TÜRK STANDARDI

TURKISH STANDARD

TS ISO 31000

Aralık 2011

ICS 03.100.01

RİSK YÖNETİMİ - PRENSİPLER VE KILAVUZLAR

Risk Management - Principles and guidelines

TÜRK STANDARDLARI ENSTİTÜSÜ
Necatibey Caddesi No.112 Bakanlıklar/ANKARA

- Bugünkü teknik ve uygulamaya dayanılarak hazırlanmış olan bu standardın, zamanla ortaya çıkacak gelişme ve değişikliklere uydurulması mümkün olduğundan ilgililerin yayınları izlemelerini ve standardın uygulanmasında karşılaştıkları aksaklıkları Enstitümüze iletmelerini rica ederiz.

- Bu standardı oluşturan İhtisas Grubu üyesi değerli uzmanların emeklerini; tasarılar üzerinde görüşlerini bildirmek suretiyle yardımcı olan bilim, kamu ve özel sektör kuruluşları ile kişilerin değerli katkılarını şükranla anarız.

Kalite Sistem Belgesi
İmalât ve hizmet sektörlerinde faaliyet gösteren kuruluşların sistemlerini TS EN ISO 9000 Kalite Standardlarına uygun olarak kurmaları durumunda TSE tarafından verilen belgedir.

Türk Standardlarına Uygunluk Markası (TSE Markası)
TSE Markası, üzerine veya ambalâjına konulduğu malların veya hizmetin ilgili Türk Standardına uygun olduğunu ve mamulle veya hizmetle ilgili bir problem ortaya çıktığında Türk Standardları Enstitüsü'nün garantisi altında olduğunu ifade eder.

Kritere Uygunluk Belgesi (TSEK Markası Kullanma Hakkı)
Kritere Uygunluk Belgesi; Türk Standardları bulunmayan konularda firmaların ürünlerinin ilgili uluslararası standardlar, benzeri Türk Standardları, diğer ülkelerin milli standardları, teknik literatür esas alınarak Türk Standardları Enstitüsü tarafından kabul edilen Kalite Faktör ve Değerlerine uygunluğunu belirten ve akdedilen sözleşme ile TSEK Markası kullanma hakkı verilen firma adına düzenlenen ve üzerinde TSEK Markası kullanılacak ürünlerin ticari Markası, cinsi, sınıfı, tipi ve türünü belirten geçerlilik süresi bir yıl olan belgedir.

DİKKAT!

TS işareti ve yanında yer alan sayı tek başına iken (TS 4600 gibi), mamulün Türk Standardına uygun üretildiğine dair üreticinin beyanını ifade eder. **Türk Standardları Enstitüsü tarafından herhangi bir garanti söz konusu değildir.**

Standardlar ve standardizasyon konusunda daha geniş bilgi Enstitümüzden sağlanabilir.

Ön söz

- Bu standard, ISO tarafından kabul edilen ISO 31000: 2009 standardı esas alınarak TSE Mühendislik Hizmetleri İhtisas Grubu'nca hazırlanmış ve TSE Teknik Kurulu'nun 13 Aralık 2011 tarihli toplantısında Türk Standardı olarak kabul edilerek yayımına karar verilmiştir.

- Bu standardda kullanılan bazı kelime ve/veya ifadeler patent haklarına konu olabilir. Böyle bir patent hakkının belirlenmesi durumunda TSE sorumlu tutulamaz.

İçindekiler

Risk yönetimi – Prensipler ve kılavuzlar

0 Giriş

Her türde ve büyüklükte kuruluşlar, kendi hedeflerini gerçekleştirip gerçekleştirmeyeceklerini veya nezaman gerçekleştireceklerini belirsiz kılan iç ve dış faktörler ve etkilerle karşılaşır. Bir kuruluşun hedefleri üzerindeki bu belirsizlik etkisi "risk"tir.

Bir kuruluşun bütün faaliyetleri risk içerir. Kuruluşlar, riski belirleyerek, analiz ederek ve daha sonra risk kriterlerini sağlamak için risk iyileştirmesi yoluyla riski değiştirip değiştirmeyeceğini değerlendirerek yönetir. Bu süreç boyunca, paydaşlarıyla iletişim kurar ve onlara danışır ve daha fazla risk iyileştirmesi gerekmeyeceğinden emin olmak için riski değiştiren kontrolleri ve riski izler ve gözden geçirir. Bu standard, bu sistematik ve mantıksal süreci ayrıntısıyla açıklar.

Bütün kuruluşlar riski bir dereceye kadar yönetirken, bu standard risk yönetimini etkili kılmak için sağlanması gereken pek çok sayıdaki prensibi tesis eder. Bu standard kuruluşların, kuruluşun toplam idaresi, strateji ve planlaması, yönetimi, rapor verme süreçleri, politikaları, değerleri ve kültürü doğrultusunda risk yönetimi ile ilgili süreci bütünleştirmek amaçlı bir çerçeve geliştirmesini, tesis etmesini ve sürekli olarak iyileştirmesini tavsiye eder.

Risk yönetimi, pek çok alanlarında ve seviyelerinde, herhangi bir zamanda, bütün bir kuruluşa ve aynı zamanda belli işlevlerine, projelere ve faaliyetlere uygulanabilir.

Risk yönetiminin uygulaması, yaygın ihtiyaçları karşılamak için zaman boyunca ve pek çok sektör içinde geliştirilmiş olmakla birlikte, kapsamlı bir çerçeve içinde tutarlı süreçlerin kabulü, riskin bir kuruluş çapında etkili bir şekilde, verimli olarak ve tutarlı olarak yönetilmesini temin etmede yardımcı olabilir. Bu standardda açıklanan genel yaklaşım, herhangi bir biçimdeki riski sistematik bir biçimde, saydam ve inanılır şekilde ve kapsam ve bağlam içinde yönetmek için prensipler ve kılavuzlar sağlar.

Her bir özel sektör veya risk yönetimi uygulaması kendisine ait ihtiyaçlar, izleyiciler, algılamalar ve kriterler ile gelir. Bu nedenle, bu standardın kilit özelliği "bağlam oluşturma"nın bu genel risk yönetim sürecinin başlangıcındaki bir faaliyet olarak içerilmesidir. Bu bağlamın oluşturulması kuruluşun hedeflerini, bu hedeflerin takip edildiği ortamı, paydaşlarını ve risk kriterlerinin yaygınlığını ele geçirecektir. Bunların tümü kendi risklerinin doğası ve karmaşıklığını açığa çıkarmada ve takdir etmede yardımcı olacaktır.

Riskin yönetimiyle ilgili prensipler, oluştuğu çerçeve ve bu standardda açıklanan risk yönetim süreci arasındaki ilişkiler Şekil 1'de gösterilmiştir.

Bu standarda göre tesis edildiğinde ve idame ettirildiğinde, risk yönetimi bir kuruluşun aşağıdakileri sağlamasını mümkün kılar:

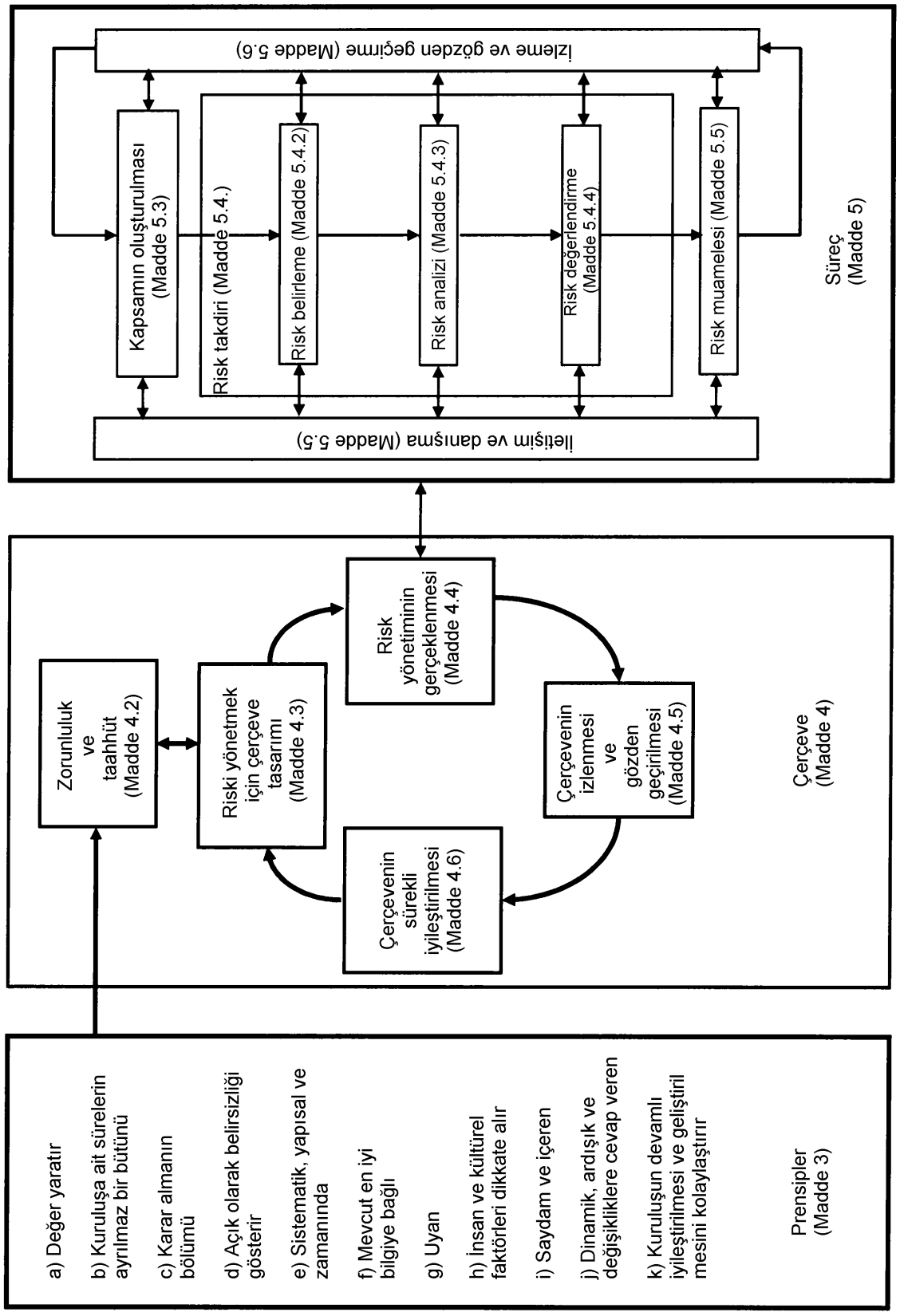
- Hedefleri gerçekleştirme ihtimalini artırma,
- Proaktif yönetimi cesaretlendirme,
- Kuruluş çapında riski belirleme ve muamele etme ihtiyacından haberdar olma,
- Fırsatlar ve tehditlerin belirlenmesini iyileştirme,
- İlgili yasal ve mevzuatla ilgili şartlara ve uluslararası normlara uyum sağlama,
- İdare etmeyi iyileştirme,
- Paydaş güvenini ve itimadını iyileştirme,
- Karar verme ve planlama ile ilgili güvenilir bir temel tesis etme,
- Kontrolleri iyileştirme,
- Risk iyileştirmesi için kaynakları etkili bir şekilde tahsis etme ve kullanma,
- Operasyonel etkinliği ve verimliliği iyileştirme,
- Sağlık ve güvenlik performansını ve aynı zamanda çevresel korumayı geliştirme,
- Kaybın önlenmesi ve kaza yönetimini iyileştirme,
- Kayıpları en aza indirme,
- Kuruluşa ait öğrenmeyi iyileştirme ve
- Kuruluşa ait esnekliği iyileştirme.

