ÖNSÖZ

5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu ile mevzuatımıza giren iç kontrol kavramı; "idarenin amaçlarına, belirlenmiş politikalara ve mevzuata uygun olarak faaliyetlerin etkili, ekonomik ve verimli bir şekilde yürütülmesini, varlık ve kaynakların korunmasını, muhasebe kayıtlarının doğru ve tam olarak tutulmasını, malî bilgi ve yönetim bilgisinin zamanında ve güvenilir olarak üretilmesini sağlamak üzere idare tarafından oluşturulan organizasyon, yöntem ve süreçle iç denetimi kapsayan malî ve diğer kontroller bütünü" olarak tanımlanmaktadır.

İç kontrol; kurumun faaliyetlerinin etkili, ekonomik ve verimliliği, mali raporların güvenilirliği, mevzuata uygunluğu ve varlıkların korunması amaçlarına ulaşılmasına yönelik güvence sağlayan, yöneticiler ve personel tarafından etkilenen bir süreçtir.

5018 sayılı Kanunun 55 inci maddesi uyarınca malî yönetim ve iç kontrol süreçlerine ilişkin standartlar ve yöntemlerin belirlenmesi, geliştirilmesi ve uyumlaştırılması, sistemlerin koordinasyonunun sağlanması ve kamu idarelerine rehberlik hizmeti verilmesi hususlarında Maliye Bakanlığı yetkilendirilmiştir. Bu doğrultuda Maliye Bakanlığı tarafından uluslararası standartlar ve iyi uygulama örnekleri çerçevesinde hazırlanan Kamu İç Kontrol Standartlarında, iç kontrolün; kontrol ortamı, risk değerlendirme, kontrol faaliyetleri, bilgi ve iletişim ile izleme bileşenleri esas alınmıştır.

İç kontrol konusunda uluslar arası standartların ve uygulamaların bilinmesi, sistemin daha iyi anlaşılmasını ve uygulanmasını sağlayacaktır. Bu bağlamda özellikle Avrupa Birliği, Uluslararası Sayıştaylar Birliği (INTOSAI) ve ABD Federal Devleti tarafından kabul edilen iç kontrol standartları çok büyük önem taşımaktadır.

Uluslar arası alanda genel kabul görmüş iç kontrol standartlarını ihtiva eden bu dokümanın, iç kontrol standartları hazırlık çalışmalarında esin kaynağı olması dileğiyle…

STRATEJİ GELİŞTİRME BAŞKANLIĞI

INTOSAI:
Kamu Kesimi İç Kontrol Standartları Rehberi

1992 tarihli INTOSAI İç Kontrol Standartları Kılavuzu*; iç kontrolü tasarlamanın, uygulamaya koymanın ve değerlendirmenin özendirilmesi gerektiği vizyonuna işaret eden standartları yaşayan bir doküman olarak tasarlamıştı. Böyle bir vizyon kılavuzu güncel halde tutmak bakımından sürekli bir çabayı gerektirmektedir.

Uluslararası Sayıştaylar Birliği'nin 17'nci Kongresi'nde (INCOSAI; Seul, 2001) 1992 Kılavuzunu güncelleştirme ihtiyacı şiddetli bir biçimde fark edilip Treadway Komisyonu Sponsor Organizasyonlar Komitesi (Committee on Sponsoring Organisations of the Treadway Commission -COSO) tarafından yayımlanan İç Kontrol -Bütünleşik Çerçevesi'ne güvenilmesi gerektiği kabul edilmiştir. Bunu izleyen etkili çabalar sonucunda Kılavuzun etik değerleri ele alması ve bilişim süreciyle bağlantılı kontrol faaliyetlerinin genel prensipleri hakkında daha fazla bilgi sunması konularında ilave tavsiye kararlan alınmıştır. Güncelleştirilen Kılavuzun bu kararları dikkate alıp iç kontrolla ilgili yeni kavramların anlaşılmasını kolaylaştırması gerekir.

Güncelleştirilen bu Kılavuzun, ayrıca, COSO' nun Teşebbüs Risk Yönetim Çerçevesıı gibi yeni gelişmelerin geçen zaman içinde yarattığı etkiyi kucaklaması bakımından daha iyi ve daha rafine şekilde hazırlanmış yaşayan bir doküman gibi düşünülmesi de gerekir.

Bu güncelleştirme INTOSAI İç Kontrol Standartları Komitesi'nin üyelerinin ortak çabalarının sonucudur. Çalışma Bolivya, Fransa, Macaristan, Litvanya, Holanda, Romanya, İngiltere, Amerika Birleşik Devletleri ve Belçika (Başkan) Sayıştay temsilcileri ile Komite üyeleri arasından oluşturulan özel bir çalışma grubu tarafından koordine edilmiştir.

Yönetim Kurulunun 50'nci toplantısında (Viyana, Kasım 2002) Kılavuzu güncelleştirmek üzere bir eylem planı sunulmuş ve bu plan kabul edilmiştir. Yönetim Kurulu 51'nci toplantısında (Budapeşte, Kasım 2003) da çalışmanın gidişi hakkında bilgilendirilmiştir. Taslak metin Şubat 2004 tarihinde Brüksel'deki bir komite toplantısında tartışılıp genel olarak kabul edilmiştir. Komite toplantısından sonra nihai metin bütün INTOSAI üyelerine

gönderilmiştir.

Bu metne yöneltilen eleştiriler analiz edilip gerek görülen değişiklikler de ilave edilmiştir.

Projenin tamamlanmasında harcadıkları üstün gayretleri ve işbirliği anlayışları için INTOSAI

İç Kontrol Standartları Komitesi'nin tüm üyelerine teşekkür etmek isterim. Özel çalışma

grubunun tüm üyelerine de teşekkürü bir borç bilirim.

Kamu Sektörü İç Kontrol Standartları Rehberi 2004 Budapeşte'deki 18'nci Kongre

(INCOSAI) toplantısında onaya sunulmuştur.

Franki VANSTAPEL

Belçika Sayıştayı Genel Sekreteri

INTOSAI İç Kontrol Standartları Komitesi Başkanı

Giriş

INCOSAI, iç kontrol alanındaki bütün önemli ve en son gelişmeleri hesaba katarak 2001 yılında, INTOSAI iç kontrol standartları rehberini güncelleştirme ve bu rehberde sözü edilen COSO İç Kontrol- Bütünleşik Çerçeve başlıklı rapor konseptiyle bütünleştirme kararı aldı.

Komite, bu Rehberdeki COSO modelini uygulamaya koymak suretiyle, sadece, iç kontrol kavramını, güncelleştirmeyi amaçlamamakta, aynı zamanda Sayıştaylar arasında ortak bir iç kontrol konsepti geliştirmeye de çalışmaktadır. Bu doküman, kuşkusuz, kamu sektörünün karakteristik özelliklerini hesaba katmaktadır. Bu durum Komiteyi kimi ilave konu başlıkları ve değişiklikleri dikkate almaya yöneltmiştir.

COSO'nun tanımlaması ve 1992 kılavuzunun karşılaştırmasına, faaliyetlerin etik cephesi ilave edilmiştir. Doksanlı yıllardan bu yana, kamu sektöründeki sahteciliğin ve yolsuzluğun önlenmesi ve ortaya çıkarılması kadar, etik tutum ve davranışların öneminin daha fazla vurgulanması iç kontrol hedeferinin içeriğini haklı çıkarmaktadır. Genel beklentiler kamu görevlilerinin kamu çıkarı için dürüst ve haktanır biçimde hizmet vermesi ve kamu kaynaklarını düzgün bir biçimde yönetmesi gerektiği yönündedir. Vatandaşların kanunlara uygunluk ve adalet temelinde önyargısız olarak muamele görmesi gerekir. Bu nedenle. kamusal etik değerler bir önkoşul olmalı ve desteklenmelidir; kamuya duyulan güven iyi yönetişimin kilit taşıdır.

Kamu sektöründeki kaynakların genellikle, kamu parası olarak ifade edilmesinden ve kamu yararına kullanmanın, çoğunlukla, özel itina gerektirmesinden dolayı, kamu sektörü kaynaklarının korunmasının vurgulanması gerekir. Ayrıca, nakit esasına göre tutulan bütçe muhasebesi halen kamu sektöründe geniş çapta uygulanmakla birlikte, kaynakların elde edilmesi, kullanılması ve elden çıkarılması bakımından yeterli güvenceyi sağlayamamaktadır. Bunun sonucunda, kamu sektöründeki organizasyonlarda, her zaman varlıkların tümünü gösteren güncel bir kayıt bulunmamakta ve bu durum onları saldırıya daha çok açık hale getirmektedir. Bu sebeple, kaynakların korunması, önemli bir iç kontrol hedefi olarak değerlendirilmişti.

İç kontrol 1992 yılında, finansal kontrol ve bununla bağlantılı idari kontrolün geleneksel bakış açısıyla tam olarak sınırlandırılmadığından ve daha kapsamlı yönetim kontrolü kavramını tam olarak içermediğinden, bu doküman, finansal olmayan bilgilerin önemine, ayrıca, vurgu yapmaktadır.

Kamu organizasyonlarının tümünde bilişim sistemlerinin yoğun biçimde kullanılmasından dolayı, bu Rehberde ayrı bir paragrafta ele alınan bilişim teknolojisi kontrolleri giderek önemli hale gelmiştir. Bilişim teknolojisi kontrolleri; kontrol ortamı, risk değerlendirmesi, kontrol faaliyetleri, bilgi ve iletişim, keza, izleme dahil olmak üzere, bir kurumun iç kontrol sürecinin her bir unsuruyla bağlantılıdır. Ancak bunlar, Rehberin sunum amaçları bakımından "Kontrol Faaliyetleri" adı altında irdelenmektedir.

Komitenin nihaî amacı kamu sektöründe etkili iç kontrolün tesis edilmesine ve bunun sürdürülmesine rehberlik etmektir. Bu nedenle, kamu yönetimi (government management), rehberin önemli bir yararlanıcısıdır. kamu yönetimi, bu rehberden kendi organizasyonlarında iç kontrolü geliştirme ve uygulamaya koyma temelinde yararlanabilir.

Kamu denetiminde; iç kontrolün değerlendirilmesi genel kabul görmüş bir çalışma standardı olduğundan, denetçiler bu Rehberden bir denetim gereci olarak yararlanabilirler. COSO Modelini ihtiva eden iç kontrol standartları, bu nedenle, hem devlet yönetimi tarafından organizasyonlarının güçlü iç kontrol yapısı bakımından bir örnek, hem de denetçiler tarafından iç kontrolü değerlendirme bakımından bir gereç olarak kullanılabilir. Ancak bu Rehber INTOSAI Denetim Standartlarını veya diğer ilgili denetim standartlarını desteklemek amacıyla tasarlanmamıştır.

Bu doküman kamu sektöründe iç kontrol için tavsiye edilmiş bir çerçeveyi tanımlayıp değerlendirilebilmesi açısından da bir temel oluşturur. Bu yaklaşım bir organizasyonun faaliyetlerinin bütün cepheleri için geçerlidir. Ancak, düzenleyici mevzuatı geliştirme, kural koyma ya da bir organizasyonda takdire dayalı diğer politika oluşturmayla ilgilenen ve yetkisi usulüne uygun biçimde devredilmiş olan makamı sınırlaması ya da onu engellemesi düşünülemez.

Kamu kesimindeki organizasyonlarda iç kontrol bu organizasyonların spesifik özellikleri bağlamında yorumlanmalıdır; örneğin, üzerine odaklandıkları sosyal veya politik hedefer; kullandıkları kamu fonları; bütçe çevriminin önemi; performanslarının karmaşıklığı (bu kanunlara uygunluk, güvenilirlik ve şeffafık gibi geleneksel değerler ile verimlilik ve etkinlik gibi modern yönetsel değer arasında denge sağlanması anlamına gelmektedir); ve kamusal hesap verme sorumluluklarının geniş kapsamıyla bağlantılı biçimde.

Son olarak, bu dokümanın açıkça, standartlara yönelik rehberliği kapsadığını belirtmek gerekir. Bu rehber iç kontrolün geliştirilmesine yönelik ayrıntılı politikalar, prosedürler ve uygulamalar tesis etmez, bununla birlikte, kurumların içinde bu türden kontrolleri oluşturabilecekleri oldukça geniş bir çerçeve çizer. Komite, açıktır ki, bu standartları uygulatmak konumunda değildir.

Bu Dokümanın Yapısı

İlk bölümde, iç kontrol kavramı tanımlanmakta ve kapsamı ayrıntılı biçimde açıklanmaktadır. Ayrıca, iç kontrolun sınırlılığına dikkat çekilmektedir. İkinci bölümde iç kontrolun unsurları sunulup irdelenmektedir. Doküman roller ve sorumluluklarla ilgili üçüncü bölümle sona ermektedir.

Her bölümde, ana prensipler, önce, gölgeli metin kutularında özlü biçimde gösterilmekte, daha sonra etraflıca bilgi verilmektedir. Eklerde görüleceği üzere, kaynaklar da somut örneklerle gösterilmektedir. Bu dokümana, ayrıca, en önemli teknik terimleri ihtiva eden bir sözlükçe de eklenmiştir.[1]

Sözü edilen grup spesifik olarak faaliyetleri yürüten personel değildir. Faaliyetleri yürüten personel iç kontroldan ve kontrolün yaşama geçirilmesinde önemli rol oynayan önlemlerin alınmasından etkilenmesine rağmen, bunların, yönetimde (yönetici) olmadıkça, bir organizasyonun iç kontrol sistemiyle bağlantılı bütün faaliyetlerinden nihaî sorumlulukları bulunmaz. Rehberin 3 Bölümünde spesifik roller ve sorumluluklar tanımlanmaktadır.

1. İç Kontrol

1.1 Tanım

İç kontrol; bir kurumun yönetimi ve personeli tarafından hayata geçirilen tamamlayıcı bir süreç olup aşağıda sıralanan hedefleri gerçekleştirmek suretiyle; kurumun misyonunu başarması için riskleri göğüslemek ve makul bir güvence sağlamak üzere tasarlanmıştır:

• Faaliyetleri düzenli, ahlak kurallarına uygun, ekonomik, verimli ve etkin biçimde gerçekleştirme;

• Hesapverme sorumluluğunun gerektirdiği yükümlülükleri yerine getirme;

• Yürürlükteki yasalara ve yönetmeliklere uyma;

• Kayıplara, kötü kullanıma ve hasarlara karşı kaynakları koruma.

İç kontrol, bir organizasyonun karşı karşıya kaldığı değişimlere sürekli bir biçimde uyum gösteren dinamik ve tamamlayıcı bir süreçtir. Yönetim ve her düzeydeki personel kurumun misyonunu ve genel hedeflerini başarması için riskleri karşılayan ve makul güvence sağlayan bu sürece müdahil olmak durumundadır.

Tamamlayıcı Bir Süreç

İç kontrol tek bir olay ya da tek bir durum olmayıp bir kurumun faaliyetlerinin içine nüfuz eden bir dizi eylemdir. Bu eylemler bir kurumun faaliyetleri boyunca süreklilik temelinde meydana gelir. Yönetimin organizasyonu çalıştırma tarzına sinmiş olup bünyeseldir. Bu yüzden iç kontrol, iç kontrola bir kurumun faaliyetlerine ilave edilmiş bir şey ya da zorunlu bir yük olarak bakan kimi gözlemcilerin bakış açısından farklıdır. İç kontrol sistemi kurumun faaliyetlerine sıkıca bağlanmış olup kurumun alt yapısı içine yerleştirildiğinde çok fazla etkilidir ve o organizasyonun temelinin ayrılmaz bir parçasıdır.

İç kontrol; faaliyetlere ek olarak tesis edilmek yerine, onların içine, ayrılmaz bir parça olarak yerleştirilmelidir. İç kontrol organizasyonun bünyesine gömülü olarak inşa edilerek, planlama, uygulama ve izleme gibi temel yönetim süreçlerinin bir parçası olur ve bu süreçlerin tamamlayıcısı haline gelir.

Organizasyonun içine tesis edilmiş olan iç kontrolün maliyeti artırma bakımından önemli etkileri de vardır. Mevcut prosedürlerden ayrı yeni kontrol prosedürleri eklenmesi maliyetleri arttırır. Mevcut faaliyetlere ve etkili iç kontrolün katkısına odaklanmak ve kontrolleri sürdürülen temel faaliyetlerle bütünleştirmek suretiyle, bir organizasyon, çoğunlukla, gereksiz prosedürleri ve maliyetleri azaltabilir.

Yönetim ve Diğer Personel Tarafından Hayata Geçirilme

İç kontrolü çalıştıranlar kişilerdir. Bu, yaptıkları ve söyledikleriyle, organizasyonun içindeki kişilerle başarılın Sonuçta, iç kontrol kişiler tarafından hayata geçirilir. Kişiler rollerini ve sorumluluklarını, yetkilerinin sınırlarını bilmelidirler. Bu kavramın önemine binaen, konuya ayrı bir bölüm (üçüncü bölüm) ayrılmıştır.

Bir organizasyonun çalışanları yönetim ve diğer personelden oluşur. Yönetim, esas itibariyle gözetimi sağlamakla birlikte, kurumun hedeferini de belirler ve iç kontrol sisteminin tümünden sorumludur. İç kontrol kurumun hedeferi bağlamında riskleri kavrayabilmek üzere gerekli mekanizmaları oluşturduğundan, yönetim iç kontrol faaliyetlerini uygulamaya koyacak, bunları izleyip değerlendirecektir. İç kontrolün uygulanması önemli yönetim inisiyatifini ve yönetimle diğer personel arasında yoğun bir iletişimi gerektirir. Bu nedenle, iç kontrol yönetimin yararlandığı bir araçtır ve kurumun hedeferiyle doğrudan bağlantılıdır. O kadar ki, yönetim iç kontrolün önemli bir unsurudur. Ancak, organizasyon içindeki bütün personel iç kontrolün oluşmasında önemli rol oynar.

Benzer şekilde, iç kontrol insan doğasından etkilenir. İç kontrol rehberi; bireylerin her zaman her şeyi kavrayamayacağı, iletişim kuramayacağı veya rolünü sürekli bir biçimde oynayamayacağı gerçeğinin farkındadır. Her birey iş yerine benzersiz bilgi ve teknik yetenek sunar ve farklı ihtiyaçlara ve önceliklere sahiptir. Bu gerçekler iç kontrolü etkiler ve iç kontroldan etkilenir.

Kurum misyonunun peşinde olma

Her bir organizasyon esasen kendi misyonunu yerine getirmekle uğraşır. Kurumlar bir amaç için vardır -kamu sektörü genellikle bir hizmetin sunumu ve kamu yararına faydalı bir çıktı ile ilgilidir.

Riskleri karşılama

Misyon ne olursa olsun, bunun başarılmasında çok sayıda riskle karşı karşıya kalınacaktır. Yönetimin görevi, kurumun misyonunu gerçekleştirme olasılığını maksimize etmek üzere bu riskleri belirlemek ve bunlara çözüm bulmaktır. İç kontrol bu risklerin ortadan kaldırılmasına yardımcı olabilirse de, misyonun yerine getirilmesi ve genel hedeferin gerçekleştirilmesi konusunda sadece makul güvence oluşturur.

Makul güvence sağlama

İç kontrol ne kadar iyi tasarlanırsa tasarlansın ve ne kadar iyi işlerse işlesin, genel hedeferin gerçekleştirilmesi konusunda yönetime mutlak güvence veremez. Bunun yerine, rehber yalnızca "makul" bir güvence düzeyini erişilebilir kabul eder.

Maliyet, fayda ve risk konuları dikkate alındığında, makul güvence, tatminkar bir güven düzeyidir. Güvencenin ne kadar makul olduğunun belirlenmesi muhakeme gerektirir.

Yöneticiler, bu muhakemeyi yaparken, faaliyetlerindeki risklerin yapısını ve değişen durumlara göre riskin kabuledilebilir düzeylerini belirlemeli ve riskleri hem nicel hem de nitel olarak değerlendirmelidirler.

Makul güvence, belirsizliği ve riski kimsenin kesinlikle öngöremediği ve gelecekle bağlantılı bir kavramı ifade eder. Keza, organizasyonun kontrolü veya etkisi dışındaki faktörlerin onun hedeferini gerçekleştirme kapasitesini etkileyebilmesidir. Sınırlamalar da şu tür durumlara sebep olabilir: karar almada insan muhakemesi yanılabilir; basit hatalar veya yanlışlıklar yüzünden krizler meydana gelebilir; iki ya da daha fazla kişinin gizlice anlaşmasıyla kontroldan kaçınılabilir. Yahut da yönetim iç kontrol sistemini önemsemeyebilir. Bunlara ek olarak iç kontrol sisteminden verilen tavizler kontrollerın bir maliyeti olduğu gerçeğine işaret eder. Bu tür sınırlamalar yönetimi hedeferin gerçekleşmesine için mutlak güvence oluşturmaktan alıkoyar.

Makul güvence; iç kontrolün maliyetinin ondan elde edilen yararı aşmaması gerektiği şeklinde tanımlanır. Risklere yanıt verme ve kontrolleı tesis etme hususlarında karar alınırken kontrol maliyetlerinin ve onun yararlarının göz önünde bulundurulması gerekir. Maliyet; belirlenen bir amacın gerçekleştirilmesinde tüketilen kaynakların finansal miktarını ve faaliyetlerdeki bir gecikme, hizmet seviyesindeki veya üretkenliğindeki bir düşüş yahut da çalışanların moral eksikliği türünden yitirilen bir fırsatın ekonomik sınırını gösterir. Yarar ise beyan edilmiş bir hedefin başarılma riskini azaltma derecesine göre ölçülür. Sahteciliği, israfı, kötüye kullanmayı veya hatayı ortaya çıkarma olasılığını arttırma, ahlaka aykırı bir faaliyetin önlenmesi veya kurallara uygunluğun pekiştirilmesi örnekler arasında sayılabilir.

Riskleri kabul edilebilir bir düzeye indirmesine rağmen maliyeti ehven iç kontrollerın tasarlanması, yöneticilerin gerçekleştirilmesi gereken genel hedeferi açık ve net bir biçimde anlamalarını gerektirir. Başka bir deyişle, kamu yöneticileri faaliyetlerinin bir alanındaki sistemlerini, başka faaliyetlerini olumsuz biçimde etkileyecek şekildeki aşırı kontrollerla tasarlayabilirler. Örneğin; çalışanlar külfet getiren prosedürleri baypas etmeye çalışabilirler; verimsiz faaliyetler gecikmelere yol açabilir; aşırı prosedürler çalışanların yaratıcılığını ve problem çözmesini önleyebilir veya fayda yaratacak hizmetlerin vaktindeliğine, maliyetine veya kalitesine gölge düşürebilir. Bu nedenle, tek bir alandaki aşırı kontroldan elde edilecek yararlar diğer faaliyetlerdeki artan maliyetler dolayısıyla dengesizlik yaratabilir.

Bununla birlikte, nitel hususlar da dikkate alınmalıdır.

Örneğin; ücretler, harcırahlar ve ağırlama masraşarı türünden yüksek riskli/düşük parasal miktarlar içeren işlemler üzerinde uygun kontrollerın bulunması önemli olabilir. Genel yönetim harcamaları ile alakalı parasal tutarlar üzerindeki uygun kontroller aşırı maliyetli görünebilirse de, bunlar yönetimlerdeki ve ilgili kuruluşlardaki kamusal güvenilirliğinin sürdürülmesi bakımından kritik önemde olabilir.

Hedeflere ulaşma

İç kontrol; genel hedeflerin ayrı ayrı değil, birbirlerine bağlı bir dizi olarak başarılmasına elverişli biçimde düzenlenir. Bu genel hedefler çok sayıda spesifik alt hedefler, fonksiyonlar, süreçler ve faaliyetler aracılığıyla gerçekleştirilir.

Bu genel hedefer şunlardır:

•*Faaliyetleri düzenli, ahlak kurallarına uygun, ekonomik, verimli ve etkin biçimde icra etme*

Kurumun faaliyetleri düzenli, ahlak kurallarına uygun, ekonomik, verimli ve etkin biçimde olmalıdır. Bunların organizasyonun misyonuyla uyum içerisinde olması gerekir.

Düzenli biçimde icra etme iyi organize olmuş bir tarzda ve metodik biçimde çalışma demektir.

Ahlak kurallarına uyma moral prensiplerle bağlantılıdır. Ahlakî davranış kurallarının önemine ve kamu sektöründe sahteciliği ve yolsuzluğu önlemeye ve ortaya çıkarmaya doksanlı yıllardan bu yana daha fazla vurgu yapılmaktadır. Genel beklentiler kamu görevlilerinin kamu çıkarına uygun biçimde hizmet etmesi ve kamu kaynaklarını düzgün biçimde yönetmesi yönündedir. Vatandaşların kanunlara uygunluk ve hakkaniyet temelinde tarafsız muamele görmesi gerekir. Bu nedenle, kamusal etik değerler bir ön koşul olmalı ve desteklenmelidir; kamuya duyulan güven iyi yönetişimin kilit taşıdır.

Ekonomik olma; savurgan olmama veya lüks harcama yapmama anlamına gelir. Kaynakların doğru miktarda, uygun kalitede elde edilip en düşük maliyetle, doğru zaman ve yerde sunulmasıdır.

Verimli olma; hedefleri başarmak için kullanılan kaynaklar ile üretilen çıktılar arasındaki ilişkiyi ifade eder. Belirli kalitede ve miktarda çıktıyı elde etmek üzere minimum kaynak girdisi kullanmak ya da belirli kalite ve miktarda kaynak girdisiyle maksimum çıktı üretmek anlamına gelir.

Etkin olma; hedeflerin başarıyla yerine getirilmesini ya da bir faaliyetin sonuçlarının hedefi karşılama derecesini veya o faaliyetin yaratmak istediği etkileri ifade eder.

•*Hesapverme sorumluluğunun gerektirdiği yükümlülüklerini yerine getirme*

Hesapverme sorumluluğu; kamu hizmeti veren organizasyonlarının ve onun bünyesinde görev yapan kişilerin, kamu fonlarının çekip çevrilmesi, kurallara uygunluğu ve performansın bütün boyutları dahil, aldıkları kararlardan ve eylemlerinden sorumlu tutuldukları süreçtir.

Bu sorumluluk güvenilir ve uygun finansal ve finansal olmayan bilgilerin hazırlanması, muhafaza edilmesi ve bunlardan yararlanılması suretiyle ve bu bilgilerin gereken zamanlarda doğru ve tarafsız biçimde, kurum dışı ve içi paydaşlara raporlar aracılığıyla açıklanmasıyla gerçekleştirilir.

Finansal olmayan bilgiler politikaların ve faaliyetlerin ekonomikliği, verimliliği ve etkinliği ile bağlantılı (performans bilgisi) ve iç kontrol ve onun etkinliğiyle ilgili olabilir.

• *Yürürlükteki yasalara ve yönetmeliklere uyma*

Organizasyonların çok sayıda yasaya ve yönetmeliğe uyması gerekir. Kamu organizasyonlarında, yasalar ve yönetmelikler, kamu parasının elde edilme, harcanma ve ödenme tarzını düzenler. Bütçe Yasası, uluslararası anlaşmalar, idarenin düzgün çalışması ile ilgili yasalar, muhasebeyle ilgili yasalar/standartlar, çevre koruması ve medeni haklar yasası, gelir vergi yönetmelikleri, sahtecilik ve yolsuzluğa karşı yasalar örnek olarak sayılabilir.

•*İsraf, suiistimal, kötü yönetim, hatalı uygulamalar, sahtecilik ve mevzuata aykırılıklar yüzünden meydana gelen kayıplara, kötüye kullanmaya ve hasara karşı kaynakları koruma.*

Dördüncü genel hedefin ilkinin (düzenli, ahlak kurallarına uygun, verimli, ekonomik ve etkin faaliyette bulunma) bir alt kategorisi olarak kabul edilmesine rağmen, kamu sektöründe kaynakları korumanın önemine vurgu yapılması gerekir. Bu husus, kamu kesimindeki kaynakların genellikle kamu parasıyla ilgili olması ve kamu çıkarları doğrultusunda kullanımlarının özel itina gerektirmesi gerçeğine dayanır. Ayrıca, kamu sektöründe hâlâ yaygın bir biçimde kullanılan nakit esasına dayalı bütçe muhasebesi kaynakların elde edilmesi, kullanılması ve elden çıkarılması konusunda yeterli güvence sağlayamaz. Sonuç olarak, kamu kesimindeki organizasyonlarda varlıkların tümünün güncel kayıtları her zaman bulunamaz ve bu onları saldırıya çok açık hale getirir. Bu nedenle, kontroller kurum kaynaklarının elde edilmesinden elden çıkarılmasına kadar yönetilmesi ile bağlantılı faaliyetlerin her birinin içine yerleştirilmiş olmalıdır.

