Türkiye Cumhuriyeti
Hazine ve Maliye Bakanlığı

KAMU KURUMSAL
RİSK YÖNETİMİ
REHBERİ

T.C. HAZİNE VE
MALİYE BAKANLIĞI

VERSİYON 1
2024

İçindekiler

SUNUŞ

Dr. İ. İlhan HATİPOĞLU
Bakan Yardımcısı

Ülkemizde kamu yönetiminin yeniden yapılandırılmasına dair yürütülen reform çalışmaları uzun yıllar öncesine dayanmakla birlikte Avrupa Birliği'ne adaylık sürecinin başlamasıyla bu alandaki çalışmalar hız kazanmıştır. 2003 yılında 1050 sayılı Muhasebe-i Umumiye Kanununun yürürlükten kaldırılması ve yerine 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanununun kabul edilmesiyle birlikte uluslararası standartlara ve Avrupa Birliği uygulamalarına uygun güçlü bir kamu mali yönetim ve kontrol sistemi oluşturulmuştur.

5018 sayılı Kanunla ülkemizde; üst politika belgelerinde belirlenen öncelikler doğrultusunda beş yıllık stratejik planların hazırlandığı, stratejik planlarda yer alan hedeflerle uyumlu olarak yıllık performans programlarının oluşturulduğu, idare bütçelerinin performans esaslı program bütçe sistemine uygun olarak hazırlandığı ve uygulandığı, iç kontrol sistemi aracılığıyla uygulamanın güvence altına alındığı bir stratejik yönetim sistemi oluşturulmuştur.

Bu sistemde, Hazine ve Maliye Bakanlığı, merkezi uyumlaştırma görevi kapsamında uluslararası standartlarla uyumlu olarak mali yönetim ve kontrol süreçlerine ilişkin standart ve yöntemler belirlemekten; kamu idareleri ise Hazine ve Maliye Bakanlığı tarafından belirlenen standartlar ve yöntemlerle uyumlu olarak iç kontrol sistemlerini oluşturmak ve uygulamaktan sorumludur.

"Kurumsal Risk Yönetimi", yukarıda belirtilen stratejik yönetim sisteminin ayrılmaz bir parçasını oluşturmakta ve bu sistemin etkin bir şekilde işlemesinde büyük önem arz etmektedir. Bu itibarla, idarelerin stratejik planlarında belirlenen amaç ve hedeflerine ulaşabilmeleri için, maruz kalabilecekleri riskleri etkin bir şekilde yönetmeleri gerekmektedir.

Bilindiği üzere, Kamu Kurumsal Risk Yönetimi Rehberinin ilk taslağı, idarelerin risk yönetimi uygulamalarına yön vermek amacıyla 2017 yılında Dünya Bankası ile yürütülen "Kamu Mali Yönetimi Reformu Uygulamalarının Desteklenmesi Projesi" kapsamında hazırlanmıştır. Takip eden dönemde söz konusu taslak rehber, mevzuatta ortaya çıkan gelişmeler ve kamu idarelerimiz tarafından iletilen görüşler çerçevesinde güncellenmiştir. 18 Ocak 2024 tarihinde OECD-SIGMA işbirliği ile Ankara'da düzenlenen çalıştayda kamu idarelerimizin Strateji Geliştirme Birim Yöneticilerine rehberin tanıtımı yapılmıştır. Akabinde ise idarelerimizin görüş ve değerlendirmeleri alınarak rehbere nihai şekli verilmiştir.

Bu rehberi hazırlayan Bakanlığımız İç Kontrol Merkezi Uyumlaştırma Dairesi çalışanlarına, rehberin geliştirilmesine katkı sağlayan kamu idarelerinin temsilcileri ile Dünya Bankası ve OECD-SIGMA yetkililerine teşekkür ediyor, kurumsal risk yönetimi uygulamalarının daha da güçlendirilmesi amacıyla hazırlanan bu rehberin tüm kamu idarelerimize faydalı olmasını diliyorum.

GİRİŞ

20. yüzyılda dünyanın farklı coğrafyalarında art arda meydana gelen krizler ve skandallar sonrasında, idareler için etkin yönetim yapısı arayışları başlamıştır. Yapılan araştırmalar ve tartışmalar neticesinde, kurumsal yönetim anlayışının oluşturulması ve belirli standartlara kavuşturularak geliştirilmesi amacıyla farklı ülkeler ve idareler tarafından çeşitli kurumsal yönetim ilkeleri yayımlanmıştır.

Kaynakların etkili, ekonomik ve verimli bir şekilde kullanılması, artan paydaş (vatandaş, çalışanlar, ilişkili idareler, sivil toplum kuruluşları vb.) beklentilerinin karşılanması, kaliteli kamu hizmeti sunulması, sürdürülebilirliğin sağlanması ve belirsizliklerin etkin yönetimi ile hedeflere ulaşabilme konusundaki güvencenin arttırılması kamu yönetiminde ön plana çıkan amaçlar arasındadır. Bu amaçlara ulaşabilmek için, performansı izlemeye ve performansı arttırmaya yönelen, şeffaflık, adillik, hesap verebilirlik ve sorumluluk ilkelerini esas alan kurumsal yönetim yaklaşımı ve uygulamaları gün geçtikçe kabul görmeye başlamıştır.

Risk yönetimi, insanlar tarafından, var oldukları günden bugüne, kendi varlıklarını tehdit eden tehlikelerin değerlendirilmesi ve söz konusu tehlikelerden korunmak için yöntemler geliştirilmesi yoluyla uygulanmıştır. İnsanlar gibi, idareler de var oldukları andan itibaren risklere maruz kalmış ve hedeflerine ulaşabilmek için bu riskleri yönetmeye çalışmıştır. İdarelerin hedeflerine ulaşmaya çalışırken maruz kalabilecekleri riskler hakkında üst yönetimin ve tüm çalışanların farkındalık sahibi olması kritik bir gereklilik olarak görülmeye başlanmıştır. Kurumsal risk yönetimi yaklaşımıyla oluşan risk bilgisi, üst yönetimin karar alma süreçlerini destekleyerek yönetim sorumluluklarını gerektiği şekilde yerine getirebilmeleri için ihtiyaç duydukları önemli bir bilgi kaynağı olmuştur.

Kurumsal risk yönetimi anlayışının gelişmesiyle birlikte, riske yönelik genel çerçeve sunan ilkelerin yer aldığı yaklaşımlar ortaya çıkmıştır. Uluslararası kurumsal risk yönetimi yaklaşımları, idarelerin risk yönetimine ilişkin izleyecekleri süreçlerde bir çerçeve yaratmak amacıyla ortaya konmuş ve zaman içinde kurumsal risk yönetiminin tanınması, uygulanması ve yaygınlaşmasında önemli bir işlev kazanmıştır.

Türkiye'de kamu yönetiminde dönüşüm ihtiyacını arttıran gelişmelerle birlikte, kurumsal yönetim yaklaşımının kamuya adapte edilmesi süreci başlamıştır. 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu; idarelerin tabi oldukları yasal düzenlemeler ile üst politika belgelerinde belirlenen stratejik amaç ve hedefler doğrultusunda kamu kaynaklarının kullanımında etkililik, ekonomiklik ve

verimlilik sağlanması ile hesap verebilirliğin ve şeffaflığın arttırılması amacıyla hazırlanarak 24/12/2003 tarihinde Resmi Gazete'de yayımlanmıştır.

5018 sayılı Kanunla ülkemizde; üst politika belgelerinde belirlenen öncelikler doğrultusunda beş yıllık stratejik planlar hazırlanmakta, stratejik planlarda yer alan hedeflerle uyumlu olarak yıllık performans programları oluşturulmakta, idareler bütçelerini performans esaslı program bütçeye göre hazırlamakta ve bu bütçeler program düzeyindeki anahtar göstergeler ve alt program düzeyindeki performans göstergelerini içermektedir. Bu yapıda kontroller, idarelerde iç kontrol sistemi vasıtasıyla yerine getirilmekte ve Hazine ve Maliye Bakanlığının merkezi uyumlaştırma görevi kapsamında belirlediği standartlar ve diğer düzenlemeler çerçevesinde tasarlanmaktadır. Planlama-programlama-bütçeleme ilişkisinin kurulabilmesi için belirlenen politikalar doğrultusunda stratejik planların hazırlanması, bu çerçevede bütçe önceliklerinin belirlenmesi ve kaynak tahsisinin yapılması, performans esaslı program bütçenin uygulanması ve uygulamaya ilişkin mali saydamlık ve hesap verebilirliğin sağlanması amacıyla faaliyet raporlarının ve performans programlarının yayımlanması gerekmektedir.

İç kontrol, bütçe ile tahsis edilmiş kaynakların etkili, ekonomik, verimli kullanımını sağlamak amacıyla, belirlenen hedeflere ulaşmak için gerekli performansı gerçekleştirmek üzere risklerin yönetilmesini kapsamaktadır. Kamu idarelerinde üst yöneticinin sahipliğinde oluşturulması istenen iç kontrol sisteminin mali saydamlık ve hesap verebilirliği sağlayacak şekilde uygulanması beklenmektedir. İç kontrol sistemi, Hazine ve Maliye Bakanlığı tarafından uluslararası genel kabul görmüş standartlar çerçevesinde belirlenen standartlara, düzenlemelere ve yöntemlere uygun olarak oluşturulur, uygulanır, izlenir ve geliştirilir. İç kontrol sisteminin işleyişi ve izlenmesinde temel sorumluluk idarelerin üst yöneticisine aittir. Üst yöneticiler, bu sorumluluğun gereklerini harcama yetkilileri, malî hizmetler birimi ve iç denetçiler aracılığıyla yerine getirmektedir.

5018 sayılı Kanunda; iç kontrolün tanımı, amacı, yapısı ve işleyişi ile iç kontrole ilişkin rol ve sorumluluklar düzenlenmiştir. Kanunun 55 inci maddesinde "Görev ve yetkileri çerçevesinde, malî yönetim ve kontrol süreçlerine ilişkin standartlar ve yöntemler Hazine ve Maliye Bakanlığınca, iç denetime ilişkin standartlar ve yöntemler ise İç Denetim Koordinasyon Kurulu tarafından belirlenir, geliştirilir ve uyumlaştırılır. Bunlar ayrıca, sistemlerin koordinasyonunu sağlar ve kamu idarelerine rehberlik hizmeti verir" hükmüne yer verilmiştir. Bu hükme dayanarak 26/12/2007 tarihli ve 26738 sayılı Resmi Gazete'de yayımlanan Kamu İç Kontrol Standartları Tebliğinde; idarelerin iç kontrol sistemlerinin oluşturulmasında, izlenmesinde ve değerlendirilmesinde dikkate almaları gereken temel yönetim kuralları olan Kamu İç Kontrol Standartları açıklanmıştır. Tebliğde yer alan 5 ve 6 ncı standartlar

kapsamında kamu idarelerinde iç kontrol sisteminin bir parçası olarak planlama, programlama ve bütçeleme ilişkisi ile bunlara ilişkin risklerin belirlenmesi ve değerlendirilmesi hususlarına yer verilmiştir. Söz konusu düzenleme, idarenin hedeflerinin gerçekleşmesini engelleyecek risklerin tanımlanması, analiz edilmesi ve gerekli önlemlerin belirlenmesine yönelik risk değerlendirme standartlarını içermektedir.

5018 sayılı Kanunun 9 uncu maddesi ve ilgili diğer yasal düzenlemelerle idarelere misyon ve vizyonlarını tanımlamaları, amaç ve hedeflerini belirlemeleri, performanslarını ölçmeleri ile izleme ve değerlendirme süreçlerini yürütmeleri amacıyla stratejik plan hazırlama yükümlülüğü getirilmiştir. Strateji ve Bütçe Başkanlığı tarafından stratejik plan hazırlanmasına ilişkin usul ve esasları belirleyen Kamu İdarelerince Hazırlanacak Stratejik Planlar ve Performans Programları ile Faaliyet Raporlarına İlişkin Usul ve Esaslar Hakkında Yönetmelik 22/4/2021 tarihli ve 31462 sayılı Resmi Gazete'de yayımlanmıştır. Yönetmelikle ilişkili olarak yayımlanan kılavuz ve rehberler, idarelerde stratejik yönetim sürecinin uygulanmasına yön vermektedir.

Söz konusu düzenlemelerle uyumlu olarak, Hazine ve Maliye Bakanlığı tarafından çıkartılmış bulunan Kamu İç Kontrol Rehberinde stratejik planlamanın etkinliğinin artması için, hedeflerin belirlenmesi aşamasında her bir hedefe ilişkin risklerin tespit edilerek analiz edilmesi ve risklere yönelik önlemlerin belirlenmesine ilişkin açıklamalar yer almaktadır. Buna ilave olarak, risklerin sadece stratejik planın hazırlanma aşamasında değil, uygulama ile izleme ve değerlendirme aşamalarında da sürekli gözden geçirilmesi gerekliliği vurgulanmaktadır.

Yukarıda bahsi geçen düzenlemeler, kurumsal risk yönetiminin stratejik planlama aşamasında başlayan ve idarenin görevlerini yerine getirirken yararlanabileceği bir araç olarak kullanılmasını esas alan bir yapıyı açıklamaktadır.

Rehberin Amacı

Kamu Kurumsal Risk Yönetimi Rehberi esas olarak;

- Kurumsal risk yönetiminin idarelere entegre edilmesinde,
- İdarelerin stratejik amaç ve hedeflerine ulaşmalarını etkileyebilecek öncelikli risklerinin tehdit ve fırsat boyutları göz önünde bulundurularak belirlenmesinde,
- Risklerin değerlendirilmesi ve önceliklendirilmesinde,
- Risklere yönelik alınacak kararların belirlenmesinde,
- Risklerin izlenmesinde ve raporlanmasında,
- Kurumsal risk yönetimine ilişkin rol ve sorumlulukların belirlenmesinde

idareleri yönlendirmek üzere hazırlanmıştır.

Bu rehber, stratejik amaç ve hedeflere ulaşılmasını etkileyebilecek risklerin yönetilmesine yönelik hazırlanmıştır. Rehber, idarelerin stratejik risklerini yönetirken yararlanabilecekleri uygulama örnekleri, ayrıntılı açıklamalar ve standart formlar vasıtasıyla uygulamayı güçlendirmeyi amaçlamaktadır.

İdareler stratejik amaç ve hedeflerine yönelik riskleri Kamu Kurumsal Risk Yönetimi Rehberinde yer alan açıklamalar çerçevesinde; birim, faaliyet ve süreçlerine yönelik riskleri ise Kamu İç Kontrol Rehberinde yer alan açıklamalar çerçevesinde ele alacaklardır.

Rehberin Kapsamı

Kamu idarelerinde kurumsal risk yönetiminin uygulamaya alınması için metodoloji, araçlar ve örnekler sunan Kamu Kurumsal Risk Yönetimi Rehberi 3 ana bölümden oluşmaktadır:

Birinci bölümde; risk ve kurumsal risk yönetimi kavramlarına, stratejik planlama ve kurumsal risk yönetiminin birbirine nasıl entegre edileceğine, kurumsal risk yönetimi ile stratejik planlama ve performans arasındaki ilişkiye, yönetişim ve idare kültürünün kurumsal risk yönetimi ile bağlantısına dair bilgilere yer verilmektedir.

İkinci bölümde; idarelerde etkili bir kurumsal risk yönetimi metodolojisinin oluşturulması için uygulanması gereken adımlar anlatılmaktadır.

Üçüncü bölümde; kurumsal risk yönetimi metodolojisinin oluşturulması, işletilmesi ve izlenmesine yönelik rol ve sorumlulukların dağılımı ile kurumsal risk yönetiminin iç kontrol, kalite yönetimi, iç denetim ve dış denetim ile ilişkisi açıklanmaktadır.

Bu rehberde yer alan örnekler, idarelerin faaliyet ve görev alanlarından esinlenerek oluşturulmuş olup söz konusu idareler için bağlayıcılığı bulunmamaktadır.

Rehberin Kullanıcıları

Bu rehber, ilgili mevzuatına göre stratejik plan hazırlamak zorunda olan idarelere yönelik olarak hazırlanmıştır. İdarelerde etkin bir kurumsal risk yönetimi yaklaşımının varlığı için rol ve sorumlulukların farklı seviyelerde belirlenmesi ve yerine getirilmesi gerekmektedir. Söz konusu rol ve sorumlulukları ana hatlarıyla tanımlayan bu rehberin temel kullanıcıları aşağıda belirtilmektedir:

- **Kurumsal risk yönetiminin oluşturulması, uygulanması, izlenmesi ve gerekli tedbirlerin alınmasından sorumlu olan Üst Yönetici,**
- **Kurumsal risk yönetimi uygulamalarının idare içerisinde etkin bir şekilde yürütülmesinden sorumlu İdare Risk Koordinatörü,**
- **Görev ve yetki alanları çerçevesinde, kurumsal risk yönetimi faaliyetlerinin uygulanmasından sorumlu olan Birim Yöneticileri ile idarede görev alan tüm çalışanlar,**
- **Kurumsal risk yönetimi yaklaşımının oluşturulması, geliştirilmesi ve uygulanmasında koordinasyon rolü üstlenen Strateji Geliştirme Birimi (SGB) yöneticileri ve çalışanları,**
- **Strateji Geliştirme Kurulu,**
- **İç Kontrol İzleme ve Yönlendirme Kurulu (İKİYK),**
- **Kurumsal risk yönetimi yaklaşımının etkinliğini değerlendirerek makul seviyede güvence vermek ve yaklaşımın etkinliğinin geliştirilmesinde danışmanlık sağlamak ile görevli olan İç Denetim Birimleri,**
- **Kurumsal risk yönetimi yaklaşımına yönelik merkezi uyumlaştırma görevini yürüten Hazine ve Maliye Bakanlığı yönetici ve çalışanları,**
- **Sayıştay Denetçileri**

1. RİSK VE KURUMSAL RİSK YÖNETİMİ

1.1 Risk Nedir?

Sözlük anlamıyla *risk* zarara uğrama tehlikesini ifade eder. *Tehlike* sözcüğü ise gerçekleşme ihtimali bulunan fakat istenmeyen sakıncalı durumlara işaret eder.

Dolayısıyla, risk;

- Belirli bir amaç veya faaliyet söz konusu olduğunda gündeme gelen,
- Geleceğe dair ve çoğu zaman negatif çağrışımları olan

bir kavramdır.

Kamu yönetimi ile ilişkili olarak risk, idarelerin stratejik amaç ve hedeflerine ulaşmalarını, olumlu ya da olumsuz yönde etkileyebilecek olaylar veya durumlar olarak tanımlanır. Olumlu yönde etkilediğinde risk fırsat olarak değerlendirilirken, olumsuz yönde etkilediğinde tehdit olarak değerlendirilir.

Küreselleşme, artan paydaş beklentileri, teknolojik gelişmeler, mevzuat değişiklikleri, karmaşık hale gelen faaliyet ve süreçler gibi birçok etken, idarelerin kısa, orta ve uzun vadeli amaç ve hedeflerini ve bunlara ulaşmak için uyguladıkları faaliyetler ile kaynak dağılımlarını önemli ölçüde etkilemektedir. Dolayısıyla karar alma süreçlerinde idarelerin stratejik amaç ve hedeflerine ulaşmalarını etkileyecek risklerini tespit edip değerlendirerek, söz konusu riskler gerçekleşmeden önce gerekli önlemleri almaları veya risklerin gerçekleşmesi halinde maruz kalınacak zararın uygun kaynak ve zaman planlaması ile en aza indirilmesini sağlayacak yöntemler geliştirmeleri ve uygulamaları gerekmektedir.

1.2 Kurumsal Risk Yönetimi Nedir?

Kurumsal risk yönetimi, idarelerin, stratejik amaç ve hedeflerini gerçekleştirmelerini etkileyebilecek olay veya durumları; bütüncül bir bakış açısıyla belirlemeleri, etki ve olasılıklarını değerlendirmeleri, önem derecelerine göre önceliklendirmeleri, risklere yönelik alınacak kararları belirlemeleri ile riskleri izleme ve raporlamalarına dayanan kapsamlı, tekrar eden ve sistematik bir süreçtir. Bu sayede, söz konusu olay veya durumların gerçekleşme ihtimalinin veya bu olay ya da durumların gerçekleşmesi halinde maruz kalınacak zararın azaltılması veya ortaya çıkabilecek fırsatların etkin bir biçimde değerlendirilmesi mümkün olabilir.

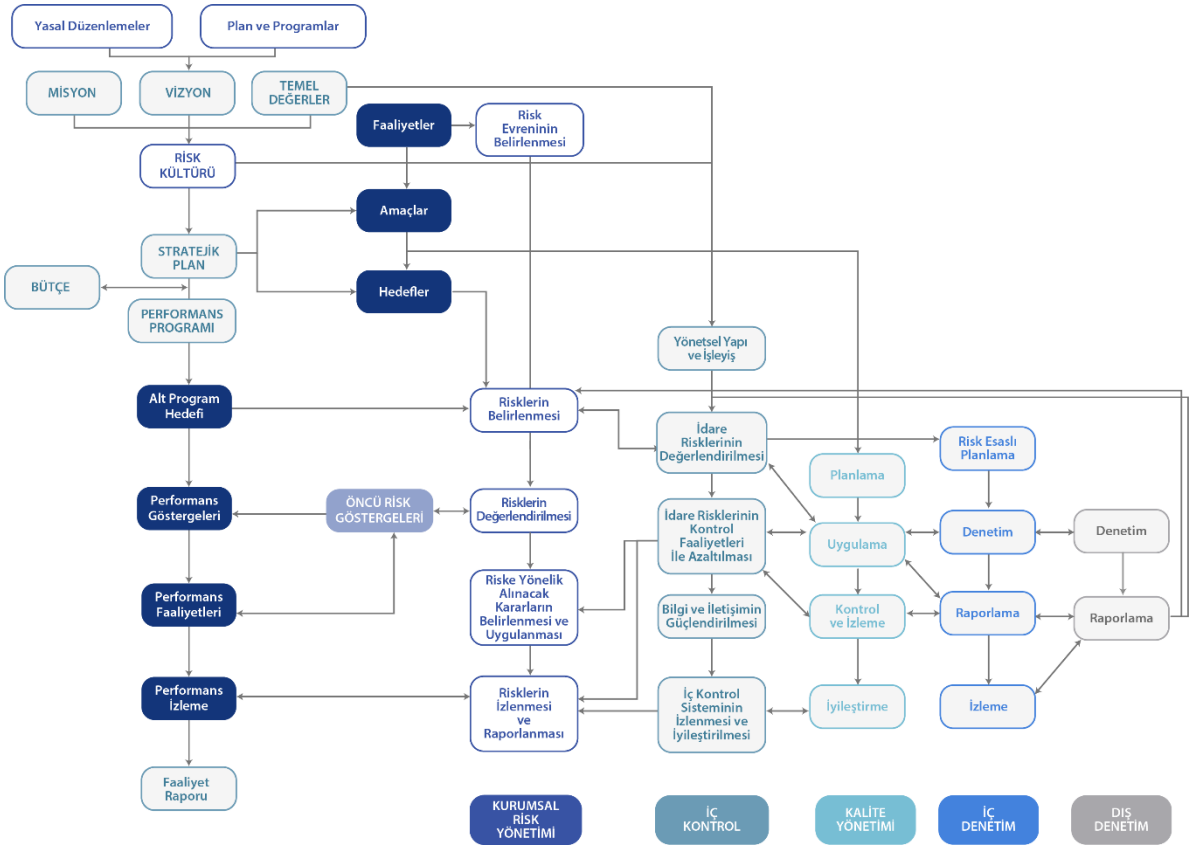
Kurumsal risk yönetimi yaklaşımının idarelere sağlayacağı katkılar aşağıdaki gibi özetlenebilir:

- İdarenin amaç ve hedeflerine ulaşmasına ve performansını geliştirmesine katkı sağlar.
- İdarenin ortak risk algısının oluşmasını destekler. Böylece kurumsal risklerin yönetiminde öznellik azaltılır.
- İdarenin risklerini yönetmede proaktif davranmasını sağlar. Riskler meydana gelmeden tespit edilir, gerekli ilave risk yönetimi faaliyetleri zamanında gerçekleştirilir ve bu sayede idare, olası risklere maruz kalmadan bunları bertaraf edebilme yeteneğine kavuşur. Riskler gerçekleşmiş ise önceden belirlenmiş kaynak ve zaman planlaması ile idarenin maruz kalacağı zararlar en aza indirilir.
- İdarenin faaliyetlerinin sürekliliği sağlanır. İdareler tarafından sağlanan hizmetin değeri artar.
- Olası kayıpların kontrol altına alınması sayesinde idarenin katlanmak zorunda kalabileceği ilave maliyetler azalır, bu sayede kamu kaynağının etkili, ekonomik ve verimli bir biçimde kullanılmasına katkı sağlanır.
- Risklerin idareler tarafından sadece tehdit olarak değil fırsat olarak da görülmesi sağlanır. Böylece idarenin maruz kalabileceği riskler idareye yeni fırsatlar sunabilir.
- Risklerden tamamen kaçınmak yerine, risklerin değerlendirilmesi ve önceliklendirilmesi sayesinde idareler tarafından ölçülü risk alma teşvik edilir, yenilikçi yaklaşımların geliştirilmesi desteklenir.
- İdarenin maruz kalabileceği riskler önceden tanımlanmış ve gerekli ilave risk yönetimi faaliyetleriyle zamanında azaltılmış olacağı için yönetim anlık problemleri çözmek için kaynak ve zaman harcamak yerine, stratejik amaç ve hedeflere daha fazla odaklanabilir. Böylece, kaynak tahsisinde etkililik ve verimlilik artar.
- İdarenin iç kontrol ve iç denetim fonksiyonlarının etkinliğini arttırmaya yardım eder.

1.2.1 Kurumsal Risk Yönetiminin İdareye Entegre Edilmesi

Kurumsal risk yönetiminin etkin bir şekilde uygulanabilmesi, idarenin mevcut iş süreçlerine ve raporlama mekanizmalarına doğru şekilde entegre edilebilmesine bağlıdır. Kurumsal risk yönetimi süreçlerinin sade, esnek ve uygulanabilir olması ve diğer temel süreçlerle (stratejik planlama, performans yönetimi, insan kaynakları yönetimi vb.) bütünleşik olarak planlanması ve yürütülmesi önem arz etmektedir. Kurumsal risk yönetimi, iç kontrolün ayrılmaz bir parçası olarak stratejik planlama süreci ile başlar ve idare çapında gelişmiş ve etkin bir karar alma mekanizmasının oluşmasına yardımcı olur.

Kurumsal risk yönetiminin; stratejik plan, performans programı ve bütçe, faaliyet raporları, iç kontrol, kalite yönetimi, iç denetim ve dış denetim ile entegre yapısı ana hatlarıyla aşağıdaki şekilde gösterilmiştir:



Şekil 1 – Kurumsal Yönetim Araçları Arasındaki İlişki

1.2.1.1 Kurumsal Risk Yönetiminin Stratejik Plan ile İlişkisinin Kurulması

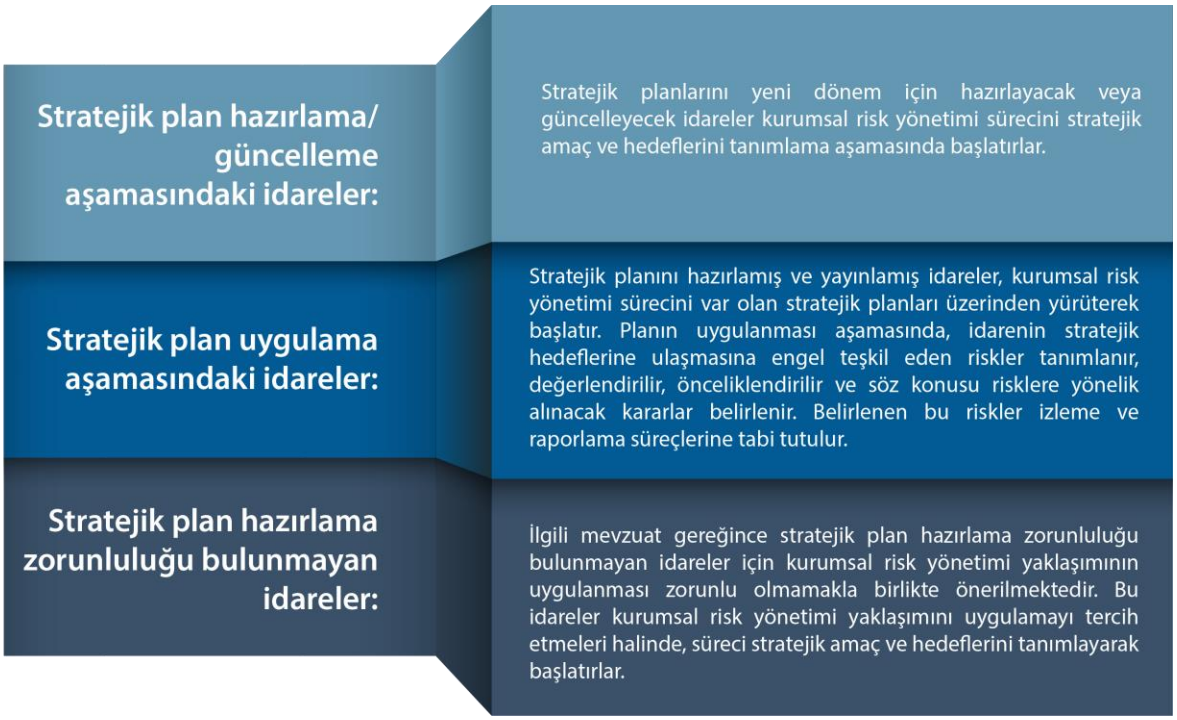
Stratejik planlama, idarenin stratejik amaç ve hedeflerini ve bunlara ulaşmayı mümkün kılacak yöntemleri belirlemesini, bütçesini bu amaca yönelik hazırlamasını ve kaynak tahsisinde önceliklendirmeyi gerektirir. Başarılı bir stratejik planlama, kamu kaynaklarının etkili, ekonomik ve verimli bir biçimde kullanılmasına ve karar alma süreçlerinin etkinliğinin sağlanmasına yardımcı olur.

> Kurumsal risk yönetimi, stratejik yönetim sürecinin ayrılmaz bir parçasıdır.

Kurumsal risk yönetiminin ana odağı, stratejik amaç ve hedeflere ulaşılmasına engel oluşturan risklerin yönetilmesidir. Bu seviyedeki risklerin belirlenmesi süreci, stratejik planlama kapsamında amaç ve hedeflerin belirlenmesi süreci ile bir bütün halinde yürütülür.

Kurumsal risk yönetimi, hem stratejik amaç ve hedeflerin seçilmesinde hem de seçilmiş stratejik amaç ve hedeflere ulaşılmasında önemli bir araçtır. Kurumsal risk yönetimi, üst yönetimin "Gitmek istediğimiz yere nasıl ulaşabiliriz?" sorusunu cevaplamasını sağlar. Kurumsal risk yönetiminin idarenin mevcut süreçleri ile bütünleştirilmesi sayesinde, stratejik amaç ve hedeflere ulaşılması konusunda tüm iç ve dış paydaşlara makul güvence sağlanmış olur.

Kurumsal risk yönetimi, yönetim döngüsünün dolayısıyla stratejik planlama sürecinin ayrılmaz bir parçasıdır. Bu kapsamda;



İdarenin stratejik planında doğrudan tanımlanmış olmasa da, önemli ekonomik, siyasi, teknolojik, vb. değişiklikler nedeniyle, idarenin stratejik amaç ve hedefleri kapsamında yeni kararlar alması ya da mevcut kararlarında değişiklikler yapması söz konusu olabilir. Kurumsal risk yönetimi yaklaşımının stratejik planlama süreciyle birlikte başlatılması genel kural olmakla birlikte, yukarıda örneklendirilen ve karar alma mekanizmasının işletilmesine gerek duyulan durumlarda da risk yönetiminin uygulanması gerekmektedir.

1.2.1.2 Kurumsal Risk Yönetiminin Performans ile İlişkisinin Kurulması

Her idare, stratejik amaç ve hedef seçimleri ve bu seçimler doğrultusunda yürüttüğü faaliyetler ile doğal olarak bazı riskler üstlenmiş olur. Bu riskler, idarenin faaliyetlerinin sürekliliğini ve başarısını, bu faaliyetlerden yararlanan yahut etkilenen paydaşları, kullandığı kaynakları, kamuoyundaki imajını, hizmetlerinin kalitesini ve idare personeli de dahil olmak üzere çok sayıda faktörü etkiler.

Kurumsal risk yönetimi ile performans arasında iki yönlü bir ilişki vardır:

Kurumsal Risk Yönetiminin İdarenin Performansını Arttırması: İdarenin stratejik amaç ve hedeflerine ulaşmasına engel teşkil eden risklerini belirlemesi ve değerlendirmesi sağlanır. İdare bu sayede öncelikli risklere yönelik gerekli ilave risk yönetimi faaliyetlerini gerçekleştirir ve bu da idarenin performansının artmasına ve hedeflerine ulaşmasına katkı sağlar.

