KAHRAMANMARAŞ SÜTÇÜ İMAM ÜNİVERSİTESİ

RİSK STRATEJİ BELGESİ

GİRİŞ

Kamu yönetiminde; kaynakların etkili, ekonomik ve verimli bir şekilde kullanılması, paydaş (vatandaş, çalışanlar, ilişkili kurumlar, sivil toplum kuruluşları vb.) beklentilerinin karşılanması, kaliteli kamu hizmetinin sunulması, sürdürülebilirliğinin sağlanması ve belirsizliklerinin etkin yönetimi ile hedeflere ulaşabilme konusundaki güvencenin arttırılması öne çıkan amaçlar arasındadır. Bu amaçlara ulaşabilmek için, ilgili hususlardaki performansı izlemeye ve performansı arttırmaya yönelik, şeffaflık, adillik, hesap verebilirlik ve sorumluluk ilkelerini esas alan kurumsal yönetim yaklaşımı ve uygulamaları kamu idarelerinin temel hedeflerinden biri haline gelmiştir.

Kurumsal yönetim yaklaşımının ayrılmaz bir parçası olarak risk yönetimi, kurumların hedeflerine ulaşmaya çalışırken maruz kalabilecekleri riskler hakkında başta üst yönetim olmak üzere tüm çalışanların farkındalık sahibi olmaları noktasında bir gereklilik olarak görülmektedir. Kurumsal risk yönetimi yaklaşımıyla oluşan risk kültürü, üst yönetimin karar alma süreçlerini destekleyerek, yönetim sorumluluklarını gerektiği şekilde yerine getirebilmeleri için ihtiyaç duydukları önemli bir bilgi kaynağı olmuştur.

5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu, kamu idarelerinin 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 artırılması amacıyla hazırlanarak yürürlüğe girmiştir. 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu ve ilgili diğer yasal düzenlemelerle kamu idarelerine misyon ve vizyonlarını tanımlamaları, amaç ve hedeflerini belirlemeleri, performanslarını ölçmeleri ve izleme değerlendirme süreçlerini işletmeleri amacıyla stratejik plan hazırlama yükümlülüğü getirilmiştir.

Stratejik plan hazırlanmasına ilişkin usul ve esasları belirleyen, Kamu İdarelerinde Stratejik Planlamaya İlişkin Usul ve Esaslar Hakkında Yönetmelik ve ilişkili olarak yayımlanan kılavuz ve rehberler, kamu idarelerinde stratejik yönetim sürecinin uygulanmasına yön vermektedir. Söz konusu düzenlemeler, stratejik planlamanın etkinliğinin artması için hedeflerin belirlenmesi aşamasında her bir hedefe ilişkin risklerin tespit edilerek, analiz edilmesi ve risklere yönelik önlemlerin belirlenmesi gerekliliğini belirtmektedir. Buna ilave olarak, risklerin stratejik planın hazırlık, uygulama, izleme ve değerlendirme aşamalarında da sürekli olarak gözden geçirilmesi gerekliliği vurgulanmaktadır. 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanununda; iç kontrolün tanımı, amacı, yapısı ve işleyişi ile iç kontrole ilişkin rol ve sorumluluklar düzenlenmiştir. Kamu İç Kontrol Standartları Tebliğinde; kamu idarelerinin iç kontrol sistemlerinin oluşturulmasında, izlenmesinde ve değerlendirilmesinde dikkate almaları gereken temel yönetim kuralları olan Kamu İç Kontrol Standartları açıklanmıştır. Söz konusu düzenleme, idarenin hedeflerinin gerçekleşmesini engelleyecek risklerin tanımlanması, analiz edilmesi ve gerekli önlemlerin belirlenmesine yönelik risk değerlendirme standartlarını içermektedir. Tüm bu gelişmelerle birlikte, stratejik planlama, performans esaslı bütçeleme, iç kontrol, iç denetim ve risk yönetimi kavramları Türk kamu yönetiminde uygulanmaya başlamış ve söz konusu yönetim araçları Türk kamu yönetimi işleyişine dâhil olmaya başlamıştır.

Kahramanmaraş Sütçü İmam Üniversitesinde, tüm bu süreçlerin düzenli olarak izlenmesini garantiye almak amacıyla sürekli değerlendirme, analiz ve geliştirme çalışmaları yürütülmektedir.

I. GENEL BİLGİLER

A. REHBERİN AMACI

Kahramanmaraş Sütçü İmam Üniversitesi bünyesinde uygulanacak kurumsal risk yönetimini içeren Kurumsal Risk Yönetimi Strateji Belgesi, kurumun ihtiyaçları göz önünde bulundurularak Üniversite Kurumsal Risk Yönetimi Yönergesi ile uyumlu olacak şekilde Strateji Geliştirme Daire Başkanlığı tarafından hazırlanmış ve İç Kontrol İzleme ve Yönlendirme Kurulu (İKİYK) tarafından incelenerek Rektör onayına sunulmuştur. Bu belge, kurumsal risk yönetimi uygulama sürecinde edinilen tecrübeler doğrultusunda yıllık periyotta gözden geçirilecek ve gerekli görülürse güncellenecektir.

Kahramanmaraş Sütçü İmam Üniversitesi Kurumsal Risk Yönetimi Strateji Belgesi;

- Üniversite Kurumsal Risk Yönetimi Yönergesinin kuruma entegre edilmesinde,
- Üniversitenin stratejik amaç ve hedeflerine ulaşma durumunu etkileyebilecek risklerin belirlenmesinde,
- Risklerin değerlendirilmesi ve önceliklendirilmesinde,
- Risklere yönelik alınacak kararların belirlenmesinde,
- Risklerin izlenmesi ve raporlanmasında,
- Kurumsal risk yönetiminde rol ve sorumlulukların, organizasyon yapısının oluşturulması, bu yapının yöneticiler ve çalışanlar arasında paylaşılmasında,
- Kurumsal risk yönetimi ile iç kontrol ve iç denetim süreçleri arasındaki ilişkinin tanımlanmasında, tüm iç ve dış paydaşların faydalanması amacıyla hazırlanmıştır.

B. REHBERİN KAPSAMI

Üniversitede, iç kontrol eylem planı hazırlama, izleme ve değerlendirme süreçlerinin etkin yönetimini sağlamak için İç Kontrol Uyum Eylem Planı uygulanmaktadır. İlgili plan kurul ve komisyon çalışmaları doğrultusunda, **"İç Kontrol Uyum Eylem Planı"** revize çalışmaları yürütülmüş ve plan uygulanmaya başlanmıştır. 2020 yılı İç Kontrol Uyum Eylem Planında yer alan "Risk Değerlendirme" bileşeni altında 6.1.1. No'lu eylemde "Üniversitemiz "Kurumsal Risk Strateji Belgesi/Yönergesi"nin oluşturularak yürürlüğe konması" planlanmış ve Strateji Geliştirme Daire Başkanlığı tarafından ilgili birimlerle çalışmalar yapılmıştır. Bu bağlamda hazırlanan, "**Kahramanmaraş Sütçü İmam Üniversitesi Kurumsal Risk Yönetimi Yönergesi"** Üniversitemiz Senatosunun 25 Mayıs 2021 tarihli ve 198 sayılı kararı ile kabul edilerek yürürlüğe girmiştir.

Yönergenin daha anlaşılır hale gelmesi ve kurumsal risk yönetimi uygulama stratejileri ve yöntemlerinin belirlenmesi amacıyla rehber niteliğinde bu belge hazırlanmıştır. Kurumsal Risk Yönetimi Strateji Belgesi, Üniversitede kurumsal risk yönetimi yaklaşımının uygulamaya alınması için metodoloji, araçlar ve örnekler sunmaktadır. **Bu belge dört ana bölümden oluşmaktadır**. Çalışmanın **birinci** bölümünde belge hakkında genel bilgilere yer verilmiştir. **İkinci bölümde**; risk ve kurumsal risk yönetimi kavramlarına, stratejik planlama, performans yönetimi, iç kontrol, iç denetim ve dış denetim arasındaki ilişkiye dair bilgilere yer verilmiştir. Çalışmanın **üçüncü bölümünde**; kurumda etkin bir kurumsal risk yönetimi sisteminin kurulması için gerekli organizasyon yapısı, görev, yetki ve sorumluluklarla ilgili bilgilere yer verilmiştir. Çalışmanın **dördüncü bölümünde ise** risklerin belirlenmesi, risklerin değerlendirilmesi, riske yönelik alınacak kararların belirlenmesi, risklerin izlenmesi ve raporlanmasına dair bilgilere yer verilmiştir.

II. RİSK VE KURUMSAL RİSK YÖNETİMİ

A. RİSK NEDİR?

Yönergemize göre Risk, ***"kurumsal veya stratejik amaç ve hedeflerine ulaşmasını olumsuz olarak etkileyecek, etki ve olasılık ile ölçülebilen her türlü eylem, durum ve olay"*** olarak tanımlanmaktadır. Ayrıca; "*Üniversitenin stratejik amaç ve hedeflerinin gerçekleşmesini engelleyecek, idari yönetimi ile eğitim faaliyetlerinin aksamasına sebep olacak, idari ve akademik personelin performansını düşürecek, sürdürülen projeleri başarısızlıkla sonuçlandıracak, yasal yükümlülüklerin yerine getirilmesinde sorunlar yaratacak, üniversitenin iç ve dış paydaşları nezdinde sahip olduğu saygınlığı zedeleyebilecek, bütçede mali kayıplar verdirecek ve çevre kirliliklerine neden olacak bütün iş ve olaylar risk olarak tanımlanır.*"

Küreselleşme, artan paydaş beklentileri, teknolojik gelişmeler, mevzuat değişiklikleri, karmaşık hale gelen süreçler gibi birçok etken, kamu idarelerinin orta ve uzun vadeli amaçlarını, hedeflerini ve bunlara ulaşmak için uyguladıkları faaliyetler ile kaynak dağılımlarını önemli ölçüde etkilemektedir. Bu etki, ileriye dönük karar alma süreçlerinde kamu idarelerinin stratejik amaç ve hedefleri ile ilişkili risklerini değerlendirerek, **söz konusu riskler gerçekleşmeden gerekli önlemleri almalarını** veya **gerçekleşmesi halinde uygun kaynak ve zaman planlaması ile maruz kalınacak zararın en aza indirgenmesini sağlayacak yöntemler geliştirmesini ve uygulaması**nı gerektirmektedir.

