacı karşılamak üzere kurumsal risk yönetimi kavramı ortaya çıkmıştır. Kurumsal risk yönetimi ile kuruma/işletmeye değer katmak, risk yönetimini bir kurum stratejisi haline getirmek ve risklerin etkin bir şekilde yönetilmesini sağlamak amaçlanmıştır.

Geleneksel risk yönetimi ile kurumsal risk yönetimi arasındaki temel farklar Tablo 3.1.'de gösterilmiştir.

Tablo 3.1: Geleneksel Risk Yönetimi ile Kurumsal Risk Yönetimi Arasındaki Temel Farklar

GELENEKSEL RİSK YÖNETİMİ	**KURUMSAL RİSK YÖNETİMİ**
Riskler ayrı ayrı birbirinden bağımsız ve diğer faktörlerle birleştirilmeden değerlendirilir.	Riskler kurum stratejileri kapsamında değerlendirilir.
Risk tanımlaması ve değerlendirilmesi söz konusudur.	Risk portföy gelişimi söz konusudur.
Risklerde önem sıralaması yapılmamaktadır.	Riskler önem derecesine göre dikkate alınır.
Risk azaltma uygulaması uygulanır.	Risk optimizasyon uygulaması uygulanır.
Risk limitleri bulunur.	Risk stratejileri vardır.
Risk sahiplenicileri yoktur.	Risk sorumluları vardır.
Rasgele risk ölçümü yapılır.	Risklere öncelik sıralamasına göre izlenme ve ölçüm yapılır.

Yapılanmamış ve tutarsız risk yönetim fonksiyonları vardır.	Risklerin yönetimi kurum genelinde organize edilir ve yürütülür.
"Risk benim sorumluluğum değil" algısı hakimdir.	"Risk herkesin sorumluluğudur " algısı hakimdir.

Kaynak: (Hall,2007)

3.3.3. Risk Yönetimi Süreci

Risk yönetimi temel olarak 4 aşamadan oluşur. Şekil 3.5'te risk yönetim sürecine yer verilmiştir.

1. Risklerin tespit edilmesi
2. Risklerin nitelendirilmesi ve değerlendirilmesi
3. Risklerin yönetimi ve kontrolü
4. Risk gelişiminin gözden geçirilmesi ve raporlanması (Vaughan ve Vaughan, 2001).

Şekil 3.5: Risk Yönetim Süreci

3.3.3.1.Risklerin Tespit Edilmesi

Bu aşamada işletmelerin maruz kaldığı veya kalabileceği risklerin özellikleri tanımlanır. İşletmelerin amaçlarına ulaşmasına engel olan veya güçleştiren riskler belirlenerek incelenir. Risklerin doğru ve tam olarak belirlenmesi risklerin kaynağına ulaşmada ve ortadan kaldırılmasında etkin rol oynayacaktır.

Risklerin tespit edilmesi aşamasında amaç risklerin probleme dönüşmeden ilk aşamalarda belirlenerek kökten çözüm sağlaması, riskleri azaltma ve karar faaliyetlerine fırsat

vermektir. Riskler artık probleme dönüştüğünde bu riskleri çözümlemekte zorlaşacaktır (Kamu İç Denetim Rehberi,2014).

Tespit edilen risklerin amaç ve hedeflerle ilişkilendirilmesi gereklidir. Bazı riskler doğrudan bazı riskler ise dolaylı olarak amaç ve hedefleri etkileyebilir.

Riskleri belirlerken öncelikle stratejik seviyede mi faaliyet seviyesinde mi dikkate alınmalıdır. Stratejik düzey yani idare düzeyi idarenin üst sorumluluğunda olan alandır. Faaliyet düzeyi ise sadece alt birimleri ilgilendiren ve sadece birim hedeflerini gerçekleştirmeye yöneliktir (Kamu İç Denetim Rehberi,2014).

Ayrıca farklı uzmanlık alanındaki kişilerin bakış açısı yeni risklerin tespit edilme olasılığını artıracaktır.

Riskleri tespit etmek için PESTLE Analizi, GZFT/SWOT Analizi ve Beyin Fırtınası gibi yöntemler kullanılabilir.

3.3.3.2.Risklerin Değerlendirilmesi

İşletmelerin amaçlarına ulaşması yolundaki risklerin etki ve olasılık açısından değerlendirilmesi gereklidir. Her işletme iç veya dış risklere maruz kalacaktır. İşletmelerin bu risklere hazırlıksız yakalanmaması ve risk değerlendirmesi yapabilmesi gereklidir (Kamu İç Denetim Rehberi,2014).

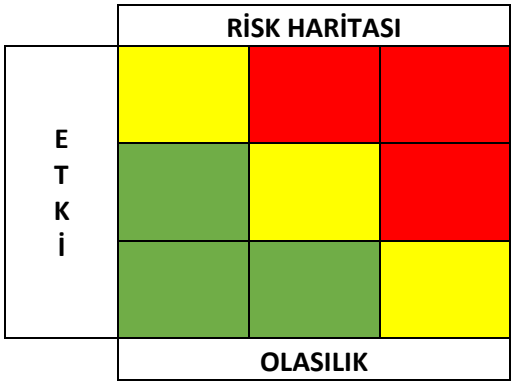
Risklerin değerlendirilmesi süreci risklerin ölçülmesi, önceliklendirilmesi ve kaydedilmesi aşamalarından oluşur.

Riskler ölçülürken her risk için etki ve olasılık tespit edilir ayrıca riskler esas alınırken doğal ve kalıntı risk olarak değerlendirilir. Doğal risk, riskler tespit edildiğinde cevap vermeden önceki seviyesi olarak, kalıntı risk ise, idarenin riskin olma olasılığını ve ortaya çıkan etkiyi azaltmak için aldığı önlemler sonrasında arta kalan risk olarak tanımlanabilir.

Risklerin önceliklendirilmesi aşamasında riskler önem sırasına göre sıralanır bu da kaynak tahsisinde etkinliği sağlar. Önceliklendirme yapıldıktan sonra risklere verilecek cevaplara karar verilir.

Risklerin kaydedilmesi aşamasıyla verilen kararlara kayıt oluşturması ve süreç içindeki kişilerin sorumluluklarını görmelerine ve izlemelerine olanak sağlanır.

Riskler değerlendirilirken risk seviyesini daha rahat görebilmek için risk haritaları kullanılabilir. Düşük risk seviyesi yeşil ile orta risk seviyesi sarı ile yüksek risk seviyesi kırmızı ile gösterilir.



Şekil 3.6: Risk Haritası

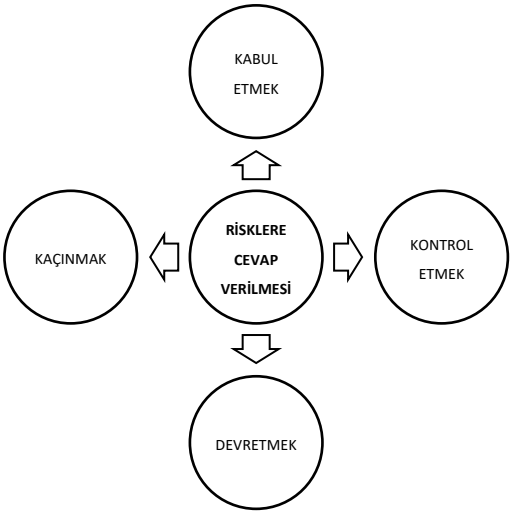
Risk puanı belirlendikten sonra riskler önem sırasına göre sıralanır. Bu da kaynak tahsisinde etkinliği sağlar. Risklerin önem sırası belirlendikten sonra risklere verilecek cevaplara karar verilir. Riskler bu cevaplara kanıt oluşturmak ve risk yönetimi içindeki kişilerin sorumluluklarını izleyebilmesi için kaydedilir (Kamu İç Denetim Rehberi,2014).

3.3.3.3.Risklere Cevap Verilmesi

Bu aşamada tespit edilen ve risk iştahı içinde yer alan risklere verilecek cevapların belirlenmesi ile birlikte beklenen tehditlerin azaltılması ve fırsat değerlendirmesi de yapılır. Risklerin daha iyi anlaşılabilmesi için analizler yapılır.

Risklere verilecek cevapta amaç, ortaya çıkacak etkiyi azaltmak ve öngörülen hedefe en etkin bir şekilde ulaşmaktır.

Riske cevap verme yöntemleri risk karşılama aksiyonları olarak da adlandırılır. Bunlar; kabul etmek, kontrol etmek, devretmek ve kaçınmak olarak sıralanabilir. Genellikle idareler tarafından riskleri kabul etmek ve kontrol etmek yöntemleri tercih edilir.



Şekil 3.7: Risklere Cevap Verme Yöntemleri

Kabul Etmek

Alınacak önlemlerin maliyeti alınacak önlemlerden sağlanan faydadan daha yüksek olduğu tahmin ediliyorsa riski kabul etmek mantıklı bir seçenek olacaktır.

Kontrol Etmek

Kontrol etmek yönteminde, riski kabul edilebilir bir seviyede tutmak için yönlendirici, önleyici, tespit edici ve düzeltici kontroller uygulanabilir.

Yönlendirici Kontrol

Bilgilendirme, koruma, davranış şekli belirlemek gibi dolaylı olarak riskleri kontrol etme yöntemidir.

Önleyici Kontrol

Risklerin gerçekleşme olasılığını azaltarak kabul edilebilir seviyede tutmak için yapılan kontrollerdir.

Tespit Edici Kontrol

Risklerin gerçekleşmesiyle meydana gelen zarar ve hasarı tespit etmek amacıyla yapılan yöntemdir.

Düzeltici Kontrol

Riskler gerçekleştikten sonra istenmeyen sonuçların etkisinin giderilmesinde uygulanan yöntemdir.

Devretmek

Devretme yönteminde işletmenin doğrudan görev alanına girmeyerek, fayda-maliyet analizi açısından değerlendirildiğinde riski çok bulunarak yapılması uygun görülmeyen faaliyetler başka bir kurum/idare/kuruluşa devredilir.

Kaçınmak

Kaçınma yönteminde, risk yönetilemeyecek kadar büyükse veya faaliyet hayati öneme sahip değilse risklere neden olan faaliyetler sonlandırılabilir ya da strateji tamamen terk edilebilir.

Riskler yönetilmeye çalışırken riskler ortaya bazı fırsatlar da çıkarabilir. Riskler her zaman olumsuz etkiler ortaya çıkarmaz. Fırsatları değerlendirmek risklere verilebilecek cevaplardan biri değil onlarla birlikte kullanılabilecek bir yöntemdir.

Risklerin yönetimi için riske en uygun aksiyonun belirlenmesi kurumlar için oldukça önemlidir. Bu süreçte risk sorumluları aksiyonların belirlenmesinden ve uygulanmasından sorumludur. Aksiyonlar belirlenme sürecinde Aksiyon Belirleme Rehberi'nden faydalanılabilir.

Aksiyonlar belirlenirken öncelikle risk puanı göz önünde bulundurulmalıdır. Risk puanı yüksek risklere öncelik verilmesi gereklidir. Fayda maliyet analizi mutlaka yapılmalıdır.