Performans İzleme Süreçlerinin Kurumsal Risk Yönetimine Katkısı: İdare performansının izlenmesi ve değerlendirilmesi, performans göstergelerinin ölçümlenmesi ve sapmaların raporlanması süreçleri, idarenin kurumsal risk yönetimi süreçlerinin yeterliliği hakkında bilgi verir. İdarenin performans programında tanımlanmış olan faaliyet ve göstergeler izlenerek, kurumsal risk yönetimi uygulamalarının etkin olup olmadığı performans değerlendirme sonuçlarıyla teyit edilir. Olumsuz performans gösterilen faaliyet ve süreçler dikkate alınarak, kurumsal risk yönetimine dair iyileştirme alanları tespit edilir, yapılan performans değerlendirmesi sonuçlarına göre, gerekli ilave risk yönetimi faaliyetlerinin gerçekleştirilmesi için çalışmalar yapılır. Söz konusu performans değerlendirmesi sonuçlarına göre, kurumsal risk yönetimi sisteminin iyileştirilmesi için ilave risk yönetimi faaliyetleri belirlenir.

İdareler, performansın iyileştirilmesi ve kurumsal risk yönetimi uygulamalarının geliştirilmesi için;

- Kurumsal risk yönetimi yaklaşımının uygulanmasının,
- Performans göstergelerinde bir sapma olması durumunda, yönetilmesi gereken bir riskin sapmaya neden olup olmadığının kontrolünün ve kayıt altına alınmamış bir risk söz konusu ise ilgili riskin kayıt altına alınmasının ve takip edilmesinin,
- Performans gösterge sonuçlarında yaşanan sapmaların nedenlerinin araştırılmasının ve araştırma sonuçlarının ilgili hedef altında tanımlanan risklerin gerçekleşme durumlarıyla ilişkisinin kurulmasının,
- İlişkili performans göstergeleri ile öncü risk göstergelerinin sonuçlarının karşılaştırılmasının

önemini göz önünde bulundurmalıdır.

1.2.1.2.1 Misyon, Vizyon ve Temel Değerler

Misyon, vizyon ve temel değerler idarenin var oluş amacı ile faaliyetlerini nasıl yönetmek istediğini tanımlar. Misyon, idarenin varlık sebebini, vizyon gelecekte ulaşmak istediği noktayı, temel değerler ise idarenin benimsediği davranış kurallarını, temel ilkeleri ve yönetim biçimini ifade eder.

İdarenin misyon, vizyon ve temel değerleri idare kültürüne ve dolayısıyla çalışanlarının kurumsal risk algısı ve riske karşı geliştireceği kurumsal yaklaşıma zemin oluştururken, idarenin stratejik amaç ve hedeflerini belirlemede ve bu hedeflere ulaşmada izleyeceği yol ise risk yönetimi yaklaşımını etkiler.

Tabi olunan yasal düzenlemeler ile üst politika belgelerindeki stratejik amaç ve hedefler, idarenin misyon, vizyon ve temel değerleri için zemin oluşturur. Misyon, vizyon ve temel değerler idarenin amaç ve hedeflerinin belirlenmesinde önemli rol oynar. Dolayısıyla, idarenin stratejik amaç ve hedeflerinin misyon, vizyon ve temel değerleri ile uyumlu olması gerekir.

1.2.1.2.2 İdare Kültürü ve Risk Kültürü

İdare kültürü, yönetici ve çalışanlar tarafından benimsenmiş olan temel değerleri ve davranış kurallarını yansıtır. İdare kültürü hem idare içi hem de idare dışı faktörlerden etkilenir:

İç faktörler; idarenin çalışma tarzı, çalışanların birbirleriyle ve paydaşlarla olan iletişimi, idare içinde belirlenmiş olan standartlar ve kurallar, fiziksel çalışma ortamı, idarenin raporlama yapısı, şeffaflık anlayışı, etik değerleri, açık iletişim kanalları olarak sıralanabilir.

Dış faktörler; yasal düzenlemeler ve bunun sonucunda idare yapısında veya yönetiminde yaşanan değişiklikler ve paydaş beklentileri olarak sıralanabilir.

Tüm bu faktörler idarenin risk algısını, idarenin riskten kaçınma ile risk almaya istekli olma aralığında nasıl konumlandığını, özetle idarenin risk kültürünü etkilemektedir. Söz konusu faktörlere bağlı olarak idarelerin risk kültürleri farklılık gösterebilmektedir.

İdare kültürü ve risk kültürü birbirleriyle etkileşim halindedir. İdare kültürü, risklerin nasıl tanımlanacağına, nasıl önceliklendirileceğine, nasıl yönetileceğine, nasıl raporlanacağına ve nasıl izleneceğine etki eder.

Etkin bir kurumsal risk yönetimi için idare içerisinde ortak bir yaklaşım oluşturulması gerekir. İdare bünyesinde risk kültürünün arzu edilir bir seviyede oluşmasına yardımcı olabilecek hususlar aşağıda sıralanmaktadır:

- Üst yönetimin riske yaklaşımı; üst politika belgelerinde yer alan plan ve programlar, idarenin misyon, vizyon ve temel değerleri ile stratejik amaç ve hedeflerini ve paydaş beklentilerini yansıtmalıdır.

- Üst yönetici kurumsal risk yönetimini desteklemeli ve idarenin genelinde tüm yöneticiler ve çalışanlar tarafından sahiplenilmesini sağlayacak adımları atmalıdır.
- Kurumsal risk yönetimi yaklaşımı kapsamında gerçekleştirilecek çalışmalar, sadece belirli bir birimin, yöneticinin ya da çalışanın görevi olarak algılanmamalıdır.
- Kurumsal risk yönetimi yaklaşımı bu Rehber ile uyumlu olacak şekilde oluşturulacak Risk Strateji Belgesinde (RSB) tanımlanmalı, söz konusu yaklaşımın hem üst yönetim hem de çalışanlar tarafından benimsenmesi sağlanmalıdır.
- Kurumsal risk yönetimi konusunda ilgili çalışanların farkındalık eğitimi alması sağlanmalı ve kurumsal risk yönetimi yaklaşımının kritik başarı faktörleri söz konusu eğitimlerde katılımcılara aktarılmalıdır.
- Risk tecrübelerinin etkin bir şekilde aktarılması adına kurumsal iletişim ve raporlama yapısı etkili ve şeffaf bir şekilde kurgulanmalıdır.
- İdare içinde hesap verebilirlik tüm birimlerde yaygınlaştırılmalıdır. İdare içinde hesap verebilirliğin yaygınlaştırılmasını destekleyecek hususlar aşağıda belirtilmektedir:
  - ✓ Üst politika belgelerinde yer alan plan ve programlar idarelerde görevli yönetici ve çalışanlar tarafından bilinmeli ve benimsenmelidir.
  - ✓ Üst yönetimin beklentilerinin net bir şekilde tüm çalışanlar tarafından anlaşılmasını sağlayacak bilgi paylaşımı yapılmalıdır.
  - ✓ İdarenin stratejik hedefleri ile alt program hedefleri arasında ilişki kurulmalıdır. Hedef gerçekleşmeleri ve meydana gelen sapmalar ve bu sapmaların nedenleri yöneticiler tarafından sorgulanmalıdır.
  - ✓ Kurumsal risk yönetimi raporları ilgili yöneticiler ile paylaşılmalı, stratejik kararların, mutlaka risk bilgisi dikkate alınarak verilmesine destek olunmalıdır.

1.2.1.3 Risk Strateji Belgesinin Oluşturulması

İdarenin kurumsal risk yönetimi yaklaşımını içeren Risk Strateji Belgesi, asgari olarak aşağıdaki başlıklar çerçevesinde, idarenin ihtiyaçları göz önünde bulundurularak ve bu Rehber ile uyumlu olacak şekilde Strateji Geliştirme Birimi tarafından birimlerden gelen görüş ve öneriler doğrultusunda hazırlanır. Risk Strateji Belgesi (Ek–1), hazırlanacak veya uygulanmakta olan stratejik planın dönemini kapsayacak şekilde hazırlanır, yıllık olarak gözden geçirilir ve gerekli görüldüğünde güncellenir.

İlgili dokümanda asgari olarak yer alması gereken bilgiler aşağıda belirtilmektedir:

Şekil 2 – Risk Strateji Belgesinde Yer Verilecek Asgari Bilgiler

- Amaç ve Kapsamı: **Risk Strateji Belgesinin amaç ve kapsamı belirlenir.**
- Öncelikli Risk Alanları: **İdarenin görev alanı kapsamında öncelikli risk alanları belirlenir. İdare tarafından öncelikli risk alanlarının belirlenmesi "Riskleri nerelerde aramalıyız?" sorusuna yanıt aranmasını sağlar ve risk evreninin belirlenmesini kolaylaştırır.**
- Risk Evreni: **Riskler temel olarak, dış riskler ve iç riskler olarak sınıflandırılmaktadır. Risklere yönelik alt kategoriler idarenin amaçlarına, hedeflerine ve faaliyet alanlarına göre değişiklik gösterebilir. Bu nedenle dış riskler ve iç riskler kendi aralarında alt kategorilere ayrılır. Risk kategorileri belirlenirken stratejik planlama çalışmalarında gerçekleştirilen durum analizi çıktılarından faydalanılır.** ***("2.1.1 Risk Evreninin Belirlenmesi" bölümünde detaylı bilgiye yer verilmektedir.)***
- Risk Etki Kriterleri: **Tanımlanmış olan belirli bir riskin yol açacağı sonuçlar, finansal, operasyonel, itibar, uyum ve stratejik açılardan sınıflandırılıp,**

ölçeklendirilebilir. Risk etki kriterleri idarenin kendine özgü koşulları göz önünde bulundurularak belirlenir. *("2.2.1.1 Risklerin Etki ve Olasılık Seviyelerinin Belirlenmesi" bölümünde detaylı bilgiye yer verilmektedir.)*

- Temel Risk Göstergeleri (TRG): Temel risk göstergeleri, idarenin amaç ve hedeflerinin gerçekleştirilmesiyle doğrudan ilgili belirli bir faaliyet veya sürecin ne ölçüde riskli olabileceğini değerlendirmek için kullanılan ve nicel olarak ifade edilebilen bir ölçüm olarak tanımlanabilir.
  TRG'ler daha önce gerçekleşmiş belirli durum ve olayları ölçebileceği gibi (gerçekleşen risk göstergeleri), ileride gerçekleşmesi muhtemel durum ve olaylarla ilgili erken uyarı sağlamak için de (öncü risk göstergeleri) kullanılabilir. TRG'ler idaredeki ve idarenin görev alanındaki eğilimlerin tespiti ve izlenmesi konusunda karar alıcılara yardımcı olabilir.
  Artık risk seviyesi orta, yüksek ve çok yüksek seviyeli riskler ile doğal risk seviyesi yüksek ve çok yüksek olan fakat mevcut risk yönetimi faaliyetleriyle düşük ve orta risk seviyesine indirilen riskler için temel risk göstergeleri belirlenebilir. Bu durumda Risk Strateji Belgesinde de temel risk göstergelerine yer verilir ve tanımlanır.
- Öncü Risk Göstergeleri (ÖRG): İdarenin stratejik amaç ve hedeflerine ulaşmasını etkileyebilecek risklerin gerçekleşme ihtimalleri konusunda idareyi uyaran ve söz konusu risklerin takibinde kullanılan risklerdir. Artık risk seviyesi yüksek ve çok yüksek olarak tanımlanan riskler için öncü risk göstergeleri belirlenir. Artık risk seviyesi orta, düşük ve çok düşük seviyeli riskler ile doğal risk seviyesi yüksek ve çok yüksek olan fakat mevcut risk yönetimi faaliyetleriyle düşük ve orta risk seviyesine indirilen riskler için ÖRG belirlenmesi idarenin inisiyatifindedir. Bu kararın idare içinde hangi yönetim seviyesinde verileceği Risk Strateji Belgesinde tanımlanır. *("2.2.3 Öncü Risk Göstergelerinin Belirlenmesi" bölümünde detaylı bilgiye yer verilmektedir.)*
- İzleme Kapsamı: Risk izlemenin hangi kapsamda gerçekleştirileceği, hangi risklerin izlemeye alınacağı *"2.4.1 Risklerin İzlenmesi"* bölümünde yer alan açıklamalar ışığında değerlendirilerek Risk Strateji Belgesinde detaylı olarak tanımlanır.
- Raporlama Kapsamı: Risk raporlama çalışmalarının kapsamı ve hangi periyotta hangi risklerin raporlanacağı *"2.4.2 Risklerin Raporlanması"* bölümünde yer alan kapsamda belirlenir. İdarenin ihtiyaçları doğrultusunda belirlenecek ek raporlamalar da raporlama kapsamına eklenir.
- Kurumsal Risk Yönetimine İlişkin Rol ve Sorumluluklar: İdare kendi organizasyon yapısını göz önünde bulundurarak Rehberle uyumlu olacak şekilde rol ve sorumlulukları belirler. Kurumsal risk yönetimi yaklaşımının tüm adımlarına (risklerin belirlenmesi, risklerin değerlendirilmesi, riske yönelik alınacak kararların belirlenmesi, risklerin izlenmesi ve raporlanması) yönelik rol ve sorumluluklar açık bir şekilde tanımlanır.

- Kurumsal Risk Yönetimi Farkındalık Eğitiminin İçeriği: Yönetici ve çalışanlara verilecek farkındalık eğitimlerinin kapsamı, içeriği, süresi ve sıklığı tanımlanır.
- Risk Yönetimi Çalışma Takvimi: SGB tarafından yıllık olarak Kurumsal Risk Yönetimi Takvimi (Risk Yönetimi Takvimi Örneği (Ek–3)) hazırlanır ve üst yönetici tarafından onaylanır.

2. KURUMSAL RİSK YÖNETİMİ METODOLOJİSİ

Kurumsal risk yönetimi döngüsü, aşağıdaki adımlardan oluşur ve dönemsel olarak kendisini tekrar eder:

Şekil 3 –Kurumsal Risk Yönetimi Döngüsü

2.1 Risklerin Belirlenmesi

2.1.1 Risk Evreninin Belirlenmesi

Kamu İdareleri İçin Stratejik Planlama Kılavuzunda belirtildiği üzere, stratejik planlama sürecinde öncelikle durum analizi gerçekleştirilir.

Durum analizi kapsamında kuruluş içi analiz, PESTLE analizi ve GZFT analizi gibi çeşitli analizler gerçekleştirilir. Kuruluş içi analiz kapsamında, insan kaynaklarının yetkinliği, idare kültürü, teknolojik altyapı, fiziki kaynaklar ve mali kaynaklar değerlendirilir. PESTLE analizi kapsamında, idareye etkisi olabilecek politik, ekonomik, sosyal, teknolojik, yasal ve çevresel dış etkenler belirlenir. GZFT analizi kapsamında, idarenin güçlü ve zayıf yönleri ile idare dışında oluşabilecek fırsat ve

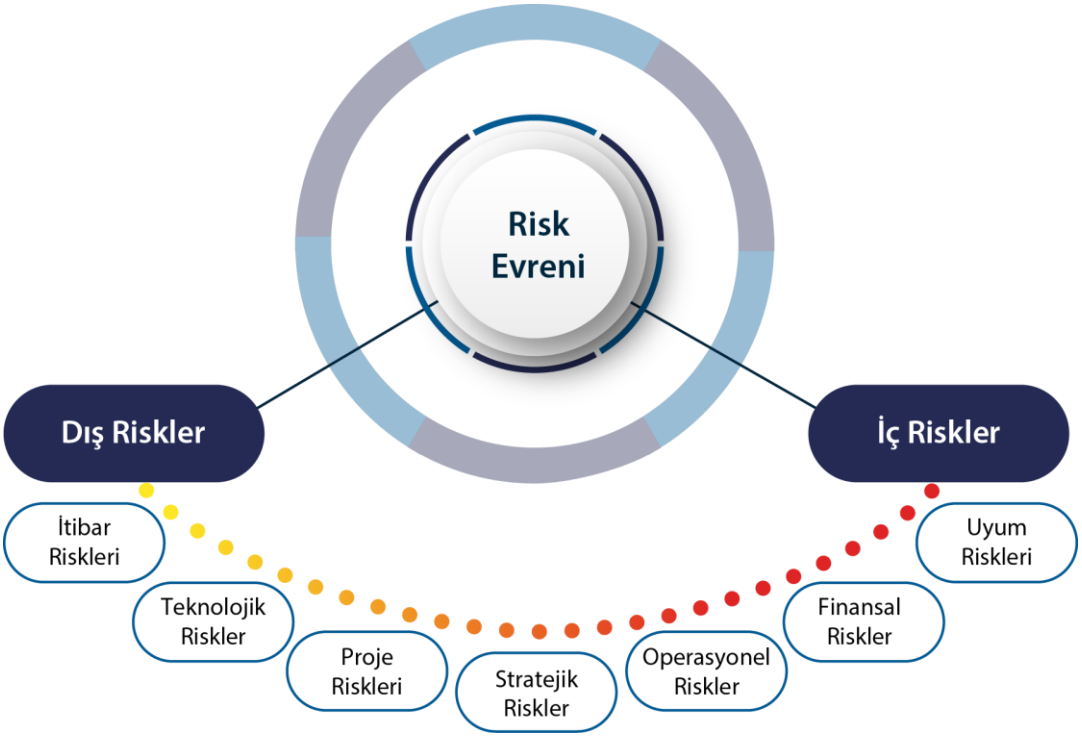
tehditler tespit edilir. Güçlü yönlerin ve fırsatların belirlenmesi idarenin stratejik amaç ve hedeflerine ulaşmasını desteklerken; zayıf yönlerin ve tehditlerin belirlenmesi hem amaç ve hedeflerin gerçekçi ve ulaşılabilir olup olmadığının değerlendirilmesini sağlar hem de seçilen stratejik amaç ve hedeflere ulaşma konusunda makul güvence verecek önlemlerin alınmasına ve uygulanmasına yardım eder.

İdarenin tabi olduğu iç ve dış çevre, görev alanı, gerçekleştirdiği faaliyetler, sunduğu hizmetler, maruz kalabileceği risklerin kaynağını oluşturur. Kurumsal risk yönetimi yaklaşımının başlangıç noktası, stratejik planlama çalışmaları kapsamında gerçekleştirilen durum analizi aşamasıdır. Bu aşamada, durum analizi çalışmalarında ulaşılan tespitlerden faydalanılarak idarenin risk evreni belirlenir ve Risk Strateji Belgesi'ne kaydedilir.

İdareler stratejik planlama hazırlık aşamasında risk evreni oluştururken riskleri 2 ana odakla ele alırlar:

1. Dış Riskler: İdarenin kontrolü dışında gerçekleşen olaylar sonucunda maruz kalabileceği, stratejik amaç ve hedeflerine ulaşmasını etkileyebilecek risklerdir. Deprem, yangın, sel, fırtına gibi doğal afetler nedeniyle idarenin yerleşkesinin zarar görmesi ve bunun neticesinde idareye ait evrak, belge ve sistemsel verilere ulaşılamaması, idare faaliyetlerinin sekteye uğraması veya yaşanan bir mevzuat değişikliğine yönelik gerekli düzenlemelerin zamanında gerçekleştirilememesi, hukuki yaptırımlarla karşı karşıya kalınması dış risklere örnek olarak gösterilebilir. Stratejik risk çalıştaylarında dış riskler ele alınırken, stratejik planlama çalışmalarının durum analizi aşamasında gerçekleştirilen GZFT analizi kapsamında tespit edilen fırsatlar ve tehditler ile PESTLE analizi ve ilgili diğer analiz sonuçlarından faydalanılır.

2. İç Riskler: İdarenin faaliyetlerini gerçekleştirirken maruz kalabileceği ve stratejik amaç ve hedeflerine ulaşmasını etkileyebilecek risklerdir. İdare bünyesinde yer alan sistemlerin, yazılımların istenilen işlemleri gerçekleştirememesi, yeterli hıza sahip olmaması, halka sunulan hizmetlerde gecikmelerin yaşanması, iş güvenliği ve sağlığını tehdit eden riskler iç risklere örnek olarak gösterilebilir. Stratejik risk çalıştaylarında iç riskler ele alınırken stratejik planlama çalışmalarında gerçekleştirilen GZFT analizi ve kuruluş içi analiz gibi ilgili tüm analiz sonuçlarından faydalanılır.



Şekil 4 – Risk Evreni

İç ve dış riskler, temel olarak operasyonel, finansal, stratejik, uyum, itibar, teknolojik ve proje riskleri olarak alt kategorilerde değerlendirilir. İdare, faaliyetlerini ve ihtiyaçlarını dikkate alarak Risk Strateji Belgesinde ilave kategoriler (güvenlik riskleri, çevresel riskler, idareler arası koordinasyon eksikliğinden kaynaklanan riskler vb.) belirleyebilir.

Kurumsal risk yönetimi yaklaşımı doğrultusunda, riskler belirlenirken, faaliyetlere ilişkin tüm kategorilerdeki risklerin tamamının belirlenmesi hedeflenmemektedir. Söz konusu riskler içinden stratejik amaç ve hedeflere ulaşılmasını etkileyebilecek olan öncelikli risklerin kapsama alınması gerekmekte olup ilgili kategoriler, idarenin odaklanacağı alanların tespiti konusunda yol göstermektedir. Diğer taraftan, stratejik amaç ve hedefleri etkilemeyecek fakat birim, süreç ve faaliyet seviyesinde değerlendirilecek riskler ise Kamu İç Kontrol Rehberi çerçevesinde ele alınmalıdır.

İdarenin Risk Strateji Belgesi'nde risk evreninin belirlenmesindeki amaç, idarenin odaklanacağı alanların tespit edilmesi, potansiyel risk kaynaklarının gözden kaçırılmaması ve risklerin nasıl takip edileceğinin belirlenmesinin sağlanmasıdır.

Risk evreni her yıl en az bir kez gözden geçirilerek Risk Strateji Belgesi'nde belgelendirilir. Belirlenen bu kategoriler yıl içerisinde gerçekleştirilecek olan çalıştaylarda kullanılır. Çalıştaylar sırasında tanımlanan risklerin hangi kategoride değerlendirileceğine karar verilerek Bireysel Risk Belirleme Formu (Ek–5) ve Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formu'na (Ek–12) kaydedilir.

Risklere ilişkin alt kategorilere, açıklamalara ve örneklere aşağıda yer verilmektedir:

KATEGORİ	AÇIKLAMA	ÖRNEK
STRATEJİK RİSKLER	İdarenin stratejik amaç ve hedef seçimlerinden dolayı maruz kalabileceği risklerdir.	- Nükleer enerji yatırımına karar verilmesi durumunda kamuoyu tepkisinin ve baskısının artması sonucu itibar kayıplarının yaşanması, projenin yarım kalması, kamu kaynaklarının etkili, ekonomik ve verimli bir şekilde kullanılmaması - Üniversite bünyesinde yeni bir bölüm oluşturulmasına (yeni bir fakülte veya bölüm vb.) yönelik gerek duyulacak kaynağa (öğretim üyesi, bina, ekipman alımı vb. için) ulaşılamaması sonucu seçilen stratejinin hayata geçirilememesi
OPERASYONEL RİSKLER	İdarenin faaliyetlerinin mevzuata uygun, zamanında, etkili, ekonomik ve verimli bir şekilde yürütülmesini etkileyebilecek risklerdir.	- Sağlık hizmetleri kapsamında kullanılan randevu sistemine yönelik yetersiz bilgi teknolojileri altyapısı nedeniyle aksaklıklar yaşanması ve vatandaşa sağlık hizmeti sunulamaması - İdarenin ilgili birimlerinden talep edilen finansal verilerin doğru şekilde ve zamanında alınamaması sonucu üst yönetime yönelik raporlamaların doğru şekilde gerçekleştirilememesi
FİNANSAL RİSKLER	İdarenin finansal yapısını ve finansal faaliyetlerini sürdürmek için ihtiyaç duyduğu kaynakları etkileyebilecek risklerdir.	- İdarenin cari ve yatırım bütçelerinin yeterli analizler gerçekleştirilmeden yapılması sonucu kaynakların etkin kullanılamaması - İdare bütçesinin etkin takip edilmemesi sonucunda finansal yükümlülüklerin yerine getirilememesi
UYUM RİSKLERİ	İdarenin mevzuata, iç ve dış düzenlemelere uygun işlemler yapmasını etkileyebilecek risklerdir.	- Veri güvenliğine yönelik politika ve prosedürlerin oluşturulmaması nedeniyle Kişisel Verilerin Korunması Kanunu'na uyumsuzluk sonucunda idarenin cezai yaptırıma maruz kalması - Doktora tezi onay sürecinde mevzuatla uyumlu olacak şekilde kontrollerin yapılmaması sonucu uygun olmayan tezlerin onaylanması
İTİBAR RİSKLERİ	İdareye duyulan güveni veya kamuoyundaki imajını etkileyebilecek risklerdir	- Bir belediye için kritik öneme sahip bir projenin taahhüt edilen sürede tamamlanamaması sonucu belediye hizmetlerinin yeterliliğinin halk tarafından sorgulanması ve idarenin itibar kaybetmesi - Eğitim takvimine uyulmaması sonucu öğrencilerin alması gereken dersleri alamaması, eğitim kalitesinin düşmesi ve nitelikli öğrenci yetiştirilememesi
TEKNOLOJİK RİSKLER	Teknolojik gelişmeler ve idarenin kullandığı teknolojilerden kaynaklanan risklerdir.	İdare tarafından gerçekleştirilen bilgi teknolojileri altyapı yatırımının etkin kullanılamaması sebebi ile beklenen maliyet düşüşünü yaratmaması ve bunun sonucu kaynakların etkin kullanılamaması
PROJE RİSKLERİ	İdarenin stratejik amaç ve hedeflerine ulaşmak üzere gerçekleştirmekte olduğu projelerle ilişkili olan risklerdir.	-Proje bütçesinin etkili bir biçimde takip edilmemesi sonucunda finansal yükümlülüklerin yerine getirilememesi -Proje gerçekleşmelerinin etkili bir biçimde takip edilmemesi ile olası eksikliklerin zamanında tespit edilememesi sonucu proje hedefine ulaşılamaması

Tablo 1 – Örnek Risk Kategorileri

Bir riskin bazen birden fazla risk kategorisi ile ilişkilendirilebilmesi mümkün olabilir. Örneğin; bilgi teknolojileri altyapısının yetersizliği nedeniyle vatandaşa hizmet sunulamaması riskinde olduğu gibi bir risk aynı anda hem operasyonel risk hem de itibar riski sınıfında yer alabilir.

2.1.2 Risklerin Stratejik Amaç ve Hedefler Seviyesinde Ele Alınması

Stratejik planlama aşamasında durum analizi sonrasındaki aşama, idarenin stratejik amaç ve hedeflerinin belirlenmesidir. Risk yönetiminin kapsamı, stratejik amaç ve hedeflerle ilişkili riskler olduğundan, etkin bir stratejik planlama ve risk yönetimi için idare amaç ve hedeflerinin tam ve doğru olarak tanımlanması kritik öneme sahiptir.

Stratejik planlama aşamasında tanımlanan amaç ve hedefler, aynı zamanda kaynakların öncelikli olarak tahsis edileceği alanları belirlediğinden idarenin, bu öncelikli alanlarda maruz kalabileceği risklere odaklanması, söz konusu riskleri tespit etmesi ve yönetmesi gerekir.

> Amaç ve hedeflerin seçimi öncesinde, yapılması planlanan seçimler sonucunda hangi risklerle karşı karşıya kalınabileceği de değerlendirilmelidir.

Kurumsal risk yönetimi, idarenin doğru stratejiyi seçerek hedeflerine ulaşmasına yardımcı olan bir araçtır. Bu kapsamda, sadece amaç ve hedeflerin seçilmesi sonucu karşı karşıya kalınabilecek risklerin ele alınması yeterli değildir. Amaç ve hedeflerin seçimi öncesinde, yapılması planlanan seçimler sonucunda hangi risklerle karşı karşıya kalınabileceği de değerlendirilmelidir. İdarenin seçmeyi planladığı stratejik amaç ve hedefler nedeniyle maruz kalabileceği riskler, idarenin almak isteyeceği ya da üstlenebileceği riskler değilse, bu durumda stratejik amaç ve hedefler de gözden geçirilmeli ve gerekiyorsa revize edilmelidir.

Stratejik amaç ve hedefler seviyesinde risk belirleme süreci 4 aşamada ele alınır:

Şekil 5 – Risk Belirleme Aşamaları

2.1.2.1 Stratejik Amaç ve Hedeflerin Yasal Düzenlemeler ve Üst Politika Belgeleri ile Uyumlu Olması

İdare stratejik amaç ve hedeflerini, tabi olduğu yasal düzenlemeler ile kalkınma planı başta olmak üzere üst politika belgeleri ile uyumlu olacak şekilde belirler. Tanımlanan stratejik amaç ve hedeflerin söz konusu temel düzenlemelerle uyumlu olmaması durumunda, kaynakların doğru alanlara tahsis edilmemesi sonucu verimsizlik ve yasal düzenlemelere uyumsuzluk gibi risklerle karşı karşıya kalınabilir. Bu nedenle, stratejik planlama aşamasında yasal düzenlemeler ve üst politika belgeleri ile uyum gözetilmeli ve bu sebeple maruz kalınabilecek riskler kapsama alınmalıdır.

2.1.2.2 Stratejik Amaç ve Hedeflerin İdarenin Misyon, Vizyon ve Temel Değerlerini Yansıtması

İdarenin misyon, vizyon ve temel değerleri var oluş amacını ve gelecekte olmayı planladığı noktayı yansıtır. Dolayısıyla misyon, vizyon ve temel değerler ile uyumsuz bir stratejik planlama, kaynakların idarenin var oluş amacı ile çelişen alanlara tahsisine, var oluş amacının gerçekleştirilememesine, itibar riskleri başta olmak üzere pek çok riskle karşı karşıya kalınmasına ve faaliyetlerin sürekliliğinin sağlanamamasına sebep olabilir. Bu nedenle idare, belirli bir amaç veya hedef için "misyon, vizyon ve temel değerlerimle uyumlu mu?" sorusuna "Hayır" yanıtını verdiği durumlarda; misyon, vizyon ve temel değerleriyle uyumlu olmayan amaç ve hedeflere stratejik planda yer verilemeyeceğinden dolayı amaç ve hedeflerini revize etmelidir.

2.1.2.3 Stratejik Amaç ve Hedefleri Belirleme Aşamasında Risklerin Ele Alınması

İdarenin mevzuat, üst politika belgeleri, misyon, vizyon ve temel değerleri ile uyumlu olarak belirlediği alternatif stratejik amaç ve hedeflerine ilişkin fırsat ve tehditler değerlendirilerek öncelikli riskler belirlenmeli ve ilgili risklerin yönetiminde kaynakların yeterli olup olmadığı değerlendirilmelidir. Bu kapsamda "Gelecekte karşılaşılabilecek hangi önemli olay veya durumlar stratejik amaç ve hedeflere ulaşmamızı engeller/destekler?" sorusunun idare tarafından yanıtlanması gerekir.

Stratejik amaç ve hedefleri belirleme aşamasında risklerin ele alınmasındaki amaç, gerçekleşmesi durumunda stratejik amaç ve hedeflere ulaşılmasını olumlu veya olumsuz anlamda etkileyebilecek öncelikli riskleri belirlemek ve bu risklere göre alternatif stratejilerden doğru olanı seçmektir. Stratejik amaç ve hedef seçimi sırasında risk değerlendirmesinin yapılmamış olması, farkında olmadan yönetilebilecek olandan daha fazla riski kabul etmek anlamına gelebilir. Öte yandan yanlış veya eksik değerlendirme sonucu yönetilebilecek olandan daha az risk alınarak stratejik amaç ve hedeflere ulaşılmasına katkı sağlayacak pek çok fırsat kaçırılabilir. Sonuç olarak, idare stratejik amaç ve hedeflerine ulaşamayabilir.

Doğru amaç ve hedef seçiminde risklerin göz önünde bulundurulması için aşağıdaki sorular cevaplandırılmalıdır:

Riskler **tehdit** yönünden değerlendirildiğinde;

- Önceki senelerde tecrübe ettiğimiz ve hedeflerimizi etkileyen faktörler nelerdi? Hedeflerden sapma nedenleri düşünüldüğünde, benzer hedefleri bu sene tekrar tanımlamalı mıyız?
- Hangi risk gerçekleşirse stratejilerimiz hayata geçemez veya ciddi anlamda etkilenir?
- Bu riskleri almaya istekli miyiz?
- Bu riskler ana faaliyetlerimizi gerçekleştirmeye engel olur mu?
- Belirlenen stratejiler yasal yükümlülükler ile uyumlu mu?
- Belirlenen stratejiler paydaşların birbiriyle olan ilişkilerinde çıkar çatışmasına neden olur mu?
- Son dönemde görev alanımız ve organizasyon yapımızda önemli değişiklikler oldu mu? Bu değişiklikler hangi riskleri doğurabilir?
- Görev alanımız ile ilgili son dönemde ülke düzeyinde, bölgesel düzeyde ve küresel düzeyde yaşanan veya yakın dönemde yaşanabilecek durum ve değişiklikler nelerdir? Bunlar hangi riskleri doğurabilir?