B. KURUMSAL RİSK YÖNETİMİ NEDİR?

Kurumsal risk yönetimi, *farklı misyon, vizyon ve temel değerlerle faaliyet gösteren kurumların stratejik amaç ve hedeflerini gerçekleştirmesini 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 ile ortaya çıkabilecek fırsatların etkin değerlendirilmesi için gerekli ve yeterli eylemlerin zamanında gerçekl eştirilmesinin sağlanması amacıyla uygulanan kapsamlı ve sistematik bir yaklaşımdır.*

Kurumsal risk yönetiminin kurumlara katkıları aşağıdaki gibi özetlenebilir:

- Kurumun ortak risk algısının oluşmasını destekler.
- Risk algısının oluşması ile risklerin yönetiminde kişiye bağlılık azaltılır.
- Kurumun risklerini yönetmede proaktif davranmasını sağlar.
- Riskler meydana gelmeden tespit edilir, gerekli ve yeterli eylemlerin zamanında gerçekleştirilmesi mümkün olur ve bu sayede kurum, olası risklere maruz kalmadan bunları bertaraf edebilme yeteneğine kavuşur veya risklerin meydana gelmesi durumunda uygun kaynak ve zaman planlaması ile kurumun maruz kaldığı zararlar azaltılır.
- Potansiyel risklere yönelik eylemlerin önceden gerçekleştirilmesi ile kurum faaliyetlerinde süreklilik sağlanır ve makul seviyede güvence altına alınır.
- Kamu idareleri tarafından iç ve dış paydaşlara verilen hizmetin kalitesi artar.
- Olası kayıpların etkilerinin kontrol altına alınması sayesinde kurumun katlanmak zorunda kalabileceği ilave maliyetler azalır, kurum kaynaklarının etkili ve verimli kullanımına katkı sağlanır.
- Risklerin kurumlar tarafından sadece tehdit olarak değil fırsat olarak da görünmesini sağlar.
- Kurumsal Risk Yönetimi yaklaşımı yöneticileri, risklerden tamamen kaçınmak yerine, risklerin değerlendirilmesi ve önceliklendirilmesi ile ölçülü risk almaya teşvik ederek, yenilikçi yaklaşımlar geliştirilmesine destek olur.

- Kurumun maruz kalabileceği riskler önceden tanımlandığı için Üst Yönetim anlık problemleri çözmekle vakit kaybetmek yerine, stratejik amaç ve hedeflere odaklanabilir.
- Böylece, Üst Yönetimin etkinliği ve verimliliği artar. Kurum bünyesindeki iç kontrol ve iç denetim fonksiyonlarının etkinliğini arttırmaya yardım eder.

C. KURUMSAL RİSK YÖNETİMİNİN KURUMA ENTEGRE EDİLMESİ

Kurumsal risk yönetiminin, kurum içerisinde etkin bir şekilde uygulanabilmesi için kurumun iş süreçlerinde, raporlama mekanizmalarına doğru şekilde entegre edilebilmesi gerekmektedir. Kurumsal risk yönetimi yaklaşımının entegre bir şekilde yönetilmesi, kurumun stratejik amaç ve hedeflerine ulaşması noktasında oldukça önemlidir.

i. Kurumsal Risk Yönetimi ve Stratejik Planlama İlişkisi

Stratejik plan, Kamu İdareleri İçin Stratejik Planlama Kılavuzu'nda belirtildiği şekilde, kamu idarelerinin orta ve uzun vadeli amaçlarını, temel ilke ve politikalarını, hedef ve önceliklerini, performans ölçütlerini, bunlara ulaşmak için izlenecek yöntemler ile kaynak dağılımlarını içeren planlama çalışmalarını ifade etmektedir. Stratejik planlama, kurumunun kaynaklarının etkili, ekonomik ve verimli kullanılmasını sağlayarak etkin karar alma süreçlerinin tesis edilmesine yardımcı olmaktadır.

Stratejik planlama sürecinde, stratejik amaç ve hedefler kurumsal risk yönetiminin ana odağını oluşturmaktadır. Stratejik planlama kapsamındaki amaç ve hedeflerin belirlenme süreci ile bu seviyedeki risklerin belirlenme süreci bir bütün halinde ve eş zamanlı olarak yürütülmelidir. Kurumsal risk yönetiminin kurum süreçlerine entegre edilmesi, kurumun stratejik amaç ve hedeflerine ulaşmasında tüm iç ve dış paydaşlara makul güvence sağlamaktadır. Kurumsal risk yönetimi, stratejik plan ile belirlenen kurum amaç ve hedeflerine ulaşılması için yürütülen faaliyetlerde ve izleme ile raporlama süreçlerinde de devam etmektedir. Kahramanmaraş Sütçü İmam Üniversitesinde tüm bu süreçler, var olan stratejik planı üzerinden yürütülerek başlatılmış olup, risklerin izlenmesi ve raporlanması bölümlerinde stratejik planda yer alan amaç ve hedeflerle ilişkili bir şekilde risklerin raporlanması ve gözden geçirilmesi hedeflenmektedir.

ii. Kurumsal Risk Yönetimi ve Performans Yönetimi İlişkisi

Kurumlar, stratejik amaç ve hedef seçimleri ve bu seçimler doğrultusunda yürüttüğü faaliyetler ile bazı riskler üstlenmektedirler. Bu riskler, kurumun faaliyetlerinin sürekliliğini ve başarısını, hizmetlerinin kalitesini, kamuoyundaki imajını ve çok sayıda faktörü etkilemektedir. Bu bağlamda, kurumsal risk yönetimi ile performans arasında iki yönlü bir ilişki bulunmaktadır.

Kurumsal risk yönetiminin kuruma entegre edilmesi ile birlikte risklerin belirlenmesi ve değerlendirilmesi sağlanmaktadır. Böylece kurumda risklere yönelik gerekli eylemlerin başarılı bir şekilde gerçekleştirilmesi ile kurumun performansının artmasına katkı sağlanmaktadır. Diğer bir yön olarak, kurumda yürütülen faaliyetlerin performansına ilişkin gerçekleştirilen izleme ve değerlendirme faaliyetleri ile performans göstergelerinin ölçümlenmesi ve raporlanması süreçleri kurumsal risk yönetim süreçlerinin etkinliği hakkında bilgi verilmektedir. Kurumun stratejik planı, performans programı vb. çalışmalar çerçevesinde tanımladığı faaliyetler ve göstergeler izlenerek, kurumsal risk yönetimi uygulamalarının etkin olup olmadığı performans değerlendirme sonuçlarıyla teyit edilmektedir.

Kahramanmaraş Sütçü İmam Üniversitesinde kurum performansının artırılmasında ve kurumsal risk yönetimi uygulamalarının geliştirilmesinde, bu iki yönlü ilişkinin Yönerge ve Performans Programı kapsamında sürdürülmesi esastır.

iii. Kurumsal Risk Yönetiminin İç Kontrol, İç Denetim ve Dış Denetim ile İlişkisi

Kurumsal risk yönetimi yaklaşımının etkin uygulanabilmesi için iç kontrol, iç denetim ve dış denetimin eşgüdüm içerisinde ele alınması gerekmektedir. Bu eşgüdüm yaklaşımının sergilenmesi ve söz konusu çalışmaların çıktılarının diğer çalışmalar için girdi olarak kullanılması, mevcut kaynakların verimli kullanılmasına ve kurumun stratejik amaç ve hedeflerine ulaşmasına önemli katkı sağlayacaktır.

Kamu İç Kontrol Rehberi'nde **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.

Kamu idarelerinde kurumsal risk yönetimi çalışmaları ile iç kontrol çalışmalarının etkileşim halinde yürütülmesi, oluşturulacak katma değer açısından oldukça önemlidir. 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, kurumun amaç ve hedeflerine ulaşmasına destek olmaktır. Kurumsal risk yönetiminin etkinliğinin sağlanması adına, kurumsal risk yönetimi ve iç kontrol yaklaşımları birbirleriyle doğrudan iletişim içinde olmalı ve gerçekleştirilen raporlamalar ile birbirlerini beslemelilerdir.

Kamu İç Denetim Rehberi'nde **iç denetim,** *"Kamu idaresinin 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, risk yönetimi süreçlerinde bağımsız izleme ile tanımlanan risk yönetimi faaliyetlerinin etkin yürütüldüğüne dair güvence ve sürecin geliştirilmesinde yönetime danışmanlık hizmeti verirken, riskleri fiilen yönetmek suretiyle yönetim sorumluluğu almaktan kaçınmak zorundadır.

İç denetim yaklaşımı açısından bakıldığında, etkin şekilde yürütülen kurumsal risk yönetimi faaliyetleri iç denetim faaliyetlerinin etkinliğinin artmasına yardımcı olmaktadır. Kurumsal risk yönetimi yaklaşımı açısından bakıldığında ise kurumun stratejik amaç ve hedefleri ile bunları etkileyebilecek risklerin belirlenmesi aşamasında iç denetimin önceki dönemde tespit ettiği bulgular göz önünde bulundurulmaktadır.

5018 sayılı Kanun'un 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. Kamu idarelerinin denetimleri sonucunda önemli görülen veya genellik arz eden konuları, yürütülen denetimlere ilişkin genel bilgileri ve mali konularda belirtilmesi uygun görülen diğer hususları içerecek şekilde hazırlanan denetim raporları kamu idarelerinin kurumsal risk yönetimi süreçlerine girdi oluşturmaktadır. Dış denetim çalışmaları sonucu kurumun iç kontrol ve iç denetim faaliyetlerinin etkinliğine yönelik tespit edilen konuların ve risklerin değerlendirilerek kurumsal risk yönetimi kapsamına alınması da kurumun stratejik amaç ve hedeflerine ulaşmasında destekleyici rol oynamaktadır. Dış denetim açısından bakıldığında, dış denetim planlaması yapılırken ve kapsamı belirlenirken kurumsal risk yönetimi yaklaşımı ile tespit edilen öncelikli risklere yönelik risk yönetimi faaliyetlerin varlığını, etkinliğini ve yeterliliğini

değerlendirmesi ile makul güvence arttırılmaktadır. Kurumsal risk yönetimi yaklaşımı açısından bakıldığında, kurumun stratejik amaç ve hedeflerini etkileyebilecek riskler belirlenirken önceki dönem dış denetim bulguları göz önünde bulundurulur.

III. RİSK YÖNETİMİ ORGANİZASYON YAPISI

A. ORGANİZASYON YAPISI

Kamu idarelerinde kurumsal risk yönetimi yaklaşımının etkin olarak işleyebilmesi için rol ve sorumlulukların tanımlanarak uygun seviyede paylaşımın sağlanması oldukça önemlidir. Kurumsal risk yönetiminde asgari şekilde görev alması gereken rol ve sorumluluklar aşağıda anlatılmaktadır. Üniversite risk yönetiminde organizasyon yapısı; Rektör, İç Kontrol İzleme ve Yönlendirme Kurulu, İdare Risk Koordinatörü, Birim Risk Koordinatörü, Alt Birim Risk Koordinatörü, Birim Risk Yönetim Ekibi, Çalışanlar, İç Denetim Birimi ve Strateji Geliştirme Daire Başkanlığından oluşur. Risk yönetimi organizasyon yapısı; birim ve birey bazlı sorumluluklar ile dikey ve yatay raporlama ve iletişim kanallarını da içeren ve fonksiyonel bir şekilde oluşturulan yapıyı ifade eder.

