SERİ: 03

REHBER

RİSK YÖNETİMİ SÜRECİ
RİSKLERİN TESPİT EDİLMESİ, RİSKLERİN DEĞERLENDİRİLMESİ, RİSKLERE CEVAP VERİLMESİ, RİSKLERİN GÖZDEN GEÇİRİLMESİ VE RAPORLANMASI

STRATEJİ GELİŞTİME DAİRE BAŞKANLIĞI

İÇ KONTROL BİRİMİ

İÇİNDEKİLER

AMAÇ, KAPSAM, DAYANAK, TANIMLAR VE İLKELER

Amaç

Bu belgenin amacı, Kütahya Dumlupınar Üniversitesinin stratejik amaç ve hedeflerine ulaşabilmek için yürüttüğü mali ve mali olmayan tüm faaliyetlerinin sürdürülmesine etki edecek risklerin tespit edilmesini, değerlendirilmesini, önceliklendirilmesini ve risklere karşı alınacak önlemlerin belirlenerek uygulanmasını sağlayacak kurumsal risk yönetimi stratejisini ve kurumsal risk yönetimi sürecinde etkin rol alacak yönetici ve personelin yetki, görev ve sorumluluklarını belirlemektir.

Kapsam

Bu belge Kütahya Dumlupınar Üniversitesinin kurumsal risk yönetimi sürecini kapsar.

Dayanak

Bu belge 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu, Kamu İç Kontrol Yönetmeliği, Kamu İç Kontrol Standartları Tebliği ile Kamu İç Kontrol Rehberine dayanılarak hazırlanmıştır.

TANIMLAR

Birim Yöneticisi: Akademik birimlerde Fakülte Dekanı, Yüksekokul, Enstitü ve Uygulama ve Araştırma Merkezlerinde Müdürü; idari birimlerde Genel Sekreteri ve İç Denetim Birim Yöneticisini, Daire Başkanlarını, Hukuk Müşavirini, Döner Sermaye İşletme ve İktisadi İşletme Müdürlerini, Genel Sekreterliğe bağlı Müdürlüklerde Müdürleri, Koordinatörlüklerde Koordinatörleri,
İç Kontrol İzleme ve Yönlendirme Kurulu: Rektörlük tarafından uygun görülen Rektör Yardımcısının Başkanlık ettiği, Genel Sekreter, Strateji Geliştirme Daire Başkanı, Hukuk Müşaviri, Personel Daire Başkanı, Bilgi İşlem Daire Başkanı, Kalite Koordinatörü ve Rektörlük tarafından görevlendirilen akademik birimlerin yöneticilerinden oluşan ve sekreterya hizmetlerini Strateji Geliştirme Daire Başkanlığının yaptığı kurul,
İdare Risk Koordinatörü: Rektörlük tarafından görevlendirilen Rektör Yardımcısını veya Strateji Geliştirme Daire Başkanını,
Birim Risk Koordinatörü: Birimlerde Birim Yöneticisi tarafından; birimin görevleri ve iç kontrol uygulamaları
Birim Risk Raporu: Birim düzeyinde Birim Risk Koordinatörü ve Birim Risk Çalışma Grubunun hazırlayacağı birimin hedeflerini etkileyebilecek risklerin tespit edilmesini sağlayan ve risk kayıtlarını içeren raporu,
Konsolide Risk Raporu: Birim Risk Raporlarından yola çıkılarak İdare Risk Koordinatörü tarafından hazırlanan ve İç Kontrol İzleme ve Yönlendirme Kurulu ile Üst Yöneticiye sunulan raporu,
Risk Eylem Planı: Konsolide Risk Raporunda tespit edilen risklerin gerçekleşme düzeyini azaltmayı hedefleyen ve kontrol faaliyetlerinden oluşan planı,
Birim Risk Çalışma Grubu: Risklerin belirlenmesi ve değerlendirmesi çalışmalarını yapmak üzere her bir birim yöneticisi tarafından görevlendirilen en az 3 üç personeli,
Risk: Amaç ve hedeflerin gerçekleşmesini olumsuz etkileyebilecek olay veya durumlar,
Doğal Risk: Amaç ve hedeflere ilişkin tespit edilen risklerin, herhangi bir kontrol önlemi alınmadan önceki seviyesini,
Kalıntı (Artık) Risk: Riskin gerçekleşme düzeyini azaltmayı hedefleyerek uygulanan kontrol faaliyetlerinden sonra arta kalan riskleri,
Risk İştahı: Amaç ve hedefler doğrultusunda Üniversitenin kabul etmeye (tolere etmeye/maruz kalmaya/önlem almamaya) hazır olduğu en yüksek risk düzeyini,
İç Risk: Üniversite tarafından kontrol edilebilecek olaylar sonucunda ortaya çıkan riskleri,
Dış Risk: Üniversitenin kontrolünün dışında gerçekleşen olaylar sonucunda ortaya çıkan riskleri,
Risk Yönetimi Süreci: Risklerin belirlenmesi, risk türlerinin tespit edilmesi, değerlendirilmesi, kontrol faaliyetlerinin belirlenmesi, risklerin izlenmesi ve raporlanması aşamaları kapsayan yönetim sürecini ifade eder.

İLKELER

Üniversitenin risk yönetimine ilişkin ilkeleri şunlardır:

1. Kurumsal risk yönetimi süreci, Üniversitenin İç Kontrol ve Yönetim Sisteminin bir parçasıdır.
2. Riskler operasyonel faaliyet riskleri olarak alt birim düzeyinde, performans programı ve proje riskleri olarak birim düzeyinde ve stratejik riskler olarak Üniversite düzeyinde gerçekleşme ihtimali ve gerçekleşmesi durumunda ortaya çıkacak olumsuz durumlar göz önünde bulundurularak tespit edilir, ölçülür ve analiz edilir.
3. Konsolide Risk Raporlarına göre hazırlanacak olan Risk Eylem Planlarında yer verilen kontrol faaliyetlerinin Kamu İç Kontrol Standartlarına Uyum Eylem Planlarında yer alması sağlanır.
4. Risklerin gerçekleşme ihtimalini veya etki düzeyini azaltmak amacıyla belirlenen kontrol faaliyetleri eylemlerine göre iş akış süreçleri ve prosedürel dokümanlar yeniden tasarlanır ve uygulanır.
5. Risk yönetiminin çıktıları stratejik planlama, performans esaslı bütçeleme gibi Üniversite yönetiminin karar verme aşamalarına entegre edilerek kullanılır.
6. Risk yönetimi süreci Üst Yöneticinin sorumluluğunda, İç Kontrol İzleme ve Yönlendirme Kurulunun gözetiminde, Strateji Geliştirme Daire Başkanlığının sekreteryasında akademik ve idari birim yöneticileri ve her kademedeki çalışanlar ile birlikte uygulanır.
7. Risk yönetimi süreci yılda en az bir defa izlenir, değerlendirilir ve raporlanır.
8. Risk yönetimi süreci, kamu mali yönetiminin mali saydamlık ve hesap verebilirlik ilkeleri doğrultusunda yürütülen mali ve mali olmayan tüm faaliyetlerin kamuoyuna makul güvence vermesi amacıyla tasarlanır ve uygulanır.

RİSK YÖNETİMİ SÜRECİNDE ORGANİZASYONEL YAPI, GÖREV, YETKİ VE SORUMLULUKLAR

Risk Yönetimi Sürecinde Organizasyonel Yapı

Üniversitenin risk yönetimi sürecinde Rektör, İç Kontrol İzleme ve Yönlendirme Kurulu, İdare Risk Koordinatörü, Birim Risk Koordinatörleri, Birim Risk Çalışma Grupları, Çalışanlar, İç Denetim Birimi ve Strateji Geliştirme Daire Başkanlığı yer alır (Ek 1).

Üst Yöneticinin Görev, Yetki ve Sorumlulukları

5018 sayılı Kanun çerçevesinde en üst düzeyde yetkili ve sorumlu olan üst yönetici aynı zamanda risk yönetimi konusunda da Üniversitenin lideri konumundadır. Üniversite Rektörün risk yönetimi sürecinde görevleri şunlardır:

a) Her üç yılda bir Üniversitenin amaç ve hedefleri doğrultusunda risklerin yönetilmesi konusunda stratejinin belirlenmesini sağlar ve bu stratejinin nasıl uygulayacağını gösteren Risk Strateji Belgesini onaylayarak, söz konusu belgeyi tüm çalışanlara yazılı olarak duyurur.
b) Risk Strateji Belgesinde risk yönetimi için gerekli yapıları oluşturarak görev ve sorumlulukları açıkça belirler.
c) Diğer idarelerle ortak yönetilmesi gereken riskler konusunda İdare Risk Koordinatörüne gerekli desteği sağlar.
d) Paydaşlar ve kamuoyuna karşı risklerin yönetilmesinde gerekli hassasiyeti ve katılımcılığı sağlamak konusunda uygun mekanizmalar oluşturulmasını sağlar.
e) İç Kontrol İzleme ve Yönlendirme Kurulu ile İdare Risk Koordinatörü tarafından kendisine sunulan değerlendirme ve öneriler doğrultusunda geleceğe ilişkin stratejik eylemler belirler.
f) Risk yönetimi konusunda İç Kontrol İzleme ve Yönlendirme Kurulundan ve İç Denetim Biriminden güvence alır.
g) Risk yönetimi süreçlerinin tutarlılığının sağlanmasını gözetir.
h) İzleme raporlarını inceler ve risk yönetiminin etkinliğini sağlar.
i) Stratejik risklerin yönetiminde örnek davranışlar sergiler.
j) Risk yönetiminin tüm aşamalarında çalışanları teşvik eder.

İç Kontrol İzleme ve Yönlendirme Kurulunun Görev, Yetki ve Sorumlulukları

Bir üst yönetici yardımcısı veya birim yöneticisi başkanlığında birim yöneticileri veya görevlendirecekleri yardımcılarından oluşan İç Kontrol İzleme ve Yönlendirme Kurulu Üniversitenin risk yönetiminin geliştirilmesine ilişkin politika ve prosedürler oluşturarak üst yöneticinin onayına sunar. Politika ve prosedürleri birimlere bildirir. İç Kontrol İzleme ve Yönlendirme Kurulu İdare Risk Koordinatörü tarafından kendisine sunulan riskler içerisinden stratejik düzeyde önemli gördüğü riskleri gündemine alır. İç Kontrol İzleme ve Yönlendirme Kurulunun sekretarya hizmetleri Strateji Geliştirme Daire Başkanlığı İç Kontrol Birimi tarafından yürütülür. Toplantılara gerek görülmesi halinde idare içerisinden veya dışarısından uzman kişiler davet edilebilir. İç Kontrol İzleme ve Yönlendirme Kurulunun risk yönetimi sürecinde görevleri şunlardır:

a) Üniversitenin Risk Strateji Belgesini hazırlayarak Üst Yöneticinin onayına sunar.
b) Üniversitenin risk yönetimi kültürünün oluşturulmasında politikalar belirler.
c) Risklerin kurumda tutarlı bir şekilde yönetilmesini gözetir.
d) Harcama birimlerine ait risklerden ortak yönetilmesi gerekenleri ve bunlara ilişkin politika ve prosedürleri belirleyerek koordine etmesi açısından İdare Risk Koordinatörüne bildirir.
e) Diğer idarelerle ortak yönetilmesi gereken riskleri belirler ve bunları İdare Risk Koordinatörüne bildirerek ilgili idarelerle ortak yönetilmesi konusunda gerekli önlemlerin alınmasını sağlar.
f) İç Kontrol İzleme ve Yönlendirme Kurulu, Kurul Başkanının çağrısı ile yılda en az iki defa İç Kontrol Sistemi İzleme veya Değerlendirme Raporlarını değerlendirmek; Konsolide Risk Raporu ve Risk Eylem Planında belirtilen riskleri görüşmek, risk yönetimi süreçlerinin etkili işleyip işlemediğini ve risklerde gelinen durumu değerlendirmek ve önerilerde bulunmak; İç Kontrol Sistemi kapsamında hazırlanacak olan doküman ve formların standardizasyonunu sağlamak ve Kamu İç Kontrol Standartlarına Uyum Eylem Planlarını görüşerek Üst Yöneticiye sunmak üzere toplanır.

g) Sayıştay ve iç denetim raporlarından da yararlanarak iyi uygulama örneklerinin tespit edilmesini ve yaygınlaştırılmasını destekler.

İdare Risk Koordinatörünün Görev, Yetki ve Sorumlulukları

Üst yönetici, yardımcılarından birini veya Strateji Geliştirme Daire Başkanını İdare Risk Koordinatörü olarak görevlendirir. İdare Risk Koordinatörü, İç Kontrol İzleme ve Yönlendirme Kurulunun doğal üyesidir ve Üniversitenin risk yönetimi süreçlerinin uygulanması konusunda üst yöneticiye karşı sorumludur. İdare Risk Koordinatörünün risk yönetimi sürecinde görevleri şunlardır:

a) Risk yönetimi çerçevesinde Birim Risk Koordinatörlerini toplantıya çağırır.
b) Her bir Birim Risk Koordinatörü tarafından yılda bir hazırlanan Birim Risk Raporlarından yola çıkarak Konsolide Risk Raporunu Aralık ayı sonuna kadar hazırlar; bu raporu belirlenen dönemlerde İç Kontrol İzleme ve Yönlendirme Kurulu ve üst yöneticiye sunar. Bu raporla birlikte izlenmesi gereken önemli risklerin ve kendi değerlendirmelerinin de yer aldığı ve risklere karşı alınması gereken kontrol faaliyetlerini içeren Risk Eylem Planını hazırlar.
c) Diğer idarelerin İdare Risk Koordinatörleri ile ortak risk alanlarına ilişkin konuların görüşülmesi ve bunların Üniversite içerisinde koordinasyonundan sorumludur.
d) Birimlerin risk yönetimi konusundaki ihtiyaçlarını belirleyerek bunu her toplantı öncesinde İç Kontrol İzleme ve Yönlendirme Kuruluna raporlar.
e) İç Kontrol İzleme ve Yönlendirme Kurulunun görüşleri, önerileri ve kararlarına ilişkin Birim Risk Koordinatörlerine geri bildirim sağlar ve Üniversitenin risk yönetimi süreçlerinin tutarlı olması konusunda gerekli önlemleri alır.

