T.C.
İSTANBUL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANABİLİM DALI
MUHASEBE BİLİM DALI

YÜKSEK LİSANS TEZİ

KURUMSAL RİSK YÖNETİMİ: BİR UYGULAMA

Sezayi AKSOY
2501920033

TEZ DANIŞMANI
Prof. Dr. F. Lerzan KAVUT

İSTANBUL - 2019

T.C.
İSTANBUL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

YÜKSEK LİSANS
TEZ ONAYI

ÖĞRENCİNİN;

Adı ve Soyadı	: SEZAYİ AKSOY	Numarası	: 2501920033
Anabilim Dalı / Anasanat Dalı / Programı	: MUHASEBE	Danışmanı	: PROF.DR.FATMA LERZAN KAVUT
Tez Savunma Tarihi	: 01.08.2019	Saati	: 11.30
Tez Başlığı	: KURUMSAL RİSK YONETİMİ: BİR UYGULAMA		

TEZ SAVUNMA SINAVI, İÜ Lisansüstü Eğitim-Öğretim Yönetmeliği'nin 36. Maddesi uyarınca yapılmış, sorulan sorulara alınan cevaplar sonunda adayın tezinin KABULÜNE OYBİRLİĞİ / ~~OYÇOKLUĞUYLA~~ karar verilmiştir.

JÜRİ ÜYESİ	İMZA	KANAATİ (KABUL / RED / DÜZELTME)
PROF.DR.FATMA LERZAN KAVUT		KABUL
PROF.DR.FATMA PAMUKÇU		KABUL
DOÇ.DR.NERGİS NALAN YAKAR		KABUL

YEDEK JÜRİ ÜYESİ	İMZA	KANAATİ (KABUL / RED / DÜZELTME)
DOÇ.DR.AYÇA ZEYNEP SÜER		
DOÇ.DR.AYÇA AKARÇAY ÖĞÜZ		

ÖZ

KURUMSAL RİSK YÖNETİMİ: BİR UYGULAMA
SEZAYİ AKSOY

Tez çalışması, üretim işletmelerinde kurumsal risk yönetimi yeteneği kazanılması amacıyla, şirkete özgü bir kurumsal risk yönetim modelinin, uyarlanması, uygulanması ve sonuçlarının ölçülmesi safhalarının örnek uygulama eşliğinde somut olarak ortaya koyulmasını kapsamaktadır.

Bu kapsamda, ekonominin bileşenleri, risk-fırsat kavramları, iç kontrol, risk yönetimi, kurumsal yönetim, iç denetim kavramları değerlendirilmiştir. Uluslararası Standart Belirleme Organizasyonu (International Organization for Standardization-ISO) Kurumsal Risk Yönetim Prensipleri, Treadway Komisyonu Himaye Örgütleri Komitesi (Comitee of Sponsoring Organizations of the Treadway-COSO), İç Kontrol Entegre Çerçevesi (COSO Internal Control- Integrated Framework-COSO İç Kontrol Sistemi), COSO'nun 2004 yılında yayınlanmış olan Kurumsal Risk Yönetimi –Entegre Çerçevesi (COSO KRY-2004), COSO Enterprise Risk Management- Integrated Framework (COSO ERM-2004) ve Haziran 2017'de güncellenen Kurumsal Risk Yönetimi-Strateji ve Performansa Entegre Çerçeve (COSO KRY-2017), Enterprise Risk Management-Integrating with Strategy and Performance (COSO ERM-2017) bileşenleri incelenmiştir. İncelenen model ve yaklaşımlardan hareketle, bir üretim şirketi için, şirketin ihtiyaçlarına uygun, özgün bir kurumsal risk yönetim çerçevesi oluşturulması konusunda çalışılmıştır.

Kurumsal risk yönetimi çerçevesinin oluşturulması ve geliştirilmesi projesinde, proje fizibilitesi eşliğinde üst yönetim desteğinin alınması gerekmektedir. Şirket içinde ortak bir risk-fırsat algısı ve terminoloji yaratılması, stratejik hedeflerin güncellenmesi, organizasyon yapısının, iç kontrol uygulamalarının, COSO İç Kontrol Entegre Çerçevesi prensipleri ve COSO KRY-2017 çerçevesi bileşenleri ele alınarak, risk ve fırsatlarla ilgili, tanımlama, planlama,

ölçme, yönetme esaslarının şirket yapısına uygun olarak oluşturulması, oluşturulan çerçevenin etkinliğinin iç denetim aracılığı ile ölçülmesi ve izlenmesi ele alınmıştır.

Sonuç olarak, risk yönetim fonksiyonunun şirketlerde bir rekabet avantajına dönüşecek yetkinlikte çalıştırılması ile ilgili, ağırlıklı olarak COSO İç Kontrol Entegre Çerçevesi prensipleri ve COSO KRY-2017 bileşenleri esas alınarak, bir üretim şirketinde Kurumsal Risk Yönetimi Çerçevesi (KRY) oluşturulması gerçekleştirilmiştir.

Anahtar Kelimeler: İç denetim, kurumsal yönetim, kurumsal risk yönetimi, COSO, iç kontrol.

ABSTRACT

ENTERPRISE RISK MANAGEMENT: AN IMPLEMENTATION

SEZAYİ AKSOY

The scope of the thesis is to build up an enterprise risk management approach, implement a risk management model for the sample production company, and measure, monitor and communicate the results for a perceptible guidance to support the companies to improve their risk management capabilities.

Within the defined scope, by considering today's economic and social life dynamics, the risk-opportunity concepts, internal control, risk management, governance, internal audit disciplines have been focused. After investigation of ISO Enterprise Risk Management principles, COSO Internal Control-Integrated Framework (COSO Internal Control) , COSO ERM-2004 and COSO ERM-2017, it is decided to work on the implementation of the risk management model for a sample production company with the reference of COSO Internal Control and COSO ERM-2017.

During the implementation process of the risk management model, having the sponsorship of the top management with the help of a sufficient feasibility, building up a common risk-opportunity terminology and increasing the awareness within the organization have been prioritized. The steps of updating the strategic goals, restructuring the organization, revision of the internal control tools in line with COSO Internal Control and COSO ERM-2017 requirements, applying to COSO ERM-2017 components and principals for a proper risk management function and control the effectiveness of the model with the help of Internal Audit have been followed.

As a result, being the risk management function a competitive advantage for the corporates, we presented a unique implementation approach of a

risk management model for a production company with the reference of COSO ERM-2017 and COSO Internal Control.

Keywords : Internal audit, corporate governance, enterprise risk management, COSO, internal control.

ÖNSÖZ

Ticari faaliyetlerin konusu, ihtiyaçları karşılayacak ve problemleri çözecek değerler yaratmak, bu değerleri ekonomik açıdan ölçeklendirerek ticari kazanç elde etmek ve bu durumu sürdürülebilir kılmaktır. Yatırımcılar da makul ekonomik kazanç beklentisi ile söz konusu faaliyetlerde ihtiyaç duyulan kaynakları tahsis edenler olarak tanımlanabilir.

Günümüz koşullarında ticari faaliyetlerde bulunurken karşılaşılan kaynak ihtiyacı, gelişen ve öncelik kazanan çevre ve sosyal sorumluluk olguları, enerji kaynakları ile ilgili zorluklar, finansal araçların karmaşık yapıları, küresel sermaye hareketleri, teknolojinin ulaştığı nokta, dijital dünyanın hızı, bilgi erişilebilirliği, yasal ve politik değişiklik ve düzenlemeler, yatırımcı profili ve beklentileri, rekabet düzeyi vb. içsel ve dışsal faktörlerdeki hızlı ve sürekli değişimin ortaya çıkardığı risk ve fırsatların zamanında anlaşılması, şirketin stratejilerine uygun olarak değerlendirilmesi ve yönetilmesi sürdürülebilirlik açısından çok önemli bir gereklilik halini almıştır. Risk yönetimi fonksiyonunun önemi ve önceliği ivmelenerek artmakta, kurumlar açısından risk yönetimi yeteneğinin geliştirilmesi çok belirleyici bir rekabet avantajı halini almaktadır.

Bu tez çalışmasında, ticari faaliyette bulunan işletmelerin kurumsal risk yönetimi yeteneğinin geliştirilmesi ile ilgili olarak, ISO Kurumsal Risk Yönetimi Prensipleri, güncellenmiş COSO İç Kontrol-Entegre Çerçevesi ve COSO KRY-2017 incelenip, kurumsal risk yönetim yetkinliği kazanmak isteyen işletmelere ışık tutması açısından örnek üretim şirketinde kurumsal risk yönetimi çerçevesinin oluşturulması gerçekleştirilmiştir.

SEZAYİ AKSOY
İSTANBUL, 2019

İÇİNDEKİLER

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR LİSTESİ

AAA : American Accounting Association (Amerikan Muhasebe Derneği)

ABC-KRY : ABC Kimya San. A.Ş. Kurumsal Risk Yönetimi Projesi

AICPA : American Institute of Certified Public Accountants (Amerikan Sertifikalı Mali Müşavirler Enstitüsü)

BBDK : Bankacılık Düzenleme ve Denetleme Kurumu

COSO : Comitee of Sponsoring Organizations of The Treadway Commission (Treadway Komisyonu Himaye Örgütleri Komitesi)

COSO ERM : COSO Enterprise Risk Management (COSO Kurumsal Risk Yönetimi)

COSO ERM-2004 : COSO Enterprise Risk Management – Integrated Framework

COSO ERM-2017 : COSO Enterprise Risk Management- Integrating with Strategy and Performance

COSO Internal Control : COSO Internal Control-Integrated Frameworl

COSO İç Kontrol Sistemi : COSO İç Kontrol-Entegre Çerçevesi

COSO KRY : COSO Kurumsal Risk Yönetimi

COSO KRY-2004 : COSO Kurumsal Risk Yönetimi-Entegre Çerçeve

COSO KRY-2017 : COSO Kurumsal Risk Yönetimi- Strateji ve Başarıya Entegre Çerçeve

ERM : Enterprise Risk Management (Kurumsal Risk Yönetimi)

FEI : Financial Executives International (Finans Yöneticileri Enstitüsü)

IIA : Institute of Internal Auditors (İç Denetçiler Enstitüsü)

IMA : Institude of Management Accountants (Yönetim Muhasebecileri Enstitüsü)

ISO	: International Organization For Standardization (Uluslararası Standart Belirleme Organizasyonu)
IT	: Information Technologies (Bilgi Teknolojileri)
KRY	: Kurumsal Risk Yönetimi
SPK	: Sermaye Piyasası Kurulu
TTK	: Türk Ticaret Kanunu
UMUÇ	: Uluslararası Mesleki Uygulama Çerçevesi
YK	: Yönetim Kurulu

GİRİŞ

Tarihte takasla başlayan ticari hayat, günümüzde çok karmaşık ilişkiler, sermaye yapıları, varlık/değer hareketleri, süreçler ve işleyişlerden oluşan iş modellerine dönüşmüş olup, ivme kazanan bir hızla değişim ve gelişimini sürdürmektedir. Burada önemli iki kavram; **işleyişler/süreçler** ve **değişim** olarak ele alınmıştır.

Bir iş sürecinin olduğu her yerde bir kontrol davranışından bahsetmek gerekir. Şirketlerde tekrar eden, bir ekip tarafından yürütülen, yönetilen iş süreçlerinden söz ettiğimiz her durumda ve her örgüt yapısında bu süreçlerin kontrollerinden de söz edilir. Bahsi geçen kontrol süreçleri, bazı hallerde kurgulanmamış düzenlenmemiş ve belgelenmiş olmakla birlikte, deneyimler sonucu geliştirilmiş davranışlar ve yaklaşımlar olarak karşımıza çıkabilir. Bazı hallerde kurgulanarak ortaya koyulmuş, ilgili taraflarla iletişimi yapılmış ve sürekliliği, sürdürülebilirliği sağlanmış bir sistem olabilir.

Kurum yöneticilerinden genel beklentinin, süreçleri tarif etmeleri, tasarlamaları ve/veya konu uzmanları tarafından tasarlanmış süreçler meydana getirmeleri, bu süreçlerin çalıştırılması ve yönetilmesiyle iş sonuçlarının hedeflendiği gibi alınmasını sağlamaları ve bu davranışı sürdürmeleridir. Ekonomik beklentiler çerçevesinde modellenmiş ticari faaliyetlerle ilgili süreçler değiştikçe kontrol davranışlarının da etkinliğini koruyacak ve/veya arttıracak biçimde değişmesi gerekmektedir. Bu sağlanmadığı taktirde kurumda kontrol davranışının etkinliği korunamaz, oluşan kontrol körlükleri (ilizyonlar) kurum ve süreçler için büyük risk oluşturur.

> *"Uluslararası denetim terminolojisinde "kontrol" kavramı tamamlanan, sonuçlanan bir işin sonradan başka biri tarafından kontrol edilmesinden ziyade planlamadan, uygulamaya ve sonuçlandırmaya kadar sürecin tamamını kontrol altında tutmayı amaçlayan tüm işlem akışı içine*

giydirilmiş sistematik bir davranış olarak düşünülmektedir." [1]

Değişimin ticari beklenti ve hedefler üzerindeki olası etkileri iş modeli ve süreçler açısından risk olarak değerlendirilebilir. Burada risk, hedeflerin gerçekleştirilmesine olumsuz etki edebilecek olayları çağrıştırmakla birlikte İç Denetçiler Enstitüsü (Institute of Internal Auditors - IIA) Standartları açısından risk şöyle tanımlanmaktadır:

"*Risk, kurum hedeflerine ulaşılması konusunda sonuçları etkileyecek bir olayın meydana gelme olasılığıdır*." [2] Çalışmamızın bütününde risk IIA tanımı kapsamında ele alınacak ve risk/fırsat beraber düşünülecektir.

Ekonomik ve sosyal hayatın gerektirdiği iletişim karmaşıktır. Kontrol ve risk yönetimi süreçleri, yürütülen faaliyetin doğası gereği hayatımıza girmiştir. Karmaşık ekonomik faaliyetler, hızlı değişen, çok çeşitli varlık ve kaynaklar, işletmelerin çevreleri ve menfaat sahipleri ile etkileşimleri iletişim biçimi ve kalitesini çok önemli kılmıştır. Bu durum, sürdürülen iletişimin yasa ve kural koyucular tarafından düzenlenmesi ve belli kural ve standartlara bağlanması sonucunu getirmiştir.

Şirketin hedef ve amaçlarını gerçekleştirmek için oluşturulması gereken süreçlerin tamamı kurumsal yönetim olarak adlandırılır.

"Kurumsallaşma; en genel ifadeyle işletmelerin "devamlılık" gayelerinin, birey ya da bireylerin kişisel tasarruflarından kurtulması şeklinde tanımlanabilir. Burada önemli olan husus; işletme faaliyetlerine devam edebilmesi adına herhangi bir kişi ya da kişilere mutlak surette bağlılık

[1] Çetin Özbek, **İç Denetim:Kurumsal Yönetim:Risk Yönetimi:İç Kontrol**, 2 c.,İstanbul, Türkiye İç Denetim Enstitüsü, Ekim 2012, s. 137.
[2] The Institute of Internal Auditors, **IIA Position Paper: The Role of Internal Auditing In Enterprise-Wide Risk Management,** The Institute of Internal Auditors, January 2009, s.7.

duyulmamasıdır." [3]

> *"Yönetim kurulunca kurum hedeflerinin gerçekleştirilmesi için oluşturulan organizasyonel yapı, operasyonel ve yönetsel fonksiyonlar arasındaki ilişkiler, yetki ve sorumluluk dağılımı, raporlama ilişkileri, kurumun sahip olduğu varlıklar ve kaynaklar, kurumun içinde faaliyette bulunduğu ekonomik ve yasal ortam kurumsal yönetimin unsurlarıdır."* [4]

Değişen sosyo ekonomik ihtiyaçlar, ekonomik faaliyetlerdeki değişim, kurumsal yönetim, risk yönetimi ve iç kontrol süreçlerini doğurmuş ve geliştirmiştir. Bu süreçlerin, hedeflenen ticari sonuçlara varma konusunda makul bir güvence sağlaması için etkili çalıştırılması, sürdürülebilir kılınması iç denetimin konusu olarak ele alınmaktadır.

Çağdaş anlamlarıyla kurumsal yönetim, risk yönetimi ve iç kontrol süreçlerinin etkinliği konusunda **makul düzeyde güvence vermek,** bu durumu sürdürülebilir kılmak ve belirtilen çerçevede talep edilen kapsamda **danışmanlık hizmeti vermek** iç denetimin iki temel unsurunu oluşturulmaktadır.

Günümüzde, şirket yönetimleri ve yönetim kurullarına çevreleri, hissedarları, tüketiciler, çalışanları ve kamuoyu ile iletişimlerinde çeşitli görev ve sorumluluklar verilmiştir. Yasal düzenlemelerin yanı sıra, şirketlerin ilişki içinde olduğu bütün ekonomik çevrelerle yürüttükleri etkileşim şeffaf, ve etkili bir iletişimi gerektirir.

Bu yönde farklılaşan şirketler bunu rekabet avantajına dönüştürmenin yollarını bulmaktadır (kontrol altındaki süreçler, gerçekleşen ekonomik hedefler, verimlilik, etkili ve başarılı iletişim, artan yatırımcı ilgisi, iyi yönetilen kamuoyu algısı vb.). Bir rekabet avantajı konusu olması sebebi ile şirketlerin bu konulara olan

---

[3] Hasan Türedi, Gencay Karakaya, Mehmet İldem, "Kurumsal Yönetim ve İç Denetim İlişkisi", **Sayıştay Dergisi,** No:96, 2015, s.56
[4] Özbek, **İç Denetim,** s.113.

ilgisi her geçen gün artarken ve bu konularda yürütülen çalışmaların kapsamı her geçen gün genişlerken, yapılan yasal düzenlemeler de bu gelişmeleri hızlandırmaktadır.

Bu çalışmada, Kurumsal Risk Yönetimi (KRY) süreci ve bir üretim şirketinde KRY sürecinin oluşturulması, uygulanması konusu incelenmiştir. Bu çerçevede, çalışmanın birinci bölümünde iç kontrol kavramı ile birlikte, COSO İç Kontrol Sistemi prensipleri ve bileşenleri incelenmiş olup, ikinci bölümde KRY kavramı, Uluslararası Standart Belirleme Organizasyonu (International Organization for Standardization - ISO) KRY prensipleri, COSO KRY çerçeveleri bileşenleri, KRY açısından iç denetimin rolü ve katkıları incelenmiştir. Üçüncü bölümde örnek bir üretim şirketi için KRY sisteminin kurulması ve uygulanması ele alınmıştır. KRY sisteminin kurulmasında, ISO KRY prensiplerinden ziyade COSO KRY çerçeveleri bileşenlerinin kuruma uyarlanması üzerinde çalışılmıştır. KRY sonuçlarının değerlendirilmesi ile ilgili mevcut iç denetim faaliyeti kurum için tasarlanan KRY sistemi ihtiyaçlarına uygun hale getirilmiş, iç denetim fonksiyonu işler hale getirilerek işletme uygulaması tamamlanmıştır.

BİRİNCİ BÖLÜM
İÇ KONTROL

1.1. İç Kontrol Kapsam ve Çerçevesi

İç kontrol kavramı tarihsel süreçte parasal hareketlerin kontrolü, usulsüzlük ve yolsuzlukların engellenmesi odaklı gelişmiştir. Genel olarak, yaşanan problemler ve sorunlardan sonra, benzerlerinin tekrarını engellemeye yönelik düzenlemeler ve tedbirler kapsamında kuramsal ve yasal gelişim göstermiştir. Yaşanan finansal raporlama skandalları, standart yapıcı kurumların ve meslek odalarının örgütlenme düzeyi, ekonomi bileşenlerinin çeşitliliği, yatırımcı ve sermaye hareketlerinin derinliği gibi özelliklerinden dolayı iç kontrol konusunda Amerika Birleşik Devletleri'nde ortaya çıkan gelişim ve düzenlemeler dünyaya ışık tutmuş ve öncülük etmiştir.

> *"1980'lerde Amerika Birleşik Devletleri'nde yaşanan finansal raporlama skandalları sonucu beş profesyonel organizasyon bir araya gelerek Committe of Sponsoring Organizations of the Treadway Commission (COSO) kurdular."* [1]

IIA, Amerikan Sertifikalı Mali Müşavirler Enstitüsü, İngilizce adı ile American Institute of Certified Public Accountants (AICPA), Amerikan Muhasebe Derneği, İngilizce adı ile American Accounting Association (AAA), Yönetim Muhasebecileri Enstitüsü, İngilizce adı ile Institute of Management Accountants (IMA) ve Finans Yöneticileri Enstitüsü, İngilizce adı ile Financial Executives International (FEI)' den oluşan beş bağımsız kurumun liderliğinde oluşturulan COSO, iç kontrol bileşenlerini, unsurlarını ve tanımları bir model olarak ele aldığı, 1992 yılında "Internal Control-Integrated Framework (İç Kontrol-Entegre Sistemi)" dökümanını yayınlayarak o güne kadar hazırlanmış en kapsamlı iç kontrol modelini

[1] The Institute of Internal Auditors, **Sawyer's Guide For Internal Auditors**,3 c.,6. bs., The Institute of Internal Auditors Research Foundation, 2012, s.36.

ortaya koymuştur. İlgili model 2013 yılında güncellenmiş olup, dünyada en geniş kabul gören iç kontrol kapsam ve çerçevesini belirlemektedir.

COSO İç Kontrol-Entegre Sistemi (COSO İç Kontrol Sistemi) yanı sıra IIA' nın 2008 yılında yayınladığı ve 2012 yılında güncellediği "İç Denetim Standartlarında" (IIA Standartları) kontrol fonksiyonu, kontrol ortamı ve kontrol süreci kavramları ele alınmıştır. IIA Standartları ortaya bir iç kontrol modeli koymaktan ziyade, iç denetim faaliyetinin iç kontrol fonksiyonu ile ilişkisini belirleme konusunda ve iç denetim faaliyetinin standartlarını belirleme konusunda temel kaynak olarak değerlendirilmektedir. İç denetim faaliyetinin kontrol fonksiyonu ile ilişkisini ortaya koyarken, kontrol kavramı ile ilgili yapılan tanımlama ve değerlendirmelerde COSO' dan çok daha dar bir çerçevede kalmıştır.

IIA Standartlarında kontrol, riskleri yönetmek, ortaya koyulmuş hedef ve amaçların gerçekleştirilme olasılığını arttırmak için şirket üst yönetim ve yönetimi tarafından atılacak her türlü adım olarak tanımlanmakta, kurum yönetiminin hedef ve amaçların gerçekleştirilmesine makul ölçüde güvence teşkil edecek yeterlilikteki eylemleri planlayıp, organize edip, yönlendireceği belirtilmektedir.[2] Yine IIA Standartlarında kontrol ortamı, kontrol fonksiyonunun organizasyondaki etkisi ile ilgili şirket üst yönetimi ve yönetimce ortaya koyulacak yaklaşım ve eylemler olarak görülmekte olup, iç kontrolün hedeflerinin yerine getirilmesini sağlayacak yapı ve disiplin olarak değerlendirilmekte, kontrol prosesi ise " kurum risklerinin arzu edilen seviyede olmasını sağlamak için tasarlanmış ve uygulanan, kontrol sisteminin parçası olmuş, politika, prosedür ve eylemler" olarak tanımlanmaktadır.[3]

[2] IIA, **International Standards for The Professional Practice of Internal Auditing (Standards),** The Institute of Internal Auditors, 2012, s.20.
[3] A.e

COSO İç Kontrol Sistemi ile anlaşılması gereken Mayıs 2013 tarihinde güncellenmiş COSO İç Kontrol-Entegre Sistemidir. Bu sistemde iç kontrol aşağıdaki gibi tanımlanmaktadır.[4]

> *"İç kontrol, bir kurumun yönetim kurulu, yönetim kadrosu ve diğer çalışanları tarafından uygulanan, operasyonla, raporlama ile ve mevzuata uyumla ilgili hedeflerinin başarılmasının makul ölçüde güvence altına alınması için tasarlanmış bir süreçtir"*

COSO yaklaşımında aşağıdaki unsurların altını çizmekte fayda bulunmaktadır; iç kontrol ile sağlanması hedeflenen güvence makul bir güvencedir, mutlak güvence değildir, iç kontrol faaliyeti iç denetçilerin veya kontrol eden otoritenin değil, yönetim kurulundan kurumun organizasyon hiyerarşisindeki en alt kademeli çalışanına kadar her kesimin sorumlu olduğu, odağında "insan" olan bir süreçtir. Anlık bir performansla ilgilenmez, yukarıda bahsedilen üç genel hedefin yerine getirilmesi ile ilgili makul bir güvence arar. Buradaki kontrol kavramı yapılanı kontrol etmekten ziyade bir süreci kontrol altında tutmaya yöneliktir. Bu çerçevesi ile, örnek işletmede bir risk yönetim modeli geliştirilirken, güncellenmiş COSO İç Kontrol Sistemi'nden yararlanılmıştır.

1.2. COSO İç Kontrol Sistemi

COSO İç Kontrol Sisteminde, iç kontrol bir **süreç** olarak değerlendirilmekte, hedeflerin **başarılmasına yönelik** olduğu, bir anla ilgili olmayıp **devamlılık** içerdiği, politika ve prosedürlerden ziyade **insanlar tarafından** organizasyonun her noktasında gerçekleştirilen uygulamalar olduğu, hedeflerin başarılmasına ilişkin üst yönetim ve yönetim kademesine yönelik **makul bir güvence** peşinde olduğu, **kurum yapısına uyarlanabilir** esneklikte bir uygulama olması gerektiği temel kavramlar olarak vurgulanmaktadır.

[4] COSO, **Executive Summary Internal Control-Integrated Framework,** May 2013, s.3 (Çevrimiçi) http//www.coso.org, 19 Şubat 2016.

1.2.1. COSO İç Kontrol Sistemi Hedefler, Bileşenler ve Prensiplerin İlişkisi

1.2.1.1. Hedefler

Kurumlar yatırımcıları ve ekonomik ilişki içinde oldukları tarafların ekonomik beklentilerine yönelik değer yaratmak ve bu durumu sürdürülebilir kılmak için stratejileri paralelinde hedefler belirlemekte ve bunları gerçekleştirmek için çalışmaktadırlar. Strateji ve hedefler kurum çalışanları tarafından anlaşılacak detayda belirlenmiş, izlenebilir ve ölçülebilir kılınmış olmalıdır. COSO İç Kontrol Sistemi, kurum hedeflerini operasyonel hedefler, raporlama hedefleri ve uyum ile ilgili hedefler olmak üzere üç ana kategoride gruplamaktadır.

Operasyonel hedefler: Kurumun operasyonları ile ilgili hedeflerdir. Operasyonel ve finansal performans ve amaçlarını, varlıkların korunmasına yönelik hedefleri kapsamaktadır.

Raporlama hedefleri: Finansal ve finansal olmayan kurum içi ve dışına yapılan raporlamalarla ilgilidir. Güvenilir, zamanlı, şeffaf, standart yapıcılar, kurum politikaları, ve diğer kural koyucuların beklentilerine uygun raporlama konularında hedefleri kapsamaktadır.

Mevzuata uygunluk hedefleri: Yasal düzenleme ve kurallara uyumla ilgili hedefleri kapsamaktadır.

1.2.1.2. Bileşenler ve Prensipler

COSO İç Kontrol Sistemi'nin beş ana bileşeni bulunmaktadır. Bunlar sırası ile standartlar, prosedürler, kurum yapısından oluşan iş ortamı, bir başka deyişle **kontrol ortamı**, risklerin tanımlanması, analizi ile ilgili dinamik bir süreç

olan **risk değerlendirmesi**, eylemlerin kurum hedef ve stratejilerini başarmaya yönelik olduğunun güvencesinin sağlanmaya çalışıldığı **kontrol faaliyetleri**, yürütülen faaliyetler ve süreçler hakkında elde edilen bilgiler ve bunların kurum içi-dışı paylaşımını sağlayan **bilgi ve iletişim,** iç kontrol faaliyetlerinin sonuçlarının izlendiği, sapmalarının değerlendirildiği **izlemedir.** Her bileşen kendi alanındaki temel kavramları temsil eden prensiplerle desteklenmektedir. Bütünsel bir görüş oluşturmak açısından Tablo 1.1'de COSO İç kontrol Sistemi bileşenleri ve prensiplerinin ilişkisi ana hatları ile özetlenmiştir. Buna göre kontrol ortamı ile ilgili beş, risk değerlendirmesi ile ilgili dört, kontrol faaliyetleri ile ilgili üç, bilgi ve iletişim ile ilgili üç, izleme ile ilgili iki prensip olmak üzere toplam on yedi prensiple bileşenlerin altındaki temel kavramlar vurgulanmaktadır.

Tablo 1.1 : COSO İç Kontrol Sistemi Bileşenleri ve Prensipleri İlişkisi

Bileşen		KONTROL ORTAMI
Prensipler	1	Organizasyon dürüstlük ve etik değerlere bağlılık göstermelidir.
	2	Yönetim Kurulu şirket yönetiminden bağımsız olup, iç kontrol performans ve gelişimi ile ilgili aktif tavır sergileyerek sürece nezaret etmesi gerekir.
	3	Kurum yönetiminin, Yönetim Kurulu nezaretinde, hedefleri gerçekleştirmeye yönelik, sorumluluk ve yetki alanlarını belirlemesi, raporlama kanallarını oluşturması ve gerekli yapılanmayı gerçekleştirmesi gerekir.
	4	Organizasyonun kurum hedeflerine uygun mesleki yeterliliğe sahip bireyleri cezbetme, geliştirme ve kurumda tutabilme konularında çaba ve bağlılık göstermesi gerekir.
	5	Organizasyonun, kurum hedeflerine uygun biçimde çalışanlarını iç kontrolle ilgili sorumlulukları açısından hesap verilebilir kılması gerekir.
Bileşen		RİSK DEĞERLENDİRMESİ
Prensipler	6	Organizasyonun, hedeflerini, bu hedeflerle ilgili risklerin belirlenmesi ve değerlendirilmesini mümkün kılacak açıklıkta belirlemesi gerekir.
	7	Organizasyonun, kurumun her noktasında hedeflerin gerçekleştirilmesi ile ilgili riskleri belirleyip, bunların yönetilmesine yönelik değerlendirmeleri ve analizleri yapması gerekir.
	8	Organizasyonun, hedeflerin başarılması ile ilgili riskleri değerlendirirken yolsuzluk ve usulsüzlük potansiyellerini dikkate alması gerekir.
	9	Organizasyonun, iç kontrol sistemini belirgin biçimde etkileyecek değişimleri tanımlaması ve değerlendirmesi gerekir.
Bileşen		KONTROL FAALİYETLERİ
Prensipler	10	Organizasyonun, hedeflere ulaşılmasına ilişkin risklerin kabul edilebilir seviyelere indirilmesine katkı sağlayacak kontrol faaliyetlerini belirlemesi ve geliştirmesi gerekir.
	11	Organizasyonun, hedeflerin gerçekleştirilmesine yönelik genel kontrol faaliyetlerini teknoloji odaklı seçip geliştirmesi gerekir.
	12	Organizasyonun, kontrol aktivitelerini, kurum politika ve prosedürlerine dayandırarak işletmesi gerekir.
Prensipler		BİLGİ VE İLETİŞİM
	13	Organizasyonun, iç kontrol fonksiyonunu destekleyecek uygunlukta ve kalitede bilgi toplaması ve kullanması gerekir.
	14	Organizasyonun, amaç ve sorumluluklar dahil olmak üzere, iç kontrol fonksiyonunu destekleyen bilgilerin kurum içi iletişimini yapması gerekir.
	15	Organizasyonun, iç kontrol fonksiyonunu etkileyen konularda kurum dışı ile de iletişim halinde olması gerekir.
Bileşen		İZLEME
Prensipler	16	Organizasyonun, iç kontrol bileşenlerinin güncel ve fonksiyon gösteriyor olduğunu doğrulayacak değerlendirmeleri oluşturma, geliştirme ve uygulaması gerekir.
	17	Organizasyonun, iç kontrol sapmaları ve farklarını belli zaman aralıklarında değerlemesi, bu sapmaların, sorumlularla, yönetimle ve yönetim kurulu üyeleri ile iletişimini yapması gerekir.

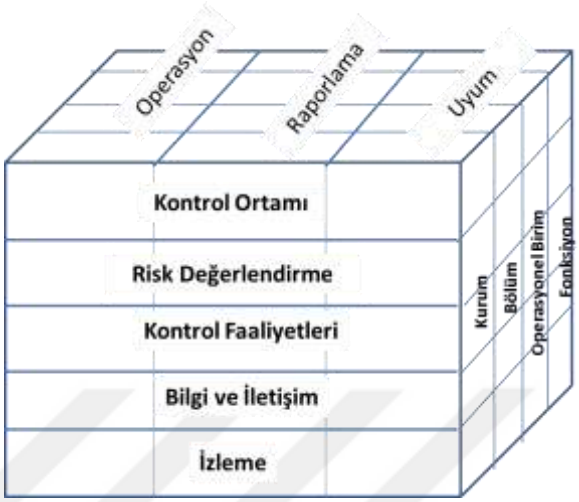
Kaynak: PWC, **COSO Internal Control-Integrated Framework,** American Institute of Certified Public Accountants, 2013

1.2.1.3. COSO İç Kontrol Sistemi Küpü

Kurum içinde, farklı yönetim kademelerinde ve farklı iş birimlerinde veya kurum yapısının farklı kademelerinde ihtiyaç duyulan iç kontrol kapsamı ve sahip olunan iç kontrol perspektifi farklı olacaktır. Örneğin, bir iş birimi doygun ve yapılandırılmış bir endüstride faaliyet gösterirken aynı kurumun başka bir iş birimi yeni bir iş kolunun ve pazarın oluştuğu farklı bir endüstride faaliyet gösteriyor olabilir. Her iki endüstrinin etkilendiği değişimler riskler, toleranslar ve kurumun bu pazarlara yönelik risk iştahı, düzenlemeler, mevzuat farklı olacaktır.

COSO İç Kontrol Sistemi, çok boyutlu yapısı ile iç kontrol bileşenleri arasındaki ilişkiyi açıklamak için aşağıda Şekil 1.1'de yer verilen iç kontrol küpünü kullanmaktadır. COSO küpü, sistemin hedef gruplamasında kullandığı ana kategoriler, sistemin bileşenleri ve kurumun yapıları arasındaki çok boyutlu ilişkiyi göstermektedir. Görüleceği gibi her hedef kategorisi altında bileşenler tarafından oluşturulan kümeler kurumun bütünü için iç kontrolün çerçevesini oluşturduğu gibi her bir faaliyet birimi için ayrı ayrı da iç kontrol çerçevesini oluşturmaktadır.

Şekil 1.1: COSO İç Kontrol Sistemi Küpü



Kaynak: COSO, **Executive Summary Internal Control-Integrated Framework,** May 2013, s.3, (Çevrimiçi) http//www.coso.org, 19 Şubat 2016.

1.2.2. COSO İç Kontrol Sistemi Bileşenleri

1.2.2.1. Kontrol Ortamı

Kontrol ortamı yönetim kurulu, yönetim ve çalışanları ile bir kurumun iş yapış ortamı, biçimi, kültürü, iç kontrol farkındalığı, yaklaşımları ve faaliyetlerinin bütünüdür. Diğer iç kontrol bileşenleri için bir alt yapı ve genel çerçeveyi oluşturmaktadır.

Dürüstlük ve etik değerlere bağlılık: COSO İç Kontrol Sistemi (Sistem) birinci prensibi, organizasyonun dürüstlük ve etik değerlere bağlılık göstermesi gereğidir. Kurumun dürüstlük ve etik değerler anlayışı iç kontrol ortamı için hayatidir. Yönetim tarafından bir etik değerler ve dürüstlük anlayışı rehberinin oluşturulup içeriğinin kurum organizasyonunun her kademesi ile iletişiminin yapılması, kurumda neyin yanlış, neyin doğru değerlendirildiği, işlerin bu kapsamda nasıl yapılmasının beklendiği konularının netleşmesini ve bu konu hakkında farkındalığın güncel kalmasını sağlayacaktır. Kurum yöneticilerinin iş anlayışları,

risk – fırsat algıları, insiyatif kullanma eğilimleri, kurum kültüründe iş yapış biçimi ile ilgili ve kurumsal davranışlarla ilgili oluşmuş ve kabul gören değerler kümesi ve bunların kurum içi iletişim biçimi, kurum yöneticilerinin iç kontrol farkındalığı kurumun iç kontrol ortamını şekillendirecektir.

Bağımsız ve aktif yönetim kurulu: Sisteminin ikinci prensibi, yönetim kurulunun şirket yönetiminden bağımsız olup iç kontrol performans ve gelişimi ile ilgili aktif tavır sergileyerek sürece nezaret etmesi gereğidir. Kurum politikaları, kültürü, iş yapış biçimi ve prensiplerinin oluşturulup temsil edildiği yer olarak düşünüldüğünde aktif ve bağımsız bir yönetim kurulu ve denetim komitesi iç kontrol ortamı için çok önemli bir ihtiyaç olarak karşımıza çıkacaktır. Bu yapının kurulması ve sürdürülmesindeki nihai sorumluluk yönetim kurulundadır.

Organizayonu yapılandırma: Sisteminin üçüncü prensibi, kurumun yönetiminin yönetim kurulu nezaretinde, hedefleri gerçekleştirmeye yönelik, sorumluluk ve yetki alanlarının belirlenmesi, raporlama kanallarının kurulması ve gerekli yapılanmayı gerçekleştirmesi gereğidir. Kurumun organizasyonel yapısı ile iç kontrol ortamı arasında sıkı bir bağ vardır. Kurum hedeflerini gerçekleştirmek için tasarladığı süreçler, planlamalar, organizasyonunun dikey veya yatay yapısı, merkezi veya merkezkaç yönetim anlayışı, kurum değerler seti ile ilgili yürütülen iletişim biçimleri vb. yapısal unsurlar kurumdaki iç kontrol ortamı ile yakın ilişki ve etkileşim içindedir.

Mesleki yeterlilik ve yetenek yönetimi: Sisteminin dördüncü prensibi, organizasyonun, kurum hedeflerine uygun mesleki yeterliliğe sahip bireyleri cezbetme, geliştirme ve kurumda tutabilme konularında çaba ve bağlılık göstermesi gereğidir. Kurumda yürütülen işlerle ilgili yeterli mesleki yeterlilik ve sorumluluk seviyesinin sağlanmış olması gerekir. Kurumun çeşitli işleri için ihtiyaç duyduğu mesleki yeterlilik ve sorumluluk seviyelerini belirleyip bunları çalışanlarına kazandıracak programları çalıştırıyor olması gerekir. Kurumun insan kaynakları politikaları ile ilgili işe alma, oryantasyon, eğitim, değerlendirme, terfi, haklar vb.. alanlardaki politika ve uygulamalarında adaletli olma, tarafsızlık, objektif olma,

şeffaflık kapsamında temsil ettiği yaklaşımlar ve taşıdığı mesajlar kurum ahlak anlayışı, kurumsal kültür, kurumsal davranışlara yönelik değer setleri konusunda çok belirleyici olur. Dolayısı ile iç kontrol ortamı üzerinde tartışmasız çok yakın etkisi bulunmaktadır.

Hesap verilebilirlik: Sisteminin beşinci prensibi, organizasyonun kurum hedeflerine uygun biçimde çalışanlarını iç kontrolle ilgili sorumlulukları açısından hesap verilebilir kılması gereğidir. Kurum içi yetki – sorumluluk dağıtımı, karar mekanizmalarının çalışma biçimi, iş tanımları ve iş akışları ile ortaya koyulup iletişimi yapılan konular olmakla birlikte kime ait olduğu tam olarak netleştirilmemiş sorumluluk ve karar alanlarının bulunması, kurum kontrol ortamında belirsiz ve çatışma alanları bırakıp ilişkilerde karmaşıklığı arttırır. Bu alanların olabildiği kadar net ve açık olarak tanımlanması ve anlaşılmasının sağlanması gerekmektedir.

Karar ve sorumluluk alanlarının yukarıdan aşağıya aktarılan süreçlerde her ne kadar karar organizasyonun alt birimlerinde alınsa ve sorumlu olarak bu birimler tarif edilmiş olsa da bu kararların sonuçlarından nihai olarak ilgili birimin yöneticisi, ondan da söz konusu yöneticinin üst yöneticisi, nihayet bütününden genel müdür ve yönetim kurulu sorumlu olacaktır. Karar ve sorumluluk aktarımın net olarak yapılıp yapılmaması, kurumda hakim hesap verilebilirlik kültürünün seviyesi, organizasyonun konu hakkında farkındalık seviyesi ve bakış açısı ile kurum iç kontrol ortamı yakından etkilenecektir.

1.2.2.2. Risk Değerlendirme

Kurumlar hedef ve stratejilerini gerçekleştirirken iç ve dış risklere maruz kalmaktadır. Kurumun bu risklerin farkında olmaya, bunları değerlendirmeye ve yönetmeye yönelik bir yaklaşım içinde olması beklenir. COSO İç Kontrol Sistemi, risklerin değerlendirilmesi ve yönetilmesi ile ilgili sorumluluğu kurum yöneticilerinin üzerinde olarak değerlendirmektedir.

Hedeflerin yeterli açıklıkta belirlenmesi: Sistemin altıncı prensibi, organizasyonun hedeflerinin, bu hedeflerle ilgili risklerin tanımlanması ve değerlendirilmesini mümkün kılacak açıklıkta belirlemesi gereğidir. Riskin, kurum hedefleri açısından sonuçları etkileyecek bir olay olduğuna daha evvel değinilmişti. Kurum hedefleri açısından hangi olayların sonuçları ne ölçüde etkileyeceğinin değerlendirilmesi aşamasında kurum hedeflerinin, hedef belirlemede ana gruplar olan, operasyonel, raporlama ve uyum gruplarına bölünmesi, kurum strateji ve politikaları ile ilişkileri net olarak ortaya koyulması gerekmektedir.

Hedeflere ilişkin sonuçların hangi olaylardan etkileneceği ve bu etkinin olumlu yönde mi, olumsuz yönde mi olduğunun hangi kriterlere göre değerlendirileceği, bu etkilerin olumsuzdan olumluya yönlendirilmesi için alınacak tedbirlerin belirlenmesi, uygulanması süreci söz konusu hedeflerin hangi açıklıkta belirlendiği, ana hedef grupları ile ilişkilerinin nasıl belirlendiği, nelerin olumlu sonuç, nelerin olumsuz sonuç olduğunun kurum strateji ve politikalarına uygun olarak ve yönetim kurulu bakışını yansıtır biçimde, açık ve ölçülebilir olarak ifade edilmiş olmasına bağlıdır.

Risklerin anlaşılması: Sistemin yedinci prensibi, organizasyonun, kurumun her noktasında, hedeflerin gerçekleştirilmesi ile ilgili riskleri belirleyip, bunların yönetilmesine yönelik değerlendirmeleri ve analizleri yapma gereğidir. **Risk iştahı** kurumun almaya hazır olduğu risk seviyesidir. Risk iştahı Yönetim Kurulu (YK) tarafından belirlenmeli, kurum içinde sürekli iletişimi yapılmalıdır. **Risk toleransı** ise riskin gerçekleşmesi durumunda kurumun katlanabileceğini düşündüğü olumsuz durumun seviyesidir. Kurum nezdinde risk kavramı tanımı mutabakatı sağlanmasına, ortak bir risk kültürü ve terminolojisi oluşturulmasına, kurum risk farkındalığının kabul edilebilir seviyeye yükseltilmesine, arama konferansları, mülakatlar, anketler, iş akış analizleri vb.. yöntemlerle çalışmaya geniş tabanlı bir katılım sağlamaya dikkat edilmesi gerekmektedir. Tüm bu çalışmaların sistematik olarak bir araya getirilmesi ile ana risk grupları ve alt risk gruplarını barındıran, risklerin detaylı tarif edildiği kurum **risk envanteri** oluşturulur.

Yolsuzluk ve usulsüzlük potansiyeli: Sistemin sekizinci prensibi, organizasyonun hedeflerin başarılması ile ilgili riskleri değerlendirirken yolsuzluk ve usulsüzlük potansiyellerini dikkate alması gereğidir. İçinde insan faktörü olan tüm süreçler yolsuzluk ve usulsüzlüklere açıktır. Yolsuzluklarla ilgili alarm sayılan işaretler belirlenmeli ve izlenmelidir. Bu işaretler genel olabileceği gibi organizayona özgü de olabilir.

> *"Kontrol faaliyetlerinin yönetim veya çalışanlarca göz ardı edilmesi, yönetim faaliyetleri hakkında düzensiz ve eksik bilgilendirmeler, iş koşullarındaki değişimlerden veya rakiplerden etkilenmeksizin sürekli olarak aşılan hedefler, rutin olmayan işlemlerde ve kayıt girişlerindeki artış, talep edilen bilginin sağlanmasında karşılaşılan problemler ve gecikmeler, müşteriler veya tedarikçilerde olağan dışı değişimler bu işaretlerdendir."* [5]

> *"Yolsuzluk değerlendirmesi sürecinde beş kritik adım bulunmaktadır. Yolsuzlukla ilgili uygun risk faktörlerinin belirlenmesi, potansiyel yolsuzluk kurgularının tanımlanması ve riskleri dikkate alarak önceliklendirilmesi, mevcut kontrollerin potansiyel usulsüzlük kurguları ile eşleştirilerek açıklıkların belirlenmesi, usulsüzlük önleme ve deşifre etmek için uygulanan kontrollerin etkinliğinin test edilmesi, yolsuzluk risk değerlendirilmesinin dökümante edilmesi ve raporlanması…Usulsüzlük risklerinin önceliklendirilmesinde şu faktörler değerlendirilmelidir: Parasal etki, kurum imajına olan etkisi, verimlilik kaybı, unsuru taşıması veya mevzuata aykırılık teşkil etmesi, veriler üzerinde doğruluk ve güvenlik ile ilgili etkisi, varlıkların kaybı, iş birimi lokasyonu ve büyüklüğü, şirket kültürü, yönetici ve çalışan devir hızı, varlıkların likiditesi, işlemlerin ölçeği, konunun taşere edilip edilemeyeceği"* [6]

Değişimlerin değerlendirilmesi: Sistemin dokuzuncu prensibi, organizasyonun, iç kontrol sistemini belirgin biçimde etkileyecek değişimleri tanımlaması ve değerlendirmesi gereğidir.

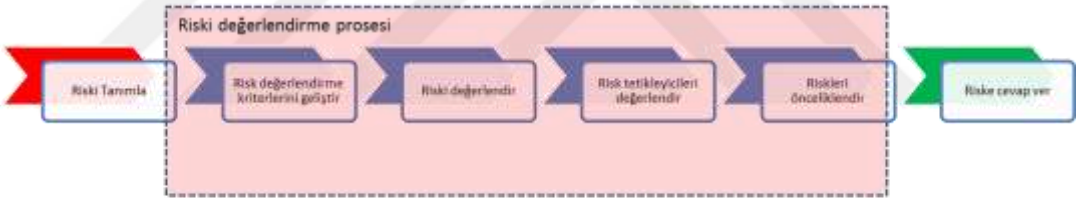
---

[5] International Professional Practices Framework, "Internal Auditing And Fraud", **Practice Guide**, December 2009, s.8. (Çevrimiçi) http/www.globaliia.org/standards-guidance, 13 Ocak 2015

[6] A.e., s.16-17

Risklerin tanımlanmasının ve risk envanterinin oluşturulmasının ardından, riskler strateji ve hedeflere uygun olarak gruplandırılır ve risk hiyerarşisi oluşturulur. Risklerin gruplanmasının ardından ana risk grupları, alt risk grupları ve detaylı risklerin teker teker gerçekleşmesi durumunda ortaya çıkabilecek olumsuz etkilerin sayısal ve/veya sayısal olmayan yöntemlerle değerlendirilerek ve ölçülerek önceliklendirildiği aşama "risk değerlendirme sürecidir". Bu sayede risk yönetimi süreci açısından doğru odaklanma ve verimli, etkili kaynak kullanımı söz konusu olur, riskler değerlendirilmiş ve önceliklendirilmiş olarak bir sonraki aşamada planlanacak "riskleri giderme" aksiyonları için doğru bir odaklanma sağlanır.

Şekil 1.2: Risk Değerlendirme Süreci



Kaynak: Dr. Patchin Curtis, Mark Carey, "Risk Assesment In Practice," **Thought Leadership in ERM**, October 2012, s.2, (Çevrimiçi) http//www.coso.org, 17 Mayıs 2017.

1.2.2.3. Kontrol Faaliyetleri

Tanımlanan risklerin yönetilmesine ilişkin prosedürler kontrol faaliyetleri olarak adlandırılır. Organizasyonun her seviyesinde olması gereken bu faaliyetlerin etki alanı çok geniş olabilir ve organizasyon içinde çeşitli seviyelerde tekrar eden benzer faaliyetler söz konusu olabilir. Kontrol faaliyetleri, **operasyonel kontrol, rapor kontrolü ve mevzuat uygunluğu kontrolü** olmak üzere üç ana grupta toplanır.