Hükümet faaliyetlerinin şeffaflığını ve hesapverme sorumluluğunu gerçekleştirmenin anahtarı olan bilgiler, başvuru dokümanları ve muhasebe kayıtları gibi diğer kaynakların muhafaza edilmesi gerekir. Bunlar da çalınma, kötüye kullanılma veya tahrip edilme tehlikesiyle karşı karşıyadır.

Hatta birtakım kaynakların ve kayıtların korunması bilgisayar sistemlerinin ortaya çıkışından bu yana giderek önem kazanmıştır. Korunmak için özen gösterilmediği takdirde, bilgisayar ortamında saklanan hassas bilgiler tahrip olabilir ya da kopyalanıp dağıtılabilir yahut da suiistimal edilebilir.

İç Kontrolün Etkinliği ile İlgili Sınırlar

İç kontrol; önceki bölümde tanımlanan genel hedeferin gerçekleştirilmesini kendi kendine sağlayamaz.

Etkin bir iç kontrol sistemi, ne kadar iyi tasarlanırsa tasarlansın ve ne kadar iyi işlerse işlesin, kurum hedeferini gerçekleştirmesi veya kurumun varlığını sürdürmesi konusunda, yönetime sadece makul -mutlak değil- güvence sağlayabilir. hedeferin başarılması doğrultusunda, yönetime kurum gelişimi veya yetersizliği hakkında bilgi verebilir. Ancak iç

kontrol kötü yönetimi kendiliğinden iyi bir yönetime dönüştüremez. Dahası, hükümet politikası ve programlarındaki, demografik veya ekonomik koşullardaki yön değiştirmeler belirgin biçimde yönetim kontrolünün sınırları dışında olup yöneticilerin kontrolleri yeniden tasarlamasını veya kabul edilebilir risk düzeyini bu duruma göre ayarlamasını gerektirebilir.

Etkin bir iç kontrol sistemi hedeferi başaramama olasılığını azaltır. Bununla birlikte, iç kontrolün yanlış tasarlanması ve istenilen şekilde işlememesi riski her zaman mevcuttur.

İç kontrol, *insan faktörüne* bağlı olması dolayısıyla, tasarım kusurları, muhakeme veya yorum hataları, yanlış anlama, özensizlik, aşırı yorgunluk, dikkat dağınıklığı, gizli anlaşma, suiistimal veya umursamazlığa maruz kalabilir.

Sınırlayıcı bir başka faktör iç kontrol sisteminin tasarımının kaynak kısıtlamalarıyla karşı karşıya kalmasıdır. kontrollerın yararları, bu nedenle, maliyetlerine göre düşünülmelidir.

Kayıp riskini tamamen ortadan kaldıran bir iç kontrol sisteminin sürdürülmesi gerçekçi olamaz, muhtemeldir ki, bu elde edilen yararı haklı gösterecek olandan çok daha maliyetli olacaktır. Özel bir kontrol tesisinin gerekip gerekmeyeceğini, risk oluşma ihtimalini ve kurumda yaratacağı potansiyel etkiyi yeni bir kontrol kurmanın maliyetleri ile bir arada dikkate almak gerekir.

Organizasyonel değişiklikler ve *yönetimin tutumu* iç kontrolün etkinliği ve sistemi çalıştıran personeli derinden etkiler. Yönetimin, bu nedenle, kontrolleri süreklilik temelinde gözden geçirmesi ve güncelleştirmesi, değişiklikleri personele duyurması ve kontrollera uyarak örnek oluşturması gerekir.

1. iç Kontrolün Unsurları

İç kontrol birbiriyle bağlantılı beş unsurdan meydana gelir:

- Kontrol ortamı
    - Risk değerlendirme
    - Kontrol faaliyetleri
    - Bilgi ve iletişim
    - İzleme

İç kontrol; kurumun genel hedeferini gerçekleştirip gerçekleştiremediği konusunda makul güvence elde etmek amacıyla tasarlanır. Bu yüzden etkin bir iç kontrol sürecinin ön şartı hedeferin açık biçimde belirlenmesidir.

Eksiksiz bir iç kontrol sisteminin temeli *kontrol ortamına,* dayanır. Kontrol ortamı iç kontrolün genel kalitesini etkileyen atmosferi yaratmanın yanı sıra iç kontrol disiplinini sağlayıp iç kontrolün temelini oluşturur. Hangi stratejinin ve ne tür amaçların belirleneceği konusunda kontrol ortamının genel bir etkisi vardır ve kontrol faaliyetlerini yapılandırır.

Açık hedefer belirlemek ve etkin bir kontrol ortamı tesis etmek suretiyle, kurum misyonunun ve hedeferinin gerçekleştirilmesine çalışılırken karşılaşılan *riskleri değerlendirme*

bu risklere uygun yanıtın geliştirilmesi için bir zemin oluşturur.

Risklerin ortadan kaldırılmasına yönelik ana strateji iç *kontrol faaliyetleri* aracılığıyla gerçekleştirilir. Kontrol faaliyetleri önleyici ve/veya ortaya çıkarıcı mahiyette olabilir. hedeferi gerçekleştirmek için iç kontrol faaliyetlerinin tamamlayıcı unsuru düzeltici önlemlerdir. Kontrol faaliyetlerinin ve düzeltici önlemlerin maliyetleri bunlardan sağlanacak yararlarla orantılı olmalıdır (maliyet etkinliği).

Etkin *bilgi ve iletişim* bir kurumun işgörmesi ve faaliyetlerini kontrol etmesi için yaşamsal önemdedir. Kurum yönetimi kurum içi işler için olduğu kadar kurum dışı işlerle bağlantılı olarak uygun, eksiksiz, güvenilir, doğru ve vaktinde iletişim kurmaya ihtiyaç duyar. hedeferini gerçekleştirmek için kurumun her kesiminde bilgiye ihtiyaç vardır.

Son olarak da, iç kontrol organizasyonun karşı karşıya kaldığı risklere ve değişikliklere sürekli biçimde uyum göstermesi gereken dinamik bir süreç olduğundan, iç kontrolün değişen hedefere, ortama, kaynaklara ve risklere ayak uydurmasını sağlamak bakımından iç kontrol sistemini *izlemek* gerekir.

Bu unsurlar kamu kesiminde iç kontrol için tavsiye edilen bir yaklaşımı tanımlayıp iç kontrolun değerlendirilmesi açısından bir temel oluşturur. Bu unsurlar bir organizasyonun faaliyetlerinin tüm cephelerinde kullanılır.

Bu rehber genel bir çerçeve sunmaktadır. Bu unsurlar uygulamaya konduğunda, organizasyonun faaliyetlerine uygun düşecek kapsamlı politikalar, prosedürler ve uygulamalar geliştirmekten, unsurların faaliyetlerin içine yerleştirilmesini ve faaliyetlerin ayrılmaz bir parçası olmasını sağlamaktan yönetim sorumludur.

Hedefler ile Unsurların İlişkisi

Bir kurumun neyi başarmaya çalıştığını gösteren genel hedefler ile bu hedefleri başarması için neye ihtiyaç duyulduğunu gösteren iç kontrol unsurları arasında doğrudan bir bağlantı bulunur. Bu ilişki küp üzerinde üç boyutlu bir matrisle resmedilmiştir.

Dört genel hedef –hesapverme sorumluluğu (raporlama), (yasalara ve yönetmeliklere) uygunluk, (düzenli ahlak kurallarına uygun, ekonomik, verimli ve etkin) faaliyetler ve kaynakları koruma– üç boyutlu matrisin dikey sütunlarında; söz konusu beş unsur yatay sütunlarında ve organizasyon veya kurum ve onun departmanları da yan sütunlarında gösterilmiştir.

Her bir unsurun satırı dört genel hedefi "enlemesine keser" ve bunlara uygulanır. Örneğin, kurum içi ve dışı kaynaklardan üretilen finansal ve finansal olmayan verilere –ki bilgi ve iletişimin unsuru ile bağlantılıdır- faaliyetleri yönetmek, hesapverme sorumluluk amaçlarını raporlayıp yerine getirmek ve yürürlükteki yasalara uymak bakımlarından ihtiyaç duyulur.

Benzer şekilde genel hedeflere bakıldığında, beş unsurun tümü de hedeflerin her biriyle ilgilidir. Faaliyetlerin etkinliği ve verimliliği gibi tek bir hedef ele alındığında, açıktır ki beş unsurun tümü verimliliğin ve etkinliğin gerçekleşmesine uygulanabilir ve bunların başarılması bakımından önemlidir.

İç kontrol sadece bir organizasyonun varlığı ile ilgili olmayıp, aynı zamanda her bir departman için de gereklidir. Bu ilişki organizasyonları, kurumları ve departmanları gösteren üçüncü boyutta gösterilmiştir. Bu itibarla, matris hücrelerinin herhangi birine odaklanabilirsiniz.

İç kontrol çerçevesi bütün organizasyonlara uygun ve uygulanabilir olduğundan, yönetimin iç kontrolu uygulama tarzı büyük ölçüde, kurumun yapısına göre değişecek ve kurumun çok sayıdaki spesifik faktörüne bağlı olacaktır. Bu faktörler arasında organizasyonel yapı, risk profili, çalışma ortamı, kurumun büyüklüğü, karmaşıklığı, faaliyetleri ve düzenlemelerin düzeyi ve bunun gibi faktörler sayılabilir. Yönetim, kurumun spesifik durumunu ele aldığında, iç kontrol çerçevesinin unsurlarını uygulamak üzere yararlanılan süreçlerin ve metodolojilerin karmaşıklığını dikkate alarak bir dizi tercihte bulunur.

Metnin sonraki bölümlerinde yukarıda sözü edilen unsurların her biri ilave yorumlarla birlikte kısaca ele alınmaktadır.

2.1 Kontrol Ortamı

Kontrol ortamını, bir organizasyonun personelinin kontrol bilincini etkileme tarzı belirler. Disiplin sağlayan ve yapı oluşturan kontrol ortamı iç kontrolun bütün diğer unsurlarının esasıdır.
Kontrol ortamının öğeleri:

(1) kişisel ve mesleki dürüstlük, yönetimin ve personelin etik değerleri ve organizasyonun bütününde her zaman iç kontrola yönelik destekleyici bir tavır içinde olma;

(2) uzmanlığa adanmış olma;

(3) "üst yönetimin tavrı" (örneğin, yönetimin felsefesi ve iş görme uslubu);

(4) organizasyonel yapı;

(5) insan kaynakları politikaları ve uygulamaları.

Kişisel ve mesleki dürüstlük, yönetimin ve personelin etik değerleri

Kişisel ve mesleki dürüstlük, yönetimin ve personelin etik değerleri onların öncelikleri ve değer yargıları olup, sosyal ve ahlaki standartlara dönüşür. Yönetim ve personel, organizasyonun bütününde, her zaman iç kontrolun gerçekleşmesi için destekleyici bir tavır göstermelidir.

Organizasyonun bünyesindeki ilgili her birey -yöneticiler ve çalışanlar- kişisel ve mesleki dürüstlüğü, etik değerleri sürdürüp sergilemek ve yürürlükteki davranış kurallarına (code of conduct) her zaman uymak durumundadır. Kişisel mali yatırımlarının açıklanması, (seçimle gelmiş görevlilerin ve üst düzey kamu görevlilerinin) kurum dışı konumları ve kabul ettikleri hediyeler ve çıkar çatışmasının bildirilmesi bu davranış kurallarına örnek olarak gösterilebilir.

Ayrıca, kamu kuruluşları da dürüstlüğü ve etik değerleri koruyup sergilemeli; misyonları ve temel değerleri çerçevesinde bunları kamuoyu nezdinde görünür kılmalıdır. Ayrıca, faaliyetleri de etik, düzenli, ekonomik, verimli ve etkin olmalıdır. Kamu kuruluşları misyonları

ile uyumlu hareket etmek durumundadır.

Uzmanlığa adanmış olma

Düzenli, etik, ekonomik, verimli ve etkin performansı sağlayabilmek için ihtiyaç duyulan bilgi ve beceri düzeyi, ayrıca iç kontrolla ilgili kişisel sorumlulukların doğru biçimde anlaşılması uzmanlığa adanmışlığın kapsamı içindedir. Organizasyon içindeki herkes kendi spesifik sorumlulukları bağlamında iç kontrola müdahildir.

Yöneticiler ve çalışanlar iç kontrolü uygun şekilde geliştirmenin, uygulamaya koymanın ve sürdürmenin önemini anlamalarına genel iç kontrol hedeferini ve kurumun misyonunu gerçekleştirmeleri için görevlerini yerine getirmelerine olanak sağlayacak bir uzmanlık düzeyini korumak durumundadırlar.

Bu nedenle, yöneticilerin ve personelinin, riskleri değerlendirmelerine, etkin ve verimli bir performans göstermelerine yetecek gerekli uzmanlık düzeyini ve sorumluluklarını layıkıyla yerine getirmelerini sağlayacak bir iç kontrol anlayışını koruyup sergilemeleri gerekir.

Eğitim verilmesi, örneğin, kamu görevlilerinin iç kontrol hedeferi ve özellikle de etiği ilgilendiren davranışların hedefi konusundaki farkındalıklarını arttırabilir, onların iç kontrol hedeferini anlamalarına ve etik açmazlarla baş etme becerilerini geliştirmelerine yardımcı olur.

Üst Yönetimin Tavrı

"Üst yönetimin tavrı" (örneğin, yönetimin felsefesi ve iş görme üslubu) şunları ifade eder:

•İç kontrolün gerçekleşmesi için her zaman destekleyici bir yaklaşım, bağımsızlık, uzmanlık ve örnek vererek yönlendirme,

•Yönetim tarafından belirlenen bir davranış kuralları bütünü, fikir danışma ve iç kontrol hedeferini ve özellikle de etik davranışlarla ilgili olanları özendiren performans değerlemeleri

Üst yönetimce takınılan tavır yönetimin aldığı önlemlerin her cephesine yansır.

"Üst yönetimin tavrı"nın oluşturulmasında en üst hükümet yetkilisinin ve yasa koyucuların taahhütleri, müdahaleleri ve desteği pozitif yaklaşımı teşvik edici olup organizasyondaki iç kontrola dönük olumlu ve özendirici yaklaşımın sürdürülmesi bakımından yaşamsal önemdedir.

Üst yönetim iç kontrolün önemli olduğuna inandığı takdirde, organizasyondakiler bunu sezer ve oluşturulan kontrollera uyma konusunda bilinçli davranırlar. Örneğin iç kontrol sisteminin parçası olarak bir iç denetim birimi kurulması iç kontrolün önemi konusunda yönetim tarafından verilmiş güçlü bir sinyaldir.

Öte yandan organizasyonun mensupları iç kontrolün üst yönetimce önemli bir mesele olarak görülmediğini ve kontrola anlamlı bir destekten ziyade, sözde destek verildiğini hissederlerse, organizasyonun kontrol hedeferini etkin biçimde gerçekleştiremeyeceği hemen hemen kesin gibidir.

Sonuç olarak, yönetimin etik davranışlar sergileyip bu konuda kararlılık göstermesi iç kontrol hedeferi bakımından yaşamsal önemdedir, özellikle de "etikle ilgili davranışlar"in hedefi bakımından. Yönetim, rolünü oynarken, kendi davranışları aracılığıyla iyi örnek oluşturmalı ve davranışları kabul edilebilir ya da çare olarak sunulandan daha çok, doğru olanı işaret etmelidir. Özellikle de, yönetimin politikaları, prosedürleri ve uygulamaları düzenli, etik, ekonomik, verimli ve etkin davranışları özendirmelidir.

Bununla birlikte, yöneticilerin ve personelin dürüstlüğü, çok sayıda unsurdan etkilenir. Bu nedenle, üst yönetim tarafından yayımlanmış olan geçerli davranış kurallarına tabi yükümlülükleri, düzenli aralıklarla, personele, hatırlatılmalıdır. Fikir danışma ve performans değerlemeleri de önemlidir. Genel performans değerlemeleri, çalışanların rolü dahil, çok sayıda kritik faktörün değerlendirilmesine dayandırılmalıdır.

Bir kurumun organizasyonel yapısını şunlar oluşturur:

- yetki ve sorumluluk dağılımı,
- yaptırımlar ve hesapverme sorumluluğu,
- raporlamaya elverişli hatlar.

Organizasyonel yapı kurumun kilit yetki ve sorumluluk alanlarını tanımlar. Yaptırımlar ve hesapverme sorumluluğu bu yetki ve sorumlulukların organizasyonun genelindeki devir biçimiyle bağlantılıdır. Bir raporlama biçimi düzenlenmeden yaptırımlardan ve hesapverme sorumluluğundan söz edilemez. Bu nedenle, raporlamaya elverişli hatların belirlenmesine ihtiyaç vardır. Yönetimin yasalara aykırılıklara bulaşması gibi, olağanüstü durumlarda raporlamanın başka hatlarının normal hatlara eklenmesi mümkün olabilmelidir.

Yönetimden bağımsız ve organizasyonun bünyesindeki en üst seviyedeki yetkiliye rapor veren bir iç denetim birimi organizasyonel yapıya dahil edilebilir.

Organizasyonel yapı, ayrıca, roller ve sorumluluklarla ilgili üçüncü bölümde de ele alınacaktır.

İnsan kaynakları politikaları ve uygulamaları

İnsan kaynaklan politikaları ve uygulamaları sözleşmeli personel çalıştırma, personel temini, rehberlik etme, personel yetiştirme (formel ve işbaşında), eğitme, değerlendirme, danışma, görevde yükseltme, ücretlendirme ve tazminat vermeyi kapsar.

İç kontrolün en önemli boyutu personeldir. Etkin kontrolün sağlanması için ehil ve güvenilir personele gerek duyulur. Bu yüzden, personel çalıştırma, işe alma, değerlendirme, ücretlendirme ve yükseltme yöntemleri kontrol ortamının önemli bir parçasıdır. Personeli işe alma ve çalıştırma kararları; bu nedenle, kişilerin dürüstlüğünün, görevlerini yerine getirebilmelerine yetecek eğitime ve deneyime sahip olduklarının ve zorunlu formel, işbaşı ve etik eğitim göreceklerinin güvencesini içermelidir. Etkili bir iç kontrol için doğru iç kontrol anlayışına sahip ve sorumluluk almaya istekli yönetici ve çalışanlar yaşamsal önemi haizdir.

İnsan kaynakları yönetimi de profesyonelliği geliştirmek ve günlük uygulamada

şeffaflığı sağlayarak etik bir ortamın özendirilmesinde esaslı bir role sahiptir. Böylece liyakat esasına dayanması gereken işe alma, performans değerleme ve yükselme süreçleri görünür hale gelir.

İşe alma kurallarının ve gerekse boş kadroların yayımlanması suretiyle seçim yapma süreçlerinin açıklığının sağlanması da insan kaynakları yönetiminin etik kurallara uygun biçimde gerçekleşmesine yardımcı olur.

Örnekler

İç kontrolun her hedefi ve her unsuruyla bütünleştirilmiş örnekler için eklere bakınız.

2.2 Risk Değerlendirmesi

Risk değerlendirmesi: kurumun hedeflerini gerçekleştirmesini engelleyen önemli riskleri tespit ve analiz etme, bunlara uygun yanıtlar verilmesini belirleme sürecidir.

Risk değerlendirmesi şu anlama gelir:

(1) Risk tespiti:

- kurum hedefleri ile bağlantılıdır,
- kapsamlıdır,
- hem kurum hem de faaliyet düzeyindeki iç ve dış faktörlere bağlı riskleri içerir.

(2) Risk ölçme:

- riskin değerinin (significance) tahmin edilmesidir,
- riskin meydana gelme olasılığının hesap edilmesidir.

(3) Organizasyonun göğüsleyeceği risk kapasitesini (risk appetite) takdir etme.

(4) Risklere verilecek yanıtları üretme:

- dikkate alınması gereken dört tür yanıt olmalıdır: riskin transferi, riski kabul etme (tolerance), riski azaltma (treatment) veya riski bertaraf etme (termination); etkili bir iç kontrol riski iyileştirmenin temel mekanizması olduğundan bu rehber açısından en uygun olan yanıt riskin azaltılmasıdır.

- uygun kontrollar ortaya çıkarıcı ya da önleyici nitelikte olabilir. Hükümetin ekonominin, sanayinin, düzenleyici kuruluşun ve faaliyetlerin koşulları devamlı olarak değişmekte olduğundan, risk değerlendirmesi süreklilik temelinde tekrarlanan bir süreç olmalıdır. Risk değerlendirmesi değişen koşulları, fırsatları, riskleri tespit ve analiz etmek (risk değerlendirme çevrimi) ve değişen riskleri göğüslemek üzere iç kontrolda değişiklik yapmayı ifade eder.

Tanımında da vurgulandığı üzere, organizasyonun hedeferini gerçekleştirebilmesi konusunda iç kontrol sadece makul güvence verebilir. İç kontrolün bir unsuru olarak risk

değerlendirmesi garantiyi sağlayacak uygun kontrol faaliyetlerinin seçilmesinde kilit rol oynar. İç kontrol kurumun hedeferini gerçekleştirmesini engelleyen riskleri tespit ve analiz etme, bunlara verilecek uygun yanıtları belirleme sürecidir.

Sonuçta, hedeferin belirlenmesi risk değerlendirmesinin önkoşuludur. Yönetim; başarısını engelleyecek riskleri tespit etmeden ve onlarla başetmeye yönelik önlemleri almadan önce hedeferini belirlemelidir. Bu, risklerin etkisini ölçmeye ve bunlara ehven maliyetle karşılık vermeye dönük süreklilik temelinde bir süreci uygulamaya koyma ve muhtemel riskleri tespit edip takdir etmeye elverişli becerilere sahip personel çalıştırma demektir. İç kontrol faaliyetleri; tespit edilen etkinin belirsizliğini kapsayacak şekilde dizayn edildiği taktirde, risklere verilmiş bir yanıttır.

Kamu kuruluşları hizmet sunma ve arzulanan çıktıları elde etme üzerinde etki yaratabilecek risklerle başa çıkabilmek zorundadır.

Risklerin Tespiti

Risk değerlendirmesiyle ilgili stratejik yaklaşım önemli organizasyonel hedefere yönelik risklerin tespit edilmesine dayanır. Bu hedeferle ilgili riskler daha sonra az sayıdaki önemli riskler ortaya çıkarıldığı zaman dikkate alınıp hesaplanır.

Önemli risklerin tespit edilmesi, sadece, risk değerlendirmesindeki kaynaklara tahsis edilmesi gereken en önemli alanları belirlemek amacıyla değil, aynı zamanda bu riskleri yönetme sorumluluğunu dağıtmak bakımından da önemlidir.

Bir kurumun performansı hem kurumsal hem de faaliyet düzeyindeki iç ve dış faktörlere bağlı olarak risk altında olabilir. Risk değerlendirmesi meydana gelebilecek bütün riskleri (yolsuzluk ve sahtecilik riski dahil olmak üzere) dikkate almalıdır. Risk tespitinin kapsamlı olmasının önemi bu yüzdendir. Risk tespiti, süreklilik temelinde ve tekrarlanan bir süreç olup, genellikle planlama süreciyle bütünleştirilir. Riski çoğunlukla, "temiz bir sayfa" yaklaşımıyla irdelemek yararlıdır, risk, sadece, önceki incelemelerle ilişkilendirilemez. Bu tür bir yaklaşım bir organizasyonun ekonomik ve düzenleyici ortamdaki, iç ve dış çalışma şartlarındaki değişikliklerle ve yeni ya da değiştirilmiş hedeferinin açıklanmasıyla ortaya çıkan risk profilindeki değişimlerin tespitini kolaylaştırır.

Risk tespiti için uygun araçları benimsemek gerekir. Yaygın biçimde en fazla yararlanılan araçlardan ikisi risk incelemesi yaptırılması ve risk özdeğerlendirmesidir.

Riski ölçme

Riskle nasıl başa çıkılacağına karar vermek için prensip olarak sadece, belirli bir riskin var olduğunu tespit etmek yetmez, aynı zamanda riskin büyüklüğünü (değerini) hesaplamak (ölçmek) ve riskin meydana gelme ihtimalini değerlendirmek de gerekir. Bazı riskler sayısal olarak teşhise elverişli olmasına rağmen (örneğin; özellikle fınansal riskler) pek çoğunu

nitelendirmek çoğunlukla zor olduğundan (örneğin; saygınlık riski), riskleri analiz etme metodolojileri farklılık gösterir. Sözü edilen bu ikinci risk, sübjektif bir bakışla daha çok sadece bir ihtimaldir. Bu açıdan risk ölçme bir bilim olmaktan çok bir sanattır. Bununla birlikte, sistematik risk derecelendirme kriterinden yararlanmak sürekli bir biçimde yapılacak değerlendirmeler için bir çerçeve sağlamak suretiyle sürecin öznelliğini hafişetir.

Risk ölçümünün önemli amaçlarından biri önlem alınması gereken ve nispeten öncelikli risk alanları konusunda yönetimi bilgilendirmektir. Bu nedenle, çoğunlukla, bütün risklerin yüksek, orta ve düşük olmak üzere sınışandıran bazı çerçeveler geliştirmek gerekir. Aslında net bir biçimde birbirinden ayrılamayan kategorilere aşırı eklemeler yapmak yapay ayrımlara yol açacağından, genellikle, kategorileri asgaride tutmak yerinde olur.

Bu tür ölçümler sayesinde, yönetim önceliklerini ve karşılık verilmesi gerekenleri (örneğin, potansiyel etkisi büyük ve meydana gelme olasılığı yüksek olanları) belirlemek suretiyle yönetimin vereceği kararlar için riskler derecelendirilebilir.

Organizasyonun göğüsleyeceği "risk kapasitesi"ni takdir etme

Riske yanıt verme üzerinde düşünülürken önem arzeden bir husus kurumun göğüsleyeceği risk kapasitesinin ("risk appetite") tespitidir. Risk kapasitesi gerekli önlemi almadan önce kurumun göğüslemeye hazırlandığı risklerin miktarıdır. Riske verilecek yanıtlarla ilgili kararlar, tolere edilebilecek risk miktarının tespitiyle birlikte alınmak durumundadır.

Risk kapasitesini belirlemek amacıyla hem bünyesel risklerin hem de göğüslenemeyen artık (bakiye) risklerin dikkate alınması gerekir. Bünyesel risk bir kurumun ya risk olasılığını ya da riskin etkisini değiştirmek için yönetimce alınabilecek önlemlerin olmadığı risktir. Göğüslenemeyen artık riskler yönetimin riske yanıt vermesinden sonra kalan risktir.

Bir organizasyonun risk kapasitesi risklerin fark edilen önemine göre değişmektedir. Tolere edilebilir finansal zararlar, ilgili bütçe büyüklüğü, zararın kaynağı ya da olumsuz reklam gibi bağlantılı diğer riskler dahil, özelliklerinin kapsamına/sınırlarına bağlı olarak değişiklik gösterir. Risk kapasitesinin tespiti sübjektif bir mesele olmakla birlikte, yine de genel risk stratejisinin formüle edilmesinde önemli bir aşamadır.

Riske verilecek karşılıkları belirleme

Yukarıda ana hatlarıyla belirtilen önlemlerin sonunda organizasyon için bir risk profili oluşturulur. Bir risk profili oluşturulduğu taktirde, organizasyon karşılık verilecek uygun cevap üzerinde düşünebilir.

Riske verilecek cevaplar dört kategoriye ayrılır. Bazı durumlarda, risk transfer edilebilir, tolere edilebilir (kabul edilebilir) ya da bertaraf edilebilir.[8] Ancak, pek çok durumda, risk azaltmak (treatment) durumdadır ve riski kabul edilebilir bir düzeyde tutmak için kurumun etkin bir iç kontrol sistemini uygulama koyup sürdürmesi gerekir.

Riski azaltmanın amacı, riski, mutlaka, yok etmek değildir, daha çok onu kontrol altında tutmaktır. Organizasyonun riski azaltmak üzere belirlediği prosedürlere iç kontrol faaliyetleri

denir. Gerçekleştirilecek uygun kontrol faaliyetlerinin seçiminde risk değerlendirmesi kilit bir rol oynamalıdır. Bütün riskleri ortadan kaldırmanın mümkün olamayacağını ve organizasyonun hedeferini gerçekleştirmesi konusunda iç kontrolün sadece makul güvence sağlayabileceğini, yeniden hatırlatmakta yarar bulunmaktadır.

Ancak, riskleri, aktif bir biçimde tespit edip yöneten kurumlar, işler yanlış gittiğinde hemen karşılık vermeye ve genellikle de, değişikliğe çabuk cevap vermeye, daha hazırlıklı olabilirler.

Bir iç kontrol sistemi dizayn edilirken, belirlenen kontrol faaliyetinin riskle orantılı olması önem arzeder. Arzu edilmeyen en uç sonuç bir yana bırakılırsa, organizasyonun risk kapasitesi içinde bulunan kayıplar için makul bir güvence sağlayan bir kontrolü dizayn etmek, normal koşullarda, yeterlidir. Her kontrolün bir maliyeti vardır ve kontrol faaliyetinin göğüslediği riskle bağlantılı maliyet değerini karşılaması gerekir.