Riskler **fırsat** yönünden değerlendirildiğinde;

- Hangi risk gerçekleşirse stratejilerimiz açısından önemli bir fırsat oluşturur?
- Geçmiş deneyimlerimize dayanarak fırsat sağlayan olaylar nelerdir? Bu olaylar değerlendirildiğinde hangi hedeflere odaklanmak bizi başarıya götürür?
- Son dönemde görev alanımızda ve organizasyon yapımızda önemli değişiklikler oldu mu? Bu değişiklikler bizim için ne tür fırsatlar doğurabilir?
- Görev alanımız ile ilgili son dönemde ülke düzeyinde, bölgesel düzeyde ve küresel düzeyde yaşanan veya yakın dönemde yaşanabilecek durum ve değişiklikler nelerdir? Bunlar hangi riskleri (fırsatları) doğurabilir?

İdare yukarıdaki ve benzeri sorulara cevap vererek öncelikli risklerini değerlendirmeli, bu değerlendirme sonucunda alternatif amaç ve hedefler arasından kendisi için en uygun olanlarını seçmelidir.

2.1.2.4 Seçilen Amaç ve Hedeflerle İlişkili Risklerin Belirlenmesi

Stratejik planlama aşamasında, idare yaptığı stratejik seçimlerle kendiliğinden bazı riskler üstlenmiş olur. Seçilen stratejik amaç ve hedeflere ulaşılması, öncelikli olarak belirlenen risklerin etkili bir biçimde yönetilebilmesine bağlıdır. Risklerin etkili bir biçimde yönetilmesi; risklerin belirlenmesi, değerlendirilmesi, önceliklendirilmesi, risklere yönelik alınacak kararların belirlenmesi, uygulanması, izlenmesi ve periyodik olarak raporlanması ile mümkün olabilir.

Riskler hedef bazında belirlenir. Bu sayede, idarenin hedeflerine ulaşmasını etkileyebilecek risklerin öncelikli olarak ele alınması sağlanır.

Risklerin Belirlenmesinde Dikkat Edilecek Hususlar

- Tanımlanan riskler açık ve kolay anlaşılır olmalıdır.
- Risklerin belirlenmesi aşamasında geçmiş tecrübelerden yararlanılır.
- Riskler tehditleri, yani kurumsal amaç ve hedeflere ulaşılmasını olumsuz yönde etkileyecek potansiyel olay veya durumları içerebildiği gibi aynı zamanda fırsatları, yani kurumsal amaç ve hedeflere ulaşılmasını olumlu yönde etkileyecek potansiyel olay veya durumları da içerebilir. Örneğin; personel devir hızının yüksek olması sonucu kurumsal hafızasının kaybedilmesi ya da kurumsal hafızasının sürekliliğinin sağlanamaması idare için bir tehdit oluşturabilir. Buna karşılık yeni başlayan personelin idareye yeni bir bakış açısı kazandırması ve iş körlüğünü engellemesi gibi yeni

fırsatlar da doğabilir. Sağlık hizmetinin sunumunda yabancı uyruklu sağlık görevlilerinin hizmet vermesi sonucu iletişim sorunlarının yaşanması bir tehdit olarak değerlendirilebilir. Öte yandan bu durum sağlık turizminin gelişmesi veya farklı ülkelerde yetişmiş sağlık görevlilerinin bilgi birikiminden ve tıbbi yetkinliklerinden yararlanılması fırsatlarını yaratabilir.

- Riskin temelinde belirsizlik yatar. Bununla birlikte, farklı kavramlar olan risk ve belirsizliğin karıştırılmaması gerekir. Marmara Bölgesi'nde beklenen şiddetli bir depremin ne zaman gerçekleşeceği bir belirsizlik örneği iken; söz konusu depremin gerçekleşmesi durumunda bu bölgede faaliyet gösteren bir AR-GE merkezine olacak etkisi söz konusu idare için bir risktir.
- Bir olayın veya durumun risk olarak tanımlanabilmesi için, söz konusu olay veya durumun idarenin stratejik amaç ve hedeflerine ulaşmasını etkileyebilmesi gerekir. Amaç ve hedeflere ulaşılmasını etkileme potansiyeli bulunmayan olay veya durumlar risk olarak tanımlanmamalıdır.
- Riskler idarenin stratejik amaç ve hedefleriyle ilişkili olmalıdır. Bu nedenle, risk tanımlamalarının doğru ve tam yapılabilmesi için öncelikle idarenin stratejik amaç ve hedeflerinin doğru ve eksiksiz tanımlanmış olması gerekir. Bu nedenle hedefler formüle edilirken; belirli, ölçülebilir, ulaşılabilir, gerçekçi ve bir süre kısıtı ile somutlaştırılmış olmalarına özen gösterilmelidir.
- İdare tarafından maruz kalınabilecek riskler, değişen iç ve dış koşullara bağlı olarak zaman içinde değişim gösterebilir. Bu nedenle, riskler tanımlanırken ve yeniden değerlendirilirken değişen koşullar mutlaka göz önünde bulundurulmalıdır.
- Risk, sadece kök neden veya etki değildir. Risklerin belirlenmesi aşamasında söz konusu kavramlar karıştırılmamalıdır. Kök neden, riskin altında yatan ana sebeptir ve riskin belirlenmesi sırasında önce ana kök neden sonra alt kök nedenler değerlendirilmelidir. Riskin doğru şekilde değerlendirilmesi ve yönetilmesi için önce ana kök neden tanımlanmalı ve risk tanımı içerisinde ana kök nedene yer verilmelidir. Daha sonra, alt kök nedenler tanımlanmalıdır. Böylece risk tanımında ana kök neden ifade edilerek sade bir tanım yapılabilmektedir. Alt kök nedenlerin ayrıca tanımlanması suretiyle, sonraki aşamalarda risklere yönelik alınacak kararların ve ilave risk yönetimi faaliyetlerinin doğru ve yeterli şekilde belirlenmesi sağlanmaktadır. Etki ise, riskin sebep olabileceği nihai durumdur. Risk, ana kök nedeni ve etkilerini içerecek şekilde tanımlanmalıdır.

Risk, ana kök neden, alt kök nedenler ve etki kavramlarına ilişkin aşağıda bazı örneklere yer verilmektedir:

RİSK TANIMI	ANA KÖK NEDEN	ALT KÖK NEDENLER	ETKİ
Personelin gelişimi için gerekli eğitim ihtiyaçlarının doğru ve etkin şekilde analiz edilmemesi sonucunda personelin performans ve yetkinliklerinin geliştirilememesi ve kritik operasyonlarda hataların ve/veya verimsizliklerin yaşanması	Personelin gelişimi için gerekli eğitim ihtiyaçlarının doğru ve etkin şekilde analiz edilmemesi	• İdarenin tüm birimlerinden personel eğitim ihtiyaçlarının temin edilmemesi • Yıllık eğitim planının oluşturulmaması ve onaylanmaması • Yıllık eğitim planının tüm idare içerisinde duyurulmaması	Kritik operasyonlarda hata ve verimsizliklerin oluşması
Enerji verimliliği ve çevre duyarlılığı konusunda ilgili paydaşları kapsayan bütüncül ve etkili bir yaklaşımın olmaması sonucunda hava kirliliğinin artması	Enerji verimliliği ve çevre duyarlılığı konusundaki farkındalığın yetersiz olması	• Kontrolsüz sanayileşme • Sürekli artan enerji talebi • Yükselişe geçen şehirleşme • Azalan ormanlık alanlar • Yoğun hayvancılık faaliyetleri • Kontrol edilmeyen sera gazı salımı	Hava kirliliğinin artması
Veri güvenliğine yönelik gerekli önlemlerin alınmaması sonucunda verilerin amacı dışında kullanılması ve idare itibarının zedelenmesi	Veri güvenliğine yönelik gerekli önlemlerin alınmaması	• Bilgi ve belgelerin korunması ile ilgili idare politika ve prosedürlerinin bulunmaması • İdare içerisinde kritik bilgilerin yönetilmesinden, işlenmesinden ve imhasından sorumlu kişilerin atanmamış olması • Kritik bilgilerin sınıflandırılmaması ve ilgili bilgilere erişim yetkilerinin belirlenmemesi • Kritik verileri içeren medyaların (usb, cd vb.) şifreli olmaması, bilgi paylaşım araçlarının güvenliğinin yeterince sağlanmaması	Varlıkların gizliliğine, bütünlüğüne ve kullanılabilirliğine ilişkin güvenlik açıklarının ortaya çıkması Kritik verilerin istenmeyen kişilerce ele geçirilmesi İdare itibarının zedelenmesi

Tablo 2 – Risk, Ana Kök Neden, Alt Kök Nedenler ve Etki Örnekleri

Risklerin belirlenmesine yönelik adımlar, Risklerin Belirlenmesine Yönelik Süreç Akış Şeması (Ek–6) dokümanında açıklanmaktadır.

Riskler idareler tarafından –mesi/ması şeklinde olabileceği gibi –olabilir/edebilir şeklinde de tanımlanabilir. Örneğin riskler;

- İdare bünyesinde yeni kullanılmaya başlanacak bir programa yönelik eğitimlerin verilmemesi sonucu çalışanların hatalı işlemler gerçekleştirmesi ve operasyonel aksaklıkların yaşanması,
- İdare bünyesinde yeni kullanılmaya başlanacak bir programa yönelik eğitimlerin verilmemesi sonucunda çalışanlar hatalı işlemler gerçekleştirebilir ve operasyonel aksaklıklar yaşanabilir

olarak 2 farklı şekilde tanımlanabilir.

Hatalı/eksik ve doğru risk tanımlamalarına ilişkin aşağıda bazı örneklere yer verilmektedir:

Stratejik Hedef	Hatalı/Eksik Risk Tanımlaması	Doğru Risk Tanımlaması
Engelli vatandaşların kamu hizmetlerine erişiminin kolaylaştırılması	Personel yetersizliği	Engelli vatandaşların kamu hizmetlerine erişiminde aktif rol alacak personel sayısının yetersizliği nedeniyle engelli vatandaşa sunulan hizmetin aksaması veya kalitesinin düşmesi
Etkin sağlık hizmeti sunulması adına ulusal ve uluslararası akreditasyonunu sağlamış, hasta memnuniyetini öne çıkaran üçüncü basamak üst düzey merkezler kurulması ve mevcut merkezlerin niteliğinin geliştirilmesi	1. İş gücü kaynağının yetersizliği 2. Laboratuvar, klinik ve poliklinik hizmetlerinin sürdürülmesinde yetersiz kalma olasılığı	1. İş gücü kaynaklarının nicelik ve nitelik açısından yeterli olmaması sonucu hastalara zamanında hizmet ulaştırılamaması 2. Laboratuvar, klinik ve poliklinik hizmetlerinin sürdürülmesinde yetersiz kalınması sonucu sağlık hizmetlerinin aksaması
İdare içerisinde raporlamalarda kullanılacak olan bilgilerin doğru aktarılması için teknik iletişim ağının geliştirilmesi	Veri ve bilgilerin iletim kanallarında sorun yaşanması	Veri ve bilgilerin iletim kanallarında meydana gelebilecek teknik (-dosya transfer protokolü, e-posta vb.) veya insan kaynağı (irtibat kişisi, kırtasiyecilik vb.) temelli sorunlardan ötürü veri akışının yavaşlaması, kesintiye uğraması veya durması
İç kontrol sisteminin kamu idaresi tarafından yürütülen stratejik yönetim etkinliğini artıracak şekilde geliştirilmesi	Personelin eğitim ihtiyaçlarının karşılanmaması	İç kontrol çalışmalarında görev alan personelin eğitim ihtiyaçlarının karşılanmaması sonucunda, gerekli olan yetkinliklerin geliştirilememesi ve sürecin istenilen kalitede gerçekleştirilememesi
Paydaşlarla iş birliği içinde sunulan hizmetlerin kalitesinin arttırılması	İdareler arası yetki çakışması	Farklı idareler arasında oluşabilecek yetki çakışması nedeniyle halka sunulacak hizmetlerde aksamalar veya kesintiler yaşanması
Uluslararası alanda tutarlı, anlamlı ve cazip bir Türkiye markası yaratmaya yönelik tanıtım stratejilerinin geliştirilmesi	İdarenin ana faaliyet konuları ile ilgili olmayan projelerin desteklenmesi	İdarenin ana faaliyetleri ile ilgili olmayan projelerin desteklenmesi sonucunda kaynakların etkin kullanılamaması ve ana faaliyetleri ilgilendiren projelerin kaynak yetersizliği nedeniyle tamamlanamaması

Tablo 3 –Hatalı/Eksik ve Doğru Risk Tanımlama Örnekleri

Risk Belirlemede Kullanılacak Temel Yöntem:

> İdarelerde SGB koordinasyonunda üst yönetici başkanlığında, hedeflerle ilişkili görev ve sorumluluğu bulunan birim yöneticilerinin katılımıyla "stratejik risk çalıştayları" organize edilir.

Stratejik risk çalıştayları, idarenin stratejik amaç ve hedeflerine ulaşmasını etkileyebilecek risklerin belirlenmesi, değerlendirilmesi, önceliklendirilmesi, bu risklere yönelik alınacak kararların belirlenmesi ve ilave risk yönetimi faaliyetinin tartışılması amacıyla üst yönetici başkanlığında gerçekleştirilen toplantılardır. Bu toplantılar, hedeflerle ilişkili görev ve sorumluluğu bulunan birim ve alt birim yöneticilerinin katılımıyla ve çalıştay kolaylaştırıcısının yönlendirmesi ile gerçekleştirilir.

Bu çalıştaylarda stratejik planlama aşamasında gerçekleştirilen analiz sonuçlarından (PESTLE, GZFT, vb.) faydalanılır. İdarenin GZFT analizi sırasında belirlenen zayıf yönleri, çoğu zaman risklerin kök nedenlerine işaret edebilmektedir. Örneğin, bir idarenin stratejik planında "Yeni işe giren işçiler tarafından iş güvenliğiyle alakalı eğitim ve uyarılara, gerekli önemin verilmemesi," zayıf yön olarak tanımlanmaktadır. İlgili zayıf yön, bu idare için iş güvenliği risklerinin doğabileceğine işaret etmektedir.

> GZFT analizi kapsamında belirlenen fırsat ve tehditler bir yandan idarenin strateji geliştirmesine yardımcı olurken aynı zamanda belirlenen stratejik amaç ve hedeflere ulaşmak için yürütülen faaliyetlerle ilgili ortaya çıkabilecek risklerin belirlenmesinde de yol göstericidir.

Örneğin, bir üniversitenin stratejik planında;

Fırsat: Araştırma ve girişimcilik konusunda verilen desteklerin artması

Amaç: Araştırma Üniversitesi statüsünü sürdürülebilir kılmak

Hedef: Araştırma proje kaynaklarının sürekli artırılması ve çeşitlendirilmesi

olarak tanımlanmıştır.

İlgili hedefe yönelik "Üniversite kaynaklarının yeterli olmaması sonucu araştırma ve girişimcilik projelerinin etkin olarak yapılamaması" bir risk olarak tanımlanabilir. Bu riske karşılık üniversite kaynaklarının yetersizliği sebebi ile dış destekli araştırmaların artırılarak kaynakların sürekli artırılması ve çeşitlendirilmesi yani riskin fırsata dönüştürülmesi sağlanabilir.

Tehdit yönünden değerlendirildiğinde ise hedefe ilişkin riskler belirlenirken yine GZFT sonuçlarından faydalanılabilir.

Üniversitenin stratejik planında;

Tehdit: Bazı programlara kapasitesinin çok üstünde öğrenci alınması nedeniyle kalitenin düşmesi

Amaç: Akredite eğitim programlarını artırmak ve nitelikli mezun vermek

Hedef: Eğitimin kalitesini geliştirerek akredite eğitim programlarının sayısının artırılması

olarak tanımlanmaktadır.

GZFT analizi sırasında tanımlanan "Bazı programlara kapasitesinin çok üstünde öğrenci alınması nedeniyle eğitim kalitesinin düşmesi" tehdidinden yola çıkılarak risk tanımlaması yapılabilir. Bu kapsamda; "Belirli programlara kapasitenin üzerinde öğrenci kabulü yapılması sebebiyle, kaliteli eğitim hizmeti verilememesi ve nitelikli mezun yetiştirilememesi" riski tanımlanabilir ve gerekli ilave risk yönetimi faaliyetleri uygulanabilir.

Çalıştay yapılırken beyin fırtınası yönteminin kullanılması yararlı olur. Bu yöntemle yönetici ve çalışanlar riskleri belirlemek için bir araya gelerek bilgi ve deneyimlerini paylaşırlar. Böylece, idare içinde risk farkındalığının artırılmasına da katkı sağlanır.

Çalıştaylarda;

- Riskler hedef bazında belirlendiğinden çalıştaylar, üzerinde çalışılacak olan stratejik amaç ve hedeflerle bağlantılı tüm birim yöneticileri dâhil edilecek şekilde organize edilir. Doğrudan hedefle ilgili olmayan fakat o hedef altında tanımlanan riskin yönetilmesinde rol alacak birimlerin de çalıştaylar sırasında görüşlerinin alınması önemlidir.
- Risklerin belirlenmesi ve değerlendirilmesi adımları önce bireysel daha sonra grup çalışmaları ile gerçekleştirilir. Risklerin belirlenmesi aşamasında, idarenin stratejik amaç ve hedeflerine yönelik riskler önce katılımcılar tarafından bireysel olarak belirlenir ve çıktısı alınan Bireysel Risk Belirleme Formuna (Ek–5) kaydedilir. Sonrasında, katılımcılar belirledikleri riskleri kendi aralarında tartışarak nihai bir sonuca ulaşırlar. Katılımcılar tarafından belirlenen bu nihai riskler Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formuna (Ek–12) kaydedilir.
- Belirlenen risklere yönelik bireysel değerlendirmeler öncelikle çıktısı alınan Bireysel Risk Değerlendirme Formunda (Ek–7) yapılır. Değerlendirme sonuçları, grup içerisinde tartışılır ve nihai kararlar bilgisayar ortamında Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formu–Katılımcı Değerlendirmeleri (Ek–12) sayfasına

aktarılır. İlgili sayfada, değerlendirme sonuçlarının ağırlıklı ortalaması otomatik hesaplanır ve konsolide edilir. Konsolide puanlama ile bilgiler aynı doküman içerisinde Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formu sayfasına otomatik aktarılır.

- Risklere yönelik alınacak kararlar ortak çalışma sonucu verildiğinden, ilgili kararlar Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formuna (Ek–12) kaydedilerek izlemeye alınır ve daha sonra takip çalışmaları ile bu form üzerinden raporlanır.

Çalıştaya ilişkin adımlar ve dikkat edilecek hususlar Stratejik Risk Çalıştayı Adımları (Ek–4) dokümanında detaylı olarak açıklanmaktadır. Çalıştay kolaylaştırıcısı tarafından, çalıştay öncesi ve çalıştay süresince dikkat edilmesi ve yerine getirilmesi gereken hususlara sırasıyla Ek–14 Çalıştay Kolaylaştırıcısına Yönelik Bilgi Notları_Risklerin Belirlenmesi, Ek–15 Çalıştay Kolaylaştırıcısına Yönelik Bilgi Notları_Risklerin Değerlendirilmesi ve Ek–16 Çalıştay Kolaylaştırıcısına Yönelik Bilgi Notları_Riske Yönelik Alınacak Kararların Belirlenmesi adlı dokümanlarda yer verilmektedir.

Çalıştayların etkin şekilde gerçekleştirilebilmesi için gerekli soruları soracak ve yönlendirmeleri yapacak bir kolaylaştırıcıya ihtiyaç vardır. Kolaylaştırıcının temel görevi, idarenin stratejik amaç ve hedeflere ulaşmasını etkileyebilecek risklerin değerlendirilmesi, önceliklendirilmesi ve idare açısından önemli kararların alınması süreçlerinde çalıştay katılımcılarına yardımcı olmaktır. Kolaylaştırıcının, bu rolde deneyim kazanmış bir kişi olması yöntemin etkili ve verimli olmasını destekleyecektir. Ek olarak, çalıştayın organize edilmesi, kapsamın, amaçların ve katılımcılara yol gösterici olabilecek kavramsal tanımlamaların katılımcılara anlatılması, katılımcılar tarafından değerlendirilecek soruların geliştirilmesi, çalıştayda kullanılacak olan formların eksiksiz ve doğru bir şekilde doldurulması, sonuçların kayıt altına alınması, katılımcı yaklaşımın gözetilmesi ile dengeli bir tartışma ortamının oluşturulması ve sürdürülmesinde kolaylaştırıcının sorumlulukları bulunmaktadır.

Kamu Kurumsal Risk Yönetimi Yaklaşımı Örnek Soru Seti (Ek–2) dokümanında risklerin belirlenmesi aşamasında sorulabilecek örnek sorulara yer verilmektedir.

2.1.2.5 Risk İştahının Belirlenmesi

Risk iştahı (risk alma istekliliği), idarenin stratejik hedefleri doğrultusunda kabul etmeye hazır olduğu en yüksek risk seviyesidir. İdare için, hangi seviyenin üzerindeki risklerin kabul edilemeyeceğinin belirlenmesine ilişkin yol gösterici rol oynar. Üst yönetici tarafından hedef bazında belirlenir.

> Risk iştahı idarenin hangi alanda ne kadar riski üstlenmeye istekli olduğuna karar vermesi açısından önemlidir ve stratejik planlama aşamasında amaç ve hedefler ile birlikte değerlendirilerek belirlenir.

Risk iştahı iç ve dış çevre, yaşanan değişimler ve idarenin risk kültürü gibi çok sayıda faktörden etkilenir. Örneğin idare, Kişisel Verilerin Korunması Kanunu ile getirilen yükümlülükler ve uyumsuzluk durumunda maruz kalınabilecek yaptırımlar nedeniyle, bilgi güvenliğinin sağlanması hedefine yönelik risk iştahı seviyesini düşürebilir. Böylece söz konusu riskin gerçekleşmesi durumunda maruz kalınacak zararları azaltmak üzere gerekli önlemleri önceden hayata geçirebilir.

İdarenin birimleri ya da alt birimlerinin risk iştahları farklılık gösterebilir. Üst yönetici tarafından hedef bazında belirlenmekle birlikte bu sınırlar içinde kalınması şartıyla birimler/alt birimler tarafından farklı iştah düzeylerinin belirlenmesi de mümkündür. Harcama birimlerinde stratejik hedeflerle ilişkisi kurulamayan riskler mevcut ise bunlara ilişkin risk iştahı birim düzeyinde belirlenir.

> İdarenin hedefleri bazında çalıştaylar sırasında tanımlanan risk iştah seviyeleri, idarenin ortak risk algısı çerçevesinde değerlendirilir ve her bir hedef için belirlenen risk iştah seviyeleri onaylanır.

Yüksek risk iştahının yüksek kayıplara neden olabileceği algısı ile gereğinden düşük seviyede risk iştahı tanımlaması idarenin fırsatları değerlendirmesine engel teşkil edebilir. Risk iştah seviyesinin gereğinden yüksek tanımlanması da idarenin dayanabileceğinden fazla risk alarak stratejik amaç ve hedeflerine ulaşmada başarısız olmasına ya da stratejik amaç ve hedeflerine ulaşırken beklenmeyen maliyetlere katlanmasına neden olabilir.

Risk iştahı, risk yönetiminin ayrılmaz bir parçasıdır. Bir organizasyonun değer yaratma arayışında, kabul etmeye istekli olduğu risk türleri ve düzeyleri hakkında alacağı kararlara rehberlik eder. Risk iştahı düzeyi; idarenin risk yönetimi kapasitesindeki değişimlere paralel olarak zamanla değişebilen bir kavramdır. Ayrıca, strateji seçme ve geliştirme süreci ile risk iştahının belirlenmesi birlikte düşünülmelidir. Birçok idare strateji ve risk iştahını birbirine paralel ve bağlantılı olacak şekilde strateji belirleme sürecinde belirler. İdarenin tüm riskleri için geçerli olan tek bir risk iştahından söz edilemez.

Bazı idareler, risk iştahını niteliksel terimlerle, diğerleri niceliksel terimlerle tanımlayabilir. Risk iştahını tanımlamada seçilen yaklaşım ne olursa olsun, risk iştahı idarenin kültürünü yansıtmalıdır. Bir idare için en iyi yaklaşım, genel olarak riski değerlendirmede kullanılan analiz ile aynı/uyumlu olandır (nitel veya nicel). Risk iştahının belirlenmesi, aslında riskler ve fırsatlar arasında bir denge kurulmasıdır. Risk iştahının belirlenmesi sorumluluğu yönetime aittir.

Risk iştahı hedef bazında tanımlanır. İdarenin bütün kademelerinde geçerli olan tek bir risk iştahı tanımından veya seviyesinden bahsedilemez.

Risk iştahı yüksek, orta ve düşük olmak üzere 3 seviyede belirlenir.

Belirli bir hedef için belirlenen risk iştahı düştükçe o hedefi gerçekleştirmek için katlanılan kaynak (işgücü, zaman, bütçe vb) maliyeti artar.

DERECE	RİSK İŞTAH SEVİYESİ	HEDEF	RİSK VE RİSK İŞTAHI
3	Yüksek	Eğitim hizmetinin zorunlu olmasına bağlı olarak her çocuğa her koşulda eğitim hizmeti verilmesi	Her öğrenciye gereken ihtimamın gösterilememesi (riski) pahasına her öğrenciye her koşulda (mevcut kaynaklarla (işgücü, zaman, bütçe) ya da ilave bir kaynak maliyetine katlanmaksızın) eğitim hizmeti verilmesi İlgili hedefe yönelik risk alma istekliliği yüksek seviyede
2	Orta	Kurumsal kapasiteyi artırmak için personelin eğitim ihtiyaçlarının karşılanması	Mevcut kaynaklarla (işgücü, zaman, bütçe) personelin eğitim ihtiyacının tam olarak karşılanamaması pahasına (yine personel yetkinliğinin mümkün olduğu ölçüde artırılması için) eğitim faaliyetleri düzenlenmesi İlgili hedefe yönelik risk alma istekliliği orta seviyede
1	Düşük	Gıda güvenilirliğinin sağlanması	Piyasada halk sağlığına tehdit oluşturan ürünlerin bulunması Kabul edilemez nitelikteki bu risk için mevcut ve ilave kaynaklarla (işgücü, zaman, bütçe) gıda güvenilirliğinin sağlanmasına yönelik her yolun denenmesi İlgili hedefe yönelik risk alma istekliliği düşük seviyede

Tablo 4 – Risk İştah Seviyeleri

Her bir hedefle ilişkili riskler ve risk iştahı seviyesi tanımlandıktan sonra, hedef bazında belirlenen risk iştahı seviyesi ile risk seviyeleri karşılaştırılır. Risk iştahı seviyesi, risklere yönelik alınacak kararlar belirlenirken göz önünde bulundurulur.

Örnek 1:

AMAÇ	Kentsel düzenleme, alt ve üst yapı çalışmaları, çağın gereklerine uygun, sosyal, kültürel değerleri ile halkın beklentilerine uygun olarak yapılacaktır.
HEDEF	Plan döneminde belediye sınırları içerisinde kalan yol, kaldırım, bordür, tretuvar vb. fiziksel şartlar iyileştirilecektir.
RİSKLER	• Yol çalışma projelerinden kaynaklanan teknik hatalar (yol eğimi, viraj açısı vb.) nedeniyle kazaların meydana gelmesi, bu nedenle can kayıpları yaşanması ve belediyenin güvenilirliği ve itibarının zedelenmesi • İdarenin bütçesinin yetersiz kalması sonucu, projelerin yarım kalması ve idarenin itibar kaybı yaşaması
RİSK İŞTAHI	**Orta** – Belediye sınırları içerisinde kalan yolların iyileştirilmesi için gerekli girişimlerin yapılması ve yeterli kaynağın ayrılması, bu hedefle ilişkili yüksek ve çok yüksek seviyedeki risklerin kabul edilmemesi ve söz konusu risklere yönelik ilave risk yönetimi faaliyetlerinin uygulanması kararlaştırılmıştır.

Örnek 2:

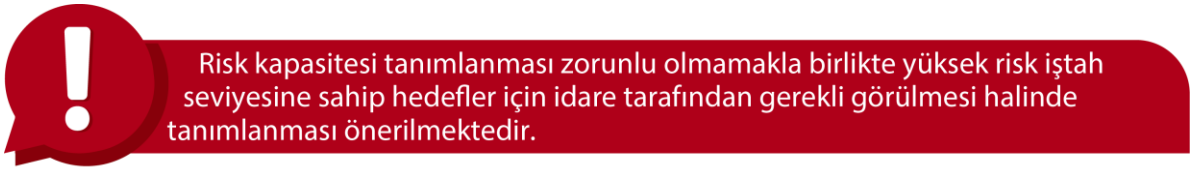
AMAÇ	Bitki sağlığını koruyucu tedbirler almak, hayvan hastalık ve zararlılarını kontrol ve bertaraf etmek, hayvan refahını sağlamak
HEDEF	Hayvan hastalıkları ile mücadelede kullanılan veteriner sağlık ürünlerinin kalite ve etkinliklerini arttırmak
RİSKLER	• Numune alma planlarına ilişkin stratejilerin doğru belirlenmemesi nedeniyle hayvanlarda var olan maddelerin tespit edilememesi • Ruhsatsız ilaç kullanımı sebebiyle bu ilaçların denetimler sırasında kontrol edilememesi ve tespit edilememesi sonucunda ilaçlı gıdaların piyasaya sürülmesi (ilgili ilaçların kullanıldığı hayvanlara ait et ve süt ürünleri)
RİSK İŞTAHI	**Düşük** – Hayvan hastalıkları ile mücadele ve gıda güvenilirliğini sağlamak idarenin en öncelikli hedefi olduğu için idare tarafından bu hedefle ilişkili olası risklerin kabul edilmemesi ve söz konusu risklere yönelik ilave risk yönetimi faaliyetlerinin uygulanması kararlaştırılmıştır.

2.1.3 Risk Kapasitesinin Belirlenmesi

Risk kapasitesi, idarenin faaliyetlerine son vermeden alabileceği en yüksek risk seviyesidir. Bir idarenin risk kapasitesi, risklere en fazla ne kadar dayanabileceğini bilmesi açısından önemlidir.

Risk kapasitesi;

- Risk iştah seviyesi tanımlandıktan sonra hedef bazında tanımlanır.
- Her hedef için tanımlanmaz. Risk iştahı yüksek olarak sınıflanan hedefler için tanımlanır.
- Nicel veya nitel olarak tanımlanabilir.



Stratejik hedeflerle ilişkili riskler risk kapasitesinin üzerinde ise yani, ilgili stratejik amaç ve hedefleri gerçekleştirmek için maruz kalınacak risk, idarenin faaliyetlerini durdurma noktasına getiriyorsa veya temel hizmetlerin kesintiye uğramasına neden oluyorsa, söz konusu stratejik amaç ve hedefler stratejik planlama aşamasında gözden geçirilerek revize edilmelidir. Aksi halde idare, kapasitesinin üzerinde iştah seviyesi tanımlar ve söz konusu risklerin neden olabileceği kayıplara dayanamayabilir. Bu nedenle risk iştahı tanımlanırken risk kapasitesi göz önünde bulundurulmalıdır. Risk kapasitesi aşağıda örneklerle açıklanmaktadır:

Örnek 1:

AMAÇ	Sunulan hizmetlerin kalitesini paydaşlarla iş birliği içinde artırmak
HEDEF	Etkin sağlık hizmeti sunmak için, ulusal ve uluslararası akreditasyonunu sağlamış, hasta memnuniyetini öne çıkaran üçüncü basamak üst düzey sağlık merkezleri kurulması ve mevcut merkezlerin niteliğinin geliştirilmesi
RİSKLER	• Gelirlerin giderleri karşılayamaması nedeniyle hastane borçlarının giderek artması sonucu, cihaz ve sarf malzeme temininde güçlük çekilmesi, hastalara etkili ve kesintisiz hizmet verilememesi • Kaynakların (sağlık görevlisi, teçhizat vb.) yeterli olmaması sonucu hastalara zamanında hizmet ulaştırılamaması ve idare itibarının zarar görmesi
RİSK İŞTAHI	**Yüksek** – Sağlık hizmetinin ertelenemez olması sebebiyle her durumda etkin ve kesintisiz hizmet verilmesi kararlaştırılmıştır.
RİSK KAPASİTESİ	• Hastanenin mevcut tüm yataklı ve ayakta hizmet kapasitesinin dolu olması • Tıbben tedavi edilebilir olsa dahi hastanenin yeni hasta kabul edecek yeterli kaynağının olmaması

İlk örnekte, paydaşlar ile iş birliği içinde sunulan hizmetlerin kalitesinin arttırılması hedeflenmektedir. Belirlenen stratejik amaç ve hedefe ilişkin öncelikli riskler ele alındığında, gelir gider arasındaki dengesizlik sonucunda cihaz ve sarf malzeme temininde güçlük çekilmesi, hastalara etkin ve kesintisiz hizmet verilememesi ve insan kaynağının yeterli olmaması sonucu hastalara zamanında hizmet ulaştırılamaması ve idare itibarının zarar görmesi ile karşı karşıya kalınabileceği öngörülmektedir. İlgili hedef ve ilişkili riskler değerlendirildiğinde risk iştahı 'yüksek' olarak tanımlanmaktadır. Bu, idarenin söz konusu hedefi gerçekleştirmek için risk almaya istekli olduğunu ifade etmektedir. Risk kapasitesi de hastanenin mevcut tüm yataklı ve ayakta hizmet kapasitesinin dolu olması ve tıbben tedavi edilebilir olsa dahi hastanenin yeni hasta kabul edecek yeterli kaynağının olmaması olarak belirlenmiştir. İlgili idarenin böyle bir durumda, hedefinin ulaşılabilir olup olmadığını gözden geçirmesi ve gerekiyorsa hedefini risk kapasitesini geçmeyecek şekilde revize etmesi gerekmektedir.