B. GÖREV, YETKİ VE SORUMLULUKLAR

Rektörün görev, yetki ve sorumlulukları

- Üniversitenin amaç ve hedefleri doğrultusunda risklerin yönetilmesi konusunda stratejinin belirlenmesi sağlar.
- Risk yönetim stratejisinin uygulama süreçlerini gösteren Üniversite Risk Yönetimi Strateji Belgesini ve Hassas Görevler Strateji Belgesini onaylar ve tüm çalışanlara yazılı olarak duyurulmasını sağlar.
- Üniversitede risk yönetimi sisteminin, iç kontrol uygulamaları ve kalite yönetim süreçleri ile bütünleşik olarak kurulmasını, uygulanmasını ve işleyişinin gözetilmesini sağlar.
- Risk yönetimi için gerekli yapıları oluşturarak görev ve sorumluluklarının açıkça belirlenmesini sağlar.
- Üniversite dışı diğer idarelerle ortak yönetilmesi gereken riskler konusunda İdare Risk Koordinatörüne gerekli desteği sağlar.
- Paydaşlara ve kamuoyuna karşı risklerin yönetilmesinde gerekli hassasiyetin gösterilmesini ve katılımcılığın teşvik edilmesi konusunda gerekli tedbirlerin alınmasını ve uygun mekanizmalar oluşturulmasını sağlar.
- İzleme ve Yönlendirme Kurulu ile İdare Risk Koordinatörü tarafından kendisine sunulan değerlendirme ve öneriler doğrultusunda gerekli önlemleri alır.
- Risk yönetim süreçlerinde izleme raporlarını inceler ve risk yönetiminin etkinliğini ve tutarlılığını sağlar.
- Risk yönetiminin sürecinin Üniversite politikaları doğrultusunda uygulanması konusunda tüm çalışanları teşvik eder.

İç kontrol izleme ve yönlendirme kurulunun görev ve sorumlulukları

- Üniversite Risk Yönetimi Strateji Belgesini ve Hassas Görevler Strateji Belgesini değerlendirir ve Rektörün onayına sunar.
- Üniversitede risk yönetim kültürünün oluşturulmasına ilişkin politikalar belirler.
- Kurumsal risk yönetimi uygulamalarının kurum içinde etkin işlemesi için görevlendirilen çalışma ekiplerinin veya görevlendirilen çalışanların rol ve sorumluluklarının belirlenmesini sağlar.
- Kurumsal risk yönetimi takvimini/eylem planını onaylar.
- Stratejik amaç ve hedefler seviyesinde belirlenen ve değerlendirilen riskleri gözden geçirir ve nihai hale getirir.

- Üniversite risk iştahını (risk alma ve kabullenme seviyesini) belirler, gerekli gördüğü hallerde günceller ve rektörün onayına sunar. (Ek-9)
- Risklere yönelik alınacak kararları belirler, belirlenen kararları gözden geçirir ve nihai hale getirir.
- Risk izleme ve raporlama mekanizmalarının kurum içinde etkin yönetilmesini sağlar.
- Kurula sunulan risk bilgisini ve riske yönelik alınacak kararları ve eylemleri inceler ve gerektiği durumlarda yeni eylemler tanımlar.
- Harcama birimlerine ait risklerden ortak yönetilmesi gerekenleri ve bunlara ilişkin politika ve prosedürleri belirleyerek koordine etmesi için İdare Risk Koordinatörüne bildirir.
- Üniversite dışı diğer idarelerle ortak yönetilmesi gereken riskleri çalışma formları, beyin fırtınası, arama konferansı vb. analiz yöntemleri ile belirler ve bunları İdare Risk Koordinatörüne bildirir ve gerekli çalışmaların yapılmasını sağlar.
- İdarenin kurumsal risk yönetimi yaklaşımını etkililiğine dair incelemelerde bulunur ve yetkileri doğrultusunda gerekli tedbir önerilerini Rektöre sunar.
- Risk yönetimi süreçlerinin üniversitede daha etkin işletilmesini sağlamak üzere gerektiği halde 'Risk İzleme ve Yönlendirme Komisyonu'nun kurulmasını Rektörün onayına sunar.
- Risk İzleme ve Yönlendirme Komisyonunun çalışma usul ve esaslarını belirler.
- Sayıştay ve iç denetim raporlarından da yararlanarak iyi uygulama örneklerinin tespit edilmesini ve yaygınlaştırılmasını sağlar.
- Kurumsal risk yönetimi yaklaşım adımlarının uygulanması sırasında belirlenen risklere yönelik altı aylık, yıllık dönemlerde izleme ve değerlendirme toplantıları yapar. Konuyla ilgili olarak Rektöre rapor sunar.
- Risk yönetim sisteminin; stratejik plan, kalite süreçleri ve performans programı doğrultusunda sürekli gelişimini, iyileştirilmesini ve kontrolünü sağlar.
- Üst Yönetime, kurumsal risk yönetimi uygulamalarının kurum içinde etkin işletilmesi için alanında yetkili kurum ve kuruluşlardan danışmanlık hizmeti almayı önerir.

İdare risk koordinatörünün görev ve sorumlulukları

- Risk yönetimi çerçevesinde Birim Risk Koordinatörlerini toplantıya çağırır.
- Birim Risk Koordinatörleri tarafından raporlanan risk yönetimi raporlarını konsolide ederek, "Üniversite Konsolide Risk Raporu" hazırlar; bu raporları belirlenen dönemlerde İç Kontrol İzleme ve Yönlendirme Kuruluna ve Rektöre sunar. Bu raporlarla birlikte izlenmesi gereken önemli riskleri ve kendi değerlendirmelerini de raporlar.
- Üniversite dışında diğer idarelerin İdare Risk Koordinatörleri ile ortak risk alanlarına ilişkin konuları görüşür ve bu konuda yapılacak çalışmaların Üniversite içerisinde koordinasyonunu sağlar.
- Birimlerin risk yönetimi konusundaki ihtiyaçlarını belirleyerek İç Kontrol İzleme ve Yönlendirme Kuruluna raporlar.
- İç Kontrol İzleme ve Yönlendirme Kurulunun görüşleri, tavsiyeleri ve kararlarına ilişkin Birim Risk Koordinatörlerine geri bildirim sağlar ve Üniversite risk yönetimi süreçlerinin tutarlı olması konusunda gerekli önlemleri alır.

Birim risk koordinatörünün görev ve sorumlulukları

- Birimin hedeflerini etkileyebilecek risklerin tespit edilmesini koordine eder ve rehberlik sağlar. Tespit edilen riskleri alt birimlerin bilgi ve uzmanlıklarından yararlanarak faaliyetler ile eşleştirir ve tüm önemli konuların ele alınmasını sağlar.
- Birim Risk Yönetim Ekibi toplantılarına başkanlık eder.
- Birim Risk Yönetim Ekibine üye olarak görevlendirilen personelin yeterli zaman ayırması ve aktif katılım göstermesi için teşvik eder.
- Yıllık periyotlarda belirlenen risk kayıtlarını ve ilgili raporları gözden geçirir ve birim yöneticisinin de onayını alarak İdare Risk Koordinatörüne raporlar.

- Alt Birim Risk Koordinatörlerinin raporladıkları riskleri birim düzeyinde izler. Mevcut risklerdeki değişiklikleri ve varsa yeni riskleri değerlendirerek birim yöneticisinin de uygun görüşünü alarak İdare Risk Koordinatörüne raporlar.
- Yıllık olarak daha önce belirlenmiş veya yıl içerisinde ortaya çıkabilecek risklerin iyi yönetilip yönetilmediğine dair kanıtları İdare Risk Koordinatörüne sunar.
- İdare Risk Koordinatörü ile İç Kontrol İzleme ve Yönlendirme Kurulunun görüşleri, tavsiyeleri ve kararları doğrultusunda varsa Alt Birim Risk Koordinatörlerine geri bildirim sağlar.
- İdare Risk Koordinatörü tarafından talep edilen bilgi ve belgeleri zamanında bildirir.
- Risk yönetimiyle ilgili eğitim ihtiyaçlarını tespit eder ve İdare Risk Koordinatörüne bildirir.

Alt birim risk koordinatörü görev ve sorumlulukları

- Alt birim düzeyindeki risklerin tespit edilmesi, değerlendirilmesi, cevap verilmesi, gözden geçirilmesi ve raporlanması görevlerinin yerine getirilmesini koordine eder.
- Alt birimin faaliyetlerine yönelik yeni tespit edilen riskleri, risk puanı değişenleri ve uygulanan kontrollerin etkinliğini belirlenen periyotlarla Birim Risk Koordinatörüne raporlar.
- Birim Risk Koordinatörü tarafından talep edilen bilgi ve belgeleri zamanında bildirir.
- Risk yönetimiyle ilgili eğitim ihtiyaçlarını tespit eder ve Birim Risk Koordinatörüne bildirir.

Birim risk yönetim ekibinin organizasyonu, görev ve sorumlulukları

- Birim Risk Yönetim Ekibi, Birim Yöneticisi, Birim Risk Koordinatörü ile Alt Birim Risk Koordinatörleri olmak üzere Birim Yöneticisi tarafından en az 3 kişiden oluşturulur. Alt birimleri olmayan birimlerde ise ilgili konuda bilgi ve tecrübesi olan en az 1 kişi ekibe dâhil edilir.
- Üniversitenin stratejik hedeflerine ulaşabilmesi açısından birimin hedeflerini etkileyebilecek risklerin tespit edilmesi, değerlendirilmesi, cevap verilmesi, izlenmesi ve raporlanması görevlerini yerine getirir. (Ek-8)
- Birime bağlı alt birimlerce yürütülen faaliyetlere yönelik risklerin tespit edilmesi, değerlendirilmesi, cevap verilmesi, izlenmesi ve raporlanması görevlerini yerine getirir.
- Birim hedeflerine ve faaliyetlerine ait yeni tespit edilen riskleri, risk puanı değişenleri ve kontrollerin etkinliğini yılda en az bir kez kontrol eder. Çalışanlardan gelen bilgileri konsolide eder.

Çalışanların görevleri ve sorumlulukları

- Risk yönetiminin başarısı, çalışanların risk yönetimini sahiplenmesine bağlıdır. Dolayısıyla, her bir çalışan, görev alanı çerçevesinde risklerin yönetilmesinden (risklerin tespit edilmesi, değerlendirilmesi, cevap verilmesi, izlenmesi ve raporlanmasından) sorumludur.
- Üniversite çalışanlarının risk yönetimi sürecindeki görev ve sorumlulukları şunlardır:
- Yeni ortaya çıkan ve değişen riskleri tanımlamak, iletmek ve bunlara cevap vermek yoluyla birimlerinde risk yönetimi süreçlerine doğrudan katkıda bulunur.
- Sürekli izleme sonucu tespit edilen yeni ve değişen risklerin ilgili birim veya Alt Birim Risk Koordinatörüne iletilmesini sağlar.
- Strateji Geliştirme Daire Başkanlığı, Alt Birim Risk Koordinatörü ve Birim Risk Koordinatörü tarafından talep edilen bilgilerin ve belgelerin amirinin bilgisi dahilinde zamanında iletilmesini sağlar.
- Görev alanındaki riskleri, belirlenen yetki ve sorumlulukları çerçevesinde yönetir.
- Görev alanındaki risklerin iyi yönetilip yönetilmediği konusunda, Birim Risk Yönetim Ekibi ve Alt Birim Risk Koordinatörü'ne gerekli kanıtları sağlar.
- Görevlendirildiği çalışma ekiplerinde veya kurullarda aktif bir şekilde çalışır, yeterli vakti ayırır ve çalışma sonuçlarını takip eder.
- Kurumsal risk yönetimi kapsamında düzenlenen toplantı, çalıştay ve eğitimlere katılır.