3.3.3.4.Risklerin Gözden Geçirilmesi ve Raporlanması

Çeşitli koşulların değişimiyle veya alınan önlemler doğrultusunda riskler etki ve olasılık yönünden değişkenlik gösterir. Bu değişkenlik ile beraber yeni risk alanları da oluşabilir. Bu sebeple tespit edilen risklerin ve yönetim sürecinin belirli aralıklarla kontrolü yapılmalıdır. Gözden geçirmelerin en az yılda bir kez yapılması önerilir. Ancak bu gözden geçirme süresi riskin derecesi doğrultusunda idare tarafından da belirlenebilir.

Riskin ve risk yönetimi sürecinin gözden geçirilmesi birbirinden ayrı olarak değerlendirilen süreçlerdir. Riskler riskin sahibi tarafından gözden geçirilirken risk yönetimi süreci üst yönetim tarafından gözden geçirilmelidir. Gözden geçirmede öncelik riskin

derecesine göre veya idare tarafından önceliklendirilmiş risklere verilmelidir. Ancak esas olarak bütün risklerin gözden geçirilmesi gerekmektedir.

Riskler gözden geçirilirken bir değişikliğe rastlanılırsa mutlaka bir üst seviyedeki kişiye bildirilmelidir. Önemli seviyede görülen bir risk ile ilgili değerlendirme ve gözden geçirme sonuçları üst yöneticiye raporlanmalıdır.

3.4.Kurumsal Risk Yönetimi

Stratejilerin oluşturulmasıyla başlayan, tüm kurumu etkileyebilecek olayların belirlenmesiyle devam eden ve risklerin kurumun hedeflerine ulaşmasına yönelik olarak yönetilmesiyle son bulan herkesin sorumluluğunun olduğu bir süreç olarak tanımlanır (COSO, 2004).

Riskler kurum stratejileri kapsamında ve önem derecesine göre değerlendirilir. Risklerin izlenmesinde ve ölçülmesinde öncelik sıralaması yapılır. Risk yönetimi kurum genelinde uygulanır ve risk herkesin sorumluluğundadır algısı hakimdir (Hall,2007).

Kurumsal risk yönetimi bir nevi kurum misyon ve vizyonunun belirlenmesiyle başlar. Misyon kapsamında stratejik hedefler ve hedeflere ulaşılmasını sağlayacak stratejiler belirlenir. Hedeflere ulaşmada karşımıza çıkabilecek engeller ve riskler gözden geçirilir risk tutumları saptanır. Risk azaltıcı kontrol faaliyetleri uygulanır. Elde edilen sonuçların raporlaması mutlaka yapılmalıdır (COSO, 2004).

Kurumsal risk yönetimi kapsamında temel faaliyetler arasında şunlar sayılabilir; (IIA,2009).

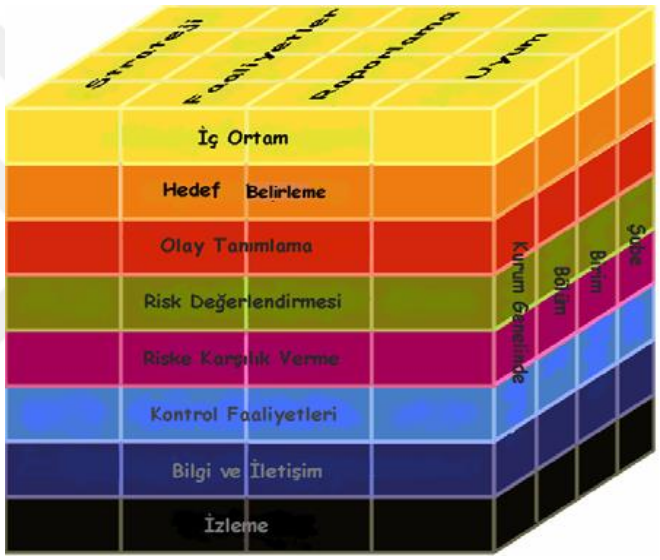
- Kurumun temel misyon ve hedeflerini doğru şekilde belirleyerek kuruma bildirmek,
- Kurumun risk iştahını belirlemek,
- Kurumun hedeflerine ulaşmasını engelleyecek olası tehditleri tanımlayarak bir risk evreni oluşturmak.
- Risk tutumlarına karar vererek uygulamak,
- Etki ve olasılık bakımından riskleri değerlendirmek,
- Kontrol ve tepki faaliyetlerini yönetmek,
- Risklerin etkili yönetildiğine dair güvence sunmak,

- Mevcut sistemlerle risk yönetimini entegre edebilmek,

3.4.1. Kurumsal Risk Yönetiminin Unsurları

Kurumsal risk yönetimi kavramı ilk olarak 2000'li yılların başında Amerika Birleşik Devletleri'nde meydana gelen ekonomik sıkıntılar, iflaslar, yeni risklerin ortaya çıkması, mevcut risklerin yönetilememesi ile ortaya çıkmıştır. Treadway komisyonu (COSO) 2004 yılında kurumsal risk yönetiminin çerçevesini belirlerken birbiriyle ilişkili 8 unsurdan oluştuğunu ortaya koymuştur. Bu unsurlar "COSO küpü" ya da "Kurumsal Risk Yönetimi-Entegre Çerçevesi" olarak da adlandırılmıştır.

Treadway komisyonu tarafından hazırlanan COSO küpü Şekil 3.8.'de gösterilmektedir.



Şekil 3.8: COSO ERM Küpü (Türkçe)

Kaynak: (COSO,2004)

Kurumsal risk yönetim unsurları iç ortam, hedef belirleme, olay tanımlama, risk değerlendirme, risk tutumu, kontrol faaliyetleri, bilgi-iletişim ve izleme olarak sıralanabilir. Tüm bu unsurlar birbiri ile ilişkilidir. Unsurların hepsi kurumsal risk yönetimi sistemini temsil etmektedir (Kinney,2003).

Küp üzerinde hedefler dikey olarak, unsurlarda yatay olarak gösterilmekte, kurum ve birimlerde üç boyutlu küp üzerinde yer almaktadır. Küp üzerinde dört hedef, sekiz unsur bulunmaktadır ve her unsur her hedefle kesişmektedir. Bu unsurlar aşağıda açıklanmıştır;

İç ortam unsuru, diğer tüm unsurlara altyapı oluşturmakta ve disiplin sağlamaktadır. İç ortam unsuru kurumun stratejileri ve kurum hedeflerinin belirlenerek faaliyetlerin

yapılandırılması, risklerin tespit edilmesi, risklerin değerlendirilmesi ve yönetilmesi süreçlerini kapsamaktadır (COSO,2004).

Hedef belirleme unsuru, yönetimin misyon ve kurumun risk iştahı ile uyumlu olmalıdır. Hedefler, risklerin tanımlanıp uygun risk tutumları belirlenmeden önce oluşturulmalıdır.

Olay tanımlama, kurumun hedeflere ulaşmasını etkileyebilme ihtimali olan iç ve dış kaynaklı olayların tanımlanması ve sınıflandırılması süreci olarak ifade edilebilir (Mattie, ve Cassidy,2008).

Risk değerlendirme, kurumun hedeflerine ulaşmasında risklerin tanımlanması, analiz edilmesi ve risklere uygun tutumların belirlenmesi süreci olarak tanımlanabilir (Intosai.2004).

Risk tutumu, riske karşılık verme olarak da adlandırılır. Riskler belirlendikten sonra kurumun risklerin nasıl yönetileceğine ve risklere nasıl cevap verileceğini belirlemesidir (Reding ve diğerleri, 2009).

Kontrol faaliyetleri, yönetim tarafından yürütülen ve risk tutumlarının etkin bir şekilde yönetildiğine dair güvence veren prosedürlerdir (Mattie, ve Cassidy,2008).

Bilgi ve iletişim, bilgi sisteminin temelinde mevcuttur. Kurumu yönetebilmek ve hedeflerine ulaşabilmesinde etkilidir.

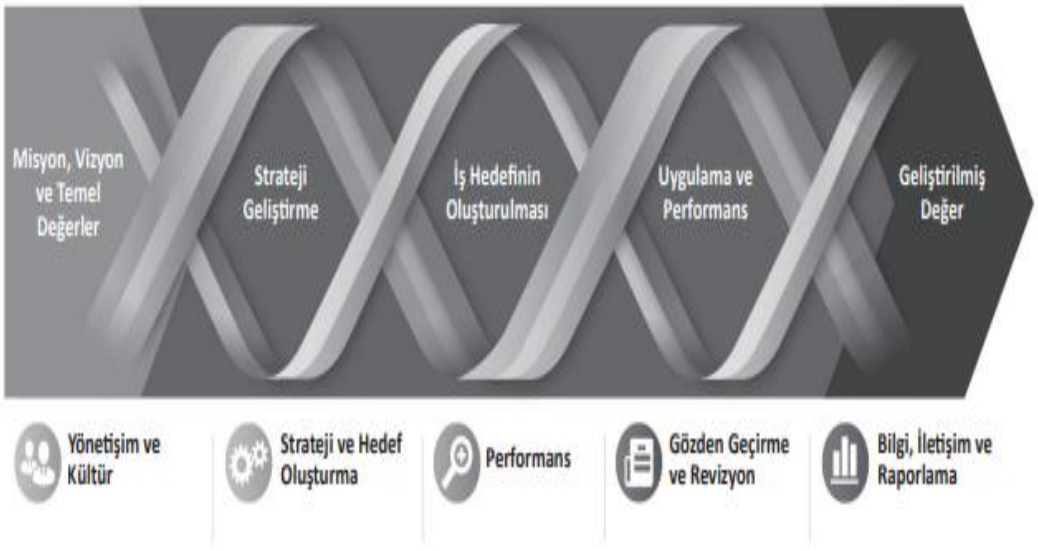
İzleme sürecinde kurum içi ve kurum dışı değişikliklerin yönetim tarafında değerlendirilmesi gerçekleştirilir.

2004 yılında yayınlanan "Kurumsal Risk Yönetimi-Entegre Çerçevesi 2017 yılında "Kurumsal Risk Yönetimi-Riskin Strateji ve Performansla Uyumlaştırılması" adıyla revize edilerek güncellenmiştir.

Güncellenen çerçevede kurumsal risk yönetimi; "Organizasyonun değer yaratma, koruma ve realize etmede, riski yönetmek için güvenebilecekleri, stratejinin belirlenmesi ve yürütülmesine entegre edilen, kültür, imkan ve uygulamalardır." şeklinde tanımlanmıştır (COSO,2017).

2004 çerçevesinde kurumsal yönetimin sekiz bileşeni, kurumun amaçları ve kurumsal yapı arasındaki ilişki küp şeklinde ifade edilirken 2017 çerçevesinde beş adet bileşen helezon (sarmal) şeklinde ifade edilmiştir. Ayrıca 2004 çerçevesinde bileşenlerin altında prensiplere yer verilmez iken 2017 çerçevesinde beş bileşenin altında 20 adet prensibe yer verilmiştir.