Örnek 2:

AMAÇ	Tarımsal üretimde ihracata dayalı büyüme
HEDEF	Tarımsal üretimde ihracatı %25 arttırmak
RİSKLER	• Mevcut su kaynaklarının yetersizliği sonucunda hedeflenen üretim seviyesine ulaşılamaması • Mevcut su kaynaklarının ihraç edilecek tarım ürünlerine tahsis edilmesi nedeniyle yurtiçi tarımsal üretim talebinin karşılanamaması
RİSK İŞTAHI	**Yüksek** – Tarımsal ürün ihracatının arttırılması için gerekli girişimlerin yapılması ve yeterli kaynağın ayrılması kararlaştırılmıştır.
RİSK KAPASİTESİ	Nitel: Ülkenin su kaynaklarının tükenme sınırına gelmesi Nicel: Kişi başına düşen su miktarının 1000m3'ten az olması

İkinci örnekte, tarımsal üretimde ihracat bazlı büyüme amacıyla ihracatın yüzde 25 oranında arttırılması hedeflenmektedir. Belirlenen stratejik amaç ve hedefe ilişkin öncelikli riskler ele alındığında, mevcut su kaynaklarının yetersizliği sonucunda hedeflenen üretim seviyesine ulaşılamaması veya su kaynaklarının ihraç edilecek tarım ürünlerine tahsis edilmesi nedeniyle yurtiçi tarımsal üretim talebinin karşılanamaması gibi risklerle karşı karşıya kalınabileceği öngörülmektedir. İlgili hedef ve ilişkili riskler değerlendirildiğinde, risk iştahı 'yüksek' olarak tanımlanmaktadır. Bu, idarenin söz konusu hedefi gerçekleştirmek için yüksek seviyede risk almaya istekli olduğunu ifade etmektedir. Risk kapasitesi olarak da ülkenin su kaynaklarının tükenme sınırına gelmesi veya kişi başına düşen su miktarının 1000 m^3'ten aşağı bir seviyeye düşmesi belirlenmektedir. İlgili idarenin böyle bir durumda, hedefinin ulaşılabilir olup olmadığını gözden geçirmesi ve gerekiyorsa hedefini risk kapasitesini geçmeyecek şekilde revize etmesi gerekmektedir.

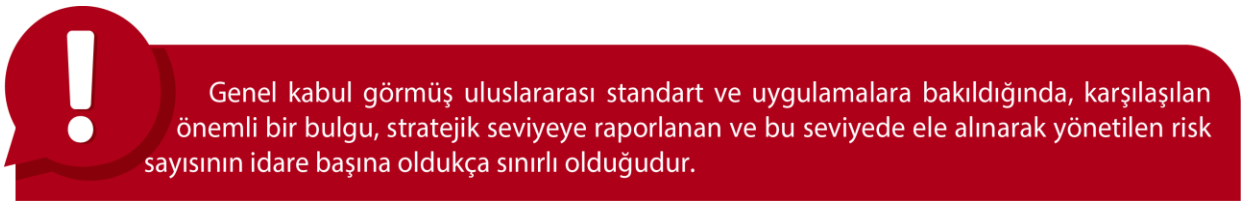
2.1.4 Risklerin Birim, Faaliyet ve Süreçler Seviyesinde Ele Alınması

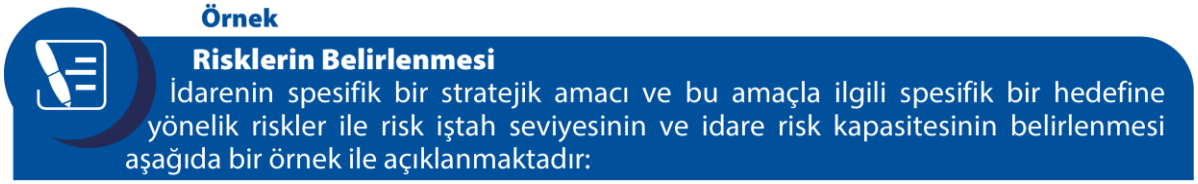
İdarelerde kurumsal risk yönetimi yaklaşımı ile iç kontrol sisteminin etkileşim halinde yürütülmesi, oluşturulacak katma değer açısından oldukça önemlidir.

Kurumsal risk yönetimi sürecinde stratejik seviyede ele alınması gereken öncelikli risklere odaklanılırken, iç kontrol sürecinde faaliyetlerin etkili, ekonomik ve verimli bir şekilde yürütülmesini, varlık ve kaynakların korunmasını, malî bilgi ve yönetim

bilgisinin zamanında ve güvenilir olarak üretilmesini olumsuz yönde etkileyebilecek birim, faaliyet ve süreç seviyesinde risklere odaklanılır.

İdarelerde stratejik planlama süreciyle başlanan ve kendini tekrar edecek şekilde uygulanan kurumsal risk yönetimi yaklaşımında, risklerin belirlenmesi aşamasında, birim, faaliyet ve süreç seviyesindeki risklerden tek başına veya bir arada değerlendirildiğinde stratejik amaç ve hedeflere ulaşılmasını etkileyebilecek öncelikte olanlar mutlaka kurumsal risk yönetimi kapsamına alınmalı, değerlendirilmeli, izlenmeli ve raporlanmalıdır. Benzer şekilde birim, faaliyet ve süreç riskleri değerlendirilirken de kurumsal risk yönetimi kapsamında belirlenmiş olan amaç ve hedeflerle ilişkili risk evreni ve öncelikli riskler mutlaka incelenmeli ve değerlendirilmelidir. Kurumsal risk yönetimi yaklaşımı ve iç kontrol sistemi arasında bilgi akışı sağlanmasının, her iki yaklaşımın katma değerini arttıracağı unutulmamalıdır.





İdarenin Stratejik Hedefine Ulaşmasını Etkileyebilecek Risklerin Belirlenmesi

AMAÇ	İdarenin hizmetlerini daha etkin ve hızlı bir şekilde sunmak
HEDEF	Bilgi teknolojisi sistemlerini ve uygulamalarını geliştirmek

İdare tarafından söz konusu stratejik amaç ve hedefe ulaşılmasını etkileyebileceği düşünülen iki adet risk belirlenmiş olsun:

	ÖRNEK RİSKLER	RİSK EVRENİ (RİSK KATEGORİSİ)
Risk 1	Yeterli ihtiyaç analizi yapılmadan idarenin organizasyon yapısı, iş yapış biçimi ve hedefleriyle uyumlu olmayan bir bilişim sisteminin seçilmesi sonucu kaynakların etkin kullanılamaması	Stratejik Risk

Risk 2	İdarenin bilgi teknoloji sistemlerinde gerçekleştirilen güncellemeler sonrasında, kullanıcı personele yetersiz eğitim verilmesi nedeniyle çalışanların güncel sistemi etkin kullanamaması ve operasyonel aksaklıkların yaşanması	Operasyonel Risk

Yukarıdaki stratejik hedefe yönelik riskler belirlenirken GZFT analizinin sonuçları (güçlü ve zayıf yönler ile idare dışında oluşabilecek tehdit ve fırsatlar) da göz önünde bulundurulmuştur.

Risk İştah Seviyesi ile Risk Kapasitesinin Belirlenmesi

İdare tarafından belirlenen söz konusu stratejik amaç ve hedefe yönelik risk iştahı ile idarenin risk kapasitesine aşağıda yer verilmektedir:

RİSK İŞTAHI	**Orta** - Bilgi teknolojisi sistemlerini ve uygulamalarını geliştirmek için gerekli girişimlerin yapılması ve yapılan analizler sonucu gerekli olan insan ve mali kaynağın ayrılması kararlaştırılmakla birlikte idarenin karşılayamayacağı seviyede teknoloji yatırımının yapılmaması gerektiği düşünülmektedir.
RİSK KAPASİTESİ	Bilgi teknolojileri sistemlerinin devre dışı kalması ile idarenin faaliyetlerini gerçekleştiremez noktaya gelmesi

2.2 Risklerin Değerlendirilmesi

Kurumsal risk yönetimi yaklaşımında, risklerin belirlenmesinden sonraki adım, risklerin değerlendirilmesidir. Risklerin değerlendirilmesi, risk seviyelerinin belirlenmesini ve risklerin önceliklendirilmesini kapsar.

Stratejik amaç ve hedeflerini gerçekleştirmek üzere faaliyet gösterirken idarenin maruz kalabileceği her risk eşit düzeyde öneme sahip değildir. Çeşitli önem düzeylerine sahip tüm risklerin yönetilmeye çalışılması, kaynakların etkili, ekonomik ve verimli kullanılması ilkesiyle çelişeceği ve maliyet etkin bir yaklaşım olamayacağı için, riskler

> Risk seviyelerinin belirlenmesi, risklerin etki ve olasılık seviyeleri ile idarenin mevcut risk yönetimi faaliyetlerinin yeterliliği göz önünde bulundurularak risklerin kendi aralarında sınıflandırılmasıdır.

önceliklendirmeye tabi tutulur ve hangi risklerin yönetileceği tespit edilir.

Risk değerlendirme çalışmalarında ilgili tüm tarafların katılımının sağlanması oldukça önemlidir. Bu nedenle risklerin değerlendirilmesi aşamasında çalıştay yönteminden yararlanılır. Stratejik planın hazırlık aşamasında SGB koordinasyonunda üst yöneticinin başkanlığında ilgili birim yöneticilerinin katılımıyla organize edilen stratejik risk çalıştayları sırasında riskler değerlendirilir.

Risklerin değerlendirilmesine yönelik adımlar Risklerin Değerlendirilmesine Yönelik Süreç Akış Şeması (Ek–8) dokümanında açıklanmaktadır.

2.2.1 Risk Seviyelerinin Belirlenmesi

Risk seviyelerinin belirlenmesi aşamasında, öncelikle risklerin etki ve olasılık seviyeleri puanlanır. Ardından idarenin söz konusu risklere yönelik yürütmekte olduğu mevcut risk yönetimi faaliyetlerinin yeterliliği değerlendirilerek, önceliklendirmede esas alınacak risk seviyesine ulaşılır.

2.2.1.1 Risklerin Etki ve Olasılık Seviyelerinin Belirlenmesi

Risk seviyelerinin belirlenmesinde dikkate alınan faktörlerden etki, riskin gerçekleşmesi halinde idare üzerinde yaratacağı olumlu ya da olumsuz sonuçları; olasılık ise bir olayın/durumun belli bir zaman dilimi içerisinde meydana gelme ihtimalini ifade eder.

Çok yüksek etkiye sahip bir riskin olasılığı düşük olabilirken, olasılığı çok yüksek olan bir riskin etkisi düşük olabilir. Örneğin; 4. derece deprem bölgesinde yerleşik bir idare için deprem sonucu zarar görme riskinin olasılığı düşük olmakla birlikte, riskin gerçekleşmesi durumunda o idarenin faaliyetleri üzerindeki etkisi çok yüksek seviyede olabilir. Bu nedenle, risk seviyelerinin belirlenmesinde etki ve olasılık faktörleri bir arada değerlendirilir.

Risklerin etki ve olasılıklarının değerlendirilmesinde, etki için çok düşük, düşük, orta, yüksek ve çok yüksek olmak üzere beşli bir ölçek kullanılır.

ETKİ PUANI	ETKİ SEVİYESİ	AÇIKLAMA
5	Çok Yüksek	İdarenin stratejik amaç ve hedeflerine ulaşamamasına, stratejik amaç ve hedeflerinden çok ciddi derecede sapmasına veya idare tarafından sunulan hizmetlerin uzun süre duraklamasına neden olabilecek olay veya durumlar
4	Yüksek	İdarenin stratejik amaç ve hedeflerinden önemli derecede sapmasına veya idare tarafından sunulan hizmetlerin önemli bir süre duraklamasına neden olabilecek olay veya durumlar
3	Orta	İdarenin stratejik amaç ve hedeflerinden kabul edilebilir derecede sapmasına veya idare tarafından sunulan hizmetlerin belirli bir süre duraklamasına neden olabilecek olay veya durumlar
2	Düşük	İdarenin stratejik amaç ve hedeflerine ulaşmasında düşük seviyede etkisi olabilecek olay veya durumlar
1	Çok Düşük	İdarenin stratejik amaç ve hedeflerine ulaşmasında çok düşük, kolaylıkla gözlemlenemeyecek seviyede etkisi olabilecek olay veya durumlar

Tablo 5 – Etki Seviyeleri

Etki değerlendirmesinde risklerin finansal, operasyonel, itibar, uyum ve stratejik etki kriterleriyle ele alınması mümkündür. İdareler, kendi organizasyon yapılarına ve faaliyet alanlarına uygun olarak farklı etki kriterlerini de göz önünde bulundurabilirler ve söz konusu kriterleri Risk Strateji Belgesinde tanımlayabilirler.

ETKİ PUANI	FİNANSAL ETKİ	OPERASYONEL ETKİ	İTİBAR ETKİSİ	UYUM ETKİSİ	STRATEJİK ETKİ
5	Çok ciddi maddi kayıplara neden olabilecek olay veya durumlar	Hizmet birimlerinde faaliyetlerin yürütülmesinde çok ciddi gecikmelerin yaşanması (Örneğin; 1 haftadan fazla)	Paydaşların uzun süreli ve tamamen güven kaybı	Ağır yaptırımlar Mevzuat değişikliği	İdarenin stratejik amaç ve hedeflerine ulaşamaması
4	Önemli ölçüde maddi kayba neden olabilecek olay veya durumlar	Önemli operasyonel kesintilere sebep olan olayların yaşanması, hizmet sağlanmasında gecikmelerin yaşanması (Örneğin; 2-3 gün)	Kamuoyunda uzun süreli ve geniş çaplı güven kaybı	Önemli yaptırımlar Önemli hakların kaybedilmesi	İdarenin stratejik amaç ve hedeflerine ulaşmasında önemli ölçüde başarısızlıklar yaşaması
3	Orta düzeyde maddi kayba neden olabilecek olay veya durumlar	Bazı operasyonel kesintilere sebep olan olayların yaşanması, hizmet sağlanmasında önemsiz gecikmelerin yaşanması (Örneğin; 6 saat)	Kamuoyunda önemli ancak kısa süreli güven kaybı(Örneğin; 6 saat)	Orta derece yaptırımlar Bazı hakların kaybedilmesi	İdarenin stratejik amaç ve hedeflerine ulaşmasında bazı başarısızlıklar yaşaması
2	Düşük düzeyde maddi kayba neden olabilecek olay veya durumlar	Önemsiz operasyonel kesintilere sebep olan olayların yaşanması, hizmet devamlılığının küçük aksaklıklarla devam etmesi (Örneğin; 2 saatten az)	Kısa süreli ve bazı paydaşların sınırlı ölçüde güven kaybı	Kınama Düşük derece yaptırım	İdarenin stratejik amaç ve hedeflerine ulaşmasına engel olmaması ancak bir ölçüde olumsuz etkilemesi
1	Çok düşük düzeyde maddi kayba neden olabilecek olay veya durumlar	Faaliyetlerin sürekliliğini kesintiye uğratmayacak olayların yaşanması (Örneğin; 1-2 dakika)	Güven kaybına dönüşmeyen bazı münferit durum veya olaylar	Uyarı Herhangi bir kayba sebebiyet vermeyecek seviyede çok düşük derece yaptırım	İdarenin stratejik amaç ve hedeflerine ulaşmasına engel olmaması ancak önemsiz düzeyde olumsuz etkilemesi

Tablo 6 – Etki Kriterleri

Belirlenen riskin birden fazla etki kriterinin olması durumunda, en yüksek etki seviyesine sahip kriter göz önünde bulundurulmalı ve o kriterin puanı esas alınmalıdır.

Risklerin etki ve olasılıklarının değerlendirilmesinde, olasılık için çok zayıf olasılık, zayıf olasılık, olası, yüksek olasılık ve neredeyse kesin olmak üzere yine beşli ölçek kullanılır.

OLASILIK PUANI	OLASILIK SEVİYESİ	AÇIKLAMA
5	Neredeyse Kesin	Stratejik amaç ve hedefe ulaşılması öngörülen sürede gerçekleşme olasılığı neredeyse kesin olan olay veya durumlar
4	Yüksek Olasılık	Stratejik amaç ve hedefe ulaşılması öngörülen sürede gerçekleşme olasılığı yüksek olan muhtemel olay veya durumlar
3	Olası	Stratejik amaç ve hedefe ulaşılması öngörülen sürede gerçekleşme olasılığı mümkün olay veya durumlar
2	Zayıf Olasılık	Stratejik amaç ve hedefe ulaşılması öngörülen sürede gerçekleşme olasılığı düşük olmakla birlikte imkânsız olmayan olay veya durumlar
1	Çok Zayıf Olasılık	Stratejik amaç ve hedefe ulaşılması öngörülen sürede gerçekleşme olasılığı pek muhtemel olmayan olay veya durumlar

Tablo 7 – Olasılık Seviyeleri

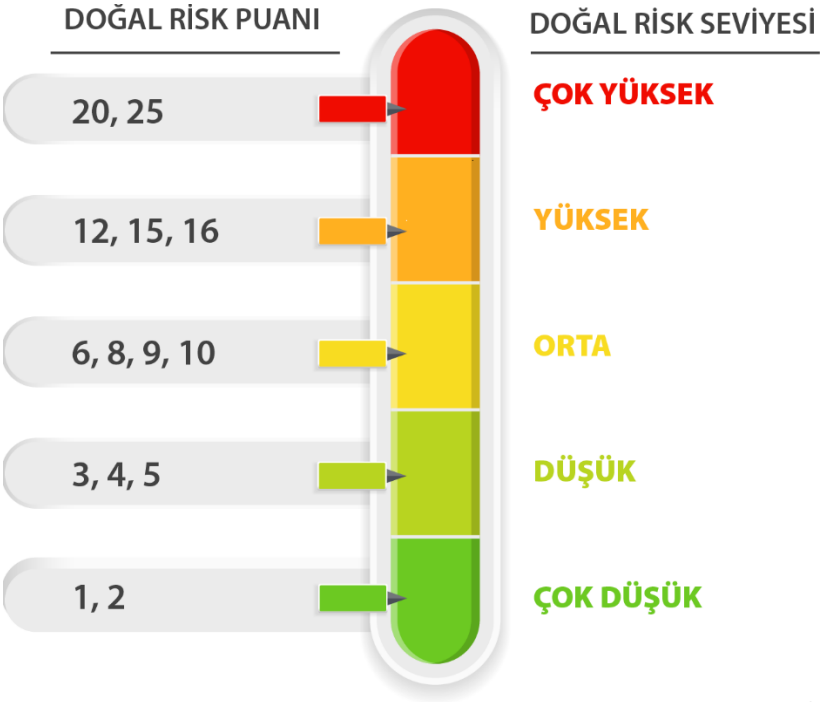
Doğal Risk Seviyesinin Hesaplanması

Doğal risk seviyesi, idare tarafından riske yönelik herhangi bir ilave risk yönetimi faaliyeti uygulanmadan önceki risk seviyesidir.

Doğal risk seviyesi, etki ve olasılık puanlarının çarpımı ile hesaplanır.

Doğal Risk Seviyesi	Etki x Olasılık

Etki ve olasılık puanları en yüksek 5 en düşük 1 olacak şekilde belirlenir. Örneğin; bir riskin olasılığı 2, etkisi 4 ise risk puanı 8 olarak hesaplanır ve doğal risk seviyesi "orta" olarak değerlendirilir. Tablo 8'de risklerin etki ve olasılıkları değerlendirilerek hesaplanan doğal risk seviyelerine ilişkin sınıflandırmaya yer verilmiştir:



Tablo 8 – Doğal Risk Seviyeleri

Kamu Kurumsal Risk Yönetimi Yaklaşımı Örnek Soru Seti (Ek–2) dokümanında risklerin değerlendirilmesi aşamasında kullanılabilecek örnek sorular bulunmaktadır.

2.2.1.2 Mevcut Risk Yönetimi Faaliyetlerinin Değerlendirilmesi

Risklerin doğru bir biçimde önceliklendirilmesi için, risk seviyeleri belirlenirken idare tarafından maruz kalınabilecek risklere yönelik olarak yürütülen mevcut risk yönetimi faaliyetlerinin yeterli olup olmadığı da değerlendirilmelidir. Mevcut risk yönetimi faaliyetleri idarenin stratejik amaç ve hedeflerine ulaşmasını etkileyebilecek risklere yönelik idare bünyesinde halihazırda uygulanan faaliyetlerdir.

Mevcut risk yönetimi faaliyetlerinin yeterli olarak kabul edilmesi ya da geliştirilmesine ilişkin karar verilmesinde aşağıda yer alan sorular göz önünde bulundurulur:

- Mevcut risk yönetimi faaliyetleri, riskin seviyesini kabul edilebilir düzeye indiriyor mu?
- Alınmış olan önlemler, gerçekleşebilecek önemli kayıpları önlüyor mu?
- Risk yönetimi faaliyetlerinin yürütülmesi için idare yeterli kaynağa sahip mi?
- Risk yönetimi faaliyetlerinde kaynaklar etkili ve verimli bir biçimde kullanılıyor mu?

Risk seviyelerinin belirlenmesinde dikkate alınan faktörlerden mevcut risk yönetimi faaliyetlerinin yeterliliğine ilişkin sınıflandırmaya aşağıdaki tabloda yer verilmektedir:

MEVCUT RİSK YÖNETİMİ FAALİYETLERİNİN YETERLİLİĞİ	YETERLİLİK KATSAYISI	AÇIKLAMA
YETERLİ	0,1	Riski yönetmek için idare bünyesinde riskin olasılığını (önleyici risk yönetimi faaliyetleri mevcuttur) ve/veya etkisini (risk gerçekleştiğinde uygulanacak acil eylem planları mevcuttur) azaltmaya yönelik olarak yeterli seviyede risk yönetimi faaliyetleri tasarlanmış ve işletilmektedir. Mevcut risk yönetimi faaliyetlerinin etkin tasarlandığı ve işletildiği konusunda üst yönetimin makul güvencesi (iç denetim ve/veya Sayıştay raporlarıyla da desteklenen) bulunmaktadır.
KISMEN YETERLİ	0,4	Riski yönetmek için yürütülen mevcut risk yönetimi faaliyetleri kısmen yeterlidir. Söz konusu risk yönetimi faaliyetlerinin riskin etkisini ve/veya olasılığını azaltmaya yönelik olarak geliştirilmesi veya ek önlemlerin tasarlanması gerekmektedir. Bu durum iç denetim veya Sayıştay raporları ile de desteklenmektedir.
ZAYIF	0,8	Mevcut risk yönetimi faaliyetleri riskin seviyesini kabul edilebilir seviyeye indirecek şekilde tasarlanmamış veya işletilmemektedir. Riskin etki ve olasılık seviyeleri göz önünde bulundurularak bunları azaltmaya yönelik önlemler alınması gerekmektedir.
YETERLİ DEĞİL	1	Riski yönetmek için tasarlanmış ve işletilen herhangi bir risk yönetimi faaliyeti bulunmamaktadır. Ek olarak, idarenin kontrolünde olmayan dış risklerin mevcut olması veya bir riske yönelik gerçekleştirilebilecek ilave bir risk yönetimi faaliyetinin idarenin inisiyatifi ve yetkisi dâhilinde alınamıyor olması mevcut risk yönetimi faaliyetlerinin yeterli olmadığını göstermektedir.

Tablo 9 – Mevcut Risk Yönetimi Faaliyetlerinin Yeterliliğine İlişkin Sınıflandırma

Aşağıda yer alan riskler için mevcut risk yönetimi faaliyetlerinin yeterliliğine yönelik sınıflandırma örnekleri tabloda yer almaktadır:

Risk 1: İdare içerisinde kritik iş süreçlerinde yer alan personelin yedeklenmemesi, kritik personelin işten ayrılması sonucunda iş süreçlerinde devamlılık sağlanamaması, operasyonların aksaması ve ilgili durumun idare hedeflerinin zamanında gerçekleştirilememesine neden olması

Risk 2: Kurumsal kaynak planlama sisteminin etkin kullanılmaması sonucu işlemlerin anlık ve kontrollü takip edilememesi, finansal kayıpların yaşanması ve üst yönetime yapılan raporlamalarda hataların bulunması

MEVCUT RİSK YÖNETİMİ FAALİYETLERİNİN YETERLİLİĞİ	YETERLİLİK KATSAYISI	ÖRNEKLER
YETERLİ	0,1	İdarenin yeterli sayıda nitelikli personeli bulunmaktadır. Faaliyetlerin sürekliliği için büyük öneme sahip anahtar personelin yokluğunda yedek personel belirlenmektedir. Tüm işlemler sistem üzerinden gerçekleştirilmekte olup idare genelinde önleyici kontroller uygulanmaktadır. Bu hususlar iç denetim veya Sayıştay raporları ile de doğrulanmaktadır.
KISMEN YETERLİ	0,4	Yedek personel uygulaması kısmen mevcuttur. İdare bünyesinde otomasyonun hâkim olduğu süreç adımları olmakla birlikte sistem bazı alanlarda manuel uygulama ve müdahalelere izin vermektedir. Bu hususlar iç denetim veya Sayıştay raporları ile de doğrulanmaktadır.
ZAYIF	0,8	Faaliyetlerin sürekliliği için büyük öneme sahip anahtar personelin pek çoğu yedeklenmemektedir. İdare bünyesinde personel sayısı düşük seviyededir. Ofis uygulamaları gibi işlemler dışında otomasyon bulunmamakta olup işlemler çoğunlukla manuel yürütülmektedir.
YETERLİ DEĞİL	1	İdarenin yedek personel uygulaması bulunmamaktadır. İdare bünyesinde yetkin personel sayısı çok düşük seviyededir. İdarenin hiçbir sürecinde otomasyon bulunmamaktadır.

Tablo 10 – Mevcut Risk Yönetimi Faaliyeti Örnekleri

Örneğin; bir riskin olasılığı 2, etkisi 4 ise doğal risk puanı 8 olarak hesaplanır. İlgili riske yönelik kurum tarafından yeterli seviyede risk yönetimi faaliyetleri tasarlanmış ve işletiliyorsa, buna bağlı olarak mevcut risk yönetimi faaliyetleri "yeterli" olarak değerlendirildiyse, artık risk değeri 8*0,1=0,8 olarak hesaplanır ve artık risk seviyesi "çok düşük" olarak değerlendirilir.

İdarenin mevcut risk yönetimi faaliyetlerinin riskin etki ve olasılığını ne kadar azalttığı göz önünde bulundurulmalı ve ilave risk yönetimi faaliyetlerinin gerekliliği buna göre değerlendirilmelidir.

Mevcut risk yönetimi faaliyetlerinin yeterliliğinin doğru şekilde değerlendirilmesi oldukça önemlidir. Yeterli olmadığı halde hatalı değerlendirme sonucu yeterli olarak belirlenen mevcut risk yönetimi faaliyetleri üzerinden gerçekleştirilen

hesaplamalar neticesinde, çok yüksek ya da yüksek artık risk seviyesine sahip olması gereken bir riskin artık risk seviyesi düşük olarak belirlenebilir. İlgili riske yönelik gerekli ilave risk yönetimi faaliyetlerinin tanımlanmaması, kurumun stratejik amaç ve hedeflere ulaşmasını etkileyebilir. Yeterli olduğu halde hatalı değerlendirme sonucu "yeterli değil" olarak belirlenen mevcut risk yönetimi faaliyetleri üzerinden gerçekleştirilen hesaplamalar neticesinde, düşük ya da orta artık risk seviyesine sahip olması gereken bir riskin artık risk seviyesi çok yüksek ya da yüksek olarak belirlenebilir. İlgili riske yönelik ilave risk yönetimi faaliyetlerinin tanımlanması sonucu kurum kaynaklarının kullanımında verimsizlik yaşanabilir.

Artık Risk Seviyesinin Hesaplanması

Artık risk seviyesi, riskin etkisini ve/veya olasılığını azaltmak için idare tarafından yürütülen mevcut risk yönetimi faaliyetlerinden sonra arta kalan risk seviyesini ifade eder.

Artık risk seviyesi hesaplanırken doğal risk seviyesi ile mevcut risk yönetimi faaliyetlerinin yeterliliği birlikte değerlendirilir. Artık risk seviyesi, doğal risk puanı ile mevcut risk yönetimi faaliyetlerinin yeterlilik katsayısının çarpımı ile hesaplanır.

Doğal Risk Seviyesi	Etki x Olasılık

Artık Risk Seviyesi	Doğal Risk Puanı x Mevcut Risk Yönetimi Faaliyetleri Yeterlilik Katsayısı

Doğal risk ve artık risk seviyesinin ayrı ayrı hesaplanması idarenin mevcut risk yönetimi faaliyetlerinin yeterliliği konusunda bilgi sağlar.

Tablo 11'de doğal risk seviyesi ve mevcut risk yönetimi faaliyetlerinin yeterliliği değerlendirilerek hesaplanan artık risk seviyeleri sınıflandırmasına yer verilmiştir:

ARTIK RİSK SEVİYESİ	ARTIK RİSK PUANI	AÇIKLAMA
ÇOK YÜKSEK	20 <= Risk Puanı <= 25	İdarenin çok yüksek derecede riske maruz kaldığını ifade eder. İlave risk yönetimi faaliyetleri gerçekleştirilmez ise idarenin stratejik amaç ve hedeflerine ulaşamaması söz konusudur. Acilen üst yönetimin dikkatine sunulması ve takibi gerekir.
YÜKSEK	12 <= Risk Puanı < 20	İdarenin yüksek derecede riske maruz kaldığını ifade eder. İlave risk yönetimi faaliyetleri gerçekleştirilmez ise idarenin stratejik amaç ve hedeflerine ulaşmasını önemli ölçüde engelleyebilir/geciktirebilir. Acilen üst yönetimin dikkatine sunulması ve takibi gerekir.
ORTA	6 <= Risk Puanı < 12	İdarenin orta derecede riske maruz kaldığını ifade eder. İdarenin stratejik amaç ve hedeflere ulaşmasını engelleyebilir/ geciktirebilir. Yönetimin takip etmesi gerekir.
DÜŞÜK	3 <= Risk Puanı < 6	İdarenin stratejik amaç ve hedeflerini gerçekleştirmesini önemli ölçüde engellemez/geciktirmez. Zaman içindeki gelişimlerinin takip edilmesi yeterlidir.
ÇOK DÜŞÜK	Risk Puanı < 3	İdarenin stratejik amaç ve hedeflerini gerçekleştirmesini engellemez/geciktirmez. Zaman içindeki gelişimlerinin takip edilmesi yeterlidir.

Tablo 11 – Artık Risk Seviyesi Sınıflandırması

Çalıştayda yapılan risk değerlendirme çalışmalarında katılımcılar tarafından, idarenin stratejik amaç ve hedeflerine yönelik risklerin etki ve olasılık puanları önce bireysel olarak değerlendirilir. İlgili etki ve olasılık puanları üzerinden risklerin doğal risk puanları hesaplanır ve katılımcılar ile çıktı halinde paylaşılan Bireysel Risk Değerlendirme Formuna (Ek–7) yazılır. Katılımcılar tarafından yapılan bu değerlendirmeler konsolide edilerek bilgisayar ortamında Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formunda (Ek–12) yer alan Katılımcı Değerlendirmeleri alanlarına kaydedilir. Bu esnada, bir riske yönelik farklı katılımcılar tarafından belirlenen etki ve olasılık değerlerinin ağırlıklı ortalaması dikkate alınır. Sonrasında ilgili risklere ilişkin idarenin mevcut risk yönetimi faaliyetlerinin yeterlilik puanlamaları grup olarak değerlendirilerek risklerin artık risk seviyeleri belirlenir. Değerlendirilen mevcut risk yönetimi faaliyetlerinin yeterlilik seviyeleri ile artık risk seviyeleri çalıştay kolaylaştırıcısı tarafından Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formuna kaydedilir.