İç denetim birim başkanlığının görev ve sorumlulukları

- Risk yönetimi sürecinin etkili olup olmadığı, risklerin gereken şekilde yönetilip yönetilmediği hususunda incelemeler yaparak, Rektöre mevzuat çerçevesinde gerekli raporlamaları yapar.
- Üniversitede risk yönetim sürecinin kurulması ve geliştirilmesine destek olmak üzere danışmanlık hizmeti yapar.
- Risk yönetimi süreçlerinde bağımsız izleme ile tanımlanan risk yönetimi faaliyetlerinin etkin yürütüldüğüne dair Rektöre güvence verir.
- Riskleri fiilen yönetmek suretiyle yönetim sorumluluğu almaktan kaçınır.

Birim yöneticilerinin görev ve sorumlulukları

- Nitelikli personelini kurumsal risk yönetimi için oluşturulan komisyonlarda, alt çalışma ekiplerinde ve çalıştaylarda görevlendirir.
- Görevlendirilen personelin yapılacak çalışmalara yeterli zaman ayırması ve aktif katılım göstermesi için gerekli tedbirleri alır.
- İç Kontrol İzleme ve Yönlendirme Kurulu ve Risk İzleme ve Yönlendirme Komisyonu tarafından talep edilen bilgi ve belgeleri zamanında ve eksiksiz hazırlar ve gönderir.
- Riskleri sürekli izler, risklerde bir değişiklik olması veya yeni bir risk oluşması durumunda İç Kontrol İzleme ve Yönlendirme Kuruluna raporlar.
- İzleme sonuçlarını belirlenen periyotlarda İç Kontrol İzleme ve Yönlendirme Kuruluna raporlar.
- Risk kayıt ve takip formunun güncellenmesine katkı sağlar.

Strateji geliştirme daire başkanlığının görev ve sorumlulukları

- Üniversite Kurumsal Risk Yönetimi Strateji Belgesini oluşturur, gerekli hallerde günceller, İç Kontrol İzleme ve Yönlendirme Kurulunun değerlendirmesine ve Rektörün onayına sunar.
- Üniversite Hassas Görevler Strateji Belgesini oluşturur, gerekli hallerde günceller, İç Kontrol İzleme ve Yönlendirme Kurulunun değerlendirmesine ve Rektörün onayına sunar.
- Mali iş ve işlemlerle ilgili riskli görülen alanlarda toplantı, rehber, kılavuz, genelge, talimat vb. yönlendirici kontrol faaliyetleri tasarlayarak uygulanmasını sağlar.
- Üniversitede risk yönetimine ilişkin çalışmaları koordine eder ve iç kontrol sisteminin değerlendirilmesi kapsamında risk yönetiminin etkinliğini de değerlendirerek belirli dönemler halinde İç Kontrol İzleme ve Yönlendirme Kuruluna rapor sunar.
- Kurumsal risk yönetimi takviminin oluşturulmasını, Kurul onayına sunulmasını, kamuoyuna duyurulmasını ve takvimde belirlenen toplantı/çalıştay/eğitimlerin organize edilmesini ve yürütülmesini sağlar.
- Birim Risk Koordinatörü ve diğer katılımcılar tarafından belirlenen risklerin, değerlendirme sonuçlarının ve riske yönelik alınacak kararların konsolide edilmesinden, risk izleme ve değerlendirme formuna kaydedilmesini sağlar.
- Risk yönetimi süreçlerinin Üniversitenin tüm birimlerinde etkin işlemesini sağlamak üzere teknik destek, danışmanlık ve sekreterya hizmetleri verir.
- Risk yönetimine ilişkin Üniversitedeki iyi uygulamaları belirler, bu uygulamaların yaygınlaştırılması için çalışmalar yapar.
- Gerekli olması halinde Yönergenin güncellenmesini Kurul'a önerir.
- Kurumsal Risk Stratejilerine uygun formlar geliştirir, geliştirilen formlar belirli periyotlarda gözden geçirir ve güncellemesini sağlar.

Rol ve Sorumluluk Matrisi:

	Çalışanlar	Birim Yöneticileri	SGDB	Birim Risk Yönetim Ekibi	Birim/Alt Birim Risk Koordinatörü	İdare Risk Koordinatörü	İç Denetim	İKİYK	Rektör
Risk Strateji Belgesinin oluşturulması	B	B	G	B	B	B	D	S	S
Risklerin tam ve doğru olarak belirlenmesi	G	S/G	K	S/G	S/G	S/G	B	S/G	S
Risklerin değerlendirilmesi ve önceliklendirilmesi	G	S/G	K	S/G	S/G	S	D	D	S/D
Risklere yönelik alınacak kararlarının belirlenmesi	B	S/G	K	S/G	S/G	S	B	B	S/D
Belirlenen risklere yönelik eylem planlarının oluşturulması	G	S/G	K	S/G	S/G	S	D/B	D/B	S/D
Eylem planlarının uygulamaya alınması	G	S/G	K	S/G	S/G	S	B	B	S/B
Eylem planlarının uygulamaya alındığının denetlenmesi	-	-	K	-	-	B	G	B	S/B
Risklerin izlenmesi ve raporlanması	G	S/G	K	S/G	S/G	S	B	S/G	S/B

Sembollerin Açıklaması:

Tanım	Açıklamalar
(G) GÖREVLİ	Belirtilen iş süreçlerini yürüten
(S) SORUMLU	Belirlenen iş süreçlerinin amacına uygun ve zamanında tamamlanmasından sorumlu olan (Onaylayan veya değerlendiren)
(D) DANIŞILAN	Belirtilen iş sürecindeki görevlerin yerine getirilmesinde, bilgileri inceleyen ve süreç veya içerik konusunda bilgi paylaşımında bulunan
(B) BİLGİ VERİLEN	Belirtilen iş süreçlerinin ilerleyişi ve sonuçları hakkında bilgi verilen
(K) KOORDİNE EDEN	Belirtilen iş süreçlerindeki görevlerin yerine getirilmesinde ilgili birimler arasındaki koordinasyonu sağlayan

Rol ve Sorumluluklar Matrisi

V. KURUMSAL RİSK YÖNETİMİ SÜRECİ

Kurumsal risk yönetimi süreci, risklerin belirlenmesinden başlayarak risklerin izlenmesi ve raporlanmasını kapsayacak şekilde aşağıda yer verilen adımlar çerçevesinde uygulanır:

A. RİSKLERİN BELİRLENMESİ

Risk belirleme sürecinin temel amacı; Üniversitenin politika, amaç ve hedeflerine ulaşmasına engel olacak ve idari performansı düşürecek her türlü olay temel alınarak, var olan tehditleri, istenmeyen durumları ve sonuçları, yaklaşmakta olan tehlikeleri içerecek kapsamlı bir risk haritası çıkarmaktır.

Risklerin Belirlenmesinde Dikkat Edilecek Hususlar

Kurumsal risk yönetimi yaklaşımına göre, risklerin belirlenmesi aşamasında aşağıda sıralanan hususlara dikkat edilmesi gerekir:

- Tanımlanan riskler açık ve kolay anlaşılır olmalıdır. Risk geçmişle veya içinde bulunulan anla ilgili değil, gelecekle ilgilidir. Bununla birlikte, risklerin belirlenmesi aşamasında geçmiş tecrübelerden yararlanılır.

- Riskler tehditleri, yani kurumsal hedefleri olumsuz yönde etkileyecek potansiyel olaylar veya durumları içerebildiği gibi aynı zamanda fırsatları, yani kurumsal hedefleri olumlu yönde etkileyerek avantaja dönüştürebilecek potansiyel olaylar veya durumları içerebilir.

- Riskin temelinde belirsizlik yatar. Bununla birlikte, farklı kavramlar olan risk ve belirsizliğin birbiri ile karıştırılmamalıdır.

- Bir olayın veya durumun risk olarak tanımlanabilmesi için, söz konusu olay veya durumun kurumun stratejik amaç ve hedeflerine ulaşmasını etkileyebilmesi veya kurumun operasyonel işleyişinde aksaklığa sebebiyet vermesi gerekir. Kurum amaç ve hedeflerine ulaşma becerisini etkileme gücü bulunmayan olaylar veya durumlar risk olarak tanımlanmamalıdır. Bununla birlikte, kurumun amaç ve hedeflerine ulaşmasını etkileyebilecek risklerin stratejik riskler olabileceği gibi, aynı zamanda operasyonel, finansal, uyum ya da dış riskler de olabileceği unutulmamalıdır.

- Riskler kurumun stratejik amaç ve hedefleri ile ilişkili olmalıdır. Bu nedenle, risk tanımlamalarının doğru ve tam yapılabilmesi için öncelikle kurumun stratejik amaç ve hedeflerinin doğru ve eksiksiz tanımlanmış olması gerekir.

- Kurum tarafından maruz kalınabilecek riskler, değişen iç ve dış koşullara bağlı olarak zaman içinde değişim gösterir. Bu nedenle, riskler tanımlanırken değişen koşullar mutlaka göz önünde bulundurulmalıdır.

- Strateji Geliştirme Daire Başkanlığı koordinasyonunda ilgili kurul/komisyonların ve üst yönetimin de katılımı ile Kurumsal Risk Yönetimi Çalıştay/Eğitim programları organize edilir. Bu çalıştay/eğitimlerde, üniversitenin stratejik amaç ve hedeflerine ulaşmasını etkileyebilecek risklerin belirlenmesi, değerlendirilmesi, önceliklendirilmesi, risklere yönelik alınacak kararların belirlenmesi ve eylem planlarının oluşturularak paylaşılması ve tartışılması için bir ortam yaratılır.

- Risklerin belirlenmesi sürecinde stratejik planlama aşamasında gerçekleştirilen analiz sonuçlarından (PESTEL, GZFT, vb.) faydalanılır. Bu analizler sırasında belirlenen kurumun zayıf yönleri gibi tespitler, kurumda oluşabilecek risklerin kök nedenlerine işaret edebilmektedir.