Makul seviyede riskler için kontrol faaliyetleri: Sistemin onuncu prensibi, organizasyonun, hedeflere ulaşılmasına ilişkin risklerin kabul edilebilir seviyelere indirilmesine katkı sağlayacak kontrol faaliyetlerini belirlemesi ve geliştirmesi gereğidir. Kontrol faaliyetleri, iç kontrol sürecinin kurum hedeflerini gerçekleştirecek olmasını makul seviyede güvence altına alacak biçimde işletilmelidir. Süreç **makul seviyede** güvence amaçlar, yüzde yüz güvence peşinde değildir. Makul seviyede güvence anlayışı fayda-maliyet dengesi açısından önem arz eder.

Teknoloji odaklı kontrol faaliyetleri: Sistemin onbirinci prensibi, organizasyonun, hedeflerin gerçekleştirilmesine yönelik genel kontrol faaliyetlerini teknoloji odaklı seçip geliştirmesi gereğidir. Teknoloji, odaklı kontroller sürece dışarıdan manuel müdahaleyi en aza indirdiği için daha güvenli sayılırlar. Organizasyonun hem iş süreçleri açısından hem kontrol faaliyetleri açısından teknolojiye gerekli yatırımı yapma konusunda istekli olması beklenir.

Kurum politika ve prosedürlerine dayanan kontrol faaliyetleri: Sistemin on ikinci prensibi, organizasyonun kontrol faaliyetlerini kurum politika ve prosedürlerine dayandırma gereğidir. Kontrol faaliyetlerinin, kurumun politika ve prosedürlerine uygun tasarlanmış, prosedürlerin güncel ve kurumun iç kontrol sistemine katlı sağlar nitelikte uygulandığını makul seviyede garanti altına alıyor olması beklenir. Kurum stratejik ve operasyonel hedeflerini güncellemeyi gerektiren içsel ve dışsal değişim faktörleri (ortaklık yapısı, sermaye akışı, yasal ve mevzuat değişiklikleri, rekabet, endüstriyel değişiklikler vb.), sonucu iş akışlarında, prosedürlerde, süreçlerde meydana gelen değişimlere uygun olarak kontrol faaliyetleri güncellenmeli, iç kontrol sisteminin değişimler karşısında etkinliğinin korunduğu makul ölçüde garanti etmelidir.

Bu prensipler, kontrol faaliyetleri ile ilgili temel yaklaşımları ortaya koymaktadır. Firmalar için standart bir kontrol faaliyeti setinden bahsedilmemekle birlikte kontrol faaliyetlerinin aşağıdaki konuları dikkate alarak tasarlanması tavsiye edilmektedir.

Üst düzey gözden geçirmeler: Üst yönetim tanımlanmış riskleri ve bunların seyrini standart gözden geçirme toplantıları ile değerlendirmelidir. Bir kontrol faaliyetinin varlığı, amacına tasarlandığı biçimde hizmet ettiği anlamına gelmez. Riskin tanımında, risk iştahında, organizasyon yapısında, rekabette, iç-dış ekonomik koşullarda meydana gelen değişiklikler kontrol faaliyetinin etkinliğini değiştirmiş ve tekrar değerlendirilmesine ihtiyaç gösterir olabilir.

İlk amir ve/veya fonksiyonel amir değerlendirmeleri: Üst yönetim değerlendirmelerinin yanı sıra kontrol faaliyetleri ilk amir ve/veya fonksiyonel amir tarafından da düzenli değerlendirmelere tabi tutulmalıdır. Ayrıca kontrol, ilizyonların en aza indirilmesi için en kritik aşamalardandır.

Bilgi prosesi: Yüksek teknolojiden yararlanıyor veya yararlanılmıyor olsun, bilgi işleme prosesleri içinde sistemsel kontroller barındırmalıdır. "Sistem kontrolleri genellikle genel kontroller ve uygulama kontrolleri olmak üzere iki gruba ayrılmaktadır." [7] İşlemlerin doğruluğu, tamlığı, bütünlüğü ve yetkilendirmenin sistematik olarak kontrolünün sağlanması gerekmektedir.

Fiziksel kontroller: Makine, teçhizat, envanter gibi varlıkların güvenilir şekilde fiziksel kontrollerinin yapılması sağlanmalıdır.

Performans göstergeleri: Günümüz işletmelerinin geniş raporlama imkanları dahilinde performans yönetimi ve performans göstergeleri kontrol faaliyetlerine yardımcı olacak ve destekleyici nitelikte tanımlanmalı, performans – risk ilişkisi kurulmuş olmalıdır.

Görevlerin ayrılığı: Çok klasik bir prensiptir. İşi yapanla onaylayan ve kontrol eden ayrı kişiler olması sağlanmalıdır.

Kontrol faaliyetleri ile ilgili COSO İç Kontrol Sistemi ile daha sonra detaylı açıklayacak olduğumuz COSO Kurumsal Risk Yönetimi (COSO KRY)

[7] Özbek, **İç Denetim**, s.432.

çerçeveleri çok benzer tanımlamalar ve tavsiyeler içermektedir. Bu nedenle ilerleyen bölümde COSO KRY çerçeveleri konuşulurken, burada yer verilen açıklamalardan yararlanılacaktır.

1.2.2.4. Bilgi ve İletişim

Hedeflerin yerine getirilmesi, stratejilerin gerçekleştirilmesi için organizasyonda her seviyede çok çeşitli bilgiye ihtiyaç duyulmaktadır. Bilginin organizasyonda aşağıdan yukarı, yukarıdan aşağı iletiliyor olması gerekmektedir. Organizayonların ihtiyaç duydukları bilgiler çok çeşitli biçimlerde ve çok çeşitli araçlarla elde edilir ve iletişimleri sağlanabilir.

Uygun içerik ve kalitede bilgi: Sistemin on üçüncü prensibi, organizasyonun, iç kontrol fonksiyonunu destekleyecek uygunlukta ve kalitede bilgi toplaması ve kullanması gereğidir. Bilgi sistemleri manuel, otomatik veya kavramsal olabilir ve bu her bir yön hem resmi hem gayri resmi biçimde kurgulanmış olabilir, hem manuel sistem proseslerinin hem Bilgi Teknolojileri (IT) sistemlerinin iyi anlaşılması ve organizasyon ihtiyaçlarına cevap verir nitelikte olması beklenir.

Kurumda kullanılan bilgi sistemlerinin yeni olması bu ihtiyaçların karşılanacağı anlamına gelmediği gibi eski olması da esas itibariyle yetersizliğe işaret etmez. Önemli olan, bilgi sistemlerinin amaca yönelik tasarlanmış olmasıve bu tasarıma uygun işletilmesidir.

Kurum bilgi sistemlerinin gelişimini göstermek için hazırlanan Şekil 1.3 için COSO İç Kontrol Sistemi'nin bilgi sistemlerine bakışından yararlanılmıştır. Buna göre; kurumlarda bilgi sistemlerinin gelişiminin en içte yer alan "çekirdek" bilgi sistemlerinden en dışta yer alan "tam entegre otomatik sistemlere" doğru gelişim gösterdiği söylenebilir.

Şekil 1.3: Kurum Bilgi Sistemleri Gelişimi

Bilginin elde edilmesi ve kalitesi kadar bu bilginin iletişim biçimi ve iletişim araçları da önemlidir. COSO İç Kontrol Sistemi, iletişimi kurum içi ve kurum dışı olarak ikiye ayırmakla birlikte, aşağıdaki iletişim biçimlerini ön görmektedir.

Kurum içi iletişimin açık olması: Sistemin on dördüncü prensibi, organizasyonun, amaç ve sorumluluklar dahil olmak üzere, iç kontrol fonksiyonunu destekleyen bilgilerin kurum içi iletişimini yapma gereğidir. Üst yönetimden düzenli aralıklarla iç kontrol prosedürlerinin önemine ilişkin mesajlar alınması, tüm tarafların yürüttükleri faaliyetle ilgili kurumun kırmızı çizgilerini bilmesi (kurum politikalarına, etik değerlere, kurum değerlerine aykırılığın nerede başladığını bilmesi), tarafların sorunlarla ve yanlış davranışlarla karşılaştıklarında bunu yöneticilerine ve üst yönetime nasıl bildirmeleri gerektiğini bilmesi ve tanımlanmış bu iletişim yollarının kendileri için daima güvenli şekilde açık tutulması, bu yöndeki

iletişim konusunda tarafların cesaretlendirilmesi ve teşvik edilmesi, üst yönetim ve yönetim kurulu arasında etkin bir iletişim kanalının bulunması kurum içi iletişime örnek gösterilebilir.

Kurum dışı iletişimin açık olması: Sistemin on beşinci prensibi, organizasyonun iç kontrol fonksiyonunu etkileyen konularda kurum dışı ile de iletişim halinde olma gereğidir. Kurum dışı iletişimin fayda yaratması için kurum içinde olduğu gibi çift taraflı çalıştırılması tavsiye edilir (içten dışa ve dıştan içe). Kurumun müşteriler, tedarikçiler, yatırımcılarla etkili ve uygun, bağımsız ve güvenilir iletişim kanallarını kurmuş ve çalıştırıyor olması, kurumun tüketici şikayetlerinin kendisine ulaşması ve bunların değerlendirilmesi için uygun araçları tahsis etmesi kurum dışı iletişime örnek gösterilebilir.

1.2.2.5. İzleme

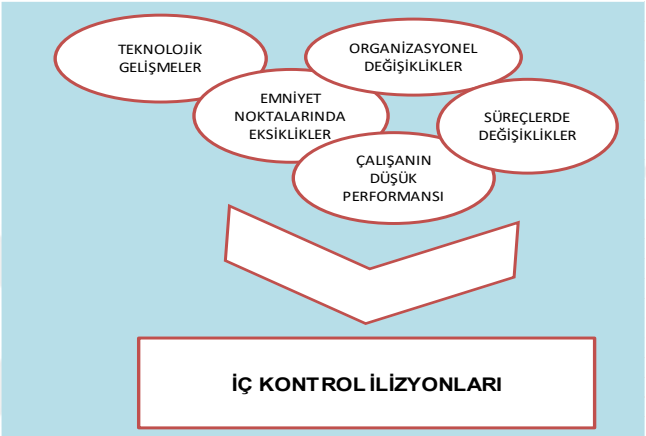
Güncel ve etkili iç kontrol bileşenleri: Sistemin on altıncı prensibi, organizasyonun, iç kontrol bileşenlerinin güncel ve fonksiyon gösteriyor olduğunu doğrulayacak değerlendirmeleri oluşturma, geliştirme ve uygulama gereğidir. Bir eylemin iç kontrol izleme eylemi olarak değerlendirilmesi için kurum faaliyetlerini düzenli olarak gözden geçirmesi ve potansiyel iyileştirme eylemler önermesi yeterli olacaktır.

İç kontrol faaliyetlerinin kurumun değişen iç ve dış koşullarına bağlı olarak değişen hedefleri öncelikleri ve iş yapış biçimleri karşısında etkinliğini kaybetmemesi ve olası ilizyonları engellemek için bu faaliyetlerin etkinliğini değerlendiren ve izleyen bir prosesin uygulamada olması gerekir.

Çalışanların birbirleri ile bilgisayar şifrelerini paylaşması, süreçlerle ilgili kontrol listelerinin tasarlandığı gibi uygulanmaması, işten ayrılan personelin bilgi sistemleri erişim yetkilerinin zamanında kapatılmaması, süreçlerde onay yetkisi olan amirlerin bu yetkilerini gayri resmi olarak alt çalışanlarına kullandırmaları, çevresel mevzuata ilişkin yeni düzenlenmiş bir standardın kalite kontrol listesine

dahil edilmemesi, organizasyonel değişiklik sonucu sorumluluk alanı ve yetkisi genişleyen bir çalışanın onay süreçlerinde yetki alanına uygun biçimde yer almaması ve benzeri durumlar iç kontrol ilizyonlarına örnek gösterilebilir.

Şekil 1.4: İç Kontrol İlizyonları Başlıca Nedenleri



Kaynak: Bill Atwood."vd", "The Illusion of Internal Control," **Strategic Finance**, October 2012, IMA, s. 3

Sapmaların iletişimi: Sistemin on yedinci prensibi, organizasyonun, iç kontrol sapmaları ve farklarını belli zaman aralıklarında değerleme, sapmaların, sorumlularla, yönetimle ve yönetim kurulu üyeleri ile iletişimini yapması gereğidir.

COSO İç Kontrol Sisteminde izleme faaliyetlerinin yanı sıra iç kontrol faaliyetlerinin değerlendirilmesi de gerekmektedir. İç kontrol faaliyetinin etkinliği ve işletme körlüğünün engellenmesi, ilizyonların düzeltilmesi açısından bu değerlendirmeler çok önemlidir. COSO İç Kontrol Sistemleri İzleme Rehberinde etkili izleme fonksiyonunun esasları ve çerçevesi ile ilgili önemli belirlemeler bulunmaktadır.

> *"Organizasyonlar, izleme süreçlerinin çerçevelerini şu unsurları içerecek biçimde çok farklı genişlikte ve değişik biçimlerde oluşturabilirler; kontrollerin iç denetim tarafından periyodik olarak değerlendirilmesi ve test edilmesi, bilgi sistemlerinin içine devamlılık içeren izleme programlarının yerleştirilmesi, bir kontrol eksikliğine işaret edebilecek anormallikleri belirlemek için operasyonel raporlar ve matrislerin uygun biçimde izlenmesi ve*

analiz edilmesi, sürecin normal parçası olan mutabakatlar gibi kontrollerin yönetsel olarak gözden geçirilmesi, yönetim kurulu ve yönetimin organizasyon içinde oluşturdukları izleme düzeyi ve nezaret görevleri konusundaki etkinlikleri hakkında öz eleştiri ve öz değerlendirmede bulunması, iç ve dış denetçilerin denetim komitesi sorguları ve iç denetimin kalite güvencesine ilişkin gözden geçirmeleri" [8]

İzleme fonksiyonunun, kurumun değişimlerden etkilenen kontrol faaliyetleri ve iç kontrol sistemi uygulamalarına, teknolojiye, süreçlerdeki değişimlere uygun olarak etkinliğini koruyacak biçimde güncel tutulması hayati önem taşımakla birlikte izleme fonksiyonunun etkili işletilmesinde fayda – maliyet analizinin her zaman göz önünde tutulması gerektiği unutulmamalıdır.

İç kontrol sistemlerimizi ne kadar güçlü kurarsak kuralım, teknolojiden ne ölçüde yararlanırsak yararlanalım, prosedürlerimiz ne kadar güncel ve eksiksiz olursa olsun, iç kontrol sürecinin merkezinde insan ve yargılama kavramı vardır. Ayrıca organizasyonumuz dış faktörlerin operasyonumuza yönelik etkilerine maruzdur. İç kontrol sistemimiz, hatalı yargılamalar, kötü iş kararları verme ve yanı sıra dışarıdan gelen etkilerin stratejik ve operasyonel hedeflerimize etkileri konusunda fazla bir güvence sağlamayacaktır.

"İç kontrol sistemlerinin stratejik ve operasyonel hedeflerle ilgili verecekleri güvenceler için sınırlar ve engeller oluşturabilecek durumlar şunlardır; karar süreçlerinde yargılamalar hatalı yapılıp önyargılı olabilirler, basit insan hatalarından kaynaklı kırılma noktaları olabilir, iç kontrol uygulamaları yönetim tarafından çiğnenebilir, yönetim, çalışanlar veya üçüncü kişiler iç kontrol sisteminin açıklarını yakalayabilirler, kurum kontrollerinin ötesinde sonuçlara etki edecek dışsal faktörler olabilir." [9]

[8] COSO, **Guidance on Monitoring Internal Control Systems: Introduction**, January 2009, s.4, (Çevrimiçi) http//www.coso.org, 07 Mart 2016.
[9] COSO, **Executive Summary Internal Control-Integrated Framework,** May 2013, (Çevrimiçi) http//www.coso.org, 19 Şubat 2016.

Bu sınırlama ve engeller sonucu iç kontrol hedeflerin başarılması konusunda mutlak güvence değil ama makul ölçüde güvence vermektedir. İç kontrol sistemleri için genel standart ve prensipler ortaya koyulmuş olunmakla birlikte bu sistemler kurumlara özgün tasarlanacak ve işletilecek sistemlerdir. Kurum hedeflerine ulaşma konusunda makul güvence seviyesinin ne olacağı yönetim kurulu, yönetim değerlendirmeleri ve kurum kültürüne göre farklılık gösterecektir. Bu nedenle ortaya koyulan sistemin fayda- maliyet analizi her zaman göz önünde bulundurulması gereken bir konu olacaktır.

İKİNCİ BÖLÜM
KURUMSAL RİSK YÖNETİMİ

İş modelleri ve bunları gerçekleştirmek için kurulan yapılar belirsizliklerle karşı karşıyadır. Bu yapıların etkileşim içinde oldukları içsel ve dışsal faktörler bu belirsizlikleri de değişir kılar. Bir başka deyişle içsel ve dışsal faktörlerdeki değişime bağlı olarak bu yapıları etkileyen belirsizlikler de değişmektedir.

Belirsizlikler söz konusu yapılar için riskler ve fırsatlar içermektedir. Hissedarların kurum yöneticilerinden temel beklentisi de söz konusu belirsizliklerin içerdiği riskler ve fırsatları yöneterek işletme faydasını arttırmak, değişimdeki sürekliliğe bağlı biçimde, bu yönetim erkinin sistematik ve sürdürülebilir bir yaklaşım olarak ortaya koyulmasını sağlamaktır. Etkin bir risk yönetim sisteminin, risklerin giderilmesi ve fırsatların değerlendirilmesi kadar, yönetişim, strateji ve hedeflerin belirlenmesi, operasyonel kalitenin arttırılması, bunlara bağlı olarak değer oluşturmas ve bu durumun sürdürülebilir kılmasına katkı sağlamak ile de ilgilenmesi beklenmelidir.

2.1. Kurumsal Risk Yönetimi Kapsam ve Çerçevesi

Risk Yönetimi ile ilgili yasal düzenlemelerde, şirketler ve yönetim kurulu sorumlulukları açısından ticaret kanunlarında belli düzenlemelere gidilmiş, ülkelere göre değişen kurumsal yönetim düzenlemelerinde de prensipler ortaya koyulmuştur. Prensiplerin genel odağı yönetim kurullarının şirket ve yatırımcılar açısından ortaya çıkabilecek risklere odaklanmasını sağlamak, hissedarların ve kamuoyunun risklerle ilgili doğru ve zamanında bilgilendirilmesi konusunda yönetim kurulları sorumluluklarını düzenlemek, şirket özellikleri dikkate alınarak riskleri yönetmeye yönelik çalışmaların başlatılmasını sağlamak ve ortak bir terminoloji oluşturmaktır.

Ülkemizde risk yönetimi konusunda sektör olarak en ileri uygulamalar bankalar ve bankacılık sektöründe olup konu Bankalar Kanunu ve Banklacılık Düzenleme ve Denetleme Kurumu (BDDK) düzenlemeleri ile çerçevelenmiştir. İşletme uygulamamızda incelediğimiz şirketin faaliyet alanının üretim ve satış olması sebebi ile banka ve bankacılık sektörü ile ilgili düzenlemelerin içeriğine yer verilmemiştir.

Öte yandan, Sermaye Piyayası Kurulu (SPK)'nun Kurumsal Yönetim İlkelerinin Belirlenmesi ve Uygulanmasına İlişkin 30 Aralık 2011 tarih ve 28158 sayılı Resmi Gazete' de yayınlanan Tebliğ ile kurumsal yönetim ilkeleri düzenlenmiş, gerekli görülen konular 11 Şubat 2012 tarihli, 28201 sayılı Resmi Gazete, 13 Eylül 2012 tarihli, 28410 sayılı Resmi Gazete, 11 Şubat 2013 tarih, 28567 sayılı Resmi Gazete' de yayınlanan değişiklik tebliğleri ile güncellenmiştir.

Çalışmamızda, kurumsal yönetim konusundan ziyade risk yönetimi konusu işlendiği için SPK'nın kurumsal yönetim konusundaki düzenlemelerinin içeriğine yer verilmemiştir.

6102 sayılı Türk Ticaret Kanunu (TTK) ile anonim şirketler açısından muhasebe ve finans denetimi ile, halka açık şirketler açısından riskin erken saptanması ve yönetimi konuları düzenlenmektedir. 13/1/2011 tarih, 6102 sayılı TTK 375. maddesinde yönetim kurulu için devredilemez ve vazgeçilemez görevler arasında muhasebe ve finans denetiminin sağlanması da sayılırken, 378. maddesinde pay senetleri borsada işlem gören şirketler için riskin erken saptanması ve yönetimi konusunu düzenlenmektedir.

> *"Kurumsal Risk Yönetimi (KRY) kurumun hedeflerine ulaşmasını etkileyen fırsatlar ve tehditlerin tespit edilmesi, tanımlanması, değerlendirilmesi, bunlara verilecek yanıtların kararlaştırılması ve bunların rapor edilmesi için tüm kuum çapında uygulanan, özel yapılandırılmış, istikrarlı*

ve kesintisiz bir süreçtir."[1]

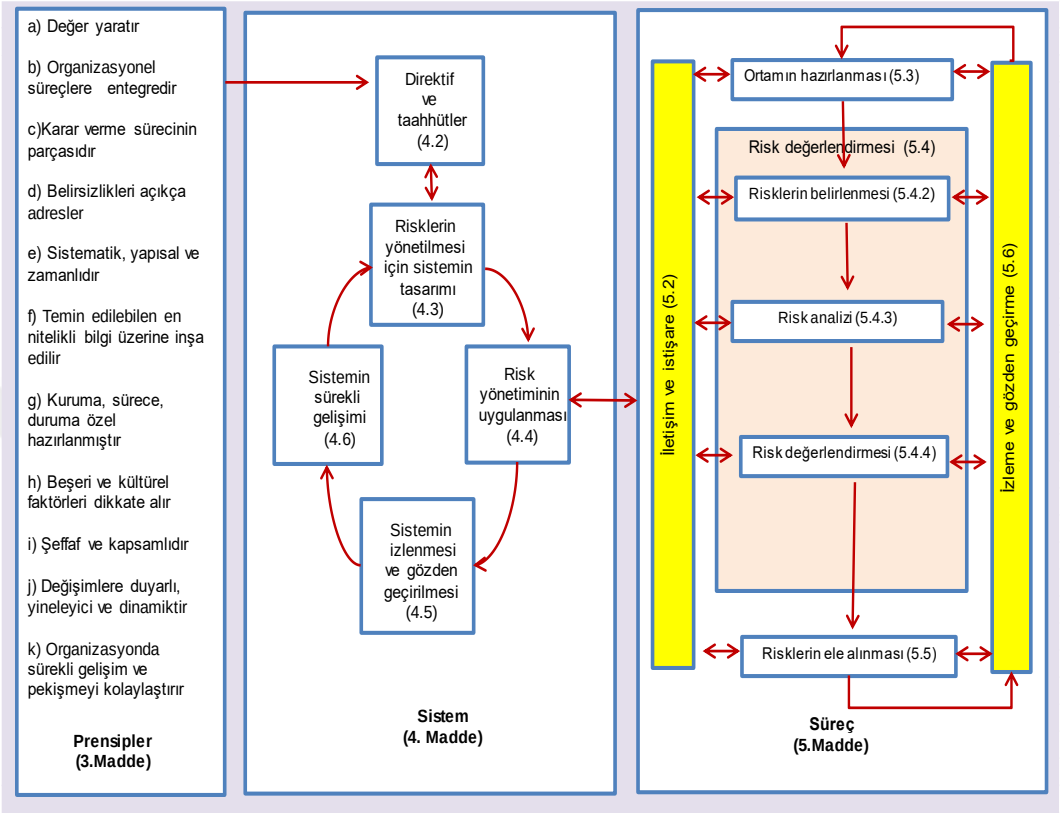
Risk yönetimi ile ilgili yayınlanmış standartlar ve düzenlemelerin kapsam ve kullanım yaygınlığı dikkate alındığında, işletme uygulamamızı yakından ilgilendiren yaklaşımlar, ISO 31000 standardı ve COSO Kurumsal Risk Yönetimi Çerçeveleridir.

ISO Kurumsal Risk Yönetimi Standardı (ISO 31000): ISO Teknik Yönetim Kurulu çalışma grubu tarafından risk yönetimi ile ilgili oluşturulmuş standart olup, etkin bir risk yönetim fonksiyonu için yapılması gereken bir dizi prensip ortaya koyulmakta, ortaya koyulan prensipler, sistem ve süreçlerin ilişkisi belirlenmektedir. Bu standartta, risk yönetiminin, organizasyonun bütünü için, pek çok alanında ve seviyesinde, her hangi bir zamanda uygulanabileceği gibi, belirli fonksiyonlar, projeler ve faaliyetler için de uygulanabileceği vurgulanmaktadır. Standart bir endüstri veya sektöre özgü değildir. Her hangi bir kurum, yapı veya organizasyon tarafından uygulanabilecek biçimde ortaya koyulmuştur.

Şekil 2.1'de ISO 31000 standardı tarafından ortaya koyulan on bir temel prensip, sistem ve süreçlerin ilişkisi gösterilmiştir. Gösterilen yapı çalışmamızın "ISO Kurumsal Risk Yönetim Standardı" bölümünde ana hatları ile ele alınmaktadır.

[1] The Institute of Internal Auditors, "İç Denetimin Kurumsal Risk Yönetiminde Oynadığı Rol", **IIA Pozisyon Raporu,** çev.,Türkiye İç Denetim Enstitüsü, Ocak 2009, (Çevrimiçi) http/www.tide.org.tr, 25 Temmuz 2016.

Şekil 2.1: ISO Risk Yönetim Prensipleri Sistem ve Süreç İlişkisi



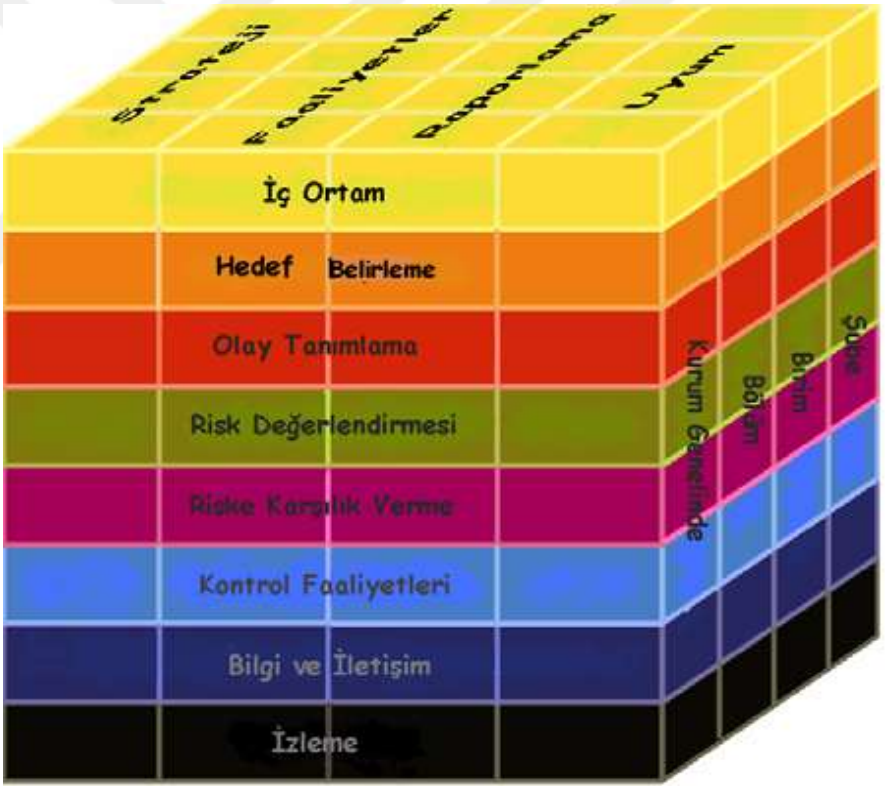
Kaynak: ISO, **International Standard ISO31000:Risk Management-Principles and Guidelines**, Switzerland, ISO, 2009

COSO Kurumsal Risk Yönetimi Çerçeveleri: 1992 yılında yayınlan , 2004'te geliştirilmiş versiyonu çıkarılan COSO Kurumsal Risk Yönetimi –Entegre Çerçevesi risk ve fırsat olgularına ve bunların yönetilmesine yönelik iken, zamanın değişen ihtiyaçlarına, değişen risk, fırsat tanımlarına, kültürel değişimnlere, iletişim alt yapı değişiklikllerine ve ekonomik değişikliklere daha iyi cevap verebilmek için Eylül 2017 tarihinde bir kez daha güncellenmiştir. Yeni güncellemede çerçevenin adı COSO Kurumsal Risk Yönetimi – Strateji ve Performansla Entegre Çerçeve olarak değiştirilmiş, bileşenlerin tanımlarında değişiklikler olurken, bileşenler alt prensiplerle desteklenmiş , kültürel değişim, strateji ve ekonomik hedefler belirleme, kaliteli operasyonel yönetim güvencesi ile değer yaratma ve bunu sürdürülebilir kılma çerçevesi öne çıkmıştır. Bu çerçeveler, birinci bölümde incelediğimiz COSO İç Kontrol–Entegre Çerçevesi üzerine inşa edilmiştir. COSO İç Kontrol Küpü,

COSO KRY-2004 Küpü olarak Şekil 2.2 ‘de gösterildiği biçimde geliştirilerek COSO KRY-2004 bileşenlerinin ilişkisini göstermektedir.

COSO İç Kontrol Sistemi bileşenlerinden “kontrol ortamı” bileşeni “iç ortam” olarak geliştirilerek, hedef belirleme, olay tanımlama ve riske karşılık verme kavramları ayrı bileşenler olarak genişletilerek ele alınmıştır. Hedef gruplama konusunda “strateji” ve “stratejik hedefler” kavramı ayrı bir grup biçiminde genişletilerek ele alınmıştır.

Şekil 2.2: COSO Kurumsal Risk Yönetimi –Entegre Çerçeve Küpü



Kaynak: COSO, **Executive Summary Enterprise Risk Management-Integrated Framework**, September 2004, (Çevrimiçi) http//www.coso.org, 20 Mayıs 2016

Haziran 2017 tarihinde güncellenen COSO Kurumsal Risk Yönetimi – Strateji ve Performansla Entegre Çerçeve’de ise var olan sekiz bileşen daha geniş kapsamlı beş bileşen olarak yeniden tanımlanmış, bileşenler yirmi prensip ile

desteklenmiştir. Şekil 2.3'te yeni yapıyı oluşturan bileşenler ve ilişkileri gösterilmiştir.

Şekil 2.3 : COSO Kurumsal Risk Yönetimi- Strateji ve Performansa Entegre Çerçeve Yapısı

Kaynak: COSO, **Enterprise Risk Management-Integrating with Strategy and Performance**, June 2017, (Çevrimiçi) http//www.coso.org, 05 Nisan 2019

Her iki COSO KRY Çerçevesi bileşenleri, takip eden alt bölümlerde açıklanmış ve üçüncü bölümdeki işletme uygulamamızın temelini oluşturmuşlardır.

2.2. ISO Kurumsal Risk Yönetimi Standardı (ISO 31000)

ISO 31000 standardı risk yönetimi konusunda temel prensipleri ve ana yönlendirici unsurları ortaya koyarken; konuyu, prensipler, sistem, risk yönetim süreci olarak üç ana grupta ele almaktadır. Standardın ortaya koyduğu yaklaşım etkin bir risk yönetimi fonksiyonu açısından bir sektöre, endüstriye, fonksiyona faaliyete özel olmayıp, hemen tüm kurumlar, organizasyonel yapılarda kullanılabilecek, kurumun hemen her seviyesinde, her fonksiyonu için her zaman bütünsel olarak ele alınabileceği gibi seçilmiş zamanlarda, seçilmiş süreçler, faaliyetler, kurum seviyeleri için de uygulanabilmek üzere tasarlanmıştır. Bu durum, ilgili standardın hemen her kurum ve faaliyet türüne göre uygulanabilecek tek tip bir sistem önerdiğini düşündürmemelidir. Standart kurumlarda uygulanacak risk yönetimi fonksiyonu için temel prensipler ve yönlendirmeyi esnek bir biçimde ortaya

koymakta, kurumların kendi özelliklerine uygun sistemleri geliştirip uygulamasına rehberlik etmeyi amaçlamaktadır.

Standart; **riski**, hedefler üzerinde belirsizliğin etkisi olarak tanımlarken, **risk yönetimini**, organizasyonu riskle ilgili yönlendiren ve kontrol eden koordineli faaliyetler olarak ortaya koymakta, **risk yönetim sistemini,** risk yönetimini organizasyonun bütününde devamlı olarak geliştirmek için, organizasyonel düzenlemelerin tasarlanması, uygulanması, izlenmesine imkan sağlayan bileşenler kümesi olarak değerlendirmekte, **risk yönetim sürecini** ise risklerin belirlenmesi, analiz edilmesi, ele alınması, izlenmesi ile ilgili faaliyetlerin iletişimi, istişaresi, ortam oluşturulmasına yönelik kurum politika ve prosedürlerinin sistematik olarak uygulanması biçiminde ele almaktadır.[2]

Standart ile ilgili, Şekil 2.1'de yer verilen on bir adet prensibi hatırlayacak olursak, birinci prensip, **risk yönetiminin değer katmak ve değerleri korumaya yönelik olduğunu** vurgulamaktadır. Risk yönetimi, kurum hedeflerinin gerçekleştirilmesi ile ilgili belirsizliklerin hedeflere olumlu ve/veya olumsuz etkilerinin yönetilmesini öngörmesi ile hedeflerin gerçekleştirilmesine yönelik önemli katkı sunabilir. Bu yönü ile, kurum açısından değer yaratması ve/veya değerleri koruması gerekmektedir.

İkinci prensipte, risk yönetiminin **organizasyonel süreçlere entegre olması** gerektiğinin, kurumun bütünü, faaliyetleri ve organizasyonel yapısından ayrı, bunlarla ilişkili olmayan, kendi başına ve bir fonksiyon olarak değerlendirilemeyeceğinin altı çizilmekte, risk yönetiminin, kurumun bütününün bir parçası olduğuna, kurumun süreçlerine entegre olmuş bir fonksiyon olarak ele alınacağına işaret edilmektedir.

Üçüncü prensip, risk yönetiminin **karar sürecinin bir parçası olması gerektiğini** vurgulamaktadır. Risk yönetimi sistemi, kurgusu itibariyle kurum

[2] ISO, **ISO 31000**, s.1-3.

hedeflerine yönelik risklerin anlaşılması, ele alınması, yönetilmesi ve izlenmesi ile ilgili kuruma entegre olmuş ve kurumun bütününde devamlı olarak değişimlerden kaynaklanan yeni ihtiyaçlara ayak uydurarak yürütülmesi beklenen bir fonksiyon olması sebebi ile karar süreçlerinin bir parçası olması, karar vericiler açısından kaynaklar ve hedeflerin önceliklendirilmesi, alternatiflerin ortaya koyulması vb. konularda katkı sağlaması beklenmektedir.

Dördüncü prensip, risk yönetiminin **belirsizliklerin anlaşılmasına katkı sağlaması** gerektiğini ortaya koyar. Riskin, hedeflere etki eden belirsizlikler olarak tanımlandığını dikkate aldığımızda, risk yönetim faaliyetlerinin belirsizliklerin anlaşılması, analizi, ele alınması konusunda eylemleri ve sürecin muhataplarını kurum açısından netleştireceği beklenmektedir.

Beşinci prensip, bu faaliyetlerin **sistemli, yapılandırılmış ve zamanlı** olması gerektiğine işaret etmektedir. Risk yönetimi faaliyetleri belirli bir sistem dahilinde kurgulanmalı, kurum organizayonu hiyerarşisine uygun yapılandırılmalı, belli bir zaman planı dahilinde uygulanmalıdır. Böylelikle ihtiyaç anında var olup kullanılabilen, güvenilir bilgiler üretilmesi bu performansını sürdürülebilir kılınması mümkün olabilecektir.

Altıncı prensip, risk yönetimi için **mümkün olan ve ulaşılabilen en nitelikli bilginin kullanılması** gereğidir. Gözlem, geri bildirimler, tarihsel veriler, tecrübe, öngörü, uzman görüşü gibi bilgi kaynakları düşünüldüğünde, bilgi kaynaklarındaki olası sınırlamalar ve kısıtlamalar, uzman bakış açılarındaki görüş ayrılıkları her zaman dikkate alınmalı, hesaba katılmalıdır.

Yedinci prensip, risk yönetiminin **kuruma ve/veya duruma özgü olması** gerektiğini vurgular. ISO 31000 ile bütün kurumların bütünü ve/veya seçilmiş faaliyetlerine yönelik uygulanabilecek bir standardın genel hatları ortaya koyulmuş olmakla birlikte, risk yönetimi fonksiyonu kurumun içsel, dışsal ortamına, hedeflerine, stratejilerine, yapısına, kaynaklarına, risk algısına, risk profiline bağlı olacağı için kuruma ve/veya duruma özgü bir uygulama ortaya çıkacaktır.

Sekizinci prensip, risk yönetiminin **beşeri ve kültürel faktörleri dikkate alması** gerektiğini ortaya koymaktadır. Risk yönetimi bir prosedür ve/veya bir iş akışından fazlası olup, kurumun organizasyon yapısı, kurum çalışanlarının mesleki yeterlilikleri, kurumun etik değerleri ve kurum kültürü, kurum beşeri kaynaklarının değer yargıları, algı ve bakış açıları, davranışlarının önemli ölçüde etkisi altında olacaktır. Kurumun içsel, dışsal, çevresel değişimleri algılama, ele alma yeteneklerinden etkilenecek, bu yaklaşımları yönlendirecektir. Bu yönüyle kurum kültürü ve etik değerleri ile bütünlük arz etmeli, bunlarla uyumlu politika ve prosedürler ve uygun bilgi sistemleri olanakları ile desteklenmelidir.

Dokuzuncu prensip, risk yönetiminin **şeffaf ve kapsamlı olması** gerektiğini ortaya koymaktadır. Kurumun stratejik hedefleri ile ilgili menfaat sahipleri risk yönetimi sürecine dahil olmalı ve risk algıları, risk iştahları, riskleri ele alış yaklaşımları itibariyle süreçte gerekli zamanlarda uygun ve etkili biçimde temsil edilmelilerdir. Risk yönetim süreci menfaat sahiplerinin doğru ve zamanlı biçimde temsil edilme güncelliğini koruyacak biçimde çalıştırılmalıdır.

Onuncu prensip, risk yönetiminin **değişimlere duyarlı, yineleyici ve dinamik olması** gerektiğini ortaya koymaktadır. Kurumu etkileyen iç ve dış koşullardaki değişimler süreklidir. Bu değişimler, kurum hedeflerinde, faaliyet planlarında, organizasyon yapılarında, kaynaklarında ve kaynak maliyetlerinde değişiklikler olmasına yol açar. Risk yönetim sistemi bahsettiğimiz bu unsurları kapsaması sonucu, söz konusu değişimlere, kurum strateji ve politikalarına uygun biçimde ayak uydurmalı, kurumun hedefleri üzerinde karşı karşıya kalınan ve sürekli değişim içinde olan belirsizliklerin etkilerini en faydalı ve olumlu sonuçları alacak biçimde ele alabilmelidir.

Onbirinci prensip, risk yönetiminin **organizasyonda sürekli gelişimi** ve bunun **pekiştirilmesini kolaylaştırıcı bir unsur** olması gerektiğini ortaya koymaktadır. Risk yönetiminin kurum hedeflerine ulaşılması konusunda sürdürülebilir bir makul güvence sağlayabilmesi için organizasyonun gelişimini,

olgunlaşmasını ve iş görme yeteneklerini arttırmasını kolaylaştırıcı, teşvik edici ve destekleyen bir unsur olarak tasarlanması ve uygulanması gerekmektedir.

ISO 31000 standardı bir yönetim sistemi önermekten ziyade risk yönetimi fonksiyonunu organizasyonun bütünü için çalışır ve etkili kılmak konusunda kurumları desteklemeyi hedeflemektedir. Bu nedenle kurumların, sistemin bileşenlerini kendi ihtiyaçlarına uygun biçimde yapılarına adapte etmeleri gerekmektedir.

Şekil 2.1'de belirtildiği biçimiyle ilk olarak **risk yönetimi sisteminde kurumsal direktifler ve taahhütlerin açıkça ortaya koyulması**, bunu yaparken risk yönetimi politikasının kurum kültürü ve politikalarına uygun olarak oluşturulması, ölçüm kriterlerinin kurumun performans kriterlerine uygun biçimde belirlenmesi, risk yönetimi hedefleri ile stratejik hedeflerin uyumlaştırılması, gerekli kaynak tahsisinin yapılması, organizasyonda yetki-sorumluluk dengesinin kurulması ve yapının hesap verilebilir kılınması, menfaat sahipleri arasında ve kurumda ortak risk algısının oluşturulmasına dikkat edilmelidir.

İkinci olarak atılması gereken adım, **risk yönetim sistem tasarımının gerçekleştirilmesidir.** Tasarım aşamasında, organizasyonun ve ortamının anlaşılması (sosyal, kültürel, yasal, ekonomik, finansal ortamın anlaşılması, kurum kültürü, iç ve dış menfaat sahiplerinin algısı, organizasyonun yapısı, yeterlilikleri, stratejileri, hedefleri, politikaları, bilgi sitemleri, iş standartları, iş modellerinin anlaşılması), risk yönetim politikasının oluşturulması, organizasyonun hesap verilebilir kılınması, risk yönetim sisteminin organizasyonun süreçlerine entegre edilmesi, gerekli kaynakların tahsisi, dış iletişim ve raporlama mekanizmalarının ve kanallarının oluşturulması aşamaları kritik aşamalar olarak vurgulanmaktadır.

Sonrasında atılacak adımlar sırası ile tasarlanan risk yönetimi sisteminin **kuruma uyarlanması** (uyarlama konusunda uygun zamanlamanın belirlenmesi, politikalar, yasalar ve düzenlemelerle uygunluğun sağlanması, menfaat sahipleri ile istişareler sonucu sistem içinde onların ilgisinin de temsilinin

sağlanması, kurumda ortak algının oluşturulması ve gerekli eğitimlerin verilmesi, üst yönetim desteğinin alınası), sistemin **izlenmesi ve gözden geçirilmesi** (risklerin düzenli olarak ölçülmesi, tanımlı göstergelerle karşılaştırılması, değişimlerin ortaya koyularak muhataplarla iletişimi, risk yönetim sisteminin etkinliğinin ölçülmesi ve izlenmesi) ve sistemin **sürekli gelişiminin** sağlanması olarak ortaya koyulmaktadır.

ISO 31000 standardında öngörülen risk yönetim süreci ile ilgili adımlar ve bunların sistem ve prensiplerle ilişkisi Şekil 2.1' de ortaya koyulmuştur. Bahsi geçen sürece daha yakından bakılacak olursa; sürecin, yönetim fonksiyonunun entegre bir parçası olarak ele alındığı, kurum kültür ve iş yapış biçimlerinin içine oturtulduğu ve kuruma özgü şekillendirilmesi gerektiği görülür.

Standartta ele alınan risk yönetim süreci ile ilgili; iç ve dış muhataplar ve menfaat sahipleri ile iletişim ve istişarelerin yapılması, kurumun içsel ve dışsal ortamın oluşturulması, risk yönetim süreci ile ilgili ortamın hazırlanması, risk kriterlerinin belirlenmesi, risk tanımlarının yapılması, risk analizlerinin yapılması, risk değerlendirmelerinin yapılması, riskleri ele alış biçimlerinin belirlenmesi, izleme ve gözden geçirme adımlarının belirlenmesi ve sonuçların kaydedilerek kurum hafızası ve karşılaştırma ortamının hazırlanması kritik alt süreçler olarak ele alınmaktadır.

ISO 31000 standardı ile risk yönetimi konusunda genel standartlar ve genel bir kılavuz hazırlanmıştır. Standart, belirli bir endüstri veya iş kolu faaliyeti için değil, tüm kurumların her türlü yapısı için ve herhangi bir zamanda uygulanabilir çerçevede bir öneri niteliğindedir. Ancak, bünyesinde etkili bir risk yönetimi fonksiyonu çalıştırmak ve bunu gelişen, olgunlaşan yapısı içinde sürekli kılmak isteyen kurumlar açısından, satandart genel bir düzenleme olarak görülüp, birebir uygulanmak yerine referans alınması gerekir. Kurumların özelinde, kendi stratejileri, hedefleri, etkileşimleri, ortamı, organizasyon yapısı, menfaat sahipleri, öncelikleri ve kaynakları dikkate alınarak ortaya koyulan genel yapının kurum özeline uyarlanması ve uygulanması tavsiye edilir.

Çalışmamızın üçüncü bölümünde örnek şirketimiz için tasarlayıp uyarlayacağımız kurumsal risk yönetimi siteminde ISO 31000 standardının düzenlemelerinden de yararlanılacak olmakla birlikte, gerek kapsam genişliği, gerekse aldığı geri bildirimler dikkate alındığında, günümüzde bahsi geçen risk yönetim sistemleri içinde kendisine en geniş uygulama alanını bulmuş ve konusunda en kapsamlı çalışma olarak kabul edilen COSO KRY Çerçeveleri örnek şirketimize uyarlanacak KRY çerşevesinin temelini oluşturmaktadır.

2.3. COSO Kurumsal Risk Yönetimi Çerçeveleri

Kurumlar ortaya koydukları faaliyetleri itibariyle kurucuları ve/veya yatırımcıları için değer yaratmak ve bunu sürdürmek ile ilgilenirler. Kurumlar faaliyette bulunurken pek çok belirsizlik ile karşılaşmaktadırlar. Belirsizlikler bazı hallerde kurum stratejilerinin gerçekleştirilmesine dönük fırsatlar içerirken bazı hallerde de tehditler içermektedir. Öte yandan kurumun etki altında kaldığı içsel ve dışsal faktörler hızlı bir değişim içindedir ve bu değişim, fırsatlar ve tehditlerin tanımlanması, anlaşılmasını ve yönetilmesi konusuna sistemsel yaklaşımları zorunlu kılmaktadır.

COSO KRY-2004 , aşağıda yer verdiğimiz tanımında da işaret edildiği gibi, kurumun her düzeydeki çalışanları tarafından organizasyonun her seviyesinde uygulanan, kurumu stratejik hedeflerini gerçekleştirmeyi makul düzeyde güvence altına almaya yönelik tasarlanmış, yaşayan bir **süreçtir.**

> "*Kurumsal risk yönetimi, sistemi bir süreçtir, kurumun yönetim kurulu, yönetimi ve tüm çalışanları tarafından strateji belirlemede, kurumun tüm seviyelerinde uygulanır, kurumu etkileyebilecek olayları belirlemek, riskleri kurumun risk iştahına uygun biçimde yönetmek ve kurum hedeflerinin gerçekleştirilmesi ile ilgili makul bir güvence vermek üzere tasarlanmıştır."* [3]

[3] COSO, **Executive Summary Enterprise Risk Management**, September 2004, (Çevrimiçi) http//www.coso.org, 20 Mayıs 2016

COSO KRY-2004, kurum hedeflerinin **stratejik, operasyonel, raporlama ve mevzuata uygunluk** olmak üzere dört farklı alanda gruplanmasını öngörerek kurumsal risk yönetiminin farklı yönlerine odaklanmayı mümkün kılmayı amaçlamaktadır. Dört grupta toplanan kurum hedeflerinin gerçekleştirilmesi konusunda makul bir güvence vermeyi hedefleyen COSO KRY-2004, **içsel ortam, hedeflerin belirlenmesi, olayların tanımlanması, risklerin değerlendirilmesi, risklerin giderilmesi, kontrol faaliyetleri, bilgi ve iletişim** ve **izleme** olmak üzere toplam sekiz bileşenden oluşmaktadır.

COSO KRY-2017 ise risk yönetimi sürecini *" organizasyonların, değer yaratırken, korurken ve arttırırken, riskleri yönetmek için güvenebilecekleri, stratejinin oluşturulması ve yürütülmesi ile entegre kültür, yetkinlik ve uygulamaları"* [4] şeklinde tanımlayarak, değer yaratmayı, arttırmayı, bu durumu sürdürmeyi odağına koymaktadır.

Etkili bir kurumsal risk yönetimi uygulamasının faydaları; fırsat portföyünün artması, risklerin tüm kurum sathı için belirlenmesi ve yönetilmesi, olumlu sonuçların ve avantajların artması, olumsuz sürprizlerin azalması, performans dalgalanmalarının azaltılması, kaynak çeşitliliğinin geliştirilmesi, kurum esnekliğinin yükseltilmesi olarak tanımlanan yeni çerçeve beş temel bileşen ve bunları destekleyen yirmi prensip ile yapılandırılmaktadır.[5]

COSO KRY- 2017 kapsamı COSO KRY-2004'ten daha geniş olup, güncellenmiş versiyonun bileşenleri, COSO KRY-2004 bileşenlerini kapsamaktadır. Daha soyut ve karmaşık bir yapıya sahip olan COSO KRY-2017'nin daha kolay anlaşılabilmesi için bir önceki versiyonun hangi bileşenlerini ne ölçüde kapsadığı, hangi konularda kapsamı genişlettiği bir karşılaştırma tablosu ile ortaya koyulmaktadır. Aşağıda, Tablo 2.1'de iki çerçeve kapsamları arasındaki ilişki belirtilmektedir.