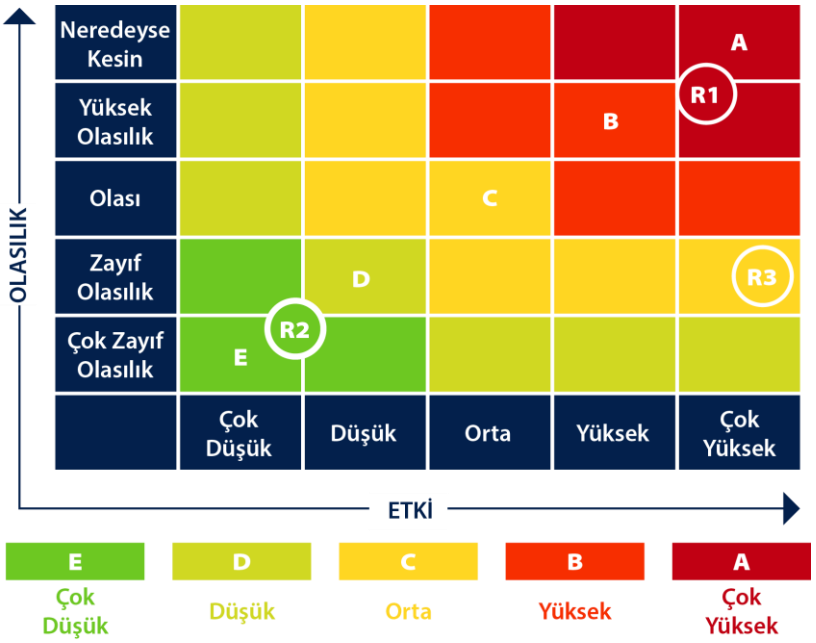
Hesaplanan doğal risk seviyelerinin izleyen yılda tekrar hesaplanmasına ilişkin değerlendirme İç Kontrol İzleme ve Yönlendirme Kurulu (İKİYK) tarafından yapılır ve idarenin ihtiyaç duyması halinde doğal risk seviyesi izleyen yılda yeniden

hesaplanır. Artık risk seviyesi ise altı aylık periyotlarda yılda en az 2 defa gözden geçirilmelidir.

Risk Haritası

İdarenin stratejik amaç ve hedeflerine ulaşmasını etkileyebilecek risklerin değerlendirilmesi kapsamında, risk seviyelerini gösteren risk haritaları oluşturulur. Risk haritaları; idarenin stratejik amaç ve hedeflerine yönelik risklerin seviyelerini daha rahat takip edebilmesini sağlar ve idarenin ortak risk algısını yansıtır.

Risklerin etki ve olasılık seviyeleri ile idarenin mevcut risk yönetimi faaliyetlerinin yeterliliği dikkate alınarak hesaplanan artık risk seviyelerinin gösteriminde kullanılan risk haritası örneği aşağıda yer almaktadır.



Tablo 12 – Örnek Risk Haritası

İlgili haritada bölgeler renklerle ifade edilmektedir. A bölgesi çok yüksek seviyeye sahip riskleri ifade ederken, E bölgesi çok düşük seviyeli riskleri ifade etmektedir. Risklerin harita üzerinde gösterimiyle idarenin risklerinin hangi alanlarda yoğunlaştığı kolayca ifade edilebilir. Ek olarak, risk haritaları idarenin risk iştahı hakkında da fikir vermektedir. Artık risk seviyeleri çok yüksek ve yüksek olan alanlarda yoğunlaşan idareler daha fazla risk alma eğiliminde iken düşük ve çok düşük alanda yoğunlaşan idareler riskten kaçınma eğilimindedir.

Risk haritaları hem doğal risklerin hem de artık risk seviyelerinin gösteriminde kullanılabilir. Doğal risk seviyesi hesaplanan bir riskin mevcut risk yönetimi faaliyetlerinin yeterliliği değerlendirilerek artık risk seviyesine ulaşılır. Burada

dikkat edilmesi gereken husus; mevcut risk yönetimi faaliyetlerinin riskin etkisi, olasılığı veya her ikisi üzerinde ne ölçüde bir azalmaya neden olduğudur. Eğer mevcut risk yönetim faaliyetleri ilgili riskin sadece olasılığını düşürmeye yönelik tasarlanmış ise risk haritasında aşağı doğru, etkisini düşürmeye yönelik ise sola doğru, ikisini birden düşürmeye yönelik ise hem sola hem aşağı doğru olacak şekilde bir gösterim yapılır.

2.2.2 Risklerin Önceliklendirilmesi

Öncelikli risklerin tespiti, stratejik amaç ve hedeflere ulaşılmasına yönelik güvencenin artırılması ve kamu kaynaklarının etkili, ekonomik ve verimli kullanılması açısından önem taşımaktadır. Risklerin etki ve olasılık seviyeleri ile idarenin mevcut risk yönetimi faaliyetleri göz önünde bulundurularak ulaşılan artık risk seviyeleri üzerinden riskler önceliklendirmeye tabi tutulur. Risklerin önceliklendirilmesinde göz önünde bulundurulması gereken hususlara aşağıda yer verilmektedir:

- Hedef bazında belirlenen risk iştahı sınırına yaklaşan riskler öncelikli olarak ele alınmalıdır. İdare, hedeflerinden birisi için risk iştahını orta düzeyde belirlemişse, ilgili hedef altında tanımladığı çok yüksek, yüksek ve orta seviyeli riskleri, düşük sınıfında yer alan diğer risklere göre öncelikli olarak değerlendirmelidir. Örneğin, kurumsal kapasiteyi arttırmaya yönelik hedefleri için risk iştahını orta seviyede belirleyen bir idarenin, bu hedeflere ilişkin belirlediği risklerden orta ve üstü seviyedeki risklerini öncelikli olarak değerlendirmesi, düşük ve çok düşük seviyeli risklere ise önceliklendirmede daha alt sıralarda yer vermesi gerekir.
- Tek başına yüksek veya çok yüksek kategorisine girmeyen bir risk diğer risklerle birleştiğinde idarenin stratejik amaç ve hedeflerini etkileyebilecek bir risk haline dönüşebilir. Dolayısıyla, risklerin değerlendirilmesi aşamasında birbirleriyle olan etkileşimlerin göz önünde bulundurulması gerekir.
- İdarenin söz konusu riske karşı dayanıklılık düzeyi ile riske konu olayın/durumun gerçekleşmesi halinde ortaya çıkan zararların telafisi için ihtiyaç duyulacak süre risk seviyesini etkileyecektir. Örneğin; idarenin bilgi teknolojisi altyapısının siber saldırılara karşı dayanıklılık düzeyi ile olası bir siber saldırı sonrasında bilgi teknolojileri altyapısının tekrar ayağa kaldırılması için ihtiyaç duyulan sürenin uzunluğu, idarenin siber saldırı sonucunda kamu hizmeti sunamaması riskinin büyüklüğü veya önceliği üzerinde önemli bir etkiye sahip olacaktır.
- İdare tarafından belirlenen risklerin önceliklendirilmesi, idarenin farklı kademelerine göre değişkenlik gösterebilir. Faaliyet düzeyinde önemli görülen bir risk, stratejik seviyede risklerle karşılaştırıldığında daha az önceliğe sahip olabilir.

- Riskin öznel bir kavram olduğu yadsınamaz ise de risklerin önceliklendirilmesinde, yönetici ve çalışanların kişisel risk algıları yerine idarenin ortak risk algısı belirleyici olmalıdır.
- SGB koordinasyonunda idarenin birden fazla birimini ilgilendiren risklerin yönetimi sağlanmalıdır.

İdare tarafından maruz kalınabilecek riskler, değişen iç ve dış koşullara bağlı olarak zaman içinde değişim gösterir. Bu nedenle, tanımlanan, ölçülen ve önceliklendirilen riskleri etkileyebilecek değişimler mutlaka göz önünde bulundurulmalıdır.

2.2.3 Öncü Risk Göstergelerinin Belirlenmesi

Artık risk seviyesi tanımlandıktan ve riskler önceliklendirildikten sonra öncü risk göstergeleri belirlenmelidir. Artık risk seviyesi yüksek ve çok yüksek olarak tanımlanan riskler için öncü risk göstergeleri belirlenir. Öncü risk göstergeleri, idarenin stratejik amaç ve hedeflerini etkileyebilecek kritik önemdeki risklerin takibinde kolaylık sağlar.

Öncü risk göstergeleriyle idare, risklerini somut veriler üzerinden daha etkin şekilde izler. Öncü risk göstergeleri, idarenin riskler gerçekleşmeden önce gerekli ilave risk yönetimi faaliyetleri gerçekleştirerek riske dayanıklılığını arttırmasına yardımcı olur.

- Öncü risk göstergeleri artık risk seviyesi "yüksek ve çok yüksek" riskler için belirlenir.
- Artık risk seviyesi orta, düşük ve çok düşük seviyeli riskler için kurum tarafından öncü risk göstergesi belirlenebilir.
- Doğal risk seviyesi yüksek ve çok yüksek riskler için de öncü risk göstergelerinin belirlenmesi kurum inisiyatifindedir.

Öncü risk göstergelerine yönelik dikkat edilmesi gereken hususlar aşağıdaki gibidir:

- Öncü risk göstergeleri, stratejik amaç ve hedefler ile bunları gerçekleştirmeye yönelik yürütülen faaliyetlerle uyumlu olmalıdır.
- Öncü risk göstergesi açık, anlaşılır ve ölçülebilir şekilde tanımlanmalıdır.
- Öncü risk göstergelerinin performans göstergeleriyle uyumuna dikkat edilmelidir. Bir hedef altında tanımlanan performans göstergesi aynı zamanda aynı hedef altında tanımlanan riskin takibi için de ÖRG olarak kullanılabilir.
- Öncü risk göstergesi üst yönetim tarafından periyodik olarak takip edilmelidir. Her bir öncü risk göstergesi için raporlama periyodu tanımlanmalı, raporlama periyodu riskin önceliğine ve öncü risk göstergesinin niteliğine göre belirlenmelidir. İdare için öncelikli bir riske atanmış gösterge aylık

raporlamalarla takip edilirken, daha az öncelikli bir risk göstergesi üç aylık raporlamalar ile takip edilebilir. Örneğin, bilişim sistemi kesintileriyle ilişkili bir öncü risk göstergesi aylık periyotta takip edilebilirken, çalışan memnuniyeti seviyesine ilişkin bir öncü risk göstergesi yıllık periyotta takip edilebilir.

- Her bir öncü risk göstergesine yönelik hedef tanımı (nümerik olarak ifade edilebilen bir değer, aralık, tavan veya taban değeri) yapılmalıdır.
- ÖRG hedefinden sapma durumunda ilave bir risk yönetimi faaliyetinin gerçekleştirip gerçekleştirilmeyeceği değerlendirilmelidir.
- Öncü risk göstergesi sonuçlarına göre riske yönelik alınan kararlar ve gerçekleştirilecek ilave risk yönetimi faaliyetleri gözden geçirilmeli ve gerekirse yeni risk yönetimi faaliyetleri tasarlanmalıdır.
- Öncü risk göstergelerinin sonuçları ilişkili performans göstergeleriyle karşılaştırılabilir. Böylece idarenin hangi riskleri yöneterek hangi alt program hedeflerine ulaştığı takip edilebilir.

Aşağıda öncü risk göstergesi bir örnek üzerinden açıklanmaktadır:

Hedef	İdarenin kalite standartlarına uyumunu arttırmak
Riskler	İç tetkikçiler tarafından periyodik değerlendirmelerin gerçekleştirilmemesi nedeniyle kalite standartlarına uyumsuzlukların zamanında tespit edilememesi ve ISO belgelerinin geçerliliklerini yitirmesi
Performans Hedefi	Kalite gerekliliklerini yerine getirerek var olan ISO sertifikalarının devamlılığını sağlamak
ÖRG	Denetimlerde açılan uygunsuzluk sayısı
ÖRG Hedefi	En fazla 3 alanda uygunsuzluk bulunması
ÖRG Raporlama Periyodu	3 aylık
ÖRG Sapması Durumunda Gerçekleştirilecek Faaliyet	Açılan uygunsuzlukların en fazla 3 ay içerisinde çözümlenmesi için gerekli tedbirlerin alınması

Tablo 13 – Öncü Risk Göstergesi Örneği

Öncü Risk Göstergesi Örnekleri (Ek–10) dokümanında ilave öncü risk göstergesi örneklerine yer verilmektedir.

Örnek

Risklerin Değerlendirilmesi

Risklerin etki ve olasılık seviyelerinin, mevcut risk yönetimi faaliyetleri göz önünde bulundurularak değerlendirilmesi aşağıda bir örnek ile açıklanmaktadır:

Risklerin Etki ve Olasılık Seviyelerinin Belirlenmesi

Belirlenen riskler çalıştay katılımcıları tarafından değerlendirilerek ve bu değerlendirmelerin ağırlıklı ortalaması hesaplanarak etki ve olasılık seviyelerine yönelik nihai sonuçlara aşağıda yer verilmektedir:

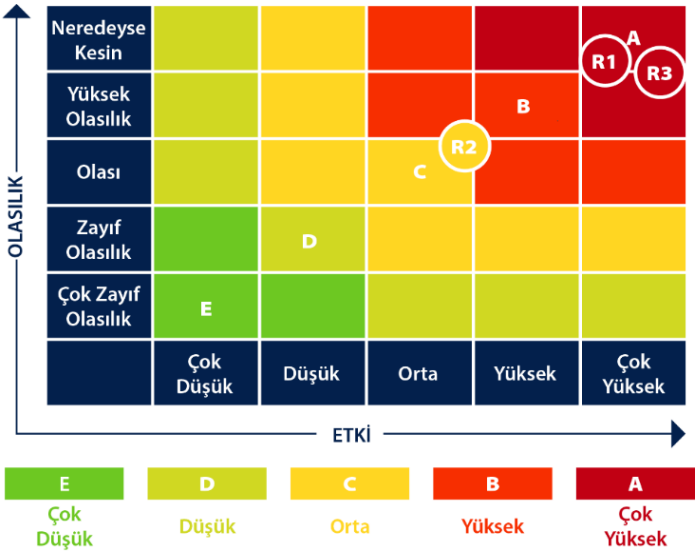
RİSKLER	ETKİ SEVİYESİ	ETKİ PUANI	OLASILIK SEVİYESİ	OLASILIK PUANI
Risk 1	Çok Yüksek	5	Yüksek Olasılık	4
Risk 2	Orta	3	Olası	3
Risk 3	Yüksek	5	Yüksek Olasılık	4

Doğal Risk Seviyesinin Hesaplanması

Belirlenen risklere yönelik doğal risk seviyesi hesaplamaları aşağıda açıklanmaktadır:

RİSKLER	ETKİ SEVİYESİ	ETKİ PUANI	OLASILIK SEVİYESİ	OLASILIK PUANI	DOĞAL RİSK PUANI	DOĞAL RİSK SEVİYESİ
Risk 1	Çok Yüksek	5	Yüksek Olasılık	4	4x5=20	Çok Yüksek
Risk 2	Orta	3	Olası	3	3x3=9	Orta
Risk 3	Yüksek	5	Yüksek Olasılık	4	5x4=20	Yüksek

Hesaplanan doğal risk seviyelerinin risk haritası üzerindeki konumları aşağıda gösterilmektedir:



Mevcut Risk Yönetimi Faaliyetlerinin Değerlendirilmesi

Belirlenen risklere yönelik idare tarafından yürütülen mevcut risk yönetimi faaliyetlerinin yeterlilik durumları aşağıda açıklandığı gibidir.

RİSKLER	RİSK YÖNETİMİ FAALİYETLERİNİN YETERLİLİĞİ	ETKİNLİK VE YETERLİLİK KATSAYISI	AÇIKLAMA
Risk 1	YETERLİ DEĞİL	1	Bu riski yönetmek için tasarlanmış ve uygulamaya konmuş herhangi bir faaliyet bulunmamaktadır. (Örneğin; doğru yönetim bilgi sistemi seçimine yönelik ihtiyaç analizi ve fayda ve maliyet değerlendirmeleri yapılmamakta, kaynakları doğru ürüne yöneltmek adına çalışma yapılmadan yönetim bilgi sistemi seçimi gerçekleştirilmektedir.)
Risk 2	YETERLİ	0.1	İdare tarafından uygulanan mevcut risk yönetimi faaliyetleri, riski yönetmek için iyi tasarlanmış ve çalışmaktadır. Çoğunlukla önleyici faaliyetlerin tasarlandığı söylenebilir. (Örneğin; eğitim içerikleri, konusunda uzman kişiler tarafından hazırlanmakta ve sistemde yer alan güncel değişikliklerin takibi kapsamında periyodik olarak eğitim içerikleri yenilenerek son kullanıcılar düzenli eğitilmektedir.)
Risk 3	KISMEN YETERLİ	0.4	Mevcut risk yönetimi faaliyetlerinin genel anlamda etkin ve çalışır durumda olmasına rağmen ilgili faaliyetlerin geliştirilmesi veya ek önlemlerin tasarlanması gerekmektedir. (Örneğin; idarenin acil durum eylem planı /felaketten kurtarma planı bulunmakla birlikte, sistemin çalışır durumda olduğuna dair ilgili planlara yönelik periyodik kontroller ve senaryo analizleri gerçekleştirilmemektedir.)

Artık Risk Seviyesinin Hesaplanması

Mevcut risk yönetimi faaliyetlerinin yeterliliği değerlendirilerek hesaplanan artık risk seviyelerine aşağıda yer verilmektedir:

RİSKLER	DOĞAL RİSK PUANI	DOĞAL RİSK SEVİYESİ	YETERLİLİK KATSAYISI	MEVCUT RİSK YÖNETİMİ FAALİYETLERİNİN YETERLİLİĞİ	ARTIK RİSK PUANI	ARTIK RİSK SEVİYESİ	DERECELENDİRME
Risk 1	20	ÇOK YÜKSEK	1	YETERLİ DEĞİL	20x1=20	ÇOK YÜKSEK	20<= Risk Puanı <= 25
Risk 2	9	ORTA	0.1	YETERLİ	9x0,1=0,9	ÇOK DÜŞÜK	Risk Puanı < 3
Risk 3	20	ÇOK YÜKSEK	0.4	KISMEN YETERLİ	20*0,4=8	ORTA	6<= Risk Puanı < 12

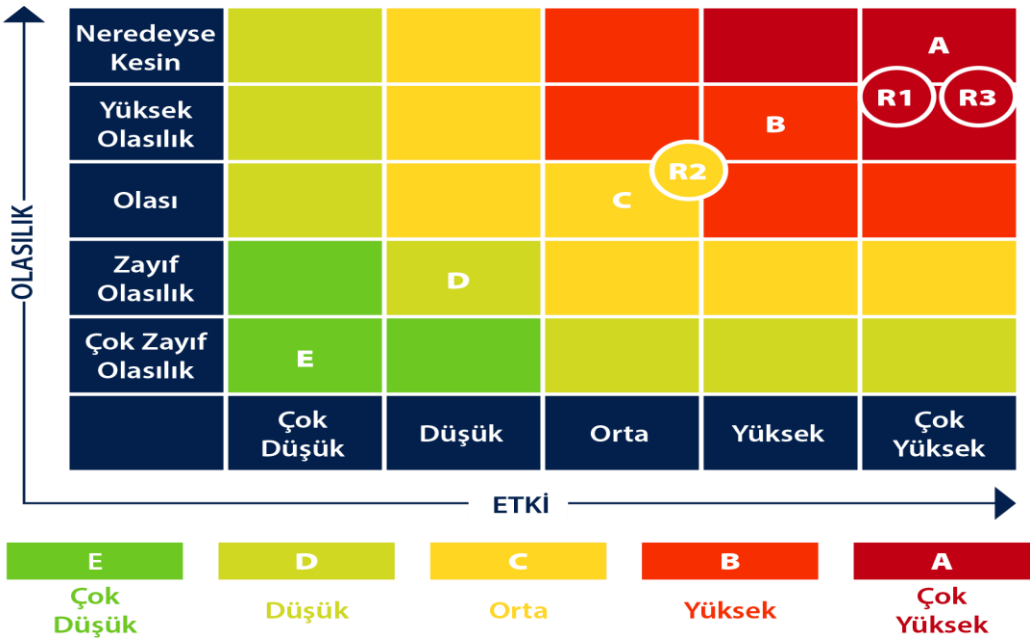
Risk seviyelerinin belirlenmesinde, idare tarafından yürütülen mevcut risk yönetimi faaliyetlerinin yeterlilik durumunun önemine ilişkin ulaşılan sonuçlara aşağıda yer verilmektedir:

- Risk 1 örneğinde, doğal risk seviyesi "çok yüksek" olarak değerlendirilen riske yönelik herhangi bir risk yönetimi faaliyetinin uygulanmamasına bağlı olarak artık risk seviyesinin değişmediği, "çok yüksek" seviyede kaldığı görülmektedir. İlgili risk, doğal risk seviyesi ile karşılaştırıldığında risk haritası üzerinde aynı yerde gözlenir.
- Risk 2 örneğinde, doğal risk seviyesi "orta" olarak değerlendirilen risk için hem etkiyi hem de olasılığı düşürmeye yönelik risk yönetimi faaliyetlerinin uygulanması sonucunda artık risk seviyesinin "çok düşük" seviyeye indiği görülmektedir. İdare aldığı önlemlerle riskin hem olasılığını hem de etkisini düşürmektedir. İlgili riskin hem etkisi hem de olasılığı azaldığı için risk düzeyi harita üzerinde hem sola hem aşağı yönde hareket ederek C bölgesinden E bölgesine hareket eder.
- Risk 3 örneğinde, doğal risk seviyesi "çok yüksek" olarak değerlendirilen riskin mevcut risk yönetimi faaliyetlerinin kısmen yeterli olmasına bağlı olarak risk seviyesinin "orta" seviyeye indiği görülmektedir. İlgili risk dış risk kategorisinde değerlendirildiğinden etki seviyesi azaltılamamakta fakat mevcut risk yönetimi faaliyetleri ile olasılığı azaltılmaktadır. İlgili risk aşağıda yer alan risk haritasında

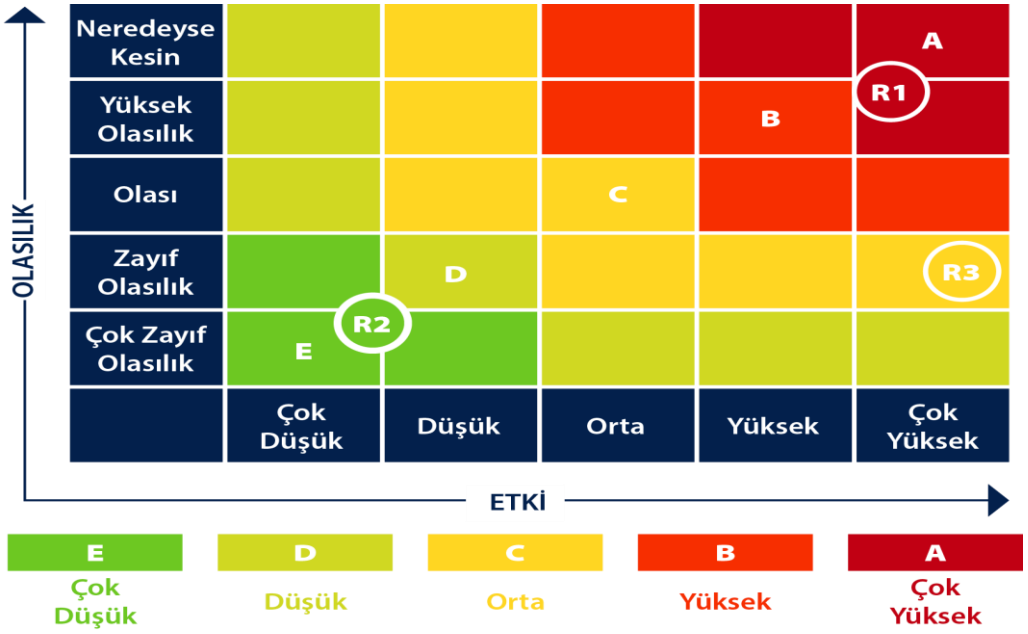
gösterildiği gibi sola doğru hareket etmiş ve A bölgesinden C bölgesine geçmiştir.

Hesaplanan artık risk seviyeleri ile daha önceden hesaplanan doğal risk seviyelerinin risk haritaları üzerindeki konumları aşağıda gösterilmektedir:

Doğal Risk Seviyesi



Artık Risk Seviyesi



Risk 2 ve Risk 3'te risk seviyesinde gözlenen değişim riskin önceliklendirmesinde idare tarafından yürütülen mevcut risk yönetimi faaliyetlerinin yeterlilik durumunun önemini göstermektedir.

Risklerin Önceliklendirilmesi

Belirlenen artık risk seviyeleri üzerinden önceliklendirme yapıldığında riskler aşağıda yer aldığı şekilde sıralanabilir:

	Belirlenen Riskler	Örnek Artık Risk Seviyesi
Risk 1	Yeterli ihtiyaç analizi yapılmadan idarenin yapısı, iş yapış biçimi ve hedefleriyle uyumlu olmayan yönetim bilgi sisteminin seçilmesi sonucu idare kaynaklarının etkin kullanılamaması	Çok Yüksek
Risk 2	Yangın, sel gibi olağanüstü durumlar sonucunda geri dönüşü olmayacak veri kayıplarının yaşanması	Orta
Risk 3	İdarenin bilgi teknoloji sistemlerinde gerçekleştirilen güncellemeler sonrasında kullanıcı personele yetersiz içerikle eğitim verilmesi sonucunda çalışanların güncel sistemi etkin kullanamaması ve operasyonel aksaklıkların yaşanması	Çok Düşük

Öncü Risk Göstergelerinin Belirlenmesi

Artık risk seviyesi "çok yüksek" ve "yüksek" riskler için öncü risk göstergesi tanımlanır. Artık risk seviyeleri sırasıyla "düşük", "çok düşük" ve "orta" olduğunda idare kendi inisiyatifi ile öncü risk göstergeleri tanımlayabilir.

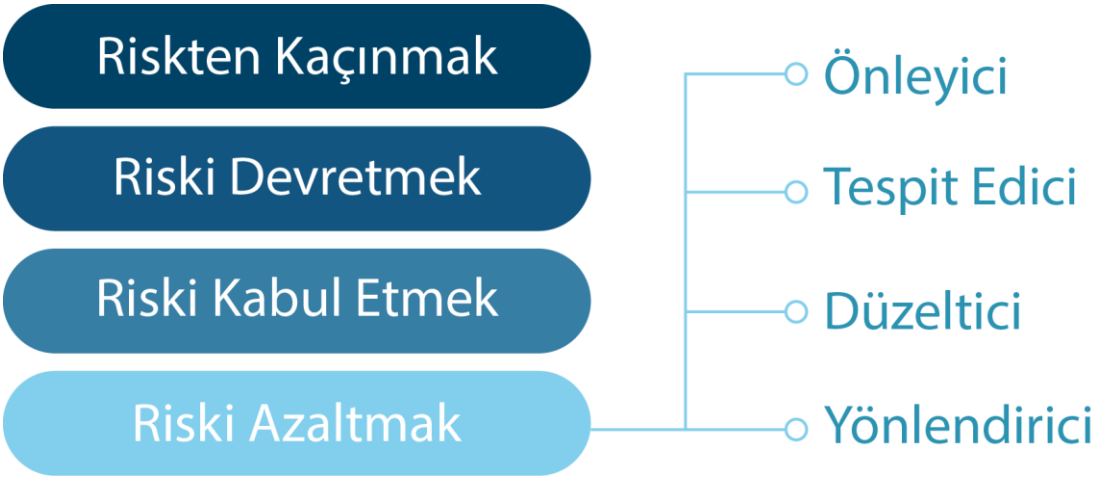
Aşağıdaki örnekte, idarenin belirlediği üç riskin tamamı için öncü risk göstergesi tanımladığı varsayılmaktadır. İdare tarafından tanımlanan örnek öncü risk göstergelerine aşağıda yer verilmektedir:

Hedef	Sağlıklı beslenme alışkanlıklarını kazandırmak ve geliştirmek		
Artık Risk Seviyesi	Çok Yüksek	Çok Düşük	Orta
Risk No	1	2	3
Riskler	Aşırı tüketimi tavsiye edilmeyen besinlere yönelik özendirici yayınların fazla oluşu sebebiyle sağlıksız beslenme ve bağlı hastalıklarda (obezite, diyabet vb.) artış yaşanması	Sağlık Bakanlığının sağlıklı beslenme alışkınlıklarını yaygınlaştırma stratejilerinin çok sektörlü yaklaşımı gerektirmesi nedeniyle gerekli koordinasyonun sağlanamaması	İlgili sektörlerin Sağlık Bakanlığının sağlıklı beslenme alışkanlıklarını yaygınlaştırma stratejilerine yeterli düzeyde uyum sağlayamamaları nedeniyle farkındalığın oluşturulamaması
Alt Program Hedefi	*Obezite Prevalansı (İlkokul 2. Sınıf Öğrencileri)nı her yıl 0,05 oranında azaltmak * Obezite Prevalansı (15 Yaş ve Üzeri Bireylerde) (Ölçüme Dayalı) (%)nı 2027 yılına kadar 29,05 düzeyine getirmek	*Her yıl 25 Restoran/Yemek Üreticisinin Sağlık Bakanlığı tarafından belirlenen kriterler çerçevesinde belgelendirilmesini yapmak	* Kişi Başı Ortalama Günlük Tuz Tüketimi (Gr/Gün) (15 Yaş ve Üzeri Bireylerde) düzeyini 7,5'a düşürmek
ÖRG	Obezite Prevalansı (15 Yaş ve Üzeri Bireylerde) (Ölçüme Dayalı) (%) Obez Öncesi Nüfus Prevalansı (15 Yaş ve Üzeri Bireylerde) (Ölçüme Dayalı)(%)	* Sağlık Bakanlığınca Belirlenmiş Kriterler Çerçevesinde Belgelendirilen Restoran/Yemek Üreticisi Sayısı (Kümülatif)	Diyabet Prevalansı (15 Yaş ve Üzeri Bireylerde) Diyabet Prevalansı (15 Yaş ve Üzeri Bireylerde) (Ölçüme Dayalı) (%) Kişi Başı Ortalama Günlük Tuz Tüketimi (Gr/Gün) (15 Yaş ve Üzeri Bireylerde)
ÖRG Hedefi	* Obezite Prevalansı (15 Yaş ve Üzeri Bireylerde) (Ölçüme Dayalı) (%)nı 2027 yılına kadar 29,05 düzeyine getirmek * Obez Öncesi Nüfus Prevalansı (15 Yaş ve Üzeri Bireylerde)nı 2027 yılına kadar 33,55 düzeyine getirmek	*Her yıl 25 Restoran/Yemek Üreticisinin Sağlık Bakanlığı tarafından belirlenen kriterler çerçevesinde belgelendirilmesini yapmak	* Diyabet Prevalansı (15 Yaş ve Üzeri Bireylerde) (Ölçüme Dayalı) (%) seyrini korumak ve 2028 yılında 12,05 düzeyine getirmek
ÖRG Raporlama Periyodu	1 Yıl	1 Yıl	1 Yıl
ÖRG Faaliyeti	•Trans yağ, yüksek şeker ve tuz içeren ürünlerin tüketimlerinin azaltılması ve bu nitelikteki besinlerin reklamlarına yönelik düzenleme yapılmasına yönelik çalışmalar yürütülecektir.	• Toplumun besin içerikleri hakkında daha iyi bilgilendirilmesini sağlamak üzere gıda ambalajlarında düzenleme yapılmasına yönelik ilgili paydaşlarla ortak çalışmalar yürütülecektir.	• Gıda üreticileri ve tedarikçileriyle daha sağlıklı besin üretilmesi hususunda iş birliği platformu geliştirilecek ve yeniden düzenleme çalışmaları yürütülecektir. •İşyerleri ve kamu kurumlarının belirli kriterler çerçevesinde değerlendirilmesi yoluyla Sağlıklı Beslenme ve Aktif Hayatı Destekleyen İşyeri /Kamu Kurumları sistemi geliştirilecektir.

2.3. Riske Yönelik Alınacak Kararların Belirlenmesi

Kurumsal risk yönetimi yaklaşımında, risk evreninin ve stratejik amaç ve hedeflere ulaşmasını etkileyebilecek risklerin belirlenmesi ve bu risklerin değerlendirilip önceliklendirilmesinden sonraki adım riske yönelik alınacak kararların belirlenmesidir. İdare bu aşamada, risk iştahı başta olmak üzere fayda/maliyet gibi diğer faktörleri de göz önünde bulundurarak risklere yönelik kararlar alır.

Risklere yönelik alınabilecek kararlar 4 ana grupta sınıflandırılır:



Şekil 6. Riske Yönelik Alınacak Kararlar

Riskten Kaçınmak: Riskin gerçekleşmesi halinde idarenin karşılaşacağı tehditler ve fırsatların değerlendirilmesi ve değerlendirme sonucunda riske neden olabilecek olay veya durumlardan kaçınılmasıdır. İdarenin, riskin gerçekleşmesi halinde maruz kalabileceği zararları, kabul edilebilir bir seviyeye indirecek ilave risk yönetimi faaliyeti oluşturamadığı durumlarda tercih edilir.

Örneğin; idare çalışanlarının, bordro bilgilerine sistem üzerinden erişebilmelerini sağlayacak yeni bir teknolojik uygulamaya geçilmesi planlanabilir. Ancak yapılan değerlendirmeler sonucunda, söz konusu uygulamanın, bilgi güvenliği riski doğuracağı ve bu riski azaltmaya yönelik gerekli ilave risk yönetimi faaliyetlerini, kaynak yetersizliği sebebiyle gerçekleştiremeyeceği sonucuna varılmış ise idare söz konusu uygulamadan vazgeçerek riskten kaçınma yolunu tercih edebilir.