Komitenin hazırladığı COSO ERM sarmalında kurumsal risk yönetiminin bileşenlerinin, kurumun misyon, vizyon ve temel değerleriyle ilişkisi gösterilmektedir. Diyagramın üç şeridi strateji ve hedef oluşturma, performans, gözden geçirme ve düzeltme kurum boyunca akan genel süreçleri temsil ettiği, diğer iki şeridin ise yönetişim ve kültür ve bilgi, iletişim ve raporlama kurumsal risk yönetiminin destekleyici unsurlarını temsil ettiği ifade edilmiştir. Sarmala göre kurumsal risk yönetimi; strateji geliştirme, iş hedeflerinin oluşturulması ve uygulanması ve performansla entegre edildiğinde, bunun kurumun değerini artıracağı ifade edilmektedir (Burca,2017).



Şekil 3.9: COSO ERM Sarmalı (Türkçe)

Kaynak: (COSO,2017)

Yenilenen çerçeve, örgütsel yapıların gözetim, yönetim ve denetiminde bulunan taraflar için, kurumsal risk yönetimi uygulamalarının gözden geçirilmesi açısından önem arz etmektedir.

2004 çerçevesinde yer alan "Kontrol Faaliyetleri" bileşenine çerçevenin 2017 yılında yapılan güncellemesinde yer verilmemiştir. Ancak 2017 yılında çerçevede yapılan güncellemede COSO İç Kontrol Çerçevesine atıf yapılarak kontrol faaliyetleri hakkında bu çerçevenin halen geçerli olduğu ifade edilmiştir.

2017 yılında güncellenen çerçevede beş adet bileşen ve bunların altında yirmi adet prensip yer almıştır. Bu beş adet bileşen ile yirmi adet prensip Tablo 3.2 'de açıklanmıştır (Burca,2017).

Tablo 3.2: COSO 2017 Kurumsal Risk Yönetim Çerçevesi Bileşenler ve Prensipler

Bileşenler	Prensipler
1-Yönetişim ve Kültür	- Yönetim Kurulu Risk Gözetimini Yerine Getirir - Operasyonel Yapıyı Oluşturur - Arzu Edilen Kültürü Tanımlar - Temel Değerlere Bağlılık Gösterir - Yetenekli Personeli Çeker, Geliştirir ve Elde Tutar
2-Stareji ve Hedef Belirleme:	- İş Ortamını Analiz Eder - Risk İştahını Tanımlar - Alternatif Stratejileri Değerlendirir - İş Hedeflerini Oluşturur
3-Performans:	- Riskleri belirler - Risklerin Şiddetini Değerlendirir - Riskleri Önceliklendirir - Risk Cevaplarını - Portföy Bakış Açısı Geliştirir
4-Gözden Geçirme ve Düzeltme:	- Önemli Değişimleri Değerlendirir - Riskleri ve Performansı Gözden Geçirir - Kurumsal Risk Yönetiminde İyileştirmeleri Takip Eder
5-Bilgi, İletişim ve Raporlama	- Bilgi ve Teknoloji Avantajlarından Yararlanır - Risk Bilgisinin İletişimini Yapar - Risk, Kültür ve Performans Hakkında Raporlama Yapar

3.4.2. ISO 31000 Kurumsal Risk Yönetimi Standardı

ISO 31000 Uluslararası Standardizasyon Örgütü tarafından risk yönetimi ile ilgili belirlenen bir standart olarak tanımlanır.

ISO (International Organization for Standardization) tarafından yapılan tanımda; "Kuruluşları etkileyen riskler, ekonomik performans ve mesleki itibarın yanı sıra çevre, güvenlik ve toplumsal sonuçlar açısından da sonuç doğurabilir. Bu nedenle, riskin iyi yönetilmesiyle beraber kuruluşların belirsizlik dolu bir ortamda iyi performans oluşur" denilmektedir.

ISO 31000 ilk sürümü 2009 yılında yayımlanmış olup, şu anda ISO 31000-Risk Yönetimi Rehberi adıyla 2018 yılında yayımlanmış olan sürümü bulunmaktadır. Bu sürüm daha önceki sürümlere göre daha stratejik yapıdadır.

ISO 31000 Risk Yönetimi standartlarının kılavuzunda prensipler ve tanımlar yer almaktadır. ISO 31000 Risk yönetimi standardı 3 kısımdan oluşmaktadır. Bunlar; Prensipler, Çerçeve ve Süreçtir. ISO 31000 standardının amacı risk yönetiminin uygulandığı işletmelerde bir risk yönetimi çerçevesi oluşturarak genel kurallar sağlamaktır.

3.4.3. ISO 31000 Kurumsal Risk Yönetimi Standardının Faydaları

ISO 31000 Kurumsal Risk Yönetimi Standardının faydaları şöyle sıralanabilir; (Altınbaş,2017)

- Operasyonel etkinliği sağlayarak verimliliği artırır.
- İş sürekliliğini sağlar.
- Zaman ve kaynak israfını önler.
- Karar verme ve planlama için bir temel oluşturur.
- Kurumsal öğrenmeyi, esnekliği ve direnci oluşturur.
- Yasal düzenlemelere uymayı sağlar.
- Riskler ve tutumların tespitine yönelik farkındalık oluşmasını sağlar.
- Etkin bir risk yönetimi sayesinde kurumun hedeflerine ulaşmasını kolaylaştırır.

4. BÖLÜM: BİLGİ YÖNETİMİ ANLAYIŞINDA RİSK YÖNETİMİ

4.1.Bilgi Riski Yönetimi

Bazı kaynaklar bilgi yönetimi ve risk yönetimi kavramlarını birleştirmeye çalışmışlardır. Bu kavramların birleşimiyle bilgi riski yönetimi olarak adlandırılan kavram akademik alanda ortaya çıkan bir kavramdır. Araştırmacılar riski anlayabilmek ve yönetebilmek için bilginin önemli bir husus olduğunu savunmuşlardır.

Bilgi riski yönetiminin 2 ana teması var olduğu düşünülmektedir. Öncelikle araştırmacılar bilginin nasıl risk yönetiminden daha çok riski azalttığını değerlendirirler. Bu araştırmaya örnek olarak; De Zoysa ve Russell (2003) bilginin risk belirlemeye ve riske nasıl yardımcı olabileceğini incelemişlerdir. Verhaegen (2005) ve Otterson (2005) bilginin kalitesinin iyileştirilmesinin karar verme sürecine nasıl katkıda bulunduğunu araştırmışlardır. İkinci olarak, araştırmacılar bilgi yönetimi sürecinin risk yönetimini nasıl geliştirdiğini inceler. Marshall ve diğerlerinin (1996) bu alanda çalışmaları bulunmaktadır (Massingham,2010).

Trkman ve Desouza (2012) bilgi yönetimiyle ilişkili risklere atıfta bulunmak için bilgi riski yönetimi ifadesini kullanmışlardır. Bilgi risklerini sınıflandırarak bu risklerin bilgi transferini nasıl etkilediğini incelemişlerdir.

Bilgi riski yönetimi, kurumsal bilginin oluşturulması, kullanılması ve depolanmasıyla ilişkili riskleri belirlemek, analiz etmek ve bu risklere yanıt vermek için araç ve yöntemleri kullanmanın sistematik bir yolu olarak görülebilir.

Bilgi riski yönetimi uzun vadeli bir süreçten oluşur. Çeşitli bilgi yönetimi uygulamaları örgütün bilgisinin zamanında ve uygun olan sürekli risk yönetimi destekleyebilir. Bu bilgi yönetimi uygulamaları arasında bilgi yaratma, bilginin transfer edilmesi ve bilginin kalıcılığının korunmasının BRY için önemli olduğu görülmektedir.

Bir şirket bilgiyi yönetemezse risklerini de etkin bir şekilde yönetemez. Birçok şirket bilgi eksikliği ya da bilgi paylaşımı eksikliği nedeniyle riski yönetmede başarısız olmuştur (Neef, 2005).

Bilgi riski yönetimi sorunlara çözüm bulmaya çalışan ve gelişmekte olan bir alandır. Bilgi risk yönetimi konuları hem bilimsel hem de pratikte son derece ilgi çekici ve önem arz etmektedir. Hatta sürekli iyileştirme gerektiren güncel bir araştırma eğilimidir.

Bazı araştırmacılar da bilgi riski ve risk yönetimi arasındaki benzerlikleri açıklamaya çalışmışlardır. Örneğin: çalışan görüşü ihtiyacı, eylemlerin önemi, öğrenilen bilgilerin değeri ve risk yönetimi eşdeğerdir bilgi yönetimine gibi sonuçlar çıkarmışlardır. Bu araştırmacılar bilgi haritalama gibi yaygın bilgi yönetimi tekniklerini, yeni bir BRY yaklaşımının temeli olarak "sert etiketleme" uzmanlarını ve uygulama topluluklarını önerirler (Massingham, 2010).

4.2.Bilgi Yönetimi Anlayışında Risk Yönetimi

Sayıları giderek artan birçok bilgi yönetimi ve risk yönetimi uzmanı için gerçek şudur ki; Kurumsal liderler organizasyonlarında zararlı, yasa dışı veya itibar zedeleyici konularda bilgisizliğini koruyor. Modern şirketlerde daha iyi bir bilgi yönetimi sağlamak için zorlukların üstesinden gelinmesi amaçlanıyor. Sonuç olarak kurumsal liderler zorlukları önceden tahmin edebilmeli ve etik krizleri yönetebilmelidir. Kurumsal etik krizler tam da bilgi yönetimi uzmanlarının konularıdır.

Bilgi yönetimindeki olumsuzluklar ve eksiklikler bu süreçte önemli bir risk kaynağıdır. Risklerin etkin yönetimi bilgi yönetimi ile direkt bağlantılıdır. Dolayısıyla bilgiye dayalı risk yönetiminde bilgide yaşanan değişiklikler risk yönetimini etkiler. Örgütsel yapılarda bilgi yönetim sistemi hem de risk yönetim sistemi kurulmalıdır. Örgütsel yapının bilgi yönetim sistemleri ile risk yönetim sistemleri bütünleşmiş olmalıdır. Risk yönetim sisteminin etkinliği bilgi yönetim sisteminin etkinliğine bağlıdır (Fıkırkoca; 2003).

İşletmeler için bilginin korunması son derece önemlidir. Bilginin korunması ise bilgi güvenliği ile sağlanmaktadır. İşletmelerin bilgi varlıkları ve bilgi sistemlerine/güvenliğine yönelik risklerin belirlenerek, değerlendirilmesi ve cevaplanması bilgiye dayalı risk yönetiminin temelini oluşturur.

Bilgi yönetiminin risk yönetimine uygulanması aşamasında süreçlerinin tanımlanarak geliştirilmesi diğer yandan da bilgi çalışanının risk modelleme bilgisine ihtiyaç duyduğu bütünsel bilginin tanımlanması gerekmektedir (Rodriguez ve Edwards, 2008).

Bilgi tabanlı bir risk yönetimi çerçevesi için kapsam oluşturma, risk tanımlaması, risk analizi, risk yanıtlaması, risk yürütme ve risk izleme adımları takip edilir.

a) Kapsam Oluşturma

Kapsam oluşturma süreci hedeflenen bilgi yönetiminin çerçevesini, sınırlarını kimliğini ve paydaşlarının hedeflerini tanımlar (aktaran Alhawari,2008). Risklerin kapsamı oluşturulurken

bilinçli kararlar alınmalıdır. Risk yönetimi süreçlerini gerçekleştirmek için gereken roller, sorumluluklar ve gerekli kaynaklar belirlenir.

b) Risk Tanımlaması

Bu aşamada hangi olası risklerin bilgi varlığını etkileyeceği belirlenir. Aksiyon alınmadan önce risk kaynaklarının ve potansiyel sonuçların tanımlanması gerekir (aktaran Alhawari,2008). Geçmiş ve güncel risk durumu bilgilerin toplanması gerekir ve bu doğrultuda risk profili oluşturulur.