Hükümetin, ekonominin, sanayinin, düzenleyici kuruluşun ve faaliyetlerin koşullan devamlı olarak değişmekte olduğundan, bir organizasyonun risk ortamı sürekli olarak değişir;

hedeflerin öncelikleri ve bunlara eşlik eden risklerin önemi farklı yöne kayıp değişikliğe uğrar. Risk değerlendirmesinin özü değişen koşulları belirlemek ve gerekli önlemleri almak üzere sürekli olarak tekrarlanan bir süreç (risk değerlendirme çevrimi) olmasıdır. Risk profilinin geçerliliğini devam ettirmesini, riske verilecek yanıtların planlandığı şekilde ve orantılı olarak sürmesini ve riskler zaman içinde değiştiğinde, hafifletici kontrolların etkin kalabilmesini güvence altına almak için risk profilleri ve bağlantılı kontrollar periyodik olarak gözden geçirilip üzerlerinde yeniden düşünülmelidir.

Örnekler

İç kontrolun her hedefi ve her unsuruyla bütünleştirilmiş örnekler için eklere bakınız.[2]

2.3 Kontrol Faaliyetleri

Kontrol faaliyetleri riskleri göğüslemek ve kurumun hedeflerini gerçekleştirmek üzere uygulamaya konulan politikalar ve prosedürlerdir. Etkin olmaları için kontrol faaliyetlerinin amaca uygun olması, dönem boyunca planlandığı şekilde sürekli işlev görmesi ve maliyet ehven, kapsamlı, makul ve kontrol hedefleriyle doğrudan bağlantılı olması gerekir.

Kontrol faaliyetleri organizasyonun geneline, bütün kademelere ve tüm fonksiyonlara konulur. Bu faaliyetler arasında aşağıdaki örnekler gibi, ortaya çıkarıcı ve önleyici türden bir dizi kontrol faaliyeti bulunur:

(1) Yetki devri ve onay prosedürleri,

2[8] Bazı risklere verilebilecek en iyi karşılık onları transfer etmektir. Klasik sigorta vasıtasıyla, bir başka biçimde risk almak üzere üçüncü kişilere ödeme yapılmak suretiyle ya da mukaveleye bağlanan şartlar yoluyla transfer yapılabilir. Kimi riskler konusunda bir şeyler yapabilme gücü sınırlıdır veya alınacak herhangi bir önlemin maliyeti elde edilecek muhtemel yarara göre çok fazladır. Böyle durumlarda, riskleri tolere etmek (kabul etmek) bir yanıt olabilir. Bazı riskler, faaliyeti ortadan kaldırmak suretiyle, yalnızca azaltılabilir ya da kabul edilebilir düzeyde tutulabilir. Kamu kesiminde faaliyetleri ortadan kaldırma şansı, özel kesimle kıyaslandığında, çok sınırlı olabilir. Kamu kesiminde, kamu yararı için gerekli olan çıktıyı veya sonucu gerçekleştirebilmenin başka yolu bulunmadığından ve bağlantılı riskler çok büyük olduğundan, faaliyetler gerçekleştirilir.

(2) Görevlerin birbirinden ayrılması (yetkiyi devretme, uygulama, kaydetme,

inceleme),

(3) Kaynaklara ve kayıtlara erişim yetkisi üzerindeki kontrollar,

(4) Teyitler,

(5) Mutabakatlar,

(6) İşgörme performansına yönelik incelemeler,

(7) Faaliyetler, süreçler ve eylemler ilgili incelemeler,

(8) Gözetim (görevlendirme, gözden geçirme ve onay verme, yönlendirme ve hizmet içi eğitime),

Kurumlar ortaya çıkarıcı ve önleyici kontrol arasında optimum bir denge kurmalıdır.

Düzeltici önlemler hedefleri gerçekleştirmek bakımından kontrol faaliyetlerini

tamamlayıcı bir gerekliliktir.

Risklere karşılık verme ve kurumun hedeflerini gerçekleştirmek için belirlenen ve uygulanan

politikalar ve prosedürler kontrol faaliyetleridir.

Kontrol faaliyetlerinin etkin olabilmesi için;

- amaca uygun olması (yani doğru yerde, doğru kontrol ve ilgili risklerle orantılı olması),
- dönem boyunca yapılmış plana göre sürekli olarak iş görmesi (yani, müdahil olan bütün çalışanlar tarafından özenle uyulması ve kilit personelin olmadığı ya da işgücünün çok fazla olduğu zamanlarda devre dışı kalmaması),
- ehven maliyetli olması (yani, kontrolün uygulamaya konma maliyetinin ondan elde edilecek yararları aşmaması),
- kapsamlı, makul ve kontrol hedeferiyle doğrudan bağlantılı olması

gerekir.

Kontrol faaliyetleri farklı farklı olduğu gibi, bir dizi politika ve prosedürü de kapsar:

(1) Yetki devri ve onay prosedürleri

Yetki devri ve icrai işler ve işlemler, sadece yetkileri kapsamı içinde vekalet eden kişilerce yapılır. Yetki devri geçerli iş ve işlemleri, sadece, yönetimce istendiğinde başlatmayı sağlayan bir temel araçtır. Dokümante edilmesi ve yöneticilere ile çalışanlara açıkça duyurulması gereken yetki devri prosedürleri; devredilen yetkilerin spesifik koşullarını ve süresini içermelidir.

Bir yetki devrinin koşullarına uygun hareket edilmesi çalışanların yönetimce ya da mevzuatla belirlenmiş direktişer ve limitler dahilinde hareket etmesi demektir.

(2) Görevlerin birbirinden ayrılması (yetki, uygulama, kaydetme, inceleme)

Hata, savurganlık veya kural ihlali risklerini ve bu türden sorunların ortaya çıkarılamama risklerini azaltmak için bir iş ya da işlemin önemli aşamalarını tümü hiçbir zaman tek kişi ya da bir ekip tarafından kontrol edilmemelidir. Aksine, karşılıklı kontrol ve dengeleme (check and balance) etkinliğini sağlamak üzere görev ve sorumluluklar çok sayıda kişi arasında sistemli bir biçimde paylaştırılmalıdır. İşlemlerin kaydının tutulması, bilgisayara geçirilmesi ve gözden geçirilmesi ya da denetlenmesi önemli görevler arasındadır. Ancak, muvazaa iç kontrol faaliyetinin etkinliğini azaltabilir ya da ortadan kaldırabilir. Küçük bir organizasyonun bu kontrolü eksiksiz biçimde uygulamaya koymaya yetecek sayıda personeli bulunmayabilir.Bu tür durumlarda yönetim risklere karşı uyanık olmalı ve bu riskleri diğer kontrollerla telafi etmelidir. Çalışanların rotasyona tabi tutulması, tek kişinin işlerin ve işlemlerin bütün önemli aşamalarıyla çok uzun bir zaman uğraşmamasını sağlamaya yardımcı olabilir. Ayrıca, yıllık izin kullanımının özendirilmesi veya zorunlu yıllık izin kullandırılması da görevlerin geçici rotasyonunu sağlayarak risklerin azaltılmasını kolaylaştırabilir.

(3) Kaynaklara ve kayıtlara erişim yetkisi üzerindeki kontroller

Kaynaklara ve kayıtlara erişim yetkisinin bunların saklanmasından ve/veya kullanılmasından sorumlu olan yetkili kişilerle sınırlandırılması gerekir. Saklamaya ilişkin hesapverme sorumluluğu; makbuzların, envanterlerin mevcudiyetiyle veya emanet görevlendirmesine ve emanetin transfer edilmesine ilişkin diğer kayıtlarla kanıtlanır.

Kaynaklara erişimin sınırlandırılması; kamu açısından bunların yetkisiz kullanımını ya da kayba uğrama riskini azaltıp yönetimin direktişerine uyulmasını kolaylaştırır. Kısıtlamanın derecesi kaynağın hassasiyetine ve kayıp ya da kötüye kullanım riskinin farkına varılmasına bağlı olup, her iki unsur da periyodik olarak gözden geçirilmelidir. Bir varlığın hassasiyetine karar verilirken maliyetinin, taşınabilirliğinin, değişim değerinin gözönünde bulundurulması gerekir.

(4) Teyitler

İşlemler ve önemli işler sürecin öncesinde ve sonrasında teyit edilir; örneğin mal teslim edilirken, sunulan malların miktarı sipariş edilen malların miktarıyla teyit edilir. Daha sonra fatura düzenlenen malların sayısı ile teslim edilen malların sayısı teyit edilir. Stok sayımı yapılmak suretiyle envanter kayıtları da doğrulanır.

(5) Mutabakatlar

Kayıtlarla gerekli dokümanlar arasında düzenli olarak mutabakat sağlanır; örneğin banka hesaplarıyla bağlantılı muhasebe kayıtları banka ekstreleriyle karşılaştırılır.

(6) Işgörme performansına yönelik incelemeler

Etkinlik ve verimlilik değerlendirilmek suretiyle faaliyet performansı bir dizi standarda göre düzenli olarak gözden geçirilir. Performans incelemeleri fiili başarıların saptanmış hedeferi veya standartları karşılamadığı sonucuna varmışsa, iyileştirmeye ihtiyaç duyulup duyulmadığını tespit etmek bakımından hedeferi gerçekleştirmek için oluşturulmuş süreçler ve faaliyetler yeniden gözden geçirilmelidir.

(7) Faaliyetler, süreçler ve eylemlerle ilgili incelemeler

Faaliyetler, süreçler ve eylemler mevcut düzenlemelere, politikalara, prosedürlere veya diğer zorunluluklara uygunluğu sağlamak bakımından periyodik olarak incelenmelidir. Bir organizasyonun günlük işletimi eriyle ilgili bu tip inceleme, bölüm 2.5'de ayrıca ele alınan iç kontrol izlemesinden ayırt edilmelidir.

(8) Gözetim (görevlendirme, gözden geçirme ve onay verme, yönlendirme ve hizmet içi eğitme)

Tatminkâr bir gözetim iç kontrol hedeferinin gerçekleşmesine yardımcı olur. Görevlendirme, inceleme ve bir çalışanın yaptığı işi onaylama şu unsurları ihtiva eder:

- görevlerin, sorumlulukların ve görevlendirilen her yönetim mensubunun hesapverme sorumluluğunun açık seçik bildirilmesi,
- her elemanın çalışmasının gerektiği ölçüde, sistemli olarak incelenmesi,
- iş akışının istenildiği şekilde olmasını sağlamak için kritik noktalarda işin onaylanması.

Gözetim yapan kişinin gözetim işini devretmesi, onun bu sorumlulukları ve görevleriyle ilgili hesapverme sorumluluğunu azaltmaz. Gözetimciler, ayrıca hata, savurganlık ve kural ihlallerinin azalmasını ve yönetim direktişerinin anlaşılıp bunlara uyulmasına yardımcı olmak amacıyla çalışanlarına gerekli yönlendirme ve hizmet içi eğitim sağlarlar.

Yukarıda sıralanan liste önleyici ve ortaya çıkarıcı kontrol faaliyetlerinin tümünü kapsamamakta, en yaygın biçimde kullanılanlardan söz etmektedir. 1-3. sıradaki kontrol faaliyetleri önleyici, 4-6. sıradakiler ortaya çıkarıcı, 7-8. sıradakiler ise hem önleyici hem de ortaya çıkarıcı niteliktedir.

Tek tek kontrollerın özel dezavantajlarını telafi etmek için karma kontrollerdan yararlanmak suretiyle, kurumların, genellikle, ortaya çıkarıcı ve önleyici kontrol faaliyetleri arasında uygun bir denge kurmaları gerekir.

Bir kontrol uygulamaya konduğunda, etkinliğinin sağlanması konusunda güvence verilmesi önem arz eder. Sonuç olarak düzeltici önlemler kontrol faaliyetlerini tamamlayan bir gerekliliktir. Ayrıca, kontrol faaliyetlerinin sadece iç kontrolün bir unsuru olarak biçimlendirildiğinin açık olması gerekir. Kontrol faaliyetleri iç kontrolün diğer dört unsuru ile

bütünleştirilmelidir.[3]

Bilişim Teknoloji Kontrol Faaliyetleri

Bilişim sistemleri spesifik türden kontrol faaliyetlerini gerektirir. Bilişim teknolojisi kontrolleri genel kontroller ve uygulama kontrolleri olmak üzere iki ana gruptan oluşur.

(1) Genel kontroller

Genel kontroller bir kurumun bilişim sistemlerinin tümüne veya geniş bir kesimine uygulanan ve bu sistemlerin düzgün işletimini sağlamaya yardımcı olan yapılar, politikalar ve prosedürlerdir. Bunlar içinde uygulama sistemlerinin ve kontrollerın işlediği bir ortam yaratır.

Genel kontrollerın başlıca kategorileri (1) kurum ölçeğinde güvenlik programı planlaması ve yönetimi (2) erişim kontrolleri (3) uygulama yazılımının geliştirilmesi, sürdürülmesi ve değiştirilmesi üzerindeki kontroller (4) sistem yazılım kontrolleri (5) görevlerin birbirinden ayrılması (6) hizmet sürekliliğidir.

(2) Uygulama kontrolleri

Uygulama kontrolleri farklı, özel uygulama sistemlerini yürüten yapı, politikalar ve prosedürler olup bireysel bilgisayarlı uygulamalarla doğrudan bağlantılıdır. Bu kontroller, genellikle, bilişim sistemleri içinde bilgi akışı olurken hataları ve düzensizlikleri önlemek, ortaya çıkarmak ve düzeltmek amacıyla tasarlanır.

Genel kontroller ve uygulama kontrolleri birbirleriyle bağlantılıdır; her ikisi de bilişim süreçlerinin eksiksiz ve doğru olmasını sağlamaya yardım etmelidir. Bilişim teknolojilerinin hızla değişmesi yüzünden, bağlantılı kontrollerın etkin kalabilmeleri bakımından sürekli olarak geliştirilmeleri gerekir.

Bilişim teknolojisinde ilerleme kaydedildiğinde, organizasyonlar faaliyetlerini gerçekleştirmek ve önemli bilgileri işleyip muhafaza etmek ve raporlamak için giderek artan biçimde bilgisayarlı bilişim sistemlerine tabi olur. Sonuç olarak, bilgileri işleyip saklayan sistemlerin ve bilgisayar ortamında bulunan verilerin güvenilirliği, korunması ve verilerin raporlanması organizasyonun hem yönetimi hem de denetçileri açısından önemli bir meseledir. Bilişim sistemleri spesifik türden kontrol faaliyetlerini gerektirmekle birlikte, bilişim teknolojisi "kendi başına" ("stand alone") bir kontrol meselesi değildir. Pek çok kontrol faaliyetinin ayrılmaz bir parçasıdır.

Bilginin işlenmesinde otomatik sistemlerin kullanılması organizasyonun dikkate alması gereken bazı riskler doğurur. Bu riskler, başka şeylerin yanı sıra; işlemlerin tek tip işleyişinden,

---

3 ***Örnekler***

İç kontrolün her hedefi ve her unsuruyla bütünleştirilmiş örnekler için eklere bakınız.

bilgisayar sistemlerinin işlemleri otomatik olarak başlatmasından, ortaya çıkarılmama potansiyeli giderek artan hatalardan, sistemin ömründen, eksikliklerinden ve denetim izlerinin hacminden; kullanılan donanım ve yazılımın doğasından, ayrıca olağandışı veya alışılmadık işlemlerin kaydedilmesinden kaynaklanır. Örneğin; bilgisayar programlama sorunları yüzünden meydana gelen ve işlemlerin tek tip işlenmesinden kaynaklanan bünyesel risk sürekli olarak benzer işlemleri doğurur. Etkin bilişim teknolojisi kontrolleri kendi sistemleri tarafından işlenmiş bilgilerin eksiksizlik, vaktindelik, verilerin doğruluğu ve güvenilirliğinin korunması gibi, arzu edilen kontrol hedeferini karşılaması bakımından yönetime makul güvence sağlar.

Bilişim teknolojisi kontrolleri genel kontroller ve uygulama kontrolleri olmak üzere iki ana gruptan oluşur.

Genel kontroller

Genel kontroller; anaçatı bilgisayar (mainframe), mini bilgisayar, ağ ve son kullanıcı ortamları gibi bir kurumun bilişim sistemlerinin tümüne ya da büyük bölümüne uygulanan yapı, politikalar ve prosedürler olup sistemin düzgün çalışmasını sağlamaya yardımcı olur. Genel kontroller içinde uygulama sistemleri ve kontrollerın çalıştığı bir ortam yaratır.

Genel kontrollerın ana kategorileri şunlardır:

(1) *Kurum ölçeğinde güvenlik programı planlaması ve yönetimi.,* riskleri yönetme, güvenlik politikaları geliştirme, sorumlulukları devretme ve kurumun bilgisayar bağlantılı kontrollerının yeterliliğini izleme faaliyetlerinin çerçevesini ve sürekli çevrimini sağlar.

(2) *Erişim kontrolleri;* bilgisayar kaynaklarını (veriler, programlar, araçlar ve mekanlar) izinsiz değiştirmeye, kayba uğramaya ve ifşa edilmeye karşı korumak suretiyle kaynaklara erişimi sınırlar ya da yetkisiz işlemleri ortaya çıkarır.

(3) *Uygulama yazılımının geliştirilmesi, sürdürülmesi ve değiştirilmesi üzerindeki kontroller;* izinsiz programlan ve mevcut programların değiştirilmelesini önler.

(4) *Sistem yazılımının kontrolleri;* bilgisayar donanımlarını kontrol eden ve sistem tarafından desteklenen uygulamaların güvenliğini sağlayan etkili programlara ve hassas dosyalara erişimi sınırlayıp izler.

(5) *Görevlerin birbirinden ayrılması;* bilgisayarla bağlantılı faaliyetlerin tüm önemli boyutlarını kontrol eden ve böylece izinsiz işlemler yürüten veya varlıklara ve kayıtlara yetkisiz erişimle sisteme giren tekil girişimleri önlemek üzere oluşturulan politikaları, prosedürleri ve organizasyonel yapıyı ifade eder.

(6) *Hizmet sürekliliği kontrolleri;* istenmeyen olaylar meydana geldiğinde kritik faaliyetlerin kesilmeden devam etmesini veya derhal başlatılıp, önemli ve hassas verilerin korunmasını sağlamaya yardımcı olur.

Uygulama kontrolleri

Uygulama kontrolleri ödenecek borçlar hesabı, envanter, ücretler, hibe veya bağışlar gibi birbirinden farklı özel uygulama sistemlerini yürüten yapı, politikalar ve prosedürler olup spesifik uygulama yazılımları içindeki verilerin işletimini kontrol etmek üzere tasarlanır. Bu kontroller, genellikle, bilişim sistemleri içinde bilgi akışı olurken hataları ve düzensizlikleri önlemek, ortaya çıkarmak ve düzeltmek amacıyla dizayn edilir.

Uygulama kontrolleri ve bilginin bilişim sistemleri içinde akış tarzı ve çevrim sürecinde üç aşamaya bölünebilir:

- ***girdi:*** veriler onaylanıp otomatik bir forma dönüştürülür ve doğru, eksiksiz ve zamanında uygulamaya sokulur.
- *işletim:* veriler bilgisayar tarafından düzgün biçimde işlenir ve dosyalar uygun biçimde güncelleştirilip
- ***çıktı:*** uygulama tarafından üretilen dosyalar ve raporlar fiilen meydana gelen işleri veya işlemleri gösterir ve sürecin sonuçlarını doğru biçimde yansıtır; ayrıca, raporlar kontrol edilip yetkili kullanıcılara dağıtılır.

Uygulama kontrolleri, işlemlere ve bilgiye onay verilip verilmediği, tam, doğru ve geçerli olup olmadığı dahil, ilgili oldukları kontrol hedeferinin türlerine göre de tasnif edilebilir. Yetki kontrolleri işlemlerin geçerliliği ile ilgilidir ve işlemlerin belirli bir periyot içinde fiilen meydana gelen olguları göstermesine yardımcı olur. Eksiksizlik kontrolleri bütün geçerli işlemlerin kaydedilip kaydedilmediğiyle ve gerektiği şekilde sınışandırılıp sınışandırılmadığıyla ilgilidir. Doğruluk kontrolleri işlemlerin yanlışsız olarak kaydedilip kaydedilmediği ve verilerin tüm unsurlarının doğru olup olmadığıyla ilgilenir. İşletimin ve veri dosyalarının güvenilirliği üzerindeki kontroller, yetersiz değillerse, yukarıda söz edilen uygulama kontrollerının her birini geçersiz kılabilir; eksik ve doğru olmayan verileri artırmak gibi, izinsiz işlemlerin oluşmasına da yol açabilir.

Uygulama kontrolleri arasında otomatik olarak yazım denetimi yapmak ve bilgisayar üretimi çıktının manuel olarak gözden geçirmek gibi, red edilen veya istenmeyen kalemleri belirleyen raporların incelenmesi türünden programlanmış kontrol faaliyetleri de bulunur.

Bilgisayar sistemleri üzerindeki genel kontroller ve uygulama kontrolleri birbirleriyle bağlantılıdır.

Uygulama kontrollerının etkinliğine karar verirken genel kontrollerın etkinliği önemli bir faktördür. Genel kontroller zayıf olduğu takdirde, özel uygulamalarla bağlantılı kontrollerın güvenilirliği önemli ölçüde azalır. Etkin genel kontroller olmadan uygulama kontrolleri önemsenmeme, kurnazca davranma veya değiştirme yollarıyla etkisiz hale getirilebilir. Örneğin, bir bordro sistemine, kullanıcıların makul olmayan sayıda çalışma saati (mesela, bir günde 24

saatten fazla) girmesini önlemek üzere tasarlanmış yazım denetimi etkili uygulama kontrolü olabilir. Ancak, genel kontroller yazım denetiminden muaf tutulmuş bazı işlemleri engelleyemiyen yetkisiz program değişikliklerine izin veriyorsa, bu kontrola güven duyulmayabilir.

Bilişim teknolojisinde meydana gelen hızlı değişiklikler, kontrol hedeflerinin esasını değiştirmemekle birlikte, etkin kalabilmeleri bakımından kontrolların mükemmelleştirilmesini gerektirir. Ağ sistemine giderek artan oranda güven duyulması, son kullanıcıların ellerindeki veri işlemcisine sorumluluk veren becerikli bilgisayarlar, elektronik ticaret ve Internet türünden değişiklikler spesifik kontrol faaliyetlerinin doğası ve bunların uygulaması üzerinde etki yaratır.

Bilişim teknolojisi kontrol faaliyetleri hakkında daha fazla bilgi Bilişim Sistemleri Denetimi ve Kontrolu Birliği'nin (ISACA- Information Sistems Audit and Control Association), özellikle de, Bilişim ve İlgili Teknolojilerine Dönük ISACA Kontrol Hedefleri'nin (COBIT) referans çerçevesinden ve INTOSAI Bilişim Teknolojisi Denetim Komitesinin tutanaklarından elde edilebilir.

2.4 Bilgi ve İletişim

Bilgi ve iletişim iç kontrolun genel hedeflerinin gerçekleştirilmesi bakımından yaşamsal önemdedir.

Bilgi

Güvenilir ve uygun bilginin önşartı işlerin ve işlemlerin anında kaydedilmesi ve düzgün biçimde sınıflandırılmasıdır. Anlamlı bilgiler, personelin iç kontrol ve diğer sorumluluklarını yerine getirmelerini sağlayacak formatta ve takvime göre belirlenip elde edilmeli ve onlara duyurulmalıdır (doğru kişilerle zamanında iletişim). Bu nedenle, iç kontrol sistemi ve bütün işlemler ve önemli işler eksiksiz olarak dokümante edilmelidir.

Bilgi sistemleri; faaliyetleri ilgilendiren, finansal olan ve olmayan, uygunlukla bağlantılı bilgileri ihtiva eden ve faaliyetlerin yürümesi ve kontrolunu olanaklı hale getiren raporlar üretir. Bu sistemler sadece kurumla ilgili olarak üretilmiş verilerle değil, keza, karar almayı ve

---

4**Örnekler**
İç kontrolun her hedefi ve her unsuruyla bütünleştirilmiş örnekler için eklere bakınız.

raporlamayı sağlamak üzere ihtiyaç duyulan kurum dışı işler, faaliyetler ve koşullar hakkındaki bilgileri de ele alır.

Yönetimin uygun kararları alma gücü, bilginin uygun, vaktinde, güncel, doğru ve erişilebilir olmasından yani, bilginin kalitesinden etkilenir.

Bilgi ve iletişim bütün iç kontrol hedeflerinin gerçekleştirilmesi bakımından yaşamsal önemi haizdir. Örneğin; iç kontrolun hedeflerinden biri kamusal hesapverme sorumluluğu ile ilgili zorunlulukların yerine getirilmesidir. Bu husus güvenilir ve uygun finansal ve finansal olmayan bilgilerin hazırlanması ve saklanması suretiyle ve bu bilgilerin vaktinde ve tarafsız açıklamalar içeren raporlar aracılığıyla duyurulması biçiminde gerçekleştirilebilir.

Organizasyonun performansı ile bağlantılı bilgi ve iletişim; faaliyetlerin düzenli, ahlak kurallarına uygun, ekonomik, verimli ve etkin olma bakımlarından değerlendirilme ihtimalini yükseltir. Pek çok durumda, birtakım bilgilerin temin edilmiş olması veya iletişimin yasalara ve yönetmeliklere uymak amacıyla kurulması gerekir.

Etkin bir iç kontrol kurmak ve kurumun hedeflerini gerçekleştirmek için bir organizasyonun bütün kademelerinde bilgiye ihtiyaç duyulur. Bu yüzden anlamlı, güvenilir ve uygun bilginin oluşturulması personelin kontrol ve diğer sorumluluklarını yerine getirmesine imkân verecek biçimde ve zaman dilimi içinde belirlenip sağlanmalı ve onlara duyurulmalıdır. Güvenilir ve uygun bilginin ön şartı iş ve işlemlerin derhal kaydedilmesi ve düzgün olarak sınışandırılmasıdır.

Faaliyetleri kontrol etmede ve karar vermede yönetim açısından bilginin anlamlı ve değerli olması isteniyorsa, işler ve işlemler, meydana gelir gelmez kaydedilmelidir Kayıt işlemi; başlangıç ve onay aşamaları dahil işlerin ve işlemlerin bütün süreçleri veya ömürleri boyunca ve hesap özetlerinin nihai tasnifine kadar sürdürülür. Bu husus, ilişki kurmak bakımından bütün dokümanların hemen güncellenmesi için de geçerlidir.

Ayrıca, yönetimin güvenilir bilgi elde etmesini sağlamak için iş ve işlemlerin düzgün biçimde sınışandırılması gerekir. Bunun anlamı hazırlanan raporlar, çizelgeler ve finansal tablolardan elde edilen bilgilerin düzenlenmesi, tasnif edilmesi ve biçimiendirilmesidir.

Bilişim sistemleri; faaliyetleri ilgilendiren, finansal ve finansal olmayan, uygunlukla bağlantılı bilgileri ihtiva eden ve faaliyetleri yürütüp kontrol etmeyi mümkün kılan raporlar üretir. Sistem, kurum içinde üretilen verilerin, sadece, nicel ve nitel biçimleriyle değil, aynı zamanda, bilgiye dayalı karar alma ve raporlama bakımından kurum dışı işlerin, faaliyetlerin ve koşulların gerektirdiği bilgilerle de ilgilenir.

Yönetimin uygun karar alma kapasitesi bilginin kalitesinden etkilenir; bu bilgilerin:

- uygun (gerekli bilgi orada bulunmakta mıdır?);

- zamanında (gerektiği zaman orada mı?);
- güncel (en son haliyle elde edilebilmekte midir?);
- doğru (yanlışsız mıdır?);
- elde edilebilir (ilgili taraşarca kolayca elde edilebilir mi?);

olması gerekir.

Bilgi ve raporlama kalitesini sağlayabilmek, iç kontrol faaliyetlerini ve sorumluluklarını başarabilmek, iç kontrol sistemini, bütün işlemleri ve önemli işleri daha etkin ve verimli şekilde izleyebilmek için gerektiği şekilde kolaylıkla anlaşılan bir dokümantasyon yapılmalıdır (örneğin; akış şemaları ve metinler). Bu dokümanlar arandığında kolayca bulunabilmelidir.

İç kontrol sisteminin dokümanları organizasyon yapısının ve politikalarının, faaliyet türlerinin ve bağlantılı hedeferinin ve kontrol prosedürlerinin tanımlamalarını kapsamalıdır. Organizasyonun hedeferi ve kontrol faaliyetleri dahil olmak üzere, iç kontrol sürecinin unsurları ile ilgili yazılı kanıtları bulunmalıdır.

Bir kurumun iç kontrol dokümantasyonunun hacmi, yine de, kurumun büyüklüğüne, karmaşıklığına ve benzer faktörlere göre farklılık gösterir.