Bu standard geniş bir aralıktaki paydaşların ihtiyaçlarını karşılamayı amaçlar. Bunlar:

a) Kendi kuruluşları içinde risk yönetim politikası geliştirme sorumluluğu olanlar,
b) Riskin kuruluş içinde bir bütün olarak veya belli bir alan, proje veya faaliyet içinde etkili bir şekilde yönetimini temin için sorumlu olanlar,
c) Risk yönetmede bir kuruluşun etkinliğini değerlendirmek için ihtiyacı olanlar,
d) Bu dokümanların belli kapsamı içinde riskin nasıl yönetileceğini bütün veya bölüm olarak veya belirleyen standardlar, kılavuzlar, işlemler ve uygulama kodları hazırlayanlar.

Pek çok kuruluşun mevcut yönetim uygulamaları ve süreçleri risk yönetiminin bileşenlerini içerir ve pek çok kuruluş hali hazırda özel risk türleri veya durumlar ile ilgili resmi bir risk yönetim sürecini kabul etmektedir. Bu tür durumlarda, bir kuruluş bu standard ışığında kendi mevcut uygulamaları ve süreçlerinin kritik bir gözden geçirmesini yapmak için karar verebilir.

Bu standardda, “risk yönetimi” ve “ riski yönetme” ifadelerinin her ikisi de kullanılır. Genel terimlerle, “risk yönetimi” riskleri etkili bir şekilde yönetmeyle ilgili mimariyi (ilkeler, çerçeve ve süreç) ima eder, “riski yönetme” ise, mimarinin özel risklere uygulanması anlamına gelir.



Şekil 1 – Risk yönetim ilkeleri, çerçeve ve süreç arasındaki ilişkiler

1 Kapsam

Bu standard, risk yönetimi hakkında ilkeleri ve genel ana hatları kapsar.

Bu standard, herhangi bir kamu, özel veya ortaklık girişimi, ortaklık, grup veya birey tarafından kullanılabilir. Bu nedenle, bu standard herhangi bir sanayi veya sektöre özgü değildir.

Not – Uygunluk açısından, bu standardın bütün farklı kullanıcıları genel terim "kuruluş" olarak adlandırılır.

Bu standard, bir kuruluşun ömrü boyunca ve stratejiler ile kararlar, operasyonlar, işlevler, projeler, ürünler, hizmetler ve tesisler dâhil, çok çeşitli faaliyetlerine uygulanabilir.

Bu standard, doğası ne olursa olsun, ister pozitif veya negatif sonuçlara sahip olsun, herhangi bir risk türüne uygulanabilir.

Bu standard, genel ana hatları verse de, kuruluşlar çapında riskin tekdüzeliğini sağlamayı amaçlamaz. Risk yönetimi plan ve çerçevelerinin tasarımı ve gerçeklenmesi özel bir kuruluşun değişen ihtiyaçlarını, onun özel hedeflerini, kapsamı, yapıyı, operasyonları, süreçleri, işlevleri, projeleri, ürünleri, hizmetleri, veya tesisleri ve kullanılan özel uygulamaları dikkate alma ihtiyacındadır.

Bu standardın mevcut ve gelecekteki standardlardaki risk yönetim süreçlerini harmonize etmek için kullanılması amaçlanmıştır. Özel riskler ve/veya sektörlerle ilgilenen standardların desteğinde genel bir yaklaşım sağlar, ancak bu standardların yerini almaz.

Bu standard sertifikasyon amaçlı değildir.

2 Terimler ve tarifler

Bu standardın amacı bakımından aşağıdaki terimler ve tarifler uygulanır.

2.1 Risk

Hedefler üzerindeki belirsizlik etkisi.

Not 1 - Bir etki beklenenden bir sapmadır (pozitif ve/veya negatif).

Not 2 - Hedefler farklı hususlara sahiptir (örneğin finansal, sağlık ve güvenlik, çevresel amaçlar) ve farklı seviyelerde uygulanır (örneğin stratejik, kuruluş çapında, proje, ürün ve süreç gibi).

Not 3 - Risk genellikle muhtemel olaylar (Madde 2.17) ve sonuçlara (Madde 2.18) göre veya bunların bir birleşimine göre karakterize edilir.

Not 4 - Risk genellikle bir olayın sonuçlarının (şartlardaki değişiklikler dahil) ve karşılık gelen olma ihtimalinin (Madde 2.19) bir birleşimi cinsinden ifade edilir.

Not 5 - Belirsizlik, kısmî de olsa, bir olayın, sonuçlarının veya ihtimalinin anlaşılması veya bilinmesine ilişkin bilgi eksikliği durumudur.

[ISO Guide 73: 2009, tarif 1.1]

2.2 Risk yönetimi

Riske (Madde 2.1) ilişkin olarak bir kuruluşun yönlendirilmesi ve kontrolü için koordineli faaliyetler.

[ISO Guide 73: 2009, tarif 2.1]

2.3 Risk yönetimi çerçevesi

Kuruluş çapında risk yönetimini (Madde 2.2) tasarımlama, gerçekleme, izleme (Madde 2.28), gözden geçirme ve sürekli olarak iyileştirme ile ilgili temel yapılar ve kuruluşa ilişkin düzenlemeleri sağlayan bileşenler kümesi.

Not 1 – Temel yapılar riski (Madde 2.1) yönetmek için politika, hedefler, yetki ve taahhütü içerir.

Not 2 – Kuruluşa ilişkin düzenlemeler planları, ilişkileri, sorumlulukları, kaynakları, süreçleri ve faaliyetleri içerir.

Not 3 – Risk yönetim çerçevesi kuruluşun toplam stratejik ve operasyonel politikaları ve uygulamaları içine oturtulur.

[ISO Guide 73:2009, tarif 2.1.1]

2.4 Risk yönetimi politikası
Risk yönetimi (Madde 2.2) ilişkin olarak bir kuruluşun toplam amaçları ve yönlendirilmesi ile ilgili beyanı.

[ISO Guide 73: 2009, tarif 2.1.2]

2.5 Risk tutumu
Kuruluşun riski (Madde 2.1) değerlendirmek ve sonuçta takip etmek, sürdürmek, almak ve ondan kaçınmak ile ilgili yaklaşımı.

[ISO Guide 73:2009, tarif 3.7.1.1]

2.6 Risk yönetim planı
Riskin (Madde 2.1) yönetimine uygulanan yaklaşımı, yönetim bileşenlerini ve kaynakları belirleyen risk yönetim çerçevesi (Madde 2.3) içindeki şema.

Not 1 – Yönetim bileşenleri tipik olarak işlemleri, uygulamaları, sorumlulukların dağıtımını, faaliyetlerin sırası ve zamanlamasını içerir.

Not 2 – Risk yönetim planı özel bir ürüne, sürece ve projeye ve kısmen veya bütün olarak kuruluşa uygulanabilir.

[ISO Guide 73: 2009, tarif 2.1.3]

2.7 Risk sahibi
Bir riski (Madde 2.1) yönetmek için sorumluluk ve yetki sahibi kişi veya birim.

[ISO Guide 73:2009, tarif 3.5.1.5]

2.8 Risk yönetim süreci
Yönetim politikaları, işlemleri ve uygulamalarının iletişim, istişare, kapsam oluşturma faaliyetlerine uygulanması ve riski (Madde 2.1) belirleyen, analiz eden, değerlendiren, iyileştirmeye tabi tutan, izleyen (Madde 2.28) ve gözden geçiren sistematik uygulama.

[ISO Guide 73: 2009, tarif 3.1]

2.9 Kapsam oluşturma
Risk yönetim politikası (Madde 2.4) için riski yönetirken ve kapsam ve risk kriterlerini (Madde 2.22) oluştururken dikkate alınacak dış ve iç parametreleri tanımlama.

[ISO Guide 73:2009, tarif 3.3.1]

2.10 Dış kapsam
İçinde kuruluşun hedeflerini gerçekleştirmek için aradığı dış ortam.

Not – Dış ortam aşağıdakileri içerebilir:

- Uluslararası, ulusal, bölgesel veya yerel olmak üzere kültürel, sosyal, politik, yasal, mevzuata ait, finansal, teknolojik, ekonomik, doğal ve rekabetçi ortam.
- Kuruluşun hedefleri üzerinde etkisi olan kilit sürücüler ve eğilimler.
- Dış paydaşlarla (Madde 2.13) ilişkiler ve onların algılamaları ve değerleri.

[ISO Guide 73: 2009, tarif 3.3.1.1]

2.11 İç kapsam
İçinde kuruluşun hedeflerini gerçekleştirmek için aradığı iç ortam.

Not – Dış ortam aşağıdakileri içerebilir:

- İdare, kuruluşa ait yapı, roller ve sorumlulukları.
- Gerçekleştirilmek üzere yerlerinde olan politikalar, hedefler ve stratejiler.