[4] COSO, **Enterprise Risk Management-Integrating with Strategy and Performance**, June 2017, (Çevrimiçi) http//www.coso.org, 05 Nisan 2019
[5] A.e

Tablo 2.1: 2004 ve 2017 Kurumsal Risk Yönetimi Çerçeveleri Karşılaştırması

2017 Çerçevesi Bileşenleri	No	2017 Çerçevesi Prensipler	2004 Çerçevesinde Bulunuyor mu?	2004 Çerçevesi Bileşenleri
Yönetişim ve Kültür	1	Yönetim Kurulu Risk Gözetimini Gerçekleştirir	EVET	İçsel Ortam
	2	Operasyonel Yapıyı Oluşturur	EVET	
	3	Arzu Edilen Kültürü Tanımlar	EVET	
	4	Temel Değerlere Bağlılık Gösterir	EVET	
	5	Yetenekli Bireylerin İlgisini Çeker, Geliştirir ve Organizasyonda Tutar	EVET	
Strateji ve Hedef Oluşturma	6	İş Ortamını Analiz Eder, İnceler	EVET	Hedeflerin Belirlenmesi
	7	Risk İştahını Tanımlar	EVET	
	8	Alternatif Stratejileri Değerlendirir	HAYIR	
	9	İş Hedeflerini Belirler	KISMEN	
Performans	10	Riskleri Tanımlar	EVET	Olayların Tanımlanması
	11	Risklerin Şiddetini Değerlendirir	KISMEN	Risklerin Değerlendirilmesi
	12	Riskleri Önceliklendirir	EVET	
	13	Risk Cevaplarını Uyarlar ve Uygular	EVET	Risklerin Giderilmesi ve Kontrol Faaliyetleri
	14	Portföy Bakış Açısını Geliştirir	EVET	Risklerin Giderilmesi
Gözden Geçirme ve Revizyon	15	Önemli Değişiklikleri Değerlendirir	EVET	İzleme
	16	Risk ve Performansı Gözden Geçirir	EVET	
	17	Kurumsal Risk Yönetimindeki Gelişmeleri İzler	EVET	
Bilgi, İletişim ve Raporlama	18	Bilgi veTeknolojinin Katkısını Kaldıraçlandırır	EVET	Bilgi ve İletişim
	19	Risk Bilgisinin İletişimini Yapar	EVET	
	20	Risk, Kültür ve Performansı Raporlar	EVET	

Kaynak: Kyleen Prewet, Andy Terry, "COSO's Updated Enterprise Risk ManagementFramework-A Quest For Depth And Clarity", **The Journal of Corporate Accounting And Finance,** July 2018 , Wiley Periodicals Inc. s.19, (Çevrimiçi) www.wileyonlinelibrary.com, 06 Mayıs 2019

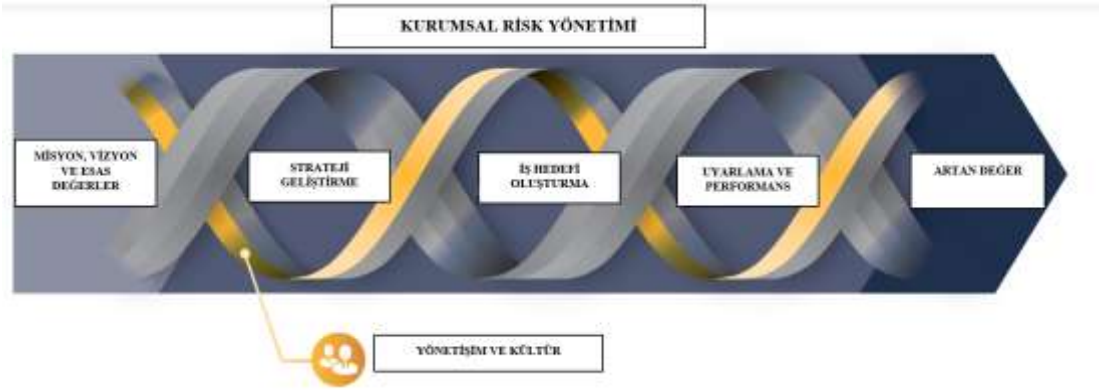
Tablo 2.1'den izlenebileceği gibi, COSO KRY-2017 bileşenleri itibariyle COSO KRY-2004'ün kapsamını belli alanlarda genişletmiştir. COSO KRY-2017 bileşenlerin birbiriyle sarmal ilkişkisi ve kapsamları nedeniyle COSO KRY-2004 çerçevesini bir miktar daha "**kurumsal yönetim**" çizgisine yaklaştırmaktadır.

2.3.1. COSO Kurumsal Risk Yönetimi-Strateji ve Performansa Entegre Çerçeve Bileşenleri

2.3.1.1. Yönetişim ve Kültür

COSO KRY-2017'nin birinci bileşeni olan **yönetişim ve kültür**, Şekil 2.4'te gösterilen beş prensip ile desteklenmekte ve COSO KRY-2004'ün birinci bileşeni olan **içsel ortam** bileşenini ile örtüşmektedir. Her beş prensip içerik ve kapsamları COSO KRY-2004 çerçevesinde içsel ortam bileşeninin unsurları iken, bu içerikler yeni çerçevede birinci bileşenin altında beş ayrı prensip olarak ifade edilmekte ve gruplanmaktadır.

Şekil 2.4: COSO KRY-2017 Yönetişim ve Kültür Bileşeni



Prensipler:

1- Yönetim Kurulu risk gözetimini gerçekleştirir.

2- Operasyonel yapıyı oluşturur.

3- Arzu edilen kültürü tanımlar.

4- Temel değerlere bağlılık gösterir.

5- Yetenekli bireylerin ilgisini çeker, geliştirir ve organizasyonda tutar.

Kaynak: COSO, **Enterprise Risk Management-Integrating with Strategy and Performance**, June 2017, (Çevrimiçi) http//www.coso.org, 05 Nisan 2019

Bileşen ve altında gruplanan prensiplerin, performans ve strateji ile entegre olarak, tüm çerçeve ile sarmal bir ilişkide olması kurgulanmaktadır.

COSO KRY-2017'de yönetişim ve kültür bileşeninin kapsamı organisasyonun tarif edilmesi, kurumsal risk yönetiminin kurulması, kuvvetlendirilmesi, gözetim sorumluluklarının belirlenmei, öneminin vurgulanması, kurum kültürünün, etik değerlerin tarif edilmesi, yaşatılması ve kurum içinde **risk** olgusunun anlaşılması olarak tarif edilmektedir.[6]

COSO KRY-2004'ün birinci bileşeni olarak tarif edilen **içsel ortam**, ile kurumun çalışma tarzı ve iş yapış biçimi kast edilmektedir. COSO KRY-2004 çerçevesinde içsel ortam aşağıdaki gibi değerlendirilmektedir. [7]

[6] COSO, **Enterprise Risk Management-Integrating with Strategy and Performance-Executive Summary**, June 2017, (Çevrimiçi) http//www.coso.org, 05 Nisan 2019

[7] Özbek, **İç Denetim**, s.289

"İçsel ortam çalışanların risk algısını etkileyen kurumun atmosferini yansıtır. KRY' nin diğer bileşenleri için bir disiplin ve yapı oluşturur. Kurumun risk felsefesini, risk iştahını, YK gözetim seviyesini, etik değerlerini, çalışan yeterlilik seviyelerini, yöneticilerin yetki ve sorumluluk dağılımını, onları organize etme ve geliştirme usullerini içermektedir."

Firmanın etkileşim içinde olduğu iç ve dış faktörlerdeki değişim baskısı (ortaklar, ticari beklentiler, sermaye yapısı, rekabet, teknoloji, tüketici ihtiyaçları, yasal düzenlemeler vb.) firmanın çalışma tarzını, yönetişimini ve kültürünü etkileyecek ve değişecektir. Bu durum değişim trendleri ve ivmesine bağlı olarak süreklilik gösterecektir. Yönetişim ve iş yapış tarzının sürekli değişerek şekillenmesinde kurum kültürü de çok önemli rol oynar. Bu noktada kurum içinde dökümante edilsin, edilmesin, varlığını hissettiren ve iş yapış biçimini yakından etkileyen kurum kültürünün KRY sistemine uygunluğu, yönetim kurulu ve üst yönetimin sahip olmak istediği kurum kültürü ile kurumda benimsenmiş davranış değerlerinin uyumluluğu mesai verilmesi gereken bir alandır. Etkili bir kaynak planlaması, yönetim kurulu ile üst yönetimin KRY sisteminden beklentilerinin gerçekçi bir şekilde belirlenmesi, desteklerinin uzun vadeli sağlanması için değerlendirilmesi gereken kritik konular; yönetim kurulu ve üst yönetimin KRY sistemini isteyip istemediği ve destekleyip desteklemediği, bu konudaki motivasyonun ne düzeyde olduğu ve nereden kaynaklandığı, orta vade ve uzun vadede ticari beklentilerinin rasyonel olup olmadığı, kurumda ortak bir risk algısı ve ortak bir risk yönetimi terminolojisi ne düzeyde yaratılmış olduğu, kurum kültürünün KRY sistemi uygulamalarını desteklemeye uygun olup olmadığı, kurumun etik değerlerinin varlığı, bu etik değerlere bağlılık seviyesinin KRY sistemini ne ölçüde desteklediği, düzenlenmiş rekabet kurallarına uyum becerisinin ne durumda olduğu, şirketin vizyonu, misyonunun ortaya koyulmuş olup olmadığı ve çalışanlarla bunun iletişiminin yapılıp yapılmadığı, şirket vizyonu ve misyonunun KRY sistemi uygulamalarını ne düzeyde desteklediği, kurum kaynaklarının mevcut yetkinlikleri ve kalitesinin KRY sistemini ne düzeyde desteklediği, insan kaynağı kalitesi ve yetkinlikleri, teknolojik alt yapı- hem ölçme, raporlama hem de kurum içi eğitim ve

iletişim olanaklarının KRY sistemi uygulamalarına uygunluğu, gereken kaynak tahsisi ve yatırım bütçesinin boyutu olarak sıralanabilir.

Kurum kültürünün KRY sistemini desteklemesi için göz önüne alınması gereken unsurlar; kurum içi yetki ve sorumluluk sınırlarının belirlenip belirlenmediği, iş yapmada öne çıkan ilişki tarzının resmi mi, gayri resmi mi olduğu, ekip çalışmasına önem verilip verilmediği, bireysel performansın ön planda olup olmadığı, organizasyon ve buna bağlı olarak yönetici – çalışan ilişkileri hiyerarşisinin dikey mi, yatay mı olduğu, çalışanların kurumu ne ölçüde içselleştirmiş ve gelecekleri ile kurumun geleceğini ne ölçüde örtüştürmüş oldukları biçiminde sıralanabilir.

2.3.1.2. Strateji ve Hedef Oluşturma

COSO KRY-2017 çerçevesinin ikinci bileşeni olan **strateji ve hedef oluşturma,** Şekil 2.5'te gösterildiği gibi, altında gruplanmış dört ana prensip ile desteklenmektedir.

Şekil 2.5: COSO KRY-2017 Strateji ve Hedef Oluşturma Bileşeni

Prensipler:

6- İş ortamını analiz eder, inceler.

7- Risk iştahını tanımlar.

8- Alternatif stratejileri değerlendirir.

9- İş hedeflerini belirler.

Kaynak: COSO, **Enterprise Risk Management-Integrating with Strategy and Performance**, June 2017, (Çevrimiçi) http//www.coso.org, 05 Nisan 2019

Strateji ve hedef oluşturma bileşeni, COSO KRY-2004 çerçevesinin ikinci bileşeni olan **hedeflerin belirlenmesi** bileşeninden daha geniş kapsamlıdır. Risk ortamının analiz edilmesi ve incelenmesi ile risk iştahının tanımlanmasını düzenleyen prensiplerin içerikleri COSO KRY-2004 hedeflerin belirlenmesi bileşenini kapsamaktayken, iş hedeflerinin belirlenmesi ile ilgili prensip COSO KRY-2004 hedeflerin belirlenmesi bileşenine göre daha geniş kapsamlı olup, alterntif stratejilerin değerlendirilmesi ile ilgili prensip yeni bir kapsamdır.

COSO KRY-2004' ün, ikinci bileşeni, **hedeflerin belirlenmesi** ile ilgili değerlendirmesi aşağıdaki gibidir. [8]

> *"Kurum hedefleri stratejik hedefler seviyesinde belirlenir ve operasyonel, raporlama ve mevzuata uyum hedeflerine temel teşkil ederler. Her kurum içsel ve dışsal nedenlerden kaynaklanan çeşitli risklerle karşılaşır ve risk tanımlama, değerlendirme, ve riskleri giderme süreçlerinin etkili olabilmesi için kurum hedeflerinin belirlenmesi gerekir. Kurum hedefleri risk toleransını etkileyen risk iştahı ile uyum içinde olmalıdır."*

[8] A.e., s.299

Risk iştahı kurumun almaya hazır olduğu risk seviyesidir. Risk iştahı yönetim kurulu tarafından belirlenmeli, kurum içinde sürekli iletişimi yapılmalıdır.

Risk toleransı ise riskin gerçekleşmesi durumunda kurumun katlanabileceğini düşündüğü olumsuz durumun seviyesidir.

> *"Risk iştahı, stratejik olup, kurum hedeflerinin gerçekleştirilmesine yöneliktir, kurumsal yönetimin bütünleyici parçasını oluşturur, kaynak dağıtımını yönlendirir, kurumun riski belirleme, değerlendirme, giderme ve izleme fonksiyonları ile ilgili alt yapısı açısından yönlendiricidir, kurumun riske karşı tutumu açısından belirleyicidir, uzun vadede stratejik planlama döngüsünün parçası olmak ve kısa vadede değeri gerçekleştirme çabalarına konu olmak açısından çok boyutludur, riskin ve kurumun sürdürülen risk iştahının etkili şekilde izlenmesine ihtiyaç gösterir."* [9]

COSO KRY-2017 çerçevesinin strateji ve hedef oluşturma bileşeni, iş ortamının analiz edilmesi, risk iştahının tanımlanması ile yetinmeyip, stratejik planlama ve strateji ile hizalı ve entegre bir risk iştahı üzerinde durmaktadır.

Risk iştahı kurumun değişen stratejilere ve iş hedeflerine göre durumsallık gösterecektir. Kurumsal risk yönetimi, stratejik planlama ve iş hedeflerinin oluşturulması ile entegre çalışacak bir proses olmalıdır. İş hedefleri ve stratejinin uygulanması, riski tanımlarken, değerlendirirken ve riske karşılık verirken bir baz oluşturacaktır.[10]

Risk iştahı ile ilgili bir örnek verilmesi gerekirse; kurum tarafından, ticari alacakları için teminat talep edilmesi bir politika olarak benimsenmiş, bu durum risk iştahı açısından alacaklarının tahsil edilememesi riskinin alınmak istenmediğini gösterecektir. Kurumun, alacakların teminat altına alınması konusunda her bir cari hesap alacağının "%80'i teminatlı, %20 si teminatsız olsun" deniyorsa,

---

[9] Larry Rittenberg, Frank Martens, "Understanding and Communicating Risk Apetite," **Thought Leadership in ERM**, January 2012, s.3, (Çevrimiçi) http//www.coso.org, 17 Mayıs 2016.
[10] COSO, **Enterprise Risk Management-Integrating with Strategy and Performance-Executive Summary**, June 2017, (Çevrimiçi) http//www.coso.org, 05 Nisan 2019

alacak tahsilat riski ile ilgili %20 tolerans aralığı belirlenmiş olacaktır. Ek olarak "kabul edilebilir teminat sadece banka teminat mektubu olmalıdır, ipotek teminat sayılmaz" gibi bir teminat tanımlanmışsa, risk iştahı açısından alacak tahsil riskinin %80'ini banka teminat mektubu ile garanti altına alınmak istendiğini ifade edilmekte, bunun müşteri portföyü genişlemesi üzerindeki olası baskıları ve satış baskısı kabul edilmiştir. Yine bu konuda "teminatların en az yarısının banka teminat mektubu olması, diğer yarısının ipotek veya teminat senedi olabileceği" şeklinde bir politika belirlenmişse, burada da teminat portföyü açısında farklı bir risk iştahına işaret ediliyordur.

Kurum açısından en önemli konulardan bir tanesi, risk iştahının yönetim kurulu seviyesinde tespiti ve riskler karşısında sürdürülen risk iştahının izlenerek kurum içi iletişiminin açık biçimde yapılmasıdır.

2.3.1.3. Performans

COSO KRY-2017 çerçevesinin üçüncü bileşeni olan **performans,** Şekil 2.6'da de gösterildiği gibi, altında gruplanan beş ana prensip ile desteklenmektedir.

Şekil 2.6: COSO KRY-2017 Performans Bileşeni

Prensipler:

10- Riskleri tanımlar.

11- Risklerin şiddetini değerlendirir.

12- Riskleri önceliklendirir.

13- Risk cevaplarını uyarlar ve uygular.

14- Portföy bakış açısını geliştirir.

Kaynak: COSO, **Enterprise Risk Management-Integrating with Strategy and Performance**, June 2017, (Çevrimiçi) http//www.coso.org, 05 Nisan 2019

COSO KRY-2017 çerçevesinin en geniş vurgusu strateji ve performans ile entegre çalışması gerekliliğidir. Performans bileşeni ve altında gruplanan prensiplerin kapsamı COSO KRY-2004 çerçevesinin, **olayların tanımlanması, risklerin değerlendirilmesi, risklerin giderilmesi ve kontrol faaliyetleri** olmak üzere dört bileşeni ile örtüşmektedir. Performans bileşeni altında gruplanmış risklerin **şiddetinin** değerlendirilmesi ile ilgili prensip tarafından, risk değerlendirme olgusunun kapsamını genişletilerek, risklerin iş hedefleri ve stratejilere olacak etkilerinin şiddetinin ölçülmesine dikkat çekilmektedir.

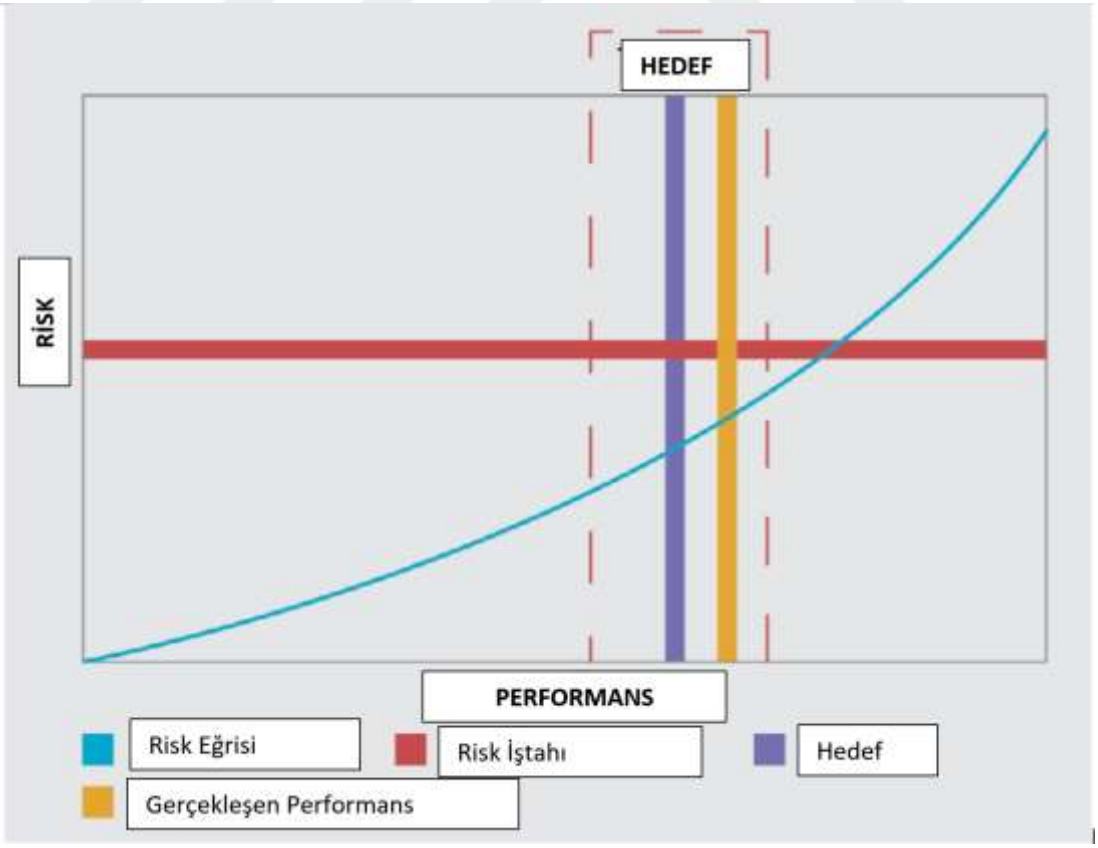
COSO KRY-2017 çerçevesinde, performans bileşeni ile; kurum stratejisinin ve iş hedeflerinin başarılmasına etki eden risklerin tanımlanması ve değerlendirilmesi gerektiği, risklerin risk iştahı içinde, sonuçları etkileme şiddetine göre önceliklendirilmesi gerektiği, organizasyonun risk cevapları ile birlikte öngördüğü risk portföyüne odaklanması ve bu sürecin sonuçlarının ilgili çıkar sahiplerine raporlanması gerektiği ifade edilmektedir.[11]

[11] A.e.

Risk iştahı, risklerin şiddetinin değerlendirilmesi, risklerin önceliklendirilmesi, kurumun risk profilinin oluşlturulması süreci, stratejik plan ve belirlenen iş hedefleri ile ilişkili olacaktır. Stratejideki değişiklikler ve/veya iş hedeflerindeki değişiklikler kurumun risk profilini ilgili strateji ve/veya iş hedefi doğrultusunda değiştirecektir. Alternatif stratejiler ve/veya iş hedefleri için değerlendirilmesi gereken risk profilindeki değişiklikler, risklere cevaplar bir risk portföyü oluşturacağı ve bu portföyün izlenmesi, alternatif stratejiler ve/veya iş hedefleri ile portföyün çeşitlendirilmesi, tüm bu süreç ile entegre çalışacak bir kurumsal risk yönetimi anlayışı ile kurumun performansına bağlı oluşacak değerinin arttırılması ve sürdürülebilir kılınması için çalışılabilecektir.

Şekil 2.7 ile kurumun risk profili örneği ve etkileşim unsurları gösterilmektedir.

Şekil 2.7: Risk Profili



Kaynak: COSO, **Enterprise Risk Management-Integrating with Strategy and Performance**, June 2017, (Çevrimiçi) http//www.coso.org, 05 Nisan 2019

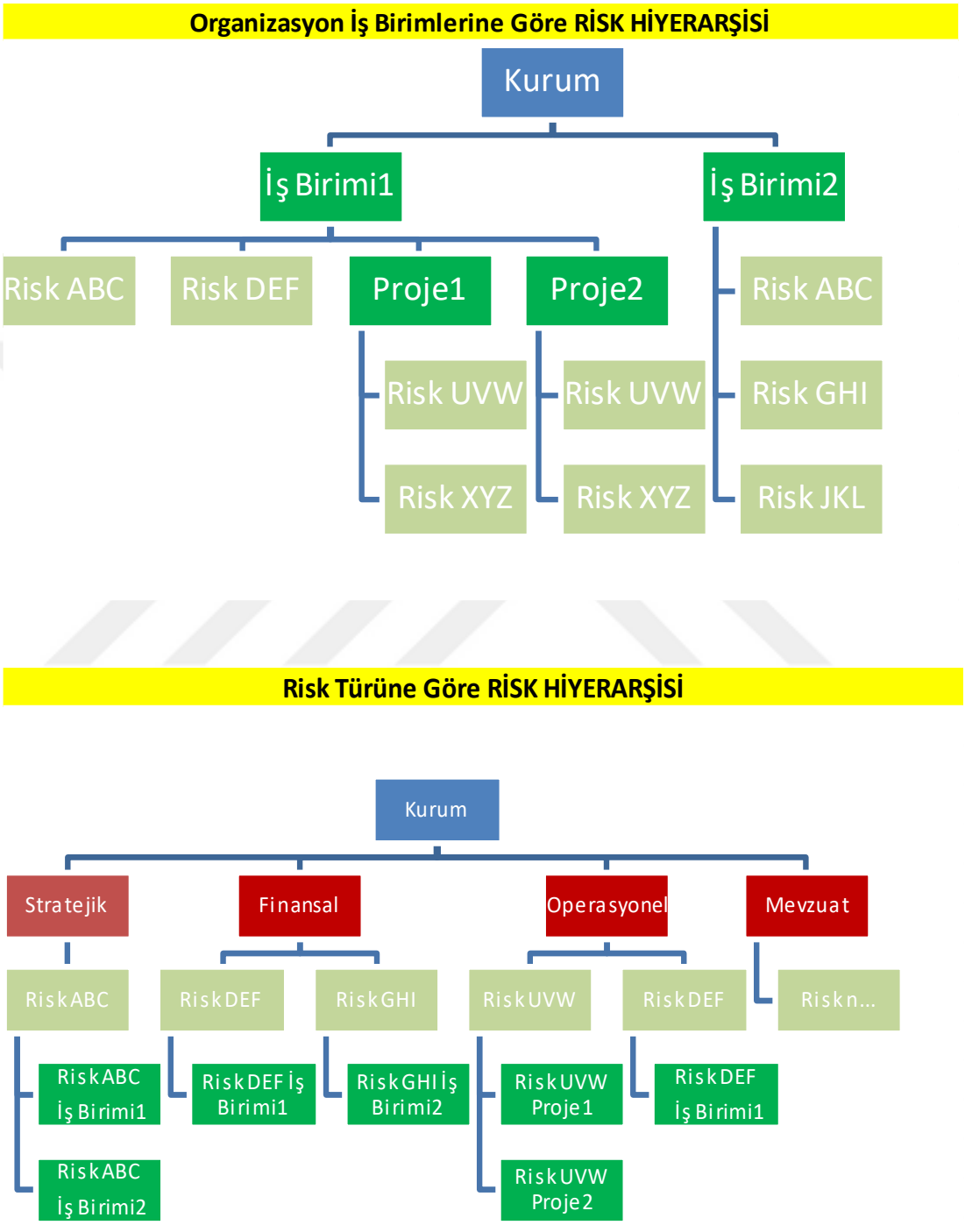
KRY sistemi tasarımı ve uyarlanması çalışmasına başlayan kurumda risk tanımı konusunda geniş katılımlı bir mutabakat sağlanması, ortak risk yönetim metodolojisinin geliştirilmesi ve risk farkındalığının kurum nezdinde yükseltilmesi çalışmalarının gerekliliğine değinmiştik. Bu aşama, kurumda ortaya koyulmuş, vizyon ve misyona hizmet eden ana stratejiler ile bunların alt stratejileri açısından belirsizlik taşıyan, sonuçları itibariyle bu stratejileri olumlu veya olumsuz etkileyebilecek olayların tanımlandığı aşamadır. Bu durum, riskler ve fırsatlar olarak ifade edilebilecek, olası olumsuz sonuçlar ve olumlu sonuçlar doğurabilecek olayların ana faktörler itibariyle gruplanmasına, bu gruplar altında söz konusu olabilecek olayların ve beklenen etkilerinin tarif edilmesine, kurum adına detaylı bir **risk envanteri** oluşturulmasına imkan vermektedir. Bu sayede sonraki adımlarda söz konusu risklerin değerlendirilmesi ve yönetilmesi için sistematik yaklaşımlar geliştirmesi için çalışılması mümkün olacaktır.

Risk sınıflandırması kuruma özgü olup doğru ya da yanlışı yoktur. Süreç, kurum özelinde risk ve fırsatların neler olabileceğinin tespiti ile ilgili olup, kuruma özgüdür.

Risk gruplaması veya başka deyişle risk hiyerarşilerinin ortaya koyulmasında, organizasyondaki iş birimlerine ve fonksiyonlara yönelik riskler ilgili departman hedefleri, operasyonel hedefler, stratejiler ve alt stratejiler ve altında toplanarak yapılabilir ki buna organizasyon **iş birimlerine göre risk hiyerarşisi** denilir. Gruplama risk çeşitlerine göre yapılırsa da buna da **risk türlerine göre hiyerarşi**, denilir.

Çeşitli kaynaklarda çeşitli risk gruplama örnekleri yer almaktadır. Bunlardan üç tanesi Şekil 2.8, Tablo 2.2 ve Tablo 2.3'te gösterilmektedir.

Şekil 2.8: İş Birimine Göre ve Risk Türüne Göre Risk Hiyerarşileri



Kaynak: Curtis, Carey, "**Risk Assesment in Practice**", s.14

Tablo 2.2: Risk Gruplama Örneği

Stratejik Riskler		
Dışsal Faktörler		İçsel Faktörler
- *İş koluna ait riskler*		- *İtibara yönelik riskler*
- *Ekonomiye ait riskler*		- *Strateji odağına ilişkin riskler*
- *Rekabetin riskleri*		- *Ana şirket desteğine ilişkin riskler*
- *Yasal düzenleme ve mevzuat değişikliği riskleri*		- *Marka/patent koruma riskleri*
- *Müşteri ihtiyaç ve isteklerine yönelik riskler*		
Operasyonel Riskler		
Proses Riskleri	Mevzuat Riskleri	İnsan Kaynağı Riskleri
- *Tedarik zinciri*	- *Çevresel riskler*	*İnsan kaynağı*
- *Müşteri tatmini*	- *Mevzuat uygunluğu*	*Çalışan dönüş hızı*
- *Döngü riski*	- *Politika ve prosedürler*	*Performans ödül programları*
- *İcra riski*	- *Yasal düzenlemeler*	*Eğitim zaafiyet ve eksiklikleri*
Finansal Riskler		
Hazine İşlemleri	Kredi İşlemleri	Ticari İşlemler
- *Faiz oranı*	- *Limit riski*	- *Ürün fiyatriski*
- *Kur riski*	- *Teminat riski*	- *Sürdürülebilirlik riski*
- *Sermaye yeterliliği*	- *Temerrüt riski*	- *Ölçüm riski*
	- *Ödeme riski*	
Bilgi teknolojileri Riskleri		
Mali İşler	Operasyon	Teknoloji
Muhasebe standartları	Fiyatlama	Bilgi erişimi
Bütçe	Performans	İş sürdürülebilirliği
Finansal raporlama	Ölçüm	Virüs
Vergi	Çalışan güvenliği	Ulaşılabilirlik
Mevzuat		Alt yapı

Kaynak: Robert R Moeller,**COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance Process,** 2.bs**,** New Jersey,John Wiley&Sons,Inc.,2011, s.35

Tablo 2.3: Üretim Şirketleri İçin Risk Gruplama Örneği

Üretim Şirlketi İçin Önerilen Risk Türlerine Göre Gruplama		
Dışsal Faktörler		
Rekabet	Tedarikçi	İktidar
Mevzuat	Politik	Felaketler
Hissedarlar	Satınal-alınma	Sermaye yeterliliği, varlığı
Çevresel düzenlemeler	Bilinirlik	Kontratlar
İçsel Faktörler		
Stratejik	Finansal	Operasyonel
Strateji geliştirme	*Ürün fiyatlama*	*Ürün kalitesi*
Hizalanma	*Transfer fiyatlama*	*Üretim kapasitesi*
Kaynak tahsisi	*Tahsilatlar*	*Döngü zamanı*
Kesişen işler	*Faiz oranları*	*Verimlilik*
	Kur	*Tamir-bakım*
Teknoloji	*Likidite*	*Tedarik kanalları*
Mevcudiyet, bulunabilirlik	*Kredi*	*Dağıtım*
Doğruluk		*Müşteri memnuniyeti*
Gizlilik		*Operasyonel mevzuata uygunluk*
Kullanışlı olmak		*İş kesintileri*
Verimlilik		*Fiziksel güvenlik*
	Bilgi /Finansal mevzuat/	*Ürün geliştirme*
İnsan kaynakları	Yönetim Raporlaması	*Marka imajı*
Mevcudiyet, bulunabilirlik	*Var olmak*	*Pazarlama ve reklam*
Mesleki yeterlilik	*Bütünlük*	*İş performansı*
Güvenlik	*Kesinlik, tamlık*	*Değişim yönetimi*
Doğruluk	*Mülkiyet*	
İletişim	*Ortaya çıkarma*	
Liderlik	*Değerlemeler*	
Ödüllendirme		
Çoklu kültür		

Kaynak: IIA, **Sawyer's Guide for Internal Auditors**,2c.,6. bs., The Institute of Internal Auditors Research Foundation, 2012, s.9.

Risk gruplamaları konusunda yapılacak çalışma her kurum için özgün olacaktır. Ancak odaklanılacak çerçevenin genişliği dikkate alındığında konu hakkında kabul görmüş saygın danışman firmalar tarafından kurgulanmış risk gruplama modellerinden yararlanılabilir veya işletmeye özgü bir model geliştirilebilir.

İşletme uygulamamızda, ele alınan işletmeye özgü bir risk gruplama modeli tasarlanacaktır. Kurumlara özgü risk modeli tanımlanırken ve/veya danışman firmalarca ortaya koyulmuş bir risk gruplama modeli kuruma uygulanırken etkili sonuçlar alınabilmesi için; kurum nezdinde risk kavramı tanımı mutabakatı sağlanmasına, ortak bir risk kültürü ve terminolojisi oluşturulmasına, kurum risk farkındalığının kabul edilebilir seviyeye yükseltilmesine, arama konferansları, mülakatlar, anketler, iş akış analizleri vb. yöntemlerle çalışmaya geniş tabanlı bir katılım sağlanmasına dikkat edilmesi gerekmektedir. Tüm bu çalışmaların sistematik olarak bir araya getirilmesi ile ana risk grupları ve alt risk gruplarını barındıran, risklerin detaylı tarif edildiği **kurum risk envanteri** oluşturulur.

Risklerin gruplanmasının ardından ana risk grupları, alt risk grupları ve detaylı risklerin teker teker gerçekleşmesi durumunda ortaya çıkabilecek olumsuz etkilerin sayısal ve/veya sayısal olmayan yöntemlerle değerlendirilerek ve ölçülerek önceliklendirildiği aşama **risk değerlendirme sürecidir**. Bu sayede risk yönetimi süreci açısından doğru odaklanma ve verimli, etkili kaynak kullanımı söz konusu olur, riskler değerlendirilmiş ve önceliklendirilmiş olarak bir sonraki aşamada planlanacak "riskleri giderme" aksiyonları için doğru bir odaklanma sağlanır.

Bu aşamada sayısal ve sayısal olmayan yöntemlerle risklerin gerçekleşme olasılıkları ve gerçekleştikten sonra ilgili stratejiye olacak olumsuz etkileri puanlanır, bu değerlendirme ışığında riskler önceliklendirilmiş olarak bir araya getirilir ve kurumun **risk haritası** oluşturulur.

Sayısal olmayan risk değerlendirme çalışmaları temelde sübjektif derecelendirmelerin üzerine kuruludur. Sayısal risk değerlendirme tekniklerinde ise olasılık hesaplarından ve istatistik modellerden yararlanılır.

Olasılık temelli tekniklerde riske maruz değer, kayıplara yol açan olayların değerlendirilmesi, geriye dönük testler gibi yaklaşımlardan bahsedilirken, olasılık temelli olmayan sayısal değerlendirme yöntemlerinde duyarlılık analizleri, senaryo analizleri, stres testi, karşılaştırma tekniklerinden bahsedilir. Karşılaştırma

tekniklerinde **sektörel** veya **rakibe göre** karşılaştırma, **kendinle karşılaştırma** ve **en iyi uygulamayla** karşılaştırma olmak üzere üç temel karşılaşma vardır. Risk değerlendirme tekniklerinde sayısal ve sayısal olmayan yöntemlerin avantaj ve dezavantajları Tablo 2.4 'te topluca gösterilmektedir.

Tablo 2.4: Risk Değerlendirme Teknikleri Avantaj ve Dezavantajları

Teknik	Avantaj	Dezavantaj
Sayısal Olmayan	Kolay ve çabuk uygulanabilir	Risk sınıflamasında sınırlı sayıda farklı sınıf verebilir (örn. çok yüksek, yüksek, orta ve düşük)
	Finansal etki ve gerçekleşme olasılığı dışında daha geniş bir kapsamda bilgilendirme yapılabilir. Örn: Riske maruz kalma, kurum itibarı, çalışan güvenliği vb..	Çok kesin değildir. Aynı risk grubunda yer alan iki riskin esasen seviyeleri farklı olabilir.
	Bir çok kurum çalışanı tarafından sofistike sayısal teknik eğitimleri vermeden kolayca anlaşılır	Riskle ilişkili olayları sayısal olarak adresleyemez
		Maliyet-fayda analizlerine kısıtlı imkan tanır
Sayısal Olan	Sayısal kümeleme imkanı verir. Risk etkileşimlerini sayısal olarak ortaya koyar.	Özellikle modelin ilk geliştirilmeye başlandığı zamanlarda olmak üzere pahalı ve zamana ihtiyaç duyan yöntemlerdir.
	Riski giderme seçenekleri açısından fayda-maliyet analizine imkan tanır.	Para birimi veya oran cinsinden ölçü kullanılması gerektiği için bazı sayısal olmayan etkilerin gözden kaçmasına yol açabilir.
	Uç olaylarda ödem egücünü korumakl için gerekli sermaye hesaplarına olanak verir	Kullanılan varsayımlar belirgin olmayabilir.
		Sayılar verilerin içerdiğinden daha yüksek seviyede kesinlilk ortaya koyabilir.

Kaynak: Curtis, Carey, "**Risk Assesment in Practice**", s.8

Risk değerlendirme aşamasında bir riskin tek başına , izole edilmiş biçimde değerlendirilmesinden ziyade risk etkileşimlerinin de farkında olunması, bu etkileşimleri değerlendirilmesi gerekir. Tek başına gerçekleşme olasılığı ve yaratacağı olumsuzluk çerçevesinde "düşük risk" olarak değerlendirilebilecek bir durum başka bir riskle etkileşimi sonucu gerçekleşme olasılığı ve etkisi açısından "yüksek risk" grubuna girebilir. Bu nedenle riskler değerlendirilirken etkileşimleri her zaman göz önünde tutulmalıdır.

Risk envanterinde gruplanmış risklerin değerlendirilmesi sonucu önceliklendirilmesi ile oluşturulacak risk haritası, kurum yöneticilerine, öncelikli

olarak hangi riskleri gidermeye odaklanmaları gerektiği konusunun anlaşılmasında ve bu risklerin giderilmesi ile ilgili planlama süreçlerinde yardımcı olur.

Kurumun risk iştahının yönetim kurulu düzeyinde belirlenmesi ve kurum içi iletişiminin yapılmasının önemine değinilmişti. Risklerin giderilmesi aşaması risk iştahı belirlenmiş, kurum içi iletişimi yapılıyor olmak üzere; kurumun risk portföyünde yer verilen her bir risk için risk iştahına uygun olarak gerçekleşme olasılığı ve riskin kuruma etkisinin de değerlendirilmesi aşamasıdır. Böylece, tolerans aralıklarının belirlenmesi, değerlendirilen risklerle ilgili belirtilen tolerans aralıklarında sonuçlar almak için yapılması gerekenlerin belirlenmesi ve sürece yönelik gerekli kaynak planlamasının fayda-maliyet dengesini gözeterek yapılması, hazırlanan riskleri giderme planının değişimlere uygun olarak güncel tutulması amaçlanır.

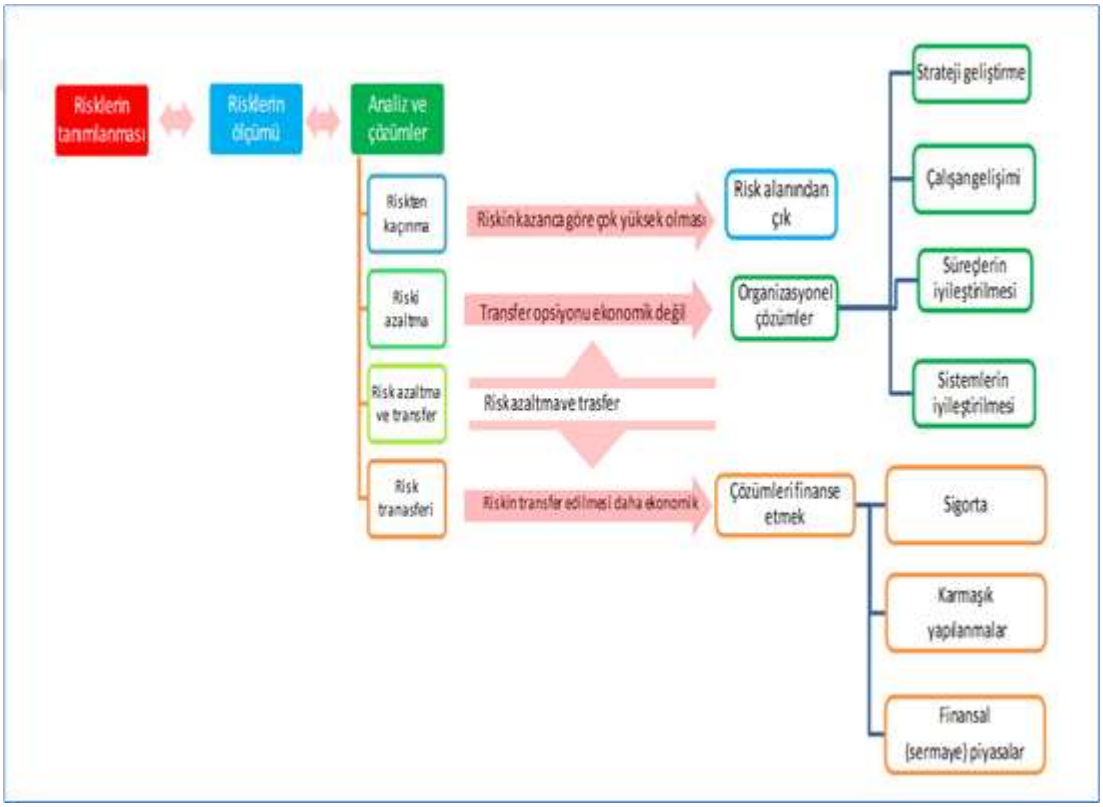
Risklerin giderilmesi adımının genel çerçevesini risklerin azaltılması çabaları oluşturur. COSO KRY sisteminde risk giderme konusu içine **riskten kaçınma**, bir başka deyişle riskli sürecin gerçekleşmemesi için çaba sarf etme ve riski kabul etmeme, **risklerin azaltılması**, bir başka deyişle kontrol yöntemleriyle risklerin azaltılması çalışmaları, **risklerin paylaşılması,** bir başka deyişle olası risklerin etkilerinin başkaları ile paylaşılmasına yönelik çalışmaları, **risklerin kabul edilmesi**, bir başka deyişle olası riskin etkisinin kabul edilerek riskin alınması ve bu riskin olası etkisine ilişkin planlamaların yapıldığı çalışmalar olmak üzere dört temel yöntem girmektedir.

Bu yöntemlerin aralarındaki ilişki ortaya koyulurken, örnek olarak tanımlanacak bir riskten yararlanılsın. Risk, müşterilere yapılan vadeli satışlardan doğan ticari alacakların vadesinde tahsil edilmeme durumu olsun. Bu durumda; riskten kaçınma, tahsilat riski yaşanacağı değerlendirilen müşteriye vadeli mal satışı yapılmayarak ticari alacak oluşmasının engellenmesidir. Risklerin azaltılması, müşteri için bir istihbarat yapılarak, derecelendirme yapılması ve buna göre oluşması muhtemel ticari alacağın belli oranı için teminat istenmesi olacaktır. Risklerin paylaşılması, karşılığında müşteriden teminat aldınan ticari alacağın bir finansal

kuruma sigorta ettirilmesi olacaktır. Risklerin kabul edilmesi, müşteriden, doğacak ticari alacağın belli oranı için muhasebe sisteminde şüpheli alacak karşılığı ayrılması, olası bir tahsilat yapamama riskinin kabul edilmesi olacaktır.

Risklerin giderilmesi süreci alt fonksiyonları ile birlikte bir bütün olarak Şekil 2.9'da gösterilmektedir.

Şekil 2.9: Risklerin Giderilmesi Süreci



Kaynak: TÜSİAD, **Kurumsal Risk Yönetimi,** İstanbul, TÜSİAD, Şubat 2008., s.60.

Risklerin giderilmesi ile ilgili eylemler planlanırken, yapılacak fayda-maliyet analizlerinin firmanın belirlenmiş risk iştahı ve risk toleransı ile birlikte değerlendirilmesi gerekir. Üst yönetim tarafından belirlenmiş, iletişimi yapılan ve değişimlere karşı sürekli güncel tutulan risk iştahı firma açısından alınabilecek riskler ve bunların giderilmesine yönelik genel çerçeveyi belirler.

Kurumun risk portföyündeki her bir risk için hazırlanması gereken risklerin giderilmesi planları genel hatları ile Tablo 2.5'te gösterilmektedir. Bu planlarda değerlendirme konusu risk için kurumun güncel risk iştahına uygun olarak belirlenmiş tolerans aralıkları, ve riskin beklenen etkisi itibariyle bu tolerans aralıklarında kalmak için planlanan davranışlar yer alır. Bu davranışın sergilenebilmesi için gerekli kaynak planlaması ve fayda/maliyet analizi de yapılır.

Tablo 2.5: Risklerin Giderilmesi Planı

Risk	Doğal Risk		Yöntem	Risk Giderme Alternatifleri	Artık Risk	
	Olasılık	Satışa Etkisi			Olasılık	Etki
Risk 1: Rakibin geliştirmekte olduğu yeni ürünlerle Pazar lideri olması	40%	$ 5mio negatif	Kabul Et	Özel bir eylem belirleme. Mevcut ürün portföyünü koru.	10%	her yıl karlarda yaklaşık %10 azalma
			Kaçın	Yeni ürünlerle ilgili AR-GE sürecini hızlandırmak için ek kaynaklar tahsis et.	30%	Geliştirme maliyetleri nedeni ile $25000 kar azalması
			Paylaş	Mevcut ürün portföyünün seçimi konusunda çeşitli müşterilere prim paketleri teklif et	20%	
			Azalt	Mevcut ürün portföyünde fiyatları düşürerek pazarın yeni ürünleri tercih etme konusundaki motivasyonunu düşür.	40%	
Risk2:	.....	.....	.....	.....	.....	.....

Risklerin Giderilmesi Planı Çalışma Kağıdı

Kaynak: Moeller, **COSO Enterprise Risk Management**, s.73.

Risk – kazanç ilişkisi dikkate alındığında, kurumların risk yönetim yetkinliklerinin bir rekabet avantajına dönüştüğü görülmektedir. Risk yönetim yetkinliğindeki gelişmişliğe bağlı olarak, risklerini yöneten kurumlar gerek risk iştahı seviyeleri, gerek risk-kazanç ilişkisi, gerekse risk giderme yöntemleri ile önemli rekabet avantajı yaratma alanı bulurlar.

Sıradaki aşama, her bir risk konusu için ne tür risk cevaplarının uyarlanacağı ve uygulanacağı belirlenmesidir. Performans bileşeninin alt prensibi olan risk cevaplarını uyarlamak ve uygulamak prensibi COSO KRY-2004 **kontrol faaliyetleri** bileşeni ile örtüşmektedir. Kontrol faaliyetleri ile kast edilenler, kurumda ekonomik faaliyetin gerçekleştirilmesinde kullanılan politikalar, planlar, prosedürler, iş akışları, yetkilendirmelerdir.

COSO İç Kontrol Sistemi Kontrol Faaliyetleri kapsamı bu konuda kurumlar için yüksek yetkinlikte bir çerçeve oluşturmaktadır. İlgili kapsam, kontrol faaliyetleri açısından işletme uygulamamızın temelini oluşturmaktadır.

Unutulmaması gereken konu, kurumda kontrol faaliyetlerinin neler olacağına ve nasıl uygulanacağına süreç sahipleri ve yöneticilerinin karar vermesi ve üst yönetimin konuya ilişkin onayının alınmasıdır. Kurum için içerden ya da dışardan iç denetim hizmeti veren iç denetçilerce kontrol yöntemlerinin etkinliğini ve değişimler karşısında oluşan yeni risk, süreç ve ihtiyaçlar karşısında ilizyona uğramadan güncel ve etkin sürdürülüp sürdürülemediğini ölçülecektir. İç denetim bizzat kontrol faaliyetlerini kurup işletmekle sorumlu görülmemelidir.

2.3.1.4. Gözden Geçirme ve Revizyon

COSO KRY-2017 çerçevesinin dördüncü bileşeni olan gözen geçirme ve revizyon, Şekil 2.10'da gösterilen üç alt prensip ile desteklenmektedir.