İletişim

Bütün unsurlar arasında ve tüm yapı içinde etkin bir iletişim aşağıdan yukarıya, enlemesine ve yukarıdan aşağıya doğru olmalıdır.

Tüm personel kontrol sorumluluklarını ciddiyetle yerine getirmelerini sağlayacak şekilde, üst yönetimden net mesajlar almalıdır. Personel kendi faaliyetleri ile diğerlerinin çalışmaları arasında nasıl bağlantı kuracaklarını ve iç kontrol sistemi içindeki rollerini bilmelidirler.

Ayrıca, kurum dışındaki üçüncü kişilerle de etkili bir iletişimin kurulması gerekir.

Grupların ve kişilerin sorumluluklarını etkin olarak yerine getirmelerini sağlayarak onların beklentilerini karşılaması gereken bilgiler iletişimin esasını oluşturur. Etkin iletişim aşağıdan yukarıya, enlemesine ve yukarıdan aşağıya doğru akmak suretiyle bütün yönlerde, bütün unsurlar ve tüm yapı arasında meydana gelmelidir.

En kritik iletişim kanallarından biri yönetim ile personeli arasında olanıdır. Yönetimin performans, gelişmeler, riskler, iç kontrol fonksiyonu, diğer bağlantılı konular ve meselelerle ilgili olarak güncellemeyi sürdürmesi gerekir. Aynı şekilde, yönetim ne tür bilgiye ihtiyaç duyulduğunu personeline bildirmeli ve onların değerlendirmelerini alıp yönlendirme sağlamalıdır. Yönetim, ayrıca, sosyal ve ahlakî davranış beklentilerini karşılayan spesifik ve emredici nitelikte iletişim de kurmalıdır. Bu, iç kontrol felsefesi ve yaklaşımı ile yetki dağılımı hakkında kurumun açık bir beyanını ifade eder.

İletişim; etkin iç kontrolun önem ve ilgisine yönelik bilinci yükseltmeli, kurumun risk göğüsleme kapasitesi ile risk kabulleri arasında bağlantı kurmalı ve iç kontrol unsurları üzerinde etki yaratıp desteklenmesinde personelin rol ve sorumluluklarını fark etmesini sağlamalıdır.

Kurum içi iletişimlere ek olarak yönetim, kurum dışı iletişimler organizasyonun hedeflerine ulaşma derecesi üzerinde çok önemli etki yaratabilecek girdiler sağlayabildiğinde, üçüncü kişilerle iletişim kurmaya ve onlardan bilgi edinmeye yarayan araçlar temin etmelidir. Yönetim; kurum içi ve kurum dışı iletişimlerden elde edilen girdilere dayalı olarak gerekli önlemleri zamanında almak ve bu önlemleri izlemek zorundadır.

[5]

[5] **Örnekler**

İç kontrolun her hedefi ve her unsuruyla bütünleştirilmiş örnekler için eklere bakınız.

2.5 İzleme

İç kontrol sistemleri; dönem içindeki sistem performans kalitesini değerlendirmek amacıyla, izlenmelidir. İzleme fonksiyonu rutin izleme faaliyetleri, özel değerlendirmeler veya her ikisinin kombinasyonu aracılığıyla gerçekleştirilir.

1. Sürekli İzleme

İç kontrolun sürekli izlenmesi kurumun normal, tekrarlanan çalışma faaliyetlerini kapsar. Bu tür izleme faaliyetleri arasında düzenli nitelikteki yönetim ve gözetim faaliyetleri ve personelin görevinin icrası sırasında aldığı diğer önlemler bulunur.

Sürekli izleme faaliyetleri; kontrolun her bir unsurunu içerir ve düzenli, ahlaki, ekonomik, verimli ve etkin olma niteliklerini taşımayan iç kontrol sistemlerine karşı alınan önlemlerle ilgilidir.

2. Özel Değerlendirmeler

Özel değerlendirmelerin kapsamını ve sıklığını esasen, risk değerlendirmesi ve sürekli izleme prosedürlerinin etkinliği belirler.

Spesifik tekil değerlendirmeler iç kontrol sistemin etkinliğinin değerlendirilmesini içerir ve önceden belirlenmiş metotlara ve prosedürlere dayalı olarak iç kontrolun arzu edilen sonuçları gerçekleştirmesini güvence altına alır. İç kontrol yetersizlikleri yönetimin uygun kademelerine rapor edilmelidir.

İzleme fonksiyonu denetim bulgularının ve tavsiyelerinin tatminkâr bir biçimde ve hemen yerine getirilmesini sağlamalıdır.

İç kontrolun izlenmesinin amacı kontrolların, arzu edildiği şekilde çalışıyor olmasını ve koşullardaki değişikliklere gerektiği biçimde uyum göstermesini sağlamaktır. İzleme fonksiyonu; kurumun misyonu doğrultusunda, iç kontrolun tanımında belirlenen genel hedeflerini gerçekleştirip gerçekleştirmediğini de değerlendirmelidir. Bu husus, iç kontrolun kurumun bütün kademelerinde ve bölümlerinde uygulanmasının sürdürülmesi ve iç kontrol faaliyetlerinin arzu edilen sonuçlan yerine getirmesi sürekli izleme faaliyetleri, özel değerlendirmeler ya da her ikisinin kombinasyonu aracılığıyla gerçekleştirilir. İç kontrol faaliyetlerinin kendilerinin izlenmesi, önceki 2.3 bölümde tasvir edildiği üzere, bir iç kontrol faaliyeti olan organizasyon faaliyetlerinin gözden geçirilmesinden açık bir biçimde ayrılmalıdır.

İç kontrolün sürekli izlenmesi bir organizasyonun normal, tekrarlanan faaliyetleri sırasında yapılır. Devamlı ve gerçek zamanlı bir esasa göre gerçekleştirilir, değişen koşullara dinamik bir biçimde cevap verir ve kurum faaliyetlerinin içine gömülüdür. Sonuçta, özel değerlendirmelerden daha etkindir ve düzeltici önlemlerden potansiyel olarak daha az maliyetlidir. Özel değerlendirmeler olaydan sonra meydana geldiğinden, sorunlar, genellikle, sürekli izleme yöntemleriyle daha çabuk tespit edilir.

Özel değerlendirmelerin kapsamı ve sıklığı, öncelikle, risklerin değerlendirilmesine ve

sürekli izleme prosedürlerinin etkinliğine bağlıdır. Bu tespit yapılırken, organizasyon hem kurum içi hem de kurum dışı işlerden kaynaklanan değişikliklerin doğasını ve düzeyini; riske verilecek yanıtları ve ilgili kontrolleri uygulayan personelin ehliyetine ve deneyimine ve sürekli izleme faaliyetinin sonuçlarını göz önünde bulundurmalıdır. Tekil kontrol değerlendirmeleri, spesifik bir zamanda, kontrollerın etkinliğine doğrudan odaklanmak suretiyle de yararlı olabilir. Özel değerlendirmeler kontrol tasarım incelemesinin ve iç kontrollerın doğrudan test edilmesinin yanı sıra öz-değerlendirme formu aracılığıyla yapılabilir. Özel değerlendirmeler, Sayıştaylar, iç ve dış denetçiler tarafından da gerçekleştirilebilir.

Genellikle, sürekli izleme faaliyetinin kimi kombinasyonları ve özel değerlendirmeler iç kontrolün dönem boyunca etkinliğini sürdürmesine yardımcı olur.

Sürekli izleme esnasında veya özel değerlendirmeler aracılığıyla tespit edilen eksikliklerin tümü, gerekli önlemleri alma konumunda olanlara bildirilmelidir. "Eksiklik" terimi, bir kurumun, genel hedeferini başarma gücünü olumsuz etkileyen bir durum demektir. Eksiklik, bu yüzden, muhtemel veya gerçek bir kusuru veya kurumun genel hedeferini başarma olasılığını artırmak bakımından iç kontrolü güçlendirme potansiyelini ifade eder.

İç kontrolün eksikliği hakkındaki gerekli bilginin doğru taraşara bildirilmesi yaşamsal önemdedir. Etkin karar alma bakımından özel bir kademenin ne tür bilgiye ihtiyaç duyduğunu belirlemek üzere protokoller yapılabilir. Bu tür protokoller; bir yöneticinin, emri altındaki personelinin eylemlerini veya davranışlarını olumsuz yönde etkileyen bir bilginin, spesifik hedeferi gerçekleştirmek üzere ihtiyaç duyulan bilgiler gibi, duyurulması genel kuralını ifade eder.

Faaliyetlerin akışı sırasında üretilmiş bilgi, çoğunlukla, normal kanallarla yani, o fonksiyondan sorumlu olan kişiye ve en azından o kişinin üstündeki bir yönetim kademesine, rapor edilir. Ancak, yasadışı veya kurallara aykırı fiiller türünden hassas bilgileri raporlamak üzere, alternatif kanallar da bulunmaktadır.

İç kontrolün izlenmesi; denetimlerin ve diğer incelemelerin bulgularının yeterli şekilde ve hemen çözüme kavuşturulmasını hedefeyen politikaları ve prosedürleri kapsamalıdır. Yöneticilerin, (1) birimlerin faaliyetlerini değerlendiren denetçiler ve diğerleri tarafından raporlanmış eksiklikleri ve tavsiyeleri ortaya koyanlar dahil denetimlerden ve diğer incelemelerden elde edilen bulguları hemen değerlendirme, (2) denetimlerden ve incelemelerden elde edilen bulgulara ve tavsiyelere cevap olarak doğru önlemleri belirleme, (3) onların dikkat çektikleri meseleleri düzelten veya başka bir şekilde çözüme kavuşturan bütün önlemleri, belirli bir zaman çizelgesi içinde almaları gerekir.

Çözüm süreci, denetimin veya incelemelerin sonuçlan yönetime rapor edildiğinde başlar ve önlemler alındıktan sonra tamamlanır; Bu önlemler; (1) tespit edilen yetersizlikleri düzeltir; (2) gelişme sağlar veya (3) bulguların ve tavsiyelerin bir yönetim eylemi gerektirmediğine işaret eder.[6]

6Örnekler

3. Roller ve Sorumluluklar

Organizasyon içindeki herkesin iç kontrolla ilgili sorumlulukları bulunmaktadır:

Yöneticiler İç kontrol sisteminin tasarlanması, uygulanması ve düzgün işlemesinin gözetilmesi dahil, sürdürülmesi ve dokümante edilmesi ile ilgili faaliyetlerden doğrudan sorumludurlar. Sorumlulukları organizasyon içindeki fonksiyonlarına ve organizasyonun karakteristik özelliklerine bağlı olarak farklılık göstermektedir.

İç Denetçiler Değerlendirmeleri ve tavsiyeleri aracılığıyla iç kontrol sisteminin etkinliğini süreklilik temelinde inceleyip ona katkıda bulunurlar ve böylece, iç kontrolun etkinleşmesinde önemli rol oynarlar. Bununla birlikte, iç denetçiler iç kontrolun tasarlanması, uygulanması, sürdürülmesi ve dokümante edilmesi bakımlarından yönetimin öncelikli sorumluluğuna sahip değillerdir.

Diğer Personel İç kontrola da katkıda bulunurlar. İç kontrol herkesin açık ya da zımnî biçimde görevinin bir parçasıdır. Personelin tümü kontrolun hayata geçirilmesinde rol oynar ve faaliyet sorunları, sosyal davranış kurallarına aykırılıklar ve politika ihlalleriyle ilgili raporlamadan sorumludur. Kurum dışındaki gruplar da iç kontrol sürecinde önemli rol oynarlar. Bu gruplar organizasyonun hedeflerini gerçekleştirmesine katkıda bulunabilirler veya iç kontrolu hayata geçirmek için yararlı bilgiler sağlayabilirler. Ancak organizasyonun iç kontrol sisteminin tasarlanmasından, uygulanmasından, düzgün işlemesinden, sürdürülmesinden veya dokümante edilmesinden bu guruplar sorumlu tutulamazlar.

Yüksek Denetim Kurumları (Sayıştaylar) İç kontrolun kamuda etkili biçimde tesisini özendirir ve desteklerler. Sayıştayların uygunluk, finansal ve performans denetimleri bakımından iç kontrol değerlendirmesi yaşamsal önemdedir. Sayıştaylar bulgularını ve tavsiyelerini ilgili paydaşlara iletirler.

Dış Denetçiler Bazı ülkelerde belirli kamu kuruluşlarını denetlerler. Dış denetçiler ve onların meslek kuruluşları iç kontrol hakkında öneriler sunup tavsiyelerde bulunurlar.

Yasa Koyucular ve Düzenleyiciler İç kontrolla ilgili kuralları koyup direktifler verirler. İç kontrolun yaygın biçimde anlaşılmasına katkı sağlarlar.

Diğer Gruplar Organizasyonla karşılıklı etkileşim içinde bulunurlar (hizmetten yararlananlar, tedarikçiler vb) ve hedeflerin gerçekleşmesi konusunda organizasyona bilgi sağlarlar.

İç kontrolün her hedefi ve her unsuruyla bütünleştirilmiş örnekler için eklere bakınız.

İç kontrol, esasen, yönetim, iç denetçiler ve diğer personel dahil olmak üzere kurum içi paydaşlar tarafından yaşama geçirilir. Ancak, kurum dışı paydaşların eylemleri de iç kontrol sistemi üzerinde etki yaratır.

Yöneticiler

İç kontrolun işletilmesinde organizasyondaki bütün personel önemli rol oynar. Ancak iç kontrol sisteminin tasarlanmasının, uygulanmasının, düzgün işlemesinin, gözetilmesinin, sürdürülmesinin ve dokümante edilmesinin genel sorumluluğu yönetime aittir. Yönetim yapısında tümü farklı rollere ve kompozisyonlara sahip olan kurul ve denetim komiteleri bulunabilir ve farklı ülkelerde bunlar farklı mevzuata tabidir.

İç Denetçiler

Yönetim, çoğunlukla, iç kontrol sisteminin ayrılmaz bir parçası olarak bir iç denetim birimi oluşturur ve ondan iç kontrol sisteminin etkinliğini izleyebilmek üzere yararlanır. İç denetçiler, iç kontrolun tasarımının ve işleyişinin değerlendirilmesinde dikkat çekici hususlara yoğunlaşarak iç kontrolun çalışması hakkında düzenli bilgi sağlarlar. İç kontrolun güçlü ve zayıf yanları hakkında bilgi sağlayıp geliştirilmesi için tavsiyelerde bulunurlar. Ancak iç denetim biriminin bağımsızlığının ve tarafsızlığının güvence altına alınması gerekir. Bu nedenle, iç denetim fonksiyonu bir organizasyonun faaliyetlerine ek değer katan ve onları geliştiren bağımsız, tarafsız güvence ve danışma sağlayan bir faaliyettir. İç denetim; risk yönetimi, kontrol ve yönetişim süreçlerinin etkinliğini değerlendirmek ve bunları geliştirmek üzere sistematik, disiplinli bir yaklaşım getirmek suretiyle, bir organizasyonun hedeflerini gerçekleştirmesine yardımcı olur. İç kontrol konusunda çok değerli bir bilgi ve danışma kaynağı olmalarına rağmen, iç denetçiler güçlü bir iç kontrol sisteminin ikamesi olarak düşünülmemelidir.

İç denetim fonksiyonunun etkin olması bakımından iç denetim personelinin yönetimden bağımsız olması, yansız, önyargısız, doğru ve dürüst bir biçimde çalışması ve raporlarını organizasyon içindeki en yüksek kademeye doğrudan vermesi yaşamsal önemdedir.

Bu husus iç denetçilerin iç kontrol değerlendirmeleri hakkında önyargısız görüşlerini ve ortaya çıkardıkları yetersizlikleri düzeltici önerileri tarafsız bir biçimde sunmalarına imkân verir. İç denetçiler meslekî yönlendiriciler açısından Tanım, Etik Kurallar, Standartlar ve Uygulamaya Dönük Tavsiyeler bölümleri dahil olmak üzere, İç Denetçiler Enstitüsünün Meslekî Uygulama Çerçevesi'nden yararlanmalıdırlar. Buna ilaveten iç denetçiler INTOSAI'in Etik Kurallarına da uymalıdırlar.

İç denetim personeli, bir kurumun iç kontrolünün izlenmesi rolüne ek olarak, dış denetçiye doğrudan destek sağlayarak dış denetim çabalarının etkinliğine de katkıda bulunur. Dış denetim prosedürlerinin yapısı, kapsamı veya zamanlaması, dış denetçinin iç denetçinin çalışmasına güven duyup duymamasına göre değişebilir.

Diğer Personel

Diğer personel ve çalışanlar da iç kontrolü yaşama geçirirler. Bunlar, genellikle, kontrolleri yürüten, gözden geçiren ve yanlış uygulanan kontrolleri düzelten ön cephedeki kişiler olup, günlük görevlendirmelerin gerçekleştirilmesinde kontroller aracılığıyla sorunları tespit ederler.

Kurumdışı Gruplar

İç kontrol paydaşlarının ikinci ana grubu dış denetçiler, (sayıştay denetçileri dahil) kanun koyucular, düzenleyici kurumlar ve diğer gruplardır. Bu gruplar organizasyonun hedeferini gerçekleştirmesine katkıda bulunabilirler veya iç kontrolün yaşama geçirilmesi bakımından yararlı olacak bilgiler sağlayabilirler. Ancak, bunlar organizasyonun iç kontrol sisteminin tasarlanmasından, uygulanmasından, düzgün çalışmasından, sürdürülmesinden ya da dokümante edilmesinden sorumlu değildirler.

Sayıştay Denetçileri ve Dış Denetçiler

Kurum dışı grupların görevleri, özellikle de dış denetçilerin ve sayıştay denetçilerinin görevleri arasında iç kontrol sisteminin çalışmasının değerlendirilmesi ve bulguları hakkında yönetime bilgi verilmesi bulunur. Ancak kurum dışı grupların iç kontrol sistemi ile ilgili mülahazalarını kendi yetkileri belirler.

Denetçilerin iç kontrol değerlendirmesi şu hususları gerektirir:

- kontrollerın değerlendirildiği riskin öneminin ve hassasiyetinin belirlenmesi,
- kaynakların kötüye kullanımının ortaya çıkaracağı duyarlılığın ve ahlak kuralları, ekonomiklik, verimlilik ve etkinlik konusunda hedefere varmadaki başarısızlığın veya hesapverme sorumluluğunun gerektirdiği zorunluluklar bakımından yetersizliğin ve yasalara ve düzenlemelere aykırılığın değerlendirilmesi,
- ilgili kontrollerın tespit edilmesi ve kavranması,
- kontrol etkinliği hakkında halihazırda bilinenlerin belirlenmesi,
- kontrol tasarımının yeterliliğinin değerlendirilmesi,
- kontrollerın etkin olması durumunda, bunun testler aracılığıyla saptanması,
- iç kontrol değerlendirmeleri hakkında rapor verilmesi ve gerekli düzeltici önlemlerin irdelenmesi.

Sayıştayların da ihtiyaç duyulan alanlarda güçlü iç denetim birimlerinin mevcudiyetini sağlamada haklı çıkarları bulunmaktadır. Bu denetim birimleri bir organizasyonun faaliyetlerinin geliştirilmesi bakımından sürekli imkânlar sağlamak suretiyle iç kontrolün önemli bir unsurunu oluşturur. Ancak, kimi ülkelerde, iç denetim birimlerinin bağımsızlığı bulunmayabilir, güçsüz olabilir veya bu birimler mevcut olmayabilir. Bu gibi durumlarda, Sayıştay, mümkün olan alanlarda, bunları oluşturmak ve kapasitelerini güçlendirmek ve iç denetim faaliyetlerinin

bağımsızlığını sağlamak üzere yardım ve rehberlik sunmalıdır. Bu yardım başka kurumlara personel göndermeyi, personel görevlendirmeyi, seminerler vermeyi, eğitim materyallerini paylaşmayı ve metodolojiler ve çalışma programları hazırlamayı kapsayabilir. Bu yardım sayıştayın veya dış denetim kurumunun bağımsızlığını zedelemeden yapılmalıdır.

Sayıştay da deneyim ve bilgi paylaşabilmek ve göreve karşılıklı biçimde katkıda bulunabilmek ve onu tamamlayabilmek için iç denetim birimleriyle iş ilişkileri geliştirmeye ihtiyaç duyar. Uygun olduğunda, dış denetim raporlarında iç denetim gözlemlerine yer vermek ve onların katkılarını takdir etmek bu ilişkiyi güçlendirebilir. Sayıştay iç denetim biriminin çalışmasına ne ölçüde güven duyabileceğini belirlemek için değerlendirme prosedürleri geliştirmelidir. Güçlü bir iç denetim birimi sayıştayın denetim yükünü hafişetip denetimdeki mükerrerliğini önleyebilir. Sayıştay iç denetim raporlarının ilgili çalışma kağıtlarının ve denetim kararlarına ilişkin bilgilerin erişim hakkında sahip olmalıdır.

Sayıştaylar, ayrıca, kendi organizasyonlarının iç kontrol çerçevesini bu rehberde belirlenen prensiplere uyacak tarzda oluşturmak suretiyle kamu kesimi bakımından liderlik yapmalıdır.

Sadece sayıştaylar değil, aynı zamanda dış denetçiler iç kontrol hedeferinin, özellikle, "hesapverme sorumluluğunun gereklerini yerine getirme"nin ve "kaynaklan koruma"nın gerçekleşmesine katkıda bulunarak önemli bir rol oynar. Bunun nedeni; finansal raporların ve bilgilerin dış denetimlerin hesapverme sorumluluğunun ve iyi yönetişimin ayrılmaz bir parçası olmasıdır. Dış denetimler, hâlâ kurum dışı paydaşların finansal olmayan bilgilerin eşliğinde performansı değerlendirmek için yararlandığı temel bir mekanizmadır.

Yasa Koyucular ve Düzenleyici Kuruluşlar

Yasalar iç kontrolün tanımı ve gerçekleştirilecek hedeferi konusunda ortak bir anlayış yaratabilir. Yasalar iç kontrol konusunda kendi rollerini ve sorumluluklarını yerine getirmede, kurum içi ve dışı paydaşlara izlemeleri gereken politikaları da bildirir.

Ekler

Örnekler

Hesapverme sorumluluğunun gereklerinin yerine getirilmesi; örnek (1): Su ve deniz yoluyla güvenli taşımadan sorumlu bir genel müdürlük; kılavuz kaptanlık, gemileri yüzdürmek, su kalitesini araştırmak, su yollarının kullanımını özendirmek, alt yapı (köprüler, bentler, kanallar ve kanal havuzları) yatırımları yapıp bunları korumak konularından sorumlu farklı hizmet birimlerini organize etmektir.

Kontrol Ortamı	Risk Değerlendirmesi	Kontrol Faaliyetleri	Bilgi ve İletişim	İzleme
Hizmet kuruluşlarının her birinde genel müdüre rapor vermek zorunda olan bir faaliyet yöneticisi görevlendirilir. Faaliyet yöneticileri uygun becerilere ve belirli kararları alma yetkisine sahip olmalıdır. Faaliyet yöneticilerinin tümü de sosyal ve ahlaki davranış kuralları tüzüğünü imzalar.	Muhtemel riskler gemilerin çarpışması, zehirli atıkların veya petrolün dökülmesi ve bentlerin yıkılmasıdır. İstenmeyen durumlar hükümet kuruluşunun ihmalinden kaynaklanıyorsa kuruluş büyük bir yükümlülükle karşı karşıya kalır.	Organize edilebilecek kontrol faaliyetleri şunlardır: ehil kılavuz kaptan aracılığıyla Gemilere yol gösterilmesi, şamandıralar, deniz fenerleri ve işaretler yerleştirilmesi, havadan görsel araştırma yapılması ve su örneklerinin alınması.	Diğer gemileri uyarmak için çarpışmaları bildirmek, gemileri hava koşullarından haberdar etmek, çevreyi kirletenlerin isimlerini, onlara verilen cezaları ve alınması gereken telafi edici önlemleri yayımlamak örnek olayla ilgili bilgi ve iletişim faaliyetleridir. örneklerinin etkinliğinin ve verimliliğinin izlenmesine yardımcı olabilir.	Gemi çarpışma sayılarını, çevre ihlallerini, su örneklerinin sonuçlarını ve diğer ülkelerle kıyaslamalarını ve geçmiş verileri takip etmek: kılavuz kaptanlığın, şamandıraların ve işaretlerin yerleştirilmesinin, incelemelerin ve su

Hesapverme sorumluluğunun gereklerinin yerine getirilmesine örnek (2): Spor yöneticisi geçtiğimiz yıl spor faaliyetlerinin önümüzdeki yılda % 15 oranında arttıracağını ileri sürmüştü.

Kontrol Ortamı	Risk Değerlendirmesi	Kontrol Faaliyetleri	Bilgi ve İletişim	İzleme
Yönetim kurulu, yöneticiye şöhreti dolayısıyla güven duyup yöneticinin çalışmalarının kontrol edileceği rutin durum toplantısını gerçekleştirmedi. *(Yukarıdaki durum iyi uygulama örneği değildir.)*	Hedeflerin açıklanmaması onların gerçekleşmeme riskini doğurur. Ayrıca, yönetici %15'lik artış Hedefinin gerçekleştiğini söyleyinceye kadar, raporunu bekletmek isteyeceğinden, bu raporun zamanında sunulamama tehlikesi vardır. Buna ek olarak %15'lik artışın nasıl ölçüleceği ortaya konulamadı. Bu nedenle yönetici spor yapan kişi sayısının veya kişilerin spor yaptığı saatlerin arttığını söyleyebilir. Rapor edilen bilginin kalitesi bu haliyle, esasen, düşük niteliktedir.	Bu risk uygun raporlama kanalları oluşturmak ve Sunulacak bilgiyi tanımlayan raporlama modeli oluşturmak suretiyle azaltılabilir.	Bu rapor zamanında ve belirlenen raporlama modeline uygun olarak sunulmalıdır. Artışa ilişkin hedefler, bunların nasıl ölçüleceğini, niçin bu şekilde ölçüldüğünü açıklanmalıdır. Yedeklenen bütün bilgilere erişebilmelidir.	Raporun tatmin edici olup olmadığını ve ne tür bilgi verildiği ve hangi bilgilerin hâlâ bulunmadığının doğrulanması izlemenin bir biçimi olabilir.

Yürürlükteki yasalara ve düzenlemelere uygunluk, örnek : Savunma Bakanlığı kamu ihalesi açarak yeni savaş uçakları almak istemektedir ve ihale şartnamesinin bütün koşullarını ve prosedürlerini yayımlar. Verilen bütün fiyat teklifleri teklif verme süresinin sonuna kadar açılmadan bekletildi. Sorumlu yöneticilerin ve bazı görevlilerin huzurunda aynı anda açıldı. En iyi teklife karar vermek üzere bütün teklifler incelenip karşılaştırıldı.

Kontrol Ortamı	Risk Değerlendirmesi	Kontrol Faaliyetleri	Bilgi ve İletişim	İzleme
Bu işlemi gerçekleştirecek ve ihale dokümanını imzalayacak ekip, teklifi verenlerle herhangi bir finansal veya akdi ilişkisibulunmayan ehil kişilerden oluşur.	İhale teklifleri ve kamu sözleşmeleri ile bağlantılı risklerden biri içeriden bilgi sızdırılmasıdır. Teklif verenlerden biri diğer ihale dosyaları hakkında önceden bilgi sahibi olabilir ve sonuçta ihale teklifi en iyi olmayan bu teklif sahibinin üzerinde kalabilir. Bir diğer risk, yanlış teklif sahibini seçerek meydana gelir ki. Bu durumda bir teklif sahibinin beklentilerini karşılamaması yüzünden yeni bir kamu ihalesi yapılması icap edebilir. Haksızlığa uğradığını düşünen diğer teklif sahipleri de itiraz edebilirler.	Riskleri asgariye indirebilmek için prosedürler geliştirilmeli ve kamu ihaleleri ile ilgili bütün yasalara ve düzenlemelere göre davranmalıdır.	Bu ihale şartnamesinin bütün koşullarının ilanı ile bağlantılı prosedürler, alınan tekliflerin değerlendirilmesi ve kazanan Teklif sahibinin açıklanması yazılı olarak ve alınan önlemler ayrıntılarıyla dökümante edilmelidir. Teklifler değerlendirilirken, tekliflerin seçilme ve seçilememe nedenlerinin tümü belgelendirilmelidir.	İç denetim dosyası incelemesi yapabilir ve itirazları takip edebilir.

Düzenli, ahlaki, ekonomik, verimli ve etkin faaliyetler; örnek (1) : Kültür Müdürlüğü halkın müze ziyaretlerinin artmasını istiyor. Bunu başarmak için, yeni müzeler inşa edilmesini, her vatandaşa bir kültür çeki verilmesini ve bilet fiyatlarının azaltılmasını öneriyor. Ekonomik, verimli ve etkin olmak bakımından, yönetimin bu önerileri, formüle edildiği şekliyle, başarılıp başaramayacağını ve bu önerilerin her birinin kaça mal olacağını göz önünde bulundurması ve değerlendirmesi gerekir.