- Kaynaklar ve bilgi birikimi açısından anlaşılan yetenekler (örneğin, anapara, zaman, kişiler, süreçler, sistemler ve teknolojiler).
- Bilgi sistemleri, bilgi akışı ve karar alma süreçleri (resmi ve resmi olmayan).
- İç paydaşlarla ilişkiler ve onların algılamaları ve değerleri.
- Kuruluşun kültürü.
- Kuruluş tarafından kabul edilen standardlar, kılavuzlar ve modeller.
- Sözleşme ile ilgili ilişkilerin biçimi ve kapsamı.

[ISO Guide 73: 2009, tarif 3.3.1.2]

2.12 İletişim ve istişare

Bir kuruluşun, bilgi sağlamak, paylaşmak ve elde etmek ve riskin (Madde 2.1) yönetimine ilişkin olarak paydaşlar (Madde 2.13) ile diyalog kurmak için icra ettiği sürekli ve ardışık süreçler.

Not 1 - Bilgi, riskin yönetiminin varlığı, doğası, biçimi, ihtimali (Madde 2.19), önemi, değerlendirmesi, kabul edilebilirliği ve azaltılması ile ilgili olabilir.

Not 2 - İstişare, bir karar almadan önce veya bir yön belirlemeden önce bir husus hakkında bir kuruluş ile onun paydaşları arasındaki iki yönlü bir bilgilendirme iletişimi sürecidir. İstişare:

- Güçten ziyade etki vasıtasıyla bir karar üzerinde etkisi olan bir süreçtir,
- Müşterek karar alma haricinde, karar almak için bir girdidir.

[ISO Guide 73:2009, tarif 3.2.1]

2.13 Paydaş

Bir karar veya faaliyet tarafından kendilerinin etkilendiğini algılayabilen veya etkilenebilen veya kararı etkileyebilen kişi veya kuruluş.

Not – Bir karar alıcı bir paydaş olabilir.

[ISO Guide 73:2009, tarif 3.2.1.1]

2.14 Risk değerlendirme

Risk tanımlama (Madde 2.15), risk analizi (Madde 2.21) ve risk değerleme (Madde 2.24) ile ilgili toplam süreç.

[ISO Guide 73:2009, tarif 3.4.1]

2.15 Risk tanımlama

Riskleri (Madde 2.1) bulma, tanıma ve açıklama süreci.

Not 1 - Risk tanımlama risk kaynaklarının (Madde 2.16), olayların (Madde 2ç17), bunların nedenleri ve muhtemel sonuçlarının (Madde 2.18) belirlenmesini gerektirir.

Not 2 - Risk tanımlama, tarihi veri, teorik analiz, bilgilendirilmiş ve uzman fikirleri ve paydaşların (Madde 2.13) ihtiyaçlarını gerektirir.

[ISO Guide 73:2009, tarif 3.5.1]

2.16 Risk kaynağı

Tek başına veya birleşik olarak doğasında riske (Madde 2.1) sebep olma ihtimali olan eleman.

Not – Bir risk kaynağı somut veya soyut olabilir.

[ISO Guide 73:2009, tarif 3.5.1.2]

2.17 Olay

Özel bir durumlar kümesinin oluşu veya değişimi.

Not 1 – Bir olay bir veya daha fazla oluştan meydana gelebilir ve birkaç sebebe sahip olabilir.

Not 2 – Bir olay oluşmayan bir şeyden ibaret olabilir.

Not 3 – Bir olay bazen bir "tesadüf" veya "kaza" olarak adlandırılabilir.

Not 4 - Sonuçları (Madde 2.18) olmayan bir olay "hemen hemen kaçan", "tesadüfi", "hemen hemen vuran" veya "çağrıya yakın" olarak da adlandırılabilir.

[ISO Guide 73: 2009, tarif 3.5.1.3]

2.18 Sonuç

Bir olayın (Madde 2.17) hedeflere etki eden çıktısı.

Not 1 – Bir olay geniş bir aralıkta sonuçlara yol açabilir.

Not 2 – Bir sonuç belli veya belirsiz olabilir ve hedefler üzerinde olumlu veya olumsuz etkileri olabilir.

Not 3 – Sonuçlar nicel veya nitel olarak ifade edilebilir.

Not 4 – İlk sonuçlar zincirleme etkiler yoluyla artabilir.

[ISO Guide 73:2009, tarif 3.6.1.3]

2.19 İhtimal

Bir şeyin olma şansı.

Not 1 - Risk yönetimi terminolojisinde "ihtimal" kelimesi; tanımlanan, ölçülen veya objektif veya subjektif olarak, nicel veya nitel olarak belirlenen ve genel terimler kullanılarak veya matematiksel olarak (örneğin verilen bir zaman periyodu içinde olasılık veya bir frekans gibi) açıklanan bir şeyin olma şansını belirtmek için kullanılır.

Not 2 - İngilizce terim olan "likelihood" (ihtimal) bazı dillerde doğrudan eşdeğeri olan bir kelime değildir. Onun yerine "probability" (olasılık) teriminin eşdeğeri sıklıkla kullanılır. Bununla birlikte, İngilizcede "probability" (olasılık) genellikle dar anlamda matematiksel bir terim olarak ifade edilir. Bu nedenle, risk yönetimi terminolojisinde "likelihood" (ihtimal) terimi, İngilizce dışındaki pek çok diğer dilde "probability" (olasılık) terimi gibi geniş anlama sahip olması gerektiği amacıyla kullanılır.

[ISO Guide 73:2009, tarif 3.6.1.1]

2.20 Risk profili

Herhangi bir riskler (Madde 2.1) kümesi tarifi.

Not - Riskler kümesi bütün kuruluşa, kuruluşun bir bölümüne veya başkaca belirlendiği şekliyle riskleri ihtiva edebilir.

[ISO Guide 73:2009, tarif 3.8.2.5]

2.21 Risk analizi

Riskin (Madde 2.1) doğasını anlama ve risk seviyesini (Madde 2.23) belirleme süreci.

Not 1 - Risk analizi risk değerlendirmesi (Madde 2.24) ve risk iyileştirmesi (Madde 2.25) hakkında kararlar için temel teşkil eder.

Not 2 - Risk analizi risk kestirimini içerir.

[ISO Guide 73:2009, tarif 3.6.1]

2.22 Risk kriterleri

Bir riskin (Madde 2.1) öneminin değerlendirildiği görev tanımı

Not 1 – Risk kriterleri kuruluşun hedeflerini, dış (Madde 2..10) ve iç kapsamını (Madde 2.11) esas alır.

Not 2 – Risk kriterleri standardlar, kanunlar, politikalar ve diğer şartlardan türetülebilir.

[ISO Guide 73:2009, tarif 3.3.1.3]

2.23 Risk seviyesi
Sonuçların (Madde 2.18) ve onların ihtimalinin (Madde 2.19) birleşimi cinsinden ifade edilen, bir riskin (Madde 2.1) büyüklüğü veya risklerin birleşimi.

[ISO Guide 73:2009, tarif 3.6.1.8]

2.24 Risk değerleme
Riskin (Madde 2.1) ve/veya onun büyüklüğünün kabul edilebilir veya tahammül edilebilir olup olmadığını belirlemek için risk analizi (Madde 2.21) sonuçlarının risk kriterleri (Madde 2.22) ile kıyaslanması süreci.

Not – Risk değerlemesi, risk iyileştirme (Madde 2.25) hakkında karara yardımcı olur.

[ISO Guide 73:2009, tarif 3.7.1]

2.25 Risk iyileştirme
Riski (Madde 2.1) değiştirme süreci.

Not 1 – Risk iyileştirme aşağıdakileri gerektirebilir:

- Riske neden olan faaliyete başlamama veya devam etmeme karar vererek riskten kaçınma,
- Bir fırsatı takip etmek için risk alma veya artırma,
- Risk kaynağını (Madde 2.16) ortadan kaldırma,
- İhtimali (Madde 2.19) değiştirme,
- Sonuçları (Madde 2.18) değiştirme,
- Riski diğer taraf veya taraflarla paylaşma (sözleşmeleri ve risk finansı dahil) ve
- Bilgilendirilmiş kararla riski sürdürme.

Not 2 – Negatif sonuçlarla uğraşan risk iyileştirme işlemi bazen “riski yumuşatma”, “riski ortadan kaldırma”, “riski önleme” ve “riski azaltma” olarak adlandırılır.

Not 3 – Risk iyileştirmesi yeni riskler yaratabilir veya varolan riskleri değiştirebilir.

[ISO Guide 73:2009, tarif 3.8.1]

2.26 Kontrol
Riski (Madde 2.1) değiştirme ölçüsü.

Not 1 – Kontroller riski değiştiren süreç, düzen, uygulama veya başka faaliyetleri içerir.

Not 2 – Kontroller her zaman amaçlanan veya varsayılan etkiyi uygulamayabilir.

[ISO Guide 73:2009, tarif 3.8.1.1]

2.27 Artık risk
Risk iyileştirmesinden (Madde 2.25) sonra geriye kalan risk (Madde 2.1).

Not 1 – Artık risk belirlenemeyen riski içerir.

Not 2 – Artık risk “muhafaza edilen risk” olarak da bilinir.

[ISO Guide 73:2009, tarif 3.8.1.6]

2.28 İzleme
Gereken veya beklenen performans seviyesinden değişimi belirlemek için durumun sürekli kontrolü, yönetilmesi, kritik olarak izlenmesi veya belirlenmesi.

Not – İzleme bir risk yönetimi çerçevesine (Madde 2.3), risk yönetim sürecine (Madde 2.8), riske (Madde 2.1) veya kontrole (Madde 2.26) uygulanabilir.

[ISO Guide 73:2009, tarif 3.8.2.1]

2.29 Gözden geçirme

Oluşturulan hedefleri gerçekleştirmek için konunun uygunluğunu, yeterliliğini ve etkinliğini belirlemek için yapılan faaliyet.

Not – Gözden geçirme bir risk yönetimi çerçevesine (Madde 2.3), risk yönetim sürecine (Madde 2.8), riske (Madde 2.1) veya kontrole (Madde 2.26) uygulanabilir.