Risk Türlerinin Tespit Edilmesi

Riskler; stratejilerle ilişkili riskler, finansal riskler, yasal uyum riskleri, çevresel riskler, operasyonel riskler, itibar ve raporlama riskleri olmak üzere altı başlıkta değerlendirilir;

a) Stratejilerle İlişkili Riskler: Üniversitenin stratejik seçimlerinden dolayı maruz kalabileceği, stratejik amaç ve hedeflerine ulaşmasına engel olabilecek risklerdir.

b) Finansal Riskler: Finansal değer kaybı olasılığı taşıyan tehditleri ifade eden, mali konularda olumsuz bir etkiye neden olabilecek potansiyel olay, koşul ya da durumlardan oluşan risklerdir.

c) Yasal Uyum Riskleri: Kanunların ve yasal düzenlemelerin değişmesinden kaynaklanan riskler ile yetersiz ya da yanlış bilgi ve dokümantasyon nedeniyle yaşanan yasal uyuşmazlıklar, yükümlülüklerin yerine getirilmesi konusundaki belirsizlik, düzenlemelerin yanlış yorumlanması veya personelin bu yükümlülükleri zamanında yerine getirmemesinden kaynaklanan risklerdir.

ç) Çevresel Riskler: Üniversitenin kontrolü dışında gerçekleşen olaylar sonucunda maruz kalabileceği risklerdir.

d) Operasyonel Riskler: Yetersiz sistemlerden, süreçlerden veya çalışanlardan kaynaklanabilecek kayıpların gerçekleşme riskidir. İş süreçleri, sistemler, faaliyetler ve işlemlerdeki hatalar, verimsizlikler, ihmaller, kötüye kullanımlar, hileler, kapasite sorunları bu kapsamda ele alınır.

e) İtibar ve Raporlama Riski: Kurum hakkında olumsuz düşüncelerin oluşması, kuruma duyulan güvenin azalması veya kurum imajının zedelenmesine sebep olan riskler ile kamuya, üst yönetime ve yasal otoritelere yapılan mali ve mali olmayan raporlamaların hatalı olması sebebiyle oluşan risklerdir.

Finansal, yasal uyum, çevresel, operasyonel, itibar ve raporlama risklerinden stratejik hedefleri etkileme olasılığı olan risklerin hangi stratejilerle ilişkili olduğu belirtilir. Risklere ilişkin kategorilere, açıklamalara ve örneklere aşağıda yer verilmektedir:

KATEGORİ	AÇIKLAMA	ÖRNEK
Stratejilerle İlişkili Riskler	Kurumun stratejik seçimlerini yürütme aşamasında aldığı stratejik kararlar dolayısıyla maruz kalabileceği risklerdir. Yönetim ve organizasyon yapısına ilişkin riskler, örgütlenme riskleri bu kapsamda değerlendirilebilir.	Öğrenme kaynaklarında dijitalleştirme çalışmalarına yönelik yeterli kurumsal altyapının oluşturulamaması sonucunda artan dijital kaynak talebinin karşılanamaması
Finansal Riskler	Kurumun finansal yapısını ve finansal faaliyetlerini sürdürmek için ihtiyaç duyduğu kaynakları etkileyebilecek risklerdir.	Proje yatırım bütçelerinin etkin takip edilmemesi sonucunda finansal yükümlülüklerin yerine getirilmemesi
Yasal Uyum Riskleri	Kurumun dış düzenlemelere (yasalar, tebliğler) ve iç düzenlemelere (politika ve prosedürler) uygun işlemler yapmasını etkileyebilecek risklerdir.	Veri güvenliğinin sağlanamaması nedeniyle Kişisel Verilerin Korunması Kanununa uyumsuzluk sonucunda kurumun cezai yaptırıma maruz kalması
Çevresel Riskler	Kurumun kontrolü dışında gerçekleşen olaylar sonucunda maruz kalabileceği risklerdir.	Dünyayı etkisi altına alan salgın koşullarının yarattığı yeni çalışma biçimlerine ilişkin düzenlemelerin yapılamaması
Operasyonel Riskler	Kurumun iş süreçlerinin doğru, uygun ve verimli gerçekleşmesini etkileyebilecek risklerdir.	Sağlık hizmetleri kapsamında kullanılan randevu sistemine yönelik yetersiz bilgi teknolojileri altyapısı nedeniyle arızaların oluşması ve vatandaşa sağlık hizmeti sunulamaması
İtibar ve Raporlama Riski	İtibar riski, kurum hakkında olumsuz düşüncelerin oluşması, kuruma duyulan güvenin azalması veya kurum imajının zedelenmesi olarak tanımlanmaktadır.	Kurum için kritik öneme sahip bir projenin taahhüt edilen sürede tamamlanamaması sonucu halkın gözünde hizmetlerin yeterliliğinin sorgulanması ve kurumun itibar kaybetmesi

Risk Örnekleri

Hatalı Risk Tanımlaması	Doğru Risk Tanımlaması
Hatalı yetki verilmesi	Görev ve sorumluluk ile bağdaşmayan yetki verilmesi sonucu yetkisiz kişiler tarafından sistemde uygun olmayan/hatalı işlemlerin gerçekleştirilmesi
Personel yetersizliği	Personel yetersizliği nedeniyle kurum operasyonlarında aksamaların yaşanması ve vatandaşa sunulan kamu hizmetinin kalitesinin düşmesi
Kaynak/ödenek yetersizliği	Kaynak yetersizliği sebebi ile gerekli ekipmanların alınamaması, sağlık eğitimlerinin etkin şekilde verilememesi sonucunda kalifiye sağlık görevlilerinin yetiştirilememesi ve vatandaşa sunulan sağlık hizmetinin kalitesinin düşmesi
Personelin eğitim ihtiyaçlarının karşılanmaması	Personelin eğitim ihtiyaçlarının karşılanmaması sonucunda gerekli yetkinliklerin geliştirilememesi ve hizmetlerin istenen kalitede sunulamaması
Kurum tarafından kullanılan araçlarda ya da makinalarda eksiklik olması	Kurum tarafından kullanılan araçlarda ya da makinalarda eksiklik olması sebebiyle operasyonlarda aksamaların yaşanması
Laboratuvar, klinik ve poliklinik hizmetlerinin sürdürülmesinde yetersiz kalma olasılığı	Laboratuvar, klinik ve poliklinik hizmetlerinin sürdürülmesinde yetersiz kalınması sonucu sağlık hizmetlerinin aksaması
Sarf malzeme kullanan personelin gerekli tertibi ve özeni göstermeme riski	Sarf malzemesi kullanan personelin gerekli tertibi ve özeni göstermemesi sonucunda sarf malzemelerinin hatalı kullanılması ve yüksek fire oranının oluşması

Hatalı ve Doğru Risk Tanımlamaya Ait Örnekler

Risk İştahı

Risk iştahı (risk alma istekliliği), kurumun amaçları doğrultusunda kabul etmeye hazır olduğu en yüksek risk düzeyidir. Kurum için hangi seviyenin üzerindeki risklerin kabul edilemeyeceği ve önlem alınması gerektiğine ilişkin yol gösterici rol oynar. Risk iştahı kurumun 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 kurumun risk kültürü gibi çok sayıda faktörden etkilenir. Kurum hedefleri bazında tanımlanan risk iştahı seviyesi, Üst Yönetim tarafından kurumun ortak risk algısı çerçevesinde belirlenir. Yüksek risk iştahının yüksek kayıplara neden olabileceği algısı ile gereğinden düşük seviyede risk iştahı tanımlaması kurumun fırsatları değerlendirmesine engel teşkil edebilir. Risk iştahının çok yüksek tanımlanması da kurumun 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 çok yüksek, yüksek, orta, düşük ve çok düşük olmak üzere 5 seviyede değerlendirilir. Her bir hedefle ilişkili riskler ve risk iştahı tanımlandıktan sonra, hedef bazında belirlenen risk iştahı ile risk seviyeleri karşılaştırılır. Risk iştahı seviyesi, risklere yönelik alınacak kararlar belirlenirken göz önünde bulundurulur.

Kurum düzeyi (stratejik düzey): Tüm idareyi kapsayan, stratejik hedeflere ilişkin kararların verildiği ve idarenin üst yönetiminin sorumluluğunda olan alandır. Stratejik hedefler orta ve uzun döneme yöneliktir ve üst düzey politika belgeleriyle ilişkilidir. Bu nedenle geleceğe ilişkin kararlar verilirken, karar vericiler (üst yönetim) 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.*

Birim düzeyi (program/proje düzeyi): Üst yönetimin politikalarının uygulandığı ve idare içinde kamu kaynaklarının kullanılmasından en üst düzeyde sorumlu olunan birimleri ifade eder. Bu düzeyde yer alan riskler, stratejik risklere göre daha kısa dönemde etkilidir. İdarenin stratejik hedeflerine ulaşabilmesi açısından birimin kendi fonksiyonlarına yönelik hedeflerini belirlemiş olması ve bu hedeflere ilişkin riskleri yönetmesi gereken alandır. Hem dışarıdan hem de idare 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.

Alt birim/Taşra birimi düzeyi (faaliyet düzeyi): 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.

Alt Birim Düzeyinde riskler **"Birim Çalışanları Risk Öneri Formu"** aracılığı ile tüm çalışanlardan istenir. Çalışanlar istemeleri halinde, birimi ile ilgili risk önerisinde bulunur. Risk önerisinde bulunan çalışan Ek-10 Forma önereceği riskleri yazar ve altını imzalayarak Alt Birim Risk Koordinatörüne iletir. Alt Birim Risk Koordinatörü çalışanlardan gelen riskleri inceler, değerlendirir ve kayda değer gördüğü riskleri

GÜYBİS sistemine işler.

B. RİSKLERİN DEĞERLENDİRİLMESİ

Kurumsal risk yönetimi yaklaşımında, kamu idareleri tarafından stratejik amaç ve hedeflere ulaşılmasını etkileyebilecek risklere ilişkin ana odak noktalarını yansıtan risk evreninin ve risklerin belirlenmesinden sonraki adım, risklerin değerlendirilmesidir. Risklerin değerlendirilmesi, risk seviyelerinin belirlenmesini ve risklerin önceliklendirilmesini kapsar.

Risk Seviyelerinin Belirlenmesi

Risk seviyelerinin belirlenmesi aşamasında, öncelikle risklerin etki ve olasılık seviyeleri ölçülür. Ardından kurumun söz konusu risklere yönelik yürütmekte olduğu risk yönetimi faaliyetlerinin etkinliği ve yeterliliği değerlendirilerek önceliklendirmeye esas alınacak risk seviyesine ulaşılır.

Risklerin Etki ve Olasılık Seviyelerinin Belirlenmesi

Risk seviyelerinin belirlenmesinde dikkate alınan faktörlerden etki, risklerin gerçekleşmesi halinde kurum üzerinde yaratacağı 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 kurum için deprem sonucunda zarar görme riskinin olasılığı düşük olmakla birlikte, riskin gerçekleşmesi durumunda kurum faaliyetleri üzerindeki etkisi çok yüksek seviyede olabilir. Bu nedenle, risk seviyelerinin belirlenmesinde etki ve olasılık faktörleri bir arada değerlendirilir. Etkisi çok yüksek, olasılığı düşük olan riskler kamu idareleri tarafından mutlaka ayrıca takip edilir.