Kontrol Ortamı	Risk Değerlendirmesi	Kontrol Faaliyetleri	Bilgi ve İletişim	İzleme
Kültür Müdürlüğü yeni müzelerin planlaması ve faaliyetleri ile yeni önerilerin tasarlanması konusundaki gözetimini desteklemek bakımından organizasyon yapısının uygun olup olmadığından emin olmalıdır.	Müze ziyaretçilerinin sayısının artamaması olgusu muhtemel risklerden biridir. Ayrıca, önerilerden bazılarının ters tepki yaratması ve bütçesini aşma olasılığı bulunmaktadır. örneğin ; düşürülen bilet Fiyatları müze ziyaretlerini arttırmazsa, bu kamu gelirlerini düşürür. Dahası doğru planlama yapılmadan yeni müzeler inşa edilmesi, aydınlatma, ısı ve güvenlik ihtiyaçlarının göz önünde bulundurulması yapılanma sırasında ve sonrasında pahalı düzenlemelere neden olabilir.	Az önce sözü edilen risklerle ilgili kontrol faaliyetleri: fiili bütçe, yapılanma sürecinin gözlemleri ile bütçeyi aşan harcama talep kararlarını Karşılaştıran bir bütçe kontrolü olabilir.	Mimarlar, yangın söndürme departmanı (güvenlik yönetmelikleri bakımından), sanatçılar ve diğerleri ile yapılan toplantıların belgelenmesi bu olayla ilgili Bilgi ve iletişim faaliyetidir. Söz konusu belgeler, bütçe ve yapı çalışmasının süreci ile ilgili izleme hakkında da farklı raporları kapsayabilir.	Ertelenen çalışmalar veya ödemeler dolayısıyla bütçe aşımı ve ilgili yatırım maliyetleri ile ilgili kararların analizleri, izlemenin parçasıdır.

Düzenli, ahlaki, ekonomik, verimli ve etkin faaliyetler, örnek (2) : Hükümet tarımı geliştirmeyi ve kırsal kesimdeki yaşam kalitesini yükseltmeyi istemektedir. Sulama kanalları ve kuyu sondajları yapımını sübvanse eden fonları temin etmektedir.

Kontrol Ortamı	Risk Değerlendirmesi	Kontrol Faaliyetleri	Bilgi ve İletişim	İzleme
Hükümet sübvansiyon faaliyetini uygulamaya koymak ve yürütmek yerine, bunları yapmaya elverişli bir departmana sahip olmalıdır.	İlkesiz birliklerin yardıma hak kazanmalarına rağmen parayı arzulanan amaç için kullanmamaları, bağlantılı Risklerdendir.	Kontrol faaliyetleri şunlar olabilir: -Yardım için başvuruda bulunan birliklerin niteliklerinçek etmek. -İnşaat işlerinin gelişimini arazi üzerinde görmek ve bunlar hakkındaki gelişme raporlarını gözden geçirmek. -Faturalarını inceleyerek birliklerin harcamalarını denetlemek ve sübvansiyonun (veya bir bölümünü) ödenmesini söz konusu inceleme tamamlanıncaya kadar ertelemek.	-Maliyetleri ve açılan kuyu sayılarını ve sulanan arazi miktarını detaylandıran gelişme raporları. -Sübvanse edilen harcamaya karar vermek için faturanın (kopyası) istenmesi.	İzleme; kuyu sondajlarının, sulama kanalı inşaatlarının takip edilmesi ve diğer benzer projelerle karşılaştırmalarını kapsar. Ayrıca, sulanan arazilerin Hasılatlarının takibi de dikkate alınabilir.

Kaynakların korunması; örnek (1) : Savunma Bakanlığının ardiyeleri, askeri malları ve silah ambarları bulunmaktadır. Ordu komutanlığının politikası, bu tür malzemelerin kişisel yararlar için değil, askeri amaçlar için kullanılmasıdır.

Kontrol Ortamı	Risk Değerlendirmesi	Kontrol Faaliyetleri	Bilgi ve İletişim	İzleme
Bu tür ardiyelerde çalıştırılacak uygun nitelikte personelin işe alınmasında ve bunların elde tutulmasında, uygun beşeri sermaye politikaları yürürlüğe konmalıdır.	Kişilerin satmak ya da uygun olmayan biçimde kullanmak amacıyla silah çalma teşebbüsünde bulunmaları riski vardır. Keza benzin gibi diğer malzeme de çalınmaya müsait Olabilir.	Bu tür risklerle baş edecek kontrol faaliyetleri ardiye ve ambarların etrafına tel örgü çekmek ve duvar örmek veya girişlerine köpekli bekçiler yerleştirmek olabilir. Stok Kayıtlarını periyodik olarak çek etmek ve bu tür malların yanlızca üst düzey yetkilinin onayı ile verilebileceğini ifade eden bir kural koymak kaynakların korunmasına da yardımcı olur.	Tahrip olan tel örgüler ve stok sayımı sırasında görülen farklılıklar hakkındaki raporlar. Stok onayları ve prosedürleri de bu hedefle bağlantılı bilgi ve iletişim sağlar.	Tel örgülerin kontrol edilmesi bildirilmeyen stok sayımlarının soruşturulması, stok hareketlerinin takibi ya da gizli bir güvenlik testi bile izleme olabilir.

Kaynakların korunması; örnek (2) : Adalet Bakanlığının bir kuruluşunda çok miktarda hassas bilgi bilgisayar ortamında saklanmaktadır. Ancak bilişim teknolojisi kontrollerinin önemi küçümsenmekte ve bu yüzden de, Bilişim Teknolojisi kontrolünde önemli ölçüde yetersizlikler bulunmaktadır.

Kontrol Ortamı	Risk Değerlendirmesi	Kontrol Faaliyetleri	Bilgi ve İletişim	İzleme
Yönetimin : Bilişim teknolojisi konusunda ehil olma, sosyal ve ahlaki davranış kurallarına uyma taahhüdünün peşinden koşulmalı ve bu alanda uygun hizmet içi eğitim sağlanmalıdır. Bilişim teknolojisi meseleleri bakımından olumlu bir kontrol ortamı oluşturulmasında beşeri sermaye politikaları da önemli rol oynar.	Genel kontroller düzeyinde kuruluş: -Kullanıcı erişimini sadece görevleri gereği bilgiye ihtiyaç duyan kullanıcılarla sınırlandırmamıştır. -Programları ve hassas verileri korumak için sistem yazılım kontrollerini yeterince geliştirmemiştir. -Yazılım değişikliklerini dokümante etmemiştir. -Bağdaşmayan görevleri birbirinden ayırmamıştır. -Hizmet devamlılığıyla ilgilenmemiştir. -Ağ sistemini yetkisi bulunmayanlardan korumamıştır. Uygulama kontrolleri düzeyinde, kuruluş erişim görevlendirmelerini sürdürmemiştir. *(Bu husus iyi bir uygulama örneği değildir.)*	Kuruluş; -Mantıklı (örneğin: şifre) ve fiziksel (örneğin: kilitler, alarmlar, kimlik belirleme işaretleri) erişim kontrollerini Uygulamaya koyabilir. -Uygulama kullanıcılarının işletim sistemine giriş yapabilmelerini engelleyebilir. -Uygulamayı geliştirme personelininüretim ortamına Erişimini sınırlandırabilir. -Bütün erişimleri (teşebbüslerini) Kaydetmek için denetim kayıtlarından yararlanabilir ve güvenlik ihlallerini ortadan kaldırabilir. -Kritik kaynaklara ulaşabilirliği sağlamak ve faaliyetlerin Sürekliliğini kolaylaştırmak bakımından bir iş sürekliliği ve afet kurtarma planlarına sahip olabilir. -Güvenlik duvarları koyup ağ sisteminin güvenliğini sağlamak için web sunucusunun faaliyetlerini izleyebilir.	Bilişim teknolojisi ile ilgili prosedürler oluşturmalı ve yazılım değişiklikleri, yazılım programı faaliyetin bünyesine yerleştirilmeden Önce dokümante edilmelidir. Görevlerin ayrılması Prensiplerini destekleyici Politikalar ve iş tanımları geliştirilmelidir. Erişim (teşebbüsleri) ile ilgili denetim kayıtları ve (onaylanmamış) emirler periyodik olarak rapor edilip gözden geçirilmelidir.	Bir bilişim teknolojisi denetimi yürütülmesi, bir felaket tatbikatı yapılması ve web sunucu faaliyetinin izlenmesi Bilişim teknolojisi ortamının izlenmesinin bir parçası olabilir.

AVRUPA TOPLULUKLARI KOMİSYONU

16 EKİM 2007, BRÜKSEL
SEC (2007)1341

EN

KOMİSYONA TEBLİĞ EDİLMEK ÜZERE

İç Kontrol Standartları ve İç kontrol Çerçevesine İlişkin Gözden Geçirme

-Kontrol Etkinliğinin Artırılması-

1. ARTALAN BİLGİSİ

Komisyon, 2000 yılında başlatılan Mali Reformun bir parçası olarak yetkilendirme yoluyla Harcama Yetkililerini, faaliyetlerinin iç kontrolü konusunda tam yetkiyle donatmak amacıyla iç kontrol yapılarını gözden geçirmeye karar vermiştir. Faaliyetlerin yönetimi konusunda Komisyona güvence vermek amacıyla, Yıllık Faaliyet Raporları yoluyla yönetim düzenlemeleri hayata geçirilmiştir.

Reforma İlişkin Beyaz Kitap 2000[1] iç kontrolün, "Bir kurum yönetiminin, hedeferine ekonomik, verimli ve etkili bir şekilde ulaşmak; dış kurallara, yönetim politikaları ve düzenlemelerine bağlılığı sağlamak; varlıklar ve önemli bilgileri korumak; yolsuzluk ve hataları ortaya çıkarmak ve önlemek; muhasebe kayıtlarının kaliteli olmasını ve güvenilir mali bilgiler ve yönetim bilgilerinin zamanında üretilmesini sağlamak amacıyla planladığı ve hayata geçirdiği genel politika ve usulleri" kapsadığını ortaya koyar.

İç kontrol çerçevesi, 24 İç Kontrol Standardı ile oluşturulmuştur. Bu çerçeve, özellikle Komisyon için geliştirilmiş olup uluslararası iyi uygulama örneklerini temel almaktadır . İç kontrol sistemlerinin aşamalı olarak uygulanmasını ve bu sistemlerin gelişim düzeylerinin ölçülebilmesini sağlamak amacıyla, 2001 yılından itibaren tüm Standartlar için, her bir birimin iç kontrol sisteminde temel alınması gereken özel uygulamalı faaliyetleri tanımlayan bir dizi "temel gereklilik" uygulanmaktadır. 2002'den bu yana, birimlerden temel gerekliliklerle uyum düzeylerini her yıl resmi olarak değerlendirmeleri istenmektedir. Yıllık değerlendirmelerin sonuçları, iç kontrol yapılarının bütün olarak başarılı bir şekilde uygulanmakta olduğunu göstermektedir. Birimlerin temel gerekliliklerle uyum düzeylerinin oldukça yüksek olduğu görülmüştür (2005 ve 2006'da %95).

Komisyon 2005 yılında bir "ortak risk yönetimi yöntemi"[3] benimsemiştir. İç Kontrol Sisteminin gözden geçirilmesinin önerildiği işbu belgede söz konusu yöntemin tüm ilkeleri dikkate alınmıştır.

2. ÖNERİLEN DEĞİŞİKLİKLERLE ULAŞILMAK İSTENEN AMAÇLAR

Tüm modern idarelerde olduğu gibi, Komisyonun iç kontrol sistemlerinin de Komisyon faaliyetlerinin yerine getirilmesi konusunda yeterli güvence sağlaması gerekmektedir. Bu yüzden her düzeydeki yönetimin, sadece kontroller yaptığını değil, bu kontrollerde ilgili riskleri de dikkate aldığını ve kontrolleri öngörüldüğü şekilde yaptığını da göstermesi gerekmektedir. Bu gereklilik, iç kontrol çerçevesine yapılan vurgunun yeniden değerlendirilmesini ve mevcut Standartların yedi yıllık deneyim temelinde modernleştirilmelerini de beraberinde getirir. Böylece Standartlar, tüm personel tarafından anlaşılabilir ve kullanılmaya hazır bir hale gelir.

Bu gerekliliğin karşılanması, mevcut Standartlarda küçük değişiklikler yapılması veya temel gerekliliklerde önemsiz değişikliklere gidilmesi anlamına gelmemektedir. Mevcut Standartlar bazı çevrelerce tam olarak anlaşılmış olsa da, birimlerden alınan geribildirimler iç kontrol çerçevesinin daha açık olması gerektiğini ve kilit alanlar üzerindeki kontrollere odaklanmaya ve risk-temelli kontrol önlemlerinin alınmasına imkan tanıyacak daha esnek bir yaklaşımın benimsenmesinin faydalı olacağını ortaya koymaktadır. Bazı çevrelerde yaygın olan "iç kontrol sadece belirli sayıdaki 'mali' personelin işidir" inancını yıkmak için, tüm personelin (özellikle de tüm yöneticilerin), faaliyetlerin sağlıklı bir iç kontrole tabi tutulmasında üstlenmeleri gereken roller güçlendirilmelidir. Bu bağlamda, görevler ayrılığı ilkesi, sadece mali sorumluluklarla sınırlandırılmamış aynı zamanda uluslararası

uygulamalara paralellik gösterecek şekilde genişletilmiştir.

Devam etmekte olan bürokrasiden uzaklaşma ve sadeleşme çabaları çerçevesinde, iç kontrolün en üst yönetimden en alt düzeydeki çalışana kadar tüm personelin sorumluluğu olduğu mesajını vermek amacıyla, gözden geçirilen Standartlar uzmanlık terimleri kullanılmaksızın daha basit bir dille yazılmıştır. İşbu tavsiye, mevcut Standartlardaki çakışmaları ortadan kaldırmakta ancak Standartların metodolojik temelini değiştirmemekte ve gerekmeyen alanlarda herhangi bir değişiklik yapmamaktadır.

Bu bilgiler ışığında, iç kontrol çerçevesi ve Standartlarda yapılan değişiklikler şunları amaçlamaktadır:

Yaklaşımın Açıklığa Kavuşturulması/Sadeleştirilmesi: Tüm personelin anlamasını kolaylaştırmak ve zorunlu yıllık raporlamayı temel gerekliliklerle uyumlu bir şekilde düzenlemek için,

Sahiplenme Hissini Artırmak: Standartları "Etkili yönetim için îç Kontrol Standartları" olarak yeniden adlandırarak daha geniş bir çalışan grubuna hitap etmek ve **iç kontrol ortanınım kalitesini artırmak** için,

İç Kontrolün Etkililiğini Artırmak: Esnek bir yaklaşım ve tercihli Etkililik Rehberi, birimlere kendi faaliyet ve risklerini dikkate alarak, etkililik artırma faaliyetleri kapsamında Standartları önceliklendirme şansı verecektir. Böylece, **Komisyonun İç Kontrol sistemlerinin etkililiğine duyulan güven artar ve kontrol kaynaklarının daha etkili kullamlması sağlanır.**

3. GÖZDEN GEÇİRİLEN İÇ KONTROL ÇERÇEVESİ

Yeni Standartların **1 Ocak 2008'de** yürürlüğe konması önerilmektedir. Gözden geçirilen iç kontrol çerçevesi, birbiriyle yakından ilişkili üç temel bileşenden oluşacaktır:

Etkili yönetim için İç Kontrol Standartları;

Daha önceki temel gereklilikleri temel alan ve yeni Standartlar çerçevesinde yeniden düzenlenen ve güncellenen "Gereklilikler" Birimlerin uygulamakta oldukları iç kontrol sistemlerinin etkililiğini ölçmelerini sağlayan İç Kontrol Etkililik değerlendirmesi. Bu bağlamda, kendilerine yardımcı olmak amacıyla tercihli rehber sunulmaktadır. [7]

7Bu hususlar Şekil l'de ortaya konmakta ve Bölüm 3.1 -3.3'te tartışılmaktadır.

Şekil 1 – İç Kontrol Çerçevesine Genel Bakış

"Etkililik Rehberi" (Tercihlidir), iç kontrol düzenlemelerinin birimin faaliyet ve risklerini yeterli düzeyde karşılayıp karşılamadığını ve bunların öngörüldüğü şekilde uygulamaya aktarılıp aktarılamadığını belirlemelerinde yönetimlere yardımcı olur.

Etkili yönetim için İç Kontrol Standartları (ICS) ve Gereklilikler, iç kontrol çerçevesinin temelini oluşturur. Temel ilkeler ve asgari gereklilikleri ortaya koyar.

Söz konusu Çerçeve yukarıda değinilenlere ek olarak ve gerekliliklere uyma şartı temelinde hangi standartlarda etkililiğe daha fazla önem verilmesi gerektiğini belirlemede birimlere gerekli esnekliği sağlayacaktır.

Etkili Yönetim İçin Gözden Geçirilen İç Kontrol Standartları

İç kontrole ilişkin yol gösterici ilkeler, Komisyon tarafından "etkili yönetim için yeni İç Kontrol Standartlarında" (EK 1) ortaya konulmuştur. Standartlar altı "yapı taşı" temelinde yapılandırılmıştır.

1. Misyon ve Değerler,
2. İnsan Kaynakları,
3. Planlama ve Risk Yönetimi Süreçleri,
4. İşlemler ve Kontrol Faaliyetleri,
5. Bilgi ve Mali Raporlama,
6. Değerlendirme ve Denetim.

Yeni çerçevede risk yönetimi güçlendirilmiştir. Temel risk yönetimi ilkeleri (kontrollerin tanımlanan risklere uyarlanması) etkili yönetim için tüm İç Kontrol Standartlarına uygulanır ve aşağıda açıklanan Yaklaşımda Esneklik ve Rehberlik (Bölüm 3.3) daha yüksek düzeyli riskleri gösteren Standartlara odaklanmalarında birimlere yardımcı olur. Ayrıca, yeni standart 6 (risk yönetimi süreci) özellikle yıllık planlama aşamasında risklerin tanımlanması sürecine yöneliktir ve ortak risk yönetimi yöntemi kapsamında ortaya konan ilkelerle uyumludur.

Uygulayıcılar için genellikle karmaşa yaratan çakışmaların ortadan kaldırılmasının ardından standartlar güncellenip modernleştirilmiştir ve sayıları 24'ten 16'ya düşürülmüştür. Bunun kontrolünde herhangi bir azalmaya neden olduğu düşünülmemelidir. Önceki iç kontrol standartlarının kapsamına giren tüm alanlar yeni standartlar temelinde yeniden gruplandırılmıştır. Standartlar iki değerlendirme aracı ile desteklenmektedir.: aşağıdaki bölümlerde ayrıntılı olarak anlatılacak olan "Gereklilikler" ve "Etkililik Rehberi"

Gereklilikler

Gereklilikler (EK 2) bir birimin iç kontrol sistemleri ve süreçlerinin taşıması gereken asgari

özellikleri tanımlar. Bu gereklilikler modernleştirilip güncellenen önceki temel gereklilikelri yansıtmaktadır. Ayrıca birimlerin, kuralların daha açık olması ve sapmaların raporlanmasına yönelik prosedürler geliştirilmesi yönündeki istekleri ile zorunlu personel yer değiştirmeleri halinde hizmetlerin devamlılığını sağlama ihtiyaçları karşısında hassas işlevlere ilişkin gerekliliklerde (Yeni standart 7, işleyiş yapısı) de değişiklikler yapılmıştır. Hassas işlevler konusunda 2007 yılı sona ermeden önce bir dizi rehberlik hizmeti daha sunulacaktır.

Gerekliliklerin görece aynı (sabit) kalması ve sadece, iç kontrol çerçevesini etkileyebilecek komisyon kararlarının alınması ya da bu etkiyi yaratabilecek diğer durumların meydana gelmesi halinde gözden geçirilmesi amaçlanmaktadır. Birimler, tüm bu gerekliliklere eksiksiz olarak uymayı temel bir hedef olarak görmeli ve bunun personel yer değiştirmeleri veya yeni gereklilikler gibi nedenlerle ulaşılması çok da kolay olmayan bir hedef olduğunu unutmamalıdırlar.

AB Delegasyonu açısından, geçmişte de olduğu gibi , Dış İlişkiler Genel Müdürlüğü ve Avrupa Yardım İşbirliği Ofisi söz konusu gereklilikleri Bütçe GM'nin de desteğini alarak çalışma ortamlarına uyumlu faaliyetlere dönüştürmeye devam edecektir.

İç Kontrolün Etkililiği

Gözden geçirilmiş çerçevede yer alan, etkililikle ilişkili, güçlendirilmiş unsur.

Yaklaşımda Esneklik

Birimler iç kontrol sistemlerinin etkili olduğunu göstermek için izleme önlemleri almaktadır. Etkili ve etkin bir iç kontrol sistemi, yönetimin riski göz önünde bulundurmasını, kontrol kaynaklarını riskin en yüksek olduğu alanlara yönlendirmesini ve tüm faaliyetler üzerinde yeterli kontrolü sağlamasını gerektirir.

Dolayısıyla gözden geçirilmiş yaklayım bazı standartların bazı faaliyetler için daha önemli olabileceğini ve bu önemin zamanla değişebileceğini ortaya koymaktadır. Bu nedenle birimlerin, belirli alanlardaki etkililiği arttırmak için gerekli önlemleri almak ve Genel Müdürlerin yıllık güvence beyanlarını daha güçlü temellere oturtmak amacıyla, belirli standartlara öncelik vermesi mümkün olur.

Yıllık yönetim planı, birimlerin -kendi faaliyet ve riskleri temelinde- gelecek yıl etkililiği arttırmak için hangi standartlara öncelik verilmesi gerektiğini belirlemelerine imkan tanıyacaktır. Öncelikli standartlar, yönetim tarafından kendi risk değerlendirmesi temelinde belirlenecektir. Sorunsuz bir geçiş için birimlerin, mevcut 24 iç kontrol standartını uygulayarak elde ettikleri bilgi birikimi ve deneyim temelinde, bu öncelikleri 2008 yıllık yönetim planında ortaya koymaları gerekmektedir (Eski ve yeni Standartların karşılaştırıldığı bir eşleştirme tablosu EK 4'te sunulmuştur). Standartların önceliklendirilmesi, risk yönetimi uygulamasının mantıklı bir sonucudur7.

İç Kontrolde Etkililik Tercihli Rehberi

Bir bütün olarak iç kontrol sisteminin etkililiği, uygun göstergeler yoluyla ölçülebilir. Ancak, Standartlar birbirlerine bağlı olduğu için, genel göstergeler yoluyla her bir Standardın ne kadar etkili uygulandığını ayrı ayrı ölçmek neredeyse imkansızdır. Bununla birlikte, her bir Standart bir dizi değişken yoluyla değerlendirilebilir (süreç gözden geçirmeleri, yönetim tarafından yapılan gözetim faaliyetleri, geçici doğrulamalar, anket ve görüşmeler, yönetimce yapılan öz değerlendirmeler, denetim raporları, paydaş geribildirimleri gibi). Bu değerlendirme, Bütçe GM tarafından hazırlanan tercihli rehberle desteklenebilir. EK'te sunulan Etkililik Rehberi, her bir Standart için şu iki unsuru içerir: (1) "Kontrol etkililiğini değerlendirmeye yönelik tavsiyeler" (EK 2), yönetimlere iç kontrol düzenlemelerinin uygulamaya öngörüldüğü şekliyle aktarılıp aktarılmadığını ve ilgili risklere uyarlanıp uyarlanmadığını belirlemelerinde yardımcı olabilecek bir dizi soru ve (2) yönetimlere, birime özgü faaliyetler ve riskleri de dikkate alarak, kendilerini en çok ilgilendiren standartları belirlemelerinde yardımcı olabilecek bir değerlendirme tablosu (EK 3).

Bu rehberin, tüm birimlerce yerine getirilmesi veya birim performansını değerlendirirken gösterge olarak kullanılması gereken herhangi bir dizi ek gereklilik veya kontrol listesi getirmesi amaçlanmamaktadır. Rehber yol gösterici olup yeterince ayrıntı içermemekte ve bağlayıcı nitelik taşımamaktadır. Birimler rehberi, kendi ihtiyaçları doğrultusunda belirli unsurları kabul ederek veya yenilerini tanımlayarak kabul etmekte serbest olacaktır. Rehberin amacının gerisinde kalmasını önlemek için

(tercihli olduğu da göz önünde bulundurularak) Bütçe GM Genel Müdürü, Genel Sekreter ve Personel ve îdare GM Genel Müdürü ile işbirliği içinde ve ilgili birimlerin de görüşünü alarak, rehberi gerekli şekilde günceller. Bütçe GM, etkililiğin değerlendirilmesi konusunda tavsiyelerde bulunacaktır.

Raporlama Zorunluluğu

Genel Müdürler, Yıllık Faaliyet Raporlarında iç kontrol sistemlerinin işleyişi hakkında güvence vermeye devam edecektir (özellikle Bölüm 2'de sunulan îç Kontrol Şablonları yoluyla). Gözden geçirilmiş iç kontrol çerçevesini hazırlamak ve sunmak için, Yıllık Faaliyet Raporu kapsamında yer alması önerilen raporlama ilkeleri şunlardır:

Gerekliliklerle uyumlu raporlama:

Gerekliliklerle uyumlu raporlama sadeleştirilecektir. 2007 Yıllık Faaliyet Raporları ile birlikte, temel gerekliliklerle uyumlu eksiksiz raporlama, zorunlu olmaktan çıkarılacaktır. Bunun yerine, Yılık Faaliyet Raporları kapsamındaki uyum raporlamaları istisnai durumlarda yapılacaktır. Sonuçların hangi gereklilikler temelinde elde edildiği ve birimin uymadığı gereklilikler (varsa), bu uyumsuzluğun nedenleri ve bu durumu çözmek için alınması planlanan önlemler belirtilecektir. Hassas işlevlerle ilgili olarak, zorunlu personel yer değiştirmelerinde ortaya çıkan sapmalar hakkında özet bilgi de verilecektir (2008 Yıllık Faaliyet Raporuyla birlikte). Son olarak, sapmalara izin verilen durumlarda ilgili yatay birimlere yazılı bildirimde bulunulması uygulamasına da son verilecektir. Temel gerekliliklere uyum konusunda eksiksiz rapor hazırlamak isteyen birimler için, Mevcut araç ("ICMT") ve Bütçe GM desteği sağlanmaya devam edecektir.

İç kontrol sistemlerinin etkililiğinin raporlanması:

Güvence konusundaki görüşleri desteklemek amacıyla; yönetimce yapılan öz değerlendirmeler, denetim raporları, harcama sonrası kontroller ve diğer ilgili kaynaklar incelenerek derlenen "iç kontrol sistemlerinin etkililiği hakkındaki" bilgiler Yıllık Faaliyet Raporlarında açıkça ortaya konmalıdır. Raporlarda (2008 Yıllık Faaliyet Raporuyla birlikte), Yıllık Yönetim Planında tanımlanan öncelikli Standartlar konusunda atılan adımların sonuçlarına da yer verilmelidir.

Verimliliğin sağlanması amacıyla; uygunluk konusunda raporlamaya istisnai durumlarda başvurulması ve birimlerin belirli standartlar üzerinde yoğunlaşmasına izin verecek şekilde esnekliğin artırılması, mevcut zorunlu raporlama sistemine gerektirdiğinden daha fazla bir iş yükü getirmemekle birlikte yüksek öncelikli iç kontrol konularına yönelme şansı da tanıyacaktır.

Yıllık Faaliyet Raporunda yer alan talimatlar gerekli şekilde güncellenecektir. 2007 Yıllık Faaliyet Raporları, mevcut 24 Standart çerçevesinde hazırlanacaktır.

ANLAYIŞ VE SAHİPLENME HİSSİNİN GELİŞTİRİLMESİNE YÖNELİK DESTEK

Gözden geçirilmiş iç kontrol çerçevesinin tüm personel tarafından daha iyi anlaşılması ve daha çok sahiplenilmesi için ve birimlerde iç kontrol etkililiğinin artırılması ve Genel Müdürlerin yıllık güvence beyanlarının desteklenmesi amacıyla aşağıdaki adımların atılması gerekmektedir:

Üst yönetim desteği: Üst yönetim, teşkilatlanmasını ve risk atmosferini de göz önünde bulundurarak, iç kontrol etkililiğinin artırılması için Standartları önceliklendirir ve iç sorumlulukları tanımlar8. Üst yönetimin, iç kontrol bilincinin artırılması ve iç kontrol becerilerinin kazandırılması için gerekli zamanı ve kaynağı ayırması, Standartların çalışma ortamına daha çok entegre edilmesi açısından çok önemlidir.