Birim Risk Koordinatörünün Görev, Yetki ve Sorumlukları

Birim Risk Koordinatörü, birim yöneticisi tarafından; birimin görevleri ve iç kontrol uygulamaları konusunda birikim ve deneyimi olan kişiler arasından belirlenir. Ancak teşkilat yapısının küçüklüğü ve personel sayısının yetersizliği gibi nedenlerle Birim Risk Koordinatörünün belirlenmesinde güçlük bulunan birimlerde birim yöneticisinin, Birim Risk Koordinatörü olması mümkündür. Birim Risk Koordinatörünün risk yönetimi sürecinde görevleri şunlardır:

a) Birim Risk Çalışma Grubuna risklerin belirlenmesi ve değerlendirmesi çalışmalarını yapmak üzere birim yöneticisi tarafından en az iki personelin görevlendirilmesini sağlar.
b) Birim Risk Çalışma Grubu toplantılarına Başkanlık eder.
c) Birimin hedeflerini etkileyebilecek risklerin tespit edilmesini koordine eder ve rehberlik sağlar. Tespit edilen riskleri alt birimlerin bilgi ve uzmanlıklarından yararlanarak faaliyetleri ile eşleştirir ve tüm önemli konuların ele alınmasını sağlar.
d) Yıllık olarak belirlenen risk kayıtlarını içeren Birim Risk Raporunu her yıl Haziran ayının sonuna kadar hazırlar ve birim yöneticisinin de onayını alarak İdare Risk Koordinatörüne Konsolide Risk Raporu için raporlar.
e) Çalışanların raporladıkları riskleri birim düzeyinde izler. Mevcut risklerdeki değişiklikleri ve varsa yeni riskleri değerlendirerek birim yöneticisinin uygun görüşünü alarak Birim Risk Raporuyla İdare Risk Koordinatörüne raporlar.
f) Yıllık olarak, daha önce belirlenmiş veya yıl içerisinde ortaya çıkabilecek risklerin iyi yönetilip yönetilmediğine dair kanıtları İdare Risk Koordinatörüne sunar.
g) İdare Risk Koordinatörü ve İç Kontrol İzleme ve Yönlendirme Kurulunun görüşleri, tavsiyeleri ve kararları doğrultusunda Birim Risk Çalışma Grubu üyelerine ve çalışanlara geri bildirim sağlar.
h) Risk yönetimiyle ilgili eğitim ihtiyaçlarını tespit eder.

Birim Risk Çalışma Grubunun Görev, Yetki ve Sorumlulukları

Birim Risk Çalışma Grubu, Birim Risk Koordinatörünün Başkanlığında ve birim yöneticisi tarafından görevlendirilecek en az iki kişi tarafından oluşur. Birim Risk Çalışma Grubunun risk yönetimi sürecinde görevleri şunlardır:

a) Birim düzeyindeki risklerin tespit edilmesi, değerlendirilmesi, cevap verilmesi, gözden geçirilmesi ve raporlanması görevlerinin yerine getirilmesini Birim Risk Koordinatörü ile birlikte yürütür.
b) Risk yönetimi sürecinde çalışanlardan gelen geri bildirimleri birleştirir, risk stratejisine uygun olarak yeni tespit edilen riskleri, risk puanı değişenleri ve bunları azaltmakta kullanılan kontrol faaliyetlerinin etkinliğini raporlar.
c) Birim Risk Koordinatörü ile birlikte Birim Risk Raporunu hazırlayarak Konsolide Risk Raporu için İdare Risk Koordinatörüne gönderir.

Çalışanların Görev, Yetki ve Sorumlulukları

Risk yönetiminin başarısı çalışanların risk yönetimini sahiplenmesine bağlıdır. Her bir çalışan, görev alanı çerçevesinde risklerin yönetilmesinden (risklerin tespit edilmesi, değerlendirilmesi, cevap verilmesi, gözden geçirilmesi ve raporlanması) sorumludur. Risk yönetimi sürecinde çalışanların görevleri şunlardır:

a) Yeni ortaya çıkan ve değişen riskleri tanımlamak, Birim Risk Koordinatörü ve Birim Risk Çalışma Grubuna iletmek ve bunlara cevap vermek yoluyla birimlerinde risk yönetimi süreçlerine doğrudan katkıda bulunur.
b) Görev alanındaki riskleri, iş akış süreçleri, görev tanım formu ve hassas görev tespit formunda belirlenen yetki ve sorumlulukları çerçevesinde yönetir.
c) Görev alanındaki risklerin iyi yönetilip yönetilmediği konusunda Birim Risk Koordinatörü ve Birim Risk Çalışma Grubuna gerekli kanıtları sağlar.

İç Denetim Biriminin Görev, Yetki ve Sorumlulukları

Risk yönetimi sürecinde İç Denetim Biriminin görevleri şunlardır:

a) İç denetim birimi, risk yönetimi sürecinin etkili olup olmadığı, risklerin gereken şekilde yönetilip yönetilmediği hususunda incelemeler yaparak üst yöneticiye mevzuatı çerçevesinde gerekli raporlamaları yapar.
b) Risk yönetimi sürecinin kurulması ve geliştirilmesinde, kolaylaştırıcılık ve eğitim gibi danışmanlık hizmetleri sunar

Strateji Geliştirme Daire Başkanlığının Görev, Yetki ve Sorumlulukları

Risk yönetimi sürecinde Strateji Geliştirme Daire Başkanlığının görevleri şunlardır:

a) İç Kontrol İzleme ve Yönlendirme Kurulunun ve Strateji Geliştirme Daire Başkanının İdare Risk Koordinatörü olmaması durumunda İdare Risk Koordinatörünün sekretarya hizmetlerini yürütür.
b) İç Kontrol Sisteminin kurulması, standartlarının uygulanması ve geliştirilmesi konusunda Üst Yönetici adına çalışmalar yapar. Bu kapsamda iki yılda bir Kamu İç Kontrol Standartlarına Uyum Eylem Planı ve üç yılda bir Risk Strateji Belgesinin ilgili Kurul, Hazırlama Grubu ve Koordinatörle birlikte hazırlanmasını sağlar.
c) Üniversitede risk yönetimine ilişkin çalışmaları koordine eder ve iç kontrol sisteminin değerlendirilmesi kapsamında risk yönetiminin etkinliğini de değerlendirerek yılın ilk 6 (altı) ayından sonra İç Kontrol Sistemi İzleme Raporu, faaliyet yılı bittikten sonra Ocak ayında İç Kontrol Sistemi Değerlendirme Raporu, yılın ilk 6 (altı) ayı içerisinde Birim Risk Raporu ve Aralık ayının sonuna kadar Konsolide Risk Raporu ve Risk Eylem Planını İç Kontrol İzleme ve Yönlendirme Kuruluna raporlar.
d) Risk yönetimi süreçlerinin Üniversitenin tüm birimlerinde etkin işlemesini sağlamak üzere teknik destek ve rehberlik hizmeti verir.
e) Risk yönetimine ilişkin eğitim ihtiyaçlarının belirlenmesi, eğitim faaliyetlerinin yürütülmesi ve koordine edilmesinden sorumludur. İhtiyaç analizine dayalı hizmet içi eğitimleri Personel Daire Başkanlığının Eğitim Birimi ile birlikte yürütür.
f) Risk yönetimine ilişkin Üniversitedeki iyi uygulamaları belirler, bu uygulamaların yaygınlaştırılması için çalışmalar yapar.

RİSK YÖNETİMİ SÜRECİ

Risk Türleri

Riskler iç ve dış riskler adı altında iki ana başlıkta değerlendirilir:

a) **İç Riskler:** Üniversite tarafından doğrudan kontrol altına alınabilecek olaylar sonucunda ortaya çıkan risklerdir.
b) **Dış Riskler:** Üniversitenin kontrolü dışında ortaya çıkan yasal çerçevenin değişmesi, siyasal yönetim mekanizmasında meydana gelen değişiklikler veya olağanüstü durumlar gibi risklerdir.

Risk Hiyerarşisi

Riskler Üniversite (idare) düzeyinde, birim düzeyinde ve alt birim düzeyinde yönetilir (Ek-2).

a) **İdare Düzeyi (Stratejik Düzey) Riskler:** Stratejik Planlama Ekibi tarafından Üniversitenin Stratejik Planının hazırlık safhasında stratejik amaç ve hedeflerin belirlenmesinin ardından bu amaç ve hedeflerin gerçekleştirilmesine olumsuz yönde etki edecek risklerin belirlenmesi bu kapsamdaki risklerdir. Tüm Üniversiteyi kapsayan, stratejik hedeflere ilişkin kararların verildiği ve Üniversitenin üst yönetiminin sorumluluğunda olan alana aittir. Stratejik hedefler orta ve uzun döneme yöneliktir ve üst düzey politika belgeleriyle ilişkilidir. Bu nedenle geleceğe ilişkin kararlar verilirken, karar vericiler çok fazla belirsizliği göz önünde bulundurmak durumundadırlar. Risklerin etkisinin en yüksek olduğu; hükümet politikaları, genel ekonomi, teknolojik gelişmeler gibi dış risklerden en fazla etkilenen alandır. Stratejik düzeyde iyi yönetilmeyen riskler diğer düzeyleri de etkileyeceğinden özel öneme sahiptir. Stratejik düzeyde yönetilmesi gereken risklerin sahibi üst yöneticidir.
b) **Birim Düzeyi (Program/Proje Düzeyi) Riskler:** Üniversite düzeyinde stratejik olarak belirlenen risklerin birim düzeyinde birimin kendi hedeflerine ulaşmasında karşılaştığı risklerdir. Bu düzeyde yer alan riskler, stratejik risklere göre daha kısa dönemde etkilidir. Üniversitenin stratejik hedeflerine ulaşabilmesi açısından birimin kendi fonksiyonlarına yönelik hedeflerini belirlemiş olması ve bu hedeflere ilişkin riskleri yönetmesi gereken alandır. Hem dışarıdan hem de Üniversite içinden kaynaklanan risklerden etkilenir. Alt ve üst düzeyden gelen risklerin bu düzeyde değerlendirilmesi ve aynı stratejik hedef doğrultusunda farklı faaliyetler gösteren birimlerle iyi bir koordinasyon gerektirmesi nedeniyle, kilit öneme sahiptir. Birim düzeyinde yönetilmesi gereken risklerin sahibi birim yöneticisidir.
c) **Alt Birim Düzeyi (Faaliyet Düzeyi) Riskler:** Bu düzeyde yürütülen faaliyetler, sadece birim hedeflerini gerçekleştirmeye yönelik faaliyet düzeyinde yapılan işlerdir. Çalışanların tüm faaliyetleri bu kapsamdadır. Kısa vadeli kararların alındığı, kamu hizmetlerinin üretildiği ve belirsizliklerin en az görüldüğü alandır. Dış risklerden ziyade iç risklerden etkilenir. Risklerin bu düzeyde iyi yönetilmemesi öncelikle birim hedeflerine ve dolayısıyla stratejik hedeflere ulaşılmasını olumsuz yönde etkiler.

Risk Yönetimi Süreci

Risk yönetiminin hedefleri şunlardır:

a) Risk yönetiminin çıktılarını kontrol faaliyeti olarak hassas görev tespit formlarında ve iş akış süreçlerinde yer vererek hata, usulsüzlük, yanlışlık ve yolsuzlukların önüne geçmek,
b) Kamu kaynaklarının kullanımında hesap verebilirliği ve mali saydamlığı artırmak,
c) Kamu kaynaklarının etkin, ekonomik ve verimli kullanılmasını sağlamak,
d) Mali ve mali olamayan tüm karar ve işlemlerin mevzuata uygun yürütülmesini sağlamak,
e) Hesap verme sorumluluğu çerçevesinde kamuoyuna ve kamuoyu adına hesap sormaya yetkili kurumlara karşı makul güvence sağlamak,
f) Kurumsal risk yönetimi modelinin, risk arz eden bir olay meydana gelmeden olayın meydana gelmesini engelleyici önlemler alacak bir yönetim modeli hâline gelmesini sağlamak,
g) Kurumsal risk yönetiminin çalışanlara indirgenmesini sağlayarak olumsuz durumlarla karşılaşma ihtimalini en aza indirmek ve risklere karşı hazırlıklı olmak,
h) Kamu kaynaklarının Üniversitenin stratejik amaç ve hedeflerine ulaşılabilmesi için yıllık bütçenin performans programları ile kullanılmasını sağlayarak; kurumsal risk yönetimi modelinin stratejik yönetimin bir parçası olmasını sağlamaktır.

Kurumsal risk yönetimi Üniversitenin amaç ve hedeflerine ulaşabilmesi açısından makul güvence sağlamaya yönelik yönetsel bir araçtır. Bu kapsamda Üniversitenin Kurumsal Risk Yönetimi çalışmaları stratejik plan ve

performans programı hazırlık çalışmaları ile eşgüdümlü olarak yürütülür. Stratejik Planlama Ekibi stratejik plan hazırlık çalışmalarında stratejik amaçları gerçekleştirmeyi sağlayacak hedefler ile riskler arasında bir denge kurarlar ve Konsolide Risk Raporu ile belirlenmiş olan risk iştahları çerçevesinde hedeflerini belirlerler.
Risk yönetimi döngüsü, stratejik plan hazırlık aşamasında hedeflerin belirlenmesi ile başlayan ve hedeflerin öngörüldüğü şekilde gerçekleştirilip gerçekleştirilmediğinin analiz edilmesini sağlayan izleme ve değerlendirme raporlarıyla sonuçlanan bütün aşamalarda dikkate alınır.
Risk yönetiminin süreci (Ek-3);

a) Risklerin tespit edilmesini
b) Risklerin değerlendirilmesini,
c) Risklere cevap verilmesini,
d) Risklerin gözlenmesini ve raporlanmasını kapsar.

Risklerin Tespit Edilmesi

Risk yönetimi sürecinin ilk aşaması olan risklerin tespit edilmesi, Üniversitenin stratejik amaç ve hedeflerine ve birim düzeyindeki hedeflere ulaşmasını engelleyen veya zorlaştıran risklerin; faaliyet düzeyindeki iş akış süreçlerinde önceden tanımlanmış yöntemlerle belirlenmesi, gruplandırılması ve güncellenmesi sürecidir. (Ek-4)
(2) Üniversitenin risklerinin tespiti sürecinde;

a) Riskleri tespit sürecine, stratejik düzeyden faaliyet düzeyine ya da faaliyet düzeyinden stratejik düzeye doğru bir yaklaşım belirlenebileceği gibi her iki yöntemi birlikte uygulayarak da risk yönetimi süreci uygulanabilir.
b) Genel kural olarak, Üniversiteyi etkileyebilecek stratejik riskler, stratejik plan hazırlama aşamasında tespit edilir. Stratejik Planlama Ekibi, mevcut Konsolide Risk Raporunda belirlenmiş olan risklerden stratejik plan hazırlama sürecinde faydalanır.
c) Faaliyet düzeyinden stratejik düzeye risklerin tespitinde Birim Risk Koordinatörü ile Birim Risk Çalışma Grubunun oylayarak derecelendirdikleri (Ek-8) riskler kaydedilerek tespit edilir (Ek-9). Birim düzeyinde hazırlanan Birim Risk Raporu için yürürlükte bulunan Risk Strateji Belgesinden, yürürlükte bulunan Stratejik Planda tespit edilmiş olan stratejik düzeydeki risklerden, yürürlükte bulunan Kurumsal Risk Yönetimi ve Risk Strateji Belgesinden ve Strateji Geliştirme Daire Başkanlığı tarafından hazırlanmış olan "Birim Risk Raporu Hazırlama Kılavuzu"ndan yararlanılır.
d) Risklerin tespitinde beyin fırtınası (Ek-7), PESTLE ve SWOT (GZFT) Analizi (Ek-4.4) yöntemlerinden faydalanılabilinir.
e) Birim Risk Raporlarıyla kayıt altına alınan riskler İdare Risk Koordinatörü tarafından konsolide edilerek Konsolide Risk Raporu hazırlanır. (Ek-10).