Risklerin tanımlanması için risk anketleri, beyin fırtınası, senaryo analizi ve diğer bilgi toplama yaklaşımları kullanılabilir.

Risk tanımlama sürecinde bilgi keşfi sayesinde yeni riskler keşfedilir. Riskleri uygun bir şekilde yönetebilmek için her bir riskin kaynağının tanımlanması gerekir (aktaran Alhawari,2008).

c) Risk Analizi

Risk analizi ile risk verilerinin karar verme bilgilerine dönüştürülmesi sağlanmış olur. Bir önceki aşamada tanımlanan her bir risk bu süreçte analiz edilir. Tespit edilen her bir riskin gerçekleşme olasılığı ve sonuçları tahmin edilmelidir.

Risk analizi ile birlikte risklerin gerçekleşme olasılığı, etkileri ve kaybın kapsamına göre sınıflandırma yapılmış olur.

Bu süreçle birlikte riskin yönetim tarafından kabul edilebilir bir düzeye inmesi için gerekli güvenlik kontrollerini oluşturmanın yolları sağlanmış olur (Alhawari ve diğerleri, 2008).

d) Riskin yanıtlanması

Risk bilgilerinin eylemlere ve yargılara dönüştürülmesini sağlar. Her bir riskle başa çıkabilmek için eylemler geliştirmeyi, önlemleri önceliklendirmeyi ve bir yönetim planı oluşturmayı amaçlar (aktaran Alhawari,2008).

Sonraki aşamalarda ihtiyaç duyulacak risk işleme eylemlerini önerir, risklerin etkisine ve olasılığa göre uygun güvenlik kontrollerinin seçilmesi sağlanır.

Bu sürecin hedefleri risk oluşma olasılığının azaltılması, kayıpların büyüklüğünün azaltılması ve riskin sonuçlarının değiştirilmesi olanak sıralanabilir (aktaran Alhawari,2008).

e) Riskleri yürütme

Bu aşamada riskten kaçınma, riskleri azaltma, risk transferi ve risk tutma aksiyonları ele alınır. Yürütme sürecinde risk kontrolü sırasında mevcut planın etkisiz olduğu tespiti gibi herhangi bir aksaklıkla beraber yeni bir risk süreci başlatmayı gerektirebilir (aktaran Alhawari,2008).

f) Risk izleme

Risk izleme aşaması bir geri bildirim süreci olarak görülmektedir. Risk izlemenin amaçları risk durumlarını ve risk yönetimi içeriğini gözden geçirmek ve bu doğrultuda güncellemek, risk işlemenin etkinliğini değerlendirmek ve yeni riskler ve kaynaklar aramaktır.

Risk meydana geldiğinde etkili bir önlem alınmasını sağlamak için ve önlemlerin çalıştığından emin olmak için riskler izlenmelidir.

4.3.Bilgi Yönetimi Anlayışında Risk Yönetimi Üzerine Bir Araştırma

Bilgi yönetimi ve güvenliği sistemlerinde risk yönetimi uygulamalarının farkındalık analizini yapmak üzere Türkiye'de faaliyet gösteren Üniversitelerde çalışan idari personele yönelik olarak "Bilgi Yönetimi Anlayışında Risk Yönetimi Anketi" düzenlenmiştir. Ankete 491 adet personel katılım sağlamıştır.

Katılımcılara 20 soruluk bir anket uygulanmıştır. Anketin ilk 5 sorusunda katılımcıların yaş, cinsiyet, eğitim durumu, meslek, çalıştığı bölüm/pozisyon bilgileri gibi demografik özelliklerine ilişkin sonuçlar elde edilmiştir. Anketin diğer 15 sorusunda ise tutum ve farkındalığı belirlemeye yönelik sorulara ilişkin sonuçlar elde edilmiştir. Anket internet üzerinden yayınlanmış ve ankete ait web adresi ile katılımcılardan anketin doldurulması istenmiştir. Araştırma da kullanılan anket soruları bilgi ve risk yönetimi kavramlarından ve mevcutta bulunan anket formlarından yararlanılarak oluşturulmuştur.

Anketin amacı; bilgi yönetimi ve güvenliği sistemlerinde risk yönetimi uygulaması arasındaki bağlantıyı, katılımcıların konuya davranış, yaklaşım, tutum ve farkındalıklarını ortaya koyabilmektir.

Araştırmada bazı kısıtlarla karşılaşılmıştır. Bunlardan biri anket çalışması Türkiye'de faaliyet gösteren Üniversitelerde çalışan idari personellere yönelik olmasına rağmen akademik personelin veya ilgisiz kişilerin ankete katılım sağladığı gözlemlenmiştir. Bir diğeri anketin Türkiye'de faaliyet gösteren tüm üniversitelere ulaşmamış olabilme olasılığıdır.

Anket yoluyla elde edilen veriler SPSS İstatistik Programı ile değerlendirilerek analiz edilmiştir. Anket bulgularına aşağıda yer verilmiştir.

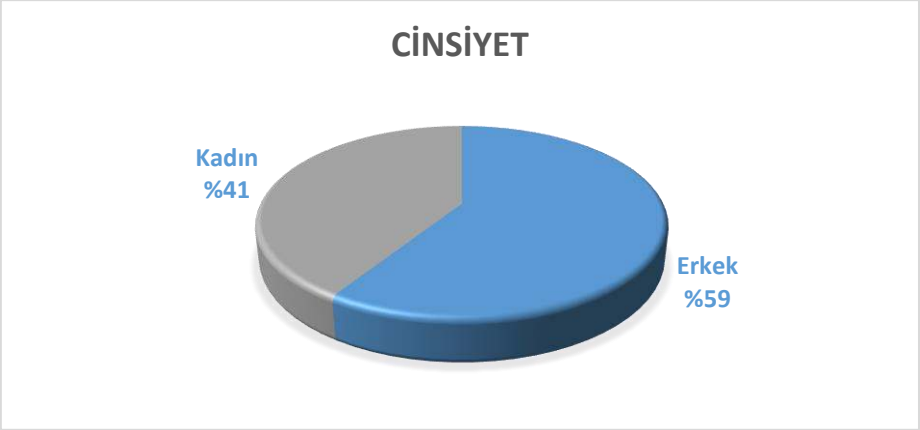
4.3.1. Demografik Özelliklere İlişkin Anket Bulguları

Katılımcıların Cinsiyeti

Tablo 4.1: Cinsiyete Göre Dağılım

Cinsiyet	Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Kadın	201	40,9	40,9	40,9
Erkek	290	59,1	59,1	100
Toplam	491	100	100	

Katılımcıların 290'ı (%59) erkek, 201'i (%41) kadındır (Grafik 4.1). Cinsiyete göre dağılımda Tablo 4.1 'de gösterilmektedir.



Grafik 4.1: Katılımcıların Cinsiyet Durumu

Katılımcıların Yaşı

Tablo 4.2: Yaş Gruplarına Göre Dağılım

Yaş Grupları	Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
18-25	66	13,4	13,4	13,4
26-35	93	18,9	18,9	32,4
36-45	174	35,4	35,4	67,8
45 üstü	158	32,2	32,2	100
Toplam	491	100	100	

Ankete katılanların % 35'i 36-45 yaş aralığında, %32'si ise 45 yaş üstüdür (Grafik 4.2). Yaş gruplarına göre dağılımda Tablo 4.2'de gösterilmektedir.

Grafik 4.2: Katılımcıların Yaş Durumu

Katılımcıların Eğitim Durumu

Tablo 4.3: Eğitim Durumu Dağılımı

Eğitim Durumu	Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Ön Lisans	104	21,2	21,2	21,2
Lisans	252	51,3	51,3	72,5
Yüksek Lisans	107	21,8	21,8	94,3
Doktora	28	5,7	5,7	100
Toplam	491	100	100	

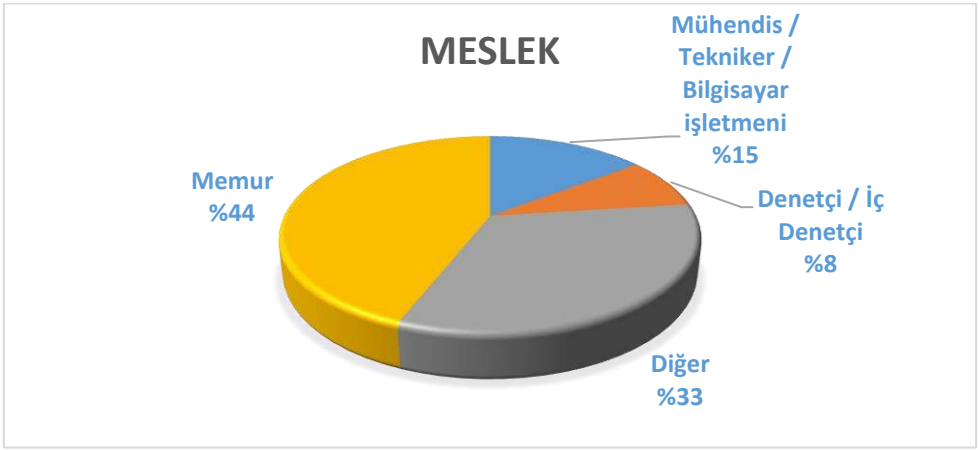
Katılımcıların %70' inden fazlası lisans ya da yüksek lisans diplomasına sahip olup, sadece %6'sı doktora diplomasına sahiptir (Grafik 4.3). Katılımcıların eğitim durumlarına göre dağılım Tablo 4.3'te gösterilmektedir.

Grafik 4.3: Katılımcıların Eğitim Durumu

Eğitim durumu, bilgi yönetimi ve risk yönetimi kavramları ile ilişkilendiririlmesi gereken bir değişkendir. Bilgi yönetiminin ve risk yönetiminin temelinde uzmanlık ve tecrübe yatmaktadır. Tüm bunları temelleri alınan eğitimin oluşturduğu bilinmektedir. Bu doğrultuda tabloya ve grafiğe bakıldığında katılımcıların %70' inden fazlasının en az lisans mezunu olması ankete katılanların bilgi yönetimi ve risk yönetimi konularında uzmanlık sahibi olabileceklerini ve anket konuları hakkında detaylı bilgiye sahip olabileceklerini göstermektedir.

Katılımcıların Meslek Bilgisi

Katılımcıların mesleklerine bakıldığında %44'ünün Memur, %15'inin Mühendis/Tekniker/Bilgisayar İşletmeni ve %8'inin Denetçi/İç Denetçi olduğu görülmüştür (Grafik 4.4). Katılımcıların meslek bilgisine göre dağılım Tablo 4.4'te, yaş-meslek karşılaştırması Tablo 4.5'te ve eğitim -meslek karşılaştırması Tablo 4.6'da gösterilmektedir.