Etkili iletişim:

Her düzeydeki personelin bilgilendirilmesi ve bu konuda bilincin artırılması amacıyla iletişim

Merkezi birimlerce verilecek destek:

Bütçe GM, birimler arasında başarılı uygulama ve deneyim alışverişi yapılmasını kolaylaştıracaktır. Etkililik Rehberi ve iletişim faaliyetleri, birimlerin deneyimleri ve geribildirimleri temelinde güncellenecektir. Geçmişte de olduğu gibi, Stratejik Planlama ve Programlama döngüsünün değişik aşamalarında -özellikle Yıllık Yönetim Planları ve Yıllık Faaliyet Raporları aşamalarında- birimlere destek verilmeye devam edilecektir.

Standartların benimsenme ve anlaşılma düzeylerinin ölçülmesi: 2008 yılı tamamlanmadan önce, bilinç ve sahiplenme düzeylerini değerlendirmek ve gerekli olması durumunda Bütçe GM ve birimleri de kapsayan destek ve iletişim faaliyetlerini yeniden düzenlemek amacıyla, İç Kontrol Koordinatörleri aracılığıyla örneklem temelli bir araştırma yapılacaktır.

SONUÇ

2000 yılındaki Mali Reformla birlikte kurulan iç kontrol yapıları, özellikle mali çevrelerin düzenlenmesi ve İç Kontrol Standartlarıyla ilgili temel gerekliliklere uyum alanları başta olmak üzere, başarılı bir şekilde hayata geçirilmiştir. Ancak, kontrollerin etkili bir şekilde uygulamaya aktarılmasını sağlamak için yapılması gereken daha çok şey vardır. Ayrıca, tüm personelin iç kontrol alanındaki sorumluluklarının bilincinde olmasını sağlamak için atılması gereken daha çok adım vardır. Etkili yönetim için Gözden Geçirilmiş İç Kontrol Standartlarının sunumu ve bu Standartları destekleyen rehber bu süreci kolaylaştıracaktır. Yeni yaklaşımla bütünleşen esneklik, birimlere, hükümleri kendi özel koşularına uyarlama şansı da verecektir.

Bu bilgiler ışığında, Komisyona şunlar teklif edilmektedir;

-EK 1 ve 2'de sunulan "etkili yönetim için İç Kontrol Standartları" ve "etkili yönetim Gerekliliklerini" de kapsayan gözden geçirilmiş İç Kontrol çerçevesini kabul etmek;

-Gereklilikler üzerinde etkisi olacak bir Komisyon Kararı hazırlayan her birime, Genel Sekreter, Personeli ve İdare GM ve Bütçe GM ile işbirliği yapması ve Karar metnine Gerekliliklerde yapılacak değişiklikleri de dahil etmesi talimatını vermek ve Bütçe GM'ye ereklilikleri güncel tutma yetkisi vermek;

-Gözden geçirilmiş Standartlar ve ilgili Gerekliliklerin 1 Ocak 2008'den itibaren uygulamaya konmasına karar vermek;

-Uygunluk arşılaştırması yapabilmek amacıyla, 2006 temel gerekliliklerinin 24 İç Kontrol Standardı

emelinde 31 Aralık 2007'de uygulamaya konmasına karar vermek (2007 'den itibaren geçerli lan tarihler ve İş Devamlılığının Planlanmasına ilişkin gereklilikler çerçevesinde güncellenmek koşuluyla);

-Birimlerden Yıllık Yönetim Planlarında (ilk kez YYP 2008 için), kontrol etkililiğini kontrol etmek amacıyla önceliklendirmek istedikleri Standartları belirtmelerini istemek (YYP 2008 dikkate alındığında, söz konusu standartların önceliklendirilmesinde mevcut 24 Standarda ilişkin bilgi birikimi ve deneyimi temel alacaktır);

-2007 Yıllık Faaliyet Raporlarından itibaren birimlerin (Temel) Gerekliliklerle uyumunun raporlanmasına ilişkin talimatları düzenlemeleri için Genel Sekreter, Personel ve İdare GM ve Bütçe GM'yi görevlendirmek; Bütçe GM'yi, bilgilendirme oturumları gerçekleştirilmek ve 2007 Sonbaharında uygulanmaya başlanacak olan iç kontrol eğitim programını gözden geçirilmekle görevlendirmek;

-Birimleri, gözden geçirilmiş standartları uygulamak konusunda teşvik etmek ve tüm personelin kontrol etkililiği konusunda anlayış ve bilincinin artırılmasına yönelik doğru eylemleri, özellikle eğitim, bilgilendirme ve destek faaliyetleri gerçekleştirmek;

-Genel Sekreter, Personel ve İdare GM ve Bütçe GM'yi 2007 bitmeden önce 2008' de uygulanmak üzere hassas işlevler konusunda gözden geçirilmiş rehberi hazırlamakla görevlendirmek;

-Bütçe GM Genel Müdürünü-Genel Sekreter ve Personel ve İdare Genel Müdürü ile anlaşma temelinde ve ilgili diğer birimlerle istişare içinde tercihli etkililik rehberinde gelecekte gerekli değişiklikleri yapmakla yetkilendirmek.

EK 1 – ETKİLİ YÖNETİM İÇİN GÖZDEN GEÇİRİLEN İÇ KONTROL STANDARTLARI

Açıklama: İşbu EK kapsamında "GM" Genel Müdürlük, birim, bakanlık veya uygulayıcı kurum anlamına gelmektedir.

Misyon ve Değerler

1. **Misyon:** GM'nin kuruluş nedeni, GM hedef kitlesinin bakış açısıyla oluşturulmuş güncel ve kesin misyon ifadeleriyle açık bir şekilde ortaya konur.
2. **Etik ve Kurumsal Değerler:** Yönetim ve personel etik ve kurumsal değerler hakkında bilgi sahibidir ve bu ortak değerleri paylaşır ve kendi davranışları ve karar alma mekanizmaları yoluyla hayata geçirip destekler.

İnsan Kaynakları

3. **Personel Atamaları ve Personel Yer Değiştirmeleri:** Personel atama ve işe alımları GM'nin hedef ve öncelikleri temelinde yapılır. Yönetim, personel sürekliliği ve yenilenmesi arasında doğru bir denge kurabilmek amacıyla personel yer değiştirmelerini düzenler ve planlar.
4. **Personel Değerlendirme ve Geliştirme:** Personel performansı, GM'nin genel hedefleriyle uyumlu yıllık bireysel hedefler temelinde değerlendirilir. Söz konusu hedeflere ulaşmak için gerekli becerileri geliştirmek amacıyla yeterli önlemler alınır.

Planlama ve Risk Yönetimi Süreçleri

5. **Hedefler ve Performans Göstergeleri:** GM'nin hedefleri açık bir şekilde tanımlanır ve gerekli durumlarda güncellenir. Hedefler, bu hedeflere ulaşılıp ulaşılamadığının izlenebilmesini mümkün kılacak şekilde belirlenir. Yönetimin hedefler konusunda kaydedilen ilerlemeyi değerlendirmesi ve raporlamasını kolaylaştırmak amacıyla kilit performans göstergeleri belirlenir.
6. **Risk Yönetimi Süreci:** Mevcut hükümler ve kılavuz ilkelerle uyumlu bir risk yönetimi süreci, yıllık faaliyet planlamasına dahil edilir.

İşlemler ve Kontrol Faaliyetleri

7. **İşleyiş Yapısı:** GM'nin işleyiş yapısı, yetkilerin uygun şekilde paylaştırılması yoluyla kararların etkili bir şekilde alınmasını sağlar. GM'nin hassas işlevleri ile ilişkili riskler, hafifletici kontroller ve gerekmesi durumunda personel yer değiştirmeleri yoluyla yönetilir. Yeterli BT yönetim yapıları mevcuttur.
8. **Süreçler ve Prosedürler:** GM'nin faaliyetlerinin hayata geçirilmesi ve kontrolünde başvurulan süreç ve prosedürler etkili ve etkindir, yeterli düzeyde belgelendirilmiştir ve mevcut hükümlere uygundur. Bu süreç ve prosedürler, görevler ayrılığının gerçekleştirilmesini sağlayan düzenlemeleri, bazı kontrollerin önceden onay verilmesine ilişkin düzenlemeleri kapsar.
9. **Yönetim Tarafından Yapılan Gözetim:** Yönetim tarafından yapılan gözetim, faaliyetlerin mevcut hükümler çerçevesinde etkin ve etkili şekilde uygulanmasını sağlamayı amaçlar.
10. **İş Sürekliliği:** "Düzenli iş akışında" meydana gelebilecek aksaklıklar durumunda birimin devamlılığını sağlamak için gerekli önlemler alınır. İş sürekliliği planları, büyük bir aksaklık halinde bile komisyonun mümkün olan en üst düzeyde çalışmaya devam edebilmesini sağlamayı amaçlar.
11. **Belge Yönetimi:** GM'nin belge yönetiminin güvenli, etkin (özellikle uygun bilginin geri çağrılması konusunda) ve mevzuata uygun bir şekilde gerçekleştirilmesini sağlamak amacıyla gerekli işlem ve prosedürler mevcuttur.

EK 2- ETKİLİ YÖNETİM İÇİN İÇ KONTROL STANDARTLARI, GEREKLİLİKLER VE TERCİHLİ ETKİLİLİK REHBERİ

(HER BİR STANDART İÇİN KULLANILACAK "ŞABLON")

Açıklama: İşbu EK kapsamında "GM" Genel Müdürlük, birim, bakanlık veya uygulayıcı kurum anlamına gelmektedir. Gereklilikler, AB Delegasyonlarına yönelik belirli faaliyetlere dönüştürülecektir.

ICS 1. Misyon: GM'nin kuruluş nedeni, GM'nin hedef kitlesinin bakış açısıyla oluşturulmuş güncel ve kesin misyon ifadeleriyle açık bir şekilde ortaya konur.

GEREKLİLİKLER

- GM, Müdürlükler ve Birimlerin, tüm hiyerarşik düzeylerle ilişkili güncel misyon tanımları olmalıdır.

- Bu misyon tanımları, personele açıklanmalı ve her zaman erişime açık olmalıdır.

KONTROL ETKİLİLİĞİNİN DEĞERLENDİRİLMESİNE YÖNELİK TAVSİYELER

Bilgi Notu: Kontrol etkililiğini değerlendirirken, iki temel soru sorulmalıdır. :

1. GM'nin kendine özgü faaliyet ve risklerini dikkate alarak, mevcut kontrol düzenlemeleri yeterli mi?
2. Kontrol düzenlemeleri öngörüldüğü şekliyle uygulamaya aktarılabilmiş mi?

Yönetimin, söz konusu ICS kapsamında kontrol etkililiğini değerlendirirken dikkate almak isteyebileceği bazı sorular aşağıda verilmiştir:

- GM/Müdürlük/Birimin misyon tanımı güncel ve yeterince yapılandırılmış mı? Etkili bir misyon tanımı , GM/Müdürlük/Birimin hedef kitlesinin bakış açısıyla oluşturulmuş bir misyon tanımı olmalıdır. Bu tanımın iki temel soruyu cevaplaması gerekmektedir. Kuruluş amacımız nedir? Komisyon yapısı içinde neredeyiz?
- Personel bağlı olduğu GM/Müdürlük/Birimin misyon tanımı hakkında yeterince bilgi sahibi mi?
- Bir misyon tanımı oluşturmak veya var olan tanımı güncellemek için belirli personel/paydaşları görevlendirmek uygun olur mu? (örn. Her bir çalışanının görevlendirilmesi sürecinin başında)?

ICS 2. Etik ve Kurumsal Değerler: Yönetim ve personel etik ve kurumsal değerler hakkında bilgi sahibidir ve bu ortak değerleri paylaşır ve kendi davranışları ve karar alma mekanizmaları yoluyla hayata geçirip destekler.

gereklilikler

• GM, tüm personelin özelikle etik kurallar başta olmak üzere ilgili etik ve kurumsal değerler hakkında bilgi sahibi olmasını sağlamak, çıkar çatışmalarını ve yolsuzluğu önlemek ve usulsüzlüklerin raporlanmasını sağlamak amacıyla -güncellemeler ve yıllık hatırlatmalar gibi- belirli prosedürler uygulamalıdır.

KONTROL ETKİLİLİĞİNİN DEĞERLENDİRİLMESİNE YÖNELİK TAVSİYELER

Bilgi Notu: Kontrol etkililiğini değerlendirirken, iki temel soru sorulmalıdır:

GM'nin kendine özgü faaliyet ve risklerini dikkate alarak, mevcut kontrol düzenlemeleri yeterli mi?

Kontrol düzenlemeleri öngörüldüğü şekliyle uygulamaya aktarılabilmiş mi?

Yönetimin, söz konusu ICS kapsamında kontrol etkililiğini değerlendirirken dikkate almak isteyebileceği bazı sorular aşağıda verilmiştir:

- GM'ye özgü etik bir rehber anlamlı olur mu? Örneğin, "Çıkar Çatışması" ile ilgili kurallar Komisyon'daki herkese uygulanıyor olsa da, önemli satın alma faaliyetleri yürüten bir GM/Müdürlük/Birim bu noktaya daha fazla önem vermek isteyebilir. İç bilginin nasıl kullanılacağı ve mali yolsuzlukları önlemek, belirli GM/Müdürlük/Birimin üzerinde durmak isteyeceği diğer önemli konulardır.
- Etik rehber açık, net ve kullanıcı dostu mu? Davranış Kuralları/Rehberin nasıl yazıldığı, söz konusu Kurallar ve Rehberin etkililiği üzerinde etkili olacaktır. Araştırmalar, en etkili davranış kurallar inin kısa ve net olan, birkaç temel mesaj üzerinde odaklanan ve açık ve net bir terminolojinin kullanıldığı kurallar olduğunu göstermektedir.
- Personel, etik ve dürüstlükle ilgili farklı gereklilikler ve hükümler hakkında yeterince bilgiye sahip mi (yeni gelenlerin eğitimi, düzenli bilgilendirme vb. yoluyla bilgilendirme)? Personelin bilinç düzeyi anketler gibi yöntemler kullanılarak analiz edilebilir.
- Davranış kuralları ve etik rehberliklerin pratikte uygulanmasına yönelik olarak yeterli kolaylık sağlanıyor mu? Örneğin, usulsüz uygulamalardan şüphelenmeleri halinde personele gizli raporlama şansı verecek erişilebilir ve güvenli kanallar sağlamak, davranış kurallarının daha etkili bir hal almasını sağlayabilir.
- Gözetim faaliyetleri, denetim raporları, raporlanan sapmalar ve diğer ilgili kaynaklardan elde edilen bilgilerle ulaşılan sonuçlar, GM7Müdürlük/Birimlerde etik sorunlar ve problemler olabileceğini ortaya koymuştur. Bu problemleri çözmek için yeterli önlemler alınmış mı?

ICS 3. Personel Atamaları ve Personel Yer Değiştirmeleri: Personel atama ve işe alımları GM'nin hedef ve öncelikleri temelinde yapılır. Yönetim, personel sürekliliği ve yenilenmesi arasmda doğru bir denge kurabilmek amacıyla personel yer değiştirmelerini düzenler ve planlar.

GEREKLİLİKLER

- Yönetim gerekli olduğu hallerde -asgari yılda bir kez-, kurumsal yapılar ve personel atamaları ile öncelikler ve iş yükü arasında bir denge kurmalıdır.
- Personel iş tanımları ile ilgili misyon tanımı arasmda tutarlılık olmalıdır.
- GM'nin, doğru kişinin doğru işte ve doğru zamanda çalışmasını sağlamak ve mümkün olduğu durumlarda insanlar için uygun kariyer fırsatları yaratmak amacıyla, personel hareketliliğini desteklemesi, uygulaması ve izlemesi gerekmektedir (örn, boş kadroların bildirilmesi, uzman kadrolarının listelerinin hazırlanması gibi yollarla).
- Ekibe entegrasyonu kolaylaştırmak amacıyla, işe yeni başlayan personele gerekli destek verilmeli ve bu desteğin niteliği tanımlanmalıdır.

KONTROL ETKİLİLİĞİNİN DEĞERLENDİRİLMESİNE YÖNELİK TAVSİYELER

Bilgi Notu: Kontrol etkililiğini değerlendirirken, iki temel soru sorulmalıdır:

GM'nin kendine özgü faaliyet ve risklerini dikkate alarak, mevcut kontrol düzenlemeleri yeterli mi?

Kontrol düzenlemeleri öngörüldüğü şekliyle uygulamaya aktarılabilmiş mi?

Yönetimin, söz konusu ICS kapsamında kontrol etkililiğini değerlendirirken dikkate almak isteyebileceği bazı sorular aşağıda verilmiştir:

- Etkili personel planlama ve atamasmı sağlamak için gerekli düzenlemeler yapılmış mı? Yönetimin, öncelikler ve personelin iş yükü ile gerekli ve mevcut beceriler konusunda yeterli bilgisi var mı?
- İşe alım ve personel ataması konularmda, GM/Müdürlük/Birimin performansını önemli düzeyde etkileyecek herhangi bir sorun veya problem var mı? Mevcut işe alım ve personel ataması prosedürlerinde GM düzeyinde yapılacak değişiklikler bu problemleri çözebilir mi? Nasıl?
- Esnek ve dinamik bir kurum yapısı sağlamak için, yoğun ve hızlandırılmış eğitimler, yeniden örgütlenme veya diğer önlemlerin almması gibi yollarla gerekli önlemler alınmış mı?
- İşe girip çıkan personel sayısı yeterli düzeyde izlenip inceleniyor mu? İşe girip çıkmaların "aşırı" ve "az" düzeyde oluşuna ilişkin GM oranlarının belirlenmesi faydalı olabilir. Personel işe giriş-çıkışlarında görülen bir düzensizliğin temel nedeni yeterince incelenip ortanda kaldırılmaya çalışılmış mı?
- İşe giren-çıkan personel sayısında bir "aşırılık" olması durumunda, gerekli becerilere sahip personelin birimde tutulması konusunda gerekli önlemler alınmış mı? Benzer şekilde, işe girip-çıkan personelin sayısı "gereğinden azsa", GM içinde veya dışarıdan personel yer değiştirmesi yapılması için gerekli önlemler alınmış mı? Bu önlemler başarılı olmuş mu? Başarılı olmamışsa, neden?
- Orta düzey yönetimin yer değiştirmesi veya yönetim ekibinin ve/veya kilit personelin tamamen değiştirilmesi planlanırken, birimin çıkarları göz önünde bulundurulmuş mu? Muhtemel bilgi eksikliği yeterli düzeyde kontrol edilebilmiş mi?

ICS 4. Personel Değerlendirme ve Geliştirme: Personel performansı, GM'nin genel hedeferiyle uyumlu yıllık bireysel hedefer temelinde değerlendirilir. Söz konusu hedefere ulaşmak için gerekli becerileri geliştirmek amacıyla yeterli önlemler alınır.

GEREKLİLİKLER

- CDR süreci bağlamında (veya CDR sürecinin uygulanmadığı durumlarda gayri resmi olarak), tüm personelle GM ve Birimin hedeferi ile uyumlu yıllık hedeferinin belirlenmesi amacıyla teker teker görüşülmelidir.
- Personel performansı, Komisyon10 tarafından belirlenen standartlar temelinde değerlendirilir.
- GM politikalarından kaynaklanan ihtiyaçlar ve merkezi birimlerden gelen talimatlar ve tavsiyeler temelinde, GM düzeyinde bir yıllık stratejik eğitim çerçevesi geliştirilmelidir. Çalışma süresinin belirli bir bölümü (Komisyon'un yıllık stratejik Öğrenme ve Gelişim çerçevesiyle belirlenmiştir), öğrenme ve gelişim faaliyetleri için ayrılmalıdır.
- Her bir görevli ve mukayese yoluyla Personel Düzenlemesi Madde 24a'nm uygulandığı diğer kişiler tarafından, her yıl bir Eğitim Haritası hazırlanmalı ve bölüm müdürüyle tartışılıp yine onun tarafından onaylanmalıdır. Personel tarafmdan gerçekleştirilen tüm eğitim faaliyetlerinin kaydedildiği bir Eğitim Pasaportu daima güncel tutulmalıdır.
- Yönetim, tüm personelin en azından (Komisyon ve GM'nin) stratejik çerçevelerinde zorunlu kılman eğitimlere katılmasını sağlamalıdır.

KONTROL ETKİLİLİĞİNİN DEĞERLENDİRİLMESİNE YÖNELİK TAVSİYELER

Bilgi Notu: Kontrol etkililiğini değerlendirirken, iki temel soru sorulmalıdır:

GM'nin kendine özgü faaliyet ve risklerini dikkate alarak, mevcut kontrol düzenlemeleri yeterli mi?

Kontrol düzenlemeleri öngörüldüğü şekliyle uygulamaya aktarılabilmiş mi?

Yönetimin, söz konusu ICS kapsamında kontrol etkililiğini değerlendirirken dikkate almak isteyebileceği bazı sorular aşağıda verilmiştir:

- Personelin yıllık hedeferi (CDR'de de belirtildiği üzere), anlamlı ve yeterince zorlayıcı mı ve ilgili kişilerce kabul edilmiş mi? Bu hedefer yıl içinde güncelleniyor mu?
- Personel değerlendirmeleri, ilgili ve güncel yılık hedefere ulaşılmasına bağlı mı? Genel veya güncelliğini yitirmiş hedefer, öznel ve taraşı değerlendirmelerin yapılması riskini artırabilir ve personel motivasyonu üzerinde olumsuz etkiler yaratabilir.
- GM'nin gerektirdiği becerileri analiz edip geliştirmek ve gelecekte doğacak İK ihtiyaçları ve becerilerine yönelik planların yapılması için gerekli önlemler almıyor mu? Etkili bir personel geliştirme planı sadece bireysel eğitim taleplerini değil GM/MüdürlükBirimin ihtiyaçlarını karşılamak için gerekli grup becerileri ve yeterliliklerini de dikkate almalıdır. Gerekli beceri ve yeterlilikler ile mevcut beceri ve yeterlilik arasında var olan ciddi uçurumların ortaya çıkarılması için analizler yapılması, personel gelişimini artırmanın etkili bir yolu olabilir.
- Gerekli eğitim istatistikleri mevcut mu? GM/Müdürlük/Birimin eğitim istatistiklerinin

analizi, birimin eğitim faaliyetlerinin odağının yeniden belirlenmesinin gerekli olup olmadığını gösterebilir. Bu analiz ışığında, personelin ilgili becerileri geliştirmek için gerekli kursları aldığını gösteren bulgular var mı?

Yıllık hedefere ilişkin değerlendirme: Yılda en az bir kez ve gerekli olduğu hallerde raporlama görevlisiyle performansı tartışma imkanı; personel performansına ilişkin hususların gecikmeden tartışılıp çözümlenmeye çalışılması; uygun düzeltici faaliyetlerin belirlenip hayata geçirilmesi.

ICS 5. hedefer ve Performans Göstergeleri: GM'nitı hedeferi açık bir şekilde tanımlanır ve gerekli durumlarda güncellenir. hedefer, bu hedefere ulaşılıp ulaşılamadığının izlenebilmesini mümkün kılacak şekilde belirlenir. Yönetimin hedefer konusunda kaydedilen ilerlemeyi değerlendirmesi ve raporlamasını kolaylaştırmak amacıyla kilit performans göstergeleri belirlenir.

Gereklilikler

- GM'nin Yıllık Yönetim Planının (YYP), herkes tarafından anlaşılması ve sahiplenilmesini sağlamak için, Yıllık Yönetim Planı gerekli rehbere uygun olarak ve üst ve orta düzey yöneticiler ve personelle diyalog temelinde hazırlanmalıdır.
- YYP, her bir yönetim düzeyinde planlanan faaliyetlerin, belirlenen hedefere ulaşılmasına nasıl bir katkı sağlayacağını (tahsis edilen kaynaklar ve tanımlanan riskleri de dikkate alarak) açıkça ortaya koymalıdır.
- YYP hedeferi, SMART ilkesine (Spesifik-Ölçülebilir-Başarılabilir-Gerçekçi-Zamanlı) mümkün olan en üst düzeyde uyacak şekilde belirlenmelidir.
- hedefer, gerekli olduğu durumlarda, faaliyetler ve önceliklerde meydana gelen önemli değişiklikler dikkate alınarak güncellenmelidir.
- Uygun olduğu durumlarda, GM sürmekte olan çok yıllı faaliyetler için yol haritaları belirlemelidir. Bu haritalarda, tüm faaliyet süresini kapsayan bütçe tahsisatları yapılmadan önce gerçekleştirilmesi gereken faaliyetlere ilişkin kritik aşamalar da ortaya konmalıdır.
- YYP'de, kazanılan başarıların izlenmesi ve raporlanması için, -hem politika alanında hem de işletme faaliyeti düzeyinde- her bir hedef için asgari bir performans göstergesine yer verilmelidir. Performans göstergeleri, RACER kriterine (İlgili-Tartışılmış-Kabul Edilmiş-Güvenilir-Kolay-Sağlıklı) mümkün olan en üst düzeyde uyacak şekilde belirlenmelidir.
- Göstergelerin, hedefere ulaşabilme ihtimalinin riske girdiğini gösterdiği durumlarda yönetimi uyarmayı sağlayacak raporlama yapıları var olmalıdır.

KONTROL ETKİLİLİĞİNİN DEĞERLENDİRİLMESİNE YÖNELİK TAVSİYELER

Bilgi Notu: Kontrol etkililiğini değerlendirirken, iki temel soru sorulmalıdır:

GM'nin kendine özgü faaliyet ve risklerini dikkate alarak, mevcut kontrol düzenlemeleri yeterli mi?

Kontrol düzenlemeleri öngörüldüğü şekliyle uygulamaya aktarılabilmiş mi?

Yönetimin, söz konusu ICS kapsamında kontrol etkililiğini değerlendirirken dikkate almak isteyebileceği bazı sorular aşağıda verilmiştir:

- "hedefere göre yönetim" kavramı (Bir başka deyişle, farklı yönetim düzeylerinde GM faaliyetlerini YYP hedeferi temelinde şekillendirmek), yönetim ve personel tarafından yeterince anlaşılmış, tartışılmış ve kabul edilmiş mi? Bu kavram, uygulamada işe yarıyor mu? Yaramıyorsa, neden?
- Hedef belirleme süreci, yüksek düzeyli bir anlayış ve sahiplenmeyi de beraberinde getiriyor mu? GM/Müdürlük/Birim YYP hedeferi personel ve yönetim tarafından biliniyor mu ve onlara anlamlı geliyor mu?
- Kaynaklarm yeniden tahsisi ve hedeferin (yeniden) önceliklendirilmesi gerekli mi?
- GM/Müdürlük/Birimin performans göstergeleri anlamlı mı? Bir başka deyişle, bu göstergeler GM faaliyetlerinin yönetimi ve izlenmesini kolaylaştırıyor ve destekliyor mu?
- Performans göstergeleri, GM/Müdürlük/Birimin kilit faaliyetleri ve riskleri temelinde mi belirleniyor? Sayıca çok fazla veya ayrmtı düzeyi çok yüksek göstergeler kafa karıştırıcı veya etkisiz olabilir.
- Performansın ölçülemediği durumlarda, ölçülebilir anlamlı performans göstergeleri belirleniyor mu?

ICS 6. Risk Yönetimi Süreci: Geçerli hükümler ve kılavuz ilkelerle uyumlu bir risk yönetimi süreci, yıllık faaliyet planlamasına dahil edilir.

GEREKLİLİKLER

- GM düzeyinde bir risk yönetimi uygulaması, yılda en az bir kez YYP sürecinin bir parçası olarak ve yönetimin gerekli gördüğü hallerde (genellikle yıl içerisinde GM faaliyetlerinde meydana gelen ciddi değişiklikler halinde) gerçekleştirilmelidir. Risk yönetimi, geçerli hükümler ve kılavuz ilkeler temelinde yapılmalıdır.
- Risk yönetimi eylem planları gerçekçi planlar olup ilgisiz kontrol önlemlerinin alınmasını önlemek amacıyla maliyet/fayda boyutunu da dikkate almalıdır. Eylemlerin, plana uygun olarak uygulanmalarını ve "ilgili olma" özelliklerini korumaya devam etmelerini sağlamak amacıyla belirli süreçler hayata geçirilmelidir.
- Genel GM perspektifinden "kritik" olarak değerlendirilen riskler (bakınız, SEC(2005) 1327 , 2.4) GM yıllık yönetim planında ortaya konmalı ve yıllık faaliyet raporunda takip edilmelidir.

KONTROL ETKİLİLİĞİNİN DEĞERLENDİRİLMESİNE YÖNELİK TAVSİYELER

Bilgi Notu: Kontrol etkililiğini değerlendirirken, iki temel soru sorulmalıdır:

1. GM'nin kendine özgü faaliyet ve risklerini dikkate alarak, mevcut kontrol düzenlemeleri yeterli mi?
2. Kontrol düzenlemeleri öngörüldüğü şekliyle uygulamaya aktarılabilmiş mi?