Risklerin Değerlendirilmesi

Risklerin değerlendirilmesi, Üniversitenin hedeflerine ulaşmasını etkileyebilecek faktörlerin analiz edilmesi ve riskin etki ve olasılık açısından öneminin değerlendirilmesidir.
Risk değerlendirme sürecinde;

a) Risklerin değerlendirilmesi risklerin tespitinden sonra risklerin ölçülmesi, önceliklendirilmesi ve kaydedilmesi aşamalarını kapsar (Ek-5).
b) Risk olasılıkları değerlendirilirken Ek-11'deki Risk Değerlendirme Kriterleri Tablosundan faydalanılır.
c) Ölçme, her riskin olma olasılığı ve etkisinin hesaplanmasıdır. Önceliklendirme, risklerin ölçme sonucu aldıkları puanlar doğrultusunda önem derecesine göre sıralanmasıdır.
d) Risklerin kaydedilmesi tespit edilen her bir riskin numaralandırılarak yetkili kişiler tarafından onaylanması ve kayıt altına alınmasıdır.
e) Risklerin ölçülmesi ve önceliklendirilmesinde Risk Oylama Formu (Ek-8) ve kaydedilmesinde Risk Kayıt Formu (Ek-9) kullanılır.

Riskler ölçülürken Etki ve Olasılıklarının çarpımlarının sonucu oluşacak olan Risk Puanı ile ölçülür.
Riskler önceliklendirilirken Etki ve Olasılık puanlarının çarpımı sonucu oluşan Risk Puanlarına göre önceliklendirilir. Ancak risk puanı düşük olsa da stratejik düzeyde dikkate alınması gereken riskler Konsolide Risk Raporunda idarece önceliklendirilebilinir.
İdare Risk Koordinatörünün önerisi, İç Kontrol İzleme ve Yönlendirme Kurulunun uygun görüşü ile Kütahya Dumlupınar Üniversitesinde 1-9 aralığındaki risk puanı düşük risk, 10-39 aralığındaki risk puanı orta risk ve 40-100 aralığındaki risk puanı ise yüksek risk olarak belirlenmiş olup; Kütahya Dumlupınar Üniversitesinin risk iştahı puan aralığı 1-39'dur.

Risklere Cevap Verilmesi

Risklerin kontrol edilebilir bir seviyede (risk iştahı içerisinde) tutulabilmesi için risklere aşağıdaki yöntemlerle cevap verilir. Risklere cevap verme yöntemleri;

a) Kabul etmek,
b) Kontrol etmek,
c) Devretmek,
d) Kaçınmaktır (Ek-6.4).

Risklere cevap verilmeden önce fayda-maliyet analizi yapılır ve maliyeti faydasından fazla olan kontrol yöntemleri uygulanmaz.

Risklerin etki ve olasılıkları risk değerlendirme kriterlerine göre risk oylama formu ve risk kayıt formu ile belirlendikten sonra risk değerlendirmesi ve cevap matrisine göre (Ek-6.1) risk iştahı için belirlenen puan aralıklarına göre değerlendirilir. Buna göre;

a) Düşük risk puanlı riskler (1-9 aralığı) kabul edilir.
b) Orta risk puanlı risklerden (10-39 aralığı) yüksek etkili ve düşük olasılıklı riskler iş sürekliliği planına alınır; yüksek olasılıklı ve düşük etkili riskler kontrol edilir veya kabul edilir.
c) Yüksek etkili ve yüksek olasılıklı riskler kontrol edilir, devredilir, kaçınılır veya kabul edilir.

Doğal riskler risk iştahı sınırlarında ise kabul edilir.

Üniversitenin kontrolünün dışındaki Dış Riskler kabul edilir.

Fayda-maliyet analizi yapıldıktan sonra maliyeti faydasını aşan riskler kabul edilir.

Risk iştahı sınırlarının dışında kalan yüksek riskler ile yüksek olasılıklı ve düşük etkili orta seviyedeki riskler alttaki yöntemlerle kontrol edilir:

a) Yönlendirici kontroller; bilgilendirme, koruma, davranış şekli belirleme gibi dolaylı faaliyetlerle riskleri kontrol etme yöntemidir.
b) Önleyici kontroller; risklerin gerçekleşme olasılığını azaltıp idare tarafından kabul edilebilir seviyede tutmak için yapılması gereken kontrollerdir.
c) Tespit edici kontroller; riskler gerçekleştikten sonra meydana gelen zarar ve hasarın ne olduğunun tespiti amacıyla yapılan kontrollerdir ve risklerin gerçekleşip gerçekleşmediğini anlamak amacıyla yapılır.
d) Düzeltici kontroller; risklerin gerçekleştiği durumlarda, istenmeyen sonuçların etkisinin giderilmesine yönelik kontrollerdir.

Üniversitenin doğrudan aslî görev alanına girmeyen veya fayda-maliyet açısından Üniversite tarafından yapılması uygun görülmeyen ve bu anlamda riskleri yüksek olduğu değerlendirilen faaliyetlerin; uzmanlığı/donanımı/kaynağı olan başka bir idare/kişi/kuruluşa devredilir. Ancak, risk devredilse bile, sorumluluk devredilemez.

Risk yönetilemeyecek kadar büyükse ve/veya faaliyet hayati öneme sahip değilse, faaliyete son verilerek riskten kaçınılabilinir. Ancak, kamu yararının gerektirdiği durumlarda Üniversitenin faaliyetlerini her zaman sonlandırması mümkün olmadığı durumlarda alternatif faaliyetlerle hizmetin gerçekleştirilmesi veya faaliyetin uygun bir döneme ertelenmesi düşünülür.

Risklere verilen cevaplar Risk Kayıt Formuna (Ek-9) kaydedilir ve Birim Risk Raporunda yer verilir. Risklere verilen cevaplara Konsolide Risk Raporuyla birlikte hazırlanan Risk Eylem Planında yer verileceği gibi kontrol faaliyeti olarak Kamu İç Kontrol Standartlarına Uyum Eylem Planında yer verilir.

Artık risk, risklere verilen cevaplardan sonra ortadan kalkmayan risktir. Artık risk seviyesi risk iştahının üzerindeyse risk yönetimi süreci tekrarlanır (Ek-6.3)

Risklerin Gözden Geçirilmesi ve Raporlanması

Riskler zaman içerisinde çeşitli koşulların değişmesi veya alınan önlemler sonucu etki ve olasılık yönünden değişiklikler gösterebileceğinden veya koşulların değişmesi ile yeni risk alanları oluşabileceğinden tespit edilen riskler ve risk yönetimi süreci her yönüyle yılda bir defa gözden geçirilir.

Risklerin gözden geçirilmesi süreci;

a) Stratejik Planlama Ekibi tarafından her beş yılda bir hazırlanan stratejik planın hazırlık safhasında stratejik düzeydeki riskler için gözden geçirme,
b) Birim Risk Koordinatörleri ve Birim Risk Çalışma Grupları tarafından yılda bir defa yılın ilk yarısına kadar hazırlanacak olan Birim Risk Raporu hazırlık safhasında birim düzeyindeki riskler için gözden geçirme,
c) Birim Risk Koordinatörleri, Birim Risk Çalışma Grupları ve Çalışanlar tarafından yürürlükte bulunan Kamu İç Kontrol Standartlarına Uyum Eylem Planları kapsamında iş akış süreçlerini oluştururken veya

güncellerken, hassas görev tanım formlarında riskleri ve risklere karşı alınacak önlemleri tespit ederken veya güncellerken faaliyet düzeyindeki riskler için gözden geçirme,

d) Yılda bir kere yıl sonuna kadar hazırlanması gereken Konsolide Risk Raporu ve Risk Eylem Planı hazırlanırken stratejik, birim-program ve faaliyet düzeyindeki riskler için gözden geçirme suretiyle yapılır.

Risklerin gözden geçirilmesi sonucu Risk Kayıt Formu (Ek-9) güncellenir ve Konsolide Risk Raporunda idare düzeyinde kullanılmak üzere Ek-10'da tespit edilen riskin eski durumu ve yeni durumu karşılaştırma için kayıt altına alınır.

Risklerin raporlanması süreci;

a) Birim Risk Koordinatörleri ve Birim Risk Çalışma Grubunun Birim Risk Raporunu hazırlaması ile başlar. Birim Risk Raporunun hazırlanmasında Üniversitenin Kurumsal Risk Yönetimi ve Risk Strateji Belgesinde belirtilen ilkeler ve Birim Risk Raporu Hazırlama Kılavuzu esas alınır. Yılda bir defa hazırlanan Birim Risk Raporu Haziran ayının sonuna kadar Strateji Geliştirme Daire Başkanlığına gönderilir.

b) İdare Risk Koordinatörü her yıl Aralık ayı sonuna kadar birim risk raporlarından yola çıkarak Konsolide Risk Raporunu, risklere karşı alınacak kontrol faaliyetlerini de öneren Risk Eylem Planı ile hazırlar ve İç Kontrol İzleme ve Yönlendirme Kurulunun uygun görüşüne sunar.

c) Konsolide Risk Raporu ve Risk Eylem Planı İç Kontrol İzleme ve Yönlendirme Kurulunun uygun görüşü ardından Üniversite Üst Yöneticisinin onayına sunulur.

d) Üst Yöneticinin onayının ardından Risk Eylem Planında yer verilen kontrol faaliyetleri, sorumlu birimlere gönderilir.

Sonraki dönem Kamu İç Kontrol Standartlarına Uyum Eylem Planı hazırlık çalışmalarında Kamu İç Kontrol Standartlarına Uyum Eylem Planı Hazırlama Grubu, Risk Eylem Planlarında yer verilen kontrol faaliyetlerine Kontrol Ortamı Standartları eylemlerinde yer verir.

DİĞER HUSUSLAR

Koordinasyon ve Sekreterya

Strateji Geliştirme Daire Başkanlığı İç Kontrol Birimi; Üniversite İç Kontrol Sisteminin kurulmasından, standartlarının uygulanması ve geliştirilmesinden sorumlu olan Üniversite Üst Yöneticisi adına, Kanun ve Strateji Geliştirme Daire Başkanlığının Çalışma Usul ve Esasları Hakkında Yönetmelik hükümleri ve Kamu İç Kontrol Yönetmeliği ile diğer ikincil mevzuat düzenlemeleri çerçevesinde Üniversitenin kurumsal risk yönetiminden ve sekreterya hizmetlerinden sorumludur.
Bu sorumluluk;

a) İç Kontrol İzleme ve Yönlendirme Kurulunun sekreterya hizmetlerini
b) Strateji Geliştirme Daire Başkanının İdare Risk Koordinatörü olarak atanmadığı durumlarda İdare Risk Koordinatörünün sekreterya hizmetlerini kapsamaktadır.

Strateji Geliştirme Daire Başkanlığı İç Kontrol Birimi Üniversitede İç Kontrol Sisteminin kurulması ve kurumsal risk yönetimi kapsamında;

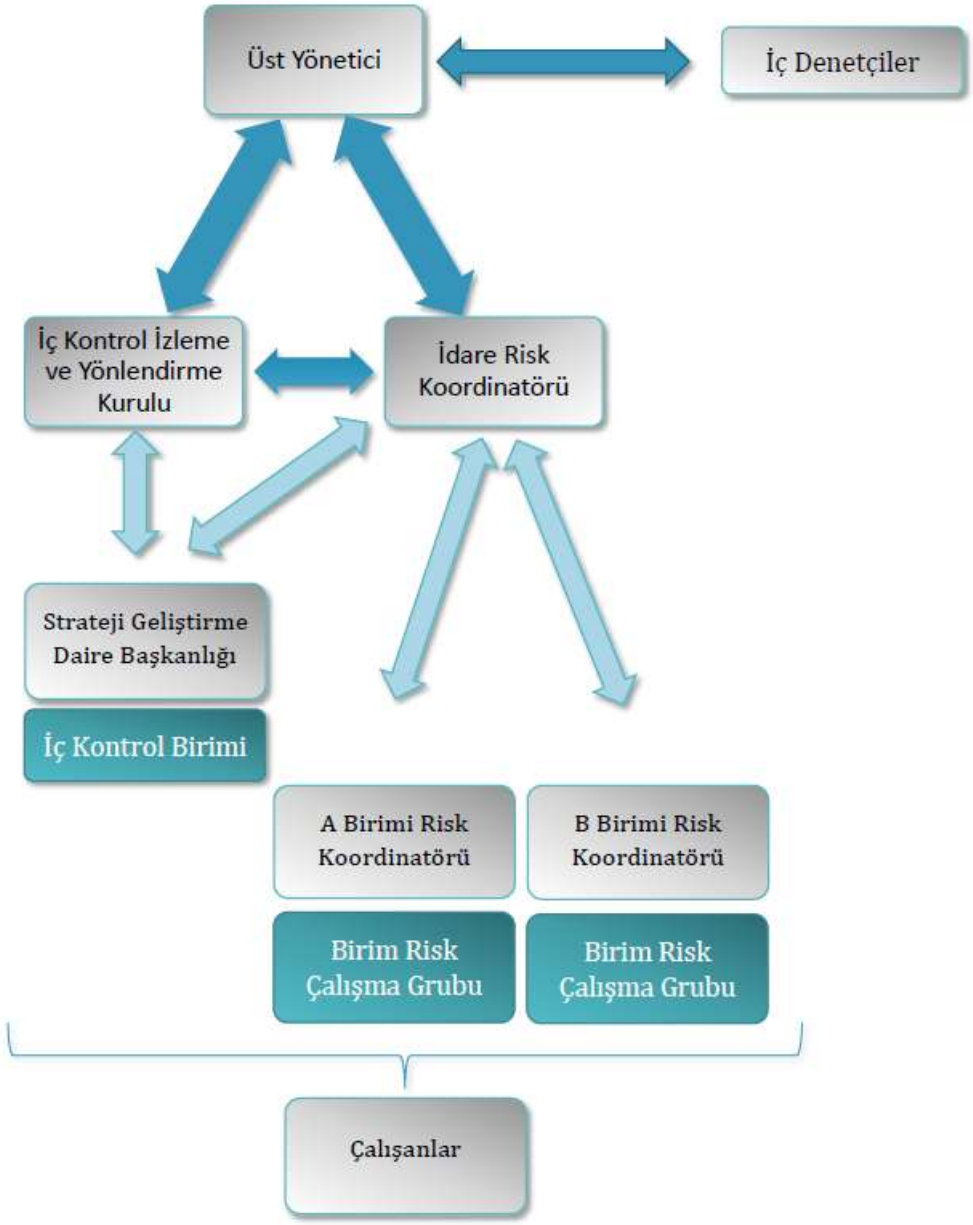
a) Kamu İç Kontrol Standartlarına Uyum Eylem Planlarının iki yılda bir hazırlanmasından,
b) Birim Risk Raporlarının Birim Risk Koordinatörleri ve Birim Risk Çalışma Grupları tarafından her yıl Haziran ayının sonuna kadar hazırlanmasını koordine etmekten,
c) Konsolide Risk Raporu ve Risk Eylem Planının her yıl Aralık ayının sonuna kadar hazırlanmasını koordine etmekten,
d) Konsolide Risk Raporu ve Risk Eylem Planının İç Kontrol İzleme ve Yönlendirme Kurulu ve Üniversite Üst Yöneticisinin uygun görüş ve onayına sunulmasının koordinasyonundan,
e) Risk Eylem Planlarında yer verilen kontrol faaliyetlerinin sorumlu birimlere gönderilmesinden ve sonraki dönem Kamu İç Kontrol Standartlarına Uyum Eylem Planında yer verilmek üzere hazırlama grubuna gönderilmesinden sorumludur.