Şekil 2.10: COSO KRY-2017 Gözden Geçirme ve Revizyon Bileşeni

Prensipler:

15- Önemli değişiklikleri değerlendirir.

16- Risk ve performansı gözden geçirir.

17- Kurumsal risk yönetimindeki gelişmeleri izler.

Kaynak: COSO, **Enterprise Risk Management-Integrating with Strategy and Performance**, June 2017, (Çevrimiçi) http//www.coso.org, 05 Nisan 2019

COSO KRY-2017 çerçeveside, **gözden geçirme ve revizyon** bileşenini; kurum performansına bağlı olarak, organizasyonun, kurumsal risk yönetimi bileşenlerinin nasıl işlediğini, zamanla ve önemli değişiklikler karşısında ne tür yenilemeler yapılması gerektiği üzerinde çalışması olarak ifade edilmektedir.[12]

Üç ana prensibinin kapsamı ile, gözden geçirme ve revizyon bileşeni, COSO KRY-2004 çerçevesinin **izleme bileşeni** ile örtüşmekle birlikte, alt prensipleri ile, kurum performansının izlenmesi, kurumsal risk yönetimi bileşenlerinin etkinliğinin arttırılması için, içsel ve dışsal faktörlere bağlı olarak değişen performans, hedeflere ve stratejiyi dikkate alarak, gerekli değişikliklerin, yenilemelerin yapılması vurgulanmaktadır. Bu bileşenin kapsamı ve COSO İç Kontrol Sistemi açıklanırken değinilen "Kontrol ve İzleme" ile ilgili içerik işletme uygulamamızın temelini oluşturmaktadır.

2.3.1.5. Bilgi, İletişim ve Raporlama

COSO KRY-2017 çerçevesinin beşinci ve son bileşeni olan bilgi, iletişim ve raporlama; Şekil 2.11'de gösterilen üç alt prensip ile desteklenmektedir.

[12] A.e.

Şekil 2.11: COSO KRY-2017 Bilgi, İletişim ve Raporlama Bileşeni

Prensipler:

18- Bilgi ve teknolojinin katkısını kaldıraçlandırır.

19- Risk bilgisinin iletişimini yapar.

20- Risk, kültür ve performansı raporlar.

Kaynak: COSO, **Enterprise Risk Management-Integrating with Strategy and Performance**, June 2017, (Çevrimiçi) http//www.coso.org, 05 Nisan 2019

Bilgi, iletişim ve raporlama bileşeni, alt prensiplerinin kapsamı ile COSO KRY-2004 çerçevesinin bilgi ve iletişim bileşeni ile örtüşmekle birlikte, gelişen elektronik ölçme ve izleme araçlarının yeteneklerinden artan bir ivme ile yararlanmanın hedeflenmesi ve kurumun bu yeteneğini kaldıraçlandırmayı önceliklendirmesi bir prensip olarak düzenlenmektedir. Bu yeteneğini geliştiren kurumların performans ve rekabet avantajı konusunda olumlu ayrışacağı beklenmelidir.

Bu sürecin çerçevesinin **kurumlara özgü**, farklı genişlik ve değişik biçimlerde tanımlanabilir. İşletme uygulamamızda ele alınan KRY sistemi ile amaçlananın kurum stratejik ve operasyonel hedeflerinin gerçekleştirilmesini **makul ölçüde** güvence altına almaktır. "makul ölçü" her kurumun yönetim kurulunun bakış açısına göre değişik seviyelerde tanımlanabilir. Kurumun maruz kaldığı içsel ve dışsal **değişimler** karşısında kontrol faaliyetlerinin etkinliğini korumasını sağlamanın ve kurum içi ilizyonları azaltmanın yolunun bilgi, iletişim ve raporlama bileşeni kapamında yer alan fonksiyonları etkili çalıştırmaya bağlı olacaktır.

2.4. Kurumsal Risk Yönetimi Çerçevesinde İç Denetim

KRY sistemi ile amaçlananın kurumun stratejik ve operasyonel hedeflerinin gerçekleştirilmesini makul ölçüde **güvence altına almak** olduğundan hareket edildiğinde, KRY sisteminin uygulama etkinliği ve uygulama sonuçları itibariyle değerlendirilmesi gündeme gelmektedir. KRY sisteminin iç denetim ilişkisi "sistemin etkinliğinin değerlendirilmesi" noktasında başlamaktadır. Bu ilişkinin çerçevesi belirlenirken, iç denetim faaliyeti ile ilgili IIA tarafından geliştirilmiş "Uluslararası Mesleki Uygulama Çerçevesi (UMUÇ)" düzenlemeleri ve yine IIA tarafından ortaya koyulan "KRY'de İç Denetimin Rolü" konulu pozisyon raporundaki düzenlemeler mesleki otoriteler tarafından yüksek kabul görmüşlük seviyeleri nedeni ile bağlı kalınacak temel referanslar olacaktır.

2.4.1. İç Denetimin Kapsam ve Çerçevesi

İç denetim faaliyetinin kapsam ve çerçevesi ile ilgili IIA tarafından ortaya koyulan ve iki ana rehberden oluşan UMUÇ düzenlemelerine bağlı kalınacak olup, bu bölümde UMUÇ düzenlemeleri çeşitli yönleri ile ortaya koyulacaktır.

Söz konusu rehberlerden birisi **zorunlu rehber** olarak anılan, **iç denetimin tanımı, etik kuralları ve standartlarını** düzenleyen rehberdir. Bahsi geçen diğer rehber, pozisyon raporları, uygulama önerileri ve uygulama rehberlerinden oluşan, **kuvvetle tavsiye edilen rehberdir**. İç denetim faaliyetinin uygulamaları, kurumun bulunduğu coğrafya, yasal düzenlemeler, sosyokültürel farklılıklar ve kurum özelinde farklılıklar içerebilir. "*Zorunlu rehberde yer alan düzenlemelere uyum, iç denetim faaliyetinin etkili bir biçimde yerine getirilmesi için elzemdir.*" [13] Uyulması beklenen bu düzenlemelerle, kurumların büyüklük ve küçüklüklerine göre farklı gereklilikler ortaya koyulmaz. Daha çok iç denetim faaliyetinin etkili bir biçimde icra edilebilmesi için bağlı kalınması gereken ilkeler,

[13] IIA, **"Uluslararası Mesleki Uygulama Çerçevesi"**, çev., Türkiye İç Denetim Enstitüsü, (Çevrimiçi) http/www.tide.org.tr, 10 Temmuz 2015.

sergilenmesi gereken davranışlar, sağlanması gereken koşullar ortaya koyulur. İç Denetim faaliyeti ile esas itibariyle yönetim kuruluna yönelik süreçler hakkında güvence vermeye ve danışmanlık rolü ile de süreçleri geliştirmeye odaklanıldığı için UMUÇ düzenlemelerinin yasal bir yaptırım gücü yoktur, iç denetim faaliyetini etkili biçimde icra etmek isteyen kurumlara yönelik bir rehber nileliğindedir. Düzenlemelere uyma zorunluluğu bu çerçevede anlaşılmalıdır.

2.4.1.1. İç Denetim Tanımı

İç denetimin tanımı UMUÇ' nin "zorunlu rehber" olarak anılan ve etkili bir iç denetim faaliyeti için uyulması zorunlu kabul edilen düzenlemesinin parçası olup, aşağıdaki gibidir. [14]

> *"İç denetim, bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden bağımsız ve objektif bir güvence ve danışmanlık faaliyetidir. Kurumun risk yönetim, kontrol ve yönetişim süreçlerinin etkinliğini değerlendirmek ve geliştirmek amacına yönelik sistemli ve disiplinli bir yaklaşım getirerek kurumun amaçlarına ulaşmasında yardımcı olur."*

Tanım ile, iç denetimin **bağımsız** ve **objektif** bir **güvence** ve **danışmanlık faaliyeti** olduğunun altı çizilmekte, iç denetimin, kurumun risk yönetimi, kontrol ve yönetişim süreçlerinin etkinliğini değerlendirerek geliştirmeyi amaçladığı, bu amaca yönelik sistemli ve disiplinli bir yaklaşım getireceğini vurgulanmaktadır. İç denetim faaliyetinin **güvence** ile ilgili kısmı ile süreçlerin etkinliğinin **değerlendirilmesi**, bu değerlendirmenin sistematik ve disiplinli bir yaklaşım ile yapılması konuları kapsanırken, **danışmanlık** ile ilgili kısmı ile süreçlerin **geliştirilmesi** ve etkinliğinin arttırılması konuları kapsanmaktadır.

[14] A.e

2.4.1.2. İç Denetimde Etik Kurallar

UMUÇ' nin zorunlu rehberi altında düzenlenen bir diğer konu iç denetim etik kuralları olup, iç denetim ilkeleri ve iç denetçilerden beklenen davranış kuralları olmak üzere iki önemli konu kapsanmaktadır.

> *"Etik kuralları iç denetim hizmeti veren kişi ve kurumları bağlamaktadır. IIA üyeleri ve/veya IIA mesleki, sertifikalarına sahip olanlar için bu kuralların ihlali, IIA' nın yönetmelikleri ve idari yönergelerine göre değerlendirilir ve ele alınır."* [15]

İç denetim faaliyeti ile ilgili **dürüstlük**, **objektiflik, gizlilik** ve **yetkinlik** olmak üzere dört ilke belirlenmiştir. Her bir ilke ile ilgili iç denetçilerden beklenen davranış kuralları ayrı ayrı belirtilmektedir. Tablo 2.6 iç denetim faaliyeti ile ilgili ilkeleri ve iç denetçilerden beklenen davranış kurallarının ilişkisini ortaya koymaktadır.

[15] IIA, **Etik Kuralları**, (Çevrim içi) http/www.theiia.org., 10 Temmuz 2015.

Tablo 2.6: İç Denetim İlkeleri ve İç Denetçiler İçin Davranış Kuralları

İlkeler	Davranış Kuralları
1-Dürüstlük;	
İç denetçilerin dürüstlüğü, güven oluşturur ve böylece verdikleri hükümlere itimat edilmesine yönelik bir zemin hazırlar.	
	1.1. Çalışmalarını doğruluk, dikkat ve sorumluluk duygusu ile yaparlar
	1.2. Hukuku gözetir ve hukukun ve mesleğin gerektirdiği özel durum açıklamalarını yaparlar
	1.3. Kanun dışı bir faaliyete bilerek ve isteyerek taraf olmaz veya iç denetim mesleği ve kurum açısından yüz kızartıcı eylemlere girişmezler.
	1.4. Kurumun meşru ve etik amaçlarına saygı duyar, katkıda bulunurlar.
2- Objektiflik;	
İç denetçiler, inceledikleri süreç veya faaliyetle ilgili bilgiyi toplarken, değerlendirirken ve raporlarken en üst seviyede mesleki objektiflik sergiler. İç denetçiler ilgili tüm şartların değerlendirmesini dengeli bir şekilde yapar ve bir yargıya varırken kendilerinin veya diğerlerinin menfaatlerinden çok etkilenmez.	
	2.1. Değerlendirmelerinin tarafsızlığına zarar verebilecek veya zarar vereceği varsayılabilecek herhangi bir ilişkiye veya faaliyete katılmazlar; bu katılım kurumun çıkarlarıyla çatışan ilişki ve faaliyetleri de içerir.
	2.2. Mesleki muhakemelerini zayıflatabilecek veya zayıflatacağı varsayılabilecek herhangi bir şeyi kabul etmezler.
	2.3. Tespit ettikleri ve açıklanmadığı taktirde gözden geçirdikleri faaliyetlere ilişkin raporları bozacak tüm önemli bulguları açıklarlar.
3- Gizlilik;	
İç denetçiler, elde ettikleri bilginin sahipliğine ve değerine saygı gösterir; hukuki ve mesleki bir mecburiyet olmadığı sürece de gerekli yetkiyi almaksızın bilgiyi açıklamaz.	
	3.1. Görevleri sırasında elde ettikleri bilgilerin korunması ve kullanımı konusunda ihtiyatlı olurlar.
	3.2. Sahip oldukları bilgileri kişisel menfaatleri için veya hukuka aykırı olarak veya kurumun meşru ve etik amaçlarına zarar verecek tarzda kullanmazlar.
4- Yetkinlik (Ehil Olma);	
İç denetçiler, iç denetim hizmetlerinin gerçekleştirilmesinde gereken bilgi, beceri ve tecrübeyi ortaya koyar.	
	4.1. Sadece görevin gerektirdiği bilgi, beceri ve tecrübeye sahip oldukları işleri üstlenmelidirler.
	4.2. İç denetim hizmetlerini, Uluslararası İç Denetim Standartlarına uygun bir şekilde yerine getirirler.
	4.3. Kendi yeterliliklerini ve hizmetlerinin etkinlik ve kalitesini devamlı geliştirirler.

Kaynak: IIA, **Etik Kuralları**, (Çevrim içi) http/www.theiia.org., 10 Temmuz 2015.

İç denetim mesleğinin etik kültürünü geliştirmek için IIA tarafından düzenlenen etik kurallar, hem mesleki ilkeler hem de mesleki davranış kurallarını düzenleyerek iç denetçiler açısından çok önemli bir davranış zemini oluşturmaktadır.

2.4.1.3. İç Denetimin Standartları

UMUÇ' nin zorunlu rehberinde ortaya koyulan "Uluslararası İç Denetim Standartları (Standartlar)" ile iç denetim faaliyetinin etkili bir şekilde icra edilebilmesi için uyulması gereken standartları düzenlenmektedir. Standartlar, **nitelik standartları** ve **performans standartları** olmak üzere iki grupta toplanmıştır.

"Nitelik standartları iç denetim faaliyetini yürüten kişi ve kurumların özelliklerine yöneliktir. Performans standartları iç denetimin tabiatını açıklar ve bu hizmetlerin performansını değerlendirmekte kullanılan kalite kıstaslarını sağlar. Nitelik ve performans standartları tüm iç denetim hizmetlerine tatbik edilmek üzere hazırlanmıştır." [16]

Etkili bir iç denetim faaliyetinin icra edilebilmesi için Standartlar' ın tamamına uyulması zorunludur. **Güvence verme** ve **danışmanlık** olarak iki ana grupta toplanabilecek standartlar, çalışmanın ekinde (Ek1), düzenledikleri konular itibariyle gruplanarak özetlenmiş, standartlarla ilgili tam metnin web bağlantısı verilmiştir. Bu özet ile, standartların çerçevesi hakkında bir farkındalık yaratılması amaçlanmıştır. Standartlar hakkında tam olarak bilgi sahibi olmak ve içeriğinin tam olarak kavranabilmesi için Ek1'de verilen özetin tanımları ve yorumları ile birlikte incelenmesi ve değerlendirilmesi gerekmektedir.

2.4.2. Kurumsal Risk Yönetiminde İç Denetimin Rolü

KRY' nin, kurum hedeflerinin gerçekleştirilmesi ile ilgili makul bir güvence vermek üzere tasarlanan bir sistemdir. İç denetim de objektif ve bağımsız bir güvence ve danışmanlık faaliyetidir. KRY sisteminin etkinliğinin değerlendirilmesi ve süreçlerinin geliştirilmesi konularında iç denetimden faydalanılır.

"İç denetçiler önceleri çalışmalarını yanlızca kontrol faaliyetlerine yönelik gerçekleştirirken, günümüzde bunlara ilaveten risk evrelerini tanımlamakta, işletmelerin risk durumlarını sürekli gözlemlemekte, isk yönetimi süreçlerini desteklemekte, ve nasıl bir sistem kurulması gerektiği hakkında yönetim kurulu ve üst yönetimi bilgilendirerek işletmelerine yardımcı olmaktadırlar." [17]

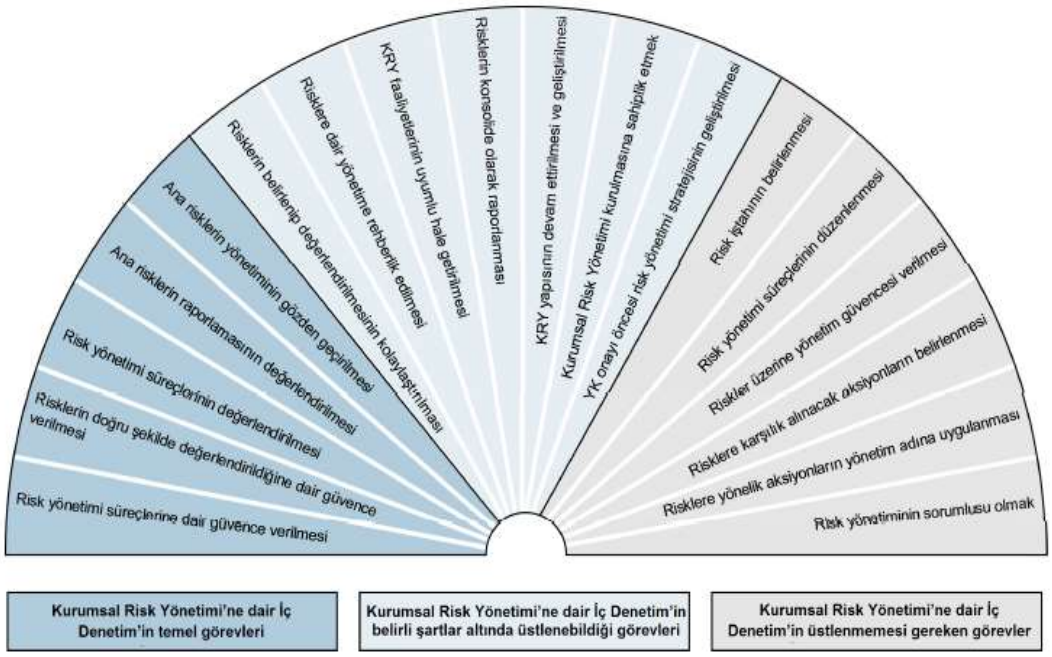
---

[16] IIA, **Uluslararası İç Denetim Standartları**, çev.,Türkiye İç Denetim Enstitüsü, Ekim 2012, (Çevrimiçi) http/www.tide.org.tr, 10 Temmuz 2015.

[17] Burcu Özgül, Banu Tarhan Mengi, **Kurumsal Sürdürülebilirlik ve Güvencesi "İç Denetim" BİST Sürdürülebilirlik Endeksi'ne Tabi Şirketlerde Anket Çalışması**, İstanbul, Beta Beta Basım Yayım Dağıtım A.Ş., 2016, s.52

UMUÇ' nde düzenlenen **2120 numaralı standartta,** iç denetim faaliyetinin, risk yönetimi süreçlerinin etkinliğini değerlendirmek ve iyileştirilmesine katkıda bulunmak zorunda olduğunu vurgulanmaktadir. **2130 numaralı standartta** da iç denetim faaliyetinin, kontrollerin etkinlik ve verimliliğini değerlendirmek ve sürekli gelişimi teşvik etmek sureti ile kurumun etkin kontrollere sahip olmasına yardımcı olmak zorunda olduğu belirtilmektedir. Bu çerçevede, iç denetim faaliyeti hem güvence sağlama rolü ile hem de danışmanlık rolü ile KRY sistemi ile ilişki içindedir.

Şekil 2.12: İç Denetimin KRY İçindeki Rolü



Kaynak: IIA, "İç Denetimin Kurumsal Risk Yönetiminde Oynadığı Rol", **IIA Pozisyon Raporu,** çev., Türkiye İç Denetim Enstitüsü, Ocak 2009, (Çevrimiçi) http/www.tide.org.tr, 25 Temmuz 2016

Şekil 2.12'ye göre iç denetimin KRY sistemi içindeki **güvence görevleri**; risk yönetimi süreçlerine dair güvence verilmesi, risklerin doğru şekilde değerlendirildiğine dair güvence verilmesi, risk yönetimi, süreçlerinin değerlendirilmesi, ana risklerin raporlamasının değerlendirilmesi, ana risklerin yönetiminin gözden geçirilmesi olarak sıralanmaktadır.

Güvence görevlerinden sonra **danışmanlık görevleri** şöyle sıralanmaktadır; risklerin belirlenip değerlendirilmesinin kolaylaştırılması, risklere dair yönetime rehberlik edilmesi, KRY faaliyetlerinin uyumlu hale getirilmesi, risklerin konsolide olarak raporlanması, KRY yapısının devam ettirilmesi ve geliştirilmesi, KRY kurulmasına sahiplik edilmesi, yönetim kurulu onayı öncesi risk yönetimi stratejilerinin geliştirilmesi.

İç denetim birimi, belirli koruma önlemleri ile objektiflik ve bağımsızlığını koruyabildiği sürece KRY sitemindeki görevlerini güvence görevlerinden danışmanlık görevlerine doğru genişletebilir. Bu **koruma önlemleri** şu biçimde ifade edilebilir: [18]

> *"Risk yönetimi sorumluluğunun kurum yönetiminde kaldığı açıkça belirtilmelidir. İç denetçinin sorumluluk ve görevleri iç denetim yönetmeliğinde açıkça ifade edilmeli ve denetim komitesi tarafından da onaylanmalıdır. İç denetim birimi herhangi bir riski kurum yönetimi adına yönetmemelidir. İç denetim birimi risk yönetimi kararları kendisi almak yerine, kurum yönetiminin karar alma sürecine tavsiye ve önerileriyle ve diğer yollarla destek olmalıdır. İç denetim birimi, KRY çerçevesinin kendi sorumluluğunda olan herhangi bir kısmı hakkında objektif güvence veremez. Bu güvence, uygun uzmanlığa sahip başka taraflarca verilmelidir. Güvence faaliyetlerinin ötesindeki iş ve görevler, bir danışmanlık görevi olarak algılanmalı ve bu göreve ilişkin uygulama standartlarına uyulmalıdır."*

KRY sistemi içinde iç denetimin üstlenmemesi gereken görevler ise şu biçimde ifade edilmektedir: kurumun risk iştahının belirlenmesi, risk yönetimi süreçlerinin düzenlenmesi, riskler üzerine yönetim güvencesi verilmesi, risklere karşılık alınacak aksiyonların belirlenmesi, risklere yönelik aksiyonların yönetim adına uygulanması ve risk yönetiminin sorumlusu olunması.

İç denetimin KRY sistemi içindeki asli rolü KRY süreçlerinin

[18] IIA, "İç Denetimin Kurumsal Risk Yönetiminde Oynadığı Rol", **IIA Pozisyon Raporu,** çev., Türkiye İç Denetim Enstitüsü, Ocak 2009, (Çevrimiçi) http/www.tide.org.tr, 25 Temmuz 2016.

etkinliği ile ilgili yönetim kurulu ve üst yönetime güvence sağlamaktır. Bu asli güvence görevlerinden danışmanlık görevlerine doğru genişlemenin mümkün olduğu, bunu yaparken bağımsızlık ve tarafsızlığın korunması gerekir. Çalışmada, iç denetimin KRY sistemi içindeki rolü, asli görevi olan "**güvence sağlama**" rolü olarak ele alınmıştır.Üçüncü bölümdeki işletme uygulamasında iç denetimin "güvence sağlama" rolü üzerinde durulacaktır.

2.4.3.Kurumsal Risk Yönetimi Sisteminin Değerlendirilmesi

KRY sisteminin etkinliğinin değerlendirilmesi sürecinde UMUÇ' nde belirtilen İç Denetim Tanımı, Etik Kuralları ve İç Denetim Standartlarına uyumlu bir iç denetim faaliyetinin Şekil 2.12'de belirtilen KRY' de "İç Denetimin Temel Görevleri" kapsamına uygun olarak çalıştırılması gerekmektedir. Bunun için öncelikle iç denetim yönetmeliği oluşturulmalı ve yönetim kurulunca onaylanmalıdır. Amaç, kapsam, hizmetlerin niteliği dikkate alınarak iç denetim ekibi organizasyonda konumlandırılmalı, iç denetim ekibi oluşturulmalı, görevlerin ifasına yönelik iç denetim faaliyet planları oluşturulmalı ve uygulanmalıdır. KRY sisteminin etkinliğinin değerlendirilmesinde, uygulanması gereken iç denetim süreçleri genel hatları şu biçimde ifade edilebilir; denetim faaliyetinin **planlanması**, denetimin **saha çalışması**, sonuçların **raporlanması**, alınması kararlaştırılan aksiyonların **takibi.**

2.4.3.1. İç Denetim Yönetmeliği ve İç Denetim Rehberi

İç denetim faaliyetinin amacının, kapsamının, yetki ve sorumluluğunun, alınacak hizmetin (güvence ve/veya danışmanlık) niteliğinin tanımlandığı, kurum içinde iç denetim faaliyetinin konumunu belirleyen resmi bir belgedir. UMUÇ' nde düzenlenen İç Denetim Tanımına, Etik Kurallara ve Uluslararası İç Denetim Standartlar' ına uyma zorunluluğu **İç Denetim Yönetmeliği'nde** belirtilmiştir.

İç Denetim Yönetmeliği ile, iç denetim yöneticisinin görev, yetki ve

sorumlulukları, kurumun üst yönetiminin ve denetlenenlerin denetim faaliyeti ile ilgili sorumlulukları, denetçilerin denetim faaliyeti çerçevesinde bilgi ve kayıtlara erişebilme yetkileri tanımlanır. Yönetmelikle, iç denetim faaliyetinin tarafsızlığı ve bağımsızlığı güvence altına alınır, tarafsızlığın sürdürülememesi durumunda yapılacaklar, iç denetim faaliyetinin kaynak ihtiyacı ve bunun nasıl karşılanacağı açıklanmıştır.

Yönetmelik iç denetim yöneticisi tarafından hazırlanır ve yönetim kurlu tarafından onaylanır. Yönetmelik en az yılda bir kez gözden geçirilip değişen kurum ihtiyaçlarını karşılayacak biçimde güncellenir.

UMUÇ' nde yer verilen Standartlar açısından , İç Denetim Yönetmeliği ile ilgili konular **1000, 1000.A1, 1000.C1, 1010 numaralı standartlarla** düzenlenmektedir.

İç Denetim Yönetmeliği, iç denetim ekibi kadar kurumun bütün birimlerini bağlayıcı özelliği vardır. Başka bir birimin kendi fonksiyonu ile ilgili iç yönetmeliği İç Denetim Yönetmeliği ile çelişkiler ve çatışmalar içeremez. Yönetim Kurulunca çıkarılan yönetmelik ve prosedürlerde İç Denetim Yönetmeliği ile çatışan alanlar olmamasına özellikle dikkat edilir.

UMUÇ' nin Standartlar bölümünde yer verilen **2040 numaralı standart ile,** iç denetim yöneticisinin, iç denetim faaliyetini yönlendirmek amacı ile iç denetim faaliyetinin politika ve prosedürlerini belirlemek zorunda olduğu belirtilmektedir. İç denetim süreci ile ilgili esas alınacak politika ve uygulanacak prosedürler detaylı bir şekilde hazırlanmalı ve iletişimi yapılmak üzere dökümante edilmelidir. Söz konusu politika ve prosedürlerin detaylandırılarak iç denetim faaliyetlerinin hangi esaslara göre yürütüleceği ve sürecin detaylarının ne olacağı konusunda iç denetim ekibi ve kuruma ışık tutan **İç Denetim Rehberi** hazırlanır.

İç Denetim Yönetmeliğince, iç denetim faaliyetinin amacı, kapsamı, yetki ve sorumluluğu, alınacak hizmetin (güvence ve/veya danışmanlık) niteliği

tanımlanır, kurum içinde iç denetim faaliyetinin konumu belirlenir. İç denetim faaliyetinin iş süreçlerinin nasıl gerçekleştirileceği, denetim planlarının nasıl yapılacağı, denetim ön çalışmalarının detayları, denetimin sahada nasıl sürdürüleceğinin detayları, bulguların değerlendirilmesi ve raporlama ile ilgili detaylar, denetim bulgularına göre planlanan aksiyonlarla ilgili takip denetimlerinin nasıl yapılacağı, sonuçların nasıl izleneceği iç denetim ile ilgili hazırlanan rehberlerde ve/veya hazırlanan İç Denetim Rehberinde yer alır. İç Denetim Rehberinde ayrıca, iç denetim ekibinin nasıl kurulacağı, nasıl işe alınacağı, adaylarda aranacak koşular, işe alma takvimi, eğitim planı ve takvimi gibi detaylar belirtilir.

2.4.3.2. İç Denetim Ekibinin Oluşturulması ve Yapılandırılması

İç denetim ekibinin oluşturulması ve yapılandırılmasında UMUÇ' nde yer verilmiş olan, "kurum içi bağımsızlık" konusunu düzenleyen **1110 numaralı standart**, "yönetim kurulu ile etkileşim" konusunu düzenleyen **1111 numaralı standart**, "bağımsızlık ve objektifliğin bozulması" konusunu düzenleyen **1130 numaralı standart**, "yeterlilik" konusunu düzenleyen **1210 numaralı standart**, "kaynak yönetimi" konusunu düzenleyen **2030 numaralı standartlar** belirleyici olmaktadır.

İç denetim yöneticisi kurum içi bağımsızlığını güvence altına alacak bir yönetim kademesine bağlı olmalıdır. İç denetim yöneticisi yönetim kurulu ile doğrudan iletişim ve etkileşimde olmalıdır. İşlevsel olarak yönetim kuruluna rapor etmesi kurum içi bağımsızlığını sağlar. Denetçilerin bağımsızlığının bozulduğu veya bozulduğu kanaatinin oluştuğu durumlarda ayrıntılar ilgili taraflara açıklanmalıdır. Kişisel çıkar çatışmaları, kapsam ve kaynak sınırlamaları, verilere ve kayıtlara ulaşmada sınırlamalar vb. durumlar bağımsızlığın bozulmasına örnek olarak verilebilir. Öte yandan, iç denetçilerin son bir yıldır yönetiminden sorunlu oldukları işleri ve/veya süreçlerin denetiminde görevlendirilmemesi gerekmektedir.

UMUÇ' nde düzenlenen **1210 numaralı standartta**, iç denetçilerin, sorumluluklarını yerine getirebilecek bilgi ve yeterliliğe sahip olmaları veya bunları edinmelerinin zorunlu olduğu belirtilmektedir. Ayrıca iç denetim ekibi suiistimal risklerini ve kilit bilgi teknolojisi risklerini değerlendirebilecek bilgiye sahip olmak zorundadır. İç denetim ekibi oluşturulurken ekibe dahil edilen denetçilerin bilgi ve becerileri ile mesleki yeterlilikleri bu standardı karşılamaya uygun olmalıdır veya iç denetim ekibinin bu yetkinliğe sahip olması sağlanmalıdır.

UMUÇ' nde düzenlenen **2030 numaralı standartta**, iç denetim yöneticisinin, iç denetim kaynaklarının uygun ve yeterli olmasını sağlaması gerektiği belirtilmektedir. İç denetim ekibinin büyüklüğü (kaç kişilik bir ekip olacağı) hiyerarşisi, (kaç kıdemli denetçi, kaç denetçi, kaç denetim asistanından oluşacağı), donanımları (sorumluluklarını yerine getirirken kullandıkları bilgisayarlar, yazılımlar, teknolojileri, haberleşme alt yapıları, seyahat standartları, ofislerinin çoklu lokasyonlarda mı olacağı, tek bir ofis mi olacağı, başkanlık düzeyinde mi organize olacakları, müdürlük düzeyinde mi organize olacakları, kullandıkları araçları, mobilyaları vb.) iç denetim kapsamına, denetime konu kurumun organizasyonunun büyüklüğüne ve yapısına, faaliyetlerin ve süreçlerin yapısına bağlı olarak değişecektir.

2.4.3.3. İç Denetim Süreçleri

Konumuz, iç denetim süreçlerini teknik detayları ile tanıtılmasından ziyade, KRY çerçevesinin etkinliğini bağımsız ve tarafsız bir biçimde güvence altına almayı hedefleyen bir iç denetim faaliyetinin güncellenmiş KRY sistemi içindeki rolünün tanıtılmasıdır. İç denetim süreçlerinin incelenmesinde, süreçler teknik uygulama detayları ile değil, ana esasları ile ele alınacak, KRY çerçevesi bulunan bir kurumda özellikle güncellenmiş COSO İç Kontrol Sistemi sonrasında iç denetim faaliyetinin değişmesi gereken geleneksel çehresi, COSO İç Kontrol Sistemi ile genel çerçevesi oluşturulan değerlendirme kriterleri ve kurumda yürütülen iç denetim faaliyetinin bu ihtiyaçlara uygun ele alınması üzerinde durulmaktadır.

Bir iç denetim faaliyetinden bahsedildiğinde çok genel hatları ile Şekil 2.13' de gösterilen süreçten bahsedilmektedir.

Şekil 2.13: İç Denetim Faaliyeti Süreci

UMUÇ, iç denetim süreci açısından uyulması zorunlu standartları düzenlemektedir. Süreci yakından incelerken, söz konusu standartlara ve düzenlemelere yer verilecektir. Öte yandan COSO İç Kontrol Sistemi ve COSO KRY sisteminin ortaya koyulması ile iç denetim faaliyetinin çehresini, iç denetim sürecinin geleneksel yapısını ve ele alınış biçimini değiştiren bakış açıları ortaya koyulmuştur.

COSO KRY Sistemi bileşenleri bir biri ile entegre çalışmak üzere tasarlanmış olup kurum özelinde, kurumun stratejik, operasyonel, raporlama ve uyum ile ilgili hedeflerinin gerçekleştirilmesini makul ölçüde güvence altına almayı hedeflemektedir. Kurumsal hedefler, sistemin bileşenlerinin bu hedeflerle ilişkileri, riskler, kurumun risk iştahı, risk toleransı, organizasyonun maruz kaldığı değişimler vb. nedenlerle söz konusu yapılar kuruma özeldir. Etkili bir KRY sisteminin

çalıştırılabilmesi için bileşenlerinin tamamının entegre ve uyum içinde çalışması gerekmektedir. Bir bileşenin yeteri kadar etkili çalışmamasını başka bir bileşenin gerekenden daha etkili çalışması tolere edemez. Bu yapının etkinliğini değerlendirmeyi hedefleyen bir iç denetim faaliyetinin süreçleri yürütülürken, iç denetim yöneticisinin kurum stratejilerini, operasyonunu, raporlama ve uyum ihtiyaçlarını, hedeflerini, bileşenlerin söz konusu hedeflerle ilişkisini kurum özelinde anlaması gerekmektedir.

> *"Denetim çalışmasında, işletmenin yapısına, faaliyuetine uygun olarak seçilen iç denetim yaklaşımından sonra, denbetçi,denetimi gerçekleştirebilmek için yeterli ve uygun denetim kaynaklarını temin eder"* [19]

COSO İç Kontrol Sisteminin kuramsal tasarımı ile bu modelin etkinliğini değerlendirecek iç denetçi açısından iç denetim faaliyetinin çehresi, kontrol faaliyetlerinin varlığını ve yokluğunu belirlemeye çalışan tabloların hazırlanmasından, sistemi oluşturan bileşenlerin, bunlarla ilişkilendirilmiş prensiplerin etkili çalışıp çalışmadığını değerlendirmeye kaymıştır. Mayıs 2013 tarihinde güncellenen COSO İç Kontrol Sistemi ile her bir bileşenle ilişkilendirilmiş prensipler ve söz konusu prensiplerin değerlendirilmesinde bakılması gereken "odak noktaları" ortaya koyulmuş, COSO İç Kontrol Sistemi ve KRY sisteminin değerlendirilmesinde nelere bakılması gerektiği ile ilgili bir çerçeve oluşturulmuştur. Bu genel çerçeve Tablo 2.7'de gösterilmektedir. Tablo 2.7, Mayıs 2013 tarihinde güncellenen COSO İç Kontrol Sistemi dökümanından derlenerek hazırlanmıştır. Ancak, bileşenlerin dinamikleri, prensiplerle ilişkileri, riskler ve odak noktaları kuruma hastır. İç denetçi, söz konusu çerçeveden hareketle, maliyet-fayda dengesini gözetir biçimde, kurum hedeflerini, organizasyonu, süreçlerin ve fonksiyonların hedeflere katkılarını, öncelikleri, kurumun risk iştahı ve risk toleransına bağlı risk değerlendirmesini anlamış olarak, kuruma özel bir değerlendirme yapmak durumundadır. Denetim sürecinin safhaları işletilirken, bu anlayışla hareket edilmeli,

[19] Burcu Adiloğlu, "İç Denetim Süreci ve Temel İşletme Faaliyetlerinin Konrol Prosedürleri ile Değerlendirilmesi: Bir Uygulama" **Doktora Tezi**, İstanbul, 2010, s.81

UMUÇ' nde düzenlenen standartlara uyum konusunda kurumda var olan KRY sistemi göz önünde tutulmalıdır.

Tablo 2.7: COSO İç Kontrol Bileşenler Prensipler ve Odak Noktaları Tablosu

Bileşen : KONTROL ORTAMI	
Prensip: 1	Organizasyon dürüstlük ve etik değerlere bağlılık göstermelidir.
Odak Noktalar	*a- Üst seviyede tutum belirler.* *b- İdari standartları belirler.* *c- İdari standartlara bağlılığı ölçer.* *d- Sapmaları belli zaman aralıkları ile ortaya koyar.*
Prensip: 2	Yönetim kurulu şirket yönetiminden bağımsız olup iç kontrol performans ve gelişimi ile ilgili aktif tavır sergileyerek sürece nezaret etmesi gerekir.
Odak Noktalar	*a- Nezaret etme konusunda sorumlulukları belirler.* *b- İlgili uzmanlıklara baş vurur.* *c- Bağımsız hareket eder.* *d- İç kontrol sistemine nezaret eder.*
Prensip: 3	Kurum yönetiminin yönetim kurulu nezaretinde, hedefleri gerçekleştirmeye yönelik, sorumluluk ve yetki alanlarının belirlemesi, raporlama kanallarını oluşturması ve gerekli yapılanmayı gerçekleştirmesi gerekir.
Odak Noktalar	*a- Kurumun tüm yapılarını dikkate alır.* *b- Raporlama kanallarını belirler.* *c- Yetki ve sorumlulukları tanımlar, atamaları yapar ve sınırlandırmaları yapar.*
Prensip: 4	Organizasyonun kurum hedeflerine uygun mesleki yeterliliğe sahip bireyleri cezbetme, geliştirme ve kurumda tutabilme konularında çaba ve bağlılık göstermesi gerekir.
Odak Noktalar	*a- Politikaları ve uygulama esaslarını belirler.* *b- Yeterlilikleri değerlendirir ve eksiklikleri adresler.* *c-Bireyleri cezbeder, geliştirir ve kurmda kalmalarını sağlar.* *d- Pozisyon yedeklemelerini ve silsileyi planlar ve hazırlar.*
Prensip: 5	Organizasyonun kurum hedeflerine uygun biçimde çalışanlarını iç kontrolle ilgili sorumlulukları açısından hesap verilebilir kılması gerekir.
Odak Noktalar	*a- Yapıları, yetki ve sorumluluk alanlarını hesap verilebilir kılar.* *b- Performans ölçüleri, teşvik ve ödül programları belirler.* *c- Mevcut performans, teşvik, ödül programlarını değerlendirir.* *d- Aşırı baskıyı dikkate alır, yönetir.* *e- Performans ve ödüllendirme değerlendirmelerini yapar.*
Bileşen: RİSK DEĞERLENDİRMESİ	
Prensip: 6	Organizasyonun hedeflerinin, bu hedeflerle ilgili risklerin belirlenmesi ve değerlendirilmesini mümkün kılacak açıklıkta belirlemesi gerekir.
Odak Noktalar	Operasyonel hedefler; *a- Yönetimin tercihlerini yansıtır.* *b- Risk toleransını dikkate alır.* *c- Operasyonel ve finansal performans hedefleri içerir.* *d- Kaynak tahsisi için baz teşkil eder.* Dış finansal raporlama hedefleri; *a- Geçerli muhasebe standartları ile uyum içindedir.* *b- Maddi önemlilik kriterini dikkate alır.* *c- Kurum aktivitelerini yansıtır.* Finansal olmayan dış raporlama hedefleri; *a- Belirlenmiş dışsal standart ve ilgili çerçevelerle uyum içindedir.* *b- Gerekli doğruluk ve tamlık seviyesini dikkate alır.* *c- Kurum aktivitelerini yansıtır.* İçsel raporlama hedefleri; *a- Yönetimin tercihlerini yansıtır.* *b- Gerekli doğruluk ve tamlık seviyesini dikkate alır.* *c- Kurum aktivitelerini yansıtır.* Mevzuata uyum hedefleri; *a- Yasalar ve düzenlemeleri yansıtır.* *b- Risk toleransını dikkate alır.*

Tablo 2.7: COSO İç Kontrol Bileşenler Prensipler ve Odak Noktaları Tablosu (Devamı)

Prensip: 7	Organizasyonun, kurumun her noktasında hedeflerin gerçekleştirilmesi ile ilgili riskleri belirleyip, bunların yönetilmesine yönelik değerlendirmeleri ve analizleri yapması gerekir.
Odak Noktalar	*a- Kurum, iştirakleri, bölümleri, iş birimlerini ve tüm fonksiyon seviyelerini içerir.* *b- İç ve dış faktörleri analiz eder.* *c- Yönetimin uygun kademelerinin katılımı vardır.* *d- Tanımlı risklerin önemlilik derecesini tayin eder.* *e- Risklere nasıl cevap verileceğini belirler.*
Prensip: 8	Organizasyonun, hedeflerin başarılması ile ilgili riskleri değerlendirirken yolsuzluk ve usulsüzlük potansiyellerini dikkate alması gerekir.
Odak Noktalar	*a- Usulsüzlüğün çeşitli biçimlerini dikkate alır.* *b- Teşvikleri ve baskıları değerlendirir.* *c- Fırsatları değerlendirir.* *d- Tavırları ve usulsüzlüğü akla yatkın hale getirme hallerini değerlendirir.*
Prensip: 9	Organizasyonun, iç kontrol sistemini belirgin biçimde etkileyecek değişimleri tanımlaması ve değerlendirmesi gerekir.
Odak Noktalar	*a- Dış çevredeki değişimleri değerlendirir.* *b- İş modelindeki değişiklikleri değerlendirir.* *c- Liderlikteki değişimleri değerlendirir.*
Bileşen: KONTROL FAALİYETLERİ	
Prensip:10	Organizasyonun, hedeflere ulaşılmasına ilişkin risklerin kabul edilebilir seviyelere indirilmesine katkı sağlayacak kontrol faaliyetlerini belirlemesi ve geliştirmesi gerekir.
Odak Noktalar	*a- Risk değerlendirme süreci ile entegredir.* *b- Kuruma özgü faktörleri dikkate alır.* *c- İlgili iş proseslerini belirler.* *d- Kontrol faaliyetleri türlerinin karışımını değerlendirir.* *e- Hangi seviyede kontrol faaliyetlerine baş vurulacağını dikkate alır.* *f- Görevler ayrılığı prensibinin uygulanmasını sağlar.*
Prensip:11	Organizasyonun, hedeflerin gerçekleştirilmesine yönelik genel kontrol faaliyetlerini teknoloji odaklı seçip geliştirmesi gerekir.
Odak Noktalar	*a- İş süreçlerinde teknoloji kullanımı ve teknoloji tabanlı kontroller arasındaki bağımlılığı belirler.* *b- İlgili teknolojik kontrol faaliyetleri alt yapısını kurar.* *c- İlgili güvenlik yönetim prosesi kontrol faaliyetlerini kurar.* *d- İlgili teknolojik satın alma, geliştirme ve bakım prosesleri kontrol faaliyetlerini kurar.*
Prensip:12	Organizasyonun, kontrol aktivitelerini kurum politika ve prosedürlerine dayandırarak işletmesi gerekir.
Odak Noktalar	*a- Yönetim direktiflerinin yayılmasını destekleyen politika ve prosedürler belirler.* *b- Politika ve prosedürlerin uygulanması için sorumluluk ve hesap verilebilirlik mekanizmaları oluşturur.* *c- Zamanlı bir biçimde performans sergiler.* *d- Düzeltmelerle ilgili eyleme geçer.* *e- Uygun yeterlilikte personel kullanılmasını sağlar.* *f- Politika ve prosedürleri tekrar değerlendirir.*
Bileşen: BİLGİ VE İLETİŞİM	
Prensip:13	Organizasyonun, iç kontrol fonksiyonunu destekleyecek uygunlukta ve kalitede bilgi toplaması ve kullanması gerekir.
Odak Noktalar	*a- Bilgi ihtiyaçlarını belirler.* *b- İç ve dış veri kaynaklarını elde tutar.* *c- İlgili veriyi bilgiye dönüştürür.* *d- Proseslerdeki kaliteyi korur.* *e- Fayda-maliyet ilişkisini dikkate alır.*

Tablo 2.7: COSO İç Kontrol Bileşenler Prensipler ve Odak Noktaları Tablosu (Devamı)

Prensip:14	Organizasyonun, amaç ve sorumluluklar dahil olmak üzere, iç kontrol fonksiyonunu destekleyen bilgilerin kurum içi iletişimini yapması gerekir.
Odak Noktalar	*a- İç kontrol bilgilerinin iletişimini yapar.* *b- Yönetim Kurulu ile iletişim sağlar.* *c- Birbirinden ayrılmış (çakışmayan) iletişim kanalları sağlar.* *d- İletişim için gerekli ve ilgili metodları seçer.*
Prensip:15	Organizasyonun, iç kontrol fonksiyonunu etkileyen konularda kurum dışı ile de iletişim halinde olması gerekir.
Odak Noktalar	*a- Üçüncü kişi ve taraflarla iletişimi sağlar.* *b- Kurum içine yönelik iletişime olanak tanır (müşterilerden, tedarikçilerden, dış denetçilerden vb.).* *c- Yönetim Kurulu ile iletişim sağlar.* *d- Birbirinden ayrılmış (çakışmayan) iletişim kanalları sağlar.* *e- İletişim için gerekli ve ilgili metodları seçer.*
Bileşen: İZLEME	
Prensip:16	Organizasyonun, iç kontrol bileşenlerinin güncel ve fonksiyon gösteriyor olduğunu doğrulayacak değerlendirmeleri oluşturma, geliştirme ve uygulaması gerekir.
Odak Noktalar	*a- Uygulamada olan ve ayrışık olan bir dizi değerlendirmeyi dikkate alır.* *b- Değişim derecesini dikkate alır.* *c- Konu hakkında baz anlayış oluşturur.* *d- Bilgili personel kullanır.* *e- İş süreçleri ile entegre olur.* *f- Değerlendirme kapsam ve sıklığında gerekli gördüğü düzeltmeleri yapar.* *g- Tarafsız olarak değerlendirir.*
Prensip:17	Organizasyonun, iç kontrol sapmaları ve farklarını belli zaman aralıklarında değerleme bu sapmaların, sorumlularla, yönetimle ve yönetim kurulu üyeleri ile iletişimini yapması gerekir.
Odak Noktalar	*a- Sonuçları değerlendirir.* *b- Sapmaların iletişimini yapar.* *c- Düzeltme eylemlerini izler.*

Kaynak: COSO, **Framework and Appendices: Internal Control-Integrated Framework,** May 2013, (Çevrimiçi) http//www.coso.org, 19 Şubat 2016.

COSO İç Kontrol Sisteminin etkili bir şekilde fonksiyon gösterebilmesi için her bir bileşenin etkili bir şekilde fonksiyon gösterdiğinin ve entegre olarak çalıştığının değerlendirilmesi gerekir. Herhangi bir bileşenin etkili biçimde fonksiyon gösterdiğinin değerlendirilebilmesi için de söz konusu bileşenle ilişkili olarak gösterilmiş her bir prensibin etkili biçimde fonksiyon gösterdiği değerlendirilmelidir.

Herhangi bir prensibin etkili bir şekilde fonksiyon gösterip göstermediğini değerlendirebilmek için altında sıralanmış ilgili odak noktalarına bakıp, odak noktalarında belirtilen kriterlerinin değerlendirilmesi gerekir. Bir prensibin etkili bir şekilde fonksiyon gösterdiğine kanaat getirebilmek için ilgili tüm

odak noktalarının aynı düzeyde etkili olduklarının değerlendirilmesi gerekmez. Önemli olan, iç denetçi tarafından, odak noktalarının bütünü itibariyle ilgili prensibin etkili bir biçimde fonksiyon gösterdiğinin değerlendirilmesidir. Örneğin; denetçi tarafından, "Kontrol Ortamı" bileşenin etkili bir biçimde fonksiyon gösterdiğinin değerlendirilebilmesi için, bu bileşenle ilgili Tablo 2.7' de belirtilmiş beş prensibin de ayrı ayrı etkili bir şekilde çalıştığı değerlendirilmelidir.

Birinci prensibi ele alırsak; "organizasyonun dürüstlük ve etil değerlere bağlılık gösterip göstermediği" denetçi tarafından değerlendirilmelidir. Bunun yapılabilmesi için, bu prensiple ilgili belirtilen dört odak noktasının kurum içinde varlığı değerlendirilmelidir. Denetçi tarafından sırası ile, organizasyonun dürüstlük ve etik değerlere bağlılıkla ilgili üst seviyede tutum belirleyip belirlemediğine, bu konuda idari standartların olup olmadığına, idari standartlar varsa, bunlara bağlılığın ölçülüp ölçülmediğine, bunlar ölçülüyorsa, sapmaların belli zaman aralıkları ile ortaya koyulup koyulmadığına bakarak birinci prensibin etkili bir biçimde çalışıp çalışmadığı ile ilgili kanaat oluştutulur. Bu değerlendirmeler için toplanması gereken veri, yapılması gereken testler, bulgulardan hareketle değerlendirmelerin içeriği kurumlara özgüdür. Denetim süreçleri iç denetim yöneticisi tarafından işletilirken, kurumun risk bazlı iç denetim planlarından başlayarak sürecin bütünü için COSO İç Kontrol Sisteminde ortaya koyulan genel değerlendirme çerçevesi dikkate alınır ve bu kuruma uyarlanarak kuruma özgü iç denetim süreci işletilmelidir.