[ISO Guide 73:2009, tarif 3.8.2.2]

3 Prensipler

Risk yönetiminin etkili olması için, bir kuruluş her seviyede aşağıdaki prensiplere uyumlu olmalıdır.

a) Risk yönetimi değer yaratır ve korur.

Risk yönetimi, örnek olarak, insan sağlığı ve selameti, güvenliği, yasal ve mevzuatla ilgili uygunluğu, genel kabulü, çevresel korumayı, ürün kalitesini, proje yönetimini, operasyonların verimliliğini idare ve tanınmışlığı içine alan hedeflerin gösterilebilir gerçeklemelerine ve perfromans iyileştirmelerine katkıda bulunur.

b) Risk yönetimi kuruluşla ilgili bütün süreçlerin ayrılmaz bir bütünüdür.

Risk yönetimi, kuruluşun ana faaliyetleri ve süreçlerinden ayrı tek başına bir faaliyet değildir. Risk yönetimi yönetimin sorumluluklarının bir bölümüdür ve stratejik planlama ve her proje ve değişme yönetimi süreçleri dahil kuruluşa ait bütün süreçlerin ayrılmaz bir bütünüdür.

c) Risk yönetimi karar almanın bir bölümüdür.

Risk yönetimi, karar alıcıların bilgilendirilmiş seçimler yapmalarına, faaliyetleri önceliklendirmelerine ve alternatif faaliyet planları arasında seçiciliklerine yardımcı olur.

d) Risk yönetimi açık olarak belirsizliği belirtir.

Risk yönetimi açık olarak belirsizliği, bu belirsizliğin doğasını ve onun nasıl belirtileceğini dikkate alır.

e) Risk yönetimi sistematik, yapısal ve zamanındadır.

Risk yönetimine sistematik, zamanında ve yapısal bir yaklaşım verimliliğe ve tutarlı, kıyaslamalı ve güvenilir sonuçlara katkıda bulunur.

f) Risk yönetimi mevcut en iyi bilgiyi esas alır.

Riski yönetme sürecine ilişkin girdiler tarihi veri, tecrübe, paydaş geribeslemesi, gözlem, öngörü ve uzman yargısı gibi bilgi kaynaklarına dayanır. Bununla birlikte, karar alıcılar verilerin herhangi sınırlamaları veya kullanılan modellemesi veya uzmanlar arasında farklılıkların ihtimalini dikkate almalı ve bunlar hakkında kendilerini bilgilendirmelidir.

g) Risk yönetimi biçimseldir.

Risk yönetimi kuruluşun iç ve dış kapsam ve risk profili ile ayarlanır.

h) Risk yönetimi insan ve kültürel faktörleri dikkate alır.

Risk yönetimi, kuruluşun hedeflerinin gerçeklemelerini kolaylaştırabilen veya engelleyebilen dış ve iç kişilerin yetenekleri, algılamaları ve niyetlerini tanır.

i) Risk yönetimi saydamdır ve içseldir.

Kuruluşun her seviyesinde paydaşların ve özelde karar alıcıların uygun ve zamanında girişimi, risk yönetiminin ilgili ve güncel kalmasını temin eder. Girişim aynı zamanda paydaşların uygun şekilde temsil edilmesine ve risk kriterlerini belirlemede onların görüşlerinin dikkate alınmasına izin verir.

j) Risk yönetimi dinamiktir, ardışıktır ve değişime tepkilidir.

Risk yönetimi, değişikliği sezer ve tepki gösterir. Dış ve iç olaylar vukuu bulduğunda, kapsam ve bilgi birikimi değiştiğinde, risklerin izlenmesi ve gözden geçirilmesi oluştuğunda, yeni riskler ortaya çıktığında, bazısı değişir ve diğerleri ortadan kaybolur.

k) Risk yönetimi kuruluşun sürekli olarak iyileştirilmesini kolaylaştırır.

Kuruluşlar, kendi kuruluşunun bütün diğer hususları çerçevesinde kendi risk yönetim olgunluğunu iyileştirmek için stratejiler geliştirmeli ve tesis etmelidir.

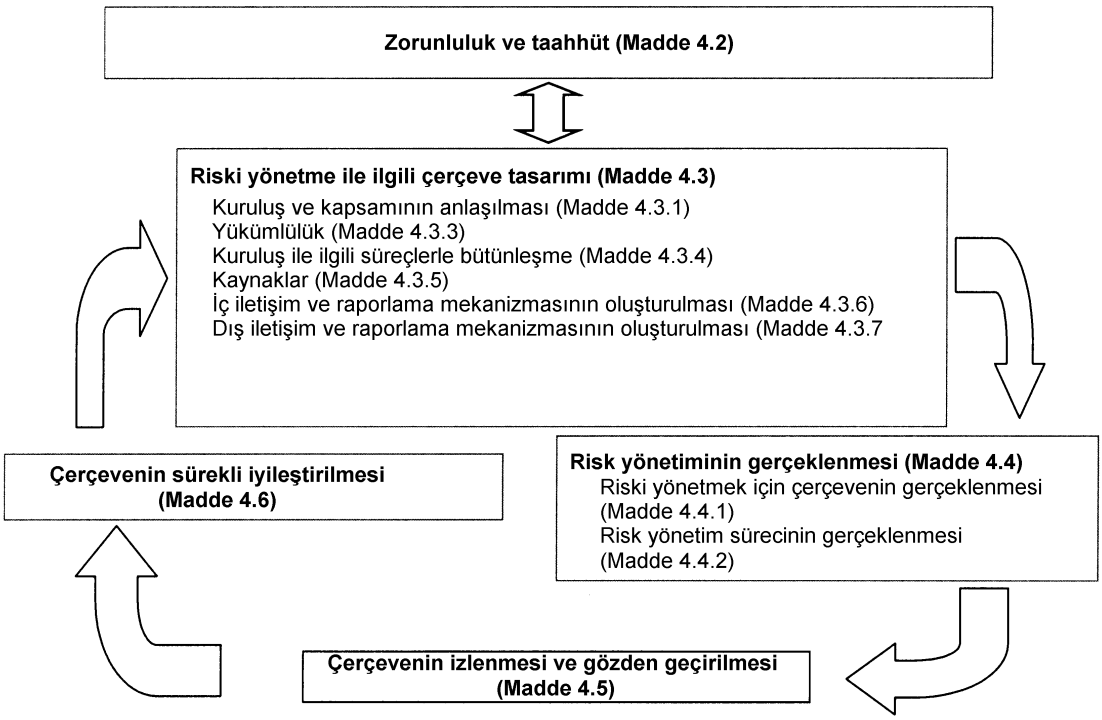
Ek A, riski daha etkili bir şekilde yönetmek isteyen kuruluşlar için daha fazla öneri sunar.

4 Çerçeve

4.1 Genel

Risk yönetiminin başarısı, her seviyede kuruluş çapında yerleştirilecek altyapılar ve düzenlemeler sağlayan yönetim çerçevesinin etkinliğine bağlı olacaktır. Bu çerçeve değişen seviyelerde ve kuruluşun belli kapsamları içinde risk yönetim sürecinin (Madde 5) uygulanması boyunca etkili bir şekilde riski yönetmede yardımcı olur. Bu çerçeve, risk yönetim sürecinin bütün ilgili kuruluş seviyelerinde karar almak ve sorumluluk için bir temel olarak kullanılmasından ve yeterli bir şekilde rapor edilmesinden türetilen risk hakkında bilgi temin eder.

Bu madde, Şekil 2'de gösterildiği gibi, riski yönetmek ve ardışık bir biçimde ilişkişli olduğu yol için gerekli çerçeve bileşenlerini açıklar.



Şekil 2 – Riski yönetmek için çerçevenin bileşenleri arasındaki ilişki

Bu çerçeve, bir yönetim sistemini açıklamayı amaçlamaz, bunun yerine kuruluşun risk yönetimini kendi bütün yönetim sistemi içine bütünleştirmesine yardımcı olur. Bu nedenle, kuruluşlar çerçeve bileşenlerini kendilerine özgü ihtiyaçlara uyarlamalıdır.

Bir kuruluşun varolan yönetim uygulamaları ve süreçlerinin risk yönetiminin bileşenlerini içermesi durumunda ve kuruluşun özel risk türleri veya durumları ile ilgili resmi bir risk yönetim sürecini halihazırda kabul etmesi durumunda, bunların yeterliliği ve etkinliğini belirlemek için, Ek A'da içerilen özellikleri dâhil, bunlar kritik bir şekilde gözden geçirilmeli ve bu standarda göre değerlendirilmelidir.

4.2 Vekâlet ve taahhüt

Risk yönetiminin konulması ve süregelen etkinliğinin temini, her seviyedeki taahhütü yerine getirmek için stratejik ve özenli planlamanın yanı sıra, kuruluşun yönetimi tarafından kuvvetli ve sürdürülebilir taahhüdü gerektirir. Yönetim aşağıdakileri içermelidir:

- Risk yönetim politikası tanımlanmalı ve onaylanmalıdır,
- Kuruluşun kültürü ve risk yönetim politikasının uyumlu olmasını temin etmelidir,
- Kuruluşun performans göstergeleri ile uyumlu olan risk yönetimi performans göstergeleri belirlenmelidir,
- Risk yönetim hedefleri kuruluşun hedefleri ve stratejileri ile uyumlu hale getirilmelidir,
- Yasal ve mevzuatla ilgili uygunluk temin edilmelidir,
- Kuruluş içinde yükümlülükler ve sorumluluklar uygun seviyelerde tahsis edilmelidir,
- Risk yönetimine gerekli kaynakların tahsis edildiği temin edilmelidir,
- Risk yönetiminin faydaları bütün paydaşlara aktarılmalıdır ve
- Riski yönetme ile ilgili çerçevenin uygun olarak devam ettiği temin edilmelidir.

4.3 Riski yönetme ile ilgili çerçevenin tasarımı

4.3.1 Kuruluşun ve kapsamının anlaşılması

Riski yönetmekle ilgili çerçevenin tasarımı ve gerçeklenmesinden önce, kuruluşun dış ve iç kapsamını değerlendirmek ve anlamak önemlidir, çünkü bunlar çerçeve tasarımını önemli ölçüde etkileyebilir.