Risklerin etki ve olasılıklarının değerlendirilmesinde, etki için “çok düşük, düşük, orta, yüksek ve çok yüksek”; olasılık için “ihtimal dışı, zayıf olasılık, olası, yüksek olasılık ve neredeyse kesin” olmak üzere beşli kategori kullanılır.

Risk Etki Değerlendirme Skalası

Etki Seviyesi	Etki Kategorisi	AÇIKLAMA
5	Çok Yüksek	Kurumun stratejik amaç ve hedeflerine ulaşamamasına, stratejik amaç ve hedeflerinden ciddi derecede sapmasına veya kurum tarafından sunulan hizmetlerin uzun süre duraklamasına neden olabilecek olay veya durumlar.
4	Yüksek	Kurumun stratejik amaç ve hedeflerinden önemli derecede sapmasına veya kurum tarafından sunulan hizmetlerin önemli bir süre duraklamasına neden olabilecek olay veya durumlar.
3	Orta	Kurumun stratejik amaç ve hedeflerinden kabul edilebilir derecede sapmasına veya kurum tarafından sunulan hizmetlerin belirli bir süre duraklamasına neden olabilecek olay veya durumlar.
2	Hafif	Kurumun stratejik amaç ve hedeflerine ulaşmasında düşük seviyede etkisi olabilecek olay veya durumlar.
1	Çok Hafif	Kurumun stratejik amaç ve hedeflerine ulaşmasında çok düşük kolaylıkla gözlemlenemeyecek seviyede etkisi olabilecek olay veya durumlar.

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

Olasılık Seviyesi	Olasılık Kategorisi	AÇIKLAMA
5	Çok Yüksek (Neredeyse Kesin)	Stratejik amaç ve hedefe ulaşılması öngörülen sürede gerçekleşme olasılığı kesin olan olay ve durumlar.
4	Yüksek (Yüksek Olasılık)	Stratejik amaç ve hedefe ulaşılması öngörülen sürede gerçekleşme olasılığı yüksek olan muhtemel olay ve durumlar.
3	Orta (Olasılık)	Stratejik amaç ve hedefe ulaşılması öngörülen sürede gerçekleşme olasılığı mümkün olan olay ve durumlar.
2	Hafif (Zayıf Olasılık)	Stratejik amaç ve hedefe ulaşılması öngörülen sürede gerçekleşme olasılığı düşük olmakla birlikte imkânsız olmayan olay ve durumlar.
1	Çok Hafif (İhtimal Dışı)	Stratejik amaç ve hedefe ulaşılması öngörülen sürede gerçekleşme olasılığı pek muhtemel olmayan olay ve durumlar.

Risklerin etki ve olasılık seviyeleri ile kurumun mevcut risk yönetimi faaliyetlerinin etkinliği ve yeterliliği dikkate alınarak hesaplanan artık risk seviyesi, aşağıdaki tabloda gösterildiği şekilde 5x5 matris şeklindeki risk haritaları ile ifade edilir:

	OLASILIK				
ETKİ	**1** Çok Düşük	**2** Düşük	**3** Orta	**4** Yüksek	**5** Çok Yüksek
5 Çok Yüksek	**5** Katlanılabilir	**10** Orta	**15** Önemli	**20** Önemli	**25** Katlanılamaz
4 Yüksek	**4** Katlanılabilir	**8** Orta	**12** Orta	**16** Önemli	**20** Önemli
3 Orta	**3** Katlanılabilir	**6** Katlanılabilir	**9** Orta	**12** Orta	**15** Önemli
2 Düşük	**2** Katlanılabilir	**4** Katlanılabilir	**6** Katlanılabilir	**8** Orta	**10** Orta
1 Çok Düşük	**1** Önemsiz	**2** Katlanılabilir	**3** Katlanılabilir	**4** Katlanılabilir	**5** Katlanılabilir

Risklerin Etki ve Olasılık Seviyelerinin Belirlenmesi

Yukarıda belirlenen risklerin etki ve olasılık seviyelerine yönelik değerlendirmeye aşağıda yer verilmektedir:

Riskler	Etki Kategorisi	Etki Seviyesi	Olasılık Kategorisi	Olasılık Seviyesi
Risk 1	Yüksek	4	Çok Yüksek Olasılık	5
Risk 2	Çok Yüksek	5	Olası	3
Risk 3	Orta	3	Olası	3

Risk Seviyesinin Hesaplanması

Belirlenen risklere yönelik risk seviyesi hesaplamaları aşağıda açıklanmaktadır:

Riskler	Etki Kategorisi	Etki Seviyesi	Olasılık Kategorisi	Olasılık Seviyesi	Risk Puanı	Risk Seviyesi
Risk 1	Yüksek	4	Çok Yüksek Olasılık	5	4*5=20	Çok Yüksek
Risk 2	Çok Yüksek	5	Olası	3	5*3=15	Yüksek
Risk 3	Orta	3	Olası	3	3*3=9	Orta

Risk Cevap Matrisi

Risk Seviyesi	Açıklama
Katlanılamaz Risk (25 Puan)	Belirlenen risk kabul edilebilir seviyeye düşürülünceye kadar işe başlanmaz veya yürütülen faaliyet durdurulur. Alınan önlemlere rağmen riski düşürmek mümkün olmuyorsa, faaliyet engellenir.
Önemli Risk (15, 16, 20 Puan)	Belirlenen risk kabul edilebilir seviyeye düşürülünceye kadar faaliyete başlanmaz veya yürütülen faaliyet durdurulur. Risk faaliyetin devam etmesi ile ilgiliyse acil önlem alınmalı ve önlemler sonucunda faaliyetin devamına karar verilmelidir.
Orta Risk (8, 9, 10, 12 Puan)	Belirlenen riskleri düşürmek için kontrol faaliyetlerine başlanmalıdır. Risk azaltmaya yönelik alınacak kontrol yöntemlerine cevap zaman alabilir.
Katlanılabilir Risk (2, 3, 4, 5, 6 Puan)	Belirlenen riskleri ortadan kaldırmak için ek kontrol faaliyetlerine ihtiyaç olmayabilir. Ancak mevcut kontroller sürdürülmeli ve denetlenmelidir.
Önemsiz Risk (1 Puan)	Belirlenen riski ortadan kaldırmaya yönelik kontrol faaliyeti planlamaya ve gerçekleştirilecek faaliyetlerin kayıtlarını saklamaya gerek olmayabilir.

C. RİSKE CEVAP VERME VE KONTROL YÖNTEMLERİNİN BELİRLENMESİ

Kurumsal Risk Yönetimi süreçlerinde; risklere yönelik verilecek cevapların ve söz konusu risklerin nasıl kontrol edileceğine dair yöntemler belirlenmesi de oldukça önemlidir.

Risklere yönelik alınacak kararlar 4 grupta sınıflandırılır:

Riski Kabul Etmek: Riskin gerçekleşmesi halinde kurumun maruz kalabileceği zararlar ile riskin yönetilmesi için katlanılacak maliyetlerin değerlendirilmesi ve değerlendirme sonucunda herhangi bir ilave eylem uygulamamaya karar verilmesidir.

Söz konusu riskin gerçekleşmesi durumunda maruz kalınabilecek zarar, kurumun hedefleri bazında belirlediği risk iştahına göre kabul edilebilir seviyede ise ilave maliyetlere katlanarak riske uygun risk yönetimi faaliyetlerinin uygulanması yerine, riskin kabul edilmesi tercih edilebilir. Örneğin; birimin/kurumun kritik çalışanlara yönelik yedek personel uygulamasının bulunmaması, ilgili çalışanları işten ayrılması durumunda operasyonel aksaklıklara ve kurumsal hafızanın gelişmemesine neden olabilir. Söz konusu riske yönelik önlem olarak kurumun seçimi, yedek personel uygulamasını başlatmak olabilir. Ancak mevcut riskin kabul edilebilir bir seviyede değerlendirilmesi ve yedek personel uygulamasıyla ek maliyetlerin oluşması sebebiyle kurum, yedek personel uygulamasını başlatmak yerine herhangi bir eylem gerçekleştirmemeyi ve riskleri kabul etmeyi seçebilir. Riskin kabul edilmesine karar verildiği durumlarda, risk seviyesinin kabul edilebilir düzeyde kaldığından emin olmak için düzenli olarak izlenmesi gerekir.

Riskten Kaçınmak: Riskin gerçekleşmesi halinde kurumun maruz kalabileceği zararların değerlendirilmesi ve değerlendirme sonucunda riske neden olabilecek olay veya durumlardan kaçınılmasıdır. Kurumun, riskin gerçekleşmesi halinde maruz kalabileceği zararları, kabul edilebilir seviyeye indirgeyecek bir eylem oluşturamadığı durumlarda tercih edilir.

Örneğin; birim/kurum üniversiteye ait tüm verilerin bütünleşik bir sistem üzerinden erişebilmelerini sağlayacak yeni bir teknolojik uygulamaya geçilmesi planlanabilir. Ancak yapılan değerlendirmeler sonucunda, söz konusu uygulamanın kurum için bilgi güvenliği riski doğuracağı ve kurumun bu riski indirgemeye yönelik gerekli eylemleri, kaynak yetersizliği sebebiyle gerçekleştiremeyeceği sonucuna varılabilir. Bu durumda kurum söz konusu uygulamadan vazgeçerek riskten kaçınma yolunu tercih edebilir.

Riski Paylaşmak: Riskin gerçekleşmesi halinde kurumun zarara maruz kalmasına neden olabilecek faaliyetlerin tamamının veya bir kısmının yapılacak sözleşmeler aracılığıyla, kurum dışı uzman kuruluşlara devredilmesidir. Kamu idarelerinin güvenlik, ulaşım vb. faaliyetlerini, konusunda uzman kuruluşlara taşere etmeleri veya büyük çaplı projelerde yüklenici olarak yer almak yerine, yap işlet devret ve benzeri modeller ile bu projelere ait finansal ve operasyonel risklerin projeyi gerçekleştiren şirketlere devretmeleri, riskin transfer edilmesine örnek gösterilebilir.

Riski Kontrol Etmek/Azaltmak: Riskin gerçekleşmesi halinde kurumun maruz kalabileceği zararların risk iştahına göre kabul edilebilir bir düzeye indirilmesi için uygun risk yönetimi faaliyetlerinin belirlenmesi ve uygulanmasıdır. Operasyonel risklerin yönetilmesi amacıyla, kritik iş süreçlerine ilişkin politika ve prosedürlerin hazırlanması ve süreç sahipleriyle paylaşılması riskin

kabul edilebilir düzeye indirilmesi için uygulanan risk yönetimi faaliyetlerine örnek olarak verilebilir.

Riskin indirgenmesi için tanımlanan eylem planı bazı durumlarda birden çok sayıda riski kabul edilebilir seviyeye indirebilir. Örneğin; kurumun tedarikçi performans değerlendirme sürecini devreye alması, hem kurumun ihtiyaç duyduğu malzemelerin zamanında ve beklenen kalitede temin edememesi sonucunda operasyonların aksaması riskini hem de kurumsal kimliğe uymayan tedarikçilerle çalışması sonucunda itibarının olumsuz yönde etkilenmesi riskini yönetmekte kullanılabilir.