2.4.3.4. İç Denetimin Planlanması

UMUÇ'nde belirtilen ilgili standartlarda da düzenlendiği hali ile , iç denetim yöneticisi, **kurumun hedeflerine** uygun olarak, iç denetim faaliyetinin **önceliklerini** belirleyerek **risk esaslı** bir planlama yapmak zorundadır. İç denetim planında kurumun hedefleri dikkate alınmalı, riskler esas alınmalı, denetim faaliyetleri önceliklendirilmelidir. İç denetim yöneticisi tarafından söz konusu faaliyetler planlanırken, iş tekrarlarını en aza indirmek için kurumun diğer güvence

ve danışmanlık sağlayan birimleri ile eş güdüm içinde olunması ve uyumlu çalışılması gerekir.

Şekil 2.14: İç Denetim Yıllık Planının Hazırlanma Süreci

Kaynak: Özbek, **İç Denetim,** s. 813

İç denetim planını risk esaslı olmak zorundadır. En az yılda bir kez yazılı bir risk değerlendirmesine dayandırılması gerekir. Yönetim kurulu ve üst yönetim de bu sürece dahil edilmelidir. iç denetim planını hazırlanırken, kurumda var olan risk yönetim çerçevesinin dikkate alınması, bir risk yönetim çerçevesi yoksa da, iç denetim yöneticisinin kendi risk değerlendirmesinin kullanılması gerekir. Bu çalışmada, iç denetim faaliyeti, mevcut bir KRY çerçevesine güvence sağlama rolü ile ele alınmaktadır. İç denetim planlaması için gerekli risk değerlendirme sürecinde COSO KRY çerçevesi dikkate alınmıştır.

> *"Geçmişte, iç denetim yıllık planlarını desteklemek için risk evreninin tanımlanması ve değerlendirmesi iç denetim faaliyetinin olağan rollerindendi. Bu rolde iç denetçiler tipik olarak risk değerlendirme sürecinin bütün aşamalarını kendileri gerçekleştirirdi. Bu durum kıymetli ve risk esaslı iç denetim planı için gerekli olsa bile, çoğu halde kurum yönetimi, bu durumu kurumun risk değerlendirmesi ile ters düşen, iç denetimin risk değerlendirmesi olarak algılardı. Bazı yönetim kurulu üyeleri bu değerlendirmeleri kıymetli bulsa da, ne iç denetimin tanımladığı risk evreni ne de buna yönelik değerlendirmeleri kurum tarafından benimsenmez ve bunun sonucu olarak KRY çerçevesinin bir parçası olamazdı…KRY kurumun bütününün içinde olması gereken bir faaliyettir ve risk değerlendirmesi ile birlikte KRY sisteminin tüm bileşenleri kurum yönetimi tarafında sahiplenilmelidir. Bu yüzden, bağımsızlık ve tarafsızlığı zedelemeyecek biçimde gerekli koruyucu tedbirlerin alınması*

koşulu ile iç denetim KRY sisteminin içeriğinin dökümante edilmesinde ve kurumla iletişimde, risk evreninin tanımlanmasının ve geliştirilmesinin kolaylaştırılmasında, risk analizlerinin teknik alt yapı ve disiplin açısından desteklenmesinde, risk değerlendirmelerin kolaylaştırılmasında rol alabilirler. İç denetimin bağımsızlık ve tarafsızlığını zedeleyecek bir rol almaması çok önemlidir. İç denetimi için bahsedilen bu roller tavsiye verme ve kolaylaştırmadan öteye geçmemelidir…Sonuç olarak, kurumun risk değerlendirmesi iç denetim açısından risk esaslı yıllık iç denetim planlarının gerekliliklerine uygun hale getirilebilir (örneğin değerlendirme doğal riski esas almak yerine artık riski esas alıyorsa). Değişimler sadece iç denetim lehine olacağından ve KRY sisteminin parçası olan kurumun risk değerlendirmesi değişmeyeceğinden bu durum iç denetimin tarafsızlık ve bağımsızlığını azaltmayacaktır." [20]

İç denetim yöneticisi tarafından, kurumda var olan KRY çerçevesinde yer alan risk değerlendirme yaklaşımını bütünüyle benimsenebileceği gibi, bu yaklaşımın gerekli görülen yönleri, risk esaslı yıllık iç denetim faaliyeti planlamasını destekleyecek biçimde iç denetim faaliyeti açısından değiştirebilir. Bu durum kurumda var olan KRY sisteminin risk değerlendirme sürecini etkilemek durumunda değildir. Burada kritik konu risk evreninin belirlenmesi, risk grupları, değerlendirme kriterleri, risk değerlendirme süreçleri açısından iç denetim yöneticisinin kurumun üst yönetim, ve yönetimi ile koordinasyon içinde olması, KRY sistemi ile ilgili iç denetimin süreçlere dahil edilmesinde iç denetimin tarafsızlık ve bağımsızlığının kesin biçimde korunmasıdır.

Denetim evreninin belirlenmesi esas itibariyle denetimi yapılacak süreçlerin ve alanların belirlenmesidir. Denetim evreni ile, söz konusu süreç ve alanların bütünü ifade edilmektedir. Çalışmada ele alınanın, iç denetim faaliyetinin KRY sistemi içindeki esas rolünün KRY sürecinin etkinliği konusunda makul bir güvence sağlamak olduğundan hareketle, çalışma kapsamında, iç denetim yıllık planlarında belirlenecek denetim evreninin, bir başka deyişle denetimi yapılacak

[20] Paul J. Sobel, Kurt F. Reding, **Enterprise Risk Management: Achieving and Sustaining Success**, Florida, The Institute of Internal Auditors Research Foundation, 2012, s. 108-110

süreçlerin tamamında, COSO KRY Sistemini oluşturan bileşenleri kapsanması gerekmektedir.

Değerlendirme kriterlerinin belirlenmesi ve **risk değerlendirmesi** aşamalarında kurumda mevcut COSO KRY çerçevesi esas alınarak, iç denetimin risk bazlı olması gereken yıllık planları açsısından, iç denetim yöneticisi tarafından değerlendirilir, iç denetim yöneticisi tarafından kurumun risk değerlendirme sürecine tamamen bağlı kalınabilir veya iç denetim açısından gerekli görülen değişiklikler iç denetim faaliyeti açısından ele alınabilir. Kurum üst yönetimi ile üst seviye bir risk değerlendirmesi konusunda iş birliği yapılarak, yıllık iç denetim planlarında ele alınacak risk değerlendirme süreci oluşturulur. Burada önemli olan COSO KRY Sisteminin etkinliği ile ilgili bağımsız bir güvence verilmesi konusunda, bağımsızlık ve tarafsızlığı zedelenmemiş olarak kurum yönetimi ile işbirliği yapılabilmesidir. Bu seviyede ele alınan risk değerlendirmesinin, denetim faaliyetinin saha çalışmalarında baş vurulacak risk değerlendirme çalışmasına göre daha üst düzey ve genel hatlara sahip olacağı söylenebilir.

> *"Bir riskin kabul edilebilir olup olmadığına kim karar verecektir? Bunun cevabı, iç denetçi vermeyecektir. İç denetçinin sorumluluğu, profesyonel değerlendirme yeteneğini ve risk ve kontrol hakkındaki bilgisini kullanarak kendi kişisel kanaatini oluşturmaktır…Sorumluluğunun bir başka yönü, risklerin kabul edilebilir bulunduğunu veya konunun yönetim tarafında uygun seviyedeki bir otoriteye adreslendiğini görmesi gereğidir."* [21]

Belirlenen denetim evreni ve benimsenen risk değerlendirme süreçlerini takiben risk bazlı yıllık iç denetim planı hazırlanır ve yönetim kurulunun onayına sunulur. "*İç denetim için önemli başarı kriterlerinden biri kurumun risk yönetimi olgunluk seviyesine göre çalışmalarını planlama becerisidir."* [22]

[21] IIA, **Sawyer's Guide for Internal Auditors**, 2c., s.98
[22] E. Handan Sümer Göğüş, **Risk Odaklı İç Denetimde Risklerin Saptanması ve Değerlendirilmesi**, İstanbul, Türkmen Kitabevi, 2012, s.68

"Yıllık iç denetim planlarının hazırlanmasında şu adımların dikkate alınması gerekir; kurum arşivinin ve diğer uygun kaynakların gözden geçirilmesi ve araştırılması (kurumun iş planları, stratejik planlar, kurum risk değerlendirmesi, yıllık raporlar, yönetim kurulu tutanakları, kurum yönetimi toplantı tutanakları, dış kaynaklı raporlar, dış denetim raporları vb.), önceki iç denetim planlarının, gelişim raporlarının ve gelişmekte olan işlere yönelik raporların gözden geçirilmesi, üst yönetimle kurumun risk alanlarına ilişkin istişare edilmesi, taslak denetim planının hazırlanması, önerilen denetim planının ilgili taraflarla iletişimi, gözden geçirilmesi gereken ana risk alanları ile ilgili geri dönüş ve onay alınması, denetim planının sonuçlandırılması, onay için yönetim kuruluna ve yönetime sunulması, değişen koşullara bağlı olarak planların düzenli biçimde izlenmesi, gözden geçirilmesi ve tekrar değerlendirilmesi." [23]

İç Denetim Faaliyetinin planlanması süreci ile ilgili UMUÇ' nde düzenlenen; planlama konusunu düzenleyen **2010 numaralı standart,** koordinasyon konusunu düzenleyen **2050 numaralı standart**, bildirim ve onay konusunu düzenleyen **2020 numaralı standart,** işin niteliği konusunu düzenleyen **2100 numaralı standart**, kurumsal yönetim konusunu düzenleyen **2110 numaralı standart**, risk yönetimi konusunu düzenleyen **2120 numaralı standart**, kontrol konusunu düzenleyen **2130 numaralı standart** ve bunlarla ilgili UMUÇ' nde düzenlenen uygulama tavsiyeleri öncelikli olarak belirleyici olacaktır.

Hazırlanan yıllık iç denetim planının yönetim kurulu tarafından onaylanmasından sonra iç denetimin yürütülmesi aşamasına geçilir.

[23] IIA, Coordinating Risk Management and Assurance," **Practice Guide**, March 2012, (Çevrimiçi) http/www.globaliia.org/standards-guidance, 13 Ocak 2015

2.4.3.5. İç Denetimin Yürütülmesi

İç denetimin yürütülmesi aşaması, **iç denetim faaliyetinin ön çalışması** ve **iç denetim faaliyetinin saha çalışması** olarak iki aşamada ele alınabilir.

İç denetim faaliyetinin ön çalışması; denetim faaliyetinin hedeflerinin, kapsamının, benimsenecek denetim yaklaşımının belirlendiği, kapsam ve denetim yaklaşımına uygun detay seviyesinde risk değerlendirme sürecinin iç denetim ihtiyaçları doğrultusunda ve iç denetim faaliyeti ile sınırlı olarak tekrar ele alındığı, çalışma planı ve denetim takvimi belirlenerek ilgili taraflarla açılış toplantısının yapıldığı safha olarak değerlendirilebilir.

> *"Denetim görev planlamalarında iç denetim ekibi risk olaylarını ve denetim konularını belirlemek için resmi, kapsamlı ve dökümante edilmiş bir risk değerlendirme süreci ile yürütmelidir. Bu durum, pek çok araştırma, denetim alanı veya kurum yönetimi ile istişare ve gözden geçirmelerle kurumu ve/veya denetim alanını yakından tanımayı gerektirecektir…Risk değerlendirme metotları farklılık gösterebilir ancak bütün risk değerlendirme metotları şu noktaları içermelidir; risk olayının tanımı (olumsuzluk, istenmeyen durum), olayın meydana gelme olasılığı (yüksek, orta, zayıf), olumsuz durumun hedefler ve amaçların başarılmasına yönelik etkisi (yüksek, orta, düşük), uygulamadaki mevcut kontroller (sistemler, politikalar, prosedürler vb.) ve bunların etki düzeyleri (etkili, etkili değil), risk olaylarının derecelendirmesi."* [24]

İç denetim çalışma planları ile ilgili UMUÇ' nde düzenlenen; görev planlamasını düzenleyen **2200 numaralı standart,** planlamada dikkate alınması gerekenler konusunu düzenleyen **2201 numaralı standart,** görev amaçları konusunu düzenleyen **2210 numaralı standart**, görev kapsamı konusunu düzenleyen **2220 numaralı standart**, görev kaynaklarının tahsisi konusunu düzenleyen **2230 standart**, görev iş programı konusunu düzenleyen **2240 numaralı standart** ve

[24] A.e

bunlarla ilgili UMUÇ' nde düzenlenen uygulama tavsiyeleri öncelikli olarak belirleyici olacaktır.

İç denetim faaliyetinin saha çalışmaları; iç denetim testlerinin gerçekleştirildiği, denetim bulgularının ve kanıtlarının toplandığı ve değerlendirildiği, önerilerin geliştirildiği, bulguların denetlenen fonksiyon amiri ile paylaşıldığı, ilgili taraflarca kapanış toplantısının yapıldığı safha olarak değerlendirilebilir.

Denetim kanıtlarının elde ediliş biçimleri ve bilgi kaynakları ile söz konusu kanıtın ne ölçüde itibar edileceğini belirlenmektedir**. Mülakat ve görüşmelerle** elde edilen denetim kanıtları, **belgelerden elde edilen** denetim kanıtları, **fiziksel olarak var olan** denetim kanıtları ve **analizlerle elde edilen** denetim kanıtları olmak üzere dört tür denetim kanıtından bahsedilir.

Fiziksel olarak var olan, denetçi tarafından gözle görülen, varlığı fiziksel olarak teşhis edilen kanıtlar en kuvvetli kanıtlar olarak kabul edilir. Belgelerden elde edilen kanıtlar ikinci derece kuvvetli kanıtlar olarak değerlendirilir. Belgelerden elde edilen kanıtlardan, kurum dışı kaynaklardan elde edilen kanıtlar genel olarak kurum içi kaynaklardan elde edilen kanıtlara oranla daha güçlü olarak kabul edilir. Belgeye dayalı kanıtlardan sonra kuvvetlilik derecesine göre, analizler sonucu elde edilen kanıtlar ve son olarak da mülakat ve görüşmelerle elde edilen kanıtlar gelmektedir.

Denetim kanıtları değişik test metotları uygulanarak derlenebilir. Hangi test metodunun kullanılacağına, test edilen konunun ne olduğu ve içerdiği riske göre karar verilmektedir. Başlıca test metotlarından; iç denetçi tarafından, denetim kapsamı ve konusuna ilişkin yapılan gözlemler, sorgulamalar, doğrulamalar, mülakatlar, araştırmalar, izlemeler (bir belgeden sonraki belgelere doğru ilerlemek veya bir belgeden önceki belgelere doğru ilerlemek sürati ile), analitik prosesler ve karşılaştırmalar (beklenen sonuçların gerçekleşenlerle karşılaştırılması, trend

analizleri, oran analizleri, sektörel karşılaştırmalar, makuliyet testleri, regresyon analizleri vb.) olarak bahsedilebilir.

Uygulamaya karar verilen test metotlarında ele alınacak işlemler genellikle kurumun bir veya birkaç faaliyet dönemine ilişkin bir grup işlemi arasından seçilmektedir. Bu seçime "**örnekleme**" adı verilmektedir. Örnekleme, bir veri havuzundan belirlenmiş kurallar ve metodolojiye göre verilerin seçilmesi olarak tanımlanabilir. Söz konusu örneklemenin yapılması ile ilgili uygulanan belli başlı teknikler; istatsistiki örneklemeler, tesadüfi örneklemeler ve yargıya dayalı örneklemeler olarak ifade edilebilir.

İç denetim faaliyetinin saha çalışması ile ilgili, UMUÇ' nde düzenlenen; görevin yapılması konusundaki **2300 numaralı standart**, bilgilerin tespiti ve tanımlanması ile ilgili **2310 numaralı standart**, analiz ve değerlendirme ile ilgili **2320 numaralı standart**, bilgilerin kayıtlı hale getirilmesi ile ilgili **2330 numaralı standart** ve bunlarla ilgili UMUÇ' nde düzenlenen uygulama tavsiyeleri öncelikli olarak belirleyici olacaktır.

Denetim bulgularının ve kanıtların değerlendirme aşamasında ihtiyaç duyulan değerlendirme kriterleri açısından geleneksel denetim faaliyetinde en yaygın kullanılan araçlar risk/kontrol matrisleri, iş akışları, politika, prosedür ve yönetmelikler olurken, COSO İç Kontrol Sisteminin güncellenmiş versiyonunda Tablo 2.7'de belirtilen, modelin prensipleri ile ilişkilendirilmiş odak noktaları, denetçi için öncelikle bakılması gereken konuların çerçevesini, bir başka deyişle etkinliği ölçülmesi gereken kriterleri oluşturmaktadır.

İç denetim faaliyeti açısından kuruma has tasarlanmış bir KRY sisteminin etkinliğinin değerlendirilmesi, kuruma has hedeflerin, önceliklerin, risklerin, kaynakların, durumsallıkların anlaşılması, maliyet- fayda dengesinin dikkate alınarak uygulamaların değerlendirilmesini gerektirmektedir. Bu nedenledir ki söz konusu değerlendirmelerin tarafsız birimlerce okunması ve anlaşılması için bu değerlendirmelerin kapsamlı ve ayrıntılı bir biçimde dökümante edilmesi çok

önemlidir. Saha çalışmalarında elde edilen bulgular ve bunlara yönelik değerlendirmeler yapılırken söz konusu değerlendirmelerin kapsamlı ve detaylı dökümantasyonunun gerekliliği sürekli göz önünde tutulmalıdır.

2.4.3.6. İç Denetimin Raporlanması

Denetimin raporlanması aşaması; taslak denetim raporunun hazırlanması ve nihai denetim raporunun hazırlanması olarak iki ana safhadan oluşmaktadır. Taslak denetim raporunun hazırlanması safhası; denetlenen birim ve/veya fonksiyon amiri ile yapılan kapanış toplantısını takiben denetçi tarafından taslak denetim raporunun hazırlandığı, taslak denetim raporunun denetlenen birim ve/veya fonksiyon amiri ile görüşülerek rapor bulgularına ilişkin geri bildirim alındığı, alınması gereken önlem ve aksiyonlar konusunda denetlenen birim ve/veya fonksiyon amiri ile istişare edilerek mutabakat sağlanan ve sağlanamayan alanların belirlendiği, mutabakat sağlanan aksiyonların takvime bağlanarak bir aksiyon planına dönüştürüldüğü safhadır.

Nihai denetim raporunun hazırlandığı safha, taslak denetim raporu ve hazırlanan aksiyon planından hareketle iç denetim yöneticisi tarafından nihai denetim raporunun hazırlanması ve UMUÇ' nde düzenlenen uyulması zorunlu standartların göz önünde tutularak, denetim raporu için yönetim kurulu başta olmak üzere kurumun belirlenmiş birimlerine raporun iletilmesi safhasıdır.

Denetim raporlarının içeriği ve formatı kuruma has olabilir ancak raporların, en azından denetim faaliyetinin amacı, kapsamı ve sonuçlarını içermesi beklenmelidir. Denetim raporunda yer alan denetçi görüşü üst yönetim, yönetim kurulu ve diğer paydaşların beklentilerini dikkate alarak, yeterli, güvenilir, ilgili ve yararlı bilgi ile desteklenmelidir. Raporlamalar, doğru, objektif, açık, özlü, yapıcı, tam olmalı, muhataplarına zamanında sunulmalıdır.

İç denetim faaliyetinin raporlama süreci ile ilgili, UMUÇ' nde düzenlenen; sonuçların raporlanması konulu **2400 numaralı standart**, raporlama kıstasları konulu **2410 numaralı standart**, raporlamaların kalitesi konulu **2420 numaralı standart**, hata ve eksiklikler konulu **2421 numaralı standart**, "Uluslararası İç Denetim Mesleki Uygulama Standartları'na Uygun Olarak Yapılmıştır" ibaresinin kullanımı konulu **2430 numaralı standart**, görevlendirmelerde aykırılıkların açıklanması konulu **2431 numaralı standart**, sonuçların dağıtımı konulu **2440 numaralı standart**, genel görüşler konulu **2450 numaralı standart** ve bunlarla ilgili UMUÇ' nde düzenlenen uygulama tavsiyeleri öncelikli olarak belirleyici olacaktır.

2.4.3.7. Sonuçların Takibi

Sonuçların izlenmesi aşaması, denetim sonuçlarının izlenmesi, denetim faaliyetinin değerlendirilmesi ve denetçinin değerlendirilmesi safhalarından oluşmaktadır.

Denetim sonuçlarının izlenmesi safhası; denetim raporunda ilgili birim/fonksiyon yöneticisi ve iç denetçi tarafından oluşturulan aksiyon planını ile ilgili gelişmelerin izlendiği safhadır. İlgili birim fonksiyon yöneticisi tarafından, aksiyon planı ile ilgili gelişmeler konusunda, belli periyotlarda iç denetim yöneticisinin bilgilendirilmesi beklenir. İç denetim yöneticisi tarafından, aksiyon planındaki gelişmelerin seyrini değerlendirmek için gerekli görülmesi durumunda yeni bir denetim faaliyeti gündeme getilebilir.

Denetim faaliyetinin değerlendirilmesi safhası; yürütülen denetim faaliyetinin denetlenen birim/fonksiyon amiri ve/veya ekibi tarafından anket vb. yöntemlerle değerlendirilmesi ve sonuçların iç denetim yöneticisi ile paylaşılması safhasıdır.

Denetçinin değerlendirilmesi safhası; denetim faaliyetini yürüten ekipte yer alan iç denetçilerin performansının iç denetim yöneticisi, tarafında ve/veya adına denetlendiği safhadır. Bu değerlendirmeler, iç denetçilerin sicil dosyalarına ve kariyer gelişimlerine konu edilir.

İç denetim faaliyetinin sonuçların takibi süreci ile ilgili, UMUÇ' nde düzenlenen; ilerlemenin gözlenmesi konulu **2500 numaralı standart**, risklerin kabul edildiğinin iletilmesi konulu **2600 numaralı standart** ve bunlarla ilgili UMUÇ' nde düzenlenen uygulama tavsiyeleri öncelikli olarak belirleyici olacaktır.

İç denetim süreci ile ilgili detaylar ve uygulama kılavuzuna hazırlanacak iç denetim rehberinde yer verilmeli, iç denetim ekibi ile iç denetim rehberinin içeriğinin iletişimi yapılmalıdır. İç denetim faaliyeti ile ilgili sürecin yürütülmesinde UMUÇ' nde düzenlenen ve uyulması zorunlu olan standartların yanı sıra COSO İç Kontrol Sisteminde düzenlenen değerlendirme kriterleri (odak noktaları) göz önünde tutulmalıdır.

ÜÇÜNCÜ BÖLÜM
BİR ÜRETİM İŞLETMESİNDE KURUMSAL RİSK YÖNETİMİ ÇERÇEVESİNİN OLUŞTURULMASINA YÖNELİK BİR UYGULAMA

3.1. Çalışmanın Amacı, Yöntemi ve İşletme Hakkında Bilgiler

Bu çalışmada, kurumsal risk yönetimi çerçevesinin oluşturulması uygulamalarına ışık tutmak amacıyla; bir üretim şirketinde, şirkete özgü bir KRY sisteminin tüm süreçleri ile kurulması, işler hale getirilmesi ve iç denetim fonksiyonu aracılığı ile etkinliğinin sağlanmasına yönelik bir işletme uygulamasına yer verilmiştir.

Uygulamamızda nitel araştırma yaklaşımı benimsenmiş olup, durum çalışması deseninden yararlanılmıştır.

> "*Durum çalışması araştırması, araştırmacının gerçek yaşam, güncel sınırlı bir sistem (bir **durum**) ya da belli bir zaman içerisindeki çoklu sınırlandırılmış sistemler (durumlar) hakkında **çoklu bilgi kaynakları** (örneğin gözlemler, mülakatlar, görsel-işitsel materyaller ve dökümanlar ve raporlar) aracılığı ile detaylı ve derinlemesine bilgi topladığı, bir **durum betimlemesi** ya da **durum temaları** ortaya koyduğu nitel bir yaklaşımdır.*" [1]

KRY Sistemini uyarlayacağımız kurumun adı ABC Kimya San. A.Ş.' dir. Bundan sonra kısaca **ABC Kimya** olarak anılacaktır. ABC Kimya, yerli sermaye ile 2007 yılında kurulmuş bir anonim şirket olup, başka bir iştiraki, ortaklığı vb. girişimi bulunmamaktadır. ABC Kimya; ev temizlik amaçlı kimyasal madde üretimi ve satışı yapmaktadır, üretim tesisi ve merkez yönetim kadroları Türkiye'dedir.

[1] John W.Creswell, **Nitel Araştırma Yöntemleri Beş Yaklaşıma Göre Nitel Araştırma ve Araştırma Deseni**, Çeviri Editörleri:Yrd. Doç. Dr. Mesut Bütün, Yrd. Doç.Dr. Selçuk Beşir Demir, Çeviri: Doç. Dr. Osman Birgin, Doç. Dr. Suat Ünal, Doç. Dr. Tuncay Özsevgeç, Doç. Dr. Yüksel Dede, Doç. Dr. Ahmet Bacanak, Yrd. Doç. Dr.Arif Bakla, Doç. Dr. Ayfer Budak, Yrd. Doç.Dr. Güney Hacıömeroğlu, Doç. Dr. İbrahim Budak, Yrd. Doç.Dr. Mahmet Aydın, Yrd. Doç. Dr. Mesut Bütün, Yrd. Doç. Dr. Miraç Aydın, Yrd. Doç. Dr. Selçuk Beşir Demir, 4.bs., Ankara, Siyasal Kitabevi, Şubat 2018, s.97 .

Şirket, kendi satış-dağıtım örgütünü kullanmaktadır. Üretimi yapılan markalı ürünler, oluşturulan ve yönetilen bölgesel bayi kanalı marifeti ile geleneksel perakende noktalarına (yerel süpermarketler, bakkallar, büfeler vb.), ve ulusal zincir olan perakende noktalarına satılmakta, bazı ulusal zincirler için özel markalı ürün üretilmektedir.

Toplam olarak sekiz üretim hattı bulunan kurumda çalışan mavi yakalı sayısı 150 olup, teknoloji yoğun üretim süreçleri ile çalışılmaktadır. Her bir üretim hattı için, pazar günleri ve resmi tatiller hariç olmak üzere günde üç vardiya üretim yapılmaktadır. İki üretim hattında modernizasyon ihtiyacı bulunan ABC Kimya'da diğer 6 üretim hattı yeni teknoloji olup, yapılan stratejik iş planlarında bir veya iki yıllık yakın gelecekte yenileme, büyük bakım, kapasite arttırma vb. konularda sabit yatırım yapılması öngörülmemektedir. Üçüncü yılın sonunda kapasite ihtiyacına bağlı olarak bir üretim hattının kapasite arttırma yatırımı ile ilgili ön fizibilite çalışmaları yapılmaktadır. Kurumun Pazar payını arttırarak ölçeğini iki katına çıkarma stratejisi bulunmakta olup, bu konuda pazar fırsatları izlenmektedir.

ABC Kimya üretim tesisleri ve diğer iş fonksiyonlarında entegre bir bilgi teknolojileri alt yapısına sahip olup, iş fonksiyonları arasında entegrasyonu sağlanmış, uluslararası kabul gören, Türkiye'de bakım ve destek hizmeti alabildikleri güvenilir bir bilgisayar yazılımı kullanılmaktadır.

Kurumda çalışan ana iş fonksiyonları üretim, tedarik zinciri yönetimi, satış-dağıtım, ve pazarlama fonksiyonları olup, insan kaynakları, idari işler, bilgi teknolojileri ve mali işler ekipleri destek fonksiyonları olarak hizmet vermektedir.

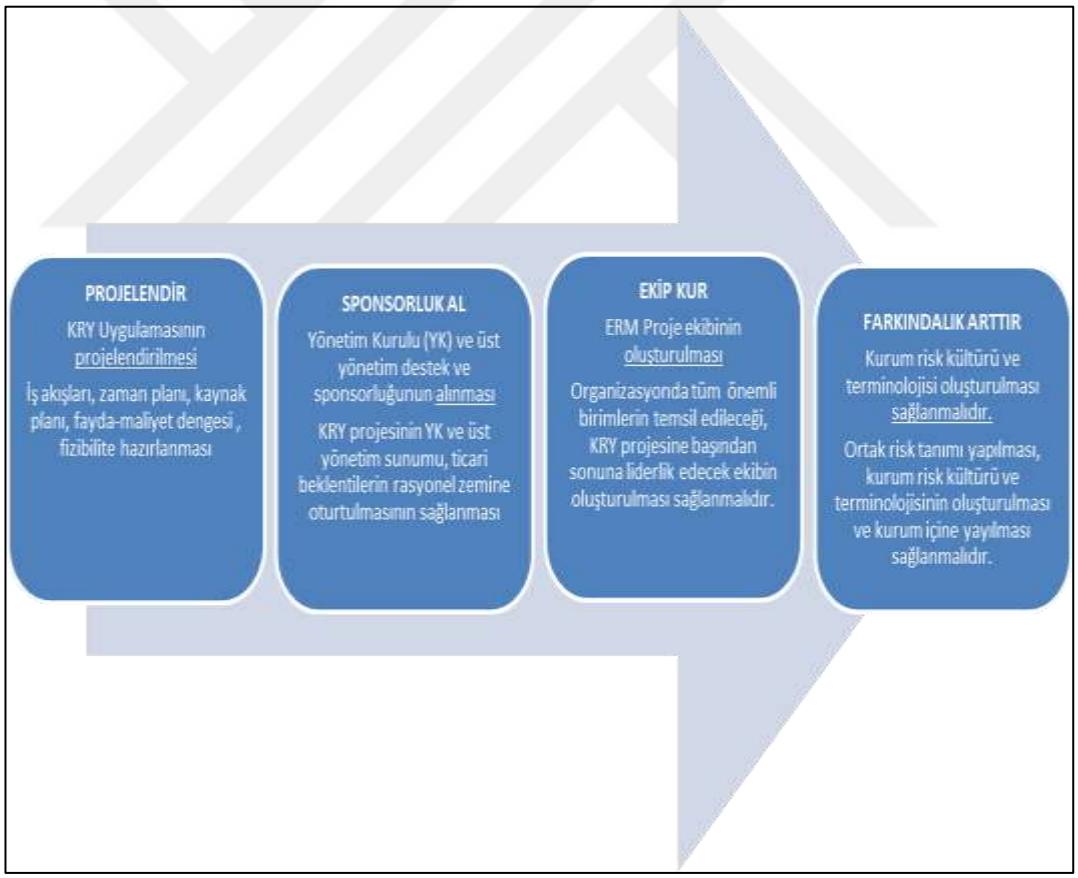
ABC Kimya, sektöründe oluşan değişimlere bağlı olarak; söz konusu tehditler ve fırsatlara karşı daha hazırlıklı olmak, stratejik ve iş hedeflerinin gerçekleştirmeye yönelik makul bir güvence sağlamak fikri ile ilgilenmekte ve bu konu ile ilgili kurumda bir KRY çerçevesi oluşturmak istenmektedir. Uygulama örneğimizde ABC Kimya'da KRY Sisteminin uyarlanması için yapılması gerekenler incelenecektir.

3.2. Kurumsal Risk Yönetimi Çerçevesinin Oluşturulması

3.2.1. Kurumsal Risk Yönetimi Projesi Hazırlıkları

Başarılı bir KRY Uygulama projesi için, proje çalışmasını başlatmadan evvel atılması gereken adımlar vardır. Söz konusu adımların genel çerçevesi Şekil 3.1'de gösterilmektedir.

Şekil 3.1: KRY Uygulama Projesi Öncesi Hazırlıklar



ABC Kimya'da KRY Sistemi uygulaması projelendirilerek hayata geçirilmesi planlanmıştır. Bu çerçevede, **projeye bir isim** verilerek çalışmalara

başlanmıştır. KRY Sistemi uygulama projesi ABC-KRY olarak isimlendirilmiş olup, bundan sonra ABC-KRY olarak anılacaktır.

3.2.1.1. Proje Ekibi Fizibilitesi ve Üst Yönetim Desteği Alınması

Proje ekibi ile ilgili olarak; ABC-KRY projesinde proje liderliğini Mali İşler Yöneticisi yapacak olup, proje ekibi, kurumda mevcut fonksiyonların yöneticilerinden oluşturulmuştur. İç denetim yöneticisi proje ekibinin dışında tutulmuş olup, bağımsızlık ve tarafsızlığını korumasına yardımcı olacak koruma tedbirleri alındıktan sonra proje ile ilgili süreçlerin dökümantasyonu ve kurum içi proje farkındalığı ile ilgili iletişim ve kurum içi eğitim süreçlerinde destek alınacaktır.

ABC-KRY projesi ile ilgili atılacak adımlar ve bu adımlarla ilgili planlanan süreler aşağıda Tablo 3.1'de gösterilmiş olup, söz konusu adımlar Tablo 3.2'de proje takvimine bağlanmıştır. Toplam proje süresi başlangıçtan itibaren 22 ay olarak öngörülmektedir.

Tablo 3.1: ABC-KRY Proje Adımları

Faaliyet	Süre (Ay)
KRY uygulaması projelendirmesi	1
Yönetim Kurulu ve üst yönetim desteği	2
Proje ekibinin oluşturulması	1
Ortak risk kültürü, kavram birliği sağlanması	14
Yönetim Kurulu düzenlemeleri	1
Kurum vizyon, misyon ve stratejilerinin güncellenmesi	3
Organizasyon yapısının güncellenmesi	2
İş akışlarının güncellenmesi	3
Kurum etik değerleri ve çalışma prensiplerinin belirlenmesi ve iletişimi	2
Politika ve prosedürlerin güncellenmesi	3
Departman hedefleri ve bireysel hedeflerin revizyonu	1
Risk envanterinin oluşturulması ve risk gruplaması	1
Risklerin değerlendirilmesi ve risk haritasının oluşturulması	1
Risklerin önceliklendirilmesi ve giderilmesi çalışmaları	1
Kontrol faaliyetlerinin gözden geçirilmesi ve güncellenmesi	2
Rapor envanteri ve dağıtım listesinin gözden geçirilmesi	1
Bilgi sistemleri yeterlilik ve güvenirliğinin gözden geçirilmesi	1
Kurum işi ve dışı iletişimin kurgusu, politikaların güncellenmesi	1

Tablo 3.2: ABC-KRY Proje Takvimi

Faaliyet	Ay											
	1	2	3	4	5	.....		19	20	21	22
KRY uygulaması projelendirmesi											
Yönetim Kurulu ve üst yönetim desteği											
Proje ekibinin oluşturulması											
Ortak risk kültürü, kavram birliği sağlanması											
Yönetim Kurulu düzenlemeleri											
Kurum vizyon, misyon ve stratejilerinin güncellenmesi											
Organizasyon yapısının güncellenmesi											
İş akışlarının güncellenmesi											
Kurum etik değerleri ve çalışma prensiplerinin belirlenmesi ve iletişimi											
Politika ve prosedürlerin güncellenmesi											
Departman hedefleri ve bireysel hedeflerin revizyonu											
Risk envanterinin oluşturulması ve risk gruplaması											
Risklerin değerlendirilmesi ve risk haritasının oluşturulması											
Risklerin önceliklendirilmesi ve giderilmesi çalışmaları											
Kontrol faaliyetlerinin gözden geçirilmesi ve güncellenmesi											
Rapor envanteri ve dağıtım listesinin gözden geçirilmesi											
Bilgi sistemleri yeterlilik ve güvenirliğinin gözden geçirilmesi											
Kurum işi ve dışı iletişimin kurgusu, politikaların güncellenmesi											

Yönetim Kurulu ve üst yönetimin desteğinin alınması aşamasında; Yönetim Kurulu ve üst yönetimin ABC- KRY' den beklentileri rasyonel bir zemine oturtularak maliyet-fayda dengesi kurulmş, gerçekçi bir proje uygulama takvimi

oluşturulmuştur. Risk yönetimi konusunda sadece olumsuzluk durumları üzerinde değil, hem olumsuzluklar hem de fırsatlar üzerinde durulmuş, proje fizibilitesi, kurumun lehine açık bir fayda-maliyet dengesi ortaya koyacak biçimde Yönetim Kurulu ve üst yönetim ile paylaşılmıştır. ABC-KRY projesinde Yönetim Kurulu ve üst yönetimin rolü açıkça ifade edilmiş ve bu durumun doğru anlaşılması sağlanmıştır.

ABC-KRY için başta Yönetim Kurulu olmak üzere üst yönetimin projeye vereceği destek çok önemlidir. Söz konusu desteğin uzun süreli olması ve gerekli üst yönetim desteğinin sağlanabilmesi için, ABC-KRY uygulaması sonucunda olası kazanım beklentilerinin gerçekçi ve rasyonel bir zemine oturtulması, proje fizibilitesinin bu rasyonel zeminde yapılması son derece önem taşımaktadır. Aksi halde proje uygulaması sırasında çeşitli sebeplerle üst yönetimin projeye olan inancı zayıflayabilir, destekleri uzun süreli olmayabilir. Sürdürülebilir üst yönetim desteği için kazanım beklentilerinin ve fizibilitenin rasyonel bir zemine oturtulması gerekir.

ABC-KRY uygulaması ile ilgili beklenen kazanımların, kaynak tahsisinin, fayda-maliyet dengesinin, fizibilitenin, uygulama takviminin yer aldığı proje dökümanı hazırlanarak üst yönetimle paylaşılmış ve üst yönetimin motivasyon kaynağı olacak **ticari beklentilerinin rasyonel bir zemine oturtulması** sağlanmıştır.

Söz konusu rasyonel ticari beklentiler şu şekli ile ele alınmaktadır; kurumun pazarpayını arttırarak ölçeğini iki katına çıkarma stratejisi paralelinde organizasyonun kurum kaynaklarının ve risklerinin daha doğru yönetilmesi yeteneğini arttıracağı beklentisi, SPK Kurumsal Yönetim İlkelerinin gerekliliklerine yaklaşmamızı ve gelecekte halka arz ile alternatif fon kaynağı yaratılmak istendiğinde, hazırlık sürecinin kısalacak olması beklentisi, risk yönetim yeteneği arttırılmış bir organizasyonun finansal derecelendirilmesindeki iyileşme paralelinde fonlama maliyetlerinin düşeceği beklentisi, kurum stratejik hedeflerinin ve operasyonel hedeflerinin gerçekleştirilmesi konusunda makul seviyede bir güvence

sağlanması ve bu durumun sürdürülebilir kılınması, iş hedeflerimizi etkileyecek risk ve fırsatların farkında olarak bunların önceliklendirilmesi ve odaklanılması, iş süreçlerimizle ilgili organizasyonumuzun yeterli ve yetkin kılınması, iş süreçlerimizin olgunluğunun arttırılarak kaynak verimliliğimizin arttırılması, öğrenen organizasyon yapısını yaşatarak rekabet avantajımızın arttırılması suretiyle karlı ve sürdürülebilir büyümenin sağlanması, karlı ve sürdürülebilir iş modeli ile çalışanlarımızın iş güvencesi ve kariyer gelişimlerine katkı sağlanması.

Projenin ilerlediği aşamalarda, risk değerlendirmesi sonrası firmanın risk haritası oluşup önceliklendirme yapıldığında ABC-KRY ile odaklanılan ve yönetilmeye başlayan risklerin finansal ve finansal olmayan ölçülmüş etkilerini göz önüne koymak mümkün olacağından bu ölçüm üst yönetimin projeye desteğinin sürmesine katkı sağlamıştır. Proje geri dönüş süresi 2,5 yıl olarak hesaplanmıştır.

3.2.1.2. KRY Ortak Terminoloji Oluşturulması ve Kurum Farkındalığının Arttırılması

Kurum risk kültürü ve ortak terminoloji oluşturma ile ilgili; risk tanımının yapıldığı, kurum risk iştahı ve risk toleransının tarif edildiği, ABC-KRY ile amaçlananın ana hatlarının tarif edildiği, ABC- KRY' nin uygulama çerçevesinin genel hatları ile tarif edildiği bir **"proje kitapçığı**" hazırlanmıştır. Proje kitapçığında; operasyonel hedef, departman hedefi ve bireysel hedef belirlenirken, beklenen davranış modellerine değinilmiş, risk envanteri oluşturulması ve risk değerlendirmesi sırasında göz önünde tutulması istenen kurumsal bakış açısı belirtilmiş, yöneticilere kendi ekipleri ile konu hakkında iletişim yöntemleri ve araçları ile ilgili öneriler yer almıştır. Proje ekibi ile yapılan toplantılarla proje tanıtılmıştır. Kurum çalışanları ile proje kitapçığında yer alan tanım ve terminolojinin ve proje başlangıcının hangi içerikte ve sıklıkta paylaşılacağı, hangi araçların kullanılacağı, yapılması gereken toplantı takvimi ve gündemleri, eğitim programları ve içeriği belirlenmiş ve uygulamaya koyulmuştur. Kurum risk yönetim felsefesi tek sayfa olarak hazırlanmış ve çalışanlarla paylaşılmıştır.

Kurumda **ortak risk terminolojisi** ile ilgili olarak şu tanımlar yapılmıştır: **"Belirsizlik"** kavramı ile kast edilen, yaratacağı gelişmeler ve sonuçlar itibariyle öngörülemeyen, bilinemeyen hal ve durumlardır. **"Risk"** kavramı ile kast edilen, belirsiz ortamların iş süreçleri ile ilgili olumsuz sonuç ve kayıplar oluşturma ihtimalidir. **"Fırsat**" kavramı ile kast edilen, belirsiz ortamların iş süreçleri ile ilgili olumlu sonuç ve kazançlar oluşturma ihtimalidir. **"Doğal (içsel) risk"** kavramı ile kast edilen, iş süreçlerimizin doğasında yer alan ve giderilmesi ile ilgili herhangi bir önlem alınmayarak gerçekleşmesi durumunda riskin olası olumsuz sonuçlarıdır. **"Artık risk"** kavramı ile kast edilen, iş süreçlerimizin doğasında bulunmakla birlikte alınan tüm önlemlere rağmen riskin gerçekleşmesi sonrası oluşan olumsuz sonuçlardır. **"Kurumun risk iştahı"** kavramı ile kast edilen, kurumun kabul etmeye gönüllü ve istekli olduğu risk seviyesidir. "**Risk toleransı"** kavramı ile kast edilen, kurumun katlanabileceği risklerin alt ve üst sınırlarıdır. Kurumun karşılaşması durumunda sonuçları itibariyle tolere edebileceği risk seviyesi olarak anlaşılmalıdır. "**Risk envanteri"** kavramı ile kast edilen, kurum iş süreçleri ve hedefleri ile ilgili tanımlanmış risklerin tamamıdır. "**Risk grubu**" kavramı, kurum risklerinin türlerine göre gruplandırılarak bir bütünlük içinde gösterilmesini ifade etmektedir. **"Risk haritası"** kavramı, kurum risklerinin değerlendirilmesi ve önceliklendirilmesi sonucu çok yüksek, yüksek, orta, düşük çok düşük olarak sınıflanmış biçimde gösterilmesidir.

Kurum risk yönetim felsefesi dökümanında bu tanımlara yer verilmiş, gerekli dökümantasyonla birlikte kurum içi iletişimleri yapılmıştır.

Kurumun risk yönetim felsefesi; "Risk yönetimi, vizyon ve misyondan başlayarak bireysel hedeflerimize kadar uzanan , iş süreçlerimizin tamamını kapsayacak bir süreçtir. Risk yönetimi aynı zamanda fırsatların da yönetimi anlamına gelip süreç sadece olumsuzluklara değil, fırsatlara da odaklanmalıdır. Risk yönetiminin kurum hedeflerinin gerçekleştirilmesine yönelik makul bir güvence sağlaması beklenmektedir. Risk yönetimi sürecine bir ekibin liderlik etmesinin yanı sıra süreç tüm kurum çalışanlarının katılımı ve katkısı ile beklenen başarıya ulaşabilir. Risk yönetim sürecinin etkin kılınmasından Yönetim

Kurulu ve üst yönetim başta olmak üzere kurumun tamamı sorumlu iken, söz konusu sürecin etkinliği konusunda iç denetim faaliyetinden bağımsız ve tarafsız bir güvence verilmesi beklenmektedir." şeklinde ifade edilmekte olup, ilgili felsefe hakkın da Yönetim Kurulu ve üst yönetimin onayları alınmış, söz konusu felsefe ABC-KRY projesinin bir parçası olarak ortaya koyulmuş ve kurum çalışanları ile paylaşılmıştır.

3.2.2. KRY Uygulamalarının Hayata Geçirilmesi

3.2.2.1. Kontrol Ortamı ve İçsel Ortamın Hazırlıkları

Kurumun kontrol ortamının ve içsel ortamının ABC-KRY çerçevesinde hazırlanması ile ilgili olarak iki ana konuya odaklanılmaktadır. Bunlardan birincisi kurumun Yönetim Kurulu açısından TTK 375. madde ve TTK 378. maddede yer alan düzenlemelerde yer verilen yasal sorumlulukların karşılanması, ikincisi de kurumun güncellenerek ortaya koyulmuş vizyon ve misyonu doğrultusunda mevcut iç kontrol sisteminin ABC-KRY gerekliliklerine uygun hale getirilmesi olacaktır.

Bunu yaparken şu gereklilikler değerlendirilmelidir: TTK 375 anonim şirketler için muhasebe ve finans denetiminin sağlanması görevini Yönetim Kuruluna vermişken , TTK 378 halka açık şirketlerde riski yönetmek amacı ile uzman bir komite kurulması ve işletilmesini YK görevi olarak düzenlemektedir. Yapılan çalışma her iki düzenlemedeki gereklilikleri karşılayacak nitelikte olmalıdır. Aktif ve bağımsız bir YK ve denetim komitesi oluşturulmalı ve çalıştırılmalıdır. YK, ABC-KRY' ni istiyor ve destekliyor olmalı, motivasyon kaynakları rasyonel bir zemine oturtulmuş olmalıdır. Kurumun vizyon ve misyonu gözden geçirilerek makro hedefler güncellenmeli ve ortaya koyulmalı, bu doğrultuda ana stratejiler tekrar değerlendirilerek gerekirse revize edilmeli ve güncellenmelidir. Stratejiler doğrultusunda temel süreçler ve bunlara yönelik kaynak planlaması yapılmalı, organizasyon yapısı ve insan kaynakları bu planlamanın içinde değerlendirilmeli, gerekli yetkinlik ve yeterliliğin sağlanması konusunda özenli davranılmalıdır.

Organizasyon yapısı ve kurum kültürü ABC-KRY' yi destekler nitelikte olmalıdır (kurum içi yetki –sorumluluk sınırları belli mi, denge sağlanmış mı? Kurum içi ilişki tarzı resmi mi, gayri resmi mi? Ekip çalışması mı ön planda, bireysellik mi ön planda? Organizasyon hiyerarşisi dikey mi, yatay mı? Çalışanlar kurumu ne ölçüde içselleştirmiş ve gelecekleri ile kurum geleceğini ne ölçüde örtüştürmüş?). Kurum içi yetki-sorumluluk dağılımı dengeli, iş-süreç akışlar net olmalıdır. Kurumun dürüstlük ve etik değerler anlayışı uygulamak istenen ABC-KRY çerçevesinde güncellenip dökümante edilmeli, çalışanlarla düzenli iletişimi sağlanmalıdır. Etik değerler ve çalışma prensipleri dökümanının kurumsal değerleri yansıtmasının yanı sıra kurumun iş anlayışı, iş yapış biçimi ile ilgili kurumsal davranışlar hakkında oluşmuş ve kabul gören değerler setini de yansıtması beklenmelidir. Kurum, başta kritik işleri olmak üzere çeşitli işleri için ihtiyaç duyacağı mesleki yeterlilik ve sorumluluk seviyelerini belirleyip iş akışları, iş tanımları, politika ve prosedürlerinde bu durumu göz önünde tutmalı, ayrıca ihtiyaç duyduğu bu mesleki yeterlilik ve sorumluluk seviyelerini çalışanlarına kazandıracak programları çalıştırmalıdır. İnsan kaynakları ve politikaları şeffaf, adaletli, objektif ve performansı ödüllendirici nitelikte olmalı ve çalıştırılmalı, kurum etik anlayışı ve çalışma prensiplerinde aktarılan değerler kümesini yansıtılmalıdır.