Yönetimin söz konusu ICS kapsamında kontrol etkililiğini değerlendirirken dikkate almak isteyebileceği bazı sorular aşağıda verilmiştir:

- Risk yönetimi kavramı, yönetim ve personel tarafından yeterli düzeyde anlaşılmış mı? Bu alandaki sorunları tespit edebilmek amacıyla anketler yapılabilir.
- Risk yönetimi, GM faaliyetlerinin planlanması, uygulanması ve kontrolü süreç ve prosedürlerine gerekli şekilde entegre edilmiş mi? Risk yönetimi düzenli olarak Müdürlük/Birim toplantılarında gündeme getiriliyor mu?
- GM risk yönetimi süreci kullanıcı dostu ve faydacı bir yapıya sahip mi yoksa "bürokratik bir yük" gibi mi görülüyor?

ICS 7. İşleyiş Yapısı: GM'nin işleyiş yapısı, yetkilerin uygun şekilde paylaştırılması yoluyla kararların etkili bir şekilde alınmasını sağlar. GM'nin hassas işlevleri ile ilişkili riskler , hafifletici kontroller ve gerekmesi durumunda personel yer değiştirmesi yoluyla yönetilir. Yeterli BT yönetim yapıları mevcuttur.

GEREKLİLİKLER

- Yetki devri açık bir şekilde tanımlanmalı, gerçekleştirilmeli ve yazılı olarak bildirilmelidir; söz konusu yetki devri yasama yükümlülükleriyle ve alınacak kararlar ve ilgili risklerin önem düzeyiyle uyumlu olmalıdır.
- Sözleşmeler ve belirli yetkilendirme araçları , harcama yetkilileri ve bir alt düzeyde yetkilendirilen harcama yetkililerine iletilmeli ve bu kişiler tarafından onaylanmalıdır.
- Mali işlemler konusunda da yetki devri ("ödeme izni verme" ve "doğruluğunu onaylama" da dahil olmak üzere) tanımlanmalı, gerçekleştirilmeli ve yazılı olarak bildirilmelidir.
- GM'nin hassas işlevleri açık bir şekilde tanımlanmalı , kaydedilmeli ve güncellenmelidir. Hassas işlevlerin her biri için:
  - Risk değerlendirilmesi yapılmalı ve ilgili hafifletici kontroller gerçekleştirilmelidir.
  - Aynı çalışan beş yıldır aynı hassas işlev (leri) yerine getiriyorsa, risk yeniden değerlendirilmelidir. Bu değerlendirmenin ardından , yönetim çalışanın yerini değiştirmeye veya hassas işlevleri başkalarına aktarmaya ya da hafifletici önlemler almaya karar vermelidir. Böylece yerleşik risk kabul edilebilir bir düzeye çekilebilir.
  - Bir çalışanın aynı hassas işlev(leri) yedi yıldır yerine getiriyor olması durumunda, genel bir kural olarak personel yer değiştirmesi gerçekleştirilmelidir.
- GM, personelin beş yılı aşkın sürelerle hassas işlevleri yerine getirmesini mümkün kılan sapmaları , risk analizi belgeleri ve hafifletici kontroller yoluyla raporlamalıdır. Bu sapmalar hakkında , uygun talimatlar temelinde yıllık faaliyet raporlarında bilgi verilmelidir.
- Komisyonun standart BT yönetimi politikası uygulanmalıdır. Özellikle:
  - GM, sahip olduğu bilgi sistemlerinin yönetimine ilişkin (genellikle BT yürütme komitesi şeklindeki) uygun teşkilatlanmayı tanımlamalıdır.
  - Bilgi sistemlerinde (bütçe kaynağına bakılmaksızın) son üç yılda kaydedilen tüm gelişmeleri kapsayan bir yıllık BT masterplan hazırlanmalıdır.
  - GM'nin sahip olduğu her bilgi sisteminin , açıkça tanımlanmış bir yöneticisi olmalı ve söz konusu bilgi sistemi bir yürütme komitesi tarafından idare edilmelidir.
  - Yeni bilgi sistemleri projelerinin tümü, bir vizyon belgesi temelinde onaylanmalıdır.
  - Yeni bilgi sistemlerinin tamamı , standart komisyon proje yönetim ve geliştirme yöntemleri kullanılarak geliştirilmeli ve ilk aşamadan itibaren güvenlik hususu göz önünde bulundurulmalıdır.

KONTROL ETKİLİLİĞİNİN DEĞERLENDİRİLMESİNE YÖNELİK TAVSİYELER

Bilgi Notu : Kontrol etkililiğini değerlendirirken, iki temel soru sorulmalıdır:

1. GM'nin kendine özgü faaliyet ve risklerini dikkate alarak , mevcut kontrol düzenlemeleri yeterli mi?
2. Kontrol düzenlemeleri öngörüldüğü şekliyle uygulamaya aktarılabilmiş mi?

Yönetimin söz konusu ICS kapsamında kontrol etkililiğini değerlendirirken dikkate almak isteyebileceği bazı sorular aşağıda verilmiştir:

- GM/Müdürlük/Birimin performansı veya kontrol ortamı üzerinde olumsuz etkiler yaratacak herhangi bir işleyiş sorunu var mı? Bunlar işleyişi hangi açılardan olumsuz yönde etkiliyor? GM/Müdürlük/Biriminyeniden teşkilatlandırılması durumu iyileştirebilir mi? Nasıl?
- Verilen işlev ve yetkilerin kapsamı ve özellikleri , ilgili tüm personel için yeterince açık mı?
- Verilen işlevler ve yetkilerle ilgili riskler yeterince analiz edilmiş mi?
- Hassas işlevlerin diğerlerinden ayrılıp farklı personelin sorumluluğuna verildiği durumlarda , yönetim ilgili risklerin etkili şekilde hafifletildiği konusunda tatmin olmuş mudur?
- Ilave yumuşatıcı kontrollerin devreye sokulduğu drumlarda, yönetim bu kontrollerin etkili olduğu ve risklerin (etkileri ve meydana gelme ihtimali de dikkate alınarak) kabul edilebilir düzeylere çekildiği hususunda tatmin olmuş mudur?
- Gözetim faaliyetleri ve denetim raporlarının sonuçları ile ilgili bilgiler , GM'nin hassas işlevlerine ilişkin problemlerle veya sorunlarla karşılaşıldığını ortaya koyuyor mu?
- Zorunlu personel yer değiştirmesini gerekli kılan hassas işlevlerin sayısı makul düzeyde mi? Aşırı düzeyde zorunlu personel yer değiştirmesinin getireceği maliyet (işlemler üzerinde olumsuz etki) , faydaları (risk, çıkar çatışmaları ve yolsuzluk riskinin azalması) aşabilir.
- Tüm BT/BS projeleri ve bunlara özel riskler, ilgili rehber kapsamında açık bir şekilde tanımlanmış ve yönetilmiş midir?
- BT yönetimi ve BS'nin geliştirilmesi kapsamında, BT yürütme komitesi ilgili tüm paydaşları yeterince temsil ediyor mu? GM'nin diğer GM'ler tarafından da kullanılmakta olan Bilgi Sistemlerine sahip olması durumunda, tüm paydaşların çıkarlarının dikkate alınmasını sağlamak amacıyla gerekli yönetim düzenlemelerine gidilmiş mi?
- GM'nin kendi Bilgi Sistemleri varsa veya GM kendisi için bir BS geliştirmek istiyorsa , GM Bilgi Sistemleri arasındaki olası sinerji yeterince araştırılmış ve bundan yeterince yararlanılmış mıdır? Sistemler arasında yeterli düzeyde "karşılıklı çalışma" mümkün mü? GM içindeki benzer sistemlerde veya dikkat edilmesi gereken diğer alanlarda mükerrer yatırımlar yapılmış mı?

ICS 8. Süreç ve Prosedürler: GM'nin faaliyetlerinin hayata geçirilmesi ve kontrolünde başvurulan süreç ve prosedürler etkili ve etkindir, yeterli düzeyde belgelendirilmiştir ve geçerli hükümlere uygundur. Bu süreç ve prosedürler; görevler ayrılığının gerçekleştirilmesini sağlayan düzenlemeleri, bazı kontrollerin atlanması uygulamalarının ve politika ve prosedürlerde görülen sapmaların takip edilmesine ve bunlara önceden onay verilmesine ilişkin düzenlemeleri kapsar.

GEREKLİLİKLER

- GM'nin temel işleyiş süreçleri ve mali süreçleri ile BT sistemleri yeterli düzeyde belgelendirilmelidir.
- GM süreç ve prosedürleri, uygun bir görev ayrımı yapılmasını sağlamalıdır (finansal olmayan faaliyetler dahil).
- GM süreç ve prosedürleri, geçerli hükümlerle ve özellikle Mali Yönetmelikle (örn, ön ve harcama sonrası doğrulamalar) ve Komisyon Uygulama Kurallarıyla uyumlu olmalıdır.
- Belirli kontrollerin atlandığı veya yerleşik süreç ve prosedürlerden sapmalarm görüldüğü durumların istisna raporlarında belirtilmesi, doğrulanması ve gerekli adım atılmadan önce onaylanması ile merkezi olarak kayda geçirilmesini sağlamaya yönelik bir yöntem benimsenmelidir.

KONTROL ETKİLİLİĞİNİN DEĞERLENDİRİLMESİNE YÖNELİK TAVSİYELER

Bilgi Notu: Kontrol etkililiğini değerlendirirken, iki temel soru sorulmalıdır:

1. GM'nin kendine özgü faaliyet ve risklerini dikkate alarak, mevcut kontrol düzenlemeleri yeterli mi?
2. Kontrol düzenlemeleri öngörüldüğü sekliyle uygulamaya aktarılabilmiş mi?

Yönetimin, söz konusu ICS kapsamında kontrol etkililiğini değerlendirirken dikkate almak isteyebileceği bazı sorular aşağıda verilmiştir:

* GM/Müdürlük/Birim faaliyetlerinin uygulanması ve kontrol edilmesine yönelik temel süreç ve işlemler kullanıcı dostu bir yaklaşımla belgeleniyor mu?

Bu belgelere halihazırda erişim mümkün mü ve söz konusu belgeler güne elleniyor mu?

- Verilerin, veri süreçlerinin elle idare edilen bölümünde korunmasını sağlamak amacıyla gerekli düzenlemeler hayata geçirilmiş mi?
- Yönetim, uygun olduğu durumlarda ve büyük değişikliklerin yapıldığı hallerde (YYP risk yönetimi uygulaması kapsamında değilse -Bakınız; ICS 6) temel süreç ve prosedürlerine ilişkin bir risk değerlendirmesi yapmış mı? Buna paralel olarak, süreç ve prosedürlerin en hassas yönleri tanımlanmış ve ilgili hafişetici kontroller hata geçirilmiş mi?
- Uygulanmakta olan süreç kontrolleri yeterli düzeyde tasarlanmış mı?
- Kontrolü kim gerçekleştiriyor?
- Kontrol nasıl yapılıyor (yöntem, örneklem büyüklüğü, vb)?

- Kontrolü yapmak için hangi bilgiler gerekiyor?
- Kontrol hangi sıklıkla yapılıyor?
- Tanımlanan "aykırılıkların" önem düzeyini tanımlamak için hangi kriterler kullanılıyor (bir başka deyişle; kontroller sırasında fark edilen sorunların hangileri önemli kabul edilecek; hangi hatalar küçük hata olarak kabul edilecek)? Sorularının cevapları açıkça biliniyor mu?
- Tüm kritik bilgi sistemlerinde, riskli faaliyetlere yönelik olarak denetim kayıtlarının tutulması ve gerekli adımların atılması için uyarılarda bulunulması öngörülüyor mu?
- İcracı yapılar, kontrol süreç ve prosedürlerine katılıyorsa (örneğin, Üye Devlet kurumları), "kontrol zinciri" baştan sona kadar yeterli düzeyde açıklanmış mı? Kontrol zincirindeki roller ve sorumluluklar katılan tüm taraşar için yeterince açık mı? Kontrol faaliyetleri ve sonuçlarına ilişkin bilgiler, tüm katılımcı taraşara yeterli düzeyde ulaştırılıyor mu?

ICS 9. Yönetim Tarafından Yapılan Gözetim : Faaliyetlerin geçerli hükümler çerçevesinde etkin ve etkili şekilde uygulanmasını sağlamak amacıyla yönetim tarafından gözetim yapılır.

GEREKLİLİKLER

- Her düzeydeki yönetim, sorumlu olduğu faaliyetleri gözetmeli ve tanımlanan temel konuların gidişatını izlemelidir. Yönetim gözetimi , hem yasallık ve düzenlilik açıları hem de işlevsel performans açılarından yaklaşılarak yapılmalıdır. (bir başka deyişle , YYP hedeflerine ulaşılması).
- Kritik potansiyel riskler içeren faaliyetlerin gözetimi yeterli düzeyde belgelendirilmelidir.
- Yönetim, üzerinde anlaşılan ECA/IAS/IAC denetim tavsiyeleri ve ilgili eylem planlarının uygulanışını gözetmelidir.
- En az yılda iki kez ve gerekli görüldüğü her durumda sorumlu Komiser, iç kontrol, denetim ve OLAF soruşturmalarıyla ilişkili önemli hususlar ve Kuruldaki konumunu, ödeneklerin sağlıklı bir şekilde yönetilmesini etkileyebilecek veya belirlenen hedeflere ulaşmayı engelleyebilecek parasal ve mali konular hakkında Genel Müdür tarafından bilgilendirilmelidir.

KONTROL ETKİLİLİĞİNİN DEĞERLENDİRİLMESİNE YÖNELİK TAVSİYELER

Bilgi Notu: Kontrol etkililiğini değerlendirirken, iki temel soru sorulmalıdır:

1. GM'nin kendine özgü faaliyet ve risklerini dikkate alarak, mevcut kontrol düzenlemeleri yeterli mi?
2. Kontrol düzenlemeleri öngörüldüğü şekliyle uygulamaya aktarılabilmiş mi?

Yönetimin, söz konusu ICS kapsamında kontrol etkililiğini değerlendirirken dikkate almak isteyebileceği bazı sorular aşağıda verilmiştir:

- Gözetim faaliyetleri yüksek riskli alanlar üzerinde odaklanmış mı? Aşağıdaki durumlar , daha üst düzeyde bir gözetim yapılmasını gerektirir. Karmaşık işlemler, yetenekli ve tecrübeli personel sayısında yetersizlik, işletme faaliyetlerinde yeniden yapılandırma veya ciddi değişiklikler, yeni veya modernize edilmiş BT sistemleri , olası çıkar çatışmaları veya dış tarafların etkisi , siyasi açıdan hassas faaliyetler, personelin çalışma koşullarını ciddi düzeyde etkileyen faaliyetler (sağlık, güvenlik, emniyet).
- Gözetim faaliyetleri yoluyla ortaya çıkarılan önemli hususlar sistematik bir şekilde izleniyor mu?
- Icracı kurumlar faaliyetlerin yürütülmesinden sorumluysa (örn, Üye Devletler veya kurumlar), sorumlu Komisyon birimi tarafından gerekli gözetim veya izleme gerçekleştiriliyor mu?
- Işletme performansının gözetimi GM'nin YYP hedefleri ve ilgili performans göstergelerini mi temel alıyor? Bu hedefler ve göstergeler uygulamada işe yarıyor mu? Yaramıyorsa neden?
- Yönetim, kilit kontrollerin yapılıp yapılmadığına ve uygulamaya öngörüldüğü şekliyle aktarılıp aktarılmadığına dair yeterli bulguya sahip mi? (örneğin, gözetim faaliyetleri, denetimler, soruşturmalar ve diğer ilgili bilgi kaynakları yoluyla)
- Raporlanan tüm iç kontrol eksiklikleri gerekli şekilde incelenmiş ve giderilmiş mi?

ICS 10. İş Sürekliliği: "Düzenli iş akışında" meydana gelebilecek aksaklıklar durumunda birimin devamlılığını sağlamak için gerekli önlemler alınır. İş Sürekliliği Planları, büyük bir aksaklık halinde bile Komisyonun çalışmaya devam edebilmesini sağlamayı amaçlar.

GEREKLİLİKLER

- Düzenli iş akışında meydana gelen kesintiler halinde (hastalık izni, personel yer değiştirmesi, yeni BT sistemlerine geçiş ve özel durumlar, vb) tüm hizmetlerin aksamadan devam edebilmesini sağlamak için -devralma dosyaları, ilgili işletme faaliyetleri ve mali işlemlerle ilgili vekillik düzenlemeleri de dahil olmak üzere- gerekli önlemler alınmalıdır.
- İş Sürekliliği Planları, iş akışında meydana gelen büyük kesintiler (salgın hastalık, terörist saldırıları, doğal afetleri vb) durumunda atılacak kriz adımları ve iyileştirme düzenlemelerini kapsamalıdır. Bu planlar, belirli bir süre içinde tamir edilmesi gereken işlevler, hizmetler ve altyapıları ve bunlar için gerekli kaynakları (kilit personel, binalar, BT, belgeler, vb) tanımlamalıdır. İlgili GM'ye özgü önlemler temelinde hazırlanan GM Planları, yatay birimlerin İş Sürekliliği Planlarını söz konusu birimlerin yapı içindeki tüm birimler temelindeki sorumlulukları çerçevesinde dikkate almalıdır.
- İş Sürekliliği Planlarını uygulamak, güncellemek ve geçerlemek için belirli prosedürler geliştirilmelidir. Gözden geçirmeler, mevcut risk yönetimi süreçleri çerçevesinde en az yılda bir kez yapılır.
- İş Sürekliliği Planlarının elektronik ve basılı kopyaları, ilgili personelin bildiği güvenli ve kolay erişilebilir yerlerde saklanmalıdır.
- Bilgi sistemlerine yönelik ek planlar ve yedekleme planları; işletme, iş sürekliliği ve güvenlik ihtiyaçları temelinde hazırlanmalı, muhafaza edilmeli, belgelendirilmeli ve denenmelidir.

KONTROL ETKİLİLİĞİNİN DEĞERLENDİRİLMESİNE YÖNELİK TAVSİYELER

Bilgi Notu: Kontrol etkililiğini değerlendirirken, iki temel soru sorulmalıdır:

GM'nin kendine özgü faaliyet ve risklerini dikkate alarak, mevcut kontrol düzenlemeleri yeterli mi?

Kontrol düzenlemeleri öngörüldüğü sekliyle uygulamaya aktarılabilmiş mi?

Yönetimin, söz konusu ICS kapsamında kontrol etkililiğini değerlendirirken dikkate almak isteyebileceği bazı sorular aşağıda verilmiştir:

Hizmet Sürekliliği (Düzenli îş Akışı): Hizmet sürekliliğini sağlamaya yönelik GM prosedürleri (teslim düzenlemeleri, yedekleme prosedürleri, vb) yeterince biliniyor mu ve halihazırda (özellikle yeni personel tarafından) erişilebilir ve kullanılabilir durumda mı?

İş Sürekliliği Planı: Yönetim ve ilgili personel İş Sürekliliği Planları konusunda yeterince bilinçli ve eğitimli mi? Yönetim ve personel, büyük iş sürekliliği kesintileri halinde personel ve varlıklara yönelik olarak ortaya çıkacak riskleri en aza indirmek için neler yapmaları gerektiğini biliyor mu? İş Sürekliliği Planı, bu plana ihtiyacı olacak kişilerin ihtiyaç anında kolayca anlayabileceği ve halihazırda erişebileceği bir durumda mı?

İş Sürekliliği Planı: Öncelikler ve kilit riskler -BT riskleri de dahil olmak üzere- İş Sürekliliği Planlarında açık bir şekilde tanımlanmış ve yeterince aydınlatılmış mı? Özellikle stresli

ortamlarda, kısa ve net mesaj ve talimatlar uzun ve ayrıntılı açıklamalardan genellikle daha etkilidir.

İş Süreklilik Planı: İş Süreklilik Planı -ilgili BT unsurları da dahil olmak üzere- yeterince denenmiş mi? Periyodik testler ve uygulama alıştırmaları, süreklilik planının etkin bir şekilde uygulamaya aktarılıp aktarılmadığını belirlemede önemli araçlardır.

İş Süreklilik Planı: Test faaliyetlerinin sonuçları yeterince incelenmiş ve belgelendirilmiş mi? Gerekli iyileştirmeler tanımlanmış ve İş Süreklilik Planı gerekli şekilde güncellenmiş mi?

ICS 11. Belge Yönetimi: GM'nin belge yönetiminin güvenli, etkin (özellikle uygun bilginin geri çağrılması konusunda) ve mevzuata uygun bir şekilde gerçekleştirilmesini sağlamak amacıyla gerekli işlem ve prosedürler mevcuttur.

GEREKLİLİKLER

- Belge yönetimi sistemleri ve ilgili prosedürler, zorunlu güvenlik önlemleri, bilgi yönetimi hakkındaki hükümler ve kişisel verilerin korunması hakkındaki kurallarla uyumlu olmalıdır.
- Özellikle, uygulama kurallarında ortaya konan koşulları karşılayan tüm belgelerin kaydedilmesi, en az bir resmi dosyaya girilmesi (her bir dosya, Dosyalama Planının belirli bir başlığı altına eklenir) ve uygun Komisyon kayıt ve dosyalama sistemleri temel olarak ADONIS ve NOMCOM kullanılarak muhafaza edilmesi gerekmektedir.

KONTROL ETKİLİLİĞİNİN DEĞERLENDİRİLMESİNE YÖNELİK TAVSİYELER

Bilgi Notu: Kontrol etkililiğini değerlendirirken, iki temel soru sorulmalıdır:

1. GM'nin kendine özgü faaliyet ve risklerini dikkate alarak, mevcut kontrol düzenlemeleri yeterli mi?
2. Kontrol düzenlemeleri öngörüldüğü şekliyle uygulamaya aktarılabilmiş mi?

Yönetim söz konusu ICS kapsamında kontrol etkililiğini değerlendirirken dikkate almak isteyebileceği bazı sorular aşağıda verilmiştir:

- Belgeler, afet, hırsızlık, yangın vb.ye karşı yeterince korunuyor mu?
- Kayıt prosedürleri yeterince biliniyor mu? Bu prosedürler uygulamaya geçirilmiş mi?
- Dosyalama prosedürleri yeterince biliniyor mu?
- Genel anlamda, belge bulmak için ayrılan süre makul bir süre mi?
- Hassas belgeler için nasıl bir sürecin izleneceğine ilişkin kurallar (komisyon ve GM'ye özgü kurallar) yeterince biliniyor ve uygulamaya başarılı bir şekilde aktarılabiliyor mu?
- GM'nin veri toplama sisteminin olduğu durumlarda, belgelerin gelecekte de okunabilir kalması için gerekli önlemler alınmış mı?

ICS 12. Bilgi ve İletişim: Kurum içi iletişim, yönetim ve personelin (iç kontrol alanındaki sorumlulukları da dahil olmak üzere) sorumluluklarını etkili ve etkin bir şekilde yerine getirmelerini sağlar. GM'nin kurum dışı iletişiminin etkili, tutarlı ve Komisyonun kilit politika mesajlarına uygun şekilde gerçekleştirilmesini sağlamak için, uygun olduğu durumlarda, GM bir "kurum dışı iletişim" stratejisi geliştirebilir. GM tarafından kullanılmakta olan ve/veya geliştirilen BT sistemleri (GM'nin sistemin sahibi olduğu durumlarda), gizlilik ve bütünlükle ilgili tüm tehlikeler karşısında yeterli düzeyde korunur.

GEREKLİLİKLER

- İç ve dış iletişimler, ilgili telif hakkı hükümlerine uygun olmalıdır.
- GM'nin temel faaliyetlerine yönelik olarak ve uygun olduğu hallerde Müdürlükler ve Birimler düzeyinde Yönetim Tabelaları (veya eşdeğer araçlar) geliştirilmelidir. Bu tabelalar, kurumun faaliyetlerini ve kaydedilen ilerlemeyi izleyebilmek için gerekli yönetim bilgilerini kapsamalıdır. Bu yönetim bilgileri performans göstergeleri, mali bilgiler, yasallık ve düzenliliğe ilişkin hata oranlan, proje teslim tarihleri, önemli denetim bulgulan, İK14 göstergeleri ve Fırsat Eşitliği hedeferi ve diğer ilgili yönetim bilgilerinden oluşmaktadır.
- Komisyon İç İletişim ve Personel Katılımı Stratejisiyle uyumlu düzenlemeler hayata geçirilmelidir; böylece, yönetim ve personelin verilen işler ve çevreleriyle ilgili karalar, proj eler veya girişimler -diğer GMTerinkiler de dahil olmak üzere- hakkında gerekli şekilde bilgilendirilmeleri sağlanır.
- Tüm personel, önemli veya sistematik olarak değerlendirilen olası iç kontrol zaaşan hakkında uygun yönetim düzeyini bilgilendirmeleri konusunda desteklenmelidir. Bu tür raporlama süreçlerini kolaylaştırmak için İletişim Kurulacak Kişi(ler) atanmalıdır.
- Uygun olduğu hallerde, GM dış iletişim için belgelendirilmiş bir strateji geliştirmelidir (Komisyon dışında). Bu strateji açıkça tanılanmış hedef kitle, mesajlar ve eylem planlarını içermelidir. İletişim stratejisi, politika geliştirmenin ilk aşamasında planlanmalı ve sorumlu Kabineyle görüşülmelidir. İletişim öncelikleri konusunda diğer GM'ler ve COMM GM'yle işbirliği fırsatları aranmalıdır.
- Komisyonun standart Bilgi Sistemleri Güvenlik Politikası uygulanmalıdır. Özellikle her bir GM, sorumluluğu altındaki BT sistemlerinin güvenlik gereklilikleri dökümünü ve risk analizini temel alan bir BT Güvenlik Planı uygulamalı ve asgari düzeyde kurumunu BT Güvenlik Politikasının ilgili kontrol önlemlerini hayata geçirmelidir.
- BT sistemleri yeterli düzeyde bir veri yönetimini desteklemelidir. Veri yönetimi veritabam yönetimi ve veri kalitesi güvencesini kapsamalıdır. Veri yönetimi sistemleri ve ilgili prosedürler, Bilgi Sistemleri Politikası, zorunlu güvenlik önlemleri ve kişisel verilerin korunması hakkındaki kurallarla uyumlu olmalıdır.

KONTROL ETKİLİLİĞİNİN DEĞERLENDİRİLMESİNE YÖNELİK TAVSİYELER

Bilgi Notu: Kontrol etkililiğini değerlendirirken, iki temel soru sorulmalıdır:

GM'nin kendine özgü faaliyet ve risklerini dikkate alarak, mevcut kontrol düzenlemeleri yeterli mi?

Kontrol düzenlemeleri öngörüldüğü şekliyle uygulamaya aktarılabilmiş mi?

Yönetimin, söz konusu ICS kapsamında kontrol etkililiğini değerlendirirken dikkate almak isteyebileceği bazı sorular aşağıda verilmiştir:

- GM/Müdürlük/Birim yönetim tabelaları yoluyla sağlanan bilgiler, geçerli ve söz konusu faaliyetlerin yönetimi noktasında faydalı mı? Mümkün olan noktalarda YYP hedeferi ile açık ve net bir bağlantı kurulabiliyor mu? Yönetim ve personel tabelalan kullanılıyor mu? Kullanmıyorsa, neden? Tabelalar güvenilir mi ve bilginin doğruluğunu kontrol etmek için daha çok şey yapılması gerekiyor mu?
- İç iletişim için kullanılmakta olan mevcut düzenlemeler incelenmiş mi? Yönetim ve personelin sorumluluk ve görevlerini etkileyebilecek olan ve diğer birimler, Müdürlükler ve GM'ler tarafından gerçekleştirilen karar/proje/girişimler konusunda bilgilendirilmelerini sağlayacak uygulamalar var mı?
- Son zamanlarda iç ve GM'ler arası iletişimde meydana gelen aksaklıkların sorunlara yol açtığı veya GM performansını etkilediği duıumlar oldu mu? Bu aksaklıklann altında yatan nedenler incelendi mi? Gelecekte de benzer iletişim sorunlannm yaşanmaması için önlemler alındı mı?

14 Olası İK Göstergeleri. İşe girip çıkan personel sayısı, işgücü değerlendirmesi, kişi başı eğitim günü sayısı, ayrılma tahminleri.