Grafik 4.4: Meslek Bilgisi

Tablo 4.4: Meslek Bilgisine Göre Dağılım

Meslek	Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Mühendis /Tekniker/Bilgisayar İşletmeni	74	15	15	15
Denetçi/İç Denetçi	39	8,1	8,1	23
Memur	216	43,9	43,9	67
Diğer	162	33	33	100
Toplam	491	100	100	

Tablo 4.5: Yaş-Meslek Karşılaştırması

	Meslek				
Yaş	Mühendis /Tekniker/Bilgisayar İşletmeni	Denetçi/İç Denetçi	Memur	Diğer	Toplam
18-25	18	10	35	3	66
26-35	20	4	39	30	93
36-45	21	11	74	68	174
45 üstü	15	14	68	61	158
Toplam	74	39	216	162	491

Ankete en çok katılım gösteren 36-45 yaş aralığında ve 45 yaş üstü katılımcıların çoğunlukla Memur ve diğer meslek alanlarından kişilerden oluştuğu görülmektedir.

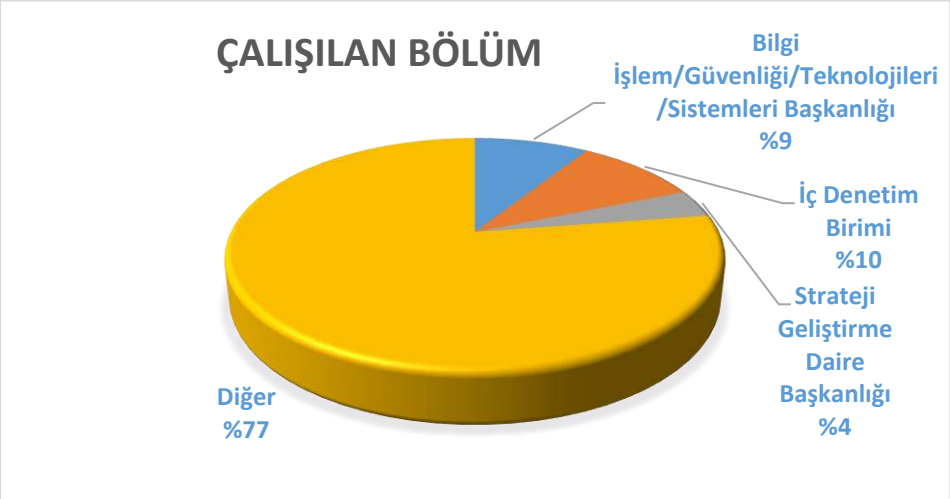
Tablo 4.6: Eğitim-Meslek Karşılaştırması

	Meslek				
Eğitim Durumu	Mühendis /Tekniker/Bilgisayar İşletmeni	Denetçi/İç Denetçi	Memur	Diğer	Toplam
Ön Lisans	25	6	50	23	104
Lisans	30	13	108	101	252
Yüksek Lisans	13	17	43	34	107
Doktora	6	3	15	4	28
Toplam	74	39	216	162	491

Ankete en çok katılım gösteren Lisans ve Yüksek Lisans mezunu katılımcıların çoğunlukla Memur ve Diğer meslek alanlarından kişilerden oluştuğu görülmektedir.

Katılımcıların Çalıştıkları Bölüm/Pozisyon

Katılımcıların %10'unun İç Denetim Biriminde, %9'unun Bilgi İşlem/Güvenliği/Teknolojileri/Sistemleri Başkanlığında, %77'sinin ise Diğer bölümlerde çalıştıkları gözlemlenmiştir. (Grafik 4.5). Katılımcıların çalıştıkları bölüm dağılımı Tablo 4.7'de, yaş-çalışılan bölüm karşılaştırması Tablo 4.8'de ve eğitim durumu-çalışılan bölüm karşılaştırması Tablo 4.9'da gösterilmiştir.



Grafik 4.5: Çalışılan Bölüm

Tablo 4.7: Çalışılan Bölüm Dağılımı

Çalışılan Bölüm/Pozisyon	Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Bilgi İşlem/ Güvenliği /Teknolojileri /Sistemleri Başkanlığı	44	9	9	9
İç Denetim Birimi	49	10	10	19
Strateji Geliştirme Daire Başkanlığı	20	4	4	23
Diğer	378	77	77	100
Toplam	491	100	100	

Tablo 4.8: Yaş-Çalışılan Bölüm Karşılaştırması

	Çalışılan Bölüm/Pozisyon				
Yaş	Bilgi İşlem/ Güvenliği /Teknolojileri /Sistemleri Başkanlığı	İç Denetim Birimi	Strateji Geliştirme Daire Başkanlığı	Diğer	Toplam
18-25	5	17	6	38	66
26-35	13	10	1	69	93
36-45	15	11	6	142	174
45 üstü	11	11	7	129	158
Toplam	44	49	20	378	491

Ankete en çok katılım gösteren 36-45 yaş aralığında ve 45 yaş üstü katılımcıların çoğunlukla anket seçeneklerinin dışında kalan alanlarda çalışan kişilerden oluştuğu görülmektedir.

Tablo 4.9: Eğitim Durumu-Çalışılan Bölüm Karşılaştırması

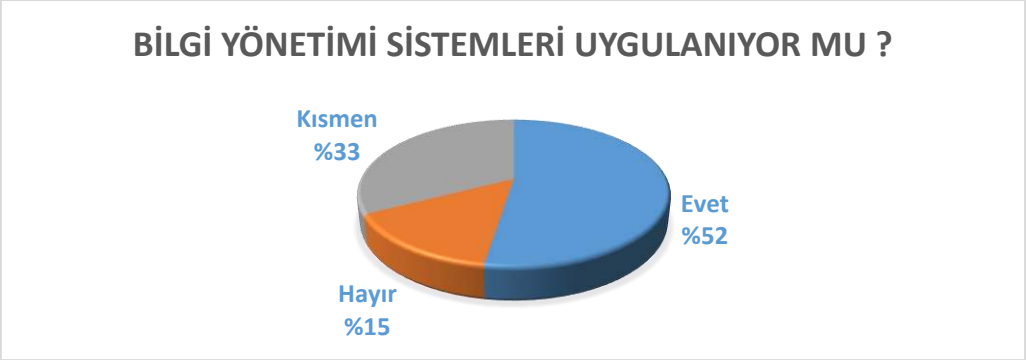
	Çalışılan Bölüm/Pozisyon				
Eğitim Durumu	Bilgi İşlem/ Güvenliği /Teknolojileri /Sistemleri Başkanlığı	İç Denetim Birimi	Strateji Geliştirme Daire Başkanlığı	Diğer	Toplam
Ön Lisans	10	16	5	73	104
Lisans	19	20	4	209	252
Yüksek Lisans	9	12	9	77	107
Doktora	6	1	2	19	28
Toplam	44	49	20	378	491

Ankete en çok katılım gösteren Lisans ve Yüksek Lisans mezunu katılımcıların çoğunlukla anket seçeneklerinin dışında kalan alanlarda çalışan kişilerden oluştuğu görülmektedir.

4.3.2. Bilgi Yönetimi ve Risk Yönetimi Tutumlarına Yönelik Anket Bulguları

Katılımcıların %80'i kurumlarında bilgi yönetimi sistemlerini uygulayan bir birim bulunduğunu, ancak katılımcıların %52'si kurumlarında bilgi yönetimi sistemlerinin uygulandığını düşünmektedir (Grafik 4.6 ve 4.7).

Grafik 4.6: Bilgi Yönetimi Sistemlerini Uygulayan Birim Varlığı



Grafik 4.7: Bilgi Yönetimi Sistemleri Uygulanması

Çalışılan Bölüm/Pozisyon ile Bilgi Yönetimi Sistemlerini uygulayan birimin varlığı bazında bakıldığında Bilgi İşlem/Güvenliği/Teknolojileri/Sistemleri Başkanlığında çalışan 44 kişiden 29 kişinin birimin varlığından haberdar olduğu, ancak İç Denetim Biriminde çalışan 48 kişiden 46 kişinin yani neredeyse tamamının bu birimin farkındalığında olduğu görülmektedir. (Tablo 4.10).

Tablo 4.10: Çalışılan Bölüm-Bilgi Yönetimi Sistemi Varlığı

Çalışılan Bölüm /Pozisyon	Kurumunuzda Bilgi Yönetimi Sistemlerini uygulayan bir birim bulunuyor
Bilgi İşlem/Güvenliği/Teknolojileri/Sistemleri Başkanlığı	29
İç Denetim Birimi	46
Strateji Geliştirme Daire Başkanlığı	16
Diğer	394

Katılımcıların %18' i Bilgi yönetiminin uygulanmasından birim çalışanlarının sorumlu olduğunu, %27 'si yöneticilerin sorumlu olduğunu, %52 'si ise herkesin sorumlu olduğunu düşünmektedir (Grafik 4.8).

Grafik 4.8: Bilgi Yönetimi Uygulaması Sorumluları

Tablo 4.11: Çalışılan Bölüm-Bilgi Yönetimi Uygulaması Sorumlusu

Çalışılan Bölüm /Pozisyon	Bilgi yönetiminin uygulanmasından kimlerin sorumlu olduğunu düşünüyorsunuz? (Herkes cevabı)
Bilgi İşlem/Güvenliği/Teknolojileri/Sistemleri Başkanlığı	23
İç Denetim Birimi	34
Strateji Geliştirme Daire Başkanlığı	11
Diğer	256

Çalışılan Bölüm/Pozisyon ile Bilgi yönetiminin uygulanmasından kimlerin sorumlu olduğu bazında bakıldığında Bilgi İşlem/Güvenliği/Teknolojileri/Sistemleri Başkanlığında çalışan 44 kişiden 23 kişinin, İç Denetim Biriminde çalışan 48 kişiden 34 kişinin uygulamadan herkesin sorumlu olduğu cevabını verdiği görülmektedir. (Tablo 4.11).

Katılımcıların %51'i kurumlarında BGYS'nin (Bilgi Güvenliği Yönetim Sistemi) uygulandığını düşünmesine rağmen, katılımcıların %62' si kurumlarında ISO 27001 sertifikasının bulunup bulunmadığı hakkında bilgiye sahip olmadığı görülmüştür (Grafik 4.9 ve 4.10).

Grafik 4.9: BGYS Uygulanması

Grafik 4.10: ISO 27001 Sertifika Varlığı

Ankete katılanlar arasında kurumlarında BGYS uygulandığını düşünen 105 kişi kurumlarının ISO 27001 sertifikasına sahip olduğunu da düşünmektedir. Bunun yanı sıra 113 kişi de BGYS sistemi uygulandığını düşünmesine rağmen ISO 27001 sertifikası hakkında bilgiye sahip olmadığı görülmüştür. (Tablo 4.12).