Bazı durumlarda ise bir riskin indirgenmesi için birden fazla risk kararının aynı anda alınması ve uygulanması gerekebilir. Örneğin; kurum belgelerinin etkin arşivleme sürecinin bulunmaması sonucu kritik verilerin kaybedilmesi riskine yönelik olarak kurumun hem riskin indirgenmesi (arşiv alanında yangın ikaz ve söndürme sistemlerinin kurulması) hem de riskin transfer edilmesi (özel güvenlik şirketlerinden izleme ve gözetim hizmeti alınması) kararlarını alması ve uygulaması gerekebilir.

Riskin indirgenmesi kararının seçilmesi durumunda, bir sonraki aşamada riskin etki ve olasılığını azaltacak risk yönetimi faaliyetleri tanımlanır. Risk kontrol faaliyetleri, üniversitenin politika, amaç ve hedeflerine ulaşmasını engelleyebilecek riskleri giderebilmek veya kabul edilebilir düzeyde tutmak için belirlenen ve uygulamaya konulan yöntemleri ifade eder.

Risklerin indirgenmesi kapsamında birim/kurum tarafından uygulanacak risk kontrol yöntemleri 4 grupta sınıflandırılır:

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

Düzeltici risk yönetimi faaliyetleri: Gerçekleşmiş olan istenmeyen sonuçların düzeltilmesi için tasarlanan risk yönetimi faaliyetleridir. Bilgi teknolojileri sistemlerine yönelik oluşturulan acil durum eylem planları veya kurtarma programları düzeltici risk yönetimi faaliyetlerine örnek verilebilir.

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

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

Risklere yönelik alınacak kararlar ile risklerin hem etki hem de olasılık seviyeleri azaltılarak, riskin gerçekleşmesi halinde kamu idarelerinin maruz kalabileceği zararların indirgenmesi mümkündür. Örneğin; kurum bilgi teknolojileri envanteri deprem riski taşıyan bir alanda bulunuyorsa, depremin gerçekleşmesi durumunda kurumun karşı karşıya kalacağı veri kaybı riskine yönelik olarak bilgi teknolojileri envanterinin öncelikli deprem bölgesi olmayan bir şehre taşıması riskin olasılık seviyesini azaltırken; kurumun mevcut yerleşkesini depreme dayanıklı hale getirmek üzere gerekli çalışmaları yürütmesi riskin etki seviyesini azaltır.

Risklere Yönelik Alınacak Kararların Belirlenmesine İlişkin Adımlar:

Risklerin Kayıt Altına Alınması: Kurumsal risk yönetimi yaklaşımında, kamu idareleri tarafından risk evreni ile stratejik amaç ve hedeflere ulaşılmasını etkileyebilecek riskler belirlenirken, değerlendirilirken, önceliklendirilirken ve kurumun risklere yönelik alacağı kararlar belirlenirken Risk Değerlendirme ve İzleme Tablosu (Birim/Kurum) kullanılır. Bu formda, riske yönelik alınacak kararlar kaydedilerek gerekli eylemler tanımlanır. Risklerin izlenmesi, kurumsal risk yönetimi uygulamalarının işlerliği ve sürdürülebilirliği ile kurumun strateji ve hedeflerine ulaşabilmesi açısından önemli bir aşamadır. İzleme sürecinin süreklilik sağlayacak şekilde tesis edilmesi ile kurumun, stratejik amaç ve hedeflerine ulaşmasını etkileyebilecek riskler ve etkileri sürekli olarak takip edilir.

Kurum tarafından maruz kalınabilecek riskler, değişen iç ve dış koşullara bağlı olarak zaman içinde değişim gösterebilir veya yeni riskler ortaya çıkabilir. Risk seviyeleri ve önceliklerinde veya kurumun riske yaklaşımı ile risk iştahında değişiklikler olabilir. Daha önce etkin ve etkili olan risk yönetimi faaliyetleri kurum hedefleriyle uyumsuz hale gelebilir, faaliyetler yetersiz kalabilir veya kullanılamaz hale gelebilir, risklere karşı uygulanması kararlaştırılan eylem planları planlandığı gibi uygulanamayabilir. Bu çerçevede Risk Değerlendirme ve İzleme Tablosu (Birim/Kurum) ile yürütülen çalışmalar sürekli olarak gözden geçirilmeli ve gerektiğinde güncellenmelidir.

Kurumsal risk yönetimi yaklaşımını etkileyebilecek ana değişim faktörleri:

Değişen Yönetim ve Süreç Yapısı: Kurumun organizasyon yapısında, faaliyet alanlarında, kullanılan kaynaklarda, yönetim şekli ve kadrosunda meydana gelen değişiklikler kurumsal risk yönetimini etkilemektedir. Örneğin, değişen yönetim kadrosu ile birlikte kurumun stratejik yaklaşımı ve risk iştahı değişime uğrayabilir.

Teknolojik Gelişmeler: Teknolojik yeniliklerin ortaya çıkması ile riske verilen tepkiler ve gerçekleştirilecek eylemler değişebilir. Örneğin; Daha önce manuel olarak kontrol edilen veriler sürecin sistem üzerinde işletilmesi ile sistem tarafından gerçekleştirilen otomatik kontrollere dönüştürülebilir, bu yüzden sistem üzerinde otomatik kontrollerin geliştirilmesi gerekebilir. Daha öncesinde değerlendirilmeye alınmayan bir risk, teknolojik yenilikler ile kritik hale gelebilir. Örneğin, teknolojilerin gelişmesi ve internetin yaygınlaşması sonucu kurumlarda siber güvenlik riski önemli hale gelebilir.

Mevzuat Değişiklikleri ve Ekonomik Gelişmeler: Mevzuat değişiklikleri ve ekonomideki gelişmeler kurumun faaliyetlerine yansıyabilir, bu durumda; kurumun yükümlülükleri artabilir, kurum stratejik amaç ve hedeflerinin yeniden gözden geçirilmesi söz konusu olabilir. Örneğin, Kişisel Verilerin Korunması Kanunun çıkması sonucu kurum bilgi güvenliği konusundaki risklerini gözden geçirebilir ve önceliklerini değiştirebilir.

Kurumun maruz kaldığı risklerin doğru olarak ve zamanında tespit edilmesi için tüm yönetici

ve çalışanlar tarafından kurum içindeki ve kurum dışındaki gelişimlerin ve değişimlerin sürekli izlenmesi ve söz konusu değişikliklerin gerektiğinde yeniden değerlendirmeye alınması gerekir. Belirlenen riskler tasarlandıkları şekilde etkin yönetilemez ise, kurum performansı olumsuz yönde etkilenebilir. Kurum performansının iyileştirilmesi izleme çalışmaları sırasında ortaya çıkan aksaklıkların zamanında giderilmesi, değişen ve gelişen koşullara yönelik gerekli adaptasyonun gerçekleştirilmesi ile mümkündür.

D. RİSKLERİN İZLENMESİ VE RAPORLANMASI

Kurumsal risk yönetiminde, risklerin raporlanması; risk sahipliğinin desteklenmesi ve kurum içerisinde risk kültürünün yaygınlaştırılarak risklerin sistematik bir şekilde izlenmesi için önemli bir aşamadır. Kurumlar etkin ve doğru karar alma mekanizmalarının işletilmesi için etkin bir risk raporlama yapısının kurulması oldukça önemlidir. Risklerin etkin yönetilmesinden kaynaklı, makul seviyede güvence alınması ve hesap verebilirliğin sağlanması için kurumun kritik risklerinin ve söz konusu risklerin mevcut durumlarının periyodik olarak raporlanması gerekir.

Kurum risk yönetimine ilişkin iş ve işlemler oluşturulan çalışma takviminde yer alan izleme ve raporlama süreçleri doğrultusunda gerçekleştirilecektir. İlgili süreç adımlarına aşağıda yer verilmiştir;

- Strateji Geliştirme Daire Başkanlığı tarafından Kurumsal Risk Yönetimi Yönergesinin uygulanmasına yönelik resmi yazının tüm birimlere gönderilmesi,
- Tüm birimlerde birim risk yönetim ekibinin oluşturulması/güncellenmesi,
- Alt birim risk koordinatörü ve birim risk koordinatörü eş güdümü ile risk tespiti toplantılarının yapılması ve toplantı sonuçlarının "Birim Risk Yönetim Ekibine" bildirilmesi,
- "Birim Risk Yönetim Ekibi" tarafından risk tespiti toplantılarının yapılması ve tutanaklarının SGDB'ye gönderilmesi,
- Birimler tarafından tespit edilen risklerin GÜYBİS'e kayıtlanması ve değerlendirilmesi,
- "Birim Risk Yönetim Ekibi" tarafından riske verilen cevaba ilişkin kontrol yöntemlerinin tespit edilmesi ve uygulanması,
- Risklere yönelik izleme ve değerlendirme toplantılarının yapılması, "Üniversite Konsolide Risk Raporunun" taslak olarak hazırlanması,
- Risklerin GÜYBİS üzerinden yeniden değerlendirilmesi,
- "Birim Risk Yönetim Ekibi" tarafından yeniden değerlendirme toplantılarının yapılması ve toplantı sonucunda riskin durumunun yeniden tespit edilmesi,
- "Üniversite Konsolide Risk Raporunun" hazırlanması,
- "Yönetimin Gözden Geçirme (YGG) Toplantısının" gerçekleştirilmesi,
- "Kurumsal Risk Yönetimi 2022-2023 Dönemi Raporunun" yayımlanması.

EKLER

EK-1 Risklerin Belirlenmesine Yönelik Sorular

	Sorular
1	Birimde/Kurumda Misyon, Vizyon ile temel amaç ve hedefler belirlendi mi?
2	Amaç ve hedeflere ulaşmada yaşanılan en büyük engel nedir?
3	Yasa ve mevzuat gibi dış faktörlerde değişimler meydana geldi mi?
4	Son zamanlarda kilit/önemli personel değişikliği yaşandı mı?
5	Geçmiş dönemlerde yüksek oranda personel değişimi oldu mu?
6	İş süreçleri sade ve sıradan mı, yoksa karmaşık ve değişken mi?
7	Çalışma Usul ve esasları ile iş süreçleri yazılı belge haline getiriliyor mu?
8	Diğer birimler benzer amaç ve hedeflerde başarısızlığa uğradı mı?
9	Bilişim sisteminde herhangi bir değişiklik oldu mu?
10	Yeni görevler üstleniliyor mu? Yeniden yapılanmaya gidildi mi?
11	İş süreçlerinde genel bir aksama olursa, acil eylem planı mevcut mu?
12	Geçmiş yıllarda hangi riskler çoğaldı veya azaldı? Neden?
13	Bu durum neden bir risk olarak tasvir edilmektedir?
14	Bu riski anlamak için ilave bir bilgiye ihtiyaç var mıdır?
15	Bu riskin hedeflere ulaşmada neden olumsuz etkisi vardır?
16	İç risklerin ortaya çıkmasına kimler sebep olmuş olabilir?
17	Tespit edilmiş iç risklerin çıkış kaynağı ve temel nedeni nedir?
18	Risklerin neden olacağı olası maliyetler ne kadardır?
19	Üniversite yönetimi hem iç hem dış riskleri dikkate alıyor mu?
20	Risklerin belirlenmesinde iç ve dış paydaşların rolü nelerdir?
21	Ulusal veya küresel salgın olursa işlerin aksaması söz konusu oluyor mu?