Kuruluşun dış kapsamının değerlendirilmesi aşağıdakileri içerir, ancak bunlarla sınırlı değildir:

a) Uluslararası, ulusal, bölgesel veya yerel olmak üzere, sosyal ve kültürel, politik, yasal, mevzuata ilişkin, finansal, teknolojik, ekonomik, doğal ve rekabetçi ortam,
b) Kuruluşun hedefleri üzerinde etkisi bulunan kilit sürücüler ve eğilimler ve
c) Dış paydaşlarla ilişkiler ve onların algılamaları ve değerleri.

Kuruluşun iç kapsamının değerlendirilmesi aşağıdakileri içerir, ancak bunlarla sınırlı değildir:

- İdare, kuruluş yapısı, roller ve yükümlülükler,
- Yerine getirilecek politikalar, hedefler ve stratejiler,
- Kaynaklar ve bilgi birikimi cinsinden anlaşılan yetenekler (örneğin, anapara, zaman, kişiler, süreçler, sistemler ve teknolojiler),
- Bilgi sistemleri, bilgi akışı ve karar alma süreçleri (resmi ve gayrı resmi),
- İç paydaşlarla ilişkiler ve onların algılamaları ve değerleri,
- Kuruluşun kültürü,
- Kuruluş tarafından uyarlanan standardlar, kılavuzlar ve modeller ve
- Sözleşmeye ilişkin ilişkilerin biçim ve genişliği.

4.3.2 Risk yönetim politikasının oluşturulması

Risk yönetim politikası açık olarak risk yönetimine ilişkin kuruluş hedeflerini ve taahhütlerini ifade etmeli ve aşağıdakileri belirtmelidir:

- Kuruluşun riski yönetme mantığını,
- Kuruluşun hedefleri ve politikaları ile risk yönetim politikası arasındaki bağları,
- Riski yönetme ile ilgili yükümlülükler ve sorumlulukları,
- Çelişen ilgi alanları ile uğraşma biçimini,
- Riski yönetme ile ilgili yükümlülük ve sorumluluklara yardımcı olmak için gerekli kaynakların bulundurulmasının taahhüdünü,
- Risk yönetim performansının ölçülme ve raporlama biçimini ve
- Risk yönetim politikasını periyodik olarak ve bir olaya ya da durumlardaki değişikliğe göre göden geçirme ve iyileştirme taahhüdünü.

Risk yönetim politikası uygun şekilde aktarılmalıdır.

4.3.3 Yükümlülük

Kuruluş, risk yönetim sürecini gerçekleme ve muhafaza etme ve herhangi kontrollerin yeterliliğini, etkinliğini ve verimliliğini temine etme dâhil, riski yönetmekle ilgili yükümlülük, yetki ve uygun yeterliliğin bulunduğunu temin etmelidir. Bu aşağıdakilerle kolaylaştırılabilir:

- Riskleri yönetme yükümlülüğü ve yetkisi bulunan risk sahiplerinin belirlenmesi,
- Riski yönetme ile ilgili çerçevenin geliştirilmesi, gerçeklenmesi ve idamesi ile ilgili olarak kimin yükümlü olduğunun belirlenmesi,
- Risk yönetim süreci ile ilgili olarak kuruluş içinde her seviyedeki kişilerin diğer sorumluluklarının belirlenmesi,
- Performans ölçümü ve dıi ve/veya iç raporlama ve eskalasyon süreçlerinin oluşturulması ve
- Uygun seviyede algılamanın temin edilmesi.

4.3.4 Kuruluş süreçleriyle bütünleşme

Risk yönetimi, ilgili, etkili ve verimli bir biçimde, kuruluşun her uygulaması ve süreci içine yerleştirilmelidir. Risk yönetim süreci, kuruluşa ait süreçlerin bir bölümü olmalı ve onlardan ayrılmamalıdır. Özelde, risk yönetimi, politika, geliştirme, iş ve stratejik planlama ve gözden geçirme içine yerleştirilmeli ve yönetim süreçlerini değiştirmelidir.

Risk yönetim politikasının gerçeklendiği ve risk yönetiminin kuruluşun bütün uygulamaları ve süreçleri içine yerleştirildiğini temin etmek için kuruluş çapında bir risk yönetim planı olmalıdır. Risk yönetim planı, stratejik plan gİbi kuruluşun diğer planları ile bütünleştirilebilir.

4.3.5 Kaynaklar

Kuruluş, risk yönetimi ile ilgili uygun kaynakları tahsis etmelidir.

Aşağıdakilere dikkat gösterilmelidir:
- Kişiler, hünerler, tecrübe ve yeterlilik,
- Risk yönetim sürecinin her bir adımı için gerekli kaynaklar,
- Riski yönetmek için kullanılacak, kuruluşa ait süreçler, yöntemler ve aletler,
- Belgelendirilmiş süreçler ve işlemler,
- Bilgi ve bilgi birikimi yönetim sistemleri ve
- Eğitim programları.

4.3.6 İç iletişim ve raporlama mekanizmalarının oluşturulması

Kuruluş, risk yükümlülüğü ve sahipliğini desteklemek ve cesaretlendirmek için iç iletişim ve raporlama mekanizmalarını oluşturmalıdır. Bu mekanizmalar aşağıdakileri temin etmelidir:
- Risk yönetim çerçevesi ve herhangi bir müteakip değişikliğin kilit bileşenlerinin uygun şekilde iletişimini,
- Çerçeve hakkında yeterli iç raporlama bulunduğunu ve onun etkinliğini ve çıktılarını,
- Risk yönetiminin uygulanmasından ortaya çıkan ilgili bilginin uygun seviyelerde ve zamanlarda mevcut olduğunu ve
- İç paydaşlarla istişare için süreçlerini bulunduğunu.

4.3.7 Dış iletişim ve raporlama mekanizmalarının oluşturulması

Kuruluş, dış paydaşlar ile nasıl iletişimde bulunacağına dair bir plan geliştirmeli ve gerçeklemelidir. Bu aşağıdakileri gerektirir:
- Uygun dış paydaşlarla teması ve etkili bir bilgi değişiminin teminini,
- Yasal, mevzuata ilişkin ve idari ihtiyaçlarla uyumlu dış raporlamayı,
- İletişim ve istişare hakkında geribesleme ve raporlama sağlamayı,
- Kuruluş içinde güven oluşturmak için iletişimi kullanmayı ve
- Bir kriz ya da ihtiyat olayında paydaşlarla iletişimi.

Bu mekanizmalar, uygun olduğu yerlerde, çeşitli kaynaklardan risk bilgisini sağlamlaştırmak için süreçleri içermelidir. Bunlar bilginin hassasiyetini dikkate alma ihtiyacında olabilir.

4.4 Risk yönetiminin gerçeklenmesi

4.4.1 Riski yönetme ile ilgili çerçevenin gerçeklenmesi

Riski yönetme ile ilgili olarak kuruluşun çerçevesini gerçeklemede, kuruluş aşağıdakileri yapmalıdır:
- Çerçeveyi gerçekleme ile ilgili uygun zamanlama ve stratejiyi tanımlama,
- Kuruluş süreçlerine risk yönetim politikası ve sürecini uygulama,
- Yasal ve mevzuatla ilgili şartlara uyma,
- Hedeflerin geliştirilmesi ve kurulması dahil, karar almanın risk yönetim süreçlerinin çıktılarıyla uyumlu olmasını temin,
- Bilgi ve eğitim oturumlarının yapılması, ve
- Risk yönetim çerçevesinin uygun olduğunu temin için paydaşlarla iletişim ve istişare.

4.4.2 Risk yönetim sürecinin gerçeklenmesi

Risk yönetimi, Uygulamalarının ve süreçlerinin bir bölümü olarak kuruluşun bütün ilgili seviyelerinde ve işlevlerinde bir risk yönetim planı yoluyla Madde 5'te özetlenen risk yönetim sürecinin uygulanmasını temin ederek gerçeklenmelidir.

4.5 Çerçevenin izlenmesi ve gözden geçirilmesi

Kuruluşun performansını desteklemek için risk yönetiminin etkili ve sürekli olduğunu temin için, kuruluş aşağıdakileri yapmalıdır:

- Risk yönetim performansını, uygunluk açısından periyodik olarak gözden geçirilen, göstergelere göre ölçmelidir,
- Risk yönetim planına ve ondan sapmalara göre süreci periyodik olarak ölçmelidir,
- Kuruluşun dış ve iç kapsamı verildiğinde, risk yönetim çerçevesi, politikası ve planının hala uygun olup olmadığını periyodik olarak gözden geçirmelidir,
- Risk, risk yönetim planı ile ilerleme ve risk yönetim politikasının iyi bir şekilde nasıl takip edildiği hakkında rapor vermeli ve
- Risk yönetim çerçevesinin etkinliğini gözden geçirmelidir.

4.6 Çerçevenin sürekli iyileştirilmesi

İzleme ve gözden geçirmenin sonuçlarına bağlı olarak, risk yönetim çerçevesi, politika ve planının nasıl iyileştirilebileceği hakkında kararlar alınmalıdır. Bu kararlar kuruluşun riskin yönetimi ve onun yönetim kültüründe iyileştirmelere yol açmalıdır.