Tablo 4.12: BGYS Uygulanması-ISO 27001 Sertifikası Varlığı

		Kurumunuzun ISO 27001 sertifikası bulunuyor mu?		
		Evet	Hayır	Bilmiyorum
Kurumunuzda Bilgi Güvenliği Yönetim Sistemi uygulanıyor mu? (BGYS)	Evet	105	30	113
	Hayır	3	28	30
	Bilmiyorum	11	11	160

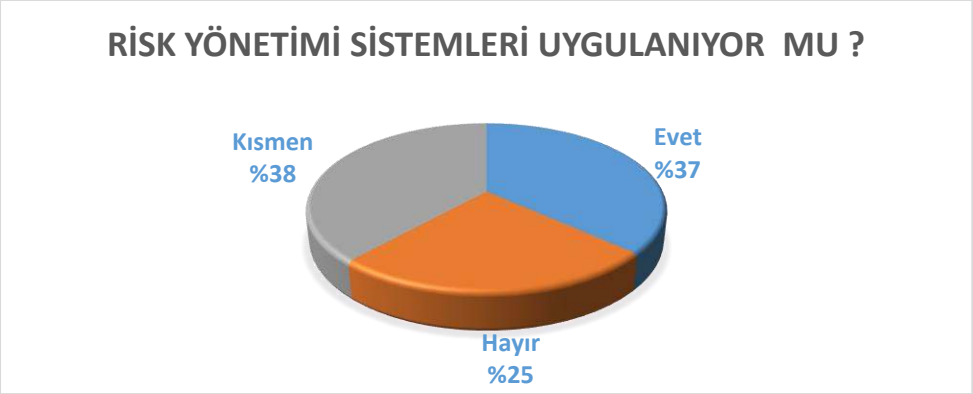
Katılımcıların %92'si bilgi yönetiminin önemli olduğunu düşünürken, sadece %46,3 ü kurumlarında bilgi yönetimi politikalarının uygulandığını düşünmektedir. (Grafik 4.11 ve 4.12)

Grafik 4.11: Bilgi Yönetiminin Önemi

Grafik 4.12: Bilgi Yönetimi Politikası

Katılımcıların %45'i kurumlarında risk yönetimi sistemlerini uygulayan bir birim bulunduğunu, ancak %38'i kurumlarında risk yönetimi sistemlerinin kısmen uygulandığını, % 25'i ise uygulanmadığını düşünmektedir. (Grafik 4.13 ve 4.14)

Grafik 4.13: Risk Yönetimi Sisteminin Uygulanması



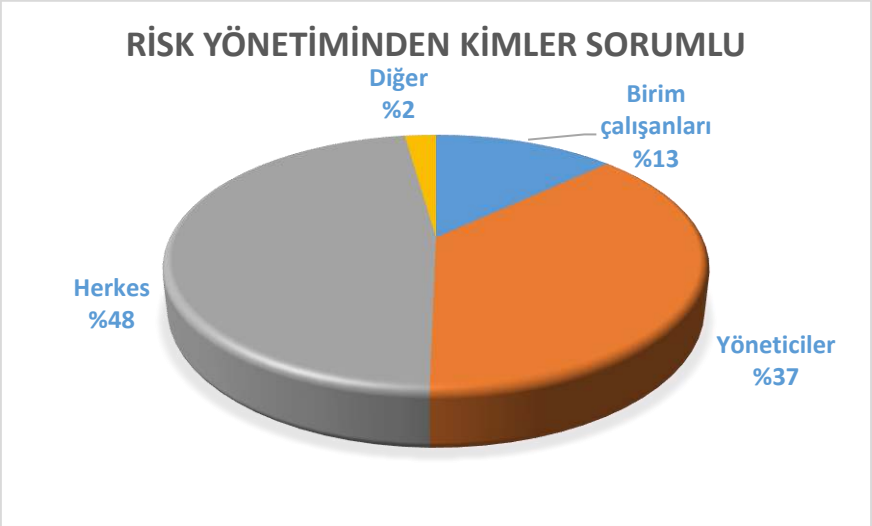
Grafik 4.14: Risk Yönetimi Sistemleri Uygulanması

Çalışılan Bölüm/Pozisyon ile Risk Yönetimi Sistemlerini uygulayan birimin varlığı bazında bakıldığında Bilgi İşlem/Güvenliği/Teknolojileri/Sistemleri Başkanlığında çalışan 44 kişiden 20 kişinin birimin varlığından haberdar olduğu, İç Denetim Biriminde çalışan 48 kişiden 15 kişinin bu birimin farkındalığında olduğu görülmektedir. İç Denetim Birimi çalışanlarının bu soruya çekimser cevap verdikleri düşünülmektedir. (Tablo 4.13).

Tablo 4.13: Çalışılan Bölüm-Risk Yönetimi Sistemleri Uygulayan Birim Varlığı

Çalışılan Bölüm /Pozisyon	Kurumunuzda Risk Yönetimi Sistemlerini uygulayan bir birim bulunuyor
Bilgi İşlem/Güvenliği/Teknolojileri/Sistemleri Başkanlığı	20
İç Denetim Birimi	15
Strateji Geliştirme Daire Başkanlığı	13
Diğer	175

Katılımcıların %13,1 i Risk yönetiminin uygulanmasından birim çalışanlarının sorumlu olduğunu, %37'si yöneticilerin sorumlu olduğunu, %48'i ise herkesin sorumlu olduğunu düşünmektedir (Grafik 4.15).



Grafik 4.15: Risk Yönetimi Sorumluları

Tablo 4.14: Çalışılan Bölüm-Risk Yönetimi Uygulamalarında Sorumlu

Çalışılan Bölüm /Pozisyon	Risk yönetiminden kimlerin sorumlu olduğunu düşünüyorsunuz? (Herkes cevabı)
Bilgi İşlem/Güvenliği/Teknolojileri/Sistemleri Başkanlığı	23
İç Denetim Birimi	16
Strateji Geliştirme Daire Başkanlığı	12
Diğer	181

Çalışılan Bölüm/Pozisyon ile Risk yönetiminden kimlerin sorumlu olduğu bazında bakıldığında Bilgi İşlem/Güvenliği/Teknolojileri/Sistemleri Başkanlığında çalışan 44 kişiden 23 kişinin, İç Denetim Biriminde çalışan 48 kişiden 16 kişinin uygulamadan herkesin sorumlu olduğu cevabını verdiği görülmektedir. İç Denetim Biriminde çalışanların bu soruya çekimser cevap verdikleri düşünülmektedir. (Tablo 4.14).

Katılımcıların %71'inin kurumlarında ISO 31000 sertifikasının bulunup bulunmadığı hakkında bilgiye sahip olmadığı görülmüştür (Grafik 4.16).

Grafik 4.16: ISO 31000 Sertifika Varlığı

Ankete katılanlar arasında kurumlarında Risk yönetimi uygulamaları uygulanıp uygulanmadığını bilmeyen 156 kişi kurumlarının ISO 31000 sertifikasına sahip olup olmadığını da bilmemektedir. Bunun yanı sıra 114 kişi ise Risk yönetimi uygulamalarının uygulandığını düşünmesine rağmen ISO 31000 sertifikası hakkında bilgiye sahip olmadığı görülmüştür (Tablo 4.15). ISO 31000 standardına ait henüz sertifikalandırılma yapılmamaktadır. Katılımcılara farkındalığı ölçmek amacıyla kurumlarının sertifikalarının olup olmadığı ya da bilgiye sahip olup olmadığı çeldirici bir soru olarak sorulmuştur.

Tablo 4.15: Risk Yönetimi Uygulanması-ISO 31000 Sertifikası Varlığı

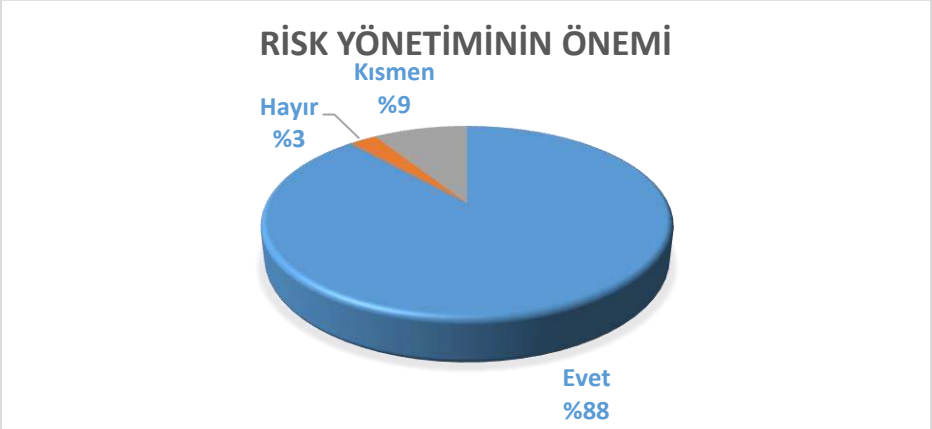
		Kurumunuzun ISO 31000 sertifikası bulunuyor mu?		
		Evet	Hayır	Bilmiyorum
Kurumunuzda Risk Yönetimi uygulamaları uygulandığını düşünüyor musunuz?	Evet	37	29	114
	Hayır	4	39	80
	Bilmiyorum	4	28	156

Katılımcıların %43'ü kurumlarında risk yönetimi politikalarının kısmen ve %36'sı uygulandığını düşünürken, %21'i uygulanmadığını düşünmektedir. Sadece %46'sı kurumlarında risk yönetimi politikalarının yararlı olduğunu düşünmektedir. (Grafik 4.17 ve 4.18)

Grafik 4.17: Risk Yönetimi Politikası

Grafik 4.18: Risk Yönetimi Politikaları Yararı

Katılımcıların %88'i risk yönetiminin önemli olduğunu düşündüğü görülmektedir. (Grafik 4.19)



Grafik 4.19: Risk Yönetimi Önemi

Son olarak katılımcıların %93 'ünün bilgi yönetimi ve risk yönetimi sistemlerinin bir arada olması gerektiğini düşündükleri görülmektedir. (Grafik 4.20).

Grafik 4.20: Bilgi Yönetimi ve Risk Yönetimi Birlikteliği

5. BÖLÜM: SONUÇ

Günümüzde artık bilgi yönetimi ve risk yönetimi konuları birbirinden ayrı düşünmek pek de mümkün değildir. Bilgi yönetiminin gelişimi risk yönetimini, risk yönetiminin gelişimi bilgi yönetimini destekler.

Hem bilgi yönetimini hem risk yönetimini başarılı olarak uygulayabilen işletmeler büyük bir rekabet avantajı sağlamaktadır. Riskleri etkin bir şekilde yönetebilmek bilgi yönetimini doğrudan etkiler.

Anket çalışmasının uygulandığı Üniversitelerde ankete katılan idari personel bilgi yönetimi sistemlerini uygulayan bir birimin varlığından haberdar olduğunu ancak sistemlerin tam ve eksiksiz uygulanmadığı düşünmektedir. Bu da bilgi yönetimi sistemlerine gereken önemi vererek tam olarak uygulamaya geçemediğimizi göstermektedir.

Bilgi yönetimi uygulamalarından sadece ilgili birim veya yöneticiler sorumlu değildir. Aksine herkesin sorumluluğu bulunmaktadır. Herkes üzerine düşen görevi yerine getirdiği takdirde başarılı işleyen bir yönetim süreci sağlanmış olur. Anket çalışmasına verilen cevaplarda bu bilgileri desteklemiştir. Ancak ilginçtir ki Bilgi İşlem/Güvenliği/Teknolojileri/Sistemleri Başkanlığında çalışanlar bu soruya diğer yerlerde çalışanlardan daha az "herkes" cevabını vermiştir.