Düzenleme Bulunmayan Durumlar

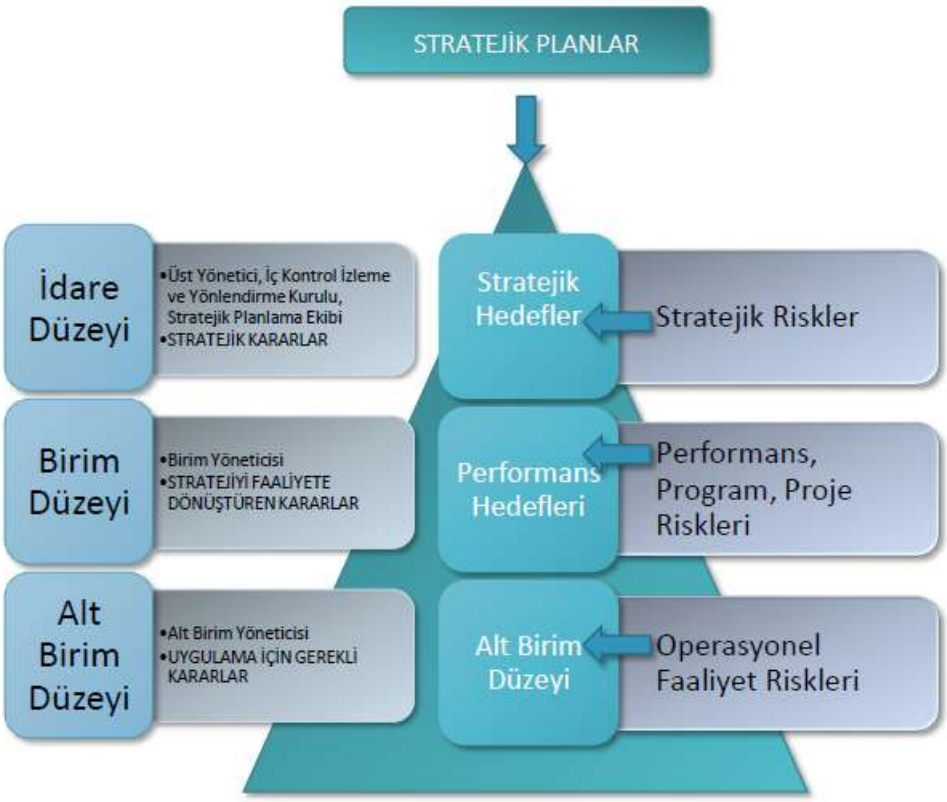
Bu belgede düzenleme bulunmayan durumlarda 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu ve ilgili mevzuatta yer verilen hükümler uygulanır.

Ekler

Ek-1 Risk Yönetimi Sürecinde Organizasyonel Yapı



Ek-2 Risk Hiyerarşisi



Ek-3 Risk Yönetimi Süreci

Ek-4 Risklerin Tespit Edilmesinde İzlenecek Yöntem

Risklerin tespit edilmesinde Ek-4.1, Ek-4.2, Ek-4.3, Ek-4.4, Ek-4.5 ve Ek-4.6'da belirtilen yöntemlerden faydalanılır.

Ek-4.1, risklerin tespit edilmesine başlanırken göz önünde bulundurulması gereken soruları içermektedir

Ek-4.1 Riskleri Tespit Etmeye Başlarken Göz Önünde Bulundurulması Gereken Sorular

- *Ana hedefler nelerdir?*
- *Kilit faaliyetler nelerdir?*
- *Paydaşlar kimlerdir?*
- *Risk Kategorilerimiz nelerdir?*

Riskler tespit edilirken Ek-4.2'deki hususlar göz önünde bulundurulması gerekmektedir.

Ek-4.2 Riskler Tespit Edilirken Göz Önünde Bulundurulması Gereken Hususlar

- İdareler riskleri tespit sürecine, stratejik düzeyden faaliyet düzeyine (top-down) ya da faaliyet düzeyinden stratejik düzeye (bottom-up) doğru bir yaklaşım belirleyebilecekleri gibi her iki yöntemi birlikte uygulayarak da risk yönetimi sürecini başlatabilirler.
- İdareler idare (stratejik), birim (program/proje) ve alt birim (faaliyet /operasyonel) düzeyinde risklerini tespit ederler.
- Genel kural olarak, idareyi etkileyebilecek stratejik riskler, stratejik plan hazırlama aşamasında tespit edilir.
- Stratejik amaç ve hedefler çerçevesinde birim ve alt birimler de yıllık hedeflerini belirleyerek bunlara ilişkin riskleri tespit ederler. Birim ve faaliyet düzeyindeki riskler belirlenirken stratejik riskler göz önünde bulundurulur. Ancak, birim ve faaliyet riskleri tespit edilirken, stratejik düzey ile sınırlı kalmayıp geniş kapsamlı düşünmek önemlidir.
- İdare risklerini tespit ederken hiyerarşik olarak yukarıdan aşağıya ya da aşağıdan yukarıya doğru bir yöntem belirleyebilir. İdarenin tercihine göre bu iki yöntem bir arada da kullanılabilir. Başlangıçta idareye ilişkin tespit edilen tüm risklerin yer aldığı bir risk kataloğu oluşturulabilmesi ve personelin risk yönetimine ilişkin sahipliğinin arttırılabilmesi açısından risklerin aşağıdan yukarıya doğru bir yöntemle (faaliyet düzeyinden stratejik düzeye) belirlenmesi yararlı olacaktır.
- Tespit edilen riskler hedefler ile ilişkilendirilmelidir. Ancak, bazı risklerin doğrudan değil dolaylı olarak hedefleri etkileyebileceğinin göz önünde bulundurulması gerekir. Örneğin kurumsal itibarın zedelenmesi, gerçekleştirilen faaliyet sonucunda doğrudan paydaş olarak belirlenmemiş grupların olumsuz etkilenmesi gibi. Riskler, sistematik yöntemler idarenin ve faaliyetlerin özelliklerine göre farklılıklar gösterebilecektir. Bu süreçte aşağıda yer verilen yöntemlerden birine veya birkaçına başvurulabileceği gibi idarelerin kendi ihtiyaçları doğrultusunda yeni yöntemler geliştirmeleri de mümkündür.
- Tespit edilen risklerin; "x" riski veya "x' in olması" riski şeklinde ifade edilmesi gerekir. Risk Kayıt Formuna da bu şekilde kaydedilmesi uygun olacaktır (Bakınız Ek 9: Risk Kayıt Formu).
- Tespit edilen riskler iç risk mi yoksa dış risk mi olduğu değerlendirilerek gruplandırılmalıdır.
    - İç riskler; doğrudan idare tarafından kontrol edilebilecek olaylar sonucunda ortaya çıkan risklerdir. İç riskler kendi içinde; stratejik riskler, birim riskleri ve faaliyet riskleri olarak üç düzeyde sınıflandırılmalıdır.
    - Dış riskler ise; idarenin kontrolü dışında gerçekleşen olaylar sonucunda ortaya çıkan risklerdir. Dış risklerin konularına göre sınıflandırılarak belirlenmesi yararlı olacaktır. Riskler tespit edildikten sonra bunların sahibi yani kimin sorumluluğunda olduğu belirlenmeli ve Risk Kayıt Formunda bu bilgiye yer verilmelidir.
- Risk yönetimi dinamik bir süreç olduğundan mevcut risklerdeki değişikliklerin yanı sıra yeni ortaya çıkabilecek risklerin de sürekli takip edilmesi gerekmektedir.

Ek-4.3 Risklerin Tespit Edilmesi Süreci

- Riskleri önce stratejik seviyede mi, faaliyet seviyesinde mi, yoksa iki yöntemi birlikte kullanarak mı belirleyeceğinize karar verin.
- Çalışma yöntemlerine karar verin.
- Riskleri iç risk ve dış risk olarak gruplandırın.

- Tehdit ya da fırsatları dikkate alarak riskleri belirleyin ve gruplandırın (ekonomik, sosyal, kültürel, politik, teknolojik, yasal, etik, çevre vb.).
- Paydaş analizi gerçekleştirin (paydaşların pozisyonu ve tutumlarını belirleyin).
- Düzenli olarak ve özellik arz eden dönemlerde (seçimler, ekonomik kriz, doğal afetler vb.) tespiti tekrarlayın.

Ek-4.4 PESTLE ve SWOT (GZFT) Analizi Yöntemi

PESTLE ANALİZİ	
Risklerin, aşağıdaki kategoriler bazında değerlendirmeler yapılarak belirlenmesidir.	
P olitic	Politik
E conomic	Ekonomik
S ocial	Sosyal
T echnologic	Teknolojik
L egal	Yasal
E nvironmental	Çevresel
Örnek:	
Politik	: Ülke yönetiminin önceliklerinin değişmesi riski
Ekonomik	: Enflasyon oranının beklenenin üzerinde gerçekleşmesi riski
Sosyal	: Nüfus artış oranının beklenin çok üzerinde gerçekleşmesi riski
Teknolojik	: Bilgi işlem altyapısının kurulmaması riski
Yasal	: İlgili alandaki düzenlemenin karmaşık olması riski
Çevresel	: Faaliyetin çevre kirliliğine yol açma riski
SWOT/GZFT ANALİZİ (KURULUŞ İÇİ ANALİZ)	
S trengths	G üçlü Yönler
W eakness	Z ayıf Yönler
O pportunities	F ırsatlar
T hreats	T ehditler
Örnek:	
Güçlü Yönler	: Konusunda yetkin personel
Zayıf Yönler	: Eski teknoloji
Fırsatlar	: Ekonomik büyüme
Tehditler	: Ani politika değişikliği

Ek-4.5 Risklerin Tespit Edilmesine İlişkin İpuçları

- Tespit edilen risk kadar, riskle ilgili kanıtların var olup olmadığı göz önünde bulundurulmalıdır. Kilit faaliyetler nelerdir?
- Farklı uzmanlıkların bir arada bulunduğu bir çalışma ekibi yeni riskleri tespit etme olasılığını arttırır.

Ek-4.6 Risk Tespiti Sürecinde Sorulabilecek Sorular

- Hedeflere ulaşma yolunda neler yanlış gidebilir?
- Kritik süreçlerimiz nelerdir?
- Paydaşlarımız kimlerdir ve faaliyetlerimiz üzerindeki etkileri veya faaliyetlerimizin paydaşlar üzerindeki etkileri neler olabilir?
- Risk kategorilerimiz nelerdir?
- Zayıf olduğumuz alanlar nelerdir?
- Hangi varlıklarımız kritik öneme sahiptir?
- Usulsüzlük ve yolsuzluk alanları neler olabilir?
- Faaliyetlerimiz hangi durum ya da olaylar karşısında aksayabilir?
- En kritik bilgi kaynaklarımız nelerdir?
- En fazla harcama yaptığımız alanlar hangileridir?
- Hangi faaliyet ya da süreçler daha karmaşıktır?
- Yasal gereklilikler nelerdir?
- Kaynak kısıtları nelerdir?

Ek-5 Risk Değerlendirilmesinde İzlenecek Yöntem

Risklerin değerlendirilmesi, idarenin hedeflerine ulaşmasını etkileyebilecek faktörlerin analiz edilmesi ve riskin etki ve olasılık açısından öneminin değerlendirilmesidir.

Riskler değerlendirilirken, idarenin karşılaşabileceği potansiyel olaylar ile birlikte idarenin kendine özgü durumu da (örneğin idarenin büyüklüğü, faaliyetlerinin karmaşıklığı, yürüttüğü faaliyetlerde tabi olduğu mevzuat, verilen hizmetlerden yararlananların fazla olması) göz önünde bulundurulmalıdır.

Risklerin değerlendirilmesi, riskler tespit edildikten sonra risklerin ölçülmesi, önceliklendirilmesi ve kaydedilmesi aşamalarını kapsar.

Ölçme, her riskin olma olasılığı ve etkisinin hesaplanmasıdır.

Önceliklendirme, risklerin ölçme sonucunda aldıkları puanlar doğrultusunda önem derecesine göre sıralanmasıdır.

Risklerin kaydedilmesi ise tespit edilen her bir riskin numaralandırılarak yetkili kişiler tarafından onaylanması ve idare tarafından belirlenmiş formlar aracılığıyla kayıt altına alınmasıdır.

Risklerin değerlendirilmesi, tespit edilmiş risklere karşılık verilip verilmeyeceğine ve karşılık verilecekse fayda/maliyet dengesi açısından en uygun olan karşılığın seçilmesine yardımcı olur.

Ek-5.1 risklerin değerlendirilmesine başlarken dikkate alınması gereken bazı soruları içermektedir.

Ek-5.1 Riskleri Değerlendirmeye Başlarken Göz Önünde Bulundurulması Gereken Sorular

- Hedefler nelerdir?
- Mevcut kontroller nelerdir?
- Risk gerçekleşirse hedefler üzerindeki olası sonuçları nelerdir?
- Başka bir idarenin / birimin faaliyeti bizim riskimizi etkiler mi?
- Paydaşlarımız kimlerdir?

Ek-5.2 Risk Değerlendirme Aşamaları

Riskleri değerlendirmenin üç önemli aşaması vardır;

Risk Değerlendirme Aşamaları

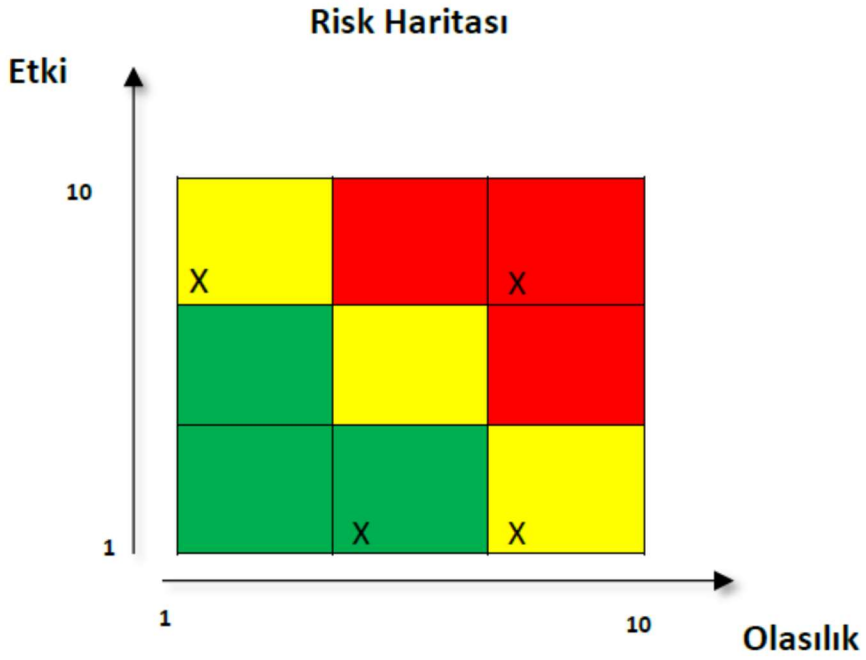
1. Risklerin Ölçülmesi

a) Her risk için etki ve olasılığın ölçülmesi

- Tespit edilen risklerin **olasılık ve etkileri** ölçülür.
- **Olasılık**, bir olayın belirli bir zaman diliminde gerçekleşmesi durumunu ifade eder.
- **Etki** ise bu olayın meydana gelmesi halinde, idarenin hedef ve faaliyetleri üzerinde yaratacağı sonucu ifade eder.
- Risklerin olasılık ve etkileri rakamla gösterilir.
- **Olasılık** için 1 rakamı, bir riskin gerçekleşme olasılığının hemen hemen olmadığı; 10 rakamı riskin gerçekleşmesinin neredeyse kesin olduğu anlamına gelir.
- **Etki** açısından ise 1 rakamı riskin gerçekleşmesinin doğuracağı sonucun çok az önemi olduğu; 10 rakamı bu sonucun çok önemli olduğu anlamına gelir. Risklerin olasılık ve etki açısından 1 ila 10 arasında hangi değeri aldığı belirlenir (Bkz: Ek-11 Risk Değerlendirme Kriterleri Tablosu, Bkz: Ek-8 Risk Oylama Formu).
- İdare, bu aşamada risk iştahını dikkate almalıdır. İdare, belirlenen risk stratejisine göre hangi puanlar arasındaki risklerin düşük, hangilerinin orta, hangilerinin de yüksek olacağını belirlemeli ve bu çerçevede idarenin risk haritasını oluşturmalıdır. (Bkz. Örnek Risk Haritası).
- Kütahya Dumlupınar Üniversitesinde İdare Risk Koordinatörü ile İç Kontrol İzleme ve Yönlendirme Kurulunun uygun görüşü ile Kurumsal Risk Yönetimi ve Risk Strateji Belgesi ile risk iştahı puanı 1-39 puan aralığı olarak belirlenmiş olup, 1-9 puan aralığı düşük risk puanı, 10-39 puan aralığı orta risk puanı, 40-100 puan aralığı ise yüksek risk puanı olarak belirlenmiştir.
- Riskler değerlendirilirken üçlü bir kategori kullanılır. Düşük risk seviyesi (yeşil ile gösterilir), orta risk seviyesi (sarı ile gösterilir) ve yüksek risk seviyesi (kırmızı ile gösterilir).