Riski Devretmek: Riskli olduğu değerlendirilen faaliyetlerin tamamen ya da kısmen, idare dışında diğer uzman kamu idarelerine veya tedarik suretiyle yapılan alımlarda üçüncü kişilere/firmalara devredilmesidir. İdarenin, ulaşım, yemek vb. faaliyetlerini, konusunda uzman olan kuruluşlara devretmeleri veya bilgi teknolojileri sistemlerinin bakım, onarım ve yenileme çalışmalarının yine bu alanlarda uzman

olan firmalar aracılığıyla yürütülmesi riskin devredilmesine örnek olarak gösterilebilir.

Riski Kabul Etmek: Riskin gerçekleşmesi halinde idarenin karşılaşabileceği tehditler ve fırsatlar ile riskin yönetilmesi için katlanılacak maliyetlerin değerlendirilmesi sonucunda herhangi bir ilave risk yönetimi faaliyetinin uygulanmamasına karar verilmesidir.

Riskin gerçekleşmesi durumunda karşılaşılabileceği değerlendirilen tehdit, idarenin risk iştah seviyesine göre kabul edilebilir bir seviyede ise idare açısından ilave maliyetler anlamına gelen risk yönetimi faaliyetlerinin tanımlanması ve uygulanması yerine, riskin kabul edilmesi tercih edilebilir. Örneğin; idarenin kritik çalışanlara yönelik yedek personel uygulamasının bulunmaması durumunda, ilgili çalışanlar işten ayrıldığında operasyonel aksaklıklar yaşanabilir ve bu durum kurumsal hafızanın kaybolmasına ya da zayıflamasına neden olabilir. Söz konusu riske yönelik olarak idarenin seçimi yedek personel uygulamasını başlatmak olabilir. Ancak mevcut riskin kabul edilebilir bir seviyede değerlendirilmesi ve yedek personel uygulamasıyla ek maliyetlerin oluşması sebebiyle idare, yedek personel uygulamasını başlatmak yerine herhangi bir ilave risk yönetimi faaliyeti gerçekleştirmemeyi ve riskleri kabul etmeyi seçebilir.

Kabul edilen riskler, söz konusu risklerin zaman içinde kabul edilebilir seviyede kaldığından emin olunması amacıyla uygun görülen periyotlarla değerlendirilmelidir.

Riski Azaltmak: Riskin gerçekleşmesi halinde oluşacak zararın risk iştah seviyesine göre kabul edilebilir bir düzeye indirilmesi için, ilave risk yönetimi faaliyetlerinin belirlenmesi ve uygulanmasıdır.

Risklerin azaltılmasına yönelik ilave risk yönetimi faaliyetlerine ilişkin örnekler aşağıda yer almaktadır:

STRATEJİK HEDEF	RİSK	İLAVE RİSK YÖNETİMİ FAALİYETİ
Bedensel engelli vatandaşların kamu hizmetlerine erişimini kolaylaştırıcı faaliyetlerde bulunmak	Kamu idare ve kuruluşlarının erişilebilirlik eğitimleri konusunda isteksiz davranması ve eğitim planlaması yapmaması sonucu bedensel engeli olan kişilerin kamu hizmetlerine yeterli düzeyde erişim sağlayamaması	Konuya ilişkin kamu idare ve kuruluşlarına eğitimler vererek bilinçlendirmenin sağlanması Erişilebilirliğe ilişkin broşür ve el kitabı hazırlanması, kamu spotu yayımlanması
Üniversitede üretilen bilginin toplumla paylaşılması	Açık Erişim Kaynakları için gerekli duyurular yapılmadığından, bu kaynaklardan yararlanan kişi sayısının yeterli düzeye ulaşmaması	Üniversitelerarası Ortak Açık Arşiv Platformunun oluşturulması
Kaliteli sağlık hizmeti sunmak için, ulusal ve uluslararası akreditasyonunu sağlamış, hasta memnuniyetini öne çıkaran üçüncü basamak üst düzey merkezler kurulması ve mevcut merkezlerin niteliğinin geliştirilmesi	Bu merkezlerde kullanılacak tıbbi cihazların seçimlerinin hatalı şekilde yapılması sonucu finansal kaynakların etkili, ekonomik ve verimli kullanılamaması nedeniyle yaşanan finansal kayıpların sunulan hizmetin kalitesini düşürmesi	İdare tarafından tıbbi cihaz alımlarının etkili, ekonomik ve verimli bir şekilde ve analizlere dayalı olarak yapılması (İhtiyaç analizi, fayda maliyet analizi gibi) Satın alımlara ilişkin politika ve prosedürlerin daha da geliştirilmesi

Tablo 14 – Riski Azaltmak İçin Gerçekleştirilecek Örnek İlave Risk Yönetimi Faaliyetleri

Riskin azaltılması için tanımlanan ilave risk yönetimi faaliyeti kimi durumlarda birden çok sayıda riski kabul edilebilir seviyeye indirebilir. Örneğin; idarenin tedarikçi performansını değerlendirme sürecini devreye alması, hem malzemelerin zamanında ve beklenen kalitede temin edilememesi sonucunda faaliyetlerin aksaması riskini hem de idarenin itibar riskini yönetmekte kullanılabilir.

Bazı durumlarda ise bir riskin azaltılması için birden fazla risk kararının aynı anda alınması ve uygulanması gerekebilir. Örneğin; idarenin uygun bir kayıt, dosyalama ve arşivleme sürecinin bulunmaması sonucu kritik verilerin kaybedilmesi riskine yönelik olarak hem riskin azaltılması (arşiv ve depolama alanında ilave güvenlik sistemlerinin kurulması ve elektronik yedekleme) hem de riskin devredilmesi (özel firmalardan veri güvenliğinin test edilmesi ve gerekli yazılım ve donanımın belirlenmesine yönelik hizmet alımı) kararlarını alması ve uygulaması gerekebilir.

Riskin azaltılması kararının seçilmesi durumunda, bir sonraki aşamada riskin etki ve olasılığını azaltacak ilave risk yönetimi faaliyetleri tanımlanarak Risk Kayıt ve İlave

Risk Yönetimi Faaliyeti Takip Formuna (Ek–12) kaydedilir. Risklerin azaltılması kapsamında uygulanacak risk yönetimi faaliyetleri 4 grupta sınıflandırılabilir:

Yönlendirici risk yönetimi faaliyetleri: Bilgilendirme, davranış şekli belirleme gibi dolaylı faaliyetler ile risklerin azaltılmasına yönelik risk yönetimi faaliyetleridir. Çalışanlara eğitim verilmesi, broşür, afiş veya el kitabı hazırlanması yönlendirici risk yönetimi faaliyetlerine örnek olarak verilebilir.

Önleyici risk yönetimi faaliyetleri: İstenmeyen durumların meydana gelmesini önleyen risk yönetimi faaliyetleridir. Bilgi teknolojisi sistemlerine erişim yetkilerinin çalışanların görev tanımları ile uyumlu olacak şekilde tanımlanması önleyici risk yönetimi faaliyetlerine örnek olarak verilebilir. Görev tanımı bazında oluşturulacak yetkilendirme sayesinde, sisteme yetkisiz erişimlerin ve yetkisiz işlemlerin önüne geçilebilir.

Tespit edici risk yönetimi faaliyetleri: Gerçekleşmiş ancak istenmeyen bir durumun tespit edilmesini sağlayan risk yönetimi faaliyetleridir. Hazırlanan raporların gözden geçirilmesi veya sistemde oluşturulan yetki tanımlamalarının periyodik olarak kontrol edilmesi tespit edici/ortaya çıkarıcı risk yönetimi faaliyetlerine örnek olarak verilebilir.

Düzeltici risk yönetimi faaliyetleri: Gerçekleşen ancak istenmeyen sonuçların düzeltilmesi yahut telafi edilmesi için tasarlanmış olan risk yönetimi faaliyetleridir. Bilgi teknolojileri sistemlerine yönelik oluşturulan acil durum eylem planları veya kurtarma programları düzeltici risk yönetimi faaliyetlerine örnek olarak verilebilir.

İlave risk yönetimi faaliyetleri uygulandıktan sonra artık risk, idare için kabul edilebilir bir seviyede ise ilgili risk için yeniden ilave risk yönetimi faaliyeti gerçekleştirilmesine gerek olmayıp, riskin izlenmesi yeterli olacaktır. İdarenin mevcut risk yönetimi faaliyetlerine rağmen hesaplanan artık risk hala kabul edilebilir seviyede değilse, ilave risk yönetimi faaliyetlerinin belirlenmesi ve uygulamaya alınması gerekir.

Risklere yönelik tanımlanacak ilave risk yönetimi faaliyetleriyle risklerin etki ve olasılık seviyelerinin azaltılması, böylece risklerin gerçekleşmesi halinde maruz kalınacak zararların azaltılması mümkündür. Örneğin; bilgi sistemleri felaket kurtarma merkezi deprem bölgesinde olan bir idare, depremin gerçekleşmesi durumunda karşı karşıya kalacağı veri kaybı riskini yönetirken; bilgi sistemleri felaket kurtarma merkezini deprem bölgesinde olmayan bir şehre taşıdığında riskin olasılık seviyesini azaltırken, mevcut yerleşkesini depreme dayanıklı hale getirmek üzere gerekli çalışmaları yaptığında riskin etki seviyesini azaltmış olur.

Risklere yönelik alınacak kararların belirlenmesinde söz konusu risklerin hangi kök nedenlerden kaynaklandığının belirlenmesi önem taşımaktadır. Risklerin belirlenmesi adımında tanımlanan kök nedenler, risk yönetimi çalışmalarının sonraki aşamalarında risklere yönelik alınacak kararların doğru ve yeterli bir şekilde belirlenmesine de yardımcı olur. Aşağıda risklere ilişkin alt kök nedenlerden yararlanılarak tanımlanan ilave risk yönetimi faaliyetlerine örnekler verilmektedir:

RİSK	ALT KÖK NEDENLER	İLAVE RİSK YÖNETİMİ FAALİYETLERİ
Personelin mesleki gelişimi için gerekli eğitim ihtiyaçlarının doğru ve etkin şekilde analiz edilmemesi sonucunda personelin performans ve yetkinliklerinin geliştirilememesi ve kritik operasyonlarda mali kayba ya da itibar kaybına yol açan verimsizliklerin ve/veya hataların yaşanması	Personel eğitim ihtiyaçlarının tüm birimlerden temin edilememesi Yıllık eğitim planının oluşturulmaması ve onaylanmaması Yıllık eğitim planının idarenin bütün kademelerinde duyurulmaması	Personelin ihtiyaç duyduğu eğitimlerin zamanında ve yeterli seviyede verilmesi Yıllık eğitim planının oluşturulması ve onaylanması Yıllık eğitim planının idarenin bütün kademelerinde duyurulması
Enerji verimliliği ve çevre duyarlılığı konusunda ilgili paydaşları kapsayan bütüncül ve etkili bir yaklaşımın olmaması sonucunda hava kirliliğinin artması	* Kontrolsüz sanayileşme * Sürekli artan enerji talebi * Yükselişe geçen şehirleşme * Azalan ormanlık alanlar * Yoğun hayvancılık faaliyetleri * Kontrol edilmeyen sera gazı salımı	Enerji verimliliği ve çevre duyarlılığı konusunda bütüncül ve etkili bir yaklaşım oluşturmak üzere kontrolsüz sanayileşme, sürekli artan enerji talebi, yükselişe geçen şehirleşme, azalan ormanlık alanlar, yoğun hayvancılık faaliyetleri ve kontrol edilmeyen sera gazı salımı konularında görevli ve sorumlu idareleri dahil eden bir eylem planının oluşturulması
Veri güvenliğinin sağlanamaması /verilerin amacı dışında kullanılması sonucu hukuki yaptırımlarla karşılaşılması ve idare itibarının zedelenmesi	Bilgi ve belgelerin korunmasına yönelik politika ve prosedürlerinin bulunmaması Kritik bilgilerin yönetilmesinden, işlenmesinden ve imhasından sorumlu kişilerin atanmamış olması Kritik bilgilerin sınıflandırılmaması ve ilgili bilgilere erişim yetkilerinin belirlenmemesi Kritik verileri içeren medyaların (usb, cd vb.) şifreli olmaması, bilgi paylaşım araçlarının güvenliğinin yeterince sağlanmaması	Bilgi ve belgelerin korunmasına yönelik politika ve prosedürlerin hazırlanması ve ilgililerle paylaşılması Kritik bilgilerin yönetilmesinden, işlenmesinden ve imhasından sorumlu kişilerin atanması Kritik bilgilerin sınıflandırılması ve ilgili bilgilere erişim yetkilerinin belirlenmesi/sınırlandırılması Kritik verileri içeren medyaların (usb, cd vb.) şifreli olması, bilgi paylaşım araçlarının güvenliğinin sağlanmasına yönelik önlemlerin alınması

Tablo 15 – Risk, Alt Kök Nedenler ve İlave Risk Yönetimi Faaliyeti Örnekleri

Riske yönelik alınacak kararlardan riskin azaltılması kararının seçilmesi durumunda uygulanacak risk yönetimi faaliyetleri açık ve net bir şekilde tanımlanmalı ve Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formuna (Ek–12) kaydedilmelidir. Riske yönelik uygulanacak ilave risk yönetimi faaliyetlerine ilişkin hatalı ve doğru tanımlama örneklerine aşağıda yer verilmektedir:

HATALI İLAVE RİSK YÖNETİMİ FAALİYETİ TANIMLAMASI	DOĞRU İLAVE RİSK YÖNETİMİ FAALİYETİ TANIMLAMASI
Vatandaşların belediye tarafından yürütülen hizmetlere ulaşımını kolaylaştıracak faaliyetlerin gerçekleştirilmesi	Vatandaşların belediye tarafından yürütülen sosyal yardım hizmetlerine ulaşımını kolaylaştırmak için yardım masası kurulması Vatandaşların afiş, broşür, reklam gibi araçlar ile bilgilendirilmesi
Harcamaların bütçe sınırı içerisinde gerçekleştirilmesi	Bütçe hedef ve gerçekleşmelerinin periyodik olarak kontrol edilmesi ve ilgili birim yöneticilerine raporlanması Bütçe kaynak planlamasından sapmaya neden olabilecek kalemlerin tespit edilerek ilgili birimlerden açıklama istenmesi ve üst yöneticiye raporlanması
Faaliyetlerin sürekliliğini sağlamaya yönelik önlemlerin alınması	Faaliyetlerin sürekliliğini sağlamaya yönelik acil durum eylem planının oluşturulması Eylem planının üst yönetici tarafından onaylanması Onaylanan eylem planının tüm çalışanlar ile paylaşılması
İdareler arası yetki çatışmasına karşı gerekli önlemlerin alınması	Farklı idarelerle etkileşim halinde olunan süreçlerin belirlenmesi, süreçte aksaklıklara neden olan noktaların tespit edilmesi ve koordinasyon sağlanarak süreçlerin iyileştirilmesine yönelik toplantılar yapılması, eylemlerin belirlenmesi ve takip edilmesi

Tablo 16 – Doğru ve Hatalı İlave Risk Yönetimi Faaliyeti Tanımlama Örnekleri

Kamu Kurumsal Risk Yönetimi Yaklaşımı Örnek Soru Seti (Ek–2) dokümanında risklere yönelik alınacak kararların belirlenmesi aşamasında sorulabilecek örnek sorular bulunmaktadır.

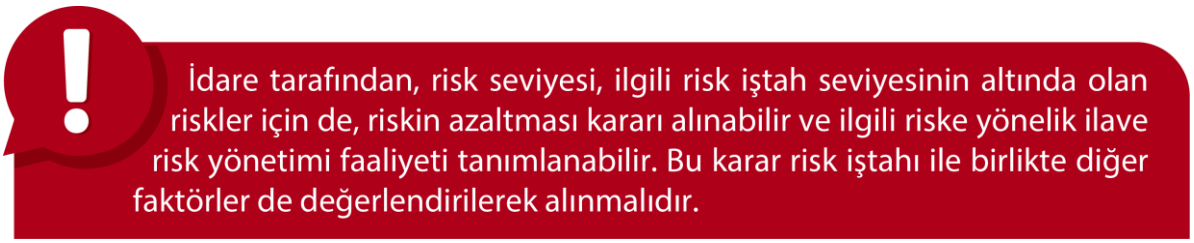
Riske yönelik alınacak kararların belirlenmesine ilişkin adımlar Riske Yönelik Alınacak Kararların Belirlenmesine Yönelik Süreç Akış Şeması (Ek–9) dokümanında açıklanmaktadır.

2.3.1 Riske Yönelik Alınacak Kararları Etkileyen Faktörler

Riske yönelik alınacak kararları etkileyen faktörler aşağıda sıralanmaktadır:

Fayda ve Maliyet Değerlendirmesi: Riski yönetmek için uygulanacak kararın maliyeti ile riskin kabul edilmesi durumunda katlanılacak maliyetin karşılaştırılması, hangi risk kararının tercih edileceği konusunda belirleyici olmaktadır. Söz konusu değerlendirme yapılırken, yönetim tarafından, alternatif kararların olası fayda ve maliyetleri birlikte değerlendirilmelidir. Bu noktada, seçilen risk kararından elde edilecek faydanın bu kararın uygulanması için harcanacak kaynaktan fazla olması gerekmektedir. Örneğin; personel yedekleme uygulaması yapılmamışsa, işten ayrılmalar söz konusu olduğunda idare bilgi birikimini kaybedebilir, faaliyetler aksayabilir, verimlilik kaybı yaşanabilir. Söz konusu riskleri bertaraf etmek için yedek personelin belirlenmesi gerekir. Yedek personelin idare içinden sağlanamaması durumunda ise ilave insan kaynağı ihtiyacı hasıl olabilir. İlave insan kaynağı için katlanılacak maliyet beklenen faydadan düşük ise idare bu ilave risk yönetimi faaliyetinden vazgeçebilir.

Risk İştahı ve Risk Önceliği: Risk iştahı, idarenin hedefleri ve ilgili riskleri çerçevesinde ne ölçüde risk alan veya ne ölçüde risklerden kaçınan bir yapıda olduğu ile ilişkilidir. Risk değerlendirmeleri sonucu elde edilen risk seviyelerinin hedef bazında belirlenmiş olan risk iştah seviyeleri ile karşılaştırılması risklere yönelik hangi kararların alınacağı konusunda yönlendirici olmaktadır.



Riske yönelik alınacak kararlarda risk iştah seviyesi ve risk seviyelerinin dikkate alınmasına yönelik aşağıdaki örnek tabloya yer verilmektedir.

RİSK İŞTAHI	ARTIK RİSK SEVİYESİ	RİSKE YÖNELİK ALINACAK ÖRNEK KARARLAR
YÜKSEK	5	Riskleri yönet, ilave risk yönetimi faaliyetleri gerçekleştir ve izle
	4	Riskleri izle, gerekirse ilave risk yönetimi faaliyeti gerçekleştir
	3	Riskleri kabul et ve izle
	2	Riskleri kabul et ve izle
	1	Riskleri kabul et ve izle
ORTA	5	Riskleri yönet, ilave risk yönetimi faaliyetleri gerçekleştir ve izle
	4	Riskleri yönet, ilave risk yönetimi faaliyetleri gerçekleştir ve izle
	3	Riskleri izle, gerekirse ilave risk yönetimi faaliyeti gerçekleştir
	2	Riskleri kabul et ve izle
	1	Riskleri kabul et ve izle
DÜŞÜK	5	Riskleri yönet, ilave risk yönetimi faaliyetleri gerçekleştir ve izle
	4	Riskleri yönet, ilave risk yönetimi faaliyetleri gerçekleştir ve izle
	3	Riskleri yönet, ilave risk yönetimi faaliyetleri gerçekleştir ve izle
	2	Riskleri izle, gerekirse ilave risk yönetimi faaliyeti gerçekleştir
	1	Riskleri kabul et ve izle

Tablo 17 – Artık Risk Seviyeleri ve Risk İştahının Birlikte Değerlendirilmesi Örneği

Görüldüğü üzere, risk iştahı seviyesi yükseldikçe kabul edilen risklerin sayısı artmakta, ilave risk yönetimi faaliyeti gerçekleştirilen risklerin sayısı azalmaktadır. Ancak, risk iştahı riske yönelik alınacak kararlarda tek etken olarak görülmemelidir.

Risk iştahı ile birlikte, örneğin;

- Riskin "dış risk" kategorisinde olması ve ilgili riske yönelik uygulanabilecek bir ilave risk yönetimi faaliyeti bulunmaması,
- Riski yönetmeye yetecek ölçüde kaynak bulunmaması veya sınırlı ölçüdeki kaynağın daha öncelikli risklere tahsis edilmesi

gibi durumlarda risk seviyesi, hedefle ilişkili risk iştahı seviyesinden yüksek olsa bile idare riski kabul edebilir. Benzer şekilde, risk seviyesi tanımlanan risk iştahı seviyesinin altında olsa bile –özellikle olasılığı düşük veya çok düşük, etkisi ise yüksek veya çok yüksek olan riskler için- idare ilave risk yönetimi faaliyeti tanımlamaya ve uygulamaya karar verebilir.

Yasal Düzenlemeler: Riske yönelik alınacak kararların belirlenmesi aşamasında, tabi olunan yasal düzenlemeler dikkate alınmalıdır.

Paydaş Beklentileri: İdarenin, doğrudan ya da dolaylı olarak etkileşim içinde olduğu tarafların beklentilerini göz önünde bulundurması ve öncelikli risklere yönelik alacağı kararları bu çerçevede değerlendirmesi gerekir. Risk kararlarının belirlenmesinde ilgili tüm tarafların beklentileri, idarenin misyon, vizyon, temel değerleri, stratejik amaç ve hedefleri ile bir bütün olarak değerlendirilmeli ve bu değerlendirme sonrasında uygun ilave risk yönetimi faaliyetleri tanımlanmalıdır.

Etki ve Olasılık Seviyeleri: İlave risk yönetimi faaliyeti tanımlanırken göz önünde bulundurulması gereken faktörlerden biri de mevcut risk yönetimi faaliyetlerinin o riskin etki ve olasılık seviyelerini hangi ölçüde azalttığıdır.

Artık risk seviyesi açısından bakıldığında, olasılık seviyesi düşük, etki seviyesi yüksek olan riskler için etkiyi azaltmaya yönelik ilave risk yönetimi faaliyeti, olasılık seviyesi yüksek etkisi düşük riskler için ise olasılık seviyesini azaltmaya yönelik ek faaliyetler tanımlanmalıdır.
Bir riskin olasılığının yüksek, etkisinin düşük olması ve olasılığını düşürmeye yönelik herhangi bir ilave risk yönetimi faaliyeti tanımlanamaması gibi durumlarda kaynakların etkin kullanılması adına etkiye yönelik ek faaliyet tanımlanmaması, riskin izlemeye alınması tercih edilmelidir.

2.3.2 Risklerin Kayıt Altına Alınması

Kurumsal risk yönetimi yaklaşımında, idare tarafından stratejik amaç ve hedeflere ulaşılmasını etkileyebilecek riskler belirlenirken, değerlendirilirken, önceliklendirilirken ve risklere yönelik kararlar belirlenirken Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formu (Ek–12) kullanılır.

Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formuna riske yönelik kararlar kaydedilerek gerekli ilave risk yönetimi faaliyetleri tanımlanır. Söz konusu ilave risk yönetimi faaliyetlerinden sorumlu birim, yönetici ve personel ile ilave risk yönetimi faaliyetlerinin tamamlanma süreleri belirlenir ve bu bilgiler de aynı forma kaydedilerek takip edilir. Belirlenen riskin dış risk olması ve riskin azaltılması için gerçekleştirilecek ilave risk yönetimi faaliyetlerinin bir başka idarenin inisiyatifine bağlı olması durumunda, ilave risk yönetimi faaliyetlerinden sorumlu birim, yönetici ve personel ile ilave risk yönetimi faaliyetlerinin tamamlanma süreleri inisiyatifine bağlı bulunulan diğer idarelerin kararları dikkate alınarak belirlenir.

Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formu yılda en az 2 defa olmak üzere periyodik olarak gözden geçirilmeli ve gerektiğinde güncellenmelidir. Yeni belirlenen, değişen veya güncelliğini yitiren riskler Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formu üzerinden takip edilmelidir.

Örnek

Risklere Yönelik Alınacak Kararların Belirlenmesi

Risklere yönelik alınacak kararların belirlenmesi aşaması aşağıda bir örnek ile açıklanmaktadır:

Risklere Yönelik Alınacak Kararların Belirlenmesi

Bilgi teknolojisi sistemlerini ve uygulamalarını geliştirme hedefine ilişkin risk iştahının "orta" seviyede olduğu göz önünde bulundurulduğunda idare, risklere yönelik aşağıda yer alan kararları uygulamayı tercih edebilir:

Risk	Artık Risk Seviyesi	Risk İştahı	Riske Yönelik Alınacak Karar
1	Çok Yüksek	Orta	Riski yönet, ilave risk yönetimi faaliyetleri gerçekleştir ve izle
2	Çok Düşük	Orta	Riski kabul et ve izle
3	Orta	Orta	Riski izle, gerekirse ilave risk yönetimi faaliyeti gerçekleştir

Bununla birlikte risk diğer faktörler açısından değerlendirildiğinde;

- İdare yaptığı değerlendirmeler sonucu Risk 1'i yönetmek için farklı kararlar verebilir.

Riski Azaltmak: Risk seviyesinin risk iştah seviyesi ile karşılaştırılması ve paydaş beklentileri düşünüldüğünde, idare ilave risk yönetimi faaliyetleri tanımlayarak ve uygulayarak riskin kabul edilebilir bir seviyeye gelmesini sağlayabilir. Yönetim bilgi sistemi seçimi öncesinde idare kendi kaynakları ile ihtiyaç değerlendirmesi yaparak ihtiyaçlarına en uygun fayda-maliyet dengesini sağlayacak yönetim bilgi sistemini araştırılabilir ve söz konusu değerlendirme ve araştırma sonuçlarını dikkate alarak karar verebilir.

Riski Devretmek: İlgili ihtiyaç analizlerinin gerçekleştirilmesi, yönetim bilgi sistemi seçimi ve işletimi idarenin kaynakları ile sağlanamıyor veya önceliklerden dolayı tercih edilmiyor olabilir. Bu durumda idare örneğin yüklenici firma ile çalışarak riski devretmeye karar verebilir.

Riskten Kaçınmak: İdare fayda-maliyet değerlendirmesi sonucunda mevcut insan kaynağı ve mali kaynaklarının yetersizliği nedeniyle yönetim bilgi sistemlerini değiştirmekten/geliştirmekten vazgeçerek riskten kaçınabilir.

- Risk 2 için risk seviyesi kabul edilebilir seviyede olduğundan ve kaynakları etkin kullanabilecek şekilde tanımlanabilecek ek faaliyet olmadığından idare

söz konusu risk için ilave risk yönetimi faaliyetine gerek duymayabilir, bu riski kabul edebilir ve izleyebilir.

- İdare, Risk 3'ü yönetmek için birden çok karar verebilir.

Riski Azaltmak: Risk seviyesinin risk iştah seviyesinin altına indirilmesi hedeflendiğinde idare ilave risk yönetimi faaliyetleri tanımlayarak ve uygulayarak riskin kabul edilebilir bir seviyeye gelmesini sağlayabilir. Bu kapsamda, acil durum planlarını düzenli aralıklarla test edebilir, planda yer alan senaryoları gerçekleştirerek planının geliştirilmesine katkı sağlarken olası bir felaket anında nasıl hareket edileceğine dair pratik yaparak idare içerisinde farkındalığı arttırabilir.

Riski Devretmek: İdarede yeterli sayıda bilgi teknolojileri personeli bulunmaması durumunda veya felaket kurtarma ve iş sürekliliğine yönelik tecrübeli personel bulunmaması durumunda, idare bu riski hizmet alımı ihalesi suretiyle yüklenici firmaya devredebilir ve ilgili çalışmalar yüklenici firma tarafından yürütülebilir. Bununla birlikte idare, yüklenici firmanın yapacağı testlere yönelik takip kontrolleri tasarlayabilir.

Riski Kabul Etmek: İlgili felaket kurtarma testlerinin yapılma sıklığına, farklı senaryoların farklı zarar büyüklüklerine göre idarenin ilgili ek faaliyete ayıracağı insan kaynağı ve finansal kaynak tutarı değişecektir. İdare yapacağı fayda-maliyet değerlendirmeleri ile felaket kurtarma testlerinin sıklığını azaltabilir veya herhangi bir risk yönetimi faaliyeti tanımlamaktan tamamen vazgeçerek riski kabul edebilir.

2.4 Risklerin İzlenmesi ve Raporlanması

2.4.1 Risklerin İzlenmesi

2.4.1.1 Risk İzleme Seviyeleri

Kurumsal risk yönetimi yaklaşımının uygulanmasından nihai olarak üst yönetici sorumludur. Bununla birlikte, tüm çalışanların risklerin yönetilmesi konusunda farklı seviyelerde de olsa sorumlulukları bulunmaktadır.

İzleme faaliyetleri sürekli izleme, yönetim izlemesi ile bağımsız izleme ve inceleme olmak üzere üç farklı seviyede gerçekleştirilir.

Sürekli izleme, idarenin günlük iş akışının bir parçası olarak ilgili riskin ilişkili bulunduğu sürecin sahipleri ve süreç sahiplerini kontrol etmekle yükümlü yönetim kademeleri tarafından gerçekleştirilirken, yönetim izlemesi ile bağımsız izleme ve inceleme belirli periyotlarda gerçekleştirilir. Bağımsız izleme ve inceleme ise iç denetçiler eliyle gerçekleştirilir.

İzleme faaliyetleri gerçekleştirilmeden önce izleme ve gözden geçirme ile ilgili sorumluluklar idare Risk Strateji Belgesinde açık bir şekilde tanımlanmalıdır.

Birinci seviye - Sürekli izleme

Sürekli izleme yürütülen faaliyetlerin, ilgili süreç sahipleri ile hiyerarşik yapı içerisinde süreç sahiplerini kontrol etmekle yükümlü yönetim tarafından gözlemlenmesi şeklinde gerçekleştirilir. Bu faaliyet günlük akıştaki tüm işlemleri kapsamaktadır.

Birinci seviye olan sürekli izlemenin amacı, risk tanımlamalarının doğruluğunu ve yeterliliğini, risk yönetimi faaliyetlerinin etkililiğini, risklerin etki ve olasılık seviyelerinin geçerliliğini, belirlenen ilave risk yönetimi faaliyetlerinin doğru ve zamanında gerçekleştirildiğini, uygulanması kararlaştırılan ilave risk yönetimi faaliyetlerinin etkililiğini, değişen süreçlere istinaden yeni risk tanımlamalarının yapıldığını, risk seviyelerinin ve risk raporlamalarının uygun seviyede ve periyotlarda gerçekleştirildiğini teyit etmektir.

Süreç sahipleri ve yöneticileri tarafından gerekli ilave risk yönetimi faaliyetlerinin daha hızlı belirlenebilmesi için, idarenin öncelikli olarak sürekli izleme faaliyetlerine önem vermesi gerekir.

Sürekli izleme sorumluluğu birim yöneticileri başta olmak üzere tüm çalışanlara aittir. İlgili süreç; günlük faaliyetlerde yeni oluşan risklerin, daha önce belirlenmiş fakat çeşitli nedenlerle seviyesi veya niteliği değişen risklerin, geçerliliğini yitiren risklerin ve gerçekleşen risklerin ilgili birim yöneticileri gözetiminde SGB'ye raporlanması ile gerçekleştirilir. Birim yöneticilerinin sürekli izleme konusunda sorumluluğu bulunmaktadır. Birim yöneticileri ilgili oldukları birimlerde risklerin sürekli izlenmesi, risklere karşı kararlaştırılan ilave risk yönetimi faaliyetlerinin gerçekleştirilmesi ve takip edilmesi konularından sorumludur.

İkinci seviye - Yönetim izlemesi

Kurumsal risk yönetiminin benimsenmesi ve etkin şekilde uygulanması için üst yönetim tarafından sürecin sahiplenilmesi gerekmektedir. Kurumsal risk yönetimine ilişkin uygulanması kararlaştırılan ilave risk yönetimi faaliyetlerinin üst yönetim tarafından gözetimi idareye üç önemli yarar sağlamaktadır:

- Risk kültürünü yaygınlaştırır.

- Olası hataların veya yanlış değerlendirmelerin zamanında düzeltilmesini sağlar.
- Kurumsal risk yönetimi konusunda yeterliliği sağlayarak güven inşa eder.

Kurumsal risk yönetimi yaklaşımının yaygınlaştırılmasında, rehberde tanımlanan metodolojinin uygulanmasında ve risklerin izlenmesi sürecinde temel sorumluluk üst yöneticiye aittir. Üst yönetici idarede risk yönetimi konusunda en üst düzeyde yetkilidir ve risk yönetimi için gerekli yapıları oluşturarak görev ve sorumlulukları açıkça belirler. Üst Yönetici izleme sorumluluğunu İKİYK, SGB ve Birim Yöneticileri vasıtasıyla yerine getirir. Bu kapsamda oluşturulan İKİYK, Risk Strateji Belgesinde belirlenen sıklıkta toplanarak idarenin risk yönetim süreçlerinin etkili işleyip işlemediğini ve risklerde gelinen durumu değerlendirerek üst yöneticiye raporlar.