Bilgi güvenliği yönetim sistemi bilginin gizliliği, bütünlüğü ve kullanabilirliğini sağlar. BGYS 'nin üst yönetim tarafından da desteklenmesi kurum yararına olacaktır. Ankete katılanlar kurumlarında BGYS'nin uygulandığını düşünmesine rağmen BGYS standardı olan ISO 27001 sertifikasına sahip olup olmadığını bilmemektedir. Bu da sürecin uygulanması ve dökümante edilmesi aşamasında ciddi sorunların olduğunu göstermektedir. Ankete katılanlar arasında çoğunluğun kurumlarında BGYS sistemi uygulandığını düşünmesine rağmen ISO 27001 sertifikası hakkında bilgiye sahip olmadığı görülmüştür. Genel olarak ISO 27001 sertifikası hakkında farkındalığın oluşmadığı sonucu çıkarılabilir.

Ankete katılanların neredeyse tamamı bilgi yönetiminin önemli olduğunun farkındalığında olsa da ankete katılanların yarısından fazlası bilgi yönetimi politikalarının uygulanmadığını düşünmektedir. Bilgi yönetimi politikalarının eksikliği hem bilgi güvenliği açıklarını hem de riskleri ortaya çıkaracaktır. Bilgi yönetimi politikaları uygulanmayan kurumlar rekabet avantajı sağlayamayacak ve geride kalacaklardır.

Anket çalışmasının uygulandığı Üniversitelerde ankete katılan idari personelin neredeyse yarısı risk yönetimi sistemlerini uygulayan bir birimin varlığından haberdar olduğunu ancak sistemlerin tam ve eksiksiz uygulanmadığı düşünmektedir. Bu da aslında tam olarak risk yönetimi sistemlerine gereken önemi vermediğimizi veya uygulamaya geçemediğimizi göstermektedir.

Risk yönetimi uygulamalarında üst yönetimin rolü ve tutumu önemli olmasına karşın risk yönetimi uygulamalarında herkesin sorumluluğu bulunmaktadır. Anket cevapları da bu bilgiyi destekler niteliktedir. Ancak çalışılan birim özelinde bakıldığında İç Denetim Biriminde çalışanların Risk yönetimi sistemlerini uygulayan birim ve risk yönetiminden kimlerin sorumlu olduğu sorularına beklenen cevabı vermedikleri veya çekimser cevap verdikleri düşünülmektedir.

Risk yönetimi standardı olarak adlandırılan ISO 31000 standardı risk yönetimi sürecinin uygulanabilirliği ve dökümante edilmesi aşamasında oldukça önemli yere sahiptir. Ankete katılanların yarısından çoğu kurumlarının ISO 31000 sertifikasına sahip olup olmadığını bilmediğini belirtmişlerdir. Hatta Risk yönetimi uygulamaları uygulanıp uygulanmadığını bilmeyen çoğu kişi kurumlarının ISO 31000 sertifikasına sahip olup olmadığını da bilmemektedir. Bunun yanı sıra ankete katılanların 3'te 1'i Risk yönetimi uygulamalarının uygulandığını düşünmesine rağmen ISO 31000 sertifikası hakkında bilgiye sahip olmadığı görülmüştür.

Ankete katılanların yarısından fazlası kurumlarında risk yönetimi politikalarının kısmen veya tamamen uygulandığını düşünmekte ve uygulanan politikaları yararlı bulmaktadır. Katılımcıların neredeyse tamamı risk yönetiminin önemli olduğunun farkındalığındadır. Ancak Risk yönetiminin tam olarak uygulandığını söyleyememektedirler.

Piyasalar geliştikçe ve değiştikçe rakipler ve teknolojiler de değişecek ve gelişecektir. Bunun sonucunda bu teknolojilere uyumlu olanlar, bilgiyi kullananlar ile risklerini ortaya koyarak yönetebilen işletmeler başarılı olacaktır. Bilgi yönetimi ve risk yönetiminin bir arada olması gerektiği birçok araştırmacı tarafından desteklenmeye ve önemi bilinmeye başlanmıştır. Anket sonuçlarına göre de katılımcıların neredeyse tamamı bilgi yönetimi ve risk yönetiminin bir arada olması gerektiği şeklinde görüş bildirmiştir.

Genel olarak bilgi yönetimi ve risk yönetimi konularında az da olsa farkındalığın olduğu ancak uygulamada eksiklikler olduğu yorumlanabilir. Bilgi yönetimi ve risk yönetimi sistemlerinin düzenli ve verimli olarak uygulanması için inceleme, araştırma ve izleme mekanizmaları kurulması ve maddi-manevi yaptırımların uygulanmasının işletmelere her anlamda olumlu dönüş sağlayacağı düşünülmektedir.

Bilgi yönetimi ve risk yönetimi konularında farkındalığı artırmak ve uygulamaya geçirmek için personellere hem kurum içi hem de kurum dışı eğitim veya seminerler düzenleneceğinin faydalı olacağı düşünülmektedir.

KAYNAKLAR

A Practical Guide to Risk Assessment. https://web.actuaries.ie/sites/default/files/erm-resources/a_practical_guide_to_risk_assessment.pdf. 16 Mart 2022.

Abdullah, R. ve Diğerleri. (2005). A Framework for Knowledge Management System Implementation in Collaborative Environment for Higher Learning Institution. Journal of Knowledge Management Practice, March, 39-54.

Akçakanat, Ö. (2012). Kurumsal Risk Yönetimi ve Kurumsal Risk Yönetim Süreci, Süleyman Demirel Üniversitesi Vizyoner Dergisi,4(7), 30-46.

Aksoy A. ve Tanrıöven, C. (2007), Sermaye Piyasası Yatırım Araçları ve Analizi, Ankara, Gazi Kitapevi.

Alhawari ve Diğerleri. (2012). Knowledge-Based Risk Management framework for Information Technology Project International Journal of Information Management 32 .50– 65.

Awad, E. ve Ghaziri, H. (2004). Knowledge Management. New Jersey: Prentice Hall Publishing.

Balay, R. (2004). 'Küreselleşme, Bilgi Toplumu ve Eğitim', Ankara Üniversitesi Eğitim Bilimleri Fakültesi Dergisi, 37(2), 61–82.

Balcılar, H. (2008). "Türkiye'nin Bilgi Toplumu Olma Yolunda Bilgi Teknolojilerinin Kullanılması", (Yayınlanmamış Yüksek Lisans Tezi), Selçuk Üniversitesi, S.B.E.

Barutçugil, İ. (2002). Bilgi Yönetimi. İstanbul: Kariyer Yayıncılık.57-70.

Beasley, M.S., B.C. Branson ve B.V. Hancock (2009). ERM: Opportunities For Improvement. Journal of Accountancy,208: S: 3. 28-33.

Bhatt, D. (2000). "Organizing Knowledge in the Knowledge Development Cycle", Journal of Knowledge Management, 4(1), ss. 15-26.

Burca, N. (2017). Yenilenen COSO Kurumsal Risk Yönetimi Çerçevesi. https://nazifburca.com/2017/09/20/yenilenen-coso-kurumsal-risk-yonetimi-cercevesi/ .08 Nisan 2022.

Büberkökü, Ö. (2018). Banka Hisselerinin Zamanla Değişen Toplam Riskinin Sistematik ve Sistematik Olmayan Risk Bileşenlerine Ayrılması: Ar (P)-Dcc-Garch (P, Q) Modelline Dayalı Bir Analiz. Uluslararası Bilimsel Araştırmalar Dergisi (IBAD), 3:1, 35-54.

Canbazoğlu, T. (2000). Yararlı Bilgi Yönetiminde İnsan Faktörü. Türkiye Bilişim Vakfı Eğitim Seminerleri:17.İstanbul.

Cooper, P. (2010). Knowledge management. Anaesthesia and Intensive Care Medicine Magazine, 12 (5), 516-520.

COSO. (2004). Enterprise Risk Management-Integrated Framework Executive Summary Framework.

COSO. (2017) Integrating with Strategy and Performance Executive Summary, https://www.coso.org/Shared%20Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf. 08 Nisan 2022.

Davenport, T. ve L. Prusak (2001). İş Dünyasında Bilgi Yönetimi, Rota Yayın Yapım Tanıtım Tic. Ltd. Şti., İstanbul.

Derici, O., Z. Tüysüz ve A. Sarı (2007). Kurumsal Risk Yönetimi ve Sayıştay Uygulaması. Sayıştay Dergisi, Nisan-Haziran.65: 151-172.

Durna, U. ve Demirel, Y. (2008). Bilgi Yönetiminde Bilgiyi Anlamak, Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 30 (1), 129-156.

Emhan, A. (2009). "Risk Yönetim Süreci Ve Risk Yönetmekte Kullanılan Teknikler", Atatürk Üniversitesi, İİBD, C.23, S.3.

Ersoy, E. (2012). ISO/IEC 27001 Bilgi Güvenliği Standardı, ODTÜ Yayıncılık, Ankara, Şubat.

Fıkırkoca, M. (2003). Bütünsel Risk Yönetimi, Kalder Yayınları, Ankara.

Güçlü, N. ve Sotırofskı, K. (2006). Bilgi Yönetimi. Türk Eğitim Bilimleri Dergisi, 4 (4), 351-373.

Fone, M. ve Young PC. (2005). Managing Risks in Public Organisations. Perpetuity Press

Gülseçen, S. (2014). Bir Değer Olarak Bilgi ve Bilginin Yönetimi. Türk Kütüphaneciliği, 28 (1), 62-68.

Grıffiths, P. (2005). Risk-Based Auditing, England: Gower Publishing.

Hall, J. (2007). Internal Auditing and ERM: Fitting in and Adding Value. www.theiia. org/download.cfm?file=66127.

Hazine ve Maliye Bakanlığı. (2014). Kamu İç Denetim Rehberi, https://ms.hmb.gov.tr/uploads/2019/08/8227kamuickontrolrehberi1versiyon12.pdf .1-132.

Hillson, D. ve Murray-Webster R. (2007). Understanding and Managing Risk Attitude, Gower Publishing, USA.

Holland, J. (1993). International Financial Management, Cambridge: Blackwell Publishing Company,139.

IIA. (2008). Uluslararası İç Denetim Standartları, Terimler Sözlüğü:39.

Intosai. (2004), Guidelines for International Control Standarts for the Public Sector, Intosai Professional Standards Committee Secretarıat,1-71.

Ipe, M. (2003). The Praxis of Knowledge Sharing in Organizations: ACase Study, Ph.D Dissertation, The University of Minnesota, 18-20.

Karabacak, H. (2021) Uzmanların Kaleminden Farklı Boyutlarıyla Risk ve Risk Yönetimi, Gazi Kitabevi,195-217

Karakaya, A. (2002). "İşletme Yönetiminde Stratejik Bilgi Kullanım Yönetimi Üzerine Bir Araştırma.303-320.

Kızılboğa, R. (2012). Geleneksel Risk Yönetiminden Kurumsal Risk Yönetimine Geçiş. Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,16:S.3,297-316.

Kinney, W. R. (2003). The Research Opportunities in Internal Audit. Auditing Risk Assessment and Risk Management Process. FL: The Institute of Internal Auditors.