- Risklerin renk kodları ile gösterilmesi riskin önem derecesinin kolayca görülmesine yardımcı olur.
- Riskin seviyesini daha rahat görmek için "risk haritaları" kullanılır. Riskler için verilen değerlerin risk haritasında basit gösterimi alttaki gibidir.

Risk Haritası Örneği:



b) Risklerin, doğal risk ve kalıntı risk esas alınarak değerlendirilmesi:

- **Doğal risk** bir idarenin, hedeflerine ilişkin olarak tespit ettiği risklerin, herhangi bir cevap verilmeden önceki seviyesini ifade eder.
- **Kalıntı risk**, yönetimin riskin olma olasılığını ve etkisini azaltmak için aldığı önlemlerden sonra arta kalan riskleri ifade eder. Yönetim, riski yönetmek adına verdiği cevaplar sonrasında arta kalan riskin seviyesini tespit etmelidir. Kalıntı riskin seviyesi kabul edilebilir risk seviyesinden yüksek çıkarsa riske verilen cevap yöntemlerinin etkinliğinin ve yeterliliğinin sorgulanması, gerekirse risklere verilecek cevapların tekrar gözden geçirilmesi gerekir.

Doğal ve Kalıntı Risk İçin Hazine ve Maliye Bakanlığından Bir Örnek:

Stratejik Amaç 1.

Sürdürülebilir Maliye Politikalarının Bütüncül Bir Yaklaşımla Belirlenmesine Öncülük Etmek ve Kaynakları 3E Temelli Yönetmek. Stratejik Hedef 3. Mali disiplini ve sürdürülebilir büyümeyi gözeterek kaynak tahsis ve kullanım süreçlerini etkinleştirmek. Performans Hedefi: Kamu idarelerinin mali yönetim ve kontrol araçlarını geliştirmek ve kamu mali yönetiminde izleme ve değerlendirme sisteminin etkinliğini artırmak. Faaliyet: Kamu idarelerinin strateji geliştirme birimlerinin idari kapasitesinin güçlendirilmesi amacıyla Mali Hizmetler Uzman Yardımcısı sınavı yapmak.

Sınavın Süreçleri:

- Taleplerin toplanması
- Sınav hazırlıkları (ÖSYM ile protokol, ilan metni, web altyapısı vb.)
- Yazılı ve sözlü sınavların yapılması ile yerleştirme işlemleri

Bilgileri yukarıda verilen örnek olaya ilişkin doğal ve kalıntı risk çalışması aşağıdaki şekilde olacaktır:

Süreç: Taleplerin toplanması

Doğal Risk: Talep toplama yazısının idarelere ulaşmaması, idarelerin taleplerinin Hazine ve Maliye Bakanlığına ulaşmaması, kadro olmaksızın talepte bulunulması,

Riske Verilen Cevaplar:

1. Talep toplama yazısının faksla da gönderilmesi, ayrıca web sayfasında yayımlanması,

2. İdarelerin talep yazılarının aynı zamanda faksla gönderilmesinin istenmesi,

3. Merkezi yönetim kapsamındaki kamu idarelerinin taleplerinin kadro cetvelleri ile uyumunun Hazine ve Maliye Bakanlığının ilgili birim kayıtları ile karşılaştırılması (Mahalli İdarelere ait kadro bilgileri Maliye Bakanlığında bulunmamaktadır). Kalıntı Risk: Boş mali hizmetler uzman yardımcısı kadrosu bulunmadığı halde talepte bulunan mahalli idarelerin kadrolarına da sınav ilanında yer verilmesi.

2. Risklerin Önceliklendirilmesi

- Risk puanı belirlendikten sonra risklerin, önem derecesine göre en yüksek puandan başlamak üzere sıralanmasıdır. Ancak, hedefleri doğrudan etkileyebilecek riskleri (kilit riskler) yönetim, puanı düşük olmakla birlikte etkileri açısından öncelikleri arasına alabilir.
- Risklerin önem sırasına göre önceliklendirilmesi kaynak tahsisinde etkinliği sağlar.
- Riskler öncelik sırasına göre belirlendikten sonra risklere verilecek cevaplara karar verilir.

3. Risklerin Kaydedilmesi

- Risklerin kaydedilmesi, verilen kararlar için kanıt oluşturulmasına, kişilerin risk yönetimi içindeki sorumluluklarını görmelerine ve izlenmesine yardımcı olur.
- Risk kayıtları iki aşamadan oluşur: Risklerin tespit edilip kaydedilmesinde kullanılan Risk Kayıt Formu (Bkz. Ek-9) ve risklerin yukarı kademelerdeki yöneticilere raporlanmasında kullanılan Konsolide Risk Raporları (Bkz. Ek-10).

Ek-5.3 Risk Değerlendirme İçin İpuçları

- Tespit edilen risklerin belli bir zaman dilimi için olasılık ve etkilerini ölçün.
- Riskin etki puanını belirlerken, ulaşılmasını zorlaştıracağı/engelleyeceği öngörülen hedef üzerindeki etkisini değerlendirin.
- Bir işin riskini en iyi o işi yapan kişinin değerlendireceğini göz önünde bulundurun.
- Başka idarelerin/birimlerin faaliyetlerinin risklerinizi etkileyebileceğini ve risklerin birbirinden bağımsız olmadığını dikkate alın.
- Tüm riskleri birlikte görebilmek için risk haritaları vb. tablolardan yararlanın.
- Riskleri risk puanlarına (Etki x Olasılık) göre veya önem derecelerine göre önceliklendirin.

Ek-5.4 Risk Değerlendirme Örneği

ÖRNEK

Uzmanlık konunuzla ilgili bir eğitim vermeniz gerekli.

Hedefiniz: Anlatacağınız konunun dinleyiciler tarafından anlaşılması

Risklerinizi tespit ettiniz:

Risk 1: Eğitime geç kalmak (bundan dolayı anlatılması gerekenler için yeterli zamanın kalmaması)

Risk 2: İçeriğin doğru belirlenememesi (eğitim verilecek grubu tanımamak)

Risk 3: Sunumun yer aldığı taşınabilir belleği unutmak (görsel etkinin ve algının azalması)

Risk 1, 2 ve 3'ün meydana gelme olasılıklarına ve gerçekleşirlerse bunun hedefinizi nasıl etkileyeceğine bakalım:

RİSK 1:

Etki: Geç kalabilirsiniz ama konuyu çok iyi biliyorsunuz. Kısa sürede anlatsanız da dinleyiciler için anlaşılır olur. Geç kalmanın hedefiniz üzerinde etkisi: 3

Olasılık: O saatte trafik fazla olur. Aynı zamanda, o gün başka işleriniz de var. Gerçekleşme ihtimali:7

Risk Puanı: 3x7 = 21

RİSK 2:

Etki: Konuyu işi bilen uzmanlara anlatacaksanız ayrıntılı, hiç bilmeyen birilerine anlatacaksanız genel hatlarıyla anlatmanız gerekir. Kişilere yanlış yaklaşımla sunum yapmanızın hedefiniz üzerindeki etkisi: 9

Olasılık: Görevlendirme yazısında konu belli, ancak kimlere anlatacağınız yazılmamış. Gerçekleşme ihtimali: 5

Risk Puanı: 9x5 = 45

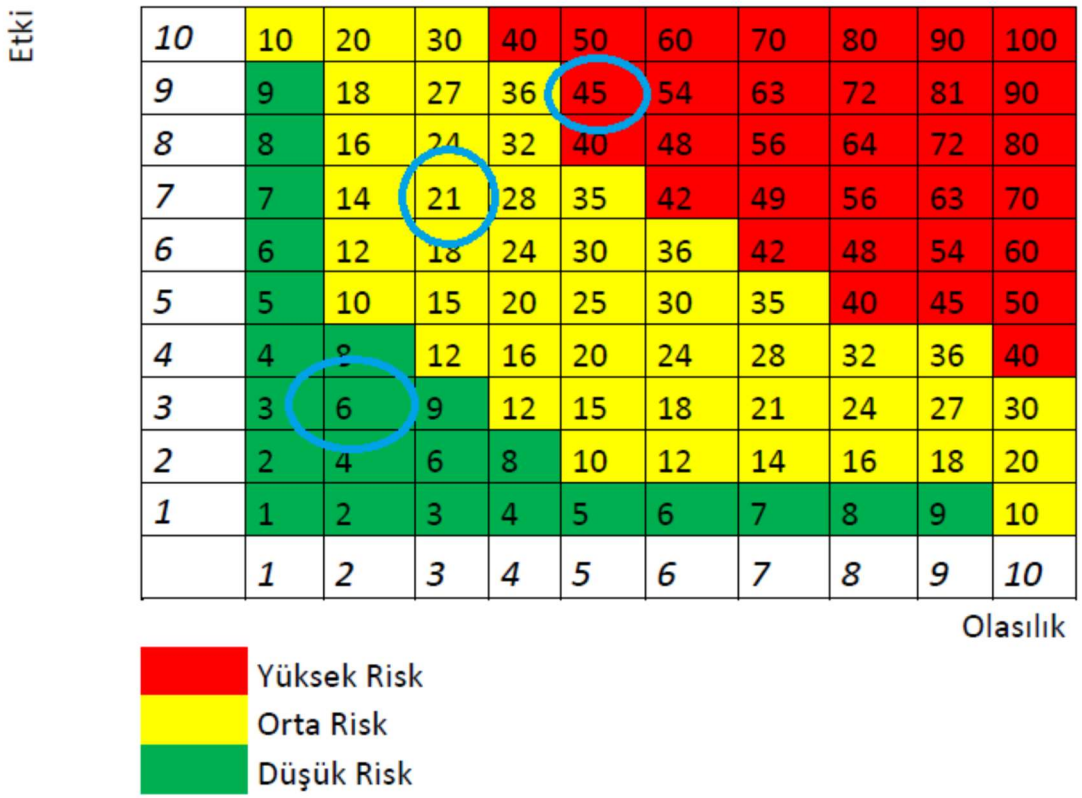
RİSK 3:

Etki: Sunumu yansıtmasanız da konuyu çok iyi biliyorsunuz. Dinleyiciler için etkili biçimde anlatabilirsiniz. Sunum olmamasının hedefiniz üzerinde etkisi: 3

Olasılık: Bilgisayarınızı yanınızdan genelde ayırmazsınız. Çalışmalarınızı taşınabilir bellek ile çantanıza atma gibi bir alışkanlığınız da var. Gerçekleşme ihtimali: 2

Risk Puanı: 3x2 = 6

Risk Haritasında Gösterimi:



Önceliklendirilmesi:

1. **Risk 2 (Risk Puanı: 45)**
2. **Risk 1 (Risk Puanı: 21)**
3. **Risk 3 (Risk Puanı: 6)**

Risklerin her zaman puanlara göre değerlendirilemeyeceğini de söylemek gerekir. Bazı stratejik riskler çok düşük puana sahip olsa bile göz önünde bulundurulmalıdır. Acil eylem planları bulunmalıdır. Olacaklar her zaman öngörülemez. Planlar esnek olmalı, beklenmeyen gerçekleştiğinde başa çıkılabilmelidir.

Ek-6 Risklere Cevap Verilmesinde İzlenecek Yöntem

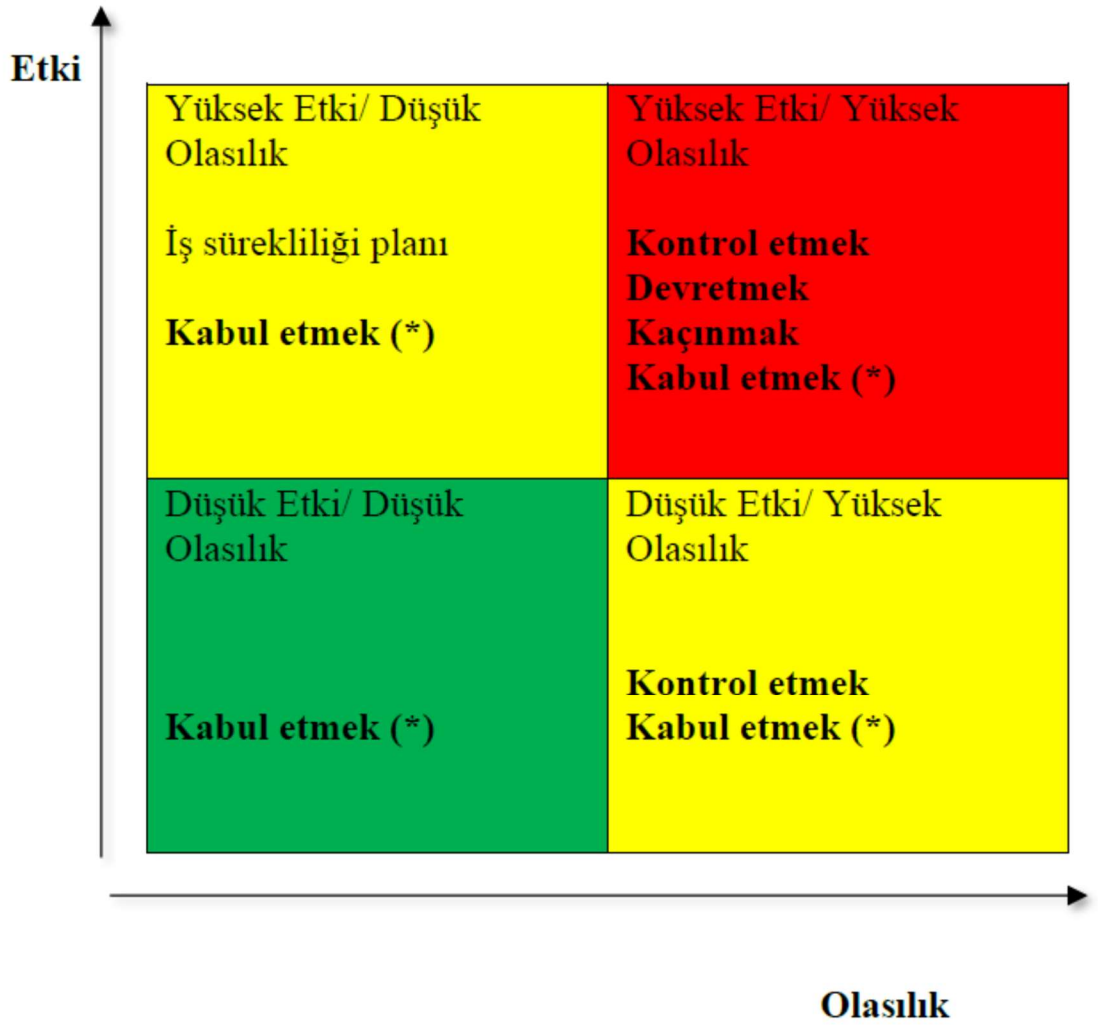
Risklere cevap verilmesi, idareler tarafından tespit edilen ve risk iştahları çerçevesinde değerlendirilen risklere verilecek yanıtın ne olacağının belirlenmesi ve bu bağlamda beklenen tehditlerin azaltılması ve/veya ortaya çıkacak fırsatların değerlendirilmesidir.