Riskler Risk Kayıt ve İlave Risk Yönetimi Faaliyetleri Takip Formu ve Kurumsal Risk Yönetimi Takip Raporu aracılığıyla takip edilir. İzleme sıklıkları yılda en az iki kez olmak üzere Risk Strateji Belgesinde idareye özgü olarak belirlenir. Belirlenen izleme sürelerine istinaden Birim Risk Koordinatörü (BRK) tarafından periyodik olarak İdare Risk Koordinatörüne (İRK) raporlama yapılır. İRK gerekli gördüğü veya üst yöneticiye danışması gerektiği durumlarda üst yöneticiye raporlama yapar.

Üçüncü seviye - Bağımsız izleme ve inceleme

Üçüncü seviye olan bağımsız izleme ve inceleme faaliyetleri, iç denetçiler tarafından yürütülür. İç denetimin risk yönetimindeki temel rolü, risk yönetimi yaklaşımının idarenin amaçlarını gerçekleştirmek üzere etkili bir şekilde uygulandığına dair üst yönetime objektif ve makul bir güvence sağlamaktır.

İç denetçiler, risk yönetimi süreçlerinde bağımsız izleme ile risk yönetimi faaliyetlerinin etkili bir biçimde yürütüldüğüne dair güvence sağlarlar. İç denetçiler aynı zamanda risk yönetiminin geliştirilmesi konusunda yönetime danışmanlık hizmeti de verebilirler. Ancak riskleri fiilen yönetmek suretiyle yönetim sorumluluğu almaktan kaçınmak zorundadırlar.

Bağımsız gözden geçirmeler aynı zamanda risk yönetimi çerçevesinin stratejik hedeflere, süreçlerdeki iyileştirme alanlarına uygun olup olmadığının tespitine katkı sağlar ve tutarlılığı arttırmak için benzer riskleri veya risk kategorilerini bir bütün olarak değerlendirerek daha etkili ilave risk yönetimi faaliyetleri gerçekleştirilmesine yardımcı olur.

2.4.1.2 Risk İzlemenin Kapsamı

Risklerin izlenmesi, kurumsal risk yönetimi uygulamalarının işlerliği ve sürdürülebilirliği ile idarenin stratejileri ve hedeflerine ulaşabilmeleri açısından önemli bir aşamadır. İzleme sürecinin süreklilik sağlayacak şekilde tesis edilmesi ile

idarenin, stratejik amaç ve hedeflerine ulaşmasını etkileyebilecek riskler sürekli olarak takip edilir.

Riskler, değişen iç ve dış koşullara bağlı olarak zaman içinde değişim gösterebilir veya yeni riskler ortaya çıkabilir. Risk seviyeleri ve önceliklerinde veya idarenin riske yaklaşımı ile risk iştah seviyesinde değişiklikler olabilir. Daha önce etkili olan risk yönetimi faaliyetleri hedeflerle uyumsuz hale gelebilir, faaliyetler yetersiz kalabilir veya kullanılamaz hale gelebilir, risklere karşı uygulanması kararlaştırılmış olan ilave risk yönetimi faaliyetleri planlandığı gibi uygulanamayabilir. Bu nedenle kurumsal risk yönetimi yaklaşımını etkileyebilecek ana değişim faktörlerini ele almak yararlı olabilir.

Değişen Yönetim ve Süreç Yapısı: İdarenin organizasyon yapısında, faaliyet alanlarında, kullandığı kaynaklarda, yönetim şekli ve kadrosunda meydana gelen değişikliklerin kurumsal risk yönetimi çerçevesine de yansıtılması gerekir. Örneğin, değişen yönetim kadrosu ile birlikte idarenin stratejik yaklaşımı ve risk iştahı değişime uğrayabilir.

Teknolojik Gelişmeler: Teknolojik yeniliklerin ortaya çıkması ile riske verilen tepkiler ve gerçekleştirilecek ilave risk yönetimi faaliyetleri değişebilir. Örneğin;

- Daha önce manuel olarak kontrol edilen verilerin kontrolü sistem tarafından gerçekleştirilen otomatik kontrollere dönüştürülebilir.
- Daha önce değerlendirilmeye alınmayan bir risk, teknolojik yenilikler nedeniyle kritik hale gelebilir. Geçmiş yıllarda hiç gündemde olmamasına rağmen teknolojinin gelişmesi ve yaygınlaşması ile siber güvenlik riski öncelikli risklerden biri haline gelebilir.

Mevzuat Değişiklikleri ve Ekonomik Gelişmeler: Mevzuat değişiklikleri ve ekonomideki gelişmeler idarenin faaliyetlerine yansıyabilir, idarenin yükümlülüklerini artırabilir, stratejik amaç ve hedeflerinin yeniden gözden geçirilmesini gerektirebilir. Kamu idarelerinin öncelikli risklerinden biri haline gelen bilgi güvenliği riski buna örnek olarak verilebilir.

İdareler bu ve benzeri değişimlerin kurumsal risk yönetimi yaklaşımı ile kurum amaç ve hedefleri üzerindeki etkilerini göz önünde bulundurmalı, bunun için de izleme faaliyetlerini etkin tasarlamalı ve yönetmelidir.

İzleme süreci idarenin yapısına göre farklılık gösterebileceği için Risk Strateji Belgesi (Ek–1) içerisinde izleme kapsamının ve periyodunun belirlenmesi gerekir. Kural olarak, riskin önem seviyesi arttıkça izleme sıklığının da artması gerekir. İdareler kendi organizasyon yapıları ve görev alanlarına göre yılda en az iki kez olmak üzere kendilerine özgü izleme periyotları belirleyebilirler. Ana değişim faktörleri göz önüne alındığında izleme süreçlerinin kapsamını belirlerken aşağıda yer alan hususlar dikkate alınmalıdır:

- Yeni Riskler: BRK tarafından stratejik amaç ve hedefleri etkileyebilecek yeni bir risk tespit edilmesi halinde en kısa sürede Anlık Bildirim Formları kullanılarak (Ek–13) İRK'ya bildirim yapılmalıdır. İRK kendisine bildirilen yeni riski, bildirim yapan birim yöneticileri ile değerlendirerek, riskin tek bir birimi mi yoksa birden fazla birimi mi ilgilendirdiğine karar verir. Tanımlanan yeni risk tek bir birimi ilgilendiriyorsa ilgili birim yöneticisinden riskin değerlendirilmesi ve riske yönelik kararların iletilmesini talep eder. Riskin birden fazla birimi ilgilendirmesi durumunda ilgili tüm Birim Yöneticileri ile bir toplantı düzenlenerek riskin değerlendirilmesi ve riske yönelik kararların alınması sağlanır. Yeni tespit edilen riskler, bu risklere ilişkin yapılan değerlendirmeler ve alınan kararlar Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formuna (Ek–12) eklenir.
- Değişen Riskler: Organizasyon yapısında, süreçlerde, teknolojide, ekonomide ve mevzuatta meydan gelen değişiklikler takip edilmeli, bu değişimlerin mevcut riskler üzerindeki etkileri gözden geçirilmeli, gerektiği durumlarda Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formunda yer alan risk tanımları, etkileri, olasılıkları riske yönelik alınan kararlar ve ilave risk yönetimi faaliyetleri gözden geçirilmelidir. Değişen riskler BRK tarafından en kısa sürede Anlık Bildirim Formları kullanılarak (Ek–13) İRK'ya bildirilmelidir. İlgili riskler, Risk Kayıt ve İlave Risk Yönetimi Faaliyeti İlave Risk Yönetimi Faaliyeti Formunda (Ek–12) yer alan "risk güncellik durumu" alanı üzerinden "değişti" olarak işaretlenir ve risklere ilişkin bilgi "açıklama" alanında açıklanır.
- Geçerliliğini Yitiren Riskler: İdareyi etkileyen değişiklikler nedeniyle geçerliliğini yitiren riskler BRK tarafından İRK'ya bildirir. İRK tarafından riskler değerlendirilerek Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formunda (Ek–12) yer alan risk güncellik durumu alanı üzerinden "güncel değil" olarak işaretlenir ve risklere ilişkin bilgi "açıklama" alanında belirtilir.
- Azaltılan ve Devredilen Riskler: Riske yönelik alınan kararın riski azaltmak veya riski devretmek olması durumunda belirlenen ilave risk yönetimi faaliyetleri RSB'de belirlenecek dönemlerde takip edilmelidir. BRK tarafından ilave risk yönetimi faaliyetlerinin mevcut durumu, Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formu (Ek–12) aracılığı ile İRK'ya raporlanmalıdır. Azaltılmasına karar verilen risklerden birim, süreç ve faaliyet düzeyinde olanlar ise yine RSB'de belirlenecek dönemlerde takip edilmelidir.
- Kabul Edilen Riskler: Yüksek ve çok yüksek seviyedeki riskler için riske yönelik alınan kararın riski kabul etmek olması durumunda riskler mutlaka İdare Risk Koordinatörü tarafından belirlenen periyotlarla izlenmeli ve yeniden değerlendirme çalışmaları gerçekleştirilmelidir.
- Gerçekleşen Riskler: Kritik önemdeki bir riskin gerçekleşmesi durumunda ilgili birim yöneticisi gecikmeksizin üst yöneticiye bildirim yapmalıdır. İlgili riskin önceden belirlenmiş olan acil eylem planı veya düzeltici ilave risk yönetimi faaliyetleri

ivedilikle uygulamaya alınmalı ve düzeltici faaliyetlerin sonuçları BRK tarafından İRK'ya raporlanmalıdır. İzleme sonuçları Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formu üzerinde açıklama alanında yapılabileceği gibi idarenin belirleyeceği başka bir formatta da raporlanabilir.

- Çok Yüksek ve Yüksek Seviyeli Riskler (ÖRG Takibi): Takip edilecek risklerin risk seviyelerine göre izleme sıklıkları farklılık gösterebilir. Çok yüksek ve yüksek seviyeli artık riskler, izleme kapsamı içerisinde mutlaka yer almalı, söz konusu riskler için öncü risk göstergeleri atanmalı ve bu göstergeler belirlenen periyotlarla takip edilmelidir.
- Orta ve Düşük Seviyeli Riskler: Artık risk seviyesi orta ve düşük olarak tanımlanan riskler, RSB'de belirlenecek dönemlerde Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formunun Gözden Geçirilmesi ve Güncellenmesi suretiyle takip edilmelidir.
- Doğal Riski Çok Yüksek ve Yüksek Riskler: Doğal risk seviyesi çok yüksek ve yüksek olan fakat mevcut risk yönetimi faaliyetleri ile düşük ve orta seviyeye indirilen riskler, RSB'de belirlenecek dönemlerde Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formunun gözden geçirilmesi ve güncellenmesi suretiyle takip edilmeli, BRK'nın gerekli gördüğü durumlarda öncü risk göstergesi tanımlanmalı ve periyodik olarak takip edilmelidir.
- Etkisi Çok Yüksek Riskler: Etkisi çok yüksek, olasılığı düşük olan riskler idareler tarafından mutlaka ayrıca takip edilir. RSB'de belirlenecek dönemlerde Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formunun (Ek–12) Gözden Geçirilmesi ve Güncellenmesi suretiyle güncellenir ve raporlanır.

  Risklerdeki değişikliklerin doğru olarak ve zamanında tespit edilmesi için tüm yönetici ve çalışanlar tarafından idare içindeki ve idare dışındaki gelişmeler ve değişimler sürekli olarak izlenir ve gerektiğinde uygun kademelere raporlanır.

  Risklerin izlenmesi ve raporlanmasına ilişkin adımlar Risklerin İzlenmesi ve Raporlanmasına Yönelik Süreç Akış Şeması (Ek–11) dokümanında açıklanmaktadır.

2.4.2 Risklerin Raporlanması

Kurumsal risk yönetiminde risklerin raporlanması; risk sahipliğinin desteklenmesi ve risk kültürünün yaygınlaştırılarak risklerin sistematik bir şekilde izlenmesi için önemli bir aşamadır. Buna ilave olarak, karar alma mekanizmalarının işletilebilmesi için etkili bir risk raporlama yapısının kurulması önem arz etmektedir.

Etkin bir iletişim ve raporlama yapısının kurulması için,

- Tüm çalışanlar idarenin risk stratejisi ve kendi rol ve sorumluluklarının kurumsal risk yönetimi içerisinde nasıl konumlandığı konusunda bilgi sahibi olmalıdır.

- Karar verme aşamasında risklerin göz önünde bulundurulmasına ilişkin yaklaşım, idarenin tüm kademelerine yayılmalıdır. Karar verme mekanizmasını desteklemek amacıyla risklerin takibi, günlük iş yapış biçiminin bir parçası haline getirilmelidir.
- Etkili ve hızlı bilgi akışının sağlanabilmesi için açık iletişim kanalları kurulmalıdır.
- Risk raporlama içerikleri ve periyotları Risk Strateji Belgesinde net olarak belirlenmeli, tüm sorumlulara duyurulmalıdır.
- Risk raporları içerisinde yer alan bilgiler açık ve anlaşılır olmalıdır.
- Raporun yapılacağı yönetim seviyesine göre risklerin önceliklendirilmesi ve gruplandırılması raporlama sürecinin verimli işletilmesini sağlayacaktır. Örneğin; üst yöneticiye yapılacak raporlamalarda kritik risklerin gruplandırılması ve risk haritaları üzerinde gösterilerek raporlanması üst yöneticinin raporları daha efektif değerlendirmesini sağlayacaktır.

Üst yöneticinin kurumsal risk yönetimine bakış açısının ve desteğinin, yöneticilerin ve çalışanların kurumsal risk yönetimine verdiği önem üzerinde büyük etkisinin olduğu unutulmamalıdır. Bu nedenle, raporlama ve izleme faaliyetlerinin etkili bir biçimde gerçekleştirilmesi için üst yönetici tarafından şeffaf bir iletişim ve raporlama yapısı kurulması gerekir.

İletişim ve raporlama mekanizmaları iki şekilde tesis edilmektedir:

İç Raporlama: İç raporlama ile iç paydaşlar arasında etkin iletişim kurulması sağlanarak idare içerisinde raporlanması planlanır, raporlama sıklıkları ve sorumlulukları belirlenir. İlgili raporlamaların içerikleri ve sıklıkları üst yönetimin beklentilerine ve idarenin risk stratejisine göre belirlenir.

Dış Raporlama: Dış raporlama ile dış paydaş beklentilerini karşılayacak raporlamalar belirlenir. İlgili raporlamaların içerikleri ve sıklıkları dış paydaş beklentilerine ve idarenin risk stratejisine göre belirlenir.

Aşağıda yer alan tabloda asgari raporlama gerekliliklerine yer verilmiştir. İdare ihtiyaçları doğrultusunda Risk Strateji Belgesinde belirleyeceği sayı ve sıklıkta raporlamalar yapabilir.

RAPOR/ DOKÜMAN	RAPORLAMA TÜRÜ	İZLEME SEVİYESİ	RAPORLAMA SIKLIĞI	RAPORU HAZIRLAYAN	RAPORUN SUNULDUĞU MERCİ
Faaliyet Raporu	İç Raporlama Dış Raporlama	İkinci Seviye	Yıllık	Birim Yöneticileri	Üst Yönetici
Sürekli İzleme Sonucu Tespit Edilen Yeni, Değişen, Gerçekleşen ve Geçerliliğini Yitiren Riskler	İç Raporlama	Birinci Seviye	Yeni risk oluştuğunda Risk değiştiğinde Risk gerçekleştiğinde Risk geçerliliğini yitirdiğinde	Tüm Çalışanlar Birim Yöneticileri Birim Risk Koordinatörü	İKİYK
Öncü Risk Göstergeleri	İç Raporlama	İkinci Seviye	Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formu'nda Belirtilen Sıklıkta	Birim Yöneticileri	İKİYK
Riski Azaltmak Adına Tanımlanan İlave Risk Yönetimi Faaliyetlerinin Mevcut Durumu	İç Raporlama	İkinci Seviye	3 Aylık	Birim Yöneticileri	İKİYK
Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formu'nun Gözden Geçirilmesi ve Güncellenmesi (Kurumsal Risk Yönetimi Takip Raporu)	İç Raporlama	İkinci Seviye	6 Aylık	Birim Yöneticileri	İKİYK

Tablo 18 – Örnek Risk Raporlamaları

Yıllık Faaliyet Raporunda Risk Raporlamalarına Yer Verilmesi: **Faaliyet raporları, stratejik plan ve performans programlarına ilişkin stratejik amaç ve hedeflere ulaşılma düzeylerini, amaç ve hedeflerde meydana gelen değişiklikler ile**

karşılaşabilecek risklere ve bunlara yönelik alınması gereken tedbirlere yer verilmek amacıyla yıllık olarak hazırlanır ve kamuoyu ile paylaşılır.

Yıllık faaliyet raporu içerisinde, gerçekleştirilen risk yönetimi faaliyetlerine yönelik özet bilgilere (genel hatlarıyla uygulanan kurumsal risk yönetimi yaklaşımı, kurumsal risk yönetimi faaliyetlerinin idare performansına etkisi, kurumsal risk yönetimi faaliyetlerinin idare bünyesinde gelişimi kapsamında hazırlanan istatistiklere, vb.) yer verilmelidir. İdarelerin kritik olan risklerinin faaliyet raporlarında yer alıp almayacağına ilişkin karar üst yöneticinin inisiyatifindedir.

Sürekli İzleme Sonucu Tespit Edilen Yeni, Değişen, Gerçekleşen ve Geçerliliğini Yitiren Risklerin Raporlanması: Organizasyon yapısının, iş süreçlerinin, bilgi teknolojileri altyapısının veya tabi olunan yasal düzenlemelerin değişmesi sonucu yeni riskler ortaya çıkabilmekte, risklerin sıklığı, etkisi veya niteliği değişebilmekte veya var olan riskler geçerliliğini yitirebilmektedir. Bu tür durumların gerçekleşmesi veya yeni yahut değişen risklerin tespit edilmesi halinde bu durum ilgili birim yöneticileri gözetiminde BRK tarafından Anlık Bildirim Formu (Ek–13) kullanılarak İRK'ya bildirilmelidir. Yeni, değişen, gerçekleşen veya geçerliliğini yitiren tüm riskler ile ilgili güncellemeler Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formuna (Ek–12) kaydedilmelidir.

Öncü Risk Göstergelerinin (ÖRG) Takibi ve Raporlanması: Kritik önemdeki riskler için öncü risk göstergeleri belirlenmişse, bu göstergelerin belirlenen aralıklarla üst yönetime raporlanması ve sürekli izlemeye tabi tutulmaları sağlanır. Örneğin, personel sirkülasyonunun fazla olması durumunda, "kurumsal hafızanın ve bilgi birikiminin korunamaması" kritik bir risk olarak tanımlanabilir. Bu riskin takibi için personel devir hızı, ilgili birim yöneticisi tarafından periyodik olarak ölçülmeli ve düzenli olarak İRK'ya raporlanmalıdır. İRK ise birimlerden gelen öncü risk gösterge sonuçlarını konsolide ederek üst yönetime raporlamalıdır. İlgili raporlama; ÖRG'nin sonuçlarını, ÖRG hedefinden sapma olup olmadığını ve ne kadarlık bir sapma olduğunu, mevcut sapma nedenlerini, sapma durumunda ilave bir risk yönetimi faaliyetinin gerçekleştirilip gerçekleştirilmeyeceğini, gerçekleştirilecek ise bu faaliyetin ayrıntılarını ve tarihini içerek şekilde yapılmalıdır. İlgili raporlama idareye özgü ayrı bir form veya Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formu (Ek–12) üzerinden gerçekleştirilebilir.

Göstergelerde bir sapma olması durumunda riskin tanımı, olasılık ve etkisi, doğal ve artık risk seviyesi değerlendirilmeli ve gerekirse Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formu (Ek-12) üzerinden güncelleme yapılmalıdır. Revizyon gerekliliğine İRK ile BRK birlikte karar vermeli ve güncelleme ilgili birim yöneticileri tarafından yapılmalıdır.

Riski Azaltmak Adına Tanımlanan İlave Risk Yönetimi Faaliyetlerinin Takibi ve Raporlanması: Riske yönelik alınacak kararın riski azaltmak olması durumunda riske yönelik ilave risk yönetimi faaliyetleri tanımlanır, bu ilave risk yönetimi faaliyetlerini yerine getirmekten sorumlu birimler ve yerine getirileceği tarih belirlenir. Bu tanımlamalar Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formu (Ek–12) içerisine kaydedilir. Tanımlanan tarihlere istinaden ilave risk yönetimi faaliyetleri birim yöneticileri tarafından takip edilmeli ve sonuçları RSB'de belirlenecek dönemlerde SGB'ye raporlanmalıdır.

İlgili raporda;

- İlave risk yönetimi faaliyetleri için yapılan planlamaya uygun olarak hayata geçirilemeyen, yönetimin dikkatini çekmesi gereken veya karar almasını gerektiren konulara,
- İlave risk yönetimi faaliyetlerinin tamamlanma durumuna,
- Hayata geçirilen ilave risk yönetimi faaliyetlerinin etkililiğine yönelik bilgilere

yer verilmelidir.

Belirlenen ilave risk yönetimi faaliyetlerinin uygulama durumları aşağıdaki şekilde sınıflandırılır. İlave risk yönetimi faaliyeti durumu, Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formu (Ek–12) içerisinde ilgili birim yöneticileri tarafından seçilerek açıklamaları ile RSB'de belirlenen periyotlarla SGB'ye raporlanır.

İLAVE RİSK YÖNETİMİ FAALİYETİNİN DURUMU	AÇIKLAMA
İlave Risk Yönetimi Faaliyeti Gerçekleştirildi	Tanımlanan ilave risk yönetimi faaliyetlerinin tamamı uygulamaya alınmıştır.
İlave Risk Yönetimi Faaliyeti Geliştirme Aşamasında	İlave risk yönetimi faaliyeti kısmen tamamlanmıştır.
İlave Risk Yönetimi Faaliyeti Planlandı	İlave risk yönetimi faaliyetine dair planlamalar yapılmış, rol ve sorumluluklar atanmış fakat henüz ilerleme kaydedilmemiştir.
İlave Risk Yönetimi Faaliyeti Gerçekleştirilmedi	Herhangi bir ilave risk yönetimi faaliyeti gerçekleştirilmemiştir.

Tablo 19 – İlave Risk Yönetimi Faaliyeti Durumu Sınıflandırması

Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formunun Gözden Geçirilmesi ve Güncellenmesi: Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formu (Ek-12), SGB'nin ilgili birimleri bilgilendirmesi ve birimlerden risklere yönelik güncel bilgileri talep etmesi ile RSB'de belirlenecek periyotlarla gözden geçirilir. Gözden geçirme

sonucunda gerekli güncellemeler yapılır ve Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formu aracılığı ile İKİYK'ya sunulur.

Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formunun gözden geçirilmesi ve güncellenmesi çalışması sırasında idarenin risk kütüğündeki tüm riskler gözden geçirilerek güncel durumları değerlendirilir ve form içerisinde gerekli düzenlemeler yapılır. Yapılan düzenlemeler İKİYK'ya "Risk Yönetimi Takip Raporu" ile sunulur. İlgili raporda yer alması gereken asgari hususlar aşağıda sıralanmaktadır. İdareler, aşağıda gösterilen hususlara yer vermek kaydıyla raporun formatını ve içeriğini Risk Strateji Belgesinde kendileri belirleyebilirler.

- Artık risk seviyesi yüksek ve çok yüksek riskler ve bu risklere yönelik gerçekleştirilen ilave risk yönetimi faaliyetleri
- Gerçekleşen riskler ve bunlara uygulanan yönetim faaliyetleri
- Öncü risk göstergelerinin sonuçları, göstergelerden sapmalar ve sapma nedenleri
- Kurumsal risk yönetimi uygulamaları sırasında tespit edilen iyileştirme noktaları ve öğrenilen iyi uygulamalar (öğrenilen dersler)

  - ❖ Öğrenilen derslerin raporlanması: Risk yönetimi yapısının sürekli olarak iyileştirilebilmesi için edinilen tecrübeler, raporlamalarla desteklenmeli, idarenin yeni bir riskle karşılaşması ve bununla başa çıkmak için etkili bir risk yönetimi faaliyeti sağlaması halinde, edinilen tecrübeler söz konusu riskle karşı karşıya kalabilecek diğer yönetici ve çalışanlara aktarılmalıdır.

- Ölçülebilmesi durumunda riskleri yönetmek için katlanılan maliyetler

  - ❖ Risk maliyetlerinin raporlanması: Kurumsal risk yönetimi süreci içerisinde var olan risklerin etki veya olasılığını azaltmak adına ilave risk yönetimi faaliyetleri tanımlanabilmektedir. İlave risk yönetimi faaliyetleri için bütçeden kaynak ayrılması gerekebilir. Bütçelenen ve gerçekleşen tutarların raporlanmasında yarar bulunmaktadır. Örneğin, bir ilave risk yönetimi faaliyetinin gerçekleştirilmesi için sistem üzerinde yazılım geliştirilmesi gerekebilir.

- Artık risk seviyesi orta ve düşük olarak tanımlanan riskler, ilgili risklerde meydana gelen değişimler ve değişim nedenleri
- Doğal risk seviyesi çok yüksek ve yüksek olan fakat mevcut risk yönetimi faaliyetleri ile düşük ve orta seviyesine indirilen riskler, bu risklere dair mevcut yönetim faaliyetlerinde bir değişiklik olup olmadığı, değişiklik olmuş ise bu değişikliklerin risk seviyeleri üzerindeki etkisi

- **Etkisi çok yüksek, olasılığı düşük olan riskler, ilgili risklerde meydana gelen değişimler ve değişim nedenleri**
- **Riske yönelik alınacak karar olarak "kabul et" kararı verilen riskler**

Kurumsal Risk Yönetimi Takip Raporu, birimlerden gelen bilgilere istinaden SGB tarafından konsolide edilir, İKİYK tarafından değerlendirilir ve onaylanır.

3 RİSK İLETİŞİMİ

3.1 Kurumsal Risk Yönetiminde Rol ve Sorumluluklar

Risk yönetimine ilişkin rol ve sorumluluklar açıkça belirlenmeli ve görev tanımları içerisinde bu rol ve sorumluluklara yer verilmelidir. İdareler organizasyon yapıları ve önceliklerine göre kendilerine özgü ilave rol ve sorumluluklar belirleyebilir ve bu rol ve sorumlulukları Risk Strateji Belgesi (Ek–1) içerisinde tanımlayabilirler.

Risk yönetiminde başlıca aktörler aşağıda yer almaktadır.

Üst Yönetici

5018 sayılı Kanunun 11 inci maddesine göre Bakanlıklarda ve diğer kamu idarelerinde en üst yönetici, il özel idarelerinde vali ve belediyelerde belediye başkanı üst yöneticidir. 9 Ağustos 2018 tarihli ve 30504 sayılı Resmi Gazetede yayımlanan 2018/5 sayılı Cumhurbaşkanlığı Genelgesi ile bakanların kendilerine doğrudan bağlı hizmet birimleri bakımından, bakan yardımcılarının kendilerine bağlı hizmet birimleri bakımından en üst yönetici sayılması uygun görülmüştür. 5018 sayılı Kanun çerçevesinde, idarelerin stratejik planlarının ve bütçelerinin kalkınma planına, yıllık programlara, stratejik plan ve performans programları ile hizmet gereklerine uygun olarak hazırlanması ve uygulanmasından, sorumlulukları altındaki kaynakların etkili, ekonomik ve verimli şekilde elde edilmesi ve kullanımını sağlamaktan, kayıp ve kötüye kullanımının önlenmesinden, malî yönetim ve kontrol sisteminin işleyişinin gözetilmesi, izlenmesi ve kanunlar ile Cumhurbaşkanlığı kararnamelerinde belirtilen görev ve sorumlulukların yerine getirilmesinden Bakana; mahallî idarelerde ise meclise karşı sorumlu olan üst yönetici aynı zamanda risk yönetimi yaklaşımının idare içinde uygulanmasından sorumludur.

Üst yönetici;

- Kurumsal risk yönetiminin oluşturulması, uygulanması, izlenmesi ve gerekli tedbirlerin zamanında alınmasının sağlanmasından,
- Kurumsal risk yönetiminin uygulanması için gerekli yapıların oluşturulması ve söz konusu yapıların rol ve sorumluluklarının belirlenmesi ile uygulama rol ve sorumluluğu bulunan personelin teşvik edilmesinden,
- Stratejik amaç ve hedeflerin belirlenmesi sırasında hedef bazında belirlenen risk iştahının onaylanmasından,
- Farklı idarelerle ortak ele alınması gereken risklerin yönetiminde o idarelerin üst yöneticileri ile iş birliği ve koordinasyon sağlanmasından,

- İdare Risk Koordinatörü ve İKİYK tarafından kendisine sunulan rapor ve bildirimlerin değerlendirilmesinden,
- Kurumsal risk yönetimi uygulamaları konusunda İç Denetim Birimi'nden makul güvence alınmasından ve risklerin etkili yönetilip yönetilmediğine ilişkin sonuçların değerlendirilmesinden,
- Kurumsal risk yönetimi yaklaşımının uygulanması sırasında belirlenen risklere yönelik RSB'de belirlenen dönemlerde izleme ve değerlendirme toplantıları yapılmasından, bu toplantılarda risklerin izlenmesi ve raporlanması süreçlerinin etkili ve verimli yönetilip yönetilmediğinin değerlendirilmesinden,
- Risk Strateji Belgesinin değerlendirilmesinden ve onaylanmasından,
- Risk yönetimi takviminin onaylanmasından,
- Risk yönetimi uygulamalarının idare içinde etkin işlemesi için görevlendirilen çalışma ekiplerinin ve çalışanların rol ve sorumluluklarının onaylanmasından,
- Risk yönetimi kapsamında idare içinde düzenlenecek eğitimlerin içeriklerinin ve katılımcılarının değerlendirilmesinden ve onaylanmasından,
- Risklerin izlenmesi ve raporlanması mekanizmalarının idare içinde etkin yönetilmesinden,
- Faaliyet raporuna eklenen risk yönetimi uygulamalarına ilişkin özet bilgilerin değerlendirilmesinden ve onaylanmasından,
- İç ve dış denetim raporlarında yer alan bilgilerin değerlendirilmesinden ve risk yönetimi kapsamına alınacak bilgilerin belirlenmesinden,
- Kurumsal risk yönetiminin uygulanması sırasında belirlenen risklere yönelik altı aylık dönemlerde izleme ve değerlendirme toplantılarının gerçekleştirilmesinden, bu toplantılarda risklerin izlenmesi ve raporlanması süreçlerinin etkin yönetilmesinden, Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formunun ve Risk Yönetimi Takip Raporunun 6 aylık dönemlerde gözden geçirilmesinden, değerlendirilmesinden ve onaylanmasından

sorumludur.

İç Kontrol İzleme ve Yönlendirme Kurulu (İKİYK)

İç Kontrol İzleme ve Yönlendirme Kurulu, üst yönetici ve harcama yetkililerinden oluşur. Toplantılara ihtiyaç duyulması halinde üst yöneticinin görevlendireceği diğer kişiler davet edilebilir. İKİYK'nin sekretarya hizmetleri SGB tarafından yürütülür.

İç Kontrol İzleme ve Yönlendirme Kurulu;

- Risk Strateji Belgesi (Ek–1) taslağının oluşturulmasından ve değerlendirilmek üzere üst yöneticiye sunulmasından,

- Kurumsal risk yönetimi uygulamalarının idare içinde etkili bir biçimde işlemesi için görevlendirilen çalışma ekiplerinin ve çalışanların rol ve sorumluluklarının belirlenmesinden, söz konusu rol ve sorumlulukların üst yöneticinin onayına sunulmasından ve Risk Strateji Belgesine aktarılmasından,
- Kurumsal risk yönetimi takviminin oluşturulmasından, üst yöneticinin onayına sunulmasından, ilgililere duyurulmasından ve takvimde belirlenen çalışmaların gerçekleştirilmesinden,
- Kurumsal risk yönetimine yönelik eğitim ihtiyaçlarının tespit edilmesinden, eğitim içeriklerinin ve katılımcılarının belirlenmesinden ve üst yöneticiye sunulmasından,
- Kurumsal risk yönetimi adımlarının idare içerisinde uygulanmasına yönelik çalışanları teşvik etmekten,
- Stratejik amaç ve hedeflere ulaşılmasını etkileyebilecek risklerin belirleneceği ve değerlendirileceği çalıştayların yapılmasını teşvik etmekten,
- İdarenin hedefleri bazında ortak risk algısı göz önünde bulundurularak çalıştaylar sırasında belirlenen risk iştahlarının değerlendirilmesinden,
- Stratejik amaçlar ve hedefler seviyesinde belirlenen ve değerlendirilen risklerin gözden geçirilmesinden ve nihai hale getirilmesinden,
- İdare Risk Koordinatörü tarafından bildirilen riskler arasından stratejik düzeyde önemli gördüğü riskleri gündemine almaktan,
- Farklı idareler veya birimler tarafından belirlenen risklerden birbiriyle ilgili olanların değerlendirilmesinden,
- Stratejik amaç ve hedeflere ilişkin risklere yönelik alınacak kararların belirlenmesinden, belirlenen kararların gözden geçirilmesinden ve nihai hale getirilmesinden,
- Risklere yönelik alınacak kararların belirlenmesi aşamasında üst yönetici tarafından değerlendirilmesi gereken risklerin İRK tarafından üst yöneticiye bildirilmesinden ve üst yönetici değerlendirmelerinin çalışmalara dâhil edilmesinden

sorumludur.