3.2.2.1.1.Yönetim Kurulu

TTK 378. maddede halka açık şirketlerde YK, riskin yönetilmesi amacıyla uzman bir komite kurmak, sistemi, çalıştırmak ve geliştirmekle yükümlü kılınmıştır. Örnek kurumumuz olan ABC Kimya, halka açık olmaması sebebi ile öncelikle TTK 375. maddede düzenlenen YK sorumluluklarının karşılanması hedeflenmiş, yanı sıra ABC- KRY kapsamında TTK 378. madde düzenlemeleri de ayrıca değerlendirilmiştir.

TTK ilgili maddelerinde aktif ve bağımsız bir YK ve denetim komitesi oluşturulması ve çalıştırılması tavsiye edilmektedir. Aktif ve bağımsız YK' ndan kasıt "bağımsız üyelerle ilgili, en azından SPK Kurumsal İlkelerin Belirlenmesi ve

Uygulanmasına İlişkin Tebliğ ile düzenlenen bağımsız YK üyeliği kriterlerini karşılaması, ana strateji ve bunlara ilişkin süreçler ile ilgili sonucu etkileyecek karar mekanizmasında yer alması, bahsedilen doğrultuda aktif görevler üstlenmesidir.

SPK ilgili tebliğinde bağımsız YK üyeliği ile ilgili hususlar şöyle düzenlenmiştir; bağımsız YK üye sayısı toplam YK üye sayısının üçte birinden az olamaz, bağımsız YK üyelerinin görev süresi en fazla 3 yıl olarak düzenlenebilir, önemli nitelikte işlem sayılan hususlar için bağımsız YK üyelerinin çoğunluğunun onayı gerekir, çoğunluk onayının olmadığı durumlarda işlem yine de yapılmak istenirse genel kurul kararı alınır, bağımsız YK üyelerinden en az yarısı Türkiye'de yerleşik olmalıdır, bağımsız YK üyeleri şirket faaliyetlerinin işleyişini takip edebilecek ve üstlendiği görevlerin gereklerini tam olarak yerine getirebilecek ölçüde şirket işlerine zaman ayırabiliyor olmalıdır.

SPK Kurumsal Yönetim İlkelerine göre YK üyeleri içim bağımsızlık kriterleri; şirket, şirketin ilişkili taraflarından biri veya şirket sermayesinde doğrudan veya dolaylı olarak %10 veya daha fazla paya sahip hissedarların yönetim veya sermaye bakımından ilişkili olduğu tüzel kişiler ile kendisi, eşi ve ikinci dereceye kadar kan ve sıhri hısımları arasında, son beş yıl içinde, doğrudan veya dolaylı önemli görev ve sorumluluklar üstlenecek yönetici pozisyonunda istihdam, sermaye veya önemli nitelikte ticari ilişkinin kurulmamış olması, son beş yıl içerisinde, başta şirketin denetimini, derecelendirilmesini ve danışmanlığını yapan şirketler olmak üzere, yapılan anlaşmalar çerçevesinde şirketin faaliyet ve organizasyonunun tamamını veya belli bir bölümünü yürüten şirketlerde çalışmamış ve yönetim kurulu üyesi olarak görev almamış olması, son beş yıl içerisinde, şirkete önemli ölçüde hizmet ve ürün sağlayan firmaların herhangi birisinde ortak, çalışan veya yönetim kurulu üyesi olmaması, YK görevi dolayısıyla hissedar ise sermayede sahip olduğu payın oranının %1'den fazla olmaması ve bu payların imtiyazlı olmaması, bağımsız yönetim kurulu üyesi olması sebebiyle üstleneceği görevleri gereği gibi yerine getirecek mesleki eğitim, bilgi ve tecrübeye sahip olması, bağlı oldukları mevzuata uygun olması şartıyla üniversite öğretim üyeleri hariç, kamu kurum ve kuruluşlarında üye olarak seçildikten sonra tam zamanlı çalışmıyor olması, Gelir Vergisi Kanunu'na

göre Türkiye'de yerleşmiş sayılması, şirket faaliyetlerine olumlu katkılarda bulunabilecek, şirket ortakları arasındaki çıkar çatışmalarında tarafsızlığını koruyabilecek, menfaat sahiplerinin haklarını dikkate alarak özgürce karar verebilecek güçlü etik standartlara, mesleki itibara ve tecrübeye sahip olması.

Örnek uygulamamızda, ABC Kimya YK, iki bağımsız üye olmak üzere toplam altı üyeden oluşturulmuştur. YK yetki ve sorumluluklarının belirlenmesi ve YK' nun aktif kılınması ile ilgili olarak; şirket stratejileri ve bunlara yönelik planlanmış süreçler üzerinde aktif olmaları beklentisi doğrultusunda şirket ana sözleşmesi ile yetki ve sorumlulukları detaylı olarak ifade edilmiştir, yetki düzenlemesi şirket imza sirküleri ve şirket içi yetki düzenlemesi için hazırlanan yetki-onay formu marifeti ile netliğe kavuşturulmuş ve yine bu belgeler marifeti ile şirket içi iletişimi yapılmıştır.

3.2.2.1.2. Ana Sözleşme ve İmza Sirküleri

Şirket ana sözleşmesi kurumun faaliyetini, ortaklık yapısını, adresini, hisse dağılımını, merkez adresini, YK ile ilgili düzenlemeleri, genel kurul ile ilgili düzenlemeleri başta olmak üzere hissedarların kurum ve faaliyeti ile ilgili üzerinde mutabık kaldıkları genel çerçeveyi ortaya koyan şirketin esas sözleşmesidir. Ticaret Sicilde tescilini takiben hüküm doğurur.

Tablo 3.3: ABC Kimya San. A.Ş. Ana Sözleşme İçerik Örneği

ABC KİMYA SAN. A.Ş. ANA SÖZLEŞME İÇERİĞİ ÖRNEĞİ		
1-	Kuruluş	:Kuruluş esasları ve kurucuların isimleri, adresleri, uyruk ve kimlik numaraları yer alır.
2-	Şirket Ünvanı	:Şirket tam ünvanı açık şekilde belirtilir.
3-	Amaç Ve Konu	:Şirketin amaç ve konusu belirtilir.
4-	Şirketin Merkezi	:Şirket merkezinin adresine yer verilir.
5-	Şirketin Faaliyet Süresi	:Şirketin faaliyet süresi belirtilir.
6-	Sermaye ve Hisse Senetleri Nevi	:Şirket taahhüt edilen sermaye tutarı, kaç paya ayrıldığı ve her bir payın değeri, bu sermayenin tutar ve pay adedi detayında pay sahiplerine dağılımı, sermaye taahhüdünün ödenmesi esasları belirtilir.
7-	Yönetim Kurulu Düzenlemeleri	: a) Üyeler, kimlik bilgileri, adresleri, b) Üyelik süresi ve üyeliğin açılması esasları, c) Yönetim Kurulu başlıca görevleri, d) YK toplantı düzeni (hangi sıklıkta toplanacağı, toplantı yeter sayısı, YK kararlarının hangi şartlarda alınabileceği, toplantı çağrısının nasıl yapılacağı).
8-	Yönetim Kurulu Kararına Tabi Konular	:YK 'kararı alınması zorunlu olan konuların ve faaliyetler detaylı olarak tanımlanarak ortaya koyulur. YK'nun şirketi temsil esasları düzenlenerek ortaya koyulur.
9-	Denetim Komitesi	:Denetim Komitesinin oluşturulma ve çalıştırılması ile ilgili esaslar düzenlenir.
10-	Olağan ve olağan üstü genel kurul ve kararlarına ilişin düzenlemeler ortaya koyulur.	
11-	Şirket hesap dönemi tanımlanarak ortaya koyulur	
12-	Karın hesaplanma ve dağıtılma esas ve prensipleri düzenlenir ve ortaya koyulur.	

Şirketin imza sirkülerinde YK kararına uygun olarak şirketin temsil ve ilzamı ile ilgili esasları düzenlemektedir. İmza sirküleri, imza yetkisi sahibi kişiler, imza yetkilerine konu faaliyetler ve yetkilerin sınırlarının detaylı olarak tarif edilip özellikle 3. kişi ve kurumlar açısından ortaya koyulduğu dökümandır. Ticaret Sicilini takiben hüküm doğurur.

3.2.2.1.3. İç Yetki Onay Tablosu

Ana sözleşme ve imza sirküleri YK yetkileri ve başta 3. kişi ve kurumlara karşı şirketin temsil esaslarını düzenlemekle birlikte **iç yetki/onay tablosu,** şirketin tanımlı tüm iş süreçleri ile ilgili gerek 3. kişi ve kurumlara karşı gerekse organizasyon içinde ihtiyaç duyulan tüm onay mekanizmalarının nasıl çalışacağı, YK, üst yönetim, fonksiyon amirleri ve ilk amirlerin yetki düzeyi ve bunun iletişim esaslarının belirlendiği dökümandır. İç kontrolün gelişimi ve üst yönetim beklentilerine uygun işletilmesi, YK ve üst yönetim onay ve yetki kurgusunun net bir şekilde ortaya koyulması ve ekiple iletişimi açısından çok önemlidir.

İç yetki/onay tablosu şirketin vizyon ve misyonundan başlamak üzere sürdüreceği faaliyetlerle ilgili olarak organizasyon yapısında yer alan ana fonksiyon amirlikleri (örneğimizde yöneticilikler) altlarında yer alan yardımcı fonksiyon amirlikleri (örneğimizde müdürlükler) ile ilgili süreçlerde bütçe dahili ve harici kırılımı ışığında gerekli onay mekanizmasının ve kurum içi bilgi akışının nasıl işletileceğini detaylı biçimde ortaya koyar.

Örneğimizde, Tedarik Kanalları Yöneticiliği altında verilen "satın alma kararları" ile ilgili bölüm Tablo 3.4'te detaylandırılmış, "makine ve ekipman alımları" kısmının yetki ve iletişim akışı belirtilmiş, diğer fonksiyonlarla ilgili çerçeveye yer verilmiştir.

Görüleceği gibi iç yetki onay belgesi başta YK olmak üzere üst yönetimin kurum faaliyetleri ve süreç işleyişleri ile ilgili işletmek istediği onay mekanizması ve kurguladığı bilgi akışının yönünü detaylı biçimde ortaya koyar, kurum çalışanları ile iletişimine olanak tanır.

Tablo 3.4: ABC Kimya San. A.Ş. İç Yetki Onay Belgesi Kesit Örneği

ÖRNEK İÇ YETKİ ONAY KESİTİ

Fonksiyon ve Durum Tarifleri	Yönetim Kurulu	Genel Müdür	Mali İşler Direktörlüğü	Tedarik Kanalları Direktörlüğü	Satış Pazarlama Direktörlüğü	Üretim Direktörlüğü	Ar-Ge Direktörlüğü	İnsan Kaynakları Direktörlüğü	IT Direktörlüğü	İlgili Müdürlük	İlgili Uzmanlık
I. ŞİRKET VİZYON VE MİSYONU	*O*	*TT*									
II. ŞİRKET POLİTİKA VE STRATEJİLERİ	*O*	*TT*									
III. TEDARİK KANALI FONKSİYONLARI											
A) Satın Alma Kararları											
1. Sabit Kıymet Alımları											
a-Makine Ekipman											
a.1.Bütçe Dahili											
-1 mio TL ve üstü	*O*	*ÖO*	*ÖB-K*	*ÖB-K*						*H(SA)*	
- 250 bin - 1 mio TL		*O*	*ÖO*	*ÖB-K*						*H(SA)*	
- 50 bin - 250 bin TL		*B*	*B*	*O*						*H(SA)*	
- 50 bin TL altı		*B*	*B*	*B*						*O (SA)*	
a.2. Bütçe Harici											
- 250 bin TL üstü	*O*	*ÖO*	*ÖB-K*	*ÖB-K*						*H(SA)*	
- 50 bin 250 bin TL arası		*O*	*ÖO*	*ÖB-K*						*H(SA)*	
- 10 bin TL 50 bin TL arası		*B*	*B*	*O*						*H(SA)*	
- 10 bin TL altı		*B*	*B*	*B*						*O (SA)*	
b- Demirbaş											
c- Nakil Vasıtası											
d- Bilgi Sistemleri Yazılım Donanım											
2. Hammadde Alımları											
3. Ambalaj Malz. Ve Yardımcı Malzeme Alımları											
4. Ticari Mamul Alımı											
5. Hizmet Alımları											
IV. ÜRETİM FONKSİYONLARI											
V. AR-GE FONKSİYONLARI											

Kısaltmalar

O	Onay
ÖO	Ön Onay
B	Bilgi
ÖB	Ön Bilgi
TT	Tavsiye
K	Kontrol
H	Hazırlık
YP	Yatırım Planlama
İK	İnsan Kaynakları
Mİ	Mali İşler
Muh	Muhasebe
AG	Ar-ge
KK	Kalite Kontrol
SA	Satınalma
ÜP	Üretim Planlama

3.2.2.1.4. Denetim ve Risk Komiteleri

Dünyada **Denetim Komitesinin** oluşturulması ile ilgili genel anlamda bir zorunluluk olmamakla birlikte bu komitenin oluşturulması ve iyi çalıştırılması durumunda iç kontrol sisteminin geliştiği gözlenmektedir. İyi uygulamalar incelendiğinde komitenin ağırlıklı olarak bağımsız YK üyelerinden oluşturulduğu görülebilir. Bizim örneğimizde bu genel davranışa uygun olarak denetim komitemizi bir bağımsız YK üyesi, bir ilişkili YK üyesinden oluşturulmuş olup, kurumun Denetim Komitesinden temel beklentileri şöyle belirlenmiştir; iç ve dış denetim fonksiyonlarının etkili bir şekilde çalıştırılması, etkili bir iç kontrol sisteminin çalıştırılması, mali tabloların genel kabul görmüş muhasebe ilkeleri çerçevesinde doğru bir şekilde hazırlanıp sunulmasının sağlanması, ABC-KRY Sistemi için Üst

Yönetim Desteğinin alınması. Denetim Komitesi görev ve sorumlulukları, "Denetimden Sorumlu Komite Görev ve Çalışma Esasları" adı altında ortaya koyularak dökümante edilmiştir.

TTK Md. 378 GEREKÇE' sinde ifade edildiği üzere; **Risk Komitesi**, YK üyelerinden veya tamamen üçüncü kişilerden kurulabilir. Komitenin bağımsız bir YK üyesi başkanlığında çalışması tavsiye edilmektedir ve komite iki ayda bir risklerin erken teşhisi ile ilgili YK' na rapor vermekle görevlidir. Bu komitenin denetim komitesinden farkı, denetim komitesi yönetimi gözetim altında tutmasına karşılık bu komite sadece riske odaklanır. Denetim geçmişe yönelik bir faaliyet olmakla birlikte risklerin teşhisi gelecek ve geleceğin yorumu ile ilgilidir ve yönetilmelidir.

Örneğimizde risk komitesi bir bağımsız YK üyesi, bir ilişkili YK üyesinden oluşturulmuş, komite başkanlığı bağımsız YK üyesine verilmiştir.

3.2.2.1.5. Kurum Vizyon ve Misyonu

Kurumun vizyon, misyon ve stratejik hedefleri pazar, rekabet, teknoloji, iş modelleri, tüketici ihtiyaçları, politik ve çevresel faktör değişimleri değerlendirilerek gözden geçirilmiş ve aşağıdaki gibi güncellenmiştir.

Kurumun vizyonu; "Markaları ve ürünleri için karlı ve sürdürülebilir iş modelleri hayata geçirerek tüketicilerimizin, müşterilerimizin, çalışanlarımızın ve hissedarlarımızın ekonomik beklentilerini her zaman karşılayan bölgesinin lider kimya şirketi olmak. " biçiminde güncellenmiştir.

Kurumun misyonu; "Tüketicilere fiyat –fayda dengesi cazip ürünler ve hizmetler sunarken sınıfının en iyi hizmetini sağlayıp müşterilerimizle güçlü ortaklıklar kuracağız. Sürdürülebilir ve istikrarlı kazançlar sağlarken çalışanlarımızın, tüketicilerimizin, toplumumuzun sağlığına itibar edeceğiz,

kurumsal sosyal sorumluluk yükümlülüklerimizi yerine getiren ve çevreye saygılı bir şirket olarak faaliyet göstereceğiz.” şeklinde güncellenmiştir.

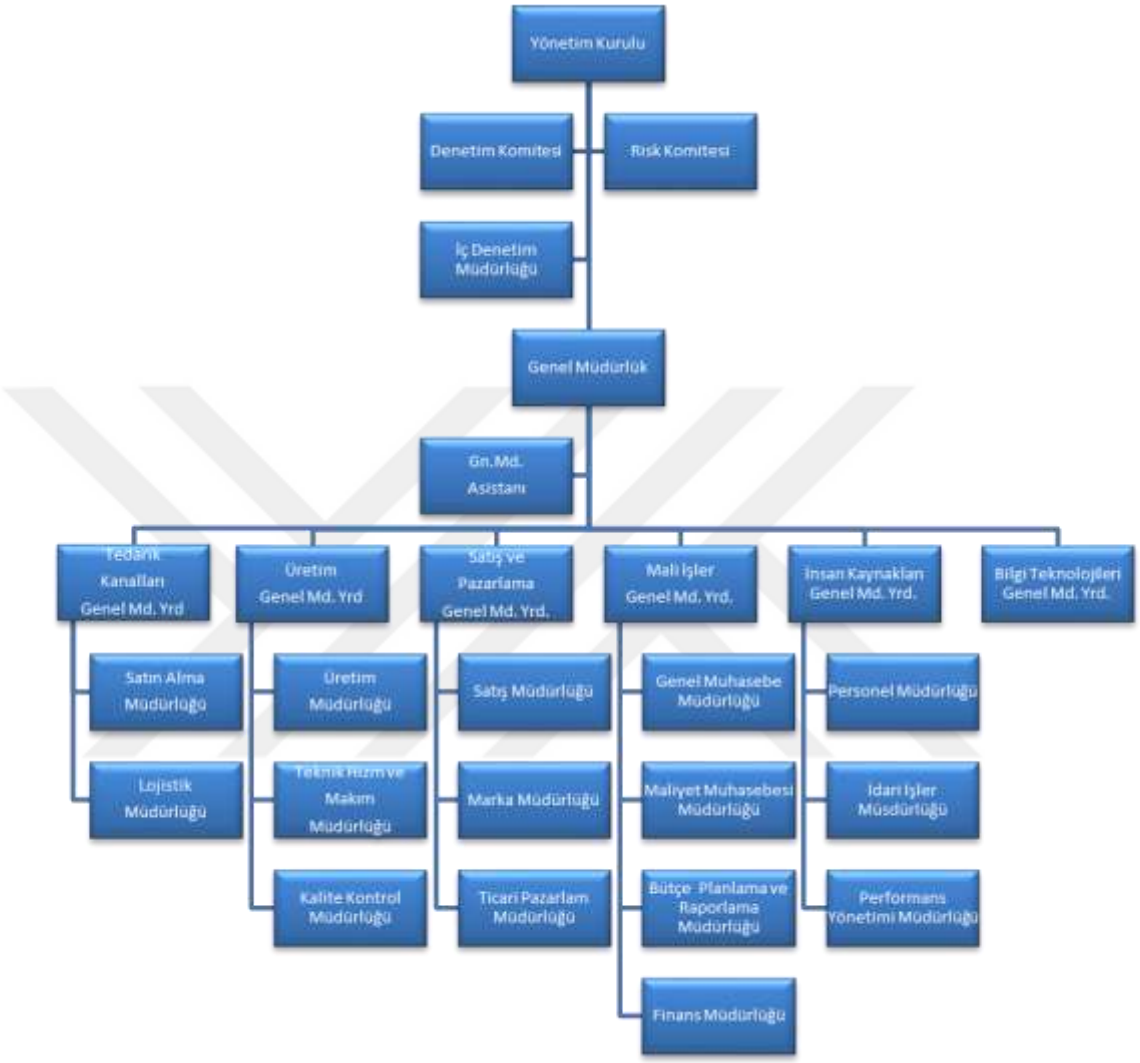
Kurumun vizyon ve misyonuna hizmet edecek **stratejik hedeflerinin** belirlenmesi ve/veya güncellenmesi gerekmektedir. ABC Kimya stratejik hedeflerin bir kısmı şöyle örneklenebilir; takip eden 7 yıl içinde Türkiye ev temizlik kimyasalları pazarının tüm segmentlerinde var olmak ve ilk 2 öncü segmentinde (ciro payı olarak ilk 2 segment) pazar lideri olmak, üretim teknolojileri ile ilgili öncelikli olarak liderlik hedeflenen segmentlerle ilgili olmak üzere üretim hatlarını en yeni teknolojiye sahip olacak biçimde yenilemek, fason üretimimizin ciromuz içindeki payını %50 oranında azaltarak bu üretim kapasitesini markalı ürünler için kullanmak, ilgili kategorilerinde pazar lideri olan markaların sayısını 2 kat arttırmak, stratejik ortaklık veya satın almalarla mevcut ölçeği en az bir kat daha arttıracak büyüme fırsatlarını değerlendirmek, kurum hisselerinin belli bölümünü halka arz yolu ile finansman alternatifi yaratmak için önümüzdeki 5 yıl içinde kurum organizasyon ve işleyişini SPK Kurumsal Yönetim İlkelerinde yer verilen düzenleme ve standartlara uygun hale getirmek.

3.2.2.1.6. Kurum Organizasyon Yapısı

Kurum hedeflerini gerçekleştirmek için tasarlanan süreçler, planlamalar, iş akışları, organizasyonun dikey ve yatay yapısı , merkezi veya merkezkaç yönetim anlayışı, kurum değerler seti ile ilgili yürütülen iletişim biçimi ABC- KRY sistemini destekler nitelikte olmalıdır.

Örnek çalışma için tasarlanan organizasyon şeması Şekil 3.2’de gösterilmektedir.

Şekil 3.2: ABC Kimya San. A.Ş. Organizasyon Şeması



3.2.2.1.7. İş Akışları

İş akışları ile ilgili; Tablo 3.5' de mal ve hizmet satın alması, Tablo 3.6' da üretim planlaması ve üretim süreci, Tablo 3.7'de satış, sevkiyat ve faturalama süreci, Tablo 3.8'de ödemeler süreci konularındaki akışlar örnek olarak detaylı verilmiştir. Örnekleri verilen aşağıdaki iş akışları kurumda hammadde alımından bunların üretimine, mamul satış ve sevkiyatından faturalamaya ve cari hesapların ödenmesine olmak üzere faaliyetin ana konularını kapsamaktadır. Kurum iş süreçleri ile ilgili diğer iş akışları örneklemeye uygun olarak yapılmıştır.

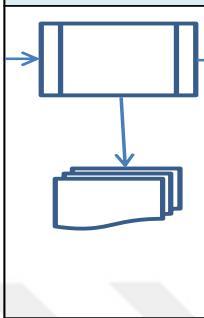
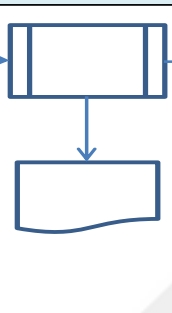
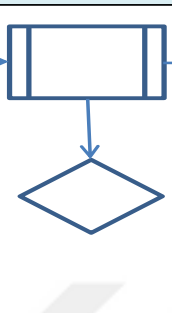
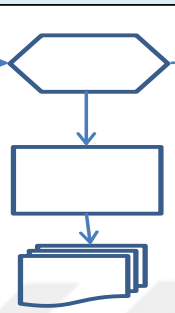
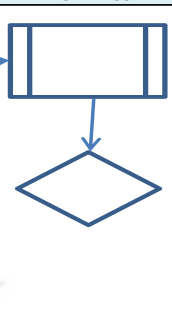
Tablo 3.5: ABC Kimya San. A.Ş. Mal ve Hizmet Satın Alma İş Akışı

MAL/HİZMET SATIN ALMASI İŞ AKIŞI

İş Akışı	İlgili müdürlük tarafından mal/hizmet talebinin planlanması ve talep formunun hazırlanması	Mal/hizmet talep formunun gerekli onayları alınarak Satın Alma Müdürlüğüne iletilmesi	İlgili birim tarafından planlanmış ve onayları alınmış mal/hizmet talep formunun kabulü	Mal, hizmet ikamelerinin, alternatiflerinin, potansiyel tedarikçilerin ve olası çalışma koşullarının araştırılması	Mal hizmet özellikleri ve olası çalışma koşulları konusunda ilgili birim ile mutabakat sağlanması
Sorumlular	Mal/hizmet talebinde bulunan müdürlük	Mal/hizmet talebinde bulunan müdürlük	Satın Alma Müdürlüğü	Satın Alma Müdürlüğü	Satın Alma Müdürlüğü
Süre					

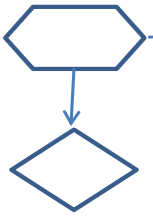
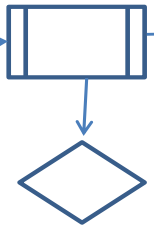
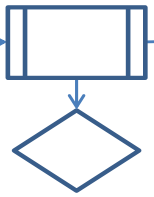
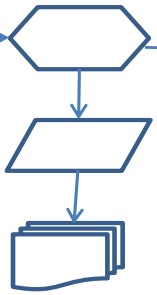
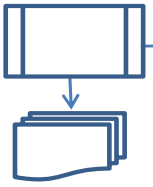
Proforma siparişin hazırlanması ve bütçe uygunluğunun kontrol edilerek gerekli onayların alınması	Sözleşme ve/veya tedarik koşulları görüşmelerinin yapılması	Pazarlıkların sonlandırılması ve siparişin verilmesi	Dökümantasyon	Sevkiyatın gerçekleştirilmesi
- Satın Alma Müdürlüğü -Bütçe Planlama ve Raporlama Müdürlüğü	Satın Alma Müdürlüğü	Satın Alma Müdürlüğü	Satın Alma Müdürlüğü	Lojistik Müdürlüğü

Tablo 3.5: ABC Kimya San. A.Ş. Mal ve Hizmet Satın Alma İş Akışı (Devamı)

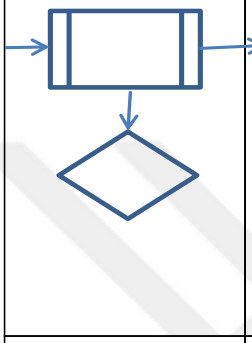
Depoya gelen malın miktar kontrolü siparişle karşılaştırılarak gerekli dökümantasyonun hazırlanması	Gelen malın kalite kontrolü ve belirlenmiş spektlerle karşılaştırılarak gerekli dökümantasyonun hazırlanması	Mal kabulü, reddi	Alınan hizmet ise hak edişinin hesaplanması ve dökümantasyonu	Sipariş ile ilgili gelen faturanın mal kabul, fiyat, miktar ve/veya hak ediş, ödeme vadesi kontrolü ve fatura kabulü için muhasebeye gerekli onayların verilmesi
				
Lojistik Müdürlüğü	Kalite Kontrol Müdürlüğü	Lojistik Müdürlüğü	Satın Alma Müdürlüğü	Satın Alma Müdürlüğü

Tablo 3.6: ABC Kimya San. A.Ş. Üretim Planlaması ve Üretim İş Akışı

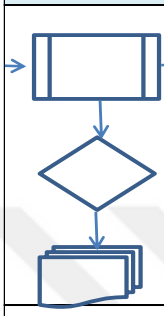
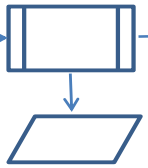
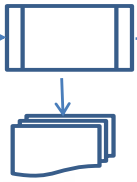
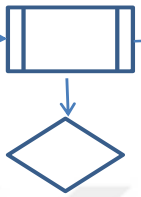
ÜRETİM PLANLAMASI VE ÜRETİM SÜRECİ İŞ AKIŞI

İş Akışı	Aylık satış öngörüleri satış bütçesi ile değerlendirilip ayın son haftası takip eden ay için satış hedefleri güncellenir.	Güncellenen satış hedeflerinden hareketle ilgili ay için üretim planı revize edilir	Güncellenen üretim planından hareketle oluşacak hm-ambalaj sarfiyatı hesaplanır	Aylık ihtiyaç değerlendirilerek üretimin talep edeceği yaklaşık miktarlar hesaplanır ve bunların talep formları hazırlanır	Hm-Ambalaj talep formları üretim programına uygun olarak Hm-Ambalaj Depoya iletilir
					
Sorumlular	Satış Pazarlama Müdürlüğü	Üretim Müdürlüğü	Üretim Müdürlüğü	Üretim Müdürlüğü	Üretim Müdürlüğü
Süre					

Tablo 3.6: ABC Kimya San. A.Ş. Üretim Planlaması ve Üretim İş Akışı (Devamı)

HM-Ambalaj üretime sevkiyat planı hazırlanır ve Üretim Müdürlüğü ile mutabık kalınır	Üretim planında yer verilen vardiya planı üzerinden işçilik ihtiyacı belirlenir ve Personel Müdürlüğü ile mutabık kalınır	Güncellenen üretim planı ile tamir bakım planı birlikte değerlendirilir ve tamir bakım planı da güncellenerek üretim planına uygun hale getirilir	Tamir bakım planından hareketle ihtiyaç duyulacak teknik malzeme için talep formları hazırlanır ve teknik malzeme deposuna iletilir	Teknik Malzeme talep formlarından hareketle ilgili ayın teknik malzeme sevkiyat planı yapılır ve Üretim Müdürlüğü ile mutabık kalınır
				
Lojistik Müdürlüğü Üretim Müdürlüğü	Üretim Müdürlüğü Personel Müdürlüğü	Üretim Müdürlüğü Teknik Hizm. Ve Bakım Mdl.	Teknik Hizm. Ve Bakım Mdl.	Lojistik Müdürlüğü

Tablo 3.6: ABC Kimya San. A.Ş. Üretim Planlaması ve Üretim İş Akışı (Devamı)

Teknik depo satok politikasına uygun olarak teknik malzeme talep formları hazırlanır ve onayları alınarak Satın alma Müdürlüğüne iletilir	Güncellenen üretim planı hakkında ilgili müdürlükler bilgilendirilir.	İlgili günleri, üretim hatlarını,ürün dönüşümlerini, vardiyaları, işçilik desenlerini, planlı duruşları içeren üretim emirleri hazırlanır ve vardiya amirleri ile paylaşılır	İlgili hatlarda üretim başlatılır	Üretilen mamulün kalite kontrolü yapılır	Kalite Kontrol onayını alan ürünler Mamul Depo'ya teslim edilir
					
Lojistik Müdürlüğü	Üretim Müdürlüğü	Üretim Müdürlüğü	Üretim Müdürlüğü	Kalite Kontrol Müdürlüğü	Üretim Müdürlüğü

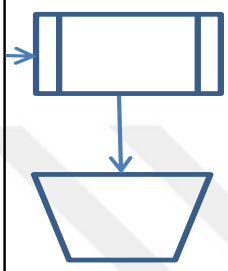
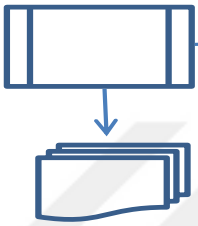
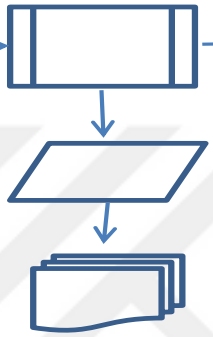
Tablo 3.7: ABC Kimya San. A.Ş. Satış-Sevkiyat-Faturalama İş Akışı

SATIŞ-SEVKİYAT-FATURALAMA İŞ AKIŞI

İş Akışı	Distribütör ve/veya perakende noktası siparişini oluşturur, sitem üzerinden sipariş şirketimizin Satış Müdürlüğü ekranına düşer. Satış Müdürlüğü siparişi onayladıktan sonra onaylı sipariş Lojistik Müdürlüğü sevkiyat planlama ekranına düşer	Sevkiyat güzergah planı (rut planı) ve kamyonlaştırma (parsiyel yüklemeye konu siparişlerin bir araya getirilerek kamyon dolduracak biçimde yükleme planı) yapılır	Kamyonlaştırılan siparişler için sistemden nakliye numarası alınır ve bu numara mamul depo ekranına ve nakliye firması ekranına iş emri olarak düşer.	Mamul depo günlük sevkiyata konu iş emirleri oluşur, sevkiyat planı yapılır
Sorumlular	Satış Müdürlüğü	Lojistik Müdürlüğü	Lojistik Müdürlüğü	Lojistik Müdürlüğü
Süre				

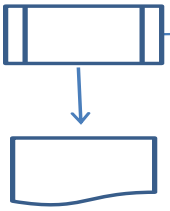
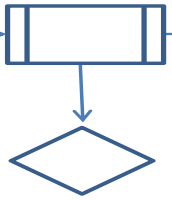
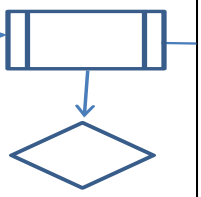
Mamul depo nakliye firmasından yüklemeler için araç talebinde bulunur	Nakliye firması daha evvel gördüğü nakliye numaraların dayanarak taslak sevkiyat planı yapmış ve hazırlıklarını tamamlamıştır	Araç talebi sonrasında araç mamul depoya gelir. Araç üzerinde nakliye numarası olan nakliye belgesini mamul depoya verir ve yükleme sırası alır	Aracın sırası gelince mamul depo sistem üzerinden ilgili nakliye numarası bilgisi ile yükleme emri verir	Yükleme emri forkliflerin ekranına "mamul toplama emri" olarak düşer ve forkliftler ilgili mamulleri toplama alanında yüklemeye hazır eder
Lojistik Müdürlüğü	Lojistik Müdürlüğü	Lojistik Müdürlüğü	Lojistik Müdürlüğü	Lojistik Müdürlüğü

Tablo 3.7: ABC Kimya San. A.Ş. Satış-Sevkiyat-Faturalama İş Akışı (Devamı)

İlgili nakliye numarasına ait yükleme tamamlanır ve iş emri kapatılır	Kapatılan iş emirleri için sistem irsaliye keser	İrsaliyeler sistem üzerinde sevkiyat miktarları ve yine sistemde kayıtlı fiyat ve çalışma koşulları referans alınarak faturalaştırılır	Faturalaştırılan kayıtlar müşteri cari hesaplarına akar
			
Lojistik Müdürlüğü	Lojistik Müdürlüğü	Muhasebe Müdürlüğü	Muhasebe Müdürlüğü

Tablo 3.8: ABC Kimya San. A.Ş. Ödemeler İş Akışı

ÖDEMELER İŞ AKIŞI

İş Akışı	Cari hesaplar bakiyeleri alış ve satış faturalarının muhasebeleştirilmesi ve ödeme talimatlarının işleme koyulması ile sistem üzerinde oluşmaktadır.	Cari hesap bakiye ve vadelerinden hareketle taslak ödeme listeleri hazırlanır	Ödeme listeleri ilgili banka bakiyeleri ile değerlendirlerek ödeme planları yapılır	Ödeme planı ödeme emirlerine dönüştürülerek gerekli onaylar alınır
				
Sorumlular	Muhasebe Müdürlüğü Finans Müdürlüğü	Finans Müdürlüğü	Finans Müdürlüğü	Finans Müdürlüğü Mali İşler Direktörlüğü
Süre				

Ödeme emirleri uygulanarak bankalara gönderilir	Cari hesap bakiyeleri sistem üzerinde otomatik olarak değişir	İlgili tedarikçilerle ödeme bilgileri paylaşılır	Mutabakat talimatına uygun olarak banka mutabakatları ve cari hesap mutabakatlar yapılır
			
Finans Müdürlüğü	Finans Müdürlüğü	Finans Müdürlüğü	Finans Müdürlüğü Muhasebe Müdürlüğü

3.2.2.1.8. Politika ve Prosedürler

İş akışlarının yan ısıra, iş süreçlerinde iç yetki onay prosedürü ile tarif edilen onay mekanizması ve iletişimin çalıştırılma biçimleri yerine getirilirken kullanılacak kurum politikaları, prosedürler, formlar aşağıda belirtilmiş olup bunların önde gelenleri çalışmamız için detaylı olarak örneklenmiştir.

Kurum içi, dışı temsil, yetkilendirme ve sorumluluk ile ilgili dökümanlar ve içerikleri Tablo 3.9'da belirtilmiştir.

Tablo 3.9: ABC Kimya San. A.Ş. Kurum İçi-Dışı Yetki ve Sorumluluk Evrakları

Anasözleşme	Kurumun kuruluş esasları, faaliyeti, adresi, sermayesi, ortaklık yapısı, süresi, yönetim kurulu, denetimi, kar hesaplaması ve dağıtımı düzenlemeleridir.
Yönetim Kurulu (YK)Kararları	Yönetim Kurulu'nun aldığı kararların yazıldığı ve YK üyelerinin imzalarını taşıyan dökümanlardır.
İmza Sirküleri	Kurumun 3. kişi ve kuruluşlar başta olmak üzere dış dünya ve resmi kanallarda nasıl temsil edileceğini, temsil yetkilerinnin dağıulımı ve tarifinin yapıldığı belgedir.
Vekaletnameler	Ana sözleşme ile ve/veya imza sirküleri ile düzenlenmiş yetkilerin kurum içinde devri ile ilgili belgelerdir.
İç Yetki Onay Tablosu	Kurum iş süreçleri ile ilgili yetki, onay mekanizması ve bilgi akışının düzenlendiği belgedir.
Bilgi Sistemleri Yetki Matrisi	Bilgi sistemlerine erişim, kullanıcı yetkilendirmeleri ve yetki düzeylerinin düzenlendiği belgedir.
İş ve süreç akışları	İş tanımları, sorumlular, süreç alkışlarının düzenlendiği belgelerdir.
Politika, prosedür ve bilgi-onay formları	Kurum politika, prosedürlerinin ve süreçlerde kullanılması tasarlanmış bilgi onay formlarının düzenlendiği belgelerdir.

Kurum politikaları kurumun süreç ve faaliyetleri ile ilgili genel ve/veya özel fonksiyonlar veya belirlenmiş genel ve/veya özel durumlar karşısında kurumun benimseyeceği davranış ve yaklaşımları yine kurumun etik değerleri ve çalışma prensiplerine uygun olarak düzenlemektedir. Politikalarla ilgili içerik örneklemesi Tablo 3.10' da gösterilmiş olup, kurumda kullanılan ve/veya kullanılacak politikaların listesi ve her birinin çerçevesi ayrıca Tablo 3.11'de gösterilmektedir.

Yazılı kurum politika ve prosedürlerinde belirlenen standartlar açısından ana başlıklar itibariyle şu kısımlar yer almalıdır; kurum adı, belge cinsi (politika, prosedür), belge kod numarası, politika ana yönetim alanı, konusu, amacı, kapsamı, belgede kullanılan tanımlar, politika sorumluluk dağılımı, politika uygulama esasları, politika güncelleme ve yayınlama esasları.

Tablo 3.10. ABC Kimya San. A.Ş Politika Belgesi İçerik ve Format Örneği

Kurum	ABC Kimya San. A.Ş.
Doküman Türü	Politika
Kod No	28/DBF - 03
Ana Yönetim Alanı	Bilgi Sistemleri
Konu	Mobil Cihaz Kullanımı

I. AMAÇ

ABC Kimya San. A.Ş. ve bağlı çalışanlarının, mobil çalışma cihazlarının kullanımı ve mobil çalışma sırasında kurumsal kurumsal bilgi varlıklarının bütünlük ve gizliliklerinin güvenliğini sağlamak.

II.KAPSAM

…. Kurumu kaynak ve sistemlerine erişim için mobil cihaz kullanan tüm kurum ve kişiler

III. TANIMLAR

Akıllı telefon: Üzerinde işletim sistemi bulunan ve üzerinde çok sayıda uygulamayı çalıştırabilen protatif iletişim cihazları

IV. SORUMLULUK DAĞILIMI

Faaliyet	Sorumlu
Politika ve prosedürleri hazırlama ve güncelleme	Bilgi Teknolojileri Müdürlüğü
Mobil cihazların ilgili politikaya uygun kullanımı	Mobilcihaz kullanıcıları
Mobil cihazların kaybolması ve/veya çalınması durumunda cihazın kapatılması	Bilgi Teknolojileri Müdürlüğü

V. UYGULAMA ESASLARI

1. Kuruma ait mobil cihazların şirket dışında kullanılması sırasında kurumun Bilgi Güvenliği politika ve prosedürlerine uyulmalıdır.
2. Mobil cihazlar sadece iş gereği ihtiyacı olan çalışanlar için temin edilmeli ve yetkilendirilen amaçlar dahilinde kullanılmalıdır.
3. Mobil cihazlarda mümkün olduğunca gizlilik derecesi yüksek ve hassas veriler bulundurul-mamalı, üzerinde bilgi tutulması için onay alınmışsa bilgilerin yedeğinin alınması sağlan-malıdır.
4. Mobil cihaz kullanımı sırasında internet erişimi sağlamak için güvenli olmayan servis sağlayıcılar ve sunucular kullanılmamalıdır.
5. İzin verilen mobil cihazlar üzerinde e-posta iletişimi için sadece kurumsal sunucular kullanılmalıdır.
6. Kurum dışında kullanım için çıkarılan cihazların iş gereği kullanım ihtiyacı kalmayınca mobil cihazlar kuruma en kısa sürede iade edilmelidir.
7. Kurumsal sistemlere erişim için kullanılan mobil cihazlara Bilgi Teknolojileri Müdürlüğü bilgi ve onayı olmadan program yüklenmemeli ve çalıştırılmamalıdır.
8. Mobil cihazların kaybolması veya çalınması halinde durum derhal yerel güvenlik birimine ve kurum Bilgi Teknolojileri Yardım Masasına bildirilmelidir.

VI. GÜNCELLEME VE YAYINLAMA ESASLARI

1. Bu politikanın uygulanmasından, kontrol ve takibinden Bilgi Teknolojileri Müdürlüğü ve kurum Genel Müdürü sorumludur.
2. Bu prosedür yayınlandığı tarihten itibaren yürürlüğe girer.

İmza

…….

Revizyon tarihi	
Revizyon No	
Revizyon Sebebi	

Tablo 3.11: ABC Kimya San. A.Ş. Kurum Politikaları ve Genel Çerçeveleri

Kurum Politikaları ve Genel Çerçeveleri	
Genel Satın Alma Politikası	Kurumun satın alma fonksiyonu ile ilgili genel politikasını düzenlemektedir.
Tedarikçi Seçim Politikası	Kurumun tedarikçi seçim kriterleri, akreditasyon için uygulamaları, konu ile ilgili işletilecek onay ve bilgilendirme biçimleri düzenlenmektedir.
Mutabakat Politikası	Kurumun varlık ve değer hareketleri sonucu oluşan bakiyeler ve kıymet pozisyonları ile ilgili kaydi ve fiziki mutabakat prensiplerini ve uygulamalarını düzenlemektedir.
Alacak Riski ve Teminat Yapısı Politikası	Kurumun müşterilerinden oluşan alacakları ile ilgili risk ve teminat algısı ile prensip ve uygulamalarını düzenlemektedir.
Stok Yönetimi Politikası	Kurumun stok yönetimi ile ilgili prensip ve uygulamalarını düzenlemektedir.
Muhasebe Kayıt Prensipler	Genel prensip olarak yürürlükteki ilgili müfredatlara uymak esas olmakla birlikte özellikle müfredatın kurumlara seçenekler ve değerlendirme imkanları sunduğu alanlarda muhasebe kayıtları açısından kurum tercihlerini, prensip ve uygulamalarını düzenler.
Maliyet Merkezi Hiyerarşisi ve Maliyet Dağıtım Anahtarları	Kurumun maliyet merkezi hiyerarşisi ve maliyet dağıtım anahtarları ile ilgili prensip ve tercihlerini ortaya koyup uygulama esaslarını düzenler. Maliyet merkezi hiyerarşisi ve dağıtım anahtarlarının üst yönetimin onay ve gözetiminde tasarlanması ve değişikliklik ihtiyaçlarında bunun üst yünetimin bilgi ve onayı doğrultusunda yapılması maliyetlerin doğru okunması ve dönemsel karşılaştırmalar için hayatidir.
Kur Riski Politikası	Kurumun kur riski algısını ve bunun yönetilmesi konsunda tercih ve prensiplerini düzenlemektedir.
Nakit Yönetimi Politikası	Kurumun nakit ve nakit benzeri varlıkları ile ilgili prensip ve uygulama esaslarını düzenlemektedir.
Şirket Bütçe Standarları	Kurumun bütçe süreci, genel değerlendirmeleri ve bir yönetim anlayışı olarak bütçe uygulamaları ile ilgili prensiplerini düzenlemektedir.
Mali İşler Rapor Envanteri ve Dağıtım Listesi	Kurumun Mali İşler Direktörlüğünün üretmesi beklenen raporlar, genel çerçevesi, yayın ve dağıtımı ile ilgili prensipleri ve uygulamayı düzenlemektedir.
Bilgi Sistemleri Güvenliği ve Veri Gizliliği Politikası	Kurumun Bilgi Sitemleri güvenliği ve veri gizliliği konusundaki prensip ve uygulamalarını düzenler.

ABC-KRY sistemini desteklemek açısından kurum içi uygulanan ve/veya uygulanacak olan politikalarla ilgili doküman özelinde ve genel çerçeve kapsamında yeterli, sayıda örnekleme yapıldığı değerlendirilerek, kurumda ABC-KRY sistemi kapsamında uygulanan ve/veya uygulanacak olan diğer politikaların, prosedürlerin ve bilgi onay formlarının listesi Tablo 3.12'de isimleri itibariyle belirtilmektedir.

Tablo 3.12: ABC Kimya San. A.Ş. Politikalar-Prosedürler –Onay Formları Listesi

Politikalar	Prosedürler	Bilgi-Onay Formları
Genel satın alma politikası	Tedarikçi akreditasyonu prosedürü	Mal/hizmet talep formu
Tedarikçi seçim politikası	İhale prosedürü	Ana veri değişiklik formu
HM-Ambalaj alım politikası	Sözleşme prosedürü	*-yeni ürün*
Sabit kıymet alım politikası	Siparişle satın alma prosedürü	*-tedarikçi, müşteri*
Teknik malzeme alım politikası	HM-ambalaj mal kabul prosedürü	*-cari hesap*
Hizmet alım politikası	Hizmet kabul prosedürü	*- banka hesabı*
Mutabakat politikası	Fatura kabul prosedürü	*-fiyat listesi*
** Kaydi mutabakat*	Stok mutabakatı prosedürü	*- çalışma koşulu vb..*
** Fiziksel mutabakat*	Cari hesap mutabakatı prosedürü	*- reçete*
Hasarlı ürün politikası	Banka mutabakatı prosedürü	Mal imha talep/onay formu
Alacak riski ve teminat politikası	Stok sayım prosedürü	Aktivite talep/onay formu
Sigorta poliçesi politikası	Hasarlı ürün satış prosedürü	Mal kabul formu
Fiyat ve marj politikası	Ürün imha prosedürü	Sevkiyat talep formu
** düzenli arzı fiyatlama*	Ana veri yönetimi prosedürü	Sipariş formu
** fırsat satışı fiyatlama*	*(Sku, tedarikçi, cari hesap, banka hesabı,*	Ödeme talimatı
Stok yönetimi politikası	*reçete, sabit kıymet, fiyat listesi, çalışma koşulu*	Ödeme emri
Muhasebe kayıt prensipleri	*müşteri vb.)*	HM-ambalaj talep formu
Maliyet merkezi hiyerarşisi	Ödeme prosedürü	Teknik malzeme talep formu
Maliyet dağıtım anahtarları	Mal kabul-kalite kontrol prosedürü	Teknik hizmet-bakım talep formu
Şirket bütçe standartları	Mamul ambarı mal kabul prosedürü	Üretim talep formu
Rapor envanteri ve dağıtım listesi	Seyahat ve ağırlama prosedürü	Üretim emri
Ana veri yönetimi politikası	Taksi kullanma prosedürü	Havuz araç talep/onay formu
Kur riski politikası	İş masrafı prosedürü	Masraf listesi
Nakit yönetimi politikası	Telefon, bilgisayar tahsis prosedürü	Ambarlar arası teslim -tesellüm formla
Menkul kıymet yatırım politikası	Araç tahsis prosedürü	Hasarlı ürün tutanağı
Sabit kıymet yatırım politikası	Havuz araç kullanma prosedürü	Tedarikçi onay formu
- gayrimenkul	Üretim hattı açma/kapama prosedürü	Personel istek formu
- yenileme	Makine duruş/başlatış prosedürü	Performans hedefleri
- kapasite ve yeni iş	Vardiye başlama/bitiş prosedürü	Ambalaj onay formu
Bilgi /veri gizliliği ve güvenliği politikası	Üretim sahası hijyen kuralları	Yatırım onay formu
Ürün iade politikası	Üretim sahası ziyaretçi prosedürü	Harcama onay formu
Fazla mesai politikası	Üretim sahası kıyafet standartları	Seyahat talep/onay formu
Avans verme politikası	Üretim sahası uyulması gereken güvenlik kuralları	Hm-ambalaj kalite kontrol onay formu
İşçi sağlığı ve güvenliği politikası	Ambarlar arası stok hareketi prosedürü	Üretim kalite kontrol onay formu
Şirket sözcülüğü politikası	İşletme sahası araç giriş-çıkış prosedürü	
Resmi ve idari tatil politikası	İşletme sahası ziyaretçi giriş-çıkış prosedürü	
Ücretli, ücretsiz izin politikası	İşletme sahası çalışan giriş-çıkış prosedürü	
Performans değerlendirme politikası	Performans hedefleri belirleme ve değerlendirme prosedürü	
İşe alım politikası	IT yedekleme ve geri yükleme prosedürü	
İş akti fesih politikası	IT bakım-onarım ve güncelleme prosedürü	
Çalışanlar ücret ve prim politikası	Mobil cihaz kullanımı prosedürü	
Çalışanlar yan haklar politikası	Bilgi sitemleri uzaktan erişim prosedürü	
Borçlanma politikası	İş tanımı hazırlama ve güncelleme prosedürü	
Mobil cihaz kullanımı politikası	İş akışı, süreç tasarımı ve iyileştirme prosedürü	
	Kartvizit basım prosedürü	
	Oda tahsis prosedürü	
	Kredi risk yönetimi yönetmeliği	
	Genel satın alma yönetmeliği	

İsimleri ve genel çerçeveleri belirtilen her bir politika ve prosedürün yukarıda verilmiş detaylı örneğe uygun hazırlanması ve kurum içi iletişimin yapılması sağlanmıştır.