Risklere cevap verme yöntemini belirlemeden önce mutlaka fayda-maliyet analizini yapmak gerekir.

Risklere cevap vermenin amacı, riskin olasılığını ve/veya etkisini azaltarak öngörülen hedefe en etkin bir şekilde ulaşmaktır.

Ek-6.1, risklerin etki ve olasılıkları değerlendirildikten sonra verilecek cevaplar hakkında bilgi vermektedir.

Ek-6.1 Risk Değerlendirmesi ve Cevap Matrisi



*** "Kabul Etmek" Seçeneği İçin Ek-6.4 Riske Cevap Yöntemlerine Bakınız.**

Ek-6.2 Risklere Cevap Verme Aşamasında Göz Önünde Bulundurulması Gereken Sorular

- Riski kabul edersem ne olur?
- Hangi risklerin kontrol edilmesi gerekir?
- Faaliyeti maliyet-etkinlik analizi çerçevesinde daha iyi yapabilecek bir idare/işletme/kuruluş var mı?
- Riskten kaçınmak adına faaliyeti başka bir döneme ertelemek veya alternatif bir faaliyetle ikame etmenin hedeflerim üzerindeki etkisi nedir?
- Fırsatın büyüklüğü riski almaya değer mi?

Ek-6.3'te risk iştahı çerçevesinde; doğal riskin, riske verilen cevap sonucunda nasıl kalıntı riske dönüştüğünü gösterilmektedir.

Ek-6.3'te yer alan Risk İştahı tablosunda;
1 ve 5. sütunlarda riske verilen cevap ile doğal risk azaltılmış ve böylece, kalıntı risk, risk iştahı ile aynı düzeye indirilmiştir. İdarenin risk iştahı ile kalıntı riskin kesiştiği bu noktalar risk yönetimi açısından ideal durumlardır.
2, 3 ve 4. sütunlarda; riske verilen cevap riski azaltmıştır. Ancak, kalıntı risk hala risk iştahından (kabul edilebilir düzeyden) daha yüksektir. Bu durum, riske verilen cevabın etkinliğinin ve yeterliliğinin sorgulanması ve daha uygun cevabın verilmesi gerektiği anlamına gelmektedir. 6. sütunda; doğal risk, risk iştahına eşit olduğu için risk kabul edilir. Ancak bu riskleri, değişiklik ihtimali olması nedeniyle diğer riskler gibi izlemek gerekir.
7. sütunda; riske verilen cevap kalıntı riski, risk iştahının altına indirmiştir. Bu durum, uygun cevabın verilmediğini, dolayısıyla kaynakların etkin kullanılmadığını göstermektedir. Bu durumda, kalıntı riski risk iştahına eşitleyecek uygun cevabı belirlemek gereklidir.

Riske cevap vermede temel olarak 4 yöntem kullanılmakta olup söz konusu yöntemler altta Ek-6.4'te sunulmuştur.

Ek-6.4 Risklere Cevap Verme Yöntemleri

Risklere Cevap Verme Yöntemleri

Kabul Etmek: İdarelerin üstlenmeyi daha uygun gördükleri bir cevap yöntemidir. Aşağıdaki durumlarda riskler kabul edilebilir;

• Doğal risk, risk iştahı içinde ise kabul edilir.

• Alınacak önlemlerden (kontrol etmek, devretmek veya kaçınmak) sağlanacak faydanın, alınacak önlemlerin maliyetinden daha düşük olduğunun anlaşılması durumunda kabul edilir. Risklere

• Bazı riskler yönetimin kontrolü dışındadır. Bazı riskler ise faaliyet sonlandırılmadıkça ortadan kalkmaz ki faaliyeti sonlandırmak her zaman mümkün değildir ya da istenmez. Bu durumlarda da risk kabul edilir. Kontrol Etmek: Risklerin kabul edilebilir bir seviyede tutulması için kontrol faaliyetleri aracılığıyla riske cevap verme yöntemidir. Bu yöntem aşağıda yer alan kontrol yöntemleri vasıtasıyla uygulanır.

• Yönlendirici Kontroller

• Önleyici Kontroller

• Tespit Edici Kontroller

• Düzeltici Kontroller

(Kontrol Faaliyetleri hakkında ayrıntılı bilgi edinmek için Kamu İç Kontrol Standartlarına Uyum Eylem Planının (2022-2023) kontrol faaliyetleri standartları mevcut durum analizi bölümüne bakınız.)

Devretmek: Daha çok idarenin doğrudan asli görev alanına girmeyen veya fayda-maliyet açısından idare tarafından yapılması uygun görülmeyen ve bu anlamda riskleri yüksek olduğu değerlendirilen faaliyetlerin, uzmanlığı/donanımı/kaynağı olan başka bir idare/kişi/kuruluşa devredilmesi şeklinde riske cevap verilmesidir. Ancak, risk devredilse bile, sorumluluğun devredilemeyeceği unutulmamalıdır. Çünkü risk gerçekleştiği takdirde bundan zarar görecek olan idarenin kendisidir. Bu bağlamda riskin devredilmesi riskin paylaşılması şeklinde de değerlendirilmelidir. Riskin devredilmesine ilişkin örnekler:

• Faaliyetin bir kısmını veya tamamını uzmanlığı olan başka bir idareye devretmek.

• İhale yöntemi ile faaliyetin yapılmasını üçüncü şahıslara devretmek.

• Sigorta yöntemi kullanarak riski devretmek (uygun olduğunda).

Kaçınmak: Risk yönetilemeyecek kadar büyükse ve/veya faaliyet hayati öneme sahip değilse, faaliyete son vermek mümkündür. Örneğin, çok fazla hava kirliliği ortaya çıkarması beklenen bir fabrikanın kurulmasından vazgeçilmesi gibi. Ancak, kamu yararının gerektirdiği durumlarda idarenin faaliyetleri her zaman sonlandırması mümkün olmayabilir. Böyle durumlarda da alternatif faaliyetlerle hizmetin gerçekleştirilmesi veya faaliyetin uygun bir döneme ertelenmesi düşünülmelidir.

Ek-6.5'te risklere cevap verme süreci özetlenmektedir.

Ek-6.5 Risklere Nasıl Cevap Verilir?

Risklere Nasıl Cevap Veririm?

• Riskleri Risk Değerlendirme aşamasından sonra Risk Oylama Formunda sırala.

• Riskin içeriğine göre cevabını belirle;

- ➢ Kabul Et
- ➢ Kontrol et
- ➢ Devret
- ➢ Kaçın

• Verilecek cevabın faydasının, getireceği maliyetten yüksek olmasına dikkat et.

Ek-6.6 Fırsatların Değerlendirilmesi

Riskler yönetilirken risklerin ortaya çıkardığı fırsatların da göz önünde bulundurulması gerekir. Risklerin meydana getirdiği bazı olumsuz etkiler yanında, zaman zaman fırsatlar da çıkmaktadır. İdarelerin hedeflerine ulaşmasında ilave katkı getirecek bu fırsatlardan yararlanabilmek için idarenin önceden belirlenmiş stratejilerinin olması gerekir. Fırsatları değerlendirmek risklere verilecek cevaplama yöntemlerinin bir alternatifi olmayıp onlarla birlikte kullanılabilecek bir yöntemdir. Ancak, fırsatlardan yararlanmayı risk yönetimi çerçevesinde değerlendirip kabul edilebilir risk seviyesinin belirlenmesinde fırsat ile fayda-maliyet analizinin birlikte düşünülmesi gerekmektedir. Fırsatın önemli görüldüğü yerlerde bir miktar daha fazla risk almak ve/veya makul bir ilave maliyete katlanmak yönetimsel bir tercih olarak düşünülebilir.

Aşağıda Belirtilen Durumlarda Fırsatlar Kullanılabilir:

• Tehditlerin azalmasının ve olumlu fırsatlardan yararlanmanın birlikte gerçekleştiği durumlarda. Bir hastalığa çare bulmak için sağlık ve bilim araştırmaları yapmak gibi (Bir yandan hastalık tehdidi azalacak; diğer yandan insanların daha az hastaneye gitmesi ile daha az maliyet fırsatı olacak).

• Olumsuz durum meydana gelmeden fırsatların ortaya çıktığı durumlarda. Daha etkili çalışabilmek için yeni teknoloji kullanmak, e-devlet ile daha fazla vatandaşa ulaşmak gibi.

Risklere cevap verme sürecine ilişkin bazı ipuçları Ek-6.7'de sunulmuştur.

Ek-6.7 Riske Cevap Verme Sürecine İlişkin İpuçları

Riske Cevap Verme Sürecine İlişkin İpuçları:

• Risklerin önceliklendirilmesi, hangi riske önce cevap verileceğine karar vermekte yardımcı olur.

• Kamu idaresi olarak risklere verilecek cevaplar belirlenirken, hizmet verilenler (veya dolaylı etkilenenler) ve onlar üzerindeki etkiler de göz önünde bulundurulmalıdır.

• Risklere cevap verirken aşırı kontrol önlemlerinden kaçınmak gerekir. Kontrol eksikliği kadar kontrollerin gereğinden fazla olması da idarenin etkinliğine zarar verir.

• Risklere verilecek cevaplarda, diğer idarelerle koordineli hareket edilmesinin daha etkin olabileceği göz önünde bulundurulmalıdır.

Ek-6.8 Örnek Riske Cevap Verme Yöntemleri Riske Cevap Verme Yöntemleri- Örnek İdareniz yeni bir Bilişim Teknolojileri (BT) sistemi almaya karar verdi. Risklerinizi tanımlıyorsunuz:

Risk 1: Yeni sistemin yanıt süresinin yetersiz olması

Risk 2: Eski BT sisteminden yeni sisteme verilerin doğru bir şekilde aktarılmaması

Risk 3: Yeni BT sistemini işletecek yetkinliğin olmaması

Risk 4: Yeni BT sisteminin çalışmaması.

Bu risklere ne tür cevaplar verebilirsiniz?

Risk 1:

Kabul et: Size yeni BT sisteminin 5 saniyelik bir yanıt hızı olduğu söylendi. Bu süre, mevcut sisteminkine benzer bir süre olduğundan daha hızlı olmasına ihtiyacınız olmadığına karar verebilirsiniz.

Risk 2:

Kontrol et: Verinin doğru bir şekilde aktarılmasını sağlamak için kontrol faaliyeti belirlemeniz gerekiyor. Yönlendirici kontroller: Yeni sistemi geliştirme üzerine çalışan BT personelinin yeterli nitelik ve deneyime sahip olmasını sağlarsınız. Önleyici kontroller: Aktarım sırasında verinin bozulmadığından emin olmak için sistemi kabul etmeden önce yeni BT sistemi üzerinde test yaparsınız. Tespit edici kontroller: Yeni sistemi işletmeye başladıktan bir ay sonra, eski sistemden yeni sisteme aktarılan sürekli verilerin doğru olup olmadığını anlamak için test yaparsınız. Düzeltici kontroller: Eski sistemden aktarılan veri ile yeni sistemdeki verinin karşılaştırılması sonucu hatalı veri aktarımı olduğu tespit edilmişse programda gerekli değişikliği yaparsınız/yaptırırsınız. İş sürekliliği planı: Yeni sistemin verileri gerektiği şekilde aktarmaması durumunda eski sistemi tekrar kullanabileceğinizden emin olmalısınız.

Risk 3:

Devret: Yeni sisteminin işletilmesinin sorumluluğunu makul bir süre hizmeti satın aldığınız yere devredersiniz.

Risk 4:

Kaçın: Eğer yeni BT sisteminin test aşamasında çalışmadığı anlaşılırsa, bu sistemi almaktan vazgeçersiniz. Alternatif bir BT sistemi araştırırsınız. Fırsatları değerlendir: Yeni BT sisteminiz daha etkin çalışmanızı sağlıyor ve başka işlerle ilgilenmek üzere personelinize daha fazla zaman bırakıyor.

Ek-6.9 Risklerin Gözden Geçirilmesinde Yöntem

Riskler zaman içerisinde çeşitli koşulların değişmesi veya alınan önlemler sonucu etki ve olasılık yönünden değişiklik gösterebilir. Ayrıca, koşulların değişmesi ile yeni risk alanlarının oluşması da muhtemeldir. Bu nedenle, tespit edilen riskler ve risk yönetimi sürecinin her yönüyle, belirli aralıklarla gözden geçirilmesi gerekir. Gözden geçirmeler yılda en az bir kez olmak üzere, risklerin önem derecesine göre idare tarafından belirlenen sıklıkta olabilir.

Olağanüstü gelişmelerin olması ve bu durumun önceden belirlenmiş riskler üzerinde ciddi etkisinin bulunması halinde İdare Risk Koordinatörü üst yöneticinin sözlü veya yazılı talimatı ile İç Kontrol İzleme ve Yönlendirme Kurulunun riskleri değerlendirmek üzere derhal toplanmasını koordine eder. Olağanüstü gelişmelere doğal afetler, ekonomik krizler, erken seçim kararı alınması gibi örnekler gösterilebilir.

Risklerin ve risk yönetimi sürecinin gözden geçirilmesi birbirinden farklı süreçlerdir; birinin yapılması diğerinin de yapıldığı anlamına gelmez. Riskler her bir riskin sahibi tarafından gözden geçirilmesine karşın risk yönetimi süreci üst yönetici (idarede bulunması halinde üst yönetici adına iç denetim birimi tarafından) ve/veya İdare Risk Koordinatörü tarafından gözden geçirilir. Risklerin ve risk yönetimi sürecinin düzenli gözden geçirilmesi, değişen şartlara uyum sağlamada idareye esneklik kazandıracaktır.

Risklerin gözden geçirilmesi aşağıdaki şekilde yapılır;

• Risklerin hala var olup olmadığı, yeni risklerin ortaya çıkıp çıkmadığı, risklerin gerçekleşme olasılıklarında veya etkilerinde bir değişiklik olup olmadığı gözden geçirilir.

• Gözden geçirmede öncelik, risk puanı yüksek olana veya yönetim tarafından önceliklendirilmiş kilit risklere verilmelidir. Ancak esas olan bütün risklerin gözden geçirilmesidir.

• Stratejik risklerin gözden geçirilmesinde; öncelikle varsa değişmiş olan politika belgeleri, diğer ülkelerdeki gelişmeler, kamuoyunun o dönem için beklentileri, iç denetim raporları, teftiş ve denetim (veya rehberlik) birimlerinin raporları, dış denetim raporları ve ilgili diğer rapor ve belgeler dikkate alınmalıdır

• Gelişmeler ışığında, risk profilinde bir değişiklik meydana gelmişse, idarenin/birimin/alt birimin risk kaydı gözden geçirilmelidir.