EK-2 Risk Etki Değerlendirme Skalası

Etki Seviyesi	Etki Kategorisi	AÇIKLAMA
5	Çok Ciddi	Kurumun stratejik amaç ve hedeflerine ulaşamamasına, stratejik amaç ve hedeflerinden ciddi derecede sapmasına veya kurum tarafından sunulan hizmetlerin uzun süre duraklamasına neden olabilecek olay veya durumlar.
4	Ciddi	Kurumun stratejik amaç ve hedeflerinden önemli derecede sapmasına veya kurum tarafından sunulan hizmetlerin önemli bir süre duraklamasına neden olabilecek olay veya durumlar.
3	Orta	Kurumun stratejik amaç ve hedeflerinden kabul edilebilir derecede sapmasına veya kurum tarafından sunulan hizmetlerin belirli bir süre duraklamasına neden olabilecek olay veya durumlar.
2	Hafif	Kurumun stratejik amaç ve hedeflerine ulaşmasında düşük seviyede etkisi olabilecek olay veya durumlar.
1	Çok Hafif	Kurumun stratejik amaç ve hedeflerine ulaşmasında çok düşük kolaylıkla gözlemlenemeyecek seviyede etkisi olabilecek olay veya durumlar.

EK-3 Risk Olasılık Değerlendirme Skalası

Olasılık Seviyesi	Olasılık Kategorisi	AÇIKLAMA
5	Çok Yüksek (Neredeyse Kesin)	Stratejik amaç ve hedefe ulaşılması öngörülen sürede gerçekleşme olasılığı kesin olan olay ve durumlar.
4	Yüksek (Yüksek Olasılık)	Stratejik amaç ve hedefe ulaşılması öngörülen sürede gerçekleşme olasılığı yüksek olan muhtemel olay ve durumlar.
3	Orta (Olasılık)	Stratejik amaç ve hedefe ulaşılması öngörülen sürede gerçekleşme olasılığı mümkün olan olay ve durumlar.
2	Hafif (Zayıf Olasılık)	Stratejik amaç ve hedefe ulaşılması öngörülen sürede gerçekleşme olasılığı düşük olmakla birlikte imkansız olmayan olay ve durumlar.
1	Çok Hafif (İhtimal Dışı)	Stratejik amaç ve hedefe ulaşılması öngörülen sürede gerçekleşme olasılığı pek muhtemel olmayan olay ve durumlar.

EK-4 Risk Matrisi

	OLASILIK				
ETKİ	**1** Çok Düşük	**2** Düşük	**3** Orta	**4** Yüksek	**5** Çok Yüksek
5 Çok Yüksek	**5** Katlanılabilir	**10** Orta	**15** Önemli	**20** Önemli	**25** Katlanılamaz
4 Yüksek	**4** Katlanılabilir	**8** Orta	**12** Orta	**16** Önemli	**20** Önemli
3 Orta	**3** Katlanılabilir	**6** Katlanılabilir	**9** Orta	**12** Orta	**15** Önemli
2 Düşük	**2** Katlanılabilir	**4** Katlanılabilir	**6** Katlanılabilir	**8** Orta	**10** Orta
1 Çok Düşük	**1** Önemsiz	**2** Katlanılabilir	**3** Katlanılabilir	**4** Katlanılabilir	**5** Katlanılabilir

EK-5 Risk Cevap Matrisi

RİSK SEVİYESİ	AÇIKLAMA
Katlanılamaz Risk (25 Puan)	Belirlenen risk kabul edilebilir seviyeye düşürülünceye kadar işe başlanmaz veya yürütülen faaliyet durdurulur. Alınan önlemlere rağmen riski düşürmek mümkün olmuyorsa, faaliyet engellenir.
Önemli Risk (15, 16, 20 Puan)	Belirlenen risk kabul edilebilir seviyeye düşürülünceye kadar faaliyete başlanmaz veya yürütülen faaliyet durdurulur. Risk faaliyetin devam etmesi ile ilgiliyse acil önlem alınmalı ve önlemler sonucunda faaliyetin devamına karar verilmelidir.
Orta Risk (8, 9, 10, 12 Puan)	Belirlenen riskleri düşürmek için kontrol faaliyetlerine başlanmalıdır. Risk azaltmaya yönelik alınacak kontrol yöntemlerine cevap zaman alabilir.
Katlanılabilir Risk (2, 3, 4, 5, 6 Puan)	Belirlenen riskleri ortadan kaldırmak için ek kontrol faaliyetlerine ihtiyaç olmayabilir. Ancak mevcut kontroller sürdürülmeli ve denetlenmelidir.
Önemsiz Risk (1 Puan)	Belirlenen riski ortadan kaldırmaya yönelik kontrol faaliyeti planlamaya ve gerçekleştirilecek faaliyetlerin kayıtlarını saklamaya gerek olmayabilir.

EK-6 Risk Değerlendirme ve İzleme Tablosu (Birim/Kurum)

1	2	3	4	5	6	7	8	9				10				11	12	6	7	8	13		14
S.N.	Risk Türü	Risk Kaynağı	İlişkili Olduğu Stratejik Hedef	Tespit Edilen Risk ve Sebebi	RİSKİN			RİSK CEVABI				RİSKİN KONTROLÜ				RİSKİN SAHİBİ	YENİDEN DEĞERLENDİRME TARİHİ	RİSKİN			RİSKİN DURUMU		AÇIKLAMA
					Etkisi	Olasılığı	Puan	Kabul Edilebilir	Kaçınılabilir	Paylaşılabilir	Kontrol Edilebilir	Önleyici Kontrol	Düzeltici Kontrol	Yönlendirici Kontrol	Saptayıcı Kontrol			Etkisi	Olasılığı	Puanı	Kontrol Altında	Ek Kontrol İhtiyacı	
1				RİSK: SEBEBİ																			
2				RİSK: SEBEBİ:																			
3				RİSK: SEBEBİ:																			
4				RİSK: SEBEBİ:																			
5				RİSK: SEBEBİ:																			

Tabloyu Dolduran **İdare/Birim/Alt Birim Koordinatörü/Çalışan Adı**		**Tarih**		**İmza**	

Risk Değerlendirme ve İzleme Tablosu Sütunlarının Açıklaması

S.N.	SÜTUN TANIMLAMALARI	DOLDURMAYA YETKİLİ OLAN GÖREVLİ KİŞİ/EKİP/KURUL
1	**Sıra No:** Risk kaydındaki sıralamayı gösterir.	Çalışan, Birim Risk Yönetim Ekibi, Alt Birim Risk Koordinatörü, Birim Risk Koordinatörü, İdare Risk Koordinatörü, İKİYK.
2	**Risk Türü**: Madde 18'de tanımlanan risk türlerini gösterir	
3	**Risk Kaynağı:** Riskin iç ve dış kaynaklı olup olmadığını gösterir. (İç Risk için (İ), Dış Risk için (D)	
4	**İlişkili Olduğu Stratejik Hedef**: Üniversitenin stratejik hedefleriyle doğrudan veya dolaylı bağlantılı ve riskten etkilenecek olan hedef bu sütuna yazılır. (H.1.1) (H.3.3 gibi) Stratejik hedeflerle ilişkili olmadığı değerlendirilen riskler bu sütunda işaretlenmez.	
5	**Tespit Edilen Risk ve Sebebi:** Tespit edilen riskler yazılır, Sebep: Bu riskin ortaya çıkmasına neden olan sebepler belirtilir.	
6	**Etki:** Katılımcıların verdikleri puanların aritmetik ortalaması alınarak riskin (ortalama) etki puanı bulunur.	Birim Risk Yönetim Ekibi, Alt Birim Risk Koordinatörü, Birim Risk Koordinatörü, İdare Risk Koordinatörü, İKİYK.
7	**Olasılık:** Katılımcıların verdikleri puanların aritmetik ortalaması alınarak riskin (ortalama) olasılık puanı bulunur.	
8	**Risk Puanı:** Etki puanı(ortalama) ile olasılık puanı (ortalama) çarpılarak Risk Puanı bulunur.	
9	**Risk Cevabı:** Madde 21'de tanımlanan gruplardan hangisi olduğunu gösterir.	
10	**Riskin Kontrolü:** Madde 22'de tanımlanan kontrol yöntemlerinim hangisi olduğunu gösterir.	
11	**Riskin Sahibi:** Riskin yönetilmesinden ve izlenmesinden sorumlu olan kişidir.	
12	**Riskin Yeniden Değerlendirme Tarihi:** Önceden belirlenen riskin kontrol altına alınmasından sonra yeniden değerlendirilme tarihini gösterir.	
13	**Riskin Durumu:** Riskin yeniden değerlendirmeden sonraki durumunu gösterir.	
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.	

EK-7 Risk İştahı Tablosu

Değerlendirilecek Faaliyet Alanları	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	1	2	3	4	5
Kalite Güvencesi Sistemi Faaliyetleri					
Eğitim ve Öğretim Faaliyetleri					
Araştırma ve Geliştirme Faaliyetleri					
Toplumsal Katkı Faaliyetleri					
Uluslararasılaşma Faaliyetleri					
Yönetim Sistemi Faaliyetleri					
Sosyal ve Kültürel Faaliyetler					
İş Sağlığı ve Güvenliği Faaliyetleri					
Bilgi Güvenliği Faaliyetleri					
Bütçe Yönetimi Faaliyetleri					
Paydaşlarla ilişkiler					
Taşınır ve Taşınmaz Yönetimi Faaliyetleri					
Kurumsal İtibar ve Algı					
Yasal Faktörler					
Operasyonel Faktörler					
Kampüs Güvenliği					

EK-8 Birim Çalışanları Risk Öneri Formu

S.N.	**RİSK TÜRÜ** • Stratejilerle İlişkili Risk • Finansal Risk • Yasal Uyum Riski • Çevresel Risk • Operasyonel Risk • İtibar ve Raporlama Riski	**RİSK KAYNAĞI** • İç Risk • Dış Risk	**TESPİT EDİLEN RİSKİN SEBEBİ** (…….. …….. ……. ……. ……. …….. sebebiyle)	**TESPİT EDİLEN RİSK** (…… ……nin oluşması riski)
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

<u>Risk Önerisinde Bulunan Çalışanın;</u>

Adı ve Soyadı :

Unvanı :

İmzası :