3.2.2.1.9. Etik Değerler

Kurum için "Etik İlkeler Ve Çalışma Prensipleri" kitapçığı oluşturulup ve tüm çalışanlarla iletişiminin yapılması tavsiye edilmektedir. Kurum içi iletişimi sağlamak için; kitapçığın kopya olarak dağıtılması, sunum ve anlatımlarla kitapçık içeriği konusunda çalışanların farkındalığının makul seviyeye getirilmesi, tüm çalışanlardan kitapçığın okunup anlaşılmış olduğunu ifade eden çalışan beyanı alınması ve belli aralıklarla kitapçık içeriğinin çalışanlar nezdinde gözden geçirilmesini sağlayacak toplantılar yapılması planlanmaktadır.

Etik İlkeler Ve Çalışma Prensipleri kitapçığı içeriği ile ilgili genel çerçeve önerisi açısından Tablo 3.13' te örnek içerik verilmiş, örneği güçlendirmek açısından bazı içerik konuları detaylı olarak kaleme alınmıştır.

Tablo 3.13: ABC Kimya San. A.Ş. Etik Değerler Kitapçığı Örnek İçeriği

ABC Kimya San. A.Ş. Etik Değerler Kitapçığı Örnek İçeriği

1- Kurum Yönetim Kurulu Başkanı mektubu

YK'nun çalışanlara seslendiği, konu hakkında düşünce ve görüşlerini ve bakış açısını ortaya koyduğu mektup.

2- Kurumun vizyon ve misyonu

Vizyonumuz: Markaları ve ürünleri için karlı ve sürdürülebilir iş modelleri hayata geçirerek tüketicilerimizin, müşterilerimizin, çalışanlarımızın ve hissedarlarımızın ekonomik beklentilerini her zaman karşılayan bölgesinin lider kimya şirketi olmak.

Misyonumuz: Tüketicilere fiyat –fayda dengesi cazip ürünler ve hizmetler sunarken sınıfının en iyi hizmetini sağlayıp müşterilerimizle güçlü ortaklıklar kuracağız. Sürdürülebilir ve istikrarlı kazançlar sağlarken, çalışanlarımızın, tüketicilerimizin, toplumumuzun sağlığına itibar edeceğiz, kurumsal sosyal sorumluluk yükümlülüklerimizi yerine getiren ve çevreye saygılı bir şirket olarak faaliyet göstereceğiz.

3- Kurumun hissedarlarına, müşterilerine ve çalışanlara taahhütleri ile kurumsal değerleri

Bu kısımda kurumun ilişkili taraflara kurumsal taahhütleri ve kurumsal değerleri açıkça ifade edilir.

Kurumsal Değerlerimiz

Müşteri önceliğimizdir.

Müşterilerimiz ve tüketicilerimizin beklentilerinin karşılanması birinci önceliğimizdir.

Müşterimiz her zaman haklıdır.

Müşteri ilişkilerimizde kazan/kazan ilkesini benimseriz.

Rekabetçiyiz.

Faaliyet alanımızda daima en iyi olmayı hedefleriz.

Çok çalışarak müşterilerimize en iyiyi en önce sunarız.

Takım çalışması esastır.

Bireysel farklılıklara saygı gösterir, aynı hedef için tekbir ekip olarak çalışırız.

Hepimizin başarısı şirketimizin başarısıdır.

Sonuç odaklıyız.

Tablo 3.13: ABC Kimya San. A.Ş. Etik Değerler Kitapçığı Örnek İçeriği (Devamı)

Vizyon ve misyonumuza hizmet eden zorlayıcı hedefler belirleriz.
Performansımızı kendi içimizde ve de rakiplerle kıyaslar, her seferinde daha iyisini hedefleriz.
Yaptığımız işe yüreğimizi koyar, hedeflediğimiz sonucu aşarız.

4- Yasalara uyum ve sorumluluklar
Bu konu hakkında kurumun anlayışı ve beklentisi ifade edilir.

5- İnsan ve çalışan hakları
İnsan hakları, din, dil, ırk, medeni hali cinsiyet, engellilik, yaş ayrımlar çocuk çalışan, fırsat eşitliği, performans değerlendirmede objektif tutum, çalışanlar arasında rekabet koşulları, çalışan aileler dayanışması, mobing vb. konularda kurum anlayışı ifade edilir.

6- Çevre, sağlık ve güvenlik

7- Hissedarlara karşı sorumluluklarımız

8- Politik faaliyetlerimiz

9- Sosyal sorumluluk, gönüllülük, bağışlar

10- Üçüncü kişilere karşı sorumluluklarımız

11- Kamu kurum ve kuruluşları ile ilişkiler
Tedarikçiler ve iş ortakları ile ilişkiler
Müşteriler ve tüketicilerle ilişkiler
Rakiplerle ilişkiler ve rekabet mevzuatına uyum
Medya ile ilişkiler

12- Kurumsal ve kişisel çıkarların ayrımı
Çıkar çatışmasının tanımı
Hediye ve menfaatlerin kabulü ve verilmesi
Çalışanlar tarafından yapılan yatırımlar
Şirketin hisse senetlerinin alım satım politikası
Dışarıda kabul edilen görevler
Çalışanların etkinliklere konuşmacı olarak katılımı
Akrabalar ve arkadaşlar
Temsil ve ağırlama
İçsel bilgi aktarılması

13- Yolsuzluklarla mücadele anlayışımız

14- Şirket varlıklarının korunması ve veri gizliliği
Kurum varlıklarının korunması
Bilgi teknolojisi kaynaklarının kullanımı
Gizli bilgi ve bunların korunması esasları
Fikri mülkiyet hakları
Ürün ve hizmet kalitesi
Süistimal ve usulsüzlük

15- Kayıtlarda ve finansal raporlamada doğruluk
Doğru ve tam kayıt tutma
Gerekli tüm yerlere doğru bilgi ve finansal raporlar sunma

16- Uyum sorumluluğu ve ihlallerin bildirilmesi
Kurumun çalışanlarında etik kurallar ve çalışma prensiplerine uyum konusunda beklentilerini net olarak ifade eder.

Yukarıda, Tablo 3.13'te örneklenen içerik çerçevesinde hazırlanan ve güncellenen bir etik kurallar kitapçığı kurumun vizyon, misyon ve kurumsal

değerlerini sürekli ve güncel biçimde göz önünde tutarken, çalışanların faaliyetleri sırasında karşılaşabilecekleri pek çok konuda kurum açısından geçerli ve benimsenen davranışın ne olacağı ve ne olmayacağı konusunu açıkça ve güncel biçimde ortaya koyacak çalışanların bu çerçevede kurumsal değerlere uygun etmesini kolaylaştıracaktır.

3.2.2.1.10. İnsan Kaynakları Politikaları

İnsan kaynakları politikaları ile ilgili işe alma, işten çıkarma oryantasyon, eğitim, performans değerlendirme, haklar, yan haklar, kariyer planlaması fonksiyonları ile ilgili prensip ve uygulama esasları belirlenirken adaletli olma, şeffaf olma, tarafsız olma, objektif olma, etik değerler ve çalışma prensipleri dökümanı ile ortaya konmuş ve iletişimi yapılan kurumun ahlak anlayışı, kurumsal kültür, kurumsal davranışlara yönelik değer setleri ile uyum içinde olmasına dikkat edilmelidir.

Bu politikalarda bahsedilen unsurların yansıtılmaması ve kurumsal ahlak anlayışı ve etik prensipleri ile ortaya çıkabilecek çelişkiler ABC-KRY sistemi açısından destek olmanın ötesinde zorlayıcı ve engelleyici olacağı unutulmamalıdır.

İhtiyaç duyulan mesleki yeterlilik seviyesinin çalışanlara kazandırılması, İK ile birlikte fonksiyon ve/veya departman amirlerinin dikkatle üzerinde durması gereken bir başka önemli konudur. Organizasyon yapısı, bilgi akışı, iş ve süreç akışlarında kurum beklentileri ortaya koyulduktan sonra bu beklentilerin gerçekleştirilmesi için ihtiyaç duyulan yetkinlik, mesleki yeterlilik ve çalışan profilinin tercihen konusunda uzman bir danışman firma ve İK iş birliği ile değerlendirilmesi ve öncelikle kurumda kritik pozisyonlar için yetkinlik ve mesleki bilgi konusunda ihtiyaçların belirlenmesi, daha sonra mevcut çalışanların yetkinlik ve mesleki yeterliliklerinin değerlendirilerek kritik pozisyonlarda ihtiyaç duyulan mesleki yeterlilik ve yetkinliklere ulaşmak için gerekli planların yapılıp üst

yönetimin mutabakatını almak ve belli bir takvimde bu yetkinlik ve yeterliliklere ulaşmak için gerekli adımları atmak gerekmektedir.

Mesleki yeterlilik ve yetkinlikler açısından stratejilere uygun tasarlanmış iş süreçlerinin ihtiyaçlarının kritik pozisyonlarda karşılanamıyor olması kurum iş sonuçları için önemli bir tehlike oluşturur.

Kurumun **performans değerlendirme sistemi** ABC-KRY gereklilikleri ile uyumlaştırılması gereken bir diğer konudur. Örnek kurumumuzda belli ağırlığı spesifik iş sonuçlarının hedeflenmesi, belli ağırlığı bireysel yetkinliklerin değerlendirilmesine dayalı, bir faaliyet yılı içinde hedef belirleme, ara dönem değerlendirme ve dönem sonu değerlendirme olmak üzere üst amirle çalışanın direkt görüşme yaparak performans hedef değerlendirme formları üzerinde mutabık kaldığı bir performans değerlendirme sistemi yürütülmekte olup sistem bilgi sistemleri üzerinde bir uygulama olarak geliştirilmiş durumdadır.

Performans hedefleri ve üst amir ile birlikte belirlenmekte hedeflerin değerlendirme kriterleri açıkça duyurularak yıl içinde kriterler değiştirilmemektedir .Ara dönem değerlendirmede gidişat karşılıklı tartışılmakta ve geri bildirimler değerlendirilmektedir. Yıl sonu değerlendirmesi sonucu alınan performans notu çalışanın ilgili yıla ait alacağı performans primini doğrudan etkilemekte ve kariyer planlama sistemine işlenmektedir.

Uygulanan performans değerlendirme yöntemi sonucu; performans ile ilgili spesifik iş hedefleri üst amir ve çalışan mutabakatı ile belirlenmekte, departman hedeflerine ve dolayısıyla operasyonel hedeflerine uygun belirlenme olanağı bulunmaktadır, performans sonuçlarının ölçüm kriterleri dönem başında ölçülebilir olarak duyurulmaktadır, ara dönemde verilen geri bildirim ve değerlendirme çalışana diğer dönem için eksikliklerini giderme ve önceliklerini gözden geçirme şansı tanımaktadır, kurum açısından çalışanın performans hedeflerine doğru odaklanmasını tazelemektedir, performans değerlendirme notu çalışanın hem yıl içindeki geliri hem de kariyer gelişimi ile doğrudan

ilişkilendirilmiştir, performans değerlendirmesi belli ağırlıkta spesifik iş hedefleri belli ağırlıkta kurum kültüründe öne çıkan yetkinlikler için yapıldığından çalışan kişisel yetkinliklerini kurum tercihi paralelinde geliştirme konusunda motive edilmektedir.

Kariyer planlama ve takip sistemi, İK politikalarının ABC-KRY gereklilikleri ile uyumlu hale getirilmesi gereken bir başka konusudur. Örnek kurumda, Bilgi Sistemleri İK uygulamaları altında geliştirilmiş bir kariyer planlama ve takip sistemi bulunmaktadır. Bu uygulama ile; çalışan kendisi ile ilgili arzu ettiği kariyer planını, kendisi ile ilgili gelişim alanlarına yönelik kendi değerlendirmesini, eğitim taleplerini kısa, orta ve uzun vade olarak sisteme girer, çalışanın veri girişi ve değerlendirmeleri üst amiri tarafından değerlendirilir ve çalışanla konu hakkında yüz yüze görüşme yapılır, üst amirin bir üst amire iletmek istediği geri bildirimi çalışan taleplerinin de olduğu formlar üzerinde sistem aracılığı ile iletilir, çalışanın performans notu yıllar itibariyle kariyer planlamalarına konu olur, çalışan kariyer plan ve beklentilerini belli bir düzende üst yönetime kadar iletme şansı bulur, aldığı geri bildirimler ve kendi gelişim alanı hakkında yaptığı değerlendirmelerle kariyerine ve gelişim alanlarına odaklanır, performans değerlendirme notunun kariyerine etkisinin farkında olur, kurum ihtiyaçları dikkate alınmak sureti ile çalışanlara yönelik etkin bir kariyer planlama ve takip uygulaması yürütülmüş olur.

Yapılan çalışmalarla örnek kurumumuzda ABC-KRY açısından iç kontrol ortamı ve içsel ortam gözden geçirilerek ABC-KRY sistemini destekler hale getirilmiştir.

3.2.2.2. Strateji ve Hedef Oluşturma

Kurum vizyon ve misyonumuzu ABC-KRY gereksinmelerini ve kurumumuzun maruz kaldığı değişimleri dikkate alarak güncelledikten sonra sıra stratejik hedeflerimizi, bunlara bağlı alt stratejilerimizi, operasyonel hedeflerimizi,

departman hedeflerimizi ve bireysel hedeflerimizi gözden geçirerek bir koordinasyon ve ilişki içinde olacak biçimde güncellemek olmalıdır.

Kurumun vizyon ve misyonuna hizmet edecek **stratejik hedeflerin belirlenmesi ve/veya güncellenmesi gerekmektedir**. Kurum için belirlenen stratejik hedeflerin bir kısmını şu biçimde örnekleyebiliriz; önümüzdeki 5 yıl içinde Türkiye ev temizlik kimyasalları pazarında var olan tüm segmentlerinde yer almak ve ilk 2 öncü segmentinde (ciro payı olarak ilk 2 segment) pazar lideri olmak, üretim teknolojileri ile ilgili öncelikli olarak liderlik hedeflenen segmentlerle ilgili olmak üzere üretim hatlarını en yeni teknolojiye sahip olacak biçimde yenilemek, fason üretimin ciro içindeki payını %50 oranında azaltarak bu üretim kapasitesini markalı ürünler için kullanmak, ilgili kategorilerinde pazar lideri olan markaların sayısını 2 kat arttırmak, stratejik ortaklık veya satın almalarla mevcut ölçeği en az bir kat daha arttıracak büyüme fırsatlarını değerlendirmek.

Stratejik hedeflere ulaşılmasını sağlayacak alt stratejilerin belirlenmesi gereklidir. Yukarıda pazar lideri olmakla ilgili strateji için alt stratejileri örneklemek gerekirse; Türkiye ev temizlik kimyasal maddeleri pazarı için 5 yıllık genişleme senaryolarının çalışılması, tüketici tercih ve trendleri ile ve pazar ihtiyaçları ile ilgili modellemelerin yapılması, kurumun mevcut rekabet avantajlarının sonuca olan etkileri itibariyle değerlendirilmesi, önceliklendirilmesi (hangileri korunacak, hangileri kuvvetlendirilecek, hangileri önemini yitirecek vb.), 5 yıllık sürede pazar lideri olmayı hedeflediğimiz 2 segmentin belirlenmesi, bunların kategorilerinin belirlenmesi, ürün gamına karar verilmesi, liderlik için sahip olunması gereken rekabet avantajlarının analizi, organizasyonel ve iş modeli değişiklik planlarının yapılması, kaynak planlamasının yapılması.

Alt stratejilere hizmet edecek nitelikte dönemsel iş planları (1-3 yıl), yıllık faaliyet bütçeleri ve kurum bütçeleri, burada hedeflenen ekonomik sonuçların alınması için yürütülmesi gereken faaliyetlerin belirlenmesi, **operasyonel hedeflerin saptanması gerekmektedir**. Alt stratejilerden daha detaylı olan operasyonel hedeflere dönemsel iş planları ve yıllık kurum faaliyet bütçeleri örnek gösterilebilir.

Örneğin Lojistik departmanı için yukarıdaki alt stratejilere hizmet edecek bir operasyonel hedefi aşağıdaki gibi örnekleyebiliriz; "Dağıtım hizmetlerinin out-source edilmesi ve depo otomatik sipariş-dağıtım programının devreye alınması ile sipariş karşılama oranını %20 arttırmak, stok dönüş hızını %15 azaltmak ve ürün dağıtım maliyetlerinde birim başına %10 iyileşme sağlamak."

Operasyonel hedeflerin ortaya koyulması için yapılan faaliyet bütçeleri aynı zamanda **departman hedeflerinin çerçevesini belirleyecektir**. Örneğin; "satış pazarlama faaliyeti olarak yürütülen rekabet rafı ve fiyatı izlemek için oluşturulan departman faaliyeti dışarıdan sağlanan hizmet olarak tanımlanması sonucu satış pazarlama maliyetlerinde %15 tasarruf sağlamak".

Bireysel hedeflerin koyulması ve doğru yönetilmesi yukarıda belirtilen strateji, alt strateji, operasyonel hedef ve departman hedeflerinin gerçekleştirilmesi noktasında çok kritik ve belirleyici olup ilk amir, fonksiyonel amir, yönetici ve genel müdür onay hiyerarşisi ile yönetilmelidir. Yukarıda yapılan genel yapıya hizmet eder nitelikte departman hedeflerini gerçekleştirmeye dönük bireysel hedefler fonksiyon amirleri seviyesinde amirler ve ekiplerinin ortak çalışması sonucu belirlenmeli, bunların dengeli olması sağlanmalı, bu hedefler için ihtiyaç duyulacak bilgi, tecrübe ve yetkinlikler değerlendirilerek, organizasyon yapısının yetkinliğinin ihtiyaç duyulan noktaya çıkarılması ve bunun sürdürülmesi çalışmaları yapılmalıdır. Bireysel hedefler adaletli, şeffaf, objektif bir performans değerlendirme sistemi uygulaması ile desteklenerek etkinliği arttırılmalıdır.

Bireysel hedeflerin belirlenmesinde dikkat edilecek konular; "bireysel hedefler departman hedeflerini gerçekleştirmeye yönelik belirlenmeli, ekip çalışanı veya ilgili fonksiyon amiri tarafından önerilmekle birlikte bir mutabakat sonucu oluşmalı (kişi için amiri önerdiyse kişinin mutabakatı aranmalı, kişi kendisi için önerdiyse amirinin mutabakatı olmalı), bireysel hedefler dökümante edilerek, performansın nasıl ölçüleceği hedef belirleme sırasında açık ve mutabakat sağlanmış ölçülebilir parametreler olarak tanımlanmalı, performans sonuçları belli ağırlıkta net ifade edilmiş ölçülebilir hedeflere dayandırılırken, belli ağırlıkta fonksiyon amirinin

kanaati ile değerlendirilecek yetkinliklere dayandırılmalı, izlenen yetkinlikler kurum etik kuralları ve çalışma prensipleri dökümanında ifade edilen kurumsal değerlerle uyumlu olmalı, bireysel hedeflerle ilgili yılda en az bir ara dönem ve bir dönem sonu değerlendirmesi olmalı, performans değerlendirmesi sonuçları kişi ile gerekçeli paylaşılmalı ve kişinin konu hakkında geri bildirimi alınmalıdır. Performans değerlendirme sürecinin ve sonuçlarının kişinin kariyer gelişimi ve maddi kazancı üzerinde çok belirgin etkisinin olması sağlanmalıdır, performans değerlendirme sürecinin şeffaf, anlaşılır, adaletli, objektif bir süreç olarak çalışması sağlanmalı, sürecin çalışanlar üzerinde bir baskı unsurundan ziyade bir teşvik unsuru olarak anlaşılması ve motivasyon aracı olarak kullanılması sağlanmalıdır" şeklinde ifade edilebilir.

Etkili çalıştırılan bir performans değerlendirme sistemi bireysel hedeflerin ana stratejiye uygun, ara strateji ve hedefler açısından sonuca etki yaratma konusunda kritik role sahip olacaktır.

Tablo 3.14'te ABC Kimya'nın belirlenen stratejileri, alt stratejileri, operasyonel hedefleri, departman hedefleri ve bireysel hedefleri ile ilgili hazırlanan dökümandan bir kesit örneklenmektedir.

Tablo 3.14: ABC Kimya San. A.Ş. Strateji ve Hedefleri Örnek Kesiti

Kurum Strateji ve Hedeflerimizin Örneklemesi	
ST: Stratejik hedefler *ALT Alt stratejiler* *Op: Operasyonel Hedefler* *Dp: Departman hedefleri*	Hedef Türü
ST1 Önümüzdeki 5 yıllık sürede Türkiye Kişisel Bakım pazarının tüm segmentlerinde var olmak ve ciro payı olarak ilk 2 segmentin pazar lideri olmak.	Stratejik
ALT1- *Türkiye Kişisel Bakım Pazarı 5 yıllık genişleme senaryoları, tüketici tercih ve trendleri, rekabet pozisyonu projeksiyonu ve Pazar ihtiyaçları ile ilgili liberal, normal ve tutucu olmak üzere 3 ana senaryonun modellenmesi*	Statejik
ALT2- *Kurumun mevcut rekabet avantajlarının analizi ve önceliklendirilmesi (hangileri korunacak, hangileri kuvvetlendirilecek, hangileri önemini yitirecek).*	Stratejik
Op1- *Dağıtım operasyonu ile ilgili olarak mamul deponun 1 yıl içinde out-source edilmesi ve depo otomatik sipariş-dağıtım programının 2 yıl içinde devreye alınması ile sipariş karşılama oranını %20 arttırmak, stok dönüş hızını %15 arttırmak, ürün dağıtım maliyetlerinde m3 başına %10 iyileşme sağlamak.*	Operasyonel
Op2- *Raftan - üretime oluşan değer zincirinde operasyonel maliyetleri %20 azaltılması, yaratılacak fonun reklam harcamalarında kullanılması*	Operasyonel
Dp1- *Perakende raf düzeni ve planogramların izlşenmesi için kullanılan "merchandising"*	Operasyonel
Op3- *Üretim süreçlerinin geliştirlmesi ile fire oranlarında %5 iyileşme sağlamak.*	Operasyonel
. ……	Stratejik
ST2 Başta Pazar lideri olmayı hedeflediğimiz alanlar olmak üzere üretim teknolojilerimizi rekabet avantajı yaratacak biçimde en son teknoloji ile yenilemek	Stratejik
ST3 Fason üretimimizin ciromuz içindeki payınmı %50 oranında azaltarak bu üretim kapasitemizi markalı ürünlerimize tahsis etmek.	Stratejik
ST4 İlgili kategorilerinde Pazar lideri olan markalarımızın sayısını 2 kat arttırmak.	Stratejik
ST5 Stratejik ortaklık veya satın almalarla mevcut ölçeğimizi en az bir kat dah arttıracak inorganik büyüme fırsatlarını değerlendirmek.	

Kurumun için strateji ve hedefler belirlenerek ve /veya güncellenerek, ABC-KRY sistemine uygun biçimde stratejik hedefler, operasyonel hedefler, raporlama hedefleri ve mevzuata uyum hedefleri olarak gruplanmıştır. Tablo 3.14'te örneklenen strateji ve hedefler ile ilgili doküman kesiti ile kurumda ABC-KRY sisteminin "strateji ve hedef oluşturma" bileşeninin nasıl uygulanacağını belirlenmektedir.

3.2.2.3. Performans: Olayların Tanımlanması

COSO İç Kontrol Modeli ve COSO KRYçerçeveleri kuramsal tasarımlarını ortaya koyarken, risk olgusunun firmaya has olduğu, risklerin firmaya özgün olacağı konusuna değinilmişti. Bu aşamada kurumun detaylı risk envanteri oluşturmak için şu akış izlenmektedir; daha önce hazırlanıp yayınlanan ve kurum çalışanlarına eğitimleri verilen kurum Risk Yönetim Felsefesi dökümanı ve dağıtımı proje ekibi ile sınırlı tutulan proje kitapçığındaki terminoloji ve yaklaşımları ışığında proje ekibi ile toplantılar yapılarak bu aşamada neyin hedeflendiği, nasıl

yapılmasının beklendiği anlatılır, sırasıyla strateji, alt strateji, operasyonel hedefler için risk ve fırsat olabilecek durumlarla ilgili tespitleri toplanır. Proje ekibi ve kritik pozisyonlarla beyin fırtınası niteliğinde toplantılar, kritik pozisyonlarla mülakatlar yapılarak bu gerçekleştirilir, proje ekibi üyeleri organizasyon yapısındaki yöneticiler (ana fonksiyon amirleri) olmaları sebebi ile onlardan da kendi ekipleri ile departman hedefleri ve ekip arkadaşlarının bireysel hedefleri için benzer yaklaşımlarla olumlu ve olumsuz durumların tespiti istenir, çalışmaların sonunda kurumun henüz değerlendirilmemiş ve gruplanmamış olmakla birlikte risk envanteri oluşturulur.

Ekip tarafından belirlenen riskler hedeflerle ilişkilendirilirken; ilk aşamada organizasyon iş birimlerine göre oluşturulmuş **risk hiyerarşisi** daha sonra proje grubu tarafından risk türlerine göre gruplanarak kurumun **risk portföyü** ortaya çıkarılır.

Risk değerlendirmesi sırasında, riskleri anlamlı bir bütün oluşturacak biçimde topluca risk haritasında gösterirken risklerin strateji, alt strateji ve organizasyon iş birimlerimizle ilişkisini koparmamak için riskleri tanımlarken basit bir kodlama yapılmaktadır. Örnek: **ST1R1:** 1 numaralı strateji, birinci riski. **ST3ALT2Op2Dp4R2:** 3 numaralı strateji, 2 numaralı alt strateji, 2 numaralı operasyon hedefi, 4 numaralı departman hedefinin ikinci riski.

Tablo 3.15’te kurumun risk envanteri ile ilgili hazırlanan dökümanın bir örnek kesiti verilmektedir.

Tablo 3.15: ABC Kimya San. A.Ş. Risk Envanteri Örnek Kesiti

Kurum Risk Envanteri Kesiti Ve Risk Değerlendirmesi	
ST: Stratejik hedefler *ALT: Alt stratejiler* *Op: Operasyonel Hedefler* *Dp: Departman hedefleri*	Hedef Türü
ST1- Önümüzdeki 5 yıllık sürede Türkiye Ev Temizlik Kimyasalları pazarının tüm segmentlerinde var olmak ve ciro payı olarak ilk 2 segmentin pazar lideri olmak.	Stratejik
ALT1- *Türkiye Ev Temizlik Kimyasalları pazarı 5 yıllık genişleme senaryoları, tüketici tercih ve trendleri, rekabet pozisyonu projeksiyonu ve pazar ihtiyaçları ile ilgili liberal, normal ve tutucu olmak üzere 3 ana senaryonun modellenmesi*	Stratejik
ST1ALT1R1: *Uluslararası bir oyuncunun pazara yeni giriş yapması*	
ST1ALT1R2 *:Rekabet halinde olduğumuz 2 oyuncunun birlikte stratejik ortaklık yapması*	
ST1ALT1R3 *: Çevresel düzenlemelerin ve kampanyaların tüketici tercihlerini radikal biçimde değiştirmesi ve trendin yönünün bugünden belirsiz olması*	
ALT2- *Kurumun mevcut rekabet avantajlarının analizi ve önceliklendirilmesi (hangileri korunacak, hangileri kuvvetlendirilecek, hangileri önemini yitirecek).*	Stratejik

3.2.2.4. Performans: Risklerin Değerlendirilmesi

Risk değerlendirmesi ve risk haritasının oluşturulması sorumluluğu esas itibariyle ABC-KRY proje ekibinde olmakla birlikte bu konuda riskleri belirlerken izlenen yönteme paralel bir yöntem izlenir. Mülakatlar, kesişmeli çalışma grupları, araştırmalar, sektörel karşılaştırmalar ve senaryo analizleri gibi yöntemlerden yararlanarak risklerin belirlenmesinde pay sahibi olan fonksiyon amirleri ve ekipleri bu risklerin gerçekleşme olasılıkları ile ilgili kurum adına belirlenmiş risk değerlendirme kriterlerine uygun olarak geri bildirim verirler. Geri bildirimlerden de yararlanarak risk değerlendirmesi esas itibariyle ABC- KRY proje ekibi tarafından yapılır.

Risk değerlendirme kriterlerinin geliştirilmesi ile ilgili olarak; kurum içi risk değerlendirmelerinin ortak kriterler ve ortak bakış açısı ile değerlendirilmesini sağlamak için risk değerlendirme kriterleri belirlenir ve iletişimi yapılır. Bu sayede kurum risk iştahı, üst yönetim mutabakatı değerlendirme sürecine katılmış olur.

Değerlendirme kriterlerinde riskin sonuçları itibariyle **etkisi** ve riskin gerçekleşme **olasılığı** üzerinde durulmaktadır.

Tablo 3.16' da kurumun risk değerlendirme kriterleri ile ilgili hazırlanan dökümanından bir örnek kesit gösterilmektedir. Tablo 3.17'de kurumun risk olasılıkları aralığı örnek kesiti gösterilmektedir.

Tablo 3.16: ABC Kimya San. A.Ş. Risk Değerlendirme Kriterleri Örnek Kesiti

Kurum Risk **ETKİSİ** Değerlendirme Kriterleri Kesiti		
Seviye	Derece	ETKİ
5	Çok Önemli	Finansal kaybın 1 mio TL ve üstü olması Kurum itibar kaybı ve pazar payı kaybı Çalışanlar ve 3. kişiler için hayati ve/veya sakatlık tehlikesi Yasalarla düzenlenmiş mevzuata uygunsuzluk (gümrük, vergi, iş güvenliği, SGK başta olmak üzere) Hayati tehlike yaratacak kaza ve yaralanmalar ……
4	Önemli	Finansal kaybın 500 binTL - 1 mio TL aralığında olması Kıdemli yöneticilerin işten ayrılması İş davaları Marka itibar kaybı, pazar payı kaybı Yönetmeliklerle düzenlenen mevzuata uygunsuzluk Bilgi sitemleri veri gizliliğinin ve güvenliğinin sağlanamaması Düzeltme imkanı bulunmayan raporlama hataları ……
3	Orta Derecede Önemli	Finansal kaybın 100 bin TL - 500 binTL aralığında olması Düzeltme verilebilen mevzuat uygunsuzlukları Düzeltme imkanı bulunan raporlama hataları Müşteri kaybı Marka imajına zarar verme ihtimali olan gelişme Departmanlarda kritilk çalışanın işten ayrılması Hayati tehlike ve sakatlık tehlikesi taşımayan, dış müdahale gerektirecek kaza ve yaralanma riski Tedarik kanalında tedarikçi rekabetini azaltan gelişmeler ……
2	Düşük Derecede Önemli	Finansal kaybın 30 bin TL- 100 bin TL aralığında olması Moral ve motivasyon kaybı Hayati tehlike ve sakatlık tehlikesi taşımayan, dış müdahale gerektirmeyecek kaza ve yaralanma riski ……
1	Önemsiz	Finansal kaybın 30 bin TL'na kadar olması Ekip çalışan hoşnutsuzluğu riski ……

Tablo 3.17: ABC Kimya San. A.Ş. Risk Olasılığı Aralıkları Örnek Kesiti

Kurum Risk OLASILIĞI Aralıkları		
Seviye	Derece	OLASILIK
5	Çok Yüksek	>%80
4	Yüksek	%60-%80
3	Orta	%30-%59
2	Düşük	%10-%29
1	Çok Düşük	<%10

Kurum risk değerlendirme kriterleri ve risk gerçekleşme olasılıkları ile ile ilgili aralıkların belirlenmesinden sonra belirlenmiş risklerle ilgili değerlendirme yapılır. Strateji ve iş hedefleri ile ilgili bağlantıyı göstermek için bu değerlendirmeler Kurum Risk Envanteri tablosu üzerinde gösterilip daha sonra ayrı bir tabloda toplanmıştır. Tablo 3.18'de kurumun risk değerlendirme tablosu örnek kesiti verilmektedir.

Tablo 3.18: ABC Kimya San. A.Ş. Risk Değerlendirme Tablosu Örnek Kesiti

Kurum Risk Envanteri Kesiti Ve Risk Değerlendirmesi			
ST: Stratejik hedefler *ALT: Alt stratejiler* *Op: Operasyonel Hedefler* *Dp: Departman hedefleri*	Hedef Türü	Olasılık	Etki
ST1- Önümüzdeki 5 yıllık sürede Türkiye Ev Temizlik Kimyasalları pazarının tüm segmentlerinde var olmak ve ciro payı olarak ilk 2 segmentin pazar lideri olmak.	Stratejik		
ALT1- *Türkiye Ev Temizlik Kimyasalları pazarı 5 yıllık genişleme senaryoları, tüketici tercih ve trendleri, rekabet pozisyonu projeksiyonu ve pazar ihtiyaçları ile ilgili liberal, normal ve tutucu olmak üzere 3 ana senaryonun modellenmesi*	Stratejik		
ST1ALT1R1: *Uluslararası bir oyuncunun pazara yeni giriş yapması*		*3*	*5*
ST1ALT1R2 *:Rekabet halinde olduğumuz 2 oyuncunun birlikte stratejik ortaklık yapması*		*4*	*5*
ST1ALT1R3 *: Çevresel düzenlemelerin ve kampanyaların tüketici tercihlerini radikal biçimde değiştirmesi ve trendin yönünün bugünden belirsiz olması*		*2*	*3*
ALT2- *Kurumun mevcut rekabet avantajlarının analizi ve önceliklendirilmesi (hangileri korunacak, hangileri kuvvetlendirilecek, hangileri önemini yitirecek).*	Stratejik		
Op1- *Dağıtım operasyonu ile ilgili olarak mamul deponun 1 yıl içinde out-source edilmesi ve depo otomatik sipariş-dağıtım programının 2 yıl içinde devreye alınması ile sipariş karşılama oranını %20 arttırmak, stok dönüş hızını %15 arttırmak, ürün dağıtım maliyetlerinde m3 başına %10 iyileşme sağlamak.*	Operasyonel		
ST1ALT2Op1R1 *:Depo otomasyonunun planlanan zamanda hayata geçirilememesi*		*2*	*4*
ST1ALT2Op1R2 *: Satış ağırlığı değişimi ile komple kamyon sayısının azalması ve parsiyel yükleme sayısının artması, buna bağlı olarak m3 dağıtım maliyetlerinin artması*		*3*	*3*

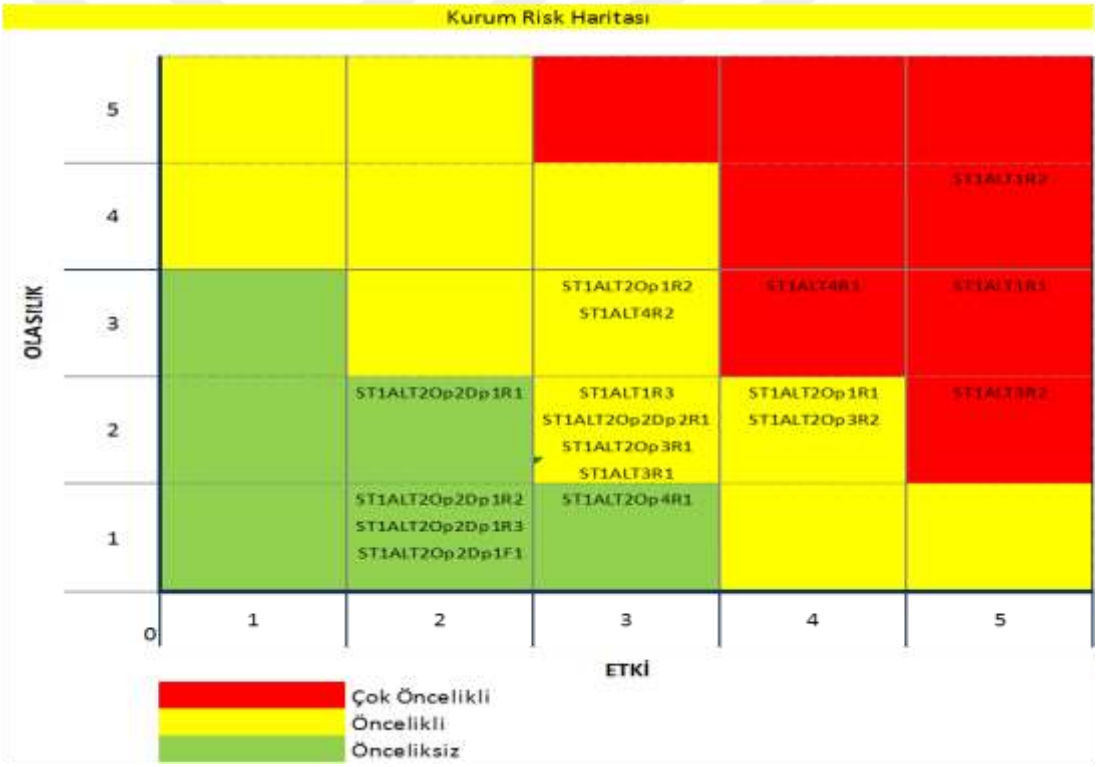
Risk değerlendirme tablosunun oluşturulmasından sonra risklere kurum değerleme kriterleri ve kurum tercihleri doğrultusunda odaklanmak için riskler önceliklendirilir. Kurum **risk haritası** hazırlanır.

Tablo 3.19'da kurum risk olasılık ve etkileri ile ilgili yapılan değerleme dökümanının örnek kesiti gösterilirken, Şekil 3.3'te kurumun risk haritası örnek kesiti gösterilmektedir.

Tablo 3.19: ABC Kimya San. Tic. A.Ş. Risk Olasılık ve Etki Değerlendirmesi Örnek Kesiti

Risk Kodu	Olasılık	Etki
ST1ALT1R1	3	5
ST1ALT1R2	4	5
ST1ALT1R3	2	3
ST1ALT2Op1R1	2	4
ST1ALT2Op1R2	3	3
ST1ALT2Op2Dp1R1	2	2

Şekil 3.3: ABC Kimya San. A.Ş. Risk Haritası Örnek Kesiti



Risklerimizi risk envanterini oluştururken kodladığımız için risk haritasını yorumlamak ve risklerin strateji ve hedefler ile ilişkisini kurmak kolaylaşmaktadır.

3.2.2.5. Performans: Risklerin Giderilmesi

Kurum açısından en önemli konulardan bir tanesi risk iştahının YK seviyesinde tespiti ve riskler karşısında sürdürülen risk iştahının izlenerek kurum içi iletişiminin açık biçimde yapılması olduğuna değinmiştik. Riskleri giderme konusunda tanımlanacak aksiyonların kurumun süren risk iştahına uygun olması ve kaynak dağılımının optimizasyonu risk iştahının ve risklerin kurum içinde etkili izlenmesi ve iletişiminin yapılması ile mümkün olacaktır.

Kurum için risk haritasının oluşturulmasından sonra risk haritasında öncelikli alanlara düşen riskler başta olmak üzere, kurum risk portföyünde bulunan riskler için risk giderilmesi planları hazırlanır, bunların kaynak planlaması, fayda/maliyet dengeleri ortaya koyulur.

Yürütülen çalışmada odaklanılan her bir risk için, **kabul etme, kaçınma, azaltma ve paylaşma** stratejileri çerçevesinde potansiyel davranışlar belirlenir ve bunların kaynak ihtiyacı gözetilerek, hem kaynak maliyet dengesi hem de kurum risk iştahına ne ölçüde uygun oldukları değerlendirilir.

Risklerin giderilmesi planları, her aşamasında pek çok stratejik karar ve değerlendirmeye ihtiyaç duyacağı için taslakları üst yönetim tarafından hazırlanıp YK ile detaylı tartışılmalı ve gerekli onaylar alınmalıdır.

Kurum için risk haritasında çok öncelikli olarak derecelendirilmiş risklere yönelik risklerin giderilmesi planlarının kesiti Tablo 3.20'de gösterilmektedir.

Tablo 3.20: ABC Kimya San. A.Ş. Risklerin Giderilmesi Belgesi Örnek Kesiti

Risk	Doğal Risk		Yöntem	Risk Giderme Alternatifleri	Artık Risk	
	Olasılık	Etkisi			Olasılık	Etki
Risk 1: ST1ALT1R2 -Rekabet içinde olduğumuz 2 rakibin stratejik ortaklık kurması	4	5	Kabul Et			
			Kaçın			
			Paylaş	Bu durmdan en çok etkilenecek 3. rakip ile stratejik iş birliği olanaklarının araştırılması	4	2
			Azalt	Bu iki rakiple ayrı ayrı stratejik ortaklık ve/veya iş birliği fırsatlarının araştırılması ve gerekli yaklaşımlarda bulunulması	2	2
Risk 2: ST1ALT1R1- Uluslararası bir şirketin pazara yeni giriş yapması	3	5	Kabul Et	Teknolojik yatırım, kapasite artışı ve maliyet tasarrufları projelerine hız vererek rekabet avantajımızı arttırmak ve rekabete hazırlık	3	3
			Kaçın			
			Paylaş			
			Azalt			
Risk 3: ST1ALT4R1-Müşteri sayısını arttırırken müşteri başına satış tutarının düşmesi	3	4	Kabul Et			
			Kaçın			
			Paylaş			
			Azalt	Müşterilere verilen ciro primi uygulamasının kotalarının düşürülerek iskontoların%5 arttırılması, hedeflerin daha ulaşılabilir olmasının sağlanması	2	3

3.2.2.6. Performans: Kontrol Faaliyetleri

ABC Kimya San. A.Ş. firması için kontrol faaliyetleri konusunu değerlendirirken hatırlanması gereken konular; kontrol faaliyetlerinin kuruma özgü olması gerektiği, süreç ve fonksiyon amirlerince tanımlanması gerekip, üst yönetimin onayının alınması gerektiği, kurumun ve faaliyet gösterdiği çevrenin maruz kaldığı değişimler dikkate alınarak, kontrol faaliyetlerinin iç kontrol ilizyonlarını engelleyecek, kurum stratejilerine ve iş süreçlerine uygun olacak biçimde güncelleniyor olması şeklinde ifade edilebilir.

Kontrol faaliyetleriyle, kurumda uygulanan ABC-KRY sistemine ait süreçlerin etkili bir biçimde çalıştığını makul seviyede güvence altına alınmaya çalışılmaktadır. Makul derece kavramı, fayda-maliyet dengesinin kurulması açısından çok önemlidir. Bir kontrol faaliyetinin tanımlanıp işletilmesi ile elde edilecek fayda ve bu faaliyetin işletilmesinin maliyeti arasında kurum lehine bir

denge bulunmuyorsa söz konusu kontrol faaliyeti kuruma uygun olarak değerlendirilmeyebilir.

Kontrol faaliyetleri mümkün mertebe teknoloji odaklı olup, fayda-maliyet dengesi gözetilmiş biçimde kurumun teknolojik alt yapısına dayandırılmalıdır.

Kontrol faaliyetlerinin sahibi süreç ve fonksiyon amirleri iken, iç denetim, bu faaliyetlerin etkinliğini değerlendirmekle ilgilidir. Kurum için kontrol faaliyetleri oluşturulurken ve/veya güncellenirken, COSO İç Kontrol Sistemi Bileşenleri Prensipleri Ve Odak Noktaları adlı Tablo2.8'de "Kontrol Faaliyetleri" bileşeni altında yer verilen 10, 11 ve 12 nolu prensipler ve bunların odak noktalarının göz önünde tutulması gerekmektedir.

ABC Kimya San. A.Ş. kurumunda kurum vizyon ve misyonu açıkça ifade edilmiş, stratejik hedefleri, alt stratejileri, operasyonel hedefleri ve bireysel hedefleri gözden geçirilerek belli bir ilişki ve uyum içinde olacak biçimde belirlenmiş, kurumun ana sözleşmesi söz konusu değişiklikleri içerecek biçimde ele alınmış, kurum içi ve dışı temsil ve yetkilendirmeyi organizasyonun her seviyesi için tanımlayan iç yetki onay tablosu hazırlanmış, organizasyon şeması ABC-KRY sistemine uygun halde tanımlanmış, iş akışları dökümante edilerek uygun yetki – sorumluluk dağılımına dikkat edilmiş, kurum faaliyetleri politika, prosedür ve onay formları olarak düzenlenmiştir. Tablo 3.11'de politikalar ve genel çerçeveleri belirtilirken, Tablo 3.12'de kurumda uygulanacak politikalar, prosedürler ve onay formlarının listesine yer verilmiştir. Kurumsal değerleri ortaya koyan Etik Değerler Kitapçığı hazırlanmış ve örnek içeriğine Tablo 3.13' te yer verilmiştir.

Kurumun İnsan Kaynakları Politikaları ABC-KRY Sistemi ihtiyaçları açısından tekrar ele alınmış, mesleki yeterlilik kazandırma politikaları, performans değerlendirme politikaları, işe alım ve işten çıkarma politikaları, kariyer planlama ve takip sistemleri güncellenerek kurumun kontrol ortamı ABC-KRY sistemini destekler hale getirilmiş, dolayısıyla buna bağlı kontrol faaliyetleri de ABC-KRY

sisteminin süreçlerinin etkili çalışmasına yönelik makul ölçüde güvence sağlamak amacı ile güncellenmiştir.

3.2.2.7. Gözden Geçirme ve Revizyon: İzleme

ABC Kimya San. A.Ş. içinde uygulanan izleme faaliyetleri ABC-KRY sistemi ihtiyaçları göz önüne alınarak güncellenmiş, Tablo2.8'de belirtilen COSO İç Kontrol Sistemi " İzleme" bileşeni ile ilgili 16. ve 17. prensipler ve bunlarla ilgili odak noktaları dikkate alınmış , izleme faaliyetleri adına yapılan raporlamalarda sapmaların dönemsel olarak ortaya koyulması, sapmaların ilgili fonksiyon amirleri ile değerlendirilmesi, önemlilik derecelerinin tespiti yapılmış, karşılaştırma raporlarının manuel süreçlerden ziyade bilgi teknolojileri uygulamalarına dayanması sağlanmıştır.

Kurumun fonksiyon amirlerince, kendi yönetimlerindeki fonksiyonların operasyonel ve finansal performanslarını ölçmek için "anahtar performans göstergeleri" tanımlanarak, bunların ölçülmesi ile ilgili esaslar belirlenmiş ve performans göstergeleri ile ilgili üst yönetimle mutabık kalınmıştır.

Kurumun yapmakta olduğu iç ve dış raporlamaya ek olarak ABC-KRY sisteminin bileşenlerinin etkinliğini değerlendirmekte yardımcı olacak göstergeler, üst yönetim ve fonksiyon amirlerinin üzerinde mutabakat sağladığı anahtar performans göstergelerine ilişkin raporlamalar değerlendirilerek kurum için bir rapor envanteri hazırlanmıştır. Raporun adı, içeriği, raporlama zamanı, dağıtım listesi söz konusu rapor envanterinde belirtilmiş, içerik tekrarlarından kaçınarak fonksiyonlar arası verimlilik gözetilirken, rapor içeriklerinin bilgi teknolojileri uygulamalarına dayandırılması ile veri güvenirliği ve şeffaflığı gözetilmiştir.

Tablo 3.21' de kurumun rapor envanterinden bir örnek kesit verilmektedir.