• Değişiklik bilgisi bir üst seviyedeki risk koordinatörüne iletilmelidir

• Stratejik seviyedeki kilit ve/veya önemli görülen risklerle ilgili önceliklendirme gözden geçirilerek, değerlendirme sonuçları, İç Kontrol İzleme ve Yönlendirme Kurulu toplantısının ardından İdare Risk Koordinatör tarafından üst yöneticiye bir rapor olarak sunulmalıdır.

• Raporun sonuç ve değerlendirme bölümünde, risk yönetimi sürecinin yeterli güvence verip vermediği ve yeni tedbirlere ihtiyaç duyulup duyulmadığı hususları mutlaka yer almalıdır. Bu kapsamda; şu sorular göz önünde bulundurulabilir:

➢ Risklerin başarılı bir şekilde yönetildiğine dair makul güvence veriyor muyuz?

➢ Risklere verilen cevapların etkili bir biçimde uygulandığına veya izlendiğine dair makul güvence veriyor muyuz?

Risklerin gözden geçirilmesi sürecine ilişkin ipuçları Ek-6.10'da sunulmuştur.

Ek-6.10 Riskleri Gözden Geçirme İpuçları Riskleri Gözden Geçirme İpuçları

➢ Faaliyetin özelliğine göre gözden geçirme dönemi belirle. Kilit riskleri sıklıkla gözden geçir

➢ Gözden geçirme sırasında risklerin etki ve olasılığını o dönem için değerlendir.

➢ Riskin hala kabul edilebilir seviyenin üstünde olup olmadığına karar ver.

➢ O dönem için yeni risklerin ortaya çıkıp çıkmadığını tespit et.

➢ Riskin durumundaki değişikliğe göre risklere verilen cevapların durumunu da gözden geçirmek gerekir. Tespit edilen bulguları risk kaydına işle

➢ Gerekli görülen riskleri raporla (Her seviyede).

➢ Riskle ilgili değişimler risk kaydında yer alır, ancak çok acil durumlarda bir üst seviyedeki sorumluyu en kısa zamanda bilgilendir.

Risklerin gözden geçirilmesinde dikkate alınması gereken sorular Ek-6.11'de sunulmuştur.

Ek-6.11 Risklerin Gözden Geçirilmesinde Dikkate Alınması Gereken Sorular

Risklerin Gözden Geçirilmesinde Dikkate Alınması Gereken Sorular

✓ Hükümet ve idarenin politika belgelerinde değişiklikler var mı?

✓ Çevre koşullarındaki değişiklikler nelerdir?

✓ Faaliyetin işleyişine etki eden iç değişiklikler nelerdir?

✓ Değişikliklerin idare üzerindeki etkileri nelerdir?

✓ Mevcut kontroller değişen durumu karşılamaya yeterli midir?

✓ Kontrollerin etkili olduğuna dair yeterli kanıt var mı?

Ek-7 Risklerin Belirlenmesi, Değerlendirilmesi ve Kaydedilmesi için Beyin Fırtınası Yöntemi

Beyin Fırtınası Yöntemi

1. Adım

Birim veya alt birimin tüm üyelerini, temsilcilerini veya projede ya da belirli bir iş sürecinde çalışan tüm personelin uygun bir ortamda bir araya gelmesini sağlayın. Beyin fırtınası çalışmasını yönlendirecek uygun bir kolaylaştırıcı (moderatör) belirleyin. Beyin fırtınası yönteminin, bu konuda kolaylaştırıcı olarak deneyim kazanmış biri tarafından yönlendirilmesi en fazla verimi sağlar.

(Not: Beyin fırtınası stratejik riskler için idaredeki tüm üst düzey yöneticileri bir araya toplamak şeklinde de yapılabilir.)

Beyin fırtınasına katılan herkes sırasıyla idare ve süreçler konusunda yeterince bilgi sahibi olmalıdır.
Kolaylaştırıcının (Moderatörün) Rolü

- Tüm risk çalıştayı katılımcılarının riskleri belirleme faaliyetine aktif şekilde katılmasını sağlamak.
- Uygulanma amacını katılımcılara aktarmak.
- Benzer risklerin tekrarlanmamasını sağlamak. (Birbirine çok benzeyen risklerin birleştirilmesini önermek)
- Belirlenen riskin etki ve olasılığı için tüm katılımcıların oy vermesini sağlamak.
- Katılımcıları birbirlerinin puanlarını değerlendirmeye, kendi puanlarını savunmaya veya uygun olduğunu düşündükleri yerlerde puanlarını değiştirmeye teşvik etmek.
- Risk puanlarının, EK-8: Risk Oylama Formuna doğru şekilde işlenmesini ve önceliklendirilmesini sağlamak.
- En öncelikli olandan başlayarak risklere verilecek cevabın eylem planını oluşturmak.
- Her bir cevap için, belirli bir bireye sorumluluk verilmesini sağlamak.
- Her bir cevap için, belirli bir gözden geçirme ve raporlama tarihi belirlenmesini sağlamak.

2. Adım

Öncelikle birimin/ alt birimin /projenin/iş sürecinin/idarenin hedeflerinin ne olduğunu net bir şekilde ortaya koyun. Bu hedefler stratejik planda tanımlanmıştır. Ancak alt birimler için tanımlanmamış olabilir. Geniş düşünün, dikkate alınmamış başka hedef olup olmadığını tartışın. Tüm katılımcılar 3. adıma geçmeden önce hedeflerin bu şekilde olduğu konusunda mutabık kalmalıdır.

3. Adım

Beyin fırtınasının tüm katılımcıları, 2. adımda belirlenen hedeflere ulaşmadaki risklerin neler olduğu konusunda çok sayıda fikir üretmelidir. Bu, tek bir grup halinde veya daha kapsamlı beyin fırtınası toplantıları için alt gruplar halinde de yapılabilir. Risk gerçekleşirse hangi hedefe(lere) ulaşılamayabileceğini net bir şekilde belirleyin, riskleri ilgili oldukları hedeflerle birlikte Risk Oylama Formuna kaydedin (Ek-8 Sütun 3, 4, 5).

4. Adım

Tüm riskler belirlendikten sonra beyin fırtınası katılımcıları riskin etki ve olasılığını oylar. Verilen oylar Risk Oylama Formuna kaydedilir. Katılımcı sayısına göre Formdaki ilgili sütunların sayısı arttırılabilir (Sütun 6, 7, 8 ile 10, 11,12). (Etki ve olasılık puanları verilirken Ek-11 Risk Değerlendirme Kriterleri Tablosuna bakınız.)

5. Adım

İlk oylar Forma kaydedildikten sonra, belirli bir riskin etki ve/veya olasılığı için verilen en yüksek ve en düşük puan arasında büyük bir farklılık olduğu durumlarda en yüksek puanı veren kişi(ler) öncelikle neden en yüksek puanı verdiği konusunda savunma yapmalı ve diğerlerini kendi puanlarını yükseltmeleri için ikna etmeye çalışmalıdır. Daha sonra, en düşük puanı veren kişi(ler), neden en düşük puanı verdiği konusunda savunma yapmalı ve diğerlerini kendi puanlarını düşürmeleri için ikna etmeye çalışmalıdır. Savunmalar yapıldıktan sonra herhangi bir savunmadan ikna olan herkese puanını değiştirme fırsatı verilmelidir.

6. Adım

Risk Oylama Formunda belirlenen riskler, beyin fırtınasından çıkan ortalama etki (Sütun 9) ve ortalama olasılığın (Sütun 13) çarpımı sonucu bulunan risk puanları (Sütun 14), yüksek puandan düşük puana doğru sıralanır. Katılımcılara, sonucun bekledikleri gibi olup olmadığı sorulur. En önemli risk olduğunu düşündükleri risk en yüksek puanlı risk mi? Eğer değilse, oylamaya tekrar göz atılır ve değiştirilmesi gereken bir şey olup olmadığına karar verilir.

7. Adım

Beyin fırtınası katılımcıları Risk Oylama Formundaki risk puanları konusunda hemfikir olduktan sonra en öncelikli riskten başlayarak bütün riskleri ilgili değerleriyle birlikte Risk Kayıt Formunun (Ek-9) ilgili sütunlarına aktarırlar.

8. Adım

Risklere verilecek cevabı belirlerken risk seviyesinin risk iştahı içerisinde olup olmadığını, hangi cevabın daha uygun olacağını ve risklerin etki ve/veya olasılığını düşürerek riskleri en iyi şekilde azaltacağını düşünün. Ayrıca, mevcut risk cevabının neler olduğunu, bunların hâlihazırda (halen) etkili olup olmadığını ve bunların geliştirilip geliştirilemeyeceğini, mevcut cevapların yanı sıra veya mevcut cevapların yerine yeni cevapların öne sürülmesinin daha uygun olup olmayacağını düşünerek tablodaki açıklamalar doğrultusunda ilgili sütunlar doldurulur (Bkz. Ek-9 Risk Kayıt Formu sütun 6, 11,12).

9. Adım

Risk Kayıt Formundaki talimatlar dikkate alınarak diğer sütunlar da doldurularak form tamamlanır (Sütun 13 ve 14). Beyin Fırtınası İçin Önerilen Temel Kurallar:

- Kolaylaştırıcı (moderatörün) belirlenmesi
- Kötü fikir diye bir şey yoktur
- Eşit konuşma hakkı ve konuşmanın belli bir süre ile sınırlandırılması
- Aktif katılım
- Zaman çizelgesine uyma
- Yönlendirmenin kolaylaştırıcı (moderatör) tarafından yapılması
- Kişisel eleştiri değil açık eleştiri

Ek-8 Risk Oylama Formu

	KÜTAHYA DUMLUPINAR ÜNİVERSİTESİ **Strateji Geliştirme Daire Başkanlığı**												
	RİSK TESPİT VE OYLAMA FORMU												
Dok. Kodu: İK. LS.	**Yayın Tarihi:**	..../..... /202...		**Revizyon Tarihi:**	..../..... /202...								
Web Sayfası Linki:											**Türkçe**		**İngilizce**
Kontrolün Yapıldığı Ay/Yıl:													

1	2	3	4	5	6	7	8	9	10	11	12	13	14
İDARE/BİRİM/ALTBİRİM:													
Sıra	**Referans No**	**Stratejik Hedef**	**Birim/ alt birim hedefi**	**Tespit edilen risk**	**Etki A**	**Etki B**	**Etki C**	**ETKİ**	**Olasılık A**	**Olasılık B**	**Olasılık C**	**OLASILIK**	**Risk Puanı**
				Risk **Sebep**				**(A+B+C)/3**				**(A+B+C)/3**	ETKİ X OLASILIK

Sütunlar	
1	**Sıra No:** Risk kaydındaki sıralamayı gösterir.
2	**Referans No:** Riskin referans numarasını gösterir. Referans Numarası risk sahibinin bağlı olduğu birimi de gösterecek şekilde yapılan bir kodlamadır. Risk devam ettiği sürece bu kod değiştirilmez. Aynı kod bir başka riske verilmez.
3	**Stratejik Hedef:** Riskin ilişkili olduğu stratejik hedefin, stratejik plandaki kodunun yazıldığı sütundur.
4	**Birim / Alt Birim Hedefi:** Risk kaydı Birim / Alt Birim düzeyinde dolduruluyorsa, idarenin stratejik hedefleriyle doğrudan veya dolaylı bağlantılı ve riskten etkilenecek olan hedef bu sütuna yazılır. Risk kaydı İdare düzeyinde dolduruluyor ise bu sütun boş bırakılabilir.

5	**Tespit Edilen Risk:** Tespit edilen riskler yazılır, Sebep: Bu riskin ortaya çıkmasına neden olan sebepler belirtilir.
6-7-8	**Etki A/B/C:** Risk değerlendirme çalışmalarında yer alan her bir katılımcının ismi ile etkiye verdiği puanlar (1-5 arası), bu sütunlara kaydedilir. **Katılımcı sayısına göre bu sütunların sayısı artırılabilir.** Puanlama yaparken Risk Değerlendirme Kriterleri Tablosuna bakınız.
9	**Etki:** Katılımcıların verdikleri puanların aritmetik ortalaması alınarak riskin (ortalama) etki puanı bulunur.
10-11-12	**Olasılık A/B/C:** Risk değerlendirme çalışmalarında yer alan her bir katılımcının ismi ile olasılığa verdiği puanlar, bu sütunlara kaydedilir. Katılımcı sayısına göre bu sütunların sayısı artırılabilir. Puanlama yaparken Bkz: Örnek Risk Değerlendirme Kriterleri
13	**Olasılık:** Katılımcıların verdikleri puanların aritmetik ortalaması alınarak riskin (ortalama) olasılık puanı bulunur.
14	**Risk Puanı:** Etki puanı(ortalama) ile olasılık puanı (ortalama) çarpılarak Risk Puanı bulunur.

Ek-9 Risk Kayıt Formu:

	KÜTAHYA DUMLUPINAR ÜNİVERSİTESİ **Strateji Geliştirme Daire Başkanlığı**				
	RİSK KAYIT FORMU				
Dok. Kodu: İK. LS.	**Yayın Tarihi:**	..../...../ 202...	**Revizyon Tarihi:**	..../...../ 202...	
Web Sayfası Linki:				**Türkçe**	**İngilizce**
Kontrolün Yapıldığı Ay/Yıl:					

İDARE/BİRİM/ALTBİRİM: **Tarih: ..../..../20..**

1	2	3	4	5	6	7	8	9	10	11	12	13	14
Sıra	**Referans No**	**Stratejik Hedef**	**Birim/ alt birim hedefi**	**Tespit edilen risk**	**Risklere verilen cevaplar: Mevcut Kontroller**	**Etki**	**Olasılık**	**Risk Puanı(R)**	**Değişim (Risk Yönü)**	**Risk verilecek cevaplar Yeni/Ek/Kaldırılan Kontroller**	**Başlangıç Tarihi**	**Risk Sahibi**	**Açıklamalar**
				Risk **Sebep**									
				Risk **Sebep**									
				Risk **Sebep**									