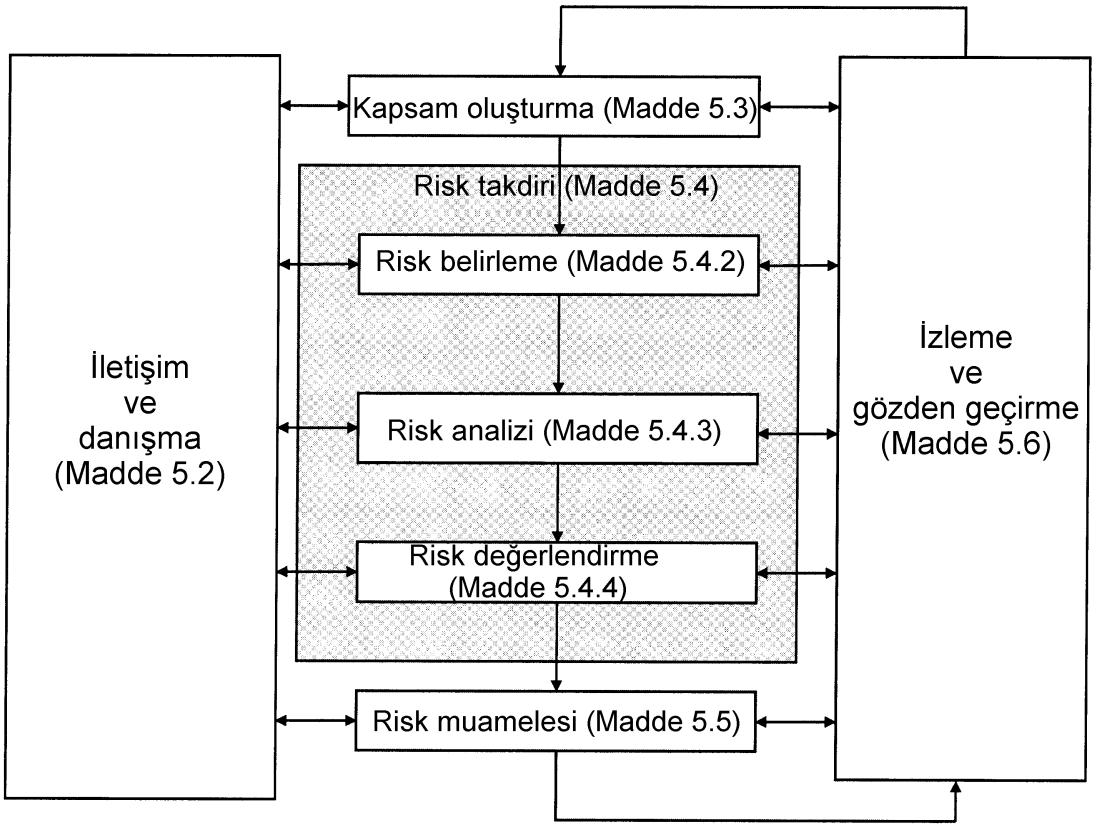
5 Süreç

5.1 Genel

Risk yönetim süreci

- Yönetimin ayrılmaz bir bütünü olmalı,
- Kültürü ve uygulamaları içine yerleştirilmeli ve
- Kuruluşun iş süreçlerine uydurulmalıdır.

Bu, Madde 5.2 ila Madde 5.6'da açıklanan faaliyetlerden oluşur. Risk yönetim süreci Şekil 3'te gösterilmiştir.



Şekil 3 – Risk yönetim süreci

5.2 İletişim ve istişare

Dış ve iç paydaşlarla iletişim ve istişare risk yönetim sürecinin her aşamasında yapılmalıdır.

Bu nedenle, iletişim ve istişare ile ilgili planlar erken bir aşamada geliştirilmelidir. Bunlar, riskin kendisine, sebeplerine ve sonuçlarına (biliniyorsa) ve onunla mücadele için alınan önlemlere ilişkin hususları belirtmelidir. Etkili dış ve iç iletişim ve istişare, risk yönetim sürecini gerçeklemekten yükümlü olanların ve paydaşların, kararların alınma temellerini ve niçin özel önlemler gerektiğini anlamalarını temin etmek için yapılmalıdır.

Bir istişare timi yaklaşımı aşağıdaki gibi olabilir:
- Kapsamı uygun şekilde oluşturmaya yardım,
- Paydaşların ilgilerinin anlaşılması ve dikkate alınmasını temin,
- Risklerin doğru bir şekilde tanındığını temine yardım,
- Riskleri analiz etmek için farklı uzmanlık alanlarını bir araya getirme,
- Risk kriterlerini tanımlarken ve riskleri değerlendirirken farklı görüşlerin uygun şekilde dikkate alındığını temin,
- Risk iyileştirme planının onaylanması ve desteklenmesi,
- Risk yönetim süreci sırasında uygun değişiklik yönetimini genişletme ve
- Uygun bir dış ve iç iletişim ve istişare planı geliştirme.

Risk algılamalarına göre risk hakkında yargıya vardıkları için paydaşlarla iletişim ve istişare önemlidir.. Bu algılamalar, değerlerde, ihtiyaçlarda, varsayımlarda, kavramlarda ve paydaşların kaygılarındaki farklılıklar nedeniyle çeşitli olabilir. Görüşleri kararların alınması üzerinde önemli bir etkiye sahip olabildiği için, paydaşların algılamaları, karar alma süreci içinde belirlenmeli, kaydedilmeli ve dikkate alınmalıdır.

İletişim ve istişare, güvenlik ve kişisel bütünlük hususlarını dikkate alarak, bilgi değişikliklerinin doğruluğu, ilgisi, hassaslığı ve anlaşılabilirliğini kolaylaştırmalıdır.

5.3 Kapsam oluşturma

5.3.1 Genel

Kapsamı oluştururken, kuruluş hedeflerini açıkça belirtir, riski yönetirken dikkate alacağı dış ve iç parametreleri tanımlar ve geri kalan süreç için kapsam ve risk kriterlerini kurar. Bu parametrelerin çoğu risk yönetim çerçevesi (Madde 4.3.1) tasarımında dikkate alınanlara benzer olmakla birlikte, risk yönetim süreci ile ilgili kapsamı oluştururken, bunların daha ayrıntılı olarak dikkate alınma ve özellikle bunların özel risk yönetim süreci kapsamıyla nasıl ilişkili olduğu ihtiyacı duyar.

5.3.2 Dış kapsam oluşturma

Dış kapsam kuruluşun hedeflerini gerçekleştirmede aradığı dış ortamdır.

Dış kapsamın anlaşılması, risk kriterlerini geliştirirken dış paydaşların hedefleri ve kaygılarını dikkate almayı temin için önemlidir. Bu, kuruluş çapında kapsama dayanır, ancak yasal ve mevzuatla ilgili şartlara ait özel ayrıntılar, paydaşların algılamaları ve risk yönetim sürecinin kapsamına özgü diğer risk hususları ile birlikte ele alınır.

Dış kapsam aşağıdakileri içerebilir, ancak bunlarla sınırlı değildir:
a) Uluslararası, ulusal, bölgesel veya yerel olmak üzere, sosyal ve kültürel, politik, yasal, mevzuata ilişkin, finansal, teknolojik, ekonomik, doğal ve rekabetçi ortam,
b) Kuruluşun hedefleri üzerinde etkisi bulunan kilit sürücüler ve eğilimler ve
c) Dış paydaşlarla ilişkiler ve onların algılamaları ve değerleri.

5.3.3 İç kapsam oluşturma

İç kapsam kuruluşun hedeflerini gerçekleştirmek için aradığı iç ortamdır.

Risk yönetim süreci kuruluşun kültürü, süreçleri, yapısı ve stratejisi ile uyumlu olmalıdır. İç kapsam kuruluşun riski yöneteceği biçimi etkileyebilen kuruluş içindeki herhangi bir şeydir. Bu oluşturulmalıdır, çünkü:
a) Risk yönetimi kuruluşun hedeflerinin kapsamında meydana gelir,
b) Özel bir proje, süreç veya faaliyetin hedefleri ve kriterleri bir bütün olarak kuruluşun hedefleri ışığında düşünülmelidir ve
c) Bazı kuruluşlar kendi stratejik, proje veya iş hedeflerini gerçekleştirmek için fırsatları tanımada başarısız olur ve bu kuruluşa ait devam eden taahhüt, inanılırlık, güven ve değeri etkiler.

İç kapsamı anlamak gereklidir. Bu aşağıdakileri içerir, ancak bunlarla sınırlı değildir:
- İdare, kuruluşa ilişkin yapı, roller ve yükümlülükler,
- Yerine getirilecek politikalar, hedefler ve stratejiler,
- Kaynaklar ve bilgi birikimi cinsinden anlaşılan yetenekler (örneğin, anapara, zaman, kişiler, süreçler, sistemler ve teknolojiler),
- İç paydaşlarla ilişkiler ve onların algılamaları ve değerleri,
- Kuruluşun kültürü,
- Bilgi sistemleri, bilgi akışı ve karar alma süreçleri (resmi ve gayrıresmi),
- Kuruluş tarafından uyarlanan standardlar, kılavuzlar ve modeller ve
- Sözleşmeye ilişkin ilişkilerin biçim ve genişliği.

5.3.4 Risk yönetim sürecinin kapsamını oluşturma

Kuruluşun faaliyetlerinin hedefleri, stratejileri, kapsam ve parametreleri veya risk yönetim sürecinin uygulandığı kuruluş bölümleri oluşturulmalıdır. Riskin yönetimi, risk yönetimi yapılmasında kullanılan kaynakları doğrulamak için ihtiyacın tam dikkate alınmasıyla sağlanmalıdır. Gerekli kaynaklar, sorumluluklar ve yetkiler ve muhafaza edilecek kayıtlar da belirtilmelidir.

Risk yönetim sürecinin kapsamı, kuruluşun ihtiyaçlarına göre değişir. Bu durum aşağıdakileri gerektirebilir, ancak bunlarla sınırlı değildir:
- Risk yönetimi faaliyetlerinin gaye ve hedeflerini tanımlama,
- Risk yönetim süreci içindeki sorumlulukları tanımlama,
- Özel dâhili ve hariciler dahil olmak üzere, yapılacak risk yönetim faaliyetlerinin derinliği ve genişliğinin yanı sıra kapsamını tanımlama,
- Zaman ve yer cinsinden, faaliyet, süreç, işlev, proje, ürün, hizmet veya tesisi tanımlama,
- Kuruluşun özel bir projesi, süreci veya faaliyeti ile diğer projeleri, süreçleri veya faaliyetleri arasındaki ilişkileri tanımlama,
- Risk takdir metodolojilerini tanımlama,
- Riski yönetmede performans ve etkinliğin değerlendirildiği biçimi tanımlama,
- Alınacak kararları tanımlama ve belirleme,
- Gerekli çalışmaları, bunların uzantısı ve hedefleri ve bu tür çalışmalar için gerekli kaynakları tanımlama, kapsamını veya çerçevesini oluşturma.

Bunlara ve diğer ilgili faktörlere gösterilen dikkat, uyarlanan risk yönetim yaklaşımının durumlara, kuruluşa ve onun hedeflerini gerçekleştirmeyi etkileyen risklere uygun olduğunu temin etmeye yardımcı olmalıdır.