Koç, S. ve Çelik, A. (2015). Kurumsal Risk Yönetimi: Türkiye'de Bankacılık Sektöründe Bir Uygulama, Cumhuriyet Üniversitesi İktisadi ve İdari Bilimler Dergisi,16(2),311.

Malhotra, Y. (2000). Knowledge Management and New Organization Forms: A Framework for Business Model Innovation. Knowledge Management and Virtual Organizations. USA: Idea Group Publishing, 2-19.

Marshall, C., Prusak, L. and Shpilberg, D. (1996), ''Financial risk and the need for superior knowledge management'', California Management Review, 38(3).77-102.

Massingham, P. (2010). Knowledge Risk Management: A Framework. Journal Of Knowledge Management,14(3).464-485.

Marttin V. ve Pehlivan İ. (2010).”ISO 27001:2005 Bilgi Güvenliği Yönetimi Standardı ve Türkiye’deki Bazı Kamu Kuruluşu Uygulamaları Üzerine Bir inceleme”, Mühendislik Bilimleri ve Tasarım Dergisi, 1(1).

Mattie, J.A. ve D.L. Cassidy. (2008). Achieving goals, protecting reputation: Enterprise Risk Management for Educational Institutions, https://regents.universityofcalifornia.edu/regmeet/july08/a7a.pdf. 11 Mart 2022.

McCumber, J. (1991). Information systems security: A comprehensive model. Proceedings 14th National Computer Security Conference,328-337.

Mercier-Laurent, E. (2016). Knowledge Management &Risk Management. Preproceedings of the Federated Conference on Computer Science and Information Systems. 1409–1413.

Neef, D. (2005), ‘‘Managing corporate risk through better knowledge management’’, The Learning Organization, Vol. 12 No. 2, 112-24.

Nonaka, I. (1994). A dynamic theory of organizational knowledge, Organization Science, 5 (1), 14-37.

Nonaka, I. (2004). The Knowledge –Cretaing Company. Hitotsubashi on Knowledge Management.

Özbek, Ç. (2012). İç Denetim, İstanbul: Türkiye İç Denetim Enstitüsü.237-242.

Özer, A. (2012). Rekabet Ortamında Girişimciler İçin Varolabilme Reçetesi: Risk Yönetimi. Girişimcilik ve Kalkınma Dergisi,7:S.1.

Özgener, Ş. (2002). “Global Ölçekte Değer Yaratan Bilgi Yönetimi Stratejileri”, 1. Ulusal Bilgi Ekonomisi ve Yönetim Kongresi Bildirileri, Kocaeli, 483-496.

Pehlivanlı, D. (2010). Modern İç Denetim, İstanbul: Beta Basım, 1. Baskı.

Reding, F.K.ve diğerleri (2009). Internal Auditing: Assurance&Consulting Services, 2.Baskı, The IIA Research Foundation.

Road to Implementation ERM for Colleges and Universities, (2009), Arthur J. Gallagher Risk Management Services, Inc. https://www.odu.edu/content/dam/odu/offices/risk-management/DOCS/erm-road-to-implementation-universities.pdf. 7 Mayıs 2022.

Rodriguez, E. ve Edwards, J. S. (2014). Knowledge Management in Support of Enterprise Risk Management. International Journal of Knowledge Management, 10(2), 43-61.

Sayılgan, G. (2003). Soru ve Yanıtlarla İşletme Finansmanı, Ankara, Turhan Kitabevi, 432.

Sobel, P J. (2015). Auditor's Risk Management Guide Integrating Auditing and ERM, CCH Incorporated, USA.

Sümer, B. (2007). "Bilgi Toplumuna Dönüşüm Sürecinin Avrupa ve Türkiye'de İstihdam Yaratmaya Etkisi", (Yayınlanmamış Doktora Tezi), Dokuz Eylül Üniversitesi, S.B.E.

Taner, B ve Akkaya, G.C. (2009). Sermaye Piyasası Faaliyet Alanı ve Menkul Kıymetler, Ankara, Detay Yayıncılık,181.

The Institute of InternalAuditors. (IIA) Position Paper: The Role of Internal Auditing in Enterprise-wide Risk Management. (2009). https://www.iia.nl/SiteFiles/IPPF_PP_Role_of_IA_in_ERM_01.09 [2].pdf .12 Nisan 2022.

The Institute of Risk Management (IRM), (2010). Kurumsal Risk Yönetimine Bakış Açısı ve ISO 31000 Yükümlülükleri.

TÜSİAD. (2008). Kurumsal Risk Yönetimi, İstanbul,19-20.

Usman, Ö. (2018). Kurumsal Risk Yönetim Sisteminde Risk Değerlendirme Raporlarının Hazırlanması, Uluslararası Toplum Araştırmaları Dergisi, C.9, S.16,1588-1607.

Usta, Ö. (2005). İşletme Finansmanı ve Finansal Yönetim, Ankara, Detay Yayıncılık, 232.

Vaughan, EJ ve Vaughan, T. (2001). Risk Yönetimi ve Sigortanın Esasları. New York, Chichester, Weinheim, Brisbane, Singapur, Toronto: John Wiley & Sons, Inc.

Vose, D. (2008). Risk Analysis: A Quantitative Guide, 3. Baskı. John Wiely ve Sons Ltd.

Wiig, K. (1997). Knowledge Management: Where did it come from and where will it go? J. Experts Systems With Applications. Special Issue on Knowledge Management, 13(1),1-14.

Zyngier, S. (2008). Risk Management: Strengthening Knowledge Management. International Journal of Knowledge Management, 4(3), 1–32.

EKLER

EK-1 ANKET SORULARI

BİLGİ YÖNETİMİ ANLAYIŞINDA RİSK YÖNETİMİ KONULU YÜKSEK LİSANS TEZİ

ANKET ÇALIŞMASI

1. Yaşınız?

- **( ) 18-25**
- **( ) 26-35**
- **( ) 36-45**
- **( ) 45 üstü**

2. Cinsiyetiniz nedir?

- **( ) Kadın**
- **( ) Erkek**

3. Eğitim durumunuz nedir?

- **( ) Ön lisans**
- **( ) Lisans**
- **( ) Yüksek Lisans**
- **( ) Doktora**

4. Mesleğiniz nedir?

5. Çalıştığınız bölüm/pozisyon nedir?

- **( ) Bilgi İşlem/Güvenliği/Teknolojileri/Sistemleri Başkanlığı**
- **( ) Risk Yönetimi /Denetim Başkanlığı**
- **( ) Strateji Geliştirme Daire Başkanlığı**
- **( ) Diğer**

6. Kurumunuzda Bilgi Yönetimi Sistemlerini uygulayan bir birim bulunuyor mu?

- **( ) Evet**
- **( ) Hayır**

7. Kurumunuzda Bilgi Yönetimi Sistemleri uygulandığını düşünüyor musunuz?

- **( ) Evet**
- **( ) Hayır**
- **( ) Kısmen**

8.Bilgi yönetiminin uygulanmasından kimlerin sorumlu olduğunu düşünüyorsunuz?

- **( ) Birim çalışanları**
- **( ) Yöneticiler**
- **( ) Herkes**
- **( ) Diğer:**

9. Kurumunuzda Bilgi Güvenliği Yönetim sistemi uygulanıyor mu? (BGYS)

- **( ) Evet**
- **( ) Hayır**
- **( ) Bilmiyorum**

10. Kurumunuzun ISO 27001 sertifikası bulunuyor mu?

- **( ) Evet**
- **( ) Hayır**
- **( ) Bilmiyorum**

11. Bilgi yönetiminin önemli olduğunu düşünüyor musunuz?

- **( ) Evet**
- **( ) Hayır**
- **( ) Kısmen**

12. Kurumunuzda bilgi yönetimi politikaları uygulanıyor mu?

- **( ) Evet**
- **( ) Hayır**
- **( ) Kısmen**

13. Kurumunuzda risk yönetimi sistemlerini uygulayan bir birim bulunuyor mu?

- **( ) Evet**
- **( ) Hayır**
- **( ) Bilmiyorum**

14. Kurumunuzda risk yönetimi uygulamaları uygulandığını düşünüyor musunuz?

- **( ) Evet**
- **( ) Hayır**
- **( ) Kısmen**

15. Risk yönetiminden kimlerin sorumlu olduğunu düşünüyorsunuz?

- **( ) Birim çalışanları**
- **( ) Yöneticiler**
- **( ) Herkes**
- **( ) Diğer:**

16. Kurumunuzun ISO 31000 sertifikası bulunuyor mu?

- **( ) Evet**
- **( ) Hayır**
- **( ) Bilmiyorum**

17. Kurumunuzda risk yönetimi politikaları uygulanıyor mu?

- **( ) Evet**
- **( ) Hayır**
- **( ) Kısmen**

18. Kurumunuzda uygulanan risk yönetim politikalarını yararlı buluyor musunuz?

- **( ) Evet**
- **( ) Hayır**
- **( ) Kısmen**

19. Risk yönetiminin önemli olduğunu düşünüyor musunuz?

- **( ) Evet**
- **( ) Hayır**
- **( ) Kısmen**

20.Bilgi yönetimi ve risk yönetimi sistemlerinin bir arada olması gerektiğini düşünüyor musunuz?

- **( ) Evet**
- **( ) Hayır**

EK-2 ETİK KURUL ONAYI

Karar: 69289

KARAR(ISSUE NUMBER): 06.03.2023/

T.C.
ANKARA SOSYAL BİLİMLER ÜNİVERSİTESİ REKTÖRLÜĞÜ
SOSYAL VE BEŞERİ BİLİMLER ARAŞTIRMALARI
VE
BİLİMSEL YAYIN ETİK KURULU
(SOCIAL SCIENCES UNIVERSITY OF ANKARA
INSTITUTIONAL ETHICS COMMITTEE OF SOCIAL SCIENCES AND
HUMANITIES RESEARCH AND PUBLICATION)

ETİK ONAY BELGESİ
(CERTIFICATE OF ETHICS APPROVAL)

Araştırma Yöntemi (Research Method)	Anket Çalışması
Araştırmanın Adı (Study Title)	Bilgi Yönetimi Anlayışında Risk Yönetimi
Sorumlu Araştırmacının Adı Soyadı (Principal Researcher Name Surname)	EMİNE İPEK
Karar (Committee Decision)	UYGUNDUR

e-imzalıdır
Prof. Dr. M. Hakan TÜRKÇAPAR
Başkan (Chair)

e-imzalıdır
Prof. Dr. Sutay YAVUZ
Üye(Member)

e-imzalıdır
Prof. Dr. Aslı AKAY
Üye(Member)

e-imzalıdır
Prof. Dr. Mustafa ÇEVİK
Üye(Member)

e-imzalıdır
Prof. Dr. İsmail ÇAKIR
Üye(Member)

e-imzalıdır
Prof. Dr. Mehmet Emin BİLGE
Üye(Member)

e-imzalıdır
Prof. Dr. Ejder OKUMUŞ
Üye(Member)

Belge Takip Adresi : [illegible]

ÖZGEÇMİŞ

Adı: Soyadı : Emine İPEK DİNÇER

Doğum Tarihi :

Doğum Yeri :

Lise :

Lisans :

Yüksek Lisans :

Çalıştığı Kurum (lar) :