Sütunlar	
1	**Sıra No:** Risk kaydındaki sıralamayı gösterir.
2	**Referans No:** Riskin referans numarasını gösterir. Referans numarası risk sahibinin bağlı olduğu birimi de gösterecek şekilde yapılan bir kodlamadır. Risk devam ettiği sürece bu kod değiştirilmez. Aynı kod bir başka riske verilmez.
3	**Stratejik Hedef:** Riskin ilişkili olduğu stratejik hedefin, stratejik plandaki kodunun yazıldığı sütundur.
4	**Birim / Alt birim hedefi:** Risk kaydı birim / alt birim düzeyinde dolduruluyorsa, idarenin stratejik hedefleriyle doğrudan veya dolaylı bağlantılı ve riskten etkilenecek olan hedef bu sütuna yazılır. Risk kaydı idare düzeyinde dolduruluyor ise bu sütun boş bırakılır.
5	**Tespit Edilen Risk:** Tespit edilen riskler yazılır, Sebep: Bu riskin ortaya çıkmasının nedenleri belirtilir.
6	**Riske verilen cevaplar: Mevcut Kontroller:** Mevcut kontroller bu sütuna yazılır.
7	**Etki:** Oylama Formu kullanılarak tespit edilen etki değeridir (1-5 arasında). Bu tespit yapılırken riskle ilgili uygulamada olan kontrol faaliyetleri, alınmış önlemler ve düzenlemelerin listelenmesi faydalıdır. Var olan önlemlere rağmen riskin gerçekleşirse etkisinin ne olacağı tespit edilir.
8	**Olasılık:** Oylama Formu kullanılarak tespit edilen olasılık değeridir (1-5 arasında). Bu tespit yapılırken riskle ilgili uygulamada olan kontrol faaliyetleri, alınmış önlemler ve düzenlemelerin listelenmesi faydalıdır. Var olan önlemlere rağmen riskin gerçekleşme olasılığının ne olduğu tespit edilir.
9	**Risk Puanı (R=ExO):** Oylama Formunda yapılan değerlendirmede tespit edilen etki ve olasılık değerlerinin çarpılması sonucu bulunan, risk puanları önceden belirlenen yüksek, orta ve düşük düzey puan aralıklarına göre yazılır.
10	**Değişim (Riskin yönü):** Bir önceki risk kaydı dikkate alınarak riskin durumundaki değişimin gösterildiği sütundur. (Yukarı/aşağı/sabit) şeklinde yazı ile belirtilebileceği gibi idarenin tercihine göre yön işaretleriyle de gösterilebilir. Daha önce risk kaydı yoksa "Yeni" olduğu belirtilir.
11	**Riske Verilen Cevaplar Yeni/ Ek/Kaldırılan Kontroller:** Öncelikle mevcut kontrollerin gerekli/yeterli olup olmadığı değerlendirilir. Yeterli olduğu değerlendiriliyor ise yeni bir kontrol öngörülmez. Yeterli değil ise yeni veya ek kontroller yazılır. Mevcut kontrollerden kaldırılması uygun bulunanlar da bu bölümde gösterilir.
12	**Başlangıç Tarihi:** Öngörülen yeni veya ek kontrollerin uygulamaya konulacağı, kaldırılması öngörülen kontrollerin ise uygulamadan kaldırılacağı kesin tarihtir.
13	**Riskin Sahibi:** Riskin yönetilmesinden ve izlenmesinden sorumlu olan kişidir. Riskle ilgili bilgiyi toplayan, izlemeyi gerçekleştiren, riske verilen cevapları yöneten ve riskin yönetildiğine ilişkin kanıtların tutulmasını sağlayan kişi riskin sahibidir. Riskin sahibinde riske verilecek cevapları gerçekleştirmek üzere gerekli kaynak ve yetki bulunmalıdır. Riskin sahibi aynı zamanda, Risk kayıtlarının güncellenmesi ve riskle ilgili olarak bir üst makama raporlama yapan kişidir.

14	**Açıklamalar:** Riskin mevcut durumu, değişim yönü, ne zaman gözden geçirileceği ve hangi aralıklarla kime raporlanacağı ve belirtilmesine ihtiyaç duyulan diğer hususlar bu sütunda belirtilir.

Renkler	
	Yüksek düzey risk
	Orta düzey risk
	Düşük düzey risk

NOT : Yıl içerisinde yeni bir risk tespit edilmesi durumunda riski tespit eden personel bir üst yöneticiye bu riski iletir. Yönetici bunun yönetilmesi gereken bir risk olduğuna karar verirse, bu risk, Risk Kayıt Formuna işlenerek ilgili yönetici tarafından onaylanır.

Ek-10 Konsolide Risk Raporu

	KÜTAHYA DUMLUPINAR ÜNİVERSİTESİ **Strateji Geliştirme Daire Başkanlığı**				
	KONSOLİDE RİSK RAPORU				
Dok. Kodu: İK. LS.	**Yayın Tarihi:**	..../..... /202...	**Revizyon Tarihi:**	..../..... /202...	
Web Sayfası Linki:				**Türkçe**	**İngilizce**
Kontrolün Yapıldığı Ay/Yıl:					

İDARE/BİRİM/ALTBİRİM: **Tarih: ..../..../20..**

1	2	3	4	5	6	7	8	9
Sıra	**Referans No**	**Stratejik Hedef**	**Birim/ alt birim hedefi**	**Tespit edilen risk**	**Durum**		**Risk Sahibi**	**Açıklamalar**
					Önceki Risk Puanı ve Rengi	**Sonraki Risk Puanı ve Rengi**		

Sütunlar

1	**Sıra No:** Risk kaydındaki sıralamayı gösterir.
2	**Referans No:** Riskin referans numarasını gösterir. Referans numarası risk sahibinin bağlı olduğu birimi de gösterecek şekilde yapılan bir kodlamadır. Risk devam ettiği sürece bu kod değiştirilmez. Aynı kod bir başka riske verilmez.
3	**Stratejik Hedef:** Riskin ilişkili olduğu stratejik hedefin, stratejik plandaki kodunun yazıldığı sütundur.
4	**Birim/Alt Birim Hedefi:** Rapor birim / alt birim düzeyinde hazırlanıyor ise Risk Kayıt Formunda yer alan Birim/Alt Birim hedefleri bu sütuna yazılır. Rapor idare düzeyinde hazırlanıyor ise bu sütun boş bırakılır.
5	**Tespit Edilen Risk:** Belirlenen risk yazılır.
6	**Önceki Risk Puanı ve Rengi:** Bir önceki Konsolide Risk Raporundaki riskin durumunu ifade eder.
7	**Mevcut Risk Puanı ve Rengi:** Rapor tarihindeki durumu gösterir.
8	**Riskin Sahibi:** Riskin yönetilmesinden ve izlenmesinden sorumlu olan kişidir. Riskle ilgili bilgiyi toplayan, izlemeyi gerçekleştiren, riske verilen cevapları yöneten ve riskin yönetildiğine ilişkin kanıtların tutulmasını sağlayan kişi riskin sahibidir. Riskin sahibinde, riske verilecek cevapları gerçekleştirmek üzere gerekli kaynak ve yetki bulunmalıdır. Risk sahibi aynı zamanda, Risk kayıtlarının güncellenmesi ve riskle ilgili olarak bir üst makama raporlama yapan kişidir.
9	**Açıklama:** Kontrol Faaliyetlerinin etkinliği ve geleceğe ilişkin öngörüler açıklama kısmında yer alır.
Renkler	
	Yüksek düzey risk
	Orta düzey risk
	Düşük düzey risk

Ek-11 Risk Değerlendirme Kriterleri Tablosu

RİSK DEĞERLENDİRME KRİTERLERİ TABLOSU						
Değer	**Aralık**	**Olasılık**	**Etki**			
			Strateji	**Faaliyetler/Süreçler**	**Mali**	**Mevzuata Uyum**
10 9 8 7	Yüksek	… yıl/ay/gün içerisinde gerçekleşmesi neredeyse kesin olan risklerdir. İdarenin yapısı göz önüne alındığında genellikle politika veya prosedürlerden kaynaklanır. İdarenin faaliyet alanı ne kadar geniş ise riskli olayların gerçekleşme olasılığı o kadar yüksektir.	Stratejik hedeflere ulaşmada önemli etkisi olabilecek risklerdir. Gerçekleşmesi durumunda idarenin hedeflerinden sapmasına dolayısıyla amaçlarını yeterince gerçekleştirememesine neden olabilecek risklerdir.	İdarenin/birimin /alt birimin faaliyetlerini etkili, ekonomik ve verimli bir biçimde gerçekleştirememesine neden olacak riskler bu kategoridedir.	İdare/birim/alt birim için önemli maddi kayba neden olabilecek risklerdir. Kamu kaynaklarının, idare tarafından kabul edilebilir düzeyin üzerinde etkili, ekonomik ve verimli kullanılmaması yüksek riskli kabul edilmelidir.	Bilerek veya bilmeyerek mevzuatla uyumun sağlanamaması durumunda idare/birim/alt birim üzerinde büyük yükümlülüklerin oluşabileceği durumlardaki risklerdir.
6 5 4	Orta	…yıl/ay/gün içerisinde gerçekleşme olasılığı olan risklerdir. Bunlar genellikle idarenin/birimin/alt birimin daha önce de karşılaştığı veya genel olarak idarelerde karşılaşılmış olan risklerdir.	Stratejik hedeflere ulaşmada belirli düzeyde etkisi olabilecek risklerdir. Bu puan aralığında yer almakla birlikte stratejik hedefleri etkileyebilecek kilit risklerin kriterlerinin belirlenmesi gerekmektedir.	İdarenin/birimin /alt birimin sunması gereken hizmeti etkili, ekonomik ve verimli bir biçimde gerçekleştirmesi üzerinde belirli düzeyde etkisi olabilecek risklerdir	İdare/birim/alt birim için belirli bir düzeyde maddi kayba neden olabilecek risklerdir. İdare tarafından kabul edilebilir düzeyde etkili, ekonomik ve verimli kullanılmaması orta riskli kabul edilmelidir.	Bilerek veya bilmeyerek mevzuatla uyumun sağlanamaması durumunda idare/birim/alt birim üzerinde belirli düzeyde yükümlülüklerin oluşabileceği risklerdir.
3	Düşük	…yıl/ay/gün içerisinde gerçekleşme ihtimali düşük olan risklerdir. Bunlar genellikle idarenin/birimin/alt birimin çok ender karşılaştığı, gerçekleşme olasılığının neredeyse olmadığı risklerdir.	Stratejik hedeflere ulaşmada çok az etkisi olabilecek risklerdir. Etkiler genellikle küçüktür ve sınırlı bir alanı kapsar.	İdarenin/birimin /alt birimin sunması gereken hizmeti etkili, ekonomik ve verimli bir biçimde gerçekleştirmesi üzerinde çok az etkisi olabilecek risklerdir.	İdare/birim/bölüm için çok az maddi kayba neden olacak riskledir. Kamu kaynaklarının idare tarafından kabul edilebilir düzeyin altında etkili, ekonomik ve verimli kullanılmaması, belirli miktarın altında harcanması düşük riskli olarak kabul edilmektedir	Bilerek veya bilmeyerek mevzuatla uyumun sağlanamaması durumunda idare/birim/alt birim üzerinde çok düşük düzeyde yükümlülüklerin ve/veya sorumlulukların oluşabileceği durumlardaki risklerdir.

Ek-12 Raporlama İş Akış Süreci ve Takvimi

Raporlama, risk yönetiminde karar alma süreçlerini doğrudan etkileyen bir unsurdur. Raporların, mümkün olduğunca kısa ve öz bilgilerden oluşması, ilgili olması, değerlendirmelere ilişkin kanıtları göstermesi, gerektiği zamanda ve gerekli kişilere sunulması özel önem taşımaktadır. İdare içerisinde raporlamanın, yatay ve dikey olarak ilgili kişilere yapılması gerekir. Risk Strateji Belgesinde raporlamanın kimler tarafından, kimlere ve hangi sıklıkta yapılacağı altta belirtilmiştir. "Birim Risk Raporu Hazırlama Kılavuzu" ile birimlerin raporlarını nasıl hazırlayacağı ve idare düzeyinde hazırlanacak konsolide risk raporlarının formatı ekleri ile belirlenmiştir.

Raporlama sıklığı, kimler tarafından hazırlanacağı ve iş akış süreci altta sunulmuştur.

Ek-13 Doğal ve Kalıntı Riske İlişkin Örnek Olay

Doğal ve kalıntı risk kavramlarını vurgulamak ve ayrıca risk sahibinin mevcut kontroller aracılığı ile sorumlu olduğu riskin ne dereceye kadar başarılı bir şekilde azaltıldığını izlemek üzere çeşitli kontrol sorumlularından (görev dağılımı çerçevesinde ilgili riskle ilgili olan kişiler) nasıl bilgi alabileceğini göstermeye yönelik bu örnek olay, içerisinde altın külçelerin tutulduğu bir depo, risk sahibi olan depo müdürü, altın külçelerin çalınma riski ve 4 kontrol faaliyeti ile ilgilidir:

Örnek Olay Çalışması

Kontrol 1: Bilişim Teknolojileri (BT) sistemi, depoya giren ve depodan çıkan altın külçelerini kontrol etmekte; her iş günü, depoya giren ve depodan çıkan külçe altınların kaydı tutulmakta ve BT yöneticisi, her gün bu kaydı risk sahibine rapor etmektedir.

Kontrol 2: Bağımsız bir şirket ayda bir kez gelerek depodaki altın külçelerin sayımını ve bunları BT yöneticisinin ilgili raporu ile karşılaştıran mutabakat kontrolünü yapmaktadır. (rapor ve stoklar arasındaki herhangi bir uyumsuzluk araştırılıyor ve mümkünse açıklaması yapılıyor) Bağımsız şirket risk sahibine yapmış olduğu iş hakkında aylık rapor yollamakta ve bu raporda, açıklanamayan uyumsuzlukları detaylı bir şekilde anlatmaktadır (açıklanamayanlar potansiyel hırsızlık vakaları olabilir).

Kontrol 3: Güvenlik görevlileri- profesyonel güvenlik görevlileri, haftada 7 gün/24 saat depoya erişimi kontrol etmekte, yalnızca yetkili personelin depoya girmesini ve tüm çantaların binadan ayrılırken metal dedektöründen geçirilmesini sağlamakta ve böylece dışarıya altın külçesi kaçırılmasını engellemektedir (altın külçeler kişinin üzerinde kolaylıkla saklayamayacağı/taşıyamayacağı kadar ağır). İşe alım sırasında, daha önceden hırsızlık sabıkası olmadığından emin olmak için güvenlik görevlilerinin sabıka kayıtları kontrol edilmektedir. Güvenlik görevlileri haftada bir kez risk sahibine rapor vermektedir.

Kontrol 4: Alarm sistemi- alarmın çalma vakaları risk sahibine rapor edilmektedir. Güvenlik görevlileri tarafından, düzenli bir şekilde (her hafta) alarm sisteminin işleyişi kontrol edilmekte ve kontrol sonuçları risk sahibine gönderilen rapora eklenmektedir

Yukarıdaki dört kontrolün yokluğunda doğal risk, yüksek risk olarak düşünülür. Bu, risk iştahının üzerinde olacaktır ve sonuç olarak yukarıda sayılan dört kontrol altın külçelerinin çalınma riskini azaltmaya yönelik tasarlanmıştır ve bu dört kontrolün öngörülen etkisi, kalıntı riskin azaltılmasıdır (Not: bu dört kontrol faaliyeti yalnızca altın külçelerinin çalınma olasılığını azaltacaktır, etkisini değil).

Risk sahibi bu dört kontrolün etkililiğine yönelik kanıt toplayacaktır. Kontroller etkili bulunurlarsa, risk sahibi, riskin başarılı bir şekilde kabul edilebilir risk sınırları içerisine düşürülüp düşürülmediğine bakacaktır.

Risk sahibi yukarıdaki kontrollerden birini veya birden fazlasını etkisiz bulursa, risk muhtemelen kabul edilebilir risk seviyesinin üzerinde olmaya devam edecektir ve böylece risk sahibinin bu sorunu yöneticisine iletmesi ve riski azaltmak için yöntem önermesi gerekecektir (ya ek kontroller sunarak ya da etkisiz bulunan kontrolleri güçlendirerek).

"**Kütahya Dumlupınar Üniversitesi Kurumsal Risk Yönetimi ve Risk Strateji Belgesi (2025-2028)**"

hazırlanmasında Hazine ve Maliye Bakanlığının Kamu İç Kontrol Rehberinden faydalanılmıştır.

Bilgi alma, öneri ve eleştirileriniz için

strateji@dpu.edu.tr