5.3.5 Risk kriterlerini tanımlama

Kuruluş, riskin önemini değerlendirmek için kullanılacak kriterleri tanımlamalıdır. Bu kriterler kuruluşun değerlerini, hedeflerini ve kaynaklarını yansıtmalıdır. Bazı kriterler yasal ve mevzuata ilişkin şartlar ve kuruluşun katıldığı diğer şartlar tarafından zorlanabilir veya türetilebilir. Risk kriterleri kuruluşun risk yönetim politikası (Madde 4.3.2) ile tutarlı olmalı, herhangi bir risk yönetim sürecinin başlangıcında tanımlanmalı ve sürekli olarak gözden geçirilmelidir.

Risk kriterlerini belirlerken, dikkate alınacak faktörler aşağıdakileri içermelidir:
- Oluşabilen sebepler ve sonuçların doğası ve türleri ve bunların nasıl ölçüleceği,
- İhtimalin nasıl tanımlanacağı,
- İhtimalin ve/veya sonucun/sonuçların zaman çerçevesi/çerçeveleri,
- Risk seviyesinin nasıl belirleneceği,
- Paydaşların görüşleri,
- Riskin kabul edilebilir veya hoşgörülebilir olma seviyesi ve
- Çoklu risklerin birleşimlerinin dikkate alınıp alınmaması, böyleyse, hangi birleşimlerin nasıl dikkate alınacağı.

5.4 Risk değerlendirmesi

5.4.1 Genel

Risk değerlendirmesi risk belirleme, risk analizi ve risk değerlemesinin toplam sürecidir.

Not – ISO/IEC 31010 risk değerlendirmesi teknikleri hakkında kılavuz sağlar.

5.4.2 Risk tanımlama

Kuruluş risk kaynaklarını, etki alanlarını, olayları (durumlardaki değişiklikler dahil) ve bunların sebepleri ve muhtemel sonuçlarını tanımlamalıdır. Bu adımın amacı, hedeflerin gerçekleştirilmesini yaratabilen, genişleten, önleyen, bozan, hızlandıran veya geciktiren olaylara dayanan kapsamlı bir riskler listesini üretmektir. Bir fırsatı takip etmeyen riskleri tanımlamak önemlidir. Kapsamlı belirleme kritiktir, çünkü bu aşamada tanımlanmayan bir risk yapılacak daha ileri analizlerde dikkate alınmayabilecektir.

Risk tanımlama, risk kaynağı veya sebebi açık olmamasına rağmen, kaynakları kuruluşun kontrolü altında olan veya olmayan riskleri içermelidir. Risk tanımlama ardışık ve toplamsal etkiler dâhil, özel sonuçlara ait zincirleme etkilerin incelenmesini içermelidir. Risk kaynağı veya sebebi açık olsa ya da olmasa dahi, geniş bir sonuçlar aralığını da dikkate almalıdır. Ne olabileceğini belirlemenin yanı sıra, ne tür sonuçların oluşabileceğini gösteren muhtemel sebepler ve senaryoları dikkate almak gereklidir. Bütün önemli sebepler ve sonuçlar dikkate alınmalıdır.

Kuruluş, hedeflerine ve yeteneklerine ve karşılaştığı risklere uyan risk belirleme aletleri ve tekniklerini uygulamalıdır. Riskleri tanımlamada ilgili ve güncel bilgi önemlidir. Bu, mümkün olduğu yerlerde uygun altyapı bilgisi içermelidir. Riskleri, uygun bilgi birikimine sahip kişiler tanımlamalıdır.

5.4.3 Risk analizi

Risk analizi, risklerin geliştirilmesi ve anlaşılmasını gerektirir. Risk analizi, risk değerlendirmesine ve risklerin azaltılma ihtiyacı olup olmadığına dair kararlara ve en uygun risk iyileştirme stratejileri ve yöntemlerine bir girdi sağlar. Risk analizi ayrıca, seçimlerin yapılacağı kararların alınmasına ve farklı türlerde ve seviyelerde risk gerektiren seçeneklere de bir girdi sağlar.

Risk analizi, riskin sebepleri ve kaynaklarının, onların olumlu ve olumsuz sonuçlarının ve bu sonuçların oluşabilme ihtimalinin dikkate alınmasını gerektirir. Sonuçları ve ihtimali etkileyen faktörler belirlenmelidir. Risk, sonuçların ve ihtimalinin belirlenmesiyle ve diğer risk özellikleriyle analiz edilir. Bir olay çoklu sonuçlara sahip olabilir ve çoklu hedefleri etkileyebilir. Mevcut kontroller ve onların etkinlikleri ve verimlilikleri de dikkate alınmalıdır.

Sonuçların ve ihtimalin ifade biçimi ve bir risk seviyesi belirlemek için birleşim biçimi riskin türünü, mevcut bilgiyi ve risk değerlendirme çıktısının kullanılma amacını yansıtmalıdır. Bunlar ayrıca risk kriterleri ile de tutarlı olmalıdır. Ayrıca, farklı risklerin ve bunların kaynaklarının karşılıklı bağımlılıklarını dikkate almak da önemlidir.

Ön koşullar ve varsayımlar için risk seviyesinin ve duyarlılığının belirlenmesinde yeterlilik analiz sırasında dikkate alınmalı ve karar alıcılara ve uygun olduğunda diğer paydaşlara etkili bir şekilde iletilmelidir. Uzmanlar arasında fikir farklılıkları, belirsizlik, mevcudiyet, nitelik, nicelik ve devam eden ilgili bilgi veya modelleme üzerindeki sınırlama gibi faktörler belirtilmeli ve vurgulanmalıdır.

Risk analizi, riske, analizin amacına ve bilgi, veri ve kaynakların mevcudiyetine bağlı olarak, değişen ayrıntı derecelerinde ele alınabilir. Analiz, durumlara bağlı olarak nitel, yarı nicel veya nitel veya bunların bir birleşimi şeklinde olabilir.

Sonuçlar ve bunların ihtimali bir olayın veya olaylar kümesinin çıktılarının veya deneysel çalışmaların ekstrapolasyonunun veya mevcut verinin modellenmesiyle belirlenebilir. Sonuçlar somut veya soyut etkiler cinsinden ifade edilebilir. Bazı durumlarda, farklı zamanlar, yerler, gruplar veya durumlar için sonuçları ve bunların ihtimalini belirlemek için birden fazla sayısal değer veya açıklayıcı gerekir.

5.4.4 Risk değerleme

Risk değerlemenin amacı, risk analizinin sonuçlarına bağlı olarak, hakkında risklerin azaltılmasına ve iyileştirmenin gerçekleştirilmesi önceliğine gerek olduğuna karar vermede yardımcı olmaktır.

Risk değerleme, kapsam dikkate alındığında oluşturulan risk kriterleri ile analiz süreci sırasında bulunan risk seviyesini kıyaslamayı gerektirir. Bu kıyaslamaya bağlı olarak, iyileştirme gereği dikkate alınabilir.

Kararlar daha geniş risk kapsamını dikkate almalıdır ve kuruluştan başka riskten çıkar sağlayan taraflar tarafından ortaya çıkarılan risklerin toleransının dikkate alınmasını içerir. Kararlar yasal, mevzuat ve diğer şartlara göre alınmalıdır.

Bazı durumlarda, risk değerleme daha fazla analiz yapma kararına yol açabilir. Risk değerleme ayrıca varolan kontrolleri idame ettirmekten başka herhangi bir biçimde riski iyileştirmeme kararına da yol açabilir. Bu karar kuruluşun risk alışkanlığı ve oluşturulan risk kriterleri tarafından etkilenecektir.

5.5 Risk iyileştirme

5.5.1 Genel

Risk iyileştirme, riskleri değiştirme ve seçenekleri gerçekleştirme ile ilgili bir veya daha fazla seçeneği seçmeyi gerektirir.

Risk iyileştirme aşağıdaki kritik bir süreci gerektirir:
- Bir risk iyileştirmenin değerlendirilmesi,
- Artık risk seviyelerinin hoşgörülebilir olup olmadığına ilişkin karar,
- Hoşgörülebilir değilse, yeni bir risk iyileştirmesi üretme ve
- İyileştirmenin etkinliğinin değerlendirilmesi.

Risk iyileştirme seçenekleri her durumda birbirinden bağımsız veya uygun olmak zorunda değildir. Bu seçenekler aşağıdakileri içerebilir:

a) Riske yol açan faaliyetle başlamama ve devam etmeme kararıyla riskten kaçınma,
b) Bir fırsatı takip etmek için riskin alınması veya artırılması,
c) Risk kaynağını ortadan kaldırma,
d) İhtimali değiştirme,
e) Sonuçları değiştirme,
f) Başka bir taraf veya taraflarla riski paylaşma (sözleşmeler ve riski finans etme dahil) ve
g) Bilgilendirilmiş karar ile riski alıkoymak.

5.5.2 Risk iyileştirme seçeneklerinin seçimi

En uygun risk iyileştirme seçeneğini seçme, sosyal sorumluluk ve doğal ortamın korunması gibi yasal, mevzuat ve diğer şartlar ile türetilen yararlarına karşı gerçeklemenin maliyetleri ve gayretlerini dengelemeyi gerektirir. Kararlar ayrıca örnek olarak ciddi (yüksek olumsuz sonuç) fakat nadir (düşük ihtimal) riskler gibi ekonomik zeminlerde doğrulanmayan risk iyileştirmesini garanti edebilen riskleri de dikkate almalıdır.

Çok sayıda seçenek dikkate alınabilir ve münferit veya birleşik olarak uygulanabilir. Kuruluş normal olarak iyileştirme seçeneklerinin bir birleşiminin uyarlanmasından yarar sağlayabilir.

Risk iyileştirme seçeneklerini seçerken, kuruluş paydaşların değerleri ve algılamalarını ve onlarla en uygun iletişim biçimlerini dikkate almalıdır. Kuruluşta veya paydaşlarla başka bir yerde risk iyileştirme seçeneklerinin etki ettiği yerlerde, bunlar kararda işin içine sokulmalıdır.

Risk iyileştirme planı açık olarak münferit risk iyileştirmenin öncelik sırasını tanımlamalıdır.

Risk iyileştirmenin kendisi de risklere yol açabilir. Önemli bir risk, risk iyileştirme önlemlerinin başarısız olması veya etkinsizleşmesi olabilir. Önlemlerin etkili kalmasını garanti etmek için, izleme, risk iyileştirme planının ayrılmaz bir bütünü olma ihtiyacındadır.