Tablo 3.21: ABC Kimya San. A.Ş. Rapor Envanteri Örnek Kesiti

Rapor No	Rapor Adı	Rapor İçeriği	Dönemi	Hazırlayan	Dağıtım Tarihi	Dağıtım Listesi
1-	Finansal Tablolar	Şirketin UFRS ve ilgili mevzuata uygun finansal tabloları (Gelir tablosu, bilanço, nakit akış, SMM tabloları) gerçekleşen, forecast ve bütçe karşılaştırmalı olmak üzere.	Aylık	Mali İşler Gn.Md.Yrd.'ğı	Her Ayın 6. İş Günü	YK, Genel Müdür, Fonksiyon Amirleri
2-	Finansal Varyans Analizleri	Gelir tablosu, bilanço ve nakit akış kalemlerinin bütçe ve forcast ile fiili sonuçlarının karşılaştırılması sonucu sapmaların belirlenen tolerans aralıklarının dışında olduğu kalemler için bu sapmaların nedenlerini ortaya koyan **köprü** analizleri	Aylık	Mali İşler Gn.Md.Yrd.'ğı	Her Ayın 6. İş Günü	Genel Müdür, Fonksiyon Amirleri
3-	Üretim Maliyetleri Analizi	Hammadde, malzeme, direkt işçilik ve genel üretim giderlerinin maliyet merkezi hiyerarşisi, sabit-değişken gruplaması, dağıtım anah-tarları dikkate alınarak kalem bazında standart maliyet- fiili maliyet karşılaştırıması.		Mali İşler Gn.Md.Yrd.'ğı	Her Ayın 5. İş Günğü	Genel Müdür, Fonksiyon Amirleri
4-	Satış Analizleri	Brüt ve net satış fiili sonuçlarının forecast ve bütçe ile miktar ve tutar bazında, satış kanalı, kategori, sku seviyesinde karşılaştırılması	Aylık	Satış ve Pazarlama Gn.Md.Yrd.'ğı	Her Ayın 3. İş Günğü	Genel Müdür, Fonksiyon Amirleri
5-	Stok Dengesi Raporu	Kurumun stok varlıklarının ambar hareketlerinin detayını gösteren, ambarlar arası başlangıç bakiyesi, dönem girişleri, dönem çıkışları ve dönbem sonu stok dengesinin kurulması	Aylık	Tedarik Kanalları Direktörlüğü	Her Ayın 3. İş Günğü	Genel Müdür, Fonksiyon Amirleri

3.2.2.8. Bilgi, İletişim ve Raporlama

ABC Kimya San. A.Ş. firması iş fonksiyonları arasında entegrasyonu sağlanmış bir bilgi teknolojileri alt yapısına sahip olup , operasyonel ve finansal raporlama, İnsan Kaynakları politikalarına yönelik işe alma, performans değerlendirme, kariyer planlama vb. uygulamalar bilgi teknolojilerinden yararlanılarak yürütülmektedir.

Kurumun vizyon, misyon, etik kurallar, iş akışları, organizasyon yapısı, iş akışları, politika ve prosedürleri, bunların arşivlenmesi ve kurum içi iletişiminde bilgi teknolojilerinden yararlanılmaktadır. Bu yönü ile COSO İç Kontrol SisteminTablo 2.7'de belirtilen "Bilgi ve İletişim" bileşeni ile ilişkili 13, 14 ve 15 numaralı prensipleri ve bunlarla ilgili odak noktaları dikkate alındığında kurumun

bilgi ve iletişim alt yapısının ABC-KRY sistemi ihtiyaçlarına uygun olarak yapılandırıldığı ve çalıştırıldığı değerlendirilmektedir.

3.2.3. KRY Sisteminin Etkinliğinin Ölçülmesi

ABC Kimya San. A.Ş. kurumunda uygulanmakta olan geleneksel iç denetim faaliyeti, ABC-KRY sistemi öngörüleri ve ihtiyaçları çerçevesinde tekrar ele alınmış, geleneksel iç denetim faaliyetinin çehresi ABC-KRY Sistemi öngörüleri ve beklentileri dikkate alınarak ve UMUÇ' nde belirtilen, uyulması zorunlu standartlar göz önünde tutularak güncellenmiştir. En belirgin değişim, yeni durumun iç denetçiler için ortaya koyduğu, kurumu, stratejilerini, organizasyon yapısını, endüstri ve iş dinamiklerini çok iyi anlamış olarak iç kontrol ve risk yönetimi süreçleri ile ilgili sadece kontrol faaliyetlerinin varlığını ve/veya yokluğunu tespit etme değil, uygulamaların etkinliğini değerlendirerek bu konuda kanaat oluşturma gerekliliğidir.

ABC-KRY Sistemi etkinliğinin ölçülmesine yönelik Tablo2.8'de belirtilen COSO İç Kontrol Sistemi bileşenleri, prensipleri ve odak noktaları iç denetim faaliyetinin yapması gereken değerlendirmenin çerçevesini oluştururken, iç denetim açısından, oluşturulacak değerlendirme kriterleri, iç denetimin planlanması, saha çalışmalarının planlanması, uygulanması, sonuçların raporlanması kuruma özgü ve kurumun maruz kaldığı değişimlerin etkilerine göre güncellenerek sürdürülmelidir.

ABC Kimya San. A.Ş. kurumu iç denetim faaliyetinin kapsamını ABC-KRY Sisteminin etkinliğinin ölçülmesi olarak benimsemiş olup, iç denetim ekibinden herhangi bir danışmanlık faaliyeti beklentisi bulunmamaktadır. Kurumun iç denetim faaliyetinden beklentisi dikkate alınarak iç denetim politikası güncellenmiş ve söz konusu beklentiyi açıkça ifade eder hale getirilmiştir.

Kurumun iç denetim politikasının güncellenmesinin ardından bu politikaya uygun İç Denetim Yönetmeliği güncellenmiştir. Kurumun İç Denetim Yönetmeliği'nin içerik örneği bir kesit olarak Tablo 3.22'de verilmektedir.

Tablo 3.22: ABC Kimya San. A.Ş. İç Denetim Yönetmeliği İçerik Örneği

ABC Kimya San.A.Ş. İç Denetim Yönetmeliği İçeriği

1. İçindekiler
2. Amaç
3. Kapsam
4. Tanımlar
5. Sorumluluk Dağılımı
   - 5.1. İç Denetim Müdürlüğünün Görevleri
   - 5.2. Hesap Verebilirlik
   - 5.3. Bağımsızlık
   - 5.4. Tarafsızlık
   - 5.5. Sorumluluk
     - 5.5.1. YK Sorunlulukları
     - 5.5.2. Üst Yönetim Sorumlulukları
     - 5.5.3. İç Denetim Müdürü Sorumlulukları
     - 5.5.4. Denetlenenlerin Sorumlulukları
6. Uygulama Esasları
   - 6.1. Yetki
     - 6.1.1. İç Denetçilerin Yetkili Oldukları Konular
     - 6.1.2. İç Denetçilerin Yetkili Olmadıkları Konular
   - 6.2. İç Denetim Uygulama Standartları
7. Yürürlük
8. Yürütme
9. Güncellenme Ve Yayınlanma Esasları
10. Ekler
    - 10.1. Uluslararası İç Denetim Standartları
    - 10.2. ABC Kimya San.A.Ş. İç Denetim Müdürlüğü Mesleki Ahlak Kuralları
    - 10.3. İşe Uygunluk Bildirimi
    - 10.4. Süreç Akış Şeması

Kurumun İç Denetim Yönetmeliği'nin güncellenmesinden sonra kurumun İç denetim ekibi yeni durum ve kapsama uygun olacak biçimde organizasyon yapısı içinde ele alınmış, ekibin ihtiyaç duyacağı mesleki yeterlilik, fayda-maliyet dengesi de gözetilerek, kurumda mevcut iç denetim ekibi, doğrudan

YK' na raporlayan, bir iç denetim yöneticisi ve üç iç denetçiden oluşan, toplam dört kişilik bir iç denetim ekibi olarak güncellenmiş olup İç Denetim Müdürlüğü olarak yapılandırılmıştır.

İç denetim ekibinin yapısının güncellenmesi takiben İç Denetim Rehberi güncellenmiş, söz konusu güncellemede ABC-KRY Sisteminin etkinliği ile ilgili özellikle Tablo 2.7'de yer verilen bileşenler, prensipler ve odak noktalarının ortaya koyduğu genel çerçeveden hareketle kuruma has iç denetim yıllık planlamaları, saha çalışması planlamaları, değerlendirme kriterleri ve diğer iç denetim süreçlerine yer verilmiştir. Kurumun İç Denetim Rehberi içerik örneği bir kesit olarak Tablo 3.23 'te gösterilmektedir.

Tablo 3.23: ABC Kimya San. A.Ş. İç Denetim Rehberi İçerik Örneği

1. Planlama
- 1.1. Yıllık İç Denetim Planı
  - 1.1.1. Denetim Evreni
  - 1.1.2. Risk Değerlendirme Kriterleri
  - 1.1.3. Risk Değerlendirmesi
  - 1.1.4. Risk Bazlı Yıllık Denetim Planının Hazırlanması
  - 1.1.5. Risk Bazlı Yıllık Denetim Planının Onaylanması
  - 1.1.6. Risk Bazlı Yıllık Denetim Planının Güncellenmesi
- 1.2. Denetim Faaliyeti Planlaması
  - 1.2.1. Denetim Amaçlarının Belirlenmesi
  - 1.2.2. Çalışma Kağıtları ve Formlar
  - 1.2.3. Bilgi Toplama Ve Ön Araştırma
  - 1.2.4. Potansiyel Sorunlu Alanların Belirlenmesi
  - 1.2.5. Kontrollerin Belirlenmesi
  - 1.2.6. Denetim Testlerinin Planlanması
  - 1.2.7. Örnekleme Tasarımı
  - 1.2.8. Örnekleme Yönteminin Belirlenmesi

2. Saha Çalışmaları
- 2.1. Açılış Toplantısı
- 2.2. Denetim Testlerinin Gerçekleştirilmesi
- 2.3. Örneklemelerin Yapılması
- 2.4. Örneklemede Dökümantasyon
- 2.5. Örnekleme Sonuçlarının Değerlendirilmesi
- 2.6. Bulguların Oluşturulması
- 2.7. Bulguların Denetlenen Süreç Sahipleri İle Paylaşılması
- 2.8. Önerilerin Geliştirilmesi
- 2.9. Kapanış Toplantısı

Tablo 3.23: ABC Kimya San. A.Ş. İç Denetim Rehberi İçerik Örneği (Devamı)

3. Raporlama
- 3.1. Taslak Denetim Raporunun Hazırlanması Ve İlgililerle Paylaşılması
- 3.2. Nihai Denetim Raporunun Hazırlanması Ve İlgilierle Paylaşılması

4. İzleme Ve Değerlendirme
- 4.1. Denetim Sonuçlarının İzlenmesi
- 4.2. Denetimin Değerlendirilmesi
- 4.3. Denetçinin Değerlendirilmesi

5. Ekler
- 5.1. Görevlendirme Yazısı Örneği
- 5.2. Denetimin İlgili Süreç Sahibine Bildirimi Yazısı Örneği
- 5.3. Çalışma Kağıtları
- 5.4. Açılış Toplantısı Tutanağı Formatı
- 5.5. Kapanış Toplantısı Tutanağı Formatı
- 5.6. Denetlenen Memnuniyet Anketi
- 5.7. Denetçi Değerlendirme Formu
- 5.8. COSO İç Kontrol Sistemi Bileşenleri, Prensipleri Ve Odak Noktaları
- 5.9. COSO KRY Sistemi Bileşenleri
- 5.10. UMUÇ
  - 5.10.1. İç Denetçiler İçin Davranış Kuralları
  - 5.10.2. Uluslararası İç Denetim Standartları

İç Denetim faaliyeti ile ilgili kurum politikası, ilgili yönetmelik ve iç denetim faaliyetinin süreçlerini detaylandıran iç denetim rehberi ışığında yürütülecek olan iç denetim faaliyetinde geleneksel çerçeveden en önemli fark, ABC-KRY Sisteminin süreçlerinin etkinliğinin değerlendirilmesinde, güncellenmiş COSO İç Kontrol Sisteminin ortaya koyduğu ve Tablo 2.7' de gösterilen genel değerlendirme çerçevesidir.

İç deneticilerden, ABC-KRY Sistemi bileşenlerinin her birinin entegre bir yapı içinde etkili bir şekilde fonksiyon gösterip göstermediğini kurum özelinde değerlendirebilmeleri beklenmektedir. Bu değerlendirmeler, ilgili fonksiyonun varlığını ve/veya yokluğunu tespit etmeye yönelik kontrol listelerinin doldurulmasında farklı olarak, değerlendirilen fonksiyonun ABC-KRY Sisteminin etkinliği açısından, kurum stratejileri, yapısı, faaliyet alanı, endüstrisi, stratejik hedefleri, risk haritası ve değişimleri dikkate alınarak, kuruma has yapılması gereken değerlendirmeler olup çok iyi ve detaylı dökümante edilmesi beklenmektedir. Bu değerlendirmelerle ilgili COSO İç Kontrol Sistemi bileşen, prensip ve odak

noktalarına yönelik hazırlanmış değerlendirme formlarından yararlanılacak olup, söz konusu formların içeriğinden bir örnek kesit Tablo 3.24' te gösterilmektedir.

Tablo 3.24: ABC Kimya San. A.Ş. COSO KRY İç Kontrol Sistemi Prensipleri Değerlendirme Formu Örneği

COSO İç Kontrol Sistemi Bileşen Ve Prensiplerinin Değerlendirilmesi Çalışma Kağıdı Örneği

Bileşen : KONTROL ORTAMI **Prensip 1:** Organizasyon dürüstlük ve etik değerlere bağlılık göstermelidir. **Odak Noktaları:** *a- Üst seviyede tutum belirler.* *b- İdari standartları belirler.* *c- İdari standartlara bağlılığı* *d- Sapmaları belli zaman*				
Prensip 1'e etki eden kontrol faaliyetlerinin özeti:				
Prensip 1 ile ilgili sapmalar:				
Bulgu No	Sapmanın Tanımı	Sapmanın Büyüklüğünü Değerlendirin *(Diğer prensipleri etkileyen kontrol faaliyetlerinin burada tespit edilen sapmayı ne ölçüde tolere edebileceğini dikkate alın)*		*Diğer prensiplerle ilgili olup, burada tespit edilen sapmayı etkileyebilecek diğer iç kontrol sapmalarını listeleyin*
		Sapma Büyük mü? (E/H)	Yorumlar / Telafi Edici Kontroller	
Prensibi değerlendirin:		E/H	Açıklama / Sonuç	
Prensip mevcut mu?				
Prensip işlevsel mi?				

Kaynak: COSO, **Illustrative Tools For Assesing Effectiveness of a System of Internal Control: Internal Control-Integrated Framework,** May 2013, (Çevrimiçi) http//www.coso.org, 15 Mart 2016.

COSO İç Kontrol Sistemi bileşenleri ve prensiplerine yönelik değerlendirmelerde, sapmaların raporlanması için Tablo 3.25'de örnek verilen format kullanılabilecektir.

Tablo 3.25: ABC Kimya San. A.Ş. İç Kontrol Sapmalarının Özeti Örneği

Sapmaların Özeti									
Bulgu No	Sapmanın Kaynağı		Sapmanın Tanımı	Sapmanın Büyüklüğü	Sapma Önemli mi? (E/H)	Sürecin Sahibi	Çözüm Planı Ve Tarihi	Mevcut İşleve Etkisi	Sapmaya katkı sağlayan diğer prensiplerle ilgili başka sapmaları listeleyin
	Bileşen	Prensip							

Kaynak: A.e.

Kurumun İç Denetim Müdürlüğünden, ABC-KRY Sistemi etkinliği konusunda güvence vermek amacıyla, kurumun iç denetim politikasına uygun olarak hazırlanmış İç Denetim Yönetmeliği ve İç Denetim Rehberi ışığında iç denetim faaliyetini yürütmesi beklenmektedir.

İç denetim fonksiyonunun çehresinin ABC-KRY Sistemi ihtiyaçlarına uygun hale getirilmesi ile ABC Kimya San. A.Ş. şirketinde risk yönetim sistemi olarak ABC-KRY Sisteminin uyarlanması tamamlanmış olmaktadır.

SONUÇ

Günümüz ekonomik koşullarında, sermaye yer değiştirme hızı ve biçimleri, teknolojik gelişmeler, dijital platformlar, bilgiye ulaşma hızı ve biçimleri, sosyal ve çevresel değerler ve tüm bu faktörlerdeki değişim hızı dikkate alındığında; bir kurumda risk yönetimi fonksiyonunun etkili bir şekilde çalıştırılması çok önemli bir rekabet avantajı konusu haline gelmektedir.

Kurumun stratejik hedeflerinin gerçekleştirilmesinden, hedeflenen iş sonuçlarının alınmasından nihai olarak yönetim kurulu ve üst yönetim sorumlu olmakla birlikte, kurumun bu konudaki yetkinliği hissedarlar, yatırımcılar ve çalışanlar başta olmak üzere, iş ilişkisi ve sosyal ilişki içinde olduğu tüm paydaşlar açısından hayati önem taşımaktadır.

Stratejik hedefleri ve iş hedeflerinin gerçekleştirilmesini makul ölçüde güvence altına almak isteyen kurumlar için öncelikli olarak organizasyonlarına risk yönetimi fonksiyonu yetkinliği kazandırmaları ve/veya var olan risk yönetimi yetkinliklerini geliştirmenin yollarını ele almaları tavsiye edilebilir.

Kurum için bir risk yönetim sistemi ve/veya çerçevesi oluşturulmak istendiğinde şu konular göz önünde tutulmalıdır:

- Kurum için söz konusu risklerin ve fırsatların etkin şekilde yönetilmesi başta yönetim kurulu ve üst yönetim olmak üzere kurum organizasyonunun tamamının sorumluluğudur.
- KRY çerçevesi ile ilgili geliştirilmiş **kuramsal tasarımlar** konunun genel çerçevesini ortaya koymakla birlikte, kurum için oluşturulması düşünülen KRY çerçevesi, bahsedilen genel kuramsal tasarımlardan hareketle, kuruma özel, kurum ihtiyaçları, beklentileri, endüstrisi, rekabet ortamı, maruz kalınan iş ve dış değişim faktörleri vb. etkilerin ışında tasarlanmalı, bir proje olarak ele alınarak kuruma uyarlanmalıdır. Bu noktada kuruma özgü KRY projesinden bahsedilir hale gelinir.

- Başarılı bir KRY projesi uygulaması, kurum açısından esas itibariyle bir "değişim projesi" niteliğinde olup, başlangıç noktası proje ile ilgili yönetim kurulu ve üst yönetimin desteğini almak, bu desteği sürekli kılmaktır.
- Yönetim kurulu ve üst yönetimin KRY projesine yönelik destekğinin alınması ve sürekli kılınması konusundaki en önemli adım, yönetim kurulu ve üst yönetimin KRY projesinden beklentilerinin rasyonel bir zemine oturtularak fayda-maliyet dengesinin kurum lehine oluşturulması aşamasıdır.
- Yönetim kurulu ve üst yönetimin KRY projesinden beklentilerini rasyonel bir zemine oturturken ve fayda maliyet- dengesini gözetirken, KRY projesi ile genel olarak amaçlananın kurumun maruz kaldığı riskler itibariyle stratejik hedeflerini gerçekleştirmesini **makul ölçüde güvence altına almak** olmasına dikkat edilmelidir.
- KRY projeleri ile yüzde yüz güvence değil, makul ölçüde güvence hedeflenmesi fayda-maliyet dengesinin kurulması açısından çok önemlidir.
- Kuruma özel bir KRY çerçevesi oluşturulurken, mesleki otoriteler ve standart koyucular tarafından genel kabul görmüş, geniş kapsamlı bir kuramsal tasarımın ortaya koyduğu genel çerçeveye bağlı kalmaya çalışmak, söz konusu genel çerçevenin bileşenlerini ve prensiplerini kurum özeline uyarlamaya çalışmak sonuç almayı kolaylaştıracak ve KRY projesinin evrensel standartlara sahip olmasını sağlayacaktır.
- KRY projesinin odağında politikalar, prosedürler oluşturmak, kontrol faaliyetleri tanımlayarak belgelendirmek ve sonrasında bu faaliyetlerin var olup olmadığını, tanımlanan politika ve prosedürlere uygun hareket edilip edilmediğini tespit etmek ve raporlamak yoktur. KRY projesinin odağında insan ve davranışlar olup, KRY çerçevesinin kuruma uyarlanması stratejik hedeflerin gerçekleştirileceğini makul ölçüde güvence altına almaz. KRY çerçevesinin etkili biçimde fonksiyon göstermesi söz konusu makul ölçüde güvenceyi sağlayacaktır.
- Kurum için oturtulmuş bir KRY çerçevesinin bulunması, etkili biçimde fonksiyon gösterdiği anlamına gelmez. KRY fonksiyon unun etkinliği, kurum içinde bağımsızlığı ve tarafsızlığı sağlanmış, Uluslararası İç Denetim Standartlarına uygun faaliyet yürüten bir iç denetim fonksiyonu marifeti ile değerlendirilmelidir.

- İç denetim fonksiyonu KRY fonksiyonlarının etkin biçimde çalıştığı ile ilgili makul ölçüde garanti vermek üzere yapılandırılmalıdır.
- İç denetim fonksiyonun odağı, kurum iç kontrol yapısına yönelik kontrol faaliyetlerinin tasarlandığı gibi yerinde olup olmadığını tespitten, KRY çerçevesini oluşturan bileşenlerin etkili çalışıp çalışmadığını değerlendirmeye kaymıştır. Bir kontrol faaliyetinin ve/veya KRY bileşeninin etkisini değerlendirebilmek için; işi, endüstriyi, kurum stratejilerini, önceliklerini, risk iştahı ve toleransını, risk değerlendirme ve giderme sürecini, maruz kalınan değişim faktörlerini vb. dinamikleri anlayabilmek ve değerlendirebilmek gerekir. İç denetim ekibine bu gereksinimlere cevap verecek mesleki yeterliliğin kazandırılması, faaliyet yöntemleri ve kaynaklarının bu gereksinmeyi karşılayabilecek şekilde güncellenmesi ve/veya buna uygun yapılandırılması gerekmektedir.
- Oluşturulan KRY çerçevesinin ve iç denetim yapısının, kurumun maruz kaldığı değişimlere bağlı olarak sürekli biçimde güncellenmesi, entegre ve yaşayan, sistematik bir süreç olarak ele alınması gerekmektedir.
- Genel kabul görmüş, saygın KRY sistemlerinin günümüze kadar ortaya koyulmuş en kapsamlısı olarak kabul edilen COSO KRY-2017 çerçevesi bir endüstriye ve/veya kuruma özel tasarlanmış olmayıp, herhangi bir kurumun bütününe ve/veya bir kısım hedeflerine tüm organizasyon açısından ve/veya organizasyonun bir kısmı açısından uyarlanabilecek bir yapıya sahiptir. Bu hali ile herhangi bir iş kolundaki her hangi bir kurum için referans alınabilecek KRY Sistemi genel çerçevesi olarak önerilebilir.

Yukarıda yer verilen unsurların göz önünde tutulması ile kurum özelinde uyarlanacak bir KRY çerçevesi ile, bu yapının etkinliği konusunda makul derecede güvence vermeyi hedefleyen, KRY çerçevesinin bileşenlerinin etkinliğini değerlendirebilecek yeterliliğe sahip yapılandırılmış bir iç denetim fonksiyonun, kurumlara stratejik hedeflerine ulaşma konusunda çok önemli avantajlar sağlayacağına inanılmakta, kurumlara, kendi yapıları ve öncelikleri özelinde bir KRY çerçevesi oluşturmak ve etkili bir şekilde çalışmasını sağlamak konusunu öncelikli olarak değerlendirmeleri tavsiye edilmektedir.

Bu çalışmada; Kimya sektöründe faaliyet gösteren bir üretim şirketi için bir kurumsal risk yönetimi çerçevesi oluşturulmuş , risklerin stratejilere ve iş sonuçlarına olan etkilerinin yönetilmesi ve şirket performansının arttırılarak ekonomik değerini arttırması ve bunu sürdürülebilir kılması için sistematik bir kurumsal risk yönetimi sistemine sahip olması sağlanmıştır.

Bundan sonraki çalışmaların farklı sektörlerde faaliyet gösteren şirketler için kurumasal risk yönetimi uygulama örneklerine yönelmesinin iş hayatı ve ekonomik dünya için yararlı olacağı kanısındayız.

KAYNAKÇA

Atwood Bill,'vd'.: "The Illusion of Internal Control," **Strategic Finance**, October 2012, IMA, s. 30-37

Adiloğlu, Burcu.: "İç Denetim Süreci ve Temel İşletme Faaliyetlerinin Konrol Prosedürleri ile Değerlendirilmesi: Bir Uygulama" **Doktora Tezi**, İstanbul, 2010

COSO.: **Executive Summary :Internal Control-Integrated Framework,** May 2013, (Çevrimiçi) http//www.coso.org, 19 Şubat 2016.

COSO.: **Framework and Appendices: Internal Control-Integrated Framework**, May 2013, (Çevrimiçi) http//www.coso.org, 19 Şubat 2016.

COSO.: **Illustrative Tools for Assesing Effectiveness of a System of Internal Control: Internal Control-Integrated Framework,** May 2013, (Çevrimiçi) http//www.coso.org, 15 Mart 2016.

COSO.: **Executive Summary Enterprise Risk Management-Integrated Framework**, September 2004, (Çevrimiçi) http//www.coso.org, 20 Mayıs 2016.

COSO.: **Guidance on Monitoring Internal Control Systems: Introduction**, January 2009, (Çevrimiçi) http//www.coso.org, 07 Mart 2016.

COSO.: **Enterprise Risk Management-Integrating with Strategy and Performance**, June 2017, (Çevrimiçi) http//www.coso.org, 05 Nisan 2019

COSO.: **Enterprise Risk Management-Integrating with Strategy and Performance-Executive Summary**, June 2017, (Çevrimiçi) http//www.coso.org, 05 Nisan 2019.

Creswell, John W.: **Nitel Araştırma Yöntemleri Beş Yaklaşıma Göre Nitel Araştırma ve Araştırma Deseni**, Çev. Ed.:Yrd. Doç. Dr. Mesut Bütün, Yrd. Doç.Dr. Selçuk Beşir Demir, Çev.: Doç. Dr. Osman Birgin, Doç. Dr. Suat Ünal, Doç. Dr. Tuncay Özsevgeç, Doç. Dr. Yüksel Dede, Doç. Dr. Ahmet Bacanak, Yrd. Doç. Dr.Arif Bakla, Doç. Dr. Ayfer Budak, Yrd. Doç.Dr. Güney Hacıömeroğlu, Doç. Dr. İbrahim Budak, Yrd. Doç.Dr. Mahmet Aydın, Yrd. Doç. Dr. Mesut Bütün, Yrd. Doç. Dr. Miraç Aydın, Yrd. Doç. Dr. Selçuk Beşir Demir, 4.bs., Ankara, Siyasal Kitabevi, Şubat 2018

Curtis, Patchin, Carey,Mark.: "Risk Assesment in Practice," **Thought Leadership in ERM**, October 2012, (Çevrimiçi) http//www.coso.org, 17 Mayıs 2017.

Göğüş, E.Handan S. **Risk Odaklı İç Denetimde Risklerin Saptanması ve Değerlendirilmesi**, İstanbul, Türkmen Kitabevi, 2012.

International Professional Practices Framework: "Internal Auditing and Fraud,"**Practice Guide**, December 2009, (Çevrimiçi) http/www.globaliia.org/standards-guidance, 13 Ocak 2015

ISO.: **International Standard ISO31000:Risk Management-Principles And Guidelines**, Switzerland,ISO, 2009.

Moeller, Robert R.: **COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance Process,** 2.bs**,** New Jersey, John Wiley&Sons, Inc., 2011.

Özbek, Çetin.: **İç Denetim:Kurumsal Yönetim:Risk Yönetimi:İç Kontrol**, 2 c.,İstanbul, Türkiye İç Denetim Enstitüsü, Ekim 2012.

Özgül, Burcu, Mengi, Banu T.: **Kurumsal Sürdürülebilirlik ve Güvencesi "İç Denetim" BİST Sürdürülebilirlik Endeksi'ne Tabi Şirketlerde Anket Çalışması,** İstanbul, Beta Beta Basım Yayım Dağıtım A.Ş., 2016.

Prewet, Kyleen,Terry, Andy: **COSO's Updated Enterprise Risk Management Framework-A Quest For Depth and Clarity** The Journal of Corporate Accounting and Finance, July 2018 , Wiley Periodicals Inc. s.19 (Çevrimiçi) www.wileyonlinelibrary.com, 06 Mayıs 2019.

PWC **COSO Internal Control-Integrated Framework,** American Institute of Certified Public Accountants, 2013.

Rittenberg, Larry, Martens, Frank: "Understanding and Communicating Risk Apetite," **Thought Leadership In ERM**, January 2012, (Çevrimiçi) http//www.coso.org, 17 Mayıs 2016.

Sobel, Paul J, Reding,Kurt F.: **Enterprise Risk Management: Achieving and Sustaining Success**, Florida, The Institute of Internal Auditors Research Foundation, 2012.

The Institute of Internal Auditors "Coordinating Risk Management and Assurance," **Practice Guide**, March 2012, (Çevrimiçi) http/www.globaliia.org/standards-guidance, 13 Ocak 2015.

The Institute of Internal Auditors **IIA Position Paper: The Role of Internal Auditing in Enterprise-Wide Risk Management,** The Institute of Internal Auditors, January 2009.

The Institute of Internal Auditors	**Sawyer's Guide for Internal Auditors**,3 c.,6. bs., Florida, The Institute of Internal Auditors Research Foundation, 2012.
The Institute of Internal Auditors.:	"Uluslararası İç Denetim Standartları," **The Institude of Internal Auditors Standards and Guidence**, 01 January 2009, (Çevrimiçi) http/www.theiia.org, 17 Mayıs 2015.
The Institute of Internal Auditors.:	Uluslararası İç Denetim Standartları, çev.,Türkiye İç Denetim Enstitüsü, Ekim 2012, (Çevrimiçi) http/www.tide.org.tr, 10 Temmuz 2015.
The Institute of Internal Auditors.:	"İç Denetimin Kurumsal Risk Yönetiminde Oynadığı Rol", **IIA Pozisyon Raporu,** çev.,Türkiye İç Denetim Enstitüsü, Ocak 2009, (Çevrimiçi) http/www.tide.org.tr, 25 Temmuz 2016.
The Institute of Internal Auditors.:	Etik Kuralları, (Çevrimiçi) http/www.theiia.org, 10 Temmuz 2015.
The Institute of Internal Auditors.:	"Uluslararası Mesleki Uygulama Çerçevesi", çev.,Türkiye İç Denetim Enstitüsü, (Çevrimiçi) http/www.tide.org.tr, 10 Temmuz 2015.
Türedi, Hasan, Karakaya, Gencer, İldem, Mehmet.:	"Kurumsal Yönetim ve İç Denetim İlişkisi", **Sayıştay Dergisi**, No:96, Ocak –Mart 2015.
Türk Ticaret Kanunu	"6102 Sayılı Türk Ticaret Kanunu," **Resmi Gazete,** Sayı: 27846, 14 Şubat 2011.
TÜSİAD.:	Kurumsal Risk Yönetimi, İstanbul, TÜSİAD, Şubat 2008.

EKLER

EK 1: Uluslararası İç Denetim Standartları Özeti

Kaynak: (Çevrimiçi) https://na.theiia.org/translations/PublicDocuments/IPPF-Standards-2017-Turkish.pdf, 17 Mayıs 2018

NİTELİK STANDARTLARI

1000 - Amaç Yetki ve Sorumluluklar
İç denetim faaliyetinin amaç, yetki ve sorumlulukları, İç Denetimin Tanımı ve Etik Kuralları ve Standartlar'la uyumlu olan ve denetim komitesi ve yönetim kurulunca da onaylanan bir iç denetim yönetmeliğinde açıkça tanımlanmak zorundadır. İç denetim yöneticisi iç denetim yönetmeliğini dönemsel olarak gözden geçirmek ve üst yönetime ve yönetim kuruluna onay için sunmak zorundadır.

1000.A1- Kuruma sağlanan güvence hizmetleri niteliği iç denetim yönetmeliğinde tanımlanır.
1000.C1- Kuruma sağlanan danışmanlık hizmetleri niteliği iç denetim yönetmeliğinde tanımlanır.
1010- İç Denetim Tanımına, Etik Kuralları ve Standartlarına uyma zorunluluğu iç denetim yönetmeliğinde tanınır.

1100 - Bağımsızlık ve Objektiflik
İç denetim faaliyeti bağımsız olmalıdır ve denetçiler görevlerini yaparken objektif davranmak zorundadır.

1110- İç denetim yöneticisi kendisine kurum içi bağımsızlık sağlayan bir yönetim kademesine bağlı olur.
1110.A1- İç denetim faaliyeti ve birimi kurum içinde bağımsız ve serbest olmalıdır.
1111- İç denetim yöneticisi yönetim kurulu ile doğrudan iletişim ve etkileşimde olmalıdır.
1120- İç denetçiler bireysel olarak tarafsız olmak zorundadır.
1130- Denetçilerin bağımsızlık veya tarafsızlığının bozulduğu durumlarda bu konu taraflara açıklanmalıdır.
1130.A1- İç denetçiler daha önce kendilerinin sorumlu olduğu faaliyetleri değerlendirmekten kaçınmalıdırlar.
1130.A2- İç denetim yöneticisi sorumluluğundaki işlevlere yönelik güvence görevi iç denetim faaliyeti dışında biri tarafından kontrol edilmelidir.
1130.C1- İç denetçiler daha önce sorumlu oldukları faaliyetlere ilişkin danışmanlık hizmeti verebilir.
1130.C2- İç denetçiler danışmanlık hizmetindeki bağımsızlıkları zarar görecekse bunu açıklarlar.

1200 - Yeterlilik ve Azami Mesleki Özen ve Dikkat
Görevler, yeterlilik ve azami mesleki özen ve dikkat ile yerine getirilmek zorundadır.

1210- İç denetçiler sorumluluklarını yerine getirmek için gerekli bilgi, beceri ve diğer vasıflara sahip olmak zorundadır.
1210.A1- İç denetim personeli gerekli vasıfların tamamına sahip değilse iç denetim yöneticisi eksik kalan kısım için dışarıdan uzman desteği almalıdır.
1210.A2- İç denetçiler suistimal risklerini değerlendirebilecek yetkinlikte olmalıdır ancak bunun esas uzmanlıkları olmadığı unutulmamalıdır.
1210.A3- İç denetçiler bilgi teknolojisi risklerini değerlendirebilecek yetkinlikte olmakla birlikte esas uzmanlıkları bu değildir ve konunun uzmanı kadar bilgi sahibi olmaları beklenemez.
1210.C1- İç denetim yöneticisi ekibin uzmanlığının yeterli olmadığı danışmanlık görevini almaz veya dışardan uzman desteği sağlayarak alır.
1220- İç denetçiler işlerine azami mesleki özen ve dikkat gösterirler. Bu hata yapılmayacağı anlamına gelmez.
1220.A1- İç denetçiler mesleki özen ve dikkat gösterirken çalışma kapsamı, güvence prosedürleri, risk- kontrol süreçleri, suistimal ihtimali, güvence görevi fayda-maliyet ilişkisini göz önüne alırlar.
1220.A2- Mesleki özen ve dikkat gösterirken teknoloji destekli veri analizlerinden yararlanılır.
1220.A3- Önemli risklere karşı uyanık ve duyarlı olunması gerekir. Önemli risklerin tamamının teşhisi garanti edilemez.
1220.C1- İç denetçiler danışmanlık görevinde mesleki özen ve dikkat gösterirken müşterilerin ihtiyaç ve beklentilerini, çalışmanın boyutu ve karmaşıklığını, görevin fayda-maliyet ilişkisini dikkate alırlar.
1230- İç denetçiler ihtiyaçlara göre sürekli mesleki gelişim göstermek zorundadırlar.

1300 - Kalite Güvence ve Geliştirme Programı
İç denetim yöneticisi, iç denetim faaliyetinin tüm yönlerini kapsayan bir kalite güvence ve geliştirme programı hazırlamak ve bunu sürdürmek zorundadır.

1310- Kalite güvence ve geliştirme programı iç ve dış değerlendirmeleri içerir.
1311- İç değerlendirmeler, iç denetim faaliyetinin performansının kurum içinde devamlı izlenmesi ve dönemsel değerlendirilmesini kapsar.
1312- Dış değerlendirmeler kurum dışından bağımsız bir uzman tarafından en az 5 yılda bir yapılmalıdır.
1320- İç denetim yöneticisi uygulanan kalite güvence ve geliştirme programı sonuçlarını üst yönetime raporlar.
1321- Ancak uygulanan kalite güvence ve geliştirme programı sonuçlarının desteklediği durumlarda iç denetim faaliyetinin Uluslararası İç Denetim Mesleki Uygulama Standartlarına uygun olduğu belirtilebilir.
1322- İç Denetim Tanımına, Etik Kurallara veya Standartlara aykırılık olması durumunda bu üst yönetime raporlanır.

EK1: Uluslararası İç Denetim Standartları Özeti (Devamı)

PERFORMANS STANDARTLARI

2000- İç Denetim Faaliyetinin Yönetimi
İç denetim yöneticisi, iç denetim faaliyetini, faaliyetin kuruma değer katmasını sağlayacak etkili bir tarzda yönetir.

2010- İç denetim yöneticisi iç denetim faaliyetini risk esaslı planlar.
2010.A1- İç denetim faaliyeti görev planı en az yılda bir yapılan yazılı bir risk değerlendirmesine dayanır. Üst yönetim ve yönetim kurulu bu sürece dahil edilir.
2010.A2- İç denetim yöneticisi iç denetim faaliyeti sonuçları açısından yönetim kurulu, üst yönetim ve diğer paydaşların beklentilerini saptamalı ve dikkate almalıdır.
2010.C1-İç denetim yöneticisi olası sonuçları itibariyle geliştirme ve değer katma potansiyelini dikkate alarak önerilen danışmanlık görevlerini kabul etme eğiliminde olmalıdır. Danışmanlık görevleri plana dahil edilmek zorundadır.
2020- İç denetim yöneticisi faaliyet planları ve kaynak planlamasını yönetim kurulu ve üst yönetime bildirir.
2030- İç denetim yöneticisi faaliyet için gerekli kaynakları ve bunların etkin kullanımını sağlamak zorundadır.
2040- İç denetim yöneticisi iç denetimin faaliyeti politika ve prosedürlerini belirler.
2050- İç denetim yöneticisi faaliyetin iç ve dış diğer güvence ve danışmanlık sağlayıcılarla koordinasyonunu sağlar.
2060- İç denetim yöneticisi faaliyetin ara sonuçları ve seyri ile ilgili üst yönetime dönemsel raporlama yapar.
2070- İç denetim faaliyeti dış hizmet sağlayıcı tarafından sunulursa, bu hizmet sağlayıcı kurumun etkili iç denetim faaliyeti sürdürülmesi konusundaki sorumluluğunun farkında olmasını sağlamalıdır.

2100- İşin Niteliği
İç denetim faaliyeti;sistematik ve disiplinli bir yaklaşımla, yönetişim (kurumsal yönetim) risk yönetimi ve kontrol süreçlerini değerlendirmek ve bu süreçlerin iyileştirilmesine katkıda bulunmak zorundadır.

2110- İç denetim faaliyeti kurumsal yönetim sürecini değerlendirmek ve geliştirmek zorundadır.
2010.A1- İç denetim faaliyeti kurumun etik ile ilgili faaliyetlerini değerlendirmek zorundadır.
2010.A2- İç denetim faaliyeti kurumun bilgi teknolojileri uygulamalarını değerlendirmek zorundadır.
2120- İç denetim faaliyeti risk yönetimi süreçlerinin etkinliğini değerlendirmek ve iyileştirilmesine katkıda bulunmak zorundadır.
2120.A1- İç denetim faaliyeti kurumun maruz kaldığı riskleri değerlendirmek zorundadır.
2120.A2- İç denetim faaliyeti kurumun suistimal riskini ve kurumun bu riski nasıl yönettiğini değerlendirmek zorundadır.
2120.C1- İç denetçiler danışmanlık görevlerinde de riskleri amaca uygun ele almak zorundadır.
2120.C2- İç denetçiler danışmanlık görevlerinde edindikleri risk bilgilerini kurumun risk değerlendirmesi sürecinde kullanmak zorundadır.
2120.C3- İç denetçiler risk yönetim süreçlerini kurup geliştirirken risklerin yönetimi sorumluluğunu almaktan kaçınmak zorundadır.
2130- İç denetim faaliyeti kurumun etkin kontrollere sahip olmasına yardımcı olmak zorundadır.
2130.A1- İç denetim faaliyeti kurumun kontrollerinin etkinliğini değerlendirmek zorundadır.
2130.C1- İç denetçiler danışmanlık faaliyetlerinde elde ettikleri kontrol bilgilerini kurumun kontrol süreçlerini değerlendirirken kullanmak zorundadır.

2200- Görev Planlaması
İç denetçiler, her görev için, amaçları, kapsamı, zamanlama ve kaynak dağılımı hususlarını da dikkate alan ayrı bir plan hazırlamak ve yazılı hale getirmek zorundadır.

2201- Görev planlanırken, denetlenecek faaliyetin hedefleri, performans kontrol araçları, potansiyel riskleri ve bunların yönetim araçları, yönetişim, risk kontrol süreçlerinin etkinliği ve gelişimi sağlama potansiyeli dikkate alınmak zorundadır.
2201.A1- Kurum dışındaki taraflara yapılan görev dağılımlarında ilgili taraflarla yazılı anlaşma yapılması zorunludur.
2201.C1- İç denetçiler danışmanlık faaliyetlerinde, görevlendirmenin amaç, kapsam ve müşteri beklentileri açısından müşterisi ile anlaşmak, önemli görevlerde bunu yazılı yapmak zorundadır.
2210- Amaçlar her bir görev için belirlenmek zorundadır.
2210.A1- Görev amaçları belirlenirken, denetlenen faaliyetle ilgili ön risk değerlendirmesi dikkate alınmak zorundadır
2210.A2- Görev amaçları belirlenirken, denetlenen faaliyetle ilgili suistimal ve aykırılıkların olasılığı dikkate alınmalıdır.
2210.A3- İç denetçiler süreçlerin değerlendirilmesinde kullanılan kıstasların yeterliliğini tespit etmek zorundadır. İç denetçiler uygun değerlendirme kıstasları geliştirmek için yönetim ve/veya yönetim kurulu ile birlikte çalışmak zorundadır.
2210.C1- Danışmanlık görevleri amaçlarında müşteri ile mutabık kalındığı ölçüde yönetişim, risk yönetimi ve kontrol süreçlerine temas etmek zorunludur.
2210.C2- Danışmanlık görevi amaçları kurum değer ve amaçları ile uyumlu olmak zorundadır.
2220- Görevin kapsamı, görevin amaçlarını karşılayacak seviyede olmak zorundadır.
2220.A1- Görevin kapsamı maddi varlıkların dikkate alınmasını içermek zorundadır.

EK1: Uluslararası İç Denetim Standartları Özeti (Devamı)

2220.A2- Bir güvence görevi sırasında önemli danışmanlık görevi fırsatları çıkarsa, yazılı bir anlaşma hazırlanmalı, danışmanlık görevi sonuçları danışmanlık standartlarına uygun olarak raporlanmalıdır.
2220.C1- İç denetçiler danışmanlık görevi yaparken görev kapsamı ve amaçlarına yeterince temas edildiğinden emin olmalı, ortaya çıkan ihtirazi kayıtlar müşteri ile tartışılmalıdır.
2220.C2- Danışmanlık görevi sırasında, iç denetçiler, görev amaçları ile uyumlu biçimde kontrolleri ele almak zorundadır.
2230- İç denetçiler görev amaçlarını gerçekleştirmek için uygun ve yeterli kaynakları tespit etmek zorundadır.
2240- İç denetçiler, görev amaçlarına ulaşacak iş programlarını hazırlamak ve dökümante etmek zorundadır.
2240.A1- İş programları, görev sırasında uygulanacak prosedürleri içermek zorundadır. İş programı işe başlamadan önce onaylanmak zorunda olup yapılan değişiklikler için de derhal onay alınması zorunludur.
2240.C1- Danışmanlık görevi iş programlarının şekil ve içeriği görevin niteliğine göre değişebilir.

2300- Görevin Yapılması
İç denetçiler, üstlendikleri görevin hedeflerine ulaşmak için yeterli bilgileri belirlemek, analiz etmek, değerlendirmek ve kayıtlı hale getirmek zorundadır.

2310- İç denetçiler görev amaçlarına ulaşmak için gerekli bilgileri tespit etmek ve tanımlamak zorundadır.
2320- İç denetçiler kanaat ve görev sonuçlarını uygun analiz ve değerlendirmelere dayandırmak zorundadır.
2330- İç denetçiler kanaatleri ve sonuçlarına dayanak teşkil eden bütün verileri dökümante etmek zorundadır.
2330.A1- İç denetim yöneticisi görev kayıtlarına erişimi kontrol etmek zorundadır. Gerektiğinde bu kayıtları kurum dışına vermeden önce üst yönetim ve/veya hukuk danışmanının onayını almak zorundadır.
2330.A2- İç denetim yöneticisi görev kayıtlarının saklanmasına ilişkin esasları belirlemek zorundadır. Bu esaslar kurumun temel ilkelerine ve ilgili mevzuata uygun olmak zorundadır.
2330.C1- İç denetim yöneticisi danışmanlık görev kayıtlarının saklanması ve paylaşılması konularında politikalar belirlemek zorundadır. Bu politikalar kurum düzenlemeleri ve ilgili mevzuata uygun olmalıdır.
2340- Görevler; görev amaçlarına ulaşılmasını, kalitenin güvence altına alınmasını, ve personelin geliştirilmesini sağlayacak tarzda gözetlenmek ve kontrol edilmek zorundadır.

2400- Sonuçların Raporlanması
İç denetçiler görev sonuçlarını raporlamak zorundadır.

2410- Raporlamalar, sonuçlar, tavsiyeler, eylem planları, görev hedefleri ve kapsamını içermek zorundadır.
2410.A1- Görev sonuçlarının nihai iletişimi, gerekli olduğu yerde iç denetçinin görüşü ve/veya sonuçlarını içermek zorundadır. Sonuçlar, yeterli, güvenilir, ilgili ve yararlı bilgi ile desteklenmelidir.
2410.A2- İç denetçiler görev raporlarında başarılı performansı da göstermeye teşvik edilir.
2410.A3- Görev sonuçları kurum dışı ile paylaşılırken, bu bildirim sonuçların kullanımı ile ilgili sınırlamaları içermek zorundadır.
2410.C1- İlerlemenin ve danışmanlık görev sonuçlarının raporlanmasının şekil ve içeriği görev niteliği ve müşteri ihtiyaçlarına göre değişir.
2420- Raporlamalar, doğru, objektif, açık, özlü, yapıcı, tam olmak ve zamanında sunulmak zorundadır.
2421- Nihai raporlama önemli bir hata veya eksiklik içeriyorsa, iç denetim yöneticisi düzeltilmiş bilgileri tüm taraflara iletmek zorundadır.
2430- İç denetçiler, yalnızca kalite güvence ve geliştirme programı sonuçları desteklerse, görevlerinin "Uluslararası İç Denetim Mesleki Uygulama Standartlarına Uygun Olarak" yapıldığına raporlarında yer verebilirler.
2431- İç Denetimin Tanımına, Etik Kurallara veya Standartlara aykırılık belli bir görevi etkilediğinde, görev sonuçları raporlanırken aykırılığın açıklanması zorunludur.
2440- İç denetim yöneticisi, görev sonuçlarını uygun taraflara dağıtmak zorundadır.
2440.A1- Taraflara görev sonuçlarının raporlanmasından iç denetim yöneticisi sorumludur.
2440.A2- İç denetim yöneticisi aksi kanunlarda emredilmediği taktirde görev sonuçlarının kurum dışındaki paylaşımını kurumun ilgili organlarıyla istişare etmek ve sonuçların raporlanmasını kısıtlayarak kontrol etmek zorundadır.
2440.C1- İç denetim yöneticisi danışmanlık görevlerinin sonuçlarının müşterilere raporlanmasından sorumludur.
2440.C2- Danışmanlık görevleri sırasında tespit edilen sorunlar kurum için önemli hale gelir gelmez üst yönetime ve yönetim kuruluna bildirilmek zorundadır.
2450- Bir genel görüş yayınlanırken, üst yönetim, yönetim kurulu ve diğer paydaşların beklentilerinin dikkate alınması ve yeterli, güvenilir, ilgili ve yararlı bilgi ile desteklenmesi zorunludur.

2500-İlerlemenin Gözlenmesi
İç denetim yöneticisi, yönetime rapor edilen sonuçların akıbetinin gözlenmesi için bir sistem kurmak ve uygulamak zorundadır.

2500.A1- İç denetim yöneticisi yönetimin aldığı tedbirler ve riski üstlenerek, almadığı tedbirlerle ilgili bir takip sureci kurmak zorundadır.
2500.C1- İç denetim faaliyeti, müşteriyle mutabakatı ölçüsünde danışmanlık görev sonuçlarını gözlemek zorundadır.

2600- Risklerin Kabul edildiğinin İletilmesi
İç denetim yöneticisi, üst yönetimin kurum için kabul edilemeyebilecek bir risk düzeyini üstlenmeyi kabul ettiği sonucuna vardığında, konuyu üst yönetimle tartışmak zorundadır. İç denetim yöneticisi konunun çözümlenmediğine hükmederse, konuyu denetim komitesi ve yönetim kuruluna iletmek zorundadır.