İdare Risk Koordinatörü (İRK)

Üst yönetici, yardımcılarından birini veya SGB yöneticisini İdare Risk Koordinatörü olarak görevlendirir. Üst yöneticinin Bakan olduğu durumlarda Bakan tarafından görevlendirilen bir Bakan Yardımcısı, üst yöneticinin Bakan Yardımcısı olduğu idarelerde ise Bakan Yardımcısı tarafından görevlendirilen Genel Müdür İRK olarak belirlenebilir.

İdare Risk Koordinatörü, risk yönetiminin uygulanmasından üst yöneticiye karşı sorumludur.

İdare Risk Koordinatörü;

- Kurumsal risk yönetimi yaklaşımının etkili bir biçimde uygulanıp uygulanmadığına dair değerlendirmelerde bulunmaktan,
- Birim, faaliyet ve süreç risklerine ilişkin olarak Birim Risk Koordinatörleri tarafından bildirilen risklerden stratejik seviyede ele alınması gerekenleri İKİYK ve üst yöneticiye sunmaktan,
- Stratejik seviyede ele alınması gereken risklere yönelik alınacak kararların belirlenmesi aşamasında üst yönetici tarafından değerlendirilmesi gereken risklerin üst yöneticiye bildirilmesinden,
- Belirlenen risklerin ve ilave kontrol faaliyetlerinin diğer idarelerle ilişkili olması durumunda gerekli koordinasyonun sağlanması için üst yöneticiyi bilgilendirmekten

sorumludur.

Birim Risk Koordinatörü (BRK)

Birim Risk Koordinatörü, birim yöneticisi tarafından; birimin görevleri ve iç kontrol uygulamaları konusunda birikim ve tecrübesi olan kişiler arasından belirlenir. Ancak teşkilat yapısının küçüklüğü ve personel sayısının yetersizliği gibi nedenlerle BRK belirlenmesinde güçlük bulunan idarelerde birim yöneticisinin, BRK olması mümkündür.

Birim Risk Koordinatörü;

- Birimin hedeflerini etkileyebilecek risklerin tespit edilmesini koordine etmekten ve rehberlik sağlamaktan, tespit edilen risklerin alt birimlerin bilgi ve uzmanlıklarından yararlanarak faaliyetleri ile eşleştirmekten ve tüm önemli konuların ele alınmasını sağlamaktan,
- Birimin hedeflerine ilişkin risklerden stratejik amaç ve hedeflerle ilgili olan ve stratejik seviyede ele alınması gerekenleri belirlemek ve birim yöneticisinin uygun görüşünü alarak İRK'ya bildirmekten,
- Yıllık olarak belirlenen risk kayıtlarının ve ilgili raporların idare tarafından belirlenecek periyotlarla gözden geçirilmesinden (aylık, 3 aylık gibi) ve birim yöneticisinin de onayını alarak İRK'ya raporlanmasından,
- Alt Birim Risk Koordinatörlerinin (ARK) raporladıkları risklerin birim düzeyinde izlenmesinden, mevcut risklerdeki değişiklikleri ve varsa yeni riskleri değerlendirerek birim yöneticisinin uygun görüşünü alarak İRK'ya raporlanmasından,
- Yıllık olarak, daha önce belirlenmiş veya yıl içerisinde ortaya çıkabilecek risklerin iyi yönetilip yönetilmediğine dair kanıtların İRK'ya sunulmasından,

- İRK ve İKİYK'nın görüşleri, tavsiyeleri ve kararları doğrultusunda varsa ARK'lara geri bildirim sağlanmasından,
- Kurumsal risk yönetimiyle ilgili eğitim ihtiyaçlarının tespit edilmesinden

sorumludur.

Alt Birim Risk Koordinatörü (ARK)

Risklerin alt birim düzeyinde yönetilmesinin uygun görüldüğü idarelerde Alt Birim Risk Koordinatörü, alt birim yöneticisi veya görevlendirdiği kişidir. ARK, risk yönetim faaliyetlerinin alt birim düzeyinde koordinasyonundan sorumludur.

Alt Birim Risk Koordinatörü;

- Alt birim düzeyindeki risklerin tespit edilmesi, değerlendirilmesi, cevap verilmesi, gözden geçirilmesi ve raporlanması görevlerinin yerine getirilmesinin koordine edilmesinden,
- İdarenin risk stratejisine uygun olarak alt birimin faaliyetlerine ait yeni tespit edilen risklerin, risk puanı değişenlerinin ve bunları azaltmakta kullanılan kontrollerin etkinliğinin BRK'nın belirlediği periyotlarla BRK'ya raporlanmasından,
- İRK tarafından talep edilen bilgi ve belgelerin verilmesinden

sorumludur.

Birim Yöneticileri

Birim Yöneticileri;

- Risk yönetimi çalışmalarına başlamadan önce SGB tarafından düzenlenecek olan bilgilendirme eğitimlerine katılım sağlanmasından,
- İKİYK ve İdare Risk Koordinatörü tarafından talep edilen bilgi ve belgelerin zamanında ve eksiksiz hazırlanmasından,
- Risklerin belirlenmesi, değerlendirilmesi, riske yönelik alınacak kararlar ile ilave kontrol faaliyetlerinin belirlenmesi ve öncü risk göstergelerinin tanımlanması çalışmalarına katılım sağlanmasından,
- Risklerin sürekli olarak izlenmesinden, risklerde bir değişiklik olması, yeni bir riskin ortaya çıkması, risklerin gerçekleşmesi veya geçerliliklerini yitirmesi durumunda İRK'ye bilgi verilmesinden,
- İzleme sonuçlarının belirlenen periyotlarla İRK'ya raporlanmasından,

- Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formunun (Ek-12) güncellenmesinin ve Kurumsal Risk Yönetimi Takip Raporu'nun hazırlanmasının sağlanmasından

sorumludur.

Strateji Geliştirme Birimi

Strateji geliştirme birimleri idarenin risk yönetimi süreçlerinin tüm birimlerde eşgüdüm halinde işlemesini sağlamak üzere teknik destek ve rehberlik hizmeti verir. İdarenin risk yönetimi çalışmalarını koordine eder. İç kontrol sisteminin değerlendirilmesi kapsamında risk yönetiminin etkinliğini de değerlendirerek belirli dönemlerde İKİYK'ya raporlar. İKİYK'nın ve İRK'nın sekretarya hizmetlerini yürütür. SGB;

- Stratejik plan hazırlık süreci çalışmalarında stratejik amaç ve hedeflere yönelik olarak yapılacak risk yönetimi çalıştaylarının koordine edilmesinden,
- Stratejik amaç ve hedeflere yönelik çalıştaylarda belirlenen risklerin, değerlendirme sonuçlarının, riske yönelik alınacak kararların ve ilave kontrol faaliyetlerine ilişkin bilgilerin konsolide edilmesinden,
- Birimlerde iç kontrol çalıştayları düzenlenerek birim, süreç ve faaliyet seviyesindeki risklerin belirlenmesi ve değerlendirilmesinin koordine edilmesinden ve teknik destek sağlanmasından,
- Harcama birimlerinde yürütülen iç kontrol çalışmaları sonucunda tespit edilen ve idarenin stratejik amaç ve hedeflerine ulaşmasını etkileyebilecek seviyede olan birim, süreç ve faaliyet seviyesindeki risklerin stratejik amaç ve hedeflere yönelik çalıştaylarda değerlendirilmesinden,
- Risk Kayıt ve İlave Risk Yönetimi Faaliyeti Takip Formunun (Ek-12) gözden geçirilerek birim yöneticileri tarafından yapılan revizelerin konsolide edilmesinden ve Kurumsal Risk Yönetimi Takip Raporunun RSB'de belirlenen periyotlarla İKİYK'ya sunulmasından,
- Kurumsal risk yönetimi izleme ve raporlama faaliyetleri kapsamında birimlerden gelen bilgilerin konsolide edilmesinden ve İKİYK'ya sunulmasından

sorumludur.

İç Denetim Birimi

İç denetim, kurumsal risk yönetimi süreçlerinin etkinliğini değerlendirmek ve geliştirmek amacına yönelik sistemli, sürekli ve disiplinli bir yaklaşım uygulayarak idarenin amaçlarına ulaşmasına yardımcı olur.

İç denetçiler, kurumsal risk yönetimi süreçlerinde; risk yönetimi süreçlerinin değerlendirilmesi, kurumsal risk yönetimi süreçlerine ilişkin güvence verilmesi, kurumsal risk yönetimi sisteminin devam ettirilmesi ve geliştirilmesi konusunda rehberlik ve danışmanlık hizmeti verilmesi gibi rol ve sorumluluklara sahiptir.

Öte yandan, iç denetçiler; kurumsal risk yönetimi sisteminin sorumlusu olmak, risklere ilişkin olarak belirlenen kontrol ve eylemleri uygulamak, risklere ilişkin yönetim güvencesi vermek ve risk iştahını belirlemek gibi rol ve sorumluluklardan kaçınmak zorundadır. Bu bakımdan, risk yönetimine ilişkin güvence ve danışmanlık faaliyetlerini gerçekleştiren iç denetçilerin bağımsız ve tarafsız olma özelliğini daima muhafaza etmesi gerekir.

İç Denetim Birimi tarafından kurumsal risk yönetimi faaliyetlerine yönelik makul güvence sunulabilmesi adına aşağıda yer alan sorulardan faydalanılabilir:

- Kurumsal risk yönetimi süreci, kurum içinde yeterince sahipleniliyor mu?
- Kurumsal risk yönetimi çerçevesinin tasarımı ve risk değerlendirme kriterleri, kurumun faaliyet gösterdiği iç ve dış ortama uygun mu?
- Hedefler bazında belirlenen risk iştahları, kurumsal yönetim yapısı ile uyumlu mu?
- Kurumsal risk yönetimi süreci çıktılarının kurum içinde uygun ve yeterli bir şekilde iletilmesini sağlayacak iç iletişim ve raporlama kanalları var mı? İlgili yasal düzenlemelere ve kurumsal yönetime uygun mu?
- Benimsenen kurumsal risk yönetimi çerçevesi kurum içinde etkili bir şekilde uygulanıyor mu?
- Risklerin belirlenmesi, bu konuda yeterli bilgiye sahip kişilerce gerçekleştiriliyor mu, mevcut risk tanımlama çalışmaları yeterli mi?
- İç ve dış ortam değişiklikleri ile kurumsal ihtiyaçlardaki değişiklikler doğrultusunda, kurumsal risk yönetimine ilişkin süreçlerde gerekli uyarlamalar yapılıyor mu?
- Risklerin değerlendirilmesinden ve risklere yönelik alınacak kararların belirlenmesinden sorumlu kişiler, yeterli bilgiye sahip mi, bu faaliyetlerin gözden geçirilmesi ve onaylanması süreçleri etkin mi?
- İlave risk yönetimi faaliyetleri izleniyor ve uygun yönetim kademelerine raporlanıyor mu?

Hazine ve Maliye Bakanlığı İç Kontrol Merkezi Uyumlaştırma Birimi

İç Kontrol Merkezi Uyumlaştırma Birimi (İKMUB); ulusal ve uluslararası iyi uygulamalar doğrultusunda, risk yönetimine ilişkin genel standartların ve ilgili diğer düzenlemelerin belirlenmesinden, uygulamanın izlenmesi ve geliştirilmesinden, idareler arasında koordinasyonun sağlanmasından sorumludur. Ayrıca İKMUB;

- İç kontrol standartlarını belirler ve bu standartlara uyulup uyulmadığını izler,
- Ön malî kontrole ilişkin standart ve yöntemler ile ön malî kontrole tâbi malî karar ve işlemleri ve bunların kontrol usul ve esaslarını belirler,
- Harcama yetkililerine ilişkin mevzuat düzenlemelerini hazırlar, harcama yetkilisinin belirlenmesine ilişkin konularda tereddütleri giderir,
- İç kontrol alanında idareler arasında koordinasyonu sağlar ve idarelere rehberlik hizmeti verir,
- İç kontrol ve ön malî kontrole ilişkin genel ve özel nitelikli düzenlemelerde idarelerle işbirliği yapar, çalışma toplantıları düzenler,
- İç kontrol ve ön malî kontrol düzenleme ve uygulamaları hakkında idarelerden rapor ve bilgi alarak sistemlerin işleyişini izler, belirlenen yöntem ve standartlara uygunluğu açısından değerlendirir, kurumsal ve konsolide raporlar düzenler,
- İdarelerin malî hizmetler birimlerinin çalışma usul ve esaslarını belirler,
- Kamu idarelerinin malî hizmetler birim yöneticilerine, diğer yönetici ve malî hizmetler uzmanlarına yönelik düzenli yıllık bilgilendirme ve değerlendirme toplantıları ile seminer, sempozyum, panel ve benzeri etkinlik ve faaliyetleri düzenler,
- İç kontrol ile mali yönetim ve kontrol sistemine ilişkin olarak eğitim programları hazırlar,
- Ulusal ve uluslararası iyi uygulama örneklerini araştırır, bunların uygulanması yönünde çalışmalar yapar.

3.2 Kurumsal Risk Yönetiminin İç Kontrol, Kalite Yönetimi, İç Denetim ve Dış Denetim ile İlişkisi

Kurumsal risk yönetimi yaklaşımının etkin uygulanabilmesi için iç kontrol, kalite yönetimi, iç denetim ve dış denetim ile eşgüdüm içerisinde ele alınması gerekir. Bütünleşik ve eşgüdümlü bir yaklaşım izlenmeden mevcut kaynaklar verimli kullanılamayabilir ve idarenin stratejik amaç ve hedeflerine ulaşmasını etkileyebilecek öncelikli riskler gerektiği gibi yönetilemeyebilir.

Kurumsal Risk Yönetiminin İç Kontrol ile İlişkisi

İdarelerde kurumsal risk yönetimi çalışmaları ile iç kontrol çalışmalarının etkileşim halinde yürütülmesi, oluşturulacak katma değer açısından oldukça önemlidir.

Kurumsal risk yönetimi yaklaşımı idarenin misyon, vizyon ve temel değerlerini yansıtan risk kültürü yapısının oluşmasını ve bu yapının çalışanlar tarafından benimsenmesini sağlar. Risk kültürü ise idarenin iç kontrol sistemini besleyerek kontrol faaliyetlerinin daha etkili bir şekilde yürütülmesine katkı sağlar. Aynı şekilde iç kontrolün geliştirilmesi ile çalışanlar arasında risk ve kontrol algısının da gelişmesi sağlanır.

5018 sayılı Kanunun 55 inci maddesinde iç kontrol *"İdarenin amaçlarına, belirlenmiş politikalara ve mevzuata uygun olarak faaliyetlerin etkili, ekonomik ve verimli bir şekilde yürütülmesini, varlık ve kaynakların korunmasını, muhasebe kayıtlarının doğru ve tam olarak tutulmasını, malî bilgi ve yönetim bilgisinin zamanında ve güvenilir olarak üretilmesini sağlamak üzere idare tarafından oluşturulan organizasyon, yöntem ve süreçle iç denetimi kapsayan malî ve diğer kontroller bütünüdür."* olarak tanımlanmaktadır.

İç kontrol sürecinde faaliyetlerin etkili, ekonomik ve verimli bir şekilde yürütülmesini, varlık ve kaynakların korunmasını, malî bilgi ve yönetim bilgisinin zamanında ve güvenilir olarak üretilmesini olumsuz yönde etkileyebilecek birim, faaliyet ve süreç seviyesinde risklere odaklanılırken, kurumsal risk yönetimi sürecinde stratejik seviyede ele alınması gereken öncelikli risklere odaklanılır. Nihai olarak hem iç kontrolde hem de kurumsal risk yönetiminde amaç idarenin amaç ve hedeflerine ulaşmasına destek olmaktır.

Stratejik planlama süreciyle başlayan ve sürekli olarak uygulanan kurumsal risk yönetimi yaklaşımında, risklerin belirlenmesi aşamasında, operasyonel seviyedeki risklerden stratejik amaç ve hedeflere ulaşılmasını etkileyebilecek öncelikte olanlar stratejik seviyede ele alınmalı, değerlendirilmeli, izlenmeli ve raporlanmalıdır. Diğer taraftan, birim, faaliyet ve süreç risklerinin değerlendirilmesi çalışmaları gerçekleştirilirken de stratejik risklerle ilgili olanlar ayrıca ele alınmalıdır.

Risklere yönelik cevapların belirlenmesi aşamasında ise riskin azaltılmasına karar verilmesi durumunda iç kontrol sürecinde yürütülen kontrol faaliyetlerinin neler olduğu ve ne düzeyde etkin olduğu değerlendirilmeli ve idare gerekli gördüğü durumlarda ilave risk yönetimi faaliyeti tanımlayarak iç kontrol çalışmaları ile entegre bir şekilde izleme sürecini yürütmelidir.

Kurumsal risk yönetiminin etkinliğinin sağlanması adına kurumsal risk yönetimi ve iç kontrol yaklaşımları birbirleriyle doğrudan iletişim içinde olmalı ve gerçekleştirilen raporlamalar ile birbirlerini beslemelidir.

Kurumsal Risk Yönetiminin Kalite Yönetimi ile İlişkisi

Kalite yönetimi, idarenin faaliyetlerinin, bütün kademelerde benimsenmiş olan bir kalite anlayışı çerçevesinde, sürekli olarak iyileştirilme esasına dayalı olarak gerçekleştirilmesidir. Kalite yönetimi ile faaliyetlere ilişkin hata ve kusurların ortaya çıktıktan sonra tespiti değil, ortaya çıkmadan önce önlenmesi amaçlanır. Önleyici bir bakış açısına sahip olmaları nedeniyle kalite yönetimi ile risk yönetimi benzeşir.

Kalite yönetim süreci kapsamında tüm süreç ve faaliyetler kalite bakış açısı ile değerlendirilir. Aynı zamanda, hedef ve amaçlar ile ilgili riskler ve fırsatlar belirlenir. Kalite standartları risk temelli düşünmeyi içeren süreç yaklaşımını uyguladığından kurumsal risk yönetimi yaklaşımı ile birçok noktada kesişmektedir. Bununla birlikte, kalite yönetimi sürecinde idarenin amaç ve hedeflerine ulaşmak amacıyla yürüttüğü tüm süreç ve faaliyetlere yönelik olası risklere ve bu risklerin bertaraf edilmesine yönelik sürekli iyileştirme faaliyetlerine odaklanılırken, kurumsal risk yönetimi sürecinde stratejik seviyede ele alınan öncelikli risklere odaklanılır.

Kalite yönetimi kapsamında oluşturulan politika ve prosedürler, tanımlanan risk ve fırsatlar, belirlenen iyileştirme planları iç denetim, iç kontrol ve risk yönetimine girdi oluştururken, benzer şekilde iç denetim, iç kontrol ve risk yönetimi çıktıları da kalite yönetimi süreçlerine katkı sağlamaktadır.

Nihai olarak kalite yönetimi, iç kontrol ve risk yönetimi uygulamaları genel performansı arttırarak daha dayanıklı, sürdürülebilir, hesap verebilir bir yönetim yapısı inşa etmeyi ve amaç ve hedeflere ulaşılmasına destek olmayı amaç edinmektedir.

Risk Yönetiminin İç Denetim ile İlişkisi

5018 sayılı Kanununun 63 üncü maddesinde iç denetim "*idarenin çalışmalarına değer katmak ve geliştirmek için kaynakların ekonomiklik, etkililik ve verimlilik esaslarına göre yönetilip yönetilmediğini değerlendirmek ve rehberlik yapmak amacıyla yapılan bağımsız, nesnel, güvence sağlama ve danışmanlık faaliyeti*" olarak tanımlanmaktadır.

İç denetçiler, idarenin; amaç ve hedeflerine ulaşmasının önündeki risklerin gerektiği gibi yönetilip yönetilmediği hususunda bağımsız ve nesnel bir izleme faaliyeti gerçekleştirerek, kaynak tahsisinin en etkili bir başka deyişle en öncelikli alanlara yapılmasına katkı sağlayabilirler. Bununla birlikte bağımsızlık ve nesnelliğin

korunabilmesi açısından, iç denetçiler risk yönetiminde bizzat görev almaktan kaçınmak zorundadır.

İç denetim yaklaşımı açısından bakıldığında, kurumsal risk yönetimi faaliyetleri iç denetim faaliyetlerinin etkinliğinin artmasına da yardımcı olur. İç denetimde risk esaslı denetim planının yapılması aşamasında, idarenin amaç hedeflerini etkileyebilecek stratejik düzeyde ele alınan riskler ile birim, faaliyet ve süreç risklerinin de yer aldığı risk evreni göz önünde bulundurur. İç denetim faaliyeti, öncelikli risklere yönelik uygulanan mevcut ve ilave risk yönetimi faaliyetlerinin yeterliliğinin değerlendirilmesini de kapsar. Risk yönetimi çalışmalarında yeterli olarak değerlendirilmiş olan kontrollerin etkinliği, iç denetim tarafından bağımsız bir gözle değerlendirilir. Böylece hem artık risk seviyeleri hesaplanırken dikkate alınan mevcut kontrollerin hem de riske yönelik olarak alınan kararların riski bertaraf etme ya da azaltma yeterliliği konusunda nesnel güvence sağlanmış olur.

Stratejik amaç ve hedefler ile bunları etkileyebilecek risklerin belirlenmesi aşamasında iç denetimin önceki dönemlerde tespit ettiği bulgular da göz önünde bulundurulur.

Kurumsal Risk Yönetiminin Dış Denetim ile İlişkisi

5018 sayılı Kanunun 68 inci maddesinde, Sayıştay tarafından yürütülen dış denetim, "*genel kabul görmüş uluslararası denetim standartları dikkate alınarak kamu idaresi hesapları ve bunlara ilişkin belgeler üzerinden mali tabloların güvenilirliği ve doğruluğuna ilişkin mali denetim ile kamu idarelerinin gelir, gider ve mallarına ilişkin mali işlemlerin kanunlara ve diğer hukuki düzenlemelere uygun olup olmadığının tespiti*" şeklinde tanımlanmıştır. Sayıştay tarafından hazırlanan Dış Denetim Genel Değerlendirme Raporu, kamu kaynağının elde edilmesi ve kullanılmasında görevli ve yetkili olanların kaynakların etkili, ekonomik, verimli ve hukuka uygun olarak elde edilmesi, kullanılması, muhasebeleştirilmesi, raporlanması ve kötüye kullanılmaması için gerekli önlemleri almasına katkı sağlayan önemli bir araçtır.

Bu kapsamda hazırlanan dış denetim raporları da kurumsal risk yönetimi süreçlerine girdi oluşturmakta, "Riskleri hangi alanlarda aramalıyız?" sorusuna cevap vermektedir. Benzer şekilde dış denetim sonucu iç kontrol ve iç denetim faaliyetlerinin etkinliğine yönelik tespit edilen bulguların kurumsal risk yönetimi kapsamına alınması da stratejik amaç ve hedeflere ulaşmada idareleri destekleyici rol oynayacaktır. Bu nedenle idarenin, stratejik amaç ve hedeflerini etkileyebilecek riskleri belirlerken önceki dönem dış denetim bulgularını göz önünde bulundurması gerekir.

TANIMLAR

Artık Risk: Riskin etkisi ve/veya olasılığının azaltılması amacıyla yürütülen kontrollerden sonra arta kalan risk seviyesidir.

Belirsizlik: Bir olayın, sonucunun veya ihtimalinin anlaşılamama veya bilinememe durumudur.

Birim: İlgili Cumhurbaşkanlığı Kararnamelerinde hizmet birimi olarak sayılanlar ile diğer bağlı ve ilgili idareler ile üniversiteler ve belediyelerde teşkilat kanunlarında birim olarak sayılanlardır.

Birim Yöneticisi: İlgili Cumhurbaşkanlığı Kararnamesinde hizmet birimi olarak sayılanlar ile diğer bağlı ve ilgili idareler ile üniversiteler ve belediyelerde teşkilat kanunlarında sayılan birimlerin en üst yöneticisidir.

Birim Risk Koordinatörü: Birim yöneticisi tarafından belirlenen ve birimin risk yönetimi çalışmalarını koordine etmekle görevli kişidir.

Çalıştay: İdarenin stratejik amaç ve hedeflerine ulaşmasını etkileyebilecek risklerin belirlenmesi, değerlendirilmesi, önceliklendirilmesi, risklere yönelik alınacak kararların belirlenmesi ve ilave risk yönetimi faaliyetlerinin tanımlanması için Çalıştay Kolaylaştırıcısı tarafından yönlendirilen uzmanların bir araya gelerek yaptıkları çalışmadır.

Çalıştay Kolaylaştırıcısı: Çalıştay süresinde, katılımcıları risklerin belirlenmesi, değerlendirilmesi, önceliklendirilmesi, risklere yönelik kararların belirlenmesi ve ilave risk yönetimi faaliyetlerinin tanımlanması aşamalarında yönlendirmekle ve çalıştayı yönetmekle görevli kişidir.

Dış Paydaşlar: İdarenin faaliyetleri ile doğrudan ilişkili olmayan ancak idareden etkilenen ya da idareyi etkileyebilecek güce sahip taraflardır.

Doğal Risk: Riske yönelik herhangi bir kontrol faaliyeti uygulanmadan önceki risk seviyesidir.

Etki: Riskin gerçekleşmesi durumunda idare üzerinde yaratacağı olumlu ya da olumsuz sonuçlardır.

Fırsat: Stratejik amaç ve hedefler üzerinde olumlu etki yaratabilecek olay veya durumlardır.

GZFT Analizi: İdarenin güçlü ve zayıf yönleri ile karşı karşıya olduğu fırsat ve tehditleri tespit etmeye yönelik yapılan analizdir.

İç Denetim: İdarenin çalışmalarına değer katmak ve geliştirmek için kaynakların ekonomiklik, etkililik ve verimlilik esaslarına göre yönetilip yönetilmediğini değerlendirmek ve rehberlik yapmak amacıyla yapılan bağımsız, nesnel güvence sağlama ve danışmanlık faaliyetidir.

İç Kontrol: İdare amaçlarına, belirlenmiş politikalar ile mevzuata uygun olarak faaliyetlerin etkili, ekonomik ve verimli bir şekilde yürütülmesini, varlık ve kaynakların korunmasını, muhasebe kayıtlarının doğru ve tam olarak tutulmasını, malî bilgi ve yönetim bilgisinin zamanında ve güvenilir olarak üretilmesini sağlamak üzere idare tarafından oluşturulan organizasyon, yöntem ve süreçle iç denetimi kapsayan malî ve diğer kontroller bütünüdür.

İç Paydaşlar: Çalışanlar ve yönetim gibi idare içinde çalışan taraflardır.

İdare Risk Koordinatörü: İdarenin risk yönetimi çalışmalarını koordine etmekle görevli ve üst yöneticiye karşı sorumlu olan üst yönetici yardımcısı veya SGB'nin en üst yöneticisidir. İRK, İKİYK'nın doğal üyesidir ve idarenin risk yönetimi süreçlerinin uygulanması konusunda üst yöneticiye karşı sorumludur.

İdare Kültürü: İdare çalışanları tarafından benimsenen ve paylaşılan değerler bütünüdür.

İlave Risk Yönetimi Faaliyeti: Riske yönelik alınacak kararlar kapsamında riskin azaltılmasına karar verilmesi halinde gerçekleştirilecek ilave kontrol faaliyetleridir.

Kök Neden: Riske neden olan etken, riskin ortaya çıkmasındaki temel sebeptir.

Kurumsal Risk Yönetimi: İdareler tarafından, stratejik amaç ve hedeflerini gerçekleştirmelerini etkileyebilecek olay veya durumların bütünsel bakış açısı ile belirlenmesi, ölçülmesi, önceliklendirilmesi sayesinde söz konusu olay veya durumların gerçekleşme ihtimalinin veya gerçekleştiğinde ortaya çıkaracağı zararın azaltılması, varsa ortaya çıkabilecek fırsatların değerlendirilmesi ve risklere yönelik alınacak kararların belirlenmesi, risklerin izlenmesi ve raporlanmasına yönelik uygulanan kapsamlı ve sistematik yaklaşımdır.

Misyon: İdarenin neyi, ne şekilde ve kim için yaptığı, idarenin var oluş sebebidir.

Nicel: Matematiksel ve istatistiki ifadeler kullanılarak, sayılarla, ölçü birimleriyle veya miktar ile belirtilebilen kavramlardır.

Nitel: Sayılamayan ve ölçülemeyen, varlığın daha çok özelliğini belirten kavramlardır.

Olasılık: Bir olay veya durumun belirli bir zaman dilimi içerisinde meydana gelme ihtimalidir.

Öncü Risk Göstergesi: İdarenin stratejik amaç ve hedeflerine ulaşmasını etkileyebilecek risklerin gerçekleşme ihtimallerini işaret eden ve söz konusu risklerin takibinde kullanılan göstergedir.

ÖRG Faaliyeti: Tanımlanan ÖRG'ye yönelik sapma olması durumunda uygulanacak faaliyettir.

ÖRG Hedefi: Kullanılan ÖRG'ye yönelik ulaşılmak istenen seviyedir.

Performans Göstergesi: İdarelerce performans hedeflerinin ölçülebilirliğini miktar ve zaman boyutuyla ifade eden araçlardır.

Performans Programı: Kamu idarelerinin performans esaslı program bütçeye uygun olarak yürütecekleri faaliyetler ile bunların kaynak ihtiyacını, amaç, hedef ve performans göstergelerini içeren programdır.

PESTLE Analizi: İdareye etkisi olabilecek politik, ekonomik, sosyal, teknolojik, çevresel ve yasal dış etkenler belirlenmesine yönelik yapılan analizdir.

Risk: Stratejik amaç ve hedeflere ulaşmayı etkileyebilecek olay veya durumlardır.

Risk Evreni: İdareye odaklanacağı alanları tespit etmesi, olası risk kaynaklarını atlamaması ve riskleri söz konusu ana odak noktaları çerçevesinde takip etmesine yardımcı risk kategorileridir.

Risk Haritası: Risklerin etki ve olasılıkları kapsamında risk seviyelerinin değerlendirilmesini sağlayan gösterim biçimidir.

Risk İştahı: İdarenin amaçları doğrultusunda kabul etmeye hazır olduğu en yüksek risk seviyesidir.

Risk Kapasitesi: İdarenin faaliyetlerini sonlandırmadan alabileceği en yüksek risk seviyesidir.

Risk Kültürü: İdarenin politika, prosedürlerini, iş yapış biçimini, çalışanlar arasındaki ilişkileri, çalışanlarla yönetim arasındaki ilişkiler ile idarenin risk farkındalığını kapsayan riske yönelik yaklaşımıdır.

Risk Strateji Belgesi: Risk yönetimine ilişkin kurumsal yaklaşımın yazılı olarak ortaya konulduğu belgedir.

Riske Yönelik Alınacak Karar: İdarenin stratejik amaç ve hedeflerine ulaşmasını etkileyebilecek riskleri değerlendirme sonrasında riski kabul etmek, riski devretmek, riskten kaçınmak ve riski azaltmak yönünde seçeceği risk yönetimi kararıdır.

Stratejik plan: : : Kamu idarelerinin misyon ve vizyonlarının oluşturulması, stratejik amaç ve ölçülebilir hedeflerin saptanması, önceden belirlenmiş olan göstergeler doğrultusunda performans ölçümü ve bu sürecin izleme ve değerlendirmesinin yapılması amacıyla ilgili idarelerce beş yıllık bir dönem için hazırlanan plandır.

Tehdit: Stratejik amaç ve hedefler üzerinde olumsuz etki yaratabilecek olay veya durumlardır.

Üst Politika Belgeleri: Üst politika belgeleri: Kalkınma planı, Cumhurbaşkanlığı programı, orta vadeli program ve Cumhurbaşkanlığı yıllık programı ile idareyi ilgilendiren ulusal, bölgesel ve sektörel strateji belgeleridir.

Vizyon: İdarenin geleceğini gösteren genel amaçtır.

Yukarıda yer almayan ancak bu rehberle ilgili hususlarda Kamu İç Kontrol Rehberi, Kamu İdareleri İçin Stratejik Planlama Kılavuzu ve Program Bütçe Rehberindeki tanım ve açıklamalar geçerlidir.

KISALTMALAR

AR-GE: Araştırma ve Geliştirme

ARK: Alt Birim Risk Koordinatörü

BRK: Birim Risk Koordinatörü

GZFT: Güçlü ve Zayıf Alanlar ile Fırsatlar ve Tehditler

ISO: International Organization for Standardization

İKİYK: İç Kontrol İzleme ve Yönlendirme Kurulu

İRK: İdare Risk Koordinatörü

ÖRG: Öncü Risk Göstergesi

PESTLE: Politik, Ekonomik, Sosyal, Teknolojik, Yasal ve Çevresel Dış Etkenler

RSB: Risk Strateji Belgesi

SGB: Strateji Geliştirme Birimi

SIGMA: Support for Improvement in Governance and Management - Yönetişim ve Yönetimi Geliştirmek için Destek

TRG: Temel Risk Göstergesi

TABLOLAR

ŞEKİLLER

EKLER