Risk iyileştirme ayrıca takdir edilmesi, muamele edilmesi, izlenmesi ve gözden geçirilmesi ihtiyacı olan ikincil riskler de ortaya çıkarır. Bu ikincil riskler, orijinal risk gibi ve yeni bir risk olarak muamele görmeksizin aynı iyileştirme planı içine konulmalıdır.

5.5.3 Risk iyileştirme planlarının hazırlanması ve gerçeklenmesi

Risk iyileştirme planlarının amacı, seçilen iyileştirme seçeneklerinin nasıl gerçekleneceğini belgelendirmektir. İyileştirme planlarında sağlanan bilgi aşağıdakileri içermelidir:
- Kazanılacak beklenen yararlar dâhil, iyileştirme seçeneklerinin seçimi için nedenler,
- Bu planı onaylama yükümlülüğü olanlar ve bu planı gerçekleme sorumluluğu olanlar,
- Önerilen faaliyetler,
- Yedeklemeler dâhil kaynak gereksinimleri,
- Performans önlemleri ve kısıtlamalar,
- Raporlama ve izleme gereksinimleri, ve
- Zamanlama ve zaman planlaması.

İyileştirme planları kuruluşun yönetim süreçleri ile bütünleştirilmeli ve uygun paydaşlarla görüşülmelidir.

Karar alıcılar ve diğer paydaşlar risk iyileştirmeden sonra artık riskin doğası ve uzantısından haberdar olmalıdır. Artık risk belgelendirilmeli ve izlenmeli, gözden geçirilmeli ve uygun olduğunda bir daha muamele edilmelidir.

5.6 İzleme ve gözden geçirme

İzleme ve gözden geçirme risk yönetim sürecinin planlanmış bir bölümü olmalı ve düzenli kontrol ve gözlem gerektirir. Bu periyodik veya düzensiz aralıklarla olabilir.

İzleme ve gözden geçirme ile ilgili sorumluluklar açık bir şekilde tanımlanmalıdır.

Kuruluşun izleme ve gözden geçirme süreçleri aşağıdaki amaçlara yönelik olarak risk yönetiminin bütün hususlarını kapsamalıdır:
- Tasarım ve operasyonda kontrollerin etkili ve verimli olmasını temin,
- Risk takdirini iyileştirmek için daha fazla bilgi elde etme,
- Olaylar (hemen hemen kaçanlar dâhil), değişiklikler, eğilimler, başarılar ve başarısızlıklardan alınan dersler ve analiz etme,
- Risk iyileştirmeleri ve önceliklerinin yeniden gözden geçirilmesini gerektiren risk kriterleri ve riskin kendisinde değişiklikler dahil, dış ve iç kapsamdaki değişiklikleri sezme,
- Yeni ortaya çıkan riskleri belirleme.

Risk yönetim planlarını gerçeklemedeki gelişme bir performans ölçüsü sağlar. Sonuçlar, kuruluşun toplam performans yönetimine, ölçme ve dış ve iç raporlama faaliyetlerine dahil edilebilir.

İzleme ve gözden geçirmenin sonuçları kaydedilmeli ve uygun olduğunda dış ve iç raporlamaya tabi tutulmalıdır ve ayrıca risk yönetim çerçevesinin (Madde 4.5) gözden geçirilmesine ilişkin bir girdi olarak kullanılmalıdır.

5.7 Risk yönetim sürecinin kaydı

Risk yönetim faaliyetleri izlenebilir olmalıdır. Risk yönetim sürecinde, kayıtlar, tüm sürecin yanı sıra yöntemler ve aletlerde iyileştirme ile ilgili altyapıyı sunar.

Kayıtların oluşturulmasına ilişkin kararlar aşağıdakileri dikkate almalıdır:
- Kuruluşun sürekli öğrenme ile ilgili ihtiyaçları,
- Yönetim amaçlarıyla ilgili olarak tekrar kullanılan bilginin yararları,
- Kayıtları oluşturma ve muhafaza etmede gerekli olan maliyetler ve gayretler,
- Kayıtlarla ilgili yasal, mevzuat ve operasyonel ihtiyaçlar,
- Erişim yöntemi, geri alma kolaylığı ve depolama ortamı,
- Durdurma periyodu, ve
- Bilginin hassasiyeti.

Ek A
(Bilgi için)

Geliştirilmiş risk yönetiminin özellikleri

A.1 Genel

Bütün kuruluşlar, alınacak kararların kritikliği ile uyumlu risk yönetim çerçevesinin uygun performans seviyesini amaçlamalıdır. Aşağıdaki özellikler listesi riski yönetmede yüksek seviyeli bir performans seviyesi sunar. Kuruluşun, bu kriterlere göre kendi performansını ölçmede yardımcı olması için, bazı somut göstergeler her bir özellik için verilir.

A.2 Kilit çıktılar

A.2.1 Kuruluş, kendi risklerinin mevcut, doğru ve kapsamlı anlaşılırlığına sahiptir.

A.2.2 Kuruluşun riskleri kendi risk kriterleri içindedir.

A.3 Özellikler

A.3.1 Sürekli iyileştirme

Risk yönetiminin sürekli iyileştirilmesi, kuruluşa ait performans amaçları, ölçme, gözden geçirme ve süreçlerin, sistemlerin, kaynakların, yeteneklerin ve hünerlerin müteakip değişikliğinin ayarlanması vasıtasıyla vurgulanır.

Bu, kuruluşun ve bireysel yöneticinin performansının ölçüldüğü açık performans amaçlarının varlığı ile gösterilebilir. Kuruluşun performansı yayımlanabilir ve aktarılabilir. Normal olarak, en azından yıllık bir performans gözden geçirmesi olacak ve daha sonra süreçlerin bir gözden geçirilmesi ve devam eden periyod için gözden geçirilmiş performans hedeflerinin ayarı yapılacaktır.

Bu risk yönetimi performans takdiri, kuruluşun toplam performans takdirinin ve şubeler ve bireyler için ölçme sisteminin ayrılmaz bir bütünüdür.

A.3.2 Riskler ile ilgili tam yükümlülük

Geliştirilmiş risk yönetimi kapsamlı, tam olarak tanımlı ve tam olarak kabul edilen risklerle ilgili yükümlülük, kontroller ve risk iyileştirme görevleri içerir. Yükümlülüğü tam olarak kabul eden tahsis edilen bireyler uygun şekilde hünerlidir ve kontrollere bakmak, riskleri izlemek, kontrolleri iyileştirmek ve riskler ile bunların yönetimi hakkında dış ve iç paydaşlara etkili bir şekilde iletmek için yeterli kaynaklara sahiptir.

Bu, riskler, kontroller ve görevlerde tam olarak haberdar olan ve bunlardan yükümlü olan bir kuruluşun bütün üyeleri tarafından gösterilebilir. Normal olarak, bu, iş/pozisyon açıklamalarında, veritabanlarında veya bilgi sistemlerinde kaydedilecektir. Risk yönetimi rolleri, yükümlülükleri ve sorumluluklarının tarifi kuruluşun bütün indüksiyon programlarının bölümü olmalıdır.

Kuruluş yükümlü olanlara, kendi yükümlülüklerini yeterince varsaymak için yetki, zaman, eğitim, kaynaklar ve hünerler sağlayarak bu rollerini yerine getirmek için donatılmalarını temin eder.

A.3.3 Her karar almada risk yönetimi uygulaması

Kuruluş içinde her karar alma, önem ve ehemmiyeti ne olursa olsun, risklerin açık olarak dikkate alınmasını ve uygun bir dereceye kadar risk yönetiminin uygulanmasını gerektirir.

Bu, riskler hakkında açık görüşmelerin yapıldığını göstermek için toplantılar ve kararlar ile gösterilebilir. İlave olarak, risk yönetiminin bütün bileşenlerinin kuruluş içinde örneğin, anaparanın tahsisi hakkında, ana projeler hakkında ve yeniden yapılanma ve kuruluşa ait değişiklikler hakkında kararlarla ilgili olarak karar alma ile ilgili kilit süreçler içinde sunulması mümkün olmalıdır. Bu nedenlerle, etkin idare ile ilgili bir temel sağlamak için kuruluş içinde esaslı risk yönetimi görülür.

A.3.4 Sürekli iletişim

Geliştirilmiş risk yönetimi, iyi idarenin bir bölümü olarak, risk yönetim performansının kapsamlı ve sık sık raporlamasını içeren, dış ve iç paydaşlar ile sürekli iletişimi içerir.

Bu, risk yönetiminin bütünleşmiş ve esas bileşeni olarak paydaşlar ile iletişim ile gösterilir. İletişim, uygun şekilde oluşturulan ve kapsamlı risk kriterlerine göre risk iyileştirmesi ile ilgili ihtiyaç ve risk seviyesi hakkında uygun şekilde bilgilendirilmiş kararların alındığı iki yönlü bir süreç olarak görülür.

Önemli riskler hakkında ve risk yönetimi performansı hakkında kapsamlı ve sık sık dış ve iç raporlama, bir kuruluş içinde etkin idareye esaslı katkı sağlar.

A.3.5 Kuruluşun idari yapısı içinde tam bütünleşme

Risk yönetimi, hedefler hakkında belirsizliğin etkisi cinsinden risklere dikkat edilecek şekilde, kuruluşun yönetim süreçlerinin merkezi olarak görülür. İdari yapı ve süreç riskin yönetimine bağlıdır. Etkili risk yönetimi yöneticiler tarafından kuruluşun hedeflerini gerçekleştirmede elzem olarak görülür.

Bu, risklerle bağlantılı “belirsizlik” terimi kullanılarak kuruluş içinde yöneticinin dili ve yazılı önemli materyaller ile gösterilir. Bu özellik ayrıca normal olarak kuruluşun özellikle risk yönetimine ilişkin olan politika beyanında, yansıtılır. Normal olarak, bu özellik yönetici ile mülakatlar yoluyla ve onların faaliyetleri ve beyanlarının kanıtı yoluyla doğrulanacaktır.

Kaynaklar

[1] ISO Guide 73: 2009, *Risk management - Vocabulary*

[2] ISO/IEC 31010, *Risk management - Risk assessment techniques*