- Dış iletişim için kullanılmakta olan mevcut prosedür ve yöntemler, güçlü ve zayıf yönleri tanımlamak için maliyet-fayda boyutlarını da dikkate alacak şekilde incelendi mi?
- İletişimin etkilerini incelemek üzere , hedef kitleden geribildirim almak ve bunları incelemek için uygulamada neler yapıldı? Elde edilen bilgi güvenilir ve ilgili mi? İlgili geribildirimler gerekli seviyeye çıkarıldı ve mevcut iletişim stratejilerini benimsenmesinde kullanıldı mı?
- İlgili personel Bilgi Sistemleri Güvenlik Politikası hakkında yeterli bilgiye sahip mi? Bilgi sistemi güvenliği yönetim toplantılarında düzenli olarak görüşülen bir konu mu? Bilgi güvenliğine yönelik olarak hedefler belirlenmiş mi ve bunlara ulaşılıp ulaşılmadığı takip ediliyor mu? BT sistemlerinin düzenli olarak gözlenmesi sonucu elde edilen sonuçlar, denetim bulguları ve diğer kaynaklardan elde edilen bilgiler BT güvenliğiyle ilgili bazı sorunların varlığına işaret ediyor mu? Bu sorunlar uygun yönetim düzeyine taşınmış ve burada tartışılıyor mu?
- BT kullanıcılarından sistem performansına ilişkin geribildirimler alınmış ve incelenmiş mi? BT kullanıcılarının yorum ve tavsiyelerinin sistematik bir şekilde alınması (anketler veya özel geribildirim kanalları yoluyla) , etkililik ve etkinlik sorunlarını saptamanın iyi bir yolu olabilir. Sistemin arıza süresi , sunucu kapasitesi ve diğer performans göstergeleri düzenli olarak inceleniyor mu? Sistem performansına ilişkin sorunlar uygun yönetim düzeyine raporlanıyor mu?
- GM kapsamında, veri saklama süreleri , veri yedekleme , veri erişimi ve arşivlemeye ilişkin etkili prosedürler var mı? Yönetim bu süreçlerin uygulamaya aktarıldığını gösterebilir mi? Gözetim faaliyetlerinin sonuçları, “tüketici şikayetleri” , denetim bulguları veya diğer kaynaklardan elde edilen bilgiler veri yönetimi alanında (veri kalitesi, eksik veya zamansız veri gibi) herhangi bir eksiklik olup olmadığını ortaya koyuyor mu?

ICS 13. Muhasebe ve Mali Raporlama: Kurumun yıllık hesapları ve mali raporlarının hazırlanmasında kullanılan muhasebe verileri ve ilgili bilgilerin doğru, eksiksiz ve zaman açısından geçerli olmasını sağlamaya yönelik yeterli prosedür ve kontroller mevcuttur.

GEREKLİLİKLER

- Her bir Harcama Yetkilisi, Topluluk varlıkları veya bütçe uygulamasına ilişkin gerçek verileri ortaya koyan hesapların üretilebilmesi için Muhasebe Yetkilisine sunulacak olan ve söz konusu Harcama Yetkilisinin kontrolü altında bulunan muhasebe bilgilerinin güvenilir ve eksiksiz olmasını sağlamakla yükümlü kılınmalıdır.
- Muhasebe muhabiri (AC) koordinatördür ve Komisyon merkezi muhasebe sistemine sunulan GM muhasebe verileri ve bilgilerinin kaliteli olmasını sağlamak amacıyla GM içinde bir yardım masası gibi çalışmalıdır.
- GM nin muhasebe prosedürleri ve kontrolleri yeterli düzeyde belgelendirilmelidir.
- GM tarafından üretilen mali bilgiler ve yönetim bilgileri –Yıllık Faaliyet Raporunda sunulan mali bilgiler de dahil olmak üzere- uygulamada olan muhasebe kuralları ve Muhasebe Uzmanlarının talimatlarıyla uyumlu olmalıdır.

KONTROL ETKİLİLİĞİNİN DEĞERLENDİRİLMESİNE YÖNELİK TAVSİYELER

Bilgi Notu: Kontrol etkililiğini değerlendirirken , iki temel soru sorulmalıdır:

1. GM nin kendine özgü faaliyet ve risklerini dikkate alarak, mevcut kontrol düzenlemeleri yeterli mi?
2. Kontrol düzenlemeleri öngörüldüğü şekliyle uygulamaya aktarılabilmiş mi?

Yönetimin, söz konusu ICS kapsamında kontrol etkililiğini değerlendirirken dikkate almak isteyebileceği bazı sorular aşağıda verilmiştir:

- GM –özellikle Muhasebe Muhabiri – muhasebe alanı ve mali alanlarda gerekli beceriler ve deneyime sahip mi?

- Muhasebe verilerine ilişkin kalite kontrolleri geçerli ve yeterince belgelendirilmiş mi? Örneğin bu tür kontroller ; genel hesapların analizini, ödenmemiş faturaların yıllık denge analizlerini, ödenmemiş önfinansmanları , görevler ayrılığını, rapor gözden geçirmelerini, Btsistem arayüzlerine yönelik kontrolleri, vb. Kapsar. Yönetim , bu kontrollerin uygulamaya öngörüldüğü şekliyle aktarıldığı konusunda tatmin olmuş mu?

- Muhasebeci tarafından muhasebe kalite projesine ilişkin olarak önerilen kılavuz ilkeler uygulamaya konmuş mu?

ICS 14. Faaliyet Değerlendirmeleri : Harcama programları, mevzuat ve diğer harcama dışı faaliyetlere ilişkin değerlendirmeler, söz konusu faaliyetlerin ulaşmayı ve karşılamayı amaçladığı sonuçlar, etkiler ve ihtiyaçları değerlendirmek amacıyla yapılır.

GEREKLİLİKLER

Değerlendirmeler, Komisyonun değerlendirme standartları kapsamındaki kılavuz ilkelere uygun olarak gerçekleştirilmelidir. Değerlendirmeye ilişkin temel gereklilikler, geriye dönük değerlendirmelere (ara, nihai ve harcama sonrası değerlendirmeler) uygulanırken, ileriye dönük değerlendirmeler (harcama sonrası değerlendirmeler ve etki değerlendirmeleri) ilgili rehberleri temel almalıdır.

KONTROL ETKİLİLİĞİNİN DEĞERLENDİRİLMESİNE YÖNELİK TAVSİYELER

Bilgi Notu: Kontrol etkililiğini değerlendirirken , iki temel soru sorulmalıdır:

1. GM nin kendine özgü faaliyet ve risklerini dikkate alarak, mevcut kontrol düzenlemeleri yeterli mi?
2. Kontrol düzenlemeleri öngörüldüğü şekliyle uygulamaya aktarılabilmiş mi?

Yönetimin, söz konusu ICS kapsamında kontrol etkililiğini değerlendirirken dikkate almak isteyebileceği bazı sorular aşağıda verilmiştir:

- Değerlendirme faaliyetleri, belirlenen amaçlara ulaşacak şekilde düzenlenmiş ve gerekli kaynaklar ayrılmış mı?
- Değerlendirme faaliyetleri şeffaf ve tutarlı bir şekilde planlanmış mı ve buna bağlı olarak , ilgili denetim sonuçları işlevsel ve stratejik karar verme ve raporlama ihtiyaçları için zamanında hazır bulundurulabilecek mi?
- Değerlendirme tasarımı açık ve belirli hedefler ile değerlendirme sürecini ve sonuçlarını yönetmede kullanılacak uygun yöntemler ve araçlar sunuyor mu?
- Değerlendirme faaliyetleri güvenilir, sağlam ve eksiksiz sonuçlar sunuyor mu? Değerlendirme raporları uygulamada yönetim tarafından kullanılıyor mu? Örneğin , GM nin karar verme süreci ve ya GM tarafından hazırlanan politika teklifleri ile yasama teklifleri üzerinde gerçekten etkililer mi? Etkili değillerse neden?
- Değerlendirme sonuçları , sonuçlardan azami fayda sağlayacak ve karar vericiler ve paydaşların ihtiyaçlarını karşılayacak şekilde duyuruluyor mu?

ICS 15. İç Kontrol Sistemlerinin Değerlendirmesi: Yönetim , uygulayıcı kurumların gerçekleştirdiği işlemler de dahil olmak üzere , GM nin kilit iç kontrol sistemlerinin etkililiğini yılda en az bir kez değerlendirmeye tabi tutar.

GEREKLİLİKLER

- Yönetim , GM kilit iç kontrol sistemlerinin etkililiğini ve uygulayıcı organların gerçekleştirdiği işlemleri en az yılda bir kez değerlendirmelidir. Bu tür bir öz değerlendirme , gözetim raporlarının yönetimce yapılan gözden geçirmeleri veya personel anketleri ile birleştirilen personel görüşmeler; değerlendirme ve harcama sonrası doğrulamaların sonuçları; denetim tavsiyeleri ve GM nin iç kontrol etkililiği hakkındaki diğer kaynaklar temelinde yapılabilir.
- Yıllık temelde – yıllık faaliyet raporunun bir parçası olarak- Kaynak Müdürü/ İç Kontrol Koordinatörü, yıllık faaliyet raporunda sunulan , yönetim ve iç kontrol sistemleri hakkındaki bilgilerin doğruluğu ve ayrıntılı ve eksiksiz olma düzeyi hakkında bir beyan imzalamalıdır.

KONTROL ETKİLİLİĞİNİN DEĞERLENDİRİLMESİNE YÖNELİK TAVSİYELER

Bilgi Notu: Kontrol etkililiğini değerlendirirken , iki temel soru sorulmalıdır:

1. GM nin kendine özgü faaliyet ve risklerini dikkate alarak, mevcut kontrol düzenlemeleri yeterli mi?
2. Kontrol düzenlemeleri öngörüldüğü şekliyle uygulamaya aktarılabilmiş mi?

Yönetimin, söz konusu ICS kapsamında kontrol etkililiğini değerlendirirken dikkate almak isteyebileceği bazı sorular aşağıda verilmiştir:

- GM nin iç kontrol sistemlerine ilişkin öz değerlendirmeye katılan yönetici ve personel, iç kontrol ve risk değerlendirmeye ilişkin yeterli bilgi ve anlayışa sahip mi? Değilse , uygulamanın çıktı ve sonuçlarını etkileyebilecek yanlış anlama ve yorumlamaları ortadan kaldırmak için neler yapılıyor?

- Öz değerlendirme gerekli şekilde düzenlenmiş mi ve fayda sağlamayı ve değer katmayı amaçlıyor mu (veya "bürokratik bir yük" olarak mı algılanıyor)? Kıdemli yöneticiler tarafından yeterince destekleniyor mu?
- Öz değerlendirme GM nin temel faaliyet ve risklerine odaklanıyor mu? Çok geniş veya çok ayrıntılı bir kapsam etkililiğini azaltabilir.

- Öz değerlendirme sonuçları yeterince destekleniyor mu; örneğin, diğer ilgili kaynaklara yapılan referanslar yoluyla?

ICS 16. İç Denetim Kapasitesi: GM bünyesinde , GM nin faaliyetlerine değer katmak ve bu faaliyetleri geliştirmek amacıyla bağımsız ve nesnel güvence ve danışmanlık hizmetleri sunan bir İç Denetim Kapasitesi (İDK) vardır.

GEREKLİLİKLER

- GM İç Denetim Kapasitesinin (İDK) görev ve sorumlulukları , resmi olarak bir denetim yönergesi ile tanımlanmalıdır.
- Yıllık denetim iş planı risk temelli bir plan olup IAS ile düzenlenen çok yıllı stratejik planın bir parçasını oluşturmalı ve GM tarafından onaylanmalıdır.
- Genel Müdür, İDK nın denetlediği faaliyetlerden bağımsız olmasını sağlamalıdır.
- Genel Müdür, İDK nın denetim iş planını hayata geçirmek için yeterli ve gerekli kaynaklara sahip olmasını sağlamalıdır.

KONTROL ETKİLİLİĞİNİN DEĞERLENDİRİLMESİNE YÖNELİK TAVSİYELER

Bilgi Notu: Kontrol etkililiğini değerlendirirken , iki temel soru sorulmalıdır:

1. GM nin kendine özgü faaliyet ve risklerini dikkate alarak, mevcut kontrol düzenlemeleri yeterli mi?
2. Kontrol düzenlemeleri öngörüldüğü şekliyle uygulamaya aktarılabilmiş mi?

Yönetimin, söz konusu ICS kapsamında kontrol etkililiğini değerlendirirken dikkate almak isteyebileceği bazı sorular aşağıda verilmiştir:

- İDK –Komisyon örgütlenmesi için uygun olduğu durumlarda- uluslar arası kabul görmüş denetim standartlarını veya eşdeğer standartları uyguluyor mu(İç Denetçiler Enstitüsü IAA tarafından yayınlanan standartlar gibi)? Özellikle , İDK nın kurumsal bağımsızlığını tehlikeye atacak herhangi bir durum söz konusu mu? Denetçiler dürüstlük, nesnelik, gizlilik ve yeterlilik ilkeleri hakkında bilgi sahibi mi ve bunların tümünü yürüttükleri denetim faaliyetlerine uygulayabiliyor mu?

EK 3- TERCİHLİ DEĞERLENDİRME MODELİ

İç kontrol çerçevesine ilişkin gözden geçirmenin amaçlarından biri esnekliği artırmaktır. Tüm ICS ler tüm GM ler-Müdürlükler ve Birimler- için her zaman aynı derecede önemli olmayabilir. Her birimin faaliyetleri, öncelikleri, temel riskleri, kontrol ortamı ve diğer hususlarına bağlı olarak; yönetim etkililiğe daha fazla önem verilmesi gereken Standartları belirleyecektir.

Aşağıda sunulan model –tercihli bir modeldir- her düzeydeki yönetime kendileriyle en çok ilgisi olan ICS leri (bir başka deyişle, en çok çaba ve kaynağın ayrılması gereken iç kontrol alanları) tanımlamada yardımcı olabilir.
DİKKAT: tabloda önerilen "yüksek düzeyde ilgili" olma nedenleri yol gösterici olup ayrıntılı değildir.

Etkili Lönetim İçin İç Kontrol Standartı	**İlgi düzeyi**	**Yüksek Düzeyde İlgi Olma Nedenleri**
1.Misyon: GM nin kuruluş nedeni, GM hedef kitlesinin bakış açısıyla oluşturulmuş güncel ve kesin misyon ifadeleriyle açık bir şekilde ortaya konur.	Yüksek? Normal?	-Kurumun genel hedefleri , stratejisi ve çalışma yöntemlerinde yapılan önemli değişiklikler -Kurumun misyon ve hedefleri hakkında yetersiz bilgi
2.Etik ve Kurumsal Değerler: Yönetim ve personel etik ve kurumsal değerler hakkında bilgi sahibidir ve bu ortak değerleri paylaşır ve kendi davranışlarıyla ve karar alma mekanizmaları yoluyla hayata geçirip destekler.	Yüksek? Normal?	-Çıkar çatışması, mali yolsuzluk, dahili bilgilerin kötüye kullanılması veya diğer etik hususlarda açık faaliyetler -Etik hükümler ve etik davranışlar hakkındaki bilinç konusunda yaşanan endişe -Bu alanda yakın zamanda yaşanan başarısızlıklara ilişkin somut bulgular
3.Personel Atamaları ve Personel Yer Değiştirmeleri: Personel atama ve işe alımları GM nin hedef ve öncelikleri temelinde yapılır. Yönetim, personel sürekliliği ve yenilenmesi arasında doğru bir denge kurabilmek amacıyla personel yer değiştirmelerini düzenler ve planlar.	Yüksek? Normal?	-Kurumun öncelik ve görevlerinde sık sık meydana gelen değişiklikler (esneklik ihtiyacı) -Katılık belirtileri değişikliğe karşı direnç -Kurumun performansını olumsuz yönde etkileyen işe alım veya personel ataması hususları -Personel planlama ve atama araçlarında artış ve gelişme ihtiyacı -İşe girip-çıkan personel sayısının , kurum performansını etkileyecek kadar yüksek oluşu. -işin içeriği veya işten beklentiler konusunda personel tatminsizliği olduğuna dair göstergeler. -Yeni fikirler ve çalışma yöntemlerine duyulan ihtiyaç (personel profilinin yenilenmesi ihtiyacı)
4.Personel Değerlendirme ve Geliştirme: Personel performansını , GM nin genel hedefleriyle uyumlu yıllık bireysel hedefler temelinde değerlendirir. Söz konusu hedeflere ulaşmak için gerekli becerileri geliştirmek amacıyla yeterli önlemler alınır.	Yüksek? Normal?	-Personel performansının artırılması ihtiyacı -Yıllık hedefler veya değerlendirmelere ilişkin önemli personel şikayetleri -Beceri ve yeterliliklerin muhafaza edilmesi veya geliştirilmesi ihtiyacı -Mevcut eğitim faaliyetleri, kurumun hedef ve faaliyetleri ile yeterince uyumlu değildir.

5. hedefer ve Performans Göstergeleri: GM'nin hedeferi açık bir şekilde tanımlanır ve gerekli durumlarda günce İlenir. hedefer, bu hedefere ulaşılıp ulaşılamadığının izlenebilmesini mümkün kılacak şekilde belirlenir. Yönetimin hedefer konusunda kaydedilen ilerlemeyi değerlendirmesi ve raporlamasını kolaylaştırmak amacıyla kilit performans göstergeleri belirlenir.	Yüksek? Normal?	-Kurum strateji, hedef ve amaçlarında yapılacak büyük değişiklikler -Mevcut hedefer yeterince açık değildir, kabul edilmemiştir ve anlaşılmamıştır -Mevcut göstergeler yeterince ilgili değildir -Mevcut hedefer/göstergeler (çeşitli nedenlerle) uygulamada yönetim aracı olarak kullanılmamaktadır -Gösterge/raporlama gerektiren yeni kilit faaliyetler geliştirmelidir.
6. Risk Yönetimi Süreci: Geçerli hükümler ve rehberlerle uyumlu bir risk yönetimi süreci, yıllık faaliyet planlamasına dahil edilir.	Yüksek? Normal?	-Yeni veya ciddi değişikliklere tabi tutulmuş faaliyetler - GMMüdürlük/Birimlere yönelik ciddi yeniden teşkilatlanmalar - Mevcut risk değerlendirme süreci ağırdır veya etkili değildir. - Risk yönetimi, düzenli yönetim süreçlerine gerekli şekilde entegre edilmemiştir - Risk yönetimi kavramı hakkındaki bilinç düzeyi düşüktür
7. işleyiş Yapısı: GM'nin işleyiş yapısı, yetkilerin uygun şekilde paylaştırılması yoluyla karaların etkili bir şekilde alınmasını sağlar. GM'nin hassas işlevleri ile ilişkili riskler, hafişetici kontroller ve gerekmesi durumunda personel yer değiştirmeleri yoluyla yönetilir. Yeterli BT yönetim yapıları mevcuttur.	Yüksek? Normal?	- GM/Müdürlüğün önemli ölçüde yeniden teşkilatlandır ılm ası - Mevcut yapılanma en uygun yapılanma olmayıp kurum performansını düşürüyor olabilir - Verilen yetkilere yönelik risk değerlendirmesinin geliştirilmesi gerekmektedir - Hassas işlevlerin sayısı oldukça yüksektir - Hassas işlevler yeterince analiz edilmemiştir - Hafişetici kontrollerin öngörüldüğü şekilde uygulamaya aktarılıp aktarılmadığı konusunda belirsizlikler (hassas işlevler) - Bilgi Sisteminin gelişimi, bakımı ve güvenliği alanlarında önemli sorumluluklar -GM faaliyetleri büyük oranda BT sistemlerine dayanır. Değişen ihtiyaçlara ayak uydurabilmesi için, BT sistemlerinin sürekli elden geçirilmesi gerekmektedir. -GM faaliyetleri, büyük BT yatırım ve geliştirmeleri gerektirmektedir.
8.Süreç ve Prosedürler : GM nin faaliyetlerinin hayata geçirilmesi ve kontrolünde başvurulan süreç ve prosedürler etkili ve etkindir, yeterli düzeyde belgelendirilmiştir ve geçerli hükümlere uygundur. Bu süreç ve prosedürler; görevler ayrılığının gerçekleştirilmesini sağlayan düzenlemeleri, bazı kontrollerin atlanması uygulamalarının ve politika ve prosedürlerde görülen sapmaların takip edilmesine ve bunlara önceden onay verilmesine ilişkin düzenlemeleri kapsar.	Yüksek? Normal?	-Karmaşık faaliyetler (işleyiş hususları) -Karmaşık faaliyetler (yasal ve düzenleyici hususlar) -Üçüncü taraşarı kapsayan faaliyetler (örn,Üye Devlet kurumları) -Önemli yasal/düzenleyici ve mali riskleri temsil eden faaliyetler - Mevcut süreç ve prosedürler oldukça hantaldır ve daha etkili bir hale getirilebilir -Süreç ve prosedürlere ilişkin belgeler güncel, kullanıcı dostu ve kolay erişebilir değildir -Kurum süreç ve prosedürlerine ilişkin risk analizinin geliştirilmesi gerekmektedir
9.Yönetim Tarafından Yapılan Gözetim.: Yönetim gözetimi, faaliyetlerin geçerli hükümler çerçevesinde etkin ve etkili şekilde uygulanmasını sağlamak amacıyla yapılır.	Yüksek? Normal?	-Karmaşık faaliyetler veya prosedürler - Siyasi açıdan hassas faaliyetler - Yüksek parasal değeri olan işlemler -Görev ayrılığının gerekli şekilde

		yapılmaması -Kontrol bilincinin iyi yerleşmemiş olması -Deneyimli ve yetenekli personel yetersizliği -işletim faaliyetlerinin yeniden düzenlenmesi veya bu alanda yapılan köklü değişiklikler -Süreç ve prosedürlerin öngörüldüğü şekliyle uygulamaya aktarılması konusunda belirsizlikler Yeni ve ya modenize edilmiş BT sistemleri -Yüksek çıkar çatışması riski -Gözetim, beceri ve teknikleri yetersiz düzeydedir. -Dış taraflara (yükleniciler, ulusal kurumlar veya denetçiler) gereğinden fazla bağımlılık
10.İş sürekliliği: "Düzenli iş akışında" meydana gelebilecek aksaklıklar durumunda birimlerin devamlılığını sağlamak için gerekli önlemler alınır. İş sürekliliği planları, büyük bir aksaklık halinde bile Komisyonun çalışmaya devam edebilmesini sağlamayı amaçlar.	Yüksek? Normal?	-Kurum faaliyetlerinin kısa süreler için bile olsa kesintiye uğraması ciddi sonuçlar doğurabilir (müşteri şikayetleri, basının olumsuz yaklaşımı, güvenlik hususları vb) -Kurumun temel faaliyetleri büyük oranda BT sistemlerine dayanmaktadır. -Yetersiz devir düzenlemeleri, yedekleme prosedürleri, yüksek personel işe giriş-çıkışı vb. Nedenlerle sıkça yaşanan sorunlar
11. Belge Yönetimi: GM nin belge yönetiminin güvenli, etkin (özellikle uygun bilginin geri çağrılması konusunda) ve mevzuata uygun bir şekilde gerçekleştirilmesini sağlamak amacıyla gerekli işlem ve prosedürler mevcuttur.	Yüksek? Normal?	-Kurum tarafından üretilen, alınan veya yönetilen belgelerin hacmi oldukça fazladır. -GM faaliyetleri, büyük miktarda belgenin incelenmesini gerektirmektedir. -Kurum, hassas belgeleri yönetmektedir.
12. Bilgi ve İletişim: Kurum içi iletişim, yönetim ve personelin (iç kontrol alanındaki sorumlulukları da dahil olmak üzere) sorumluluklarını etkili ve etkin bir şekilde yerine getirmelerini sağlar. GM nin kurum dışı iletişiminin etkili, tutarlı ve Komisyonun kilit politika mesajlarına uygun şekilde gerçekleştirilmesini sağlamak için, uygun olduğu durumlarda, GM bir "kurum dışı iletişim" stratejisi geliştirebilir. GM tarafından kullanılmakta olan ve /veya geliştirilen BT sistemleri (GM nin sahibi olduğu durumlarda), gizlilik ve bütünlükle ilgili tüm tehlikeler karşısında yeterli düzeyde korunur.	Yüksek? Normal?	İç İletişim -Kaliteli bilginin temel öneme haiz olduğu karmaşık faaliyekler -Yetki devrinin yüksek düzeyde gerçekleştirilmesi -Coğrafi olarak geniş alana yayılmış faaliyetler -Mevcut yönetim tabelaları, ilgili veya yeterli yönetim bilgisini sağlamamaktadır. -Yönetim bilgisinin personelle paylaşılması uygulaması geliştirilmelidir. -Motivasyon, bağlılık ve takım ruhu konularının etkilenmesi gerekmektedir. -Yönetim ve personelin, iç kontrol alanındaki sorumlulukları hakkında yeterince bilgili olmadıklarını gösteren hususlar Dış İletişim -Dış dünya ile sıkça gerçekleştirilen iletişim/GM faaliyetleri ile ilgili iletişim dış tarafları etkilemektedir. -Dış taraflar veya müşterilerden gelen tepkiler, dış iletişimin geliştirilmesi gerektiğini göstermektedir. -Yönetimin, müşterilerinin sunulan hizmetleri nasıl buldukları konusunda kesin bir fikri yoktur.

		Bilgi sisteminin güevnliği -Bilgi sistemi güvenliği alanındaki önemli sorumluluklar/hassas verilerin yönetimi /bilgi güvenliğini etkileyebilecek önemli veya sıkça karşılaşılan sorunlar -Kurum performansını etkileyen , sıkça karşılaşılan veya önemli Bilgi Sistemi sorunları vardır.
13. Muhasebe Ve Mali Raporlama: Kurumun^yıllık hesapları ve mali raporlarının hazırlanmasında kullanılan muhasebe verileri ve ilgili bilgilerin doğru , eksiksiz ve zaman açısından geçerli olmasını sağlamaya yönelik yeterli prosedür ve kontroller mevcuttur.	Yüksek? Normal?	-Mali işlemlerin büyüklüğü/yüksek değerlerde oluşu veya karmaşıklığı -Elle yapılan kontrollere fazlaca bağımlı olunması -Karmaşık veya yeni muhasebe sistemleri -Kurumun muhasebe veri ve bilgilerinin güvenirliği ve bütünlüğüne ilişkin belirsizlikler -Gerekli muhasebe ve mali raporlama becerilerinin eksikliği
14.Faaliyet Değerlendirmeleri: Harcama programları, mevzuat ve diğer harcama dışı faaliyetlere ilişkin değerlendirmeler, söz konusu faaliyetlerin ulaşmayı ve karşılamayı amaçladığı sonuçlar, etkiler ve ihtiyaçları değerlendirmek amacıyla yapılır.	Yüksek? Normal?	-Olumsuz tanıtım (basın) riski, politika başarılarının yetersiz düzeyde kalması durumunda oldukça yüksek bir risktir. -Değerlendirme fonksiyonu kaynak , beceri ve deneyimleri konusunda endişeler vardır. -Her yıl hazırlanan değerlendirme raporları , yönetim kararları üzerinde ya çok az etkiye sahiptir ya da hiç etkili değildir (birçok nedenden ötürü)
15.İç Kontrol Sistemlerinin Değerlendirmesi: Yönetim, uygulayıcı kurumların gerçekleştirdiği işlemler de dahil olmak üzere, GM nin kilit iç kontrol sistemlerinin etkililiğini yılda en az bir kez değerlendirmeye tabi tutar.	Yüksek? Normal?	-Karmaşık faaliyetler veya önemli riskleri içeren faaliyetler -İç kontrol sistemlerinin kalitesine ilişkin belirsizlikler -İç kontrolün yetersiz olduğuna dair işaretler (yüksek hata oranları, şikayetler) -Öz değerlendirme sürecinin yeterliliği ve öz değerlendirme sonuçlarının güvenirliği ve ilgililiği konusundaki endişeler
16. İç Denetim Kapasitesi: GM bünyesinde, GM nin faaliyetlerine değer katmak ve bu faaliyetleri geliştirmek amacıyla bağımsız ve nesnel güvence ve danışmanlık hizmetleri sunan bir İç Denetim Kapasitesi (İDK) vardır.	Yüksek? Normal?	-Mevcut İDK faaliyetleri yeterince katma değer sağlamamaktadır. -İDK kaynakları, beceriler veya deneyimlerine ilişkin endişeler _İDK nın bağımsızlık ve tarafsızlığını tehlikeye sokabilecek (çıkar çatışması, uygun olmayan raporlama satırları, denetlenen faaliyetlere katılımda uyumsuzluk, vb. Gibi nedenlerle) durumlar

EK 4- ÖNCEKİ 24 ICS İLE İLİŞKİ

Bir önceki ICS ile gözden geçirilmiş ICS yi karşılaştırdığımızda, gözden geçirilmiş ICS nin ayrıntılı ve özel gereklilikleri içermediği ancak iç kontrol için temel ilkeleri ortaya koyduğunu görüyoruz. Ayrıntılı ve özel gereklilikler ilgili "Gerekliliklerde" sunulmuştur.

Bir Önceki 24 İç Kontrol Standartı	**Gözden Geçirilmiş ICS veya İlgili Gerekllikler Kapsamına Alınanlar**
1.Etik ve Dürüstlük	2.Etik ve Kurumsal Değerler
2.Misyon, Roller ve Görevler	1.Misyon 4.Personel Değerlendirme ve Geliştirme
3.Personel Yeterliliği	4.Personel Değerlendirme ve Geliştirme
4.Personel Performansı	4.Personel Değerlendirme ve Geliştirme
5. Hassas İşlevler	7.İşleyiş Yapısı
6.Yetki Devri	7.İşleyiş Yapısı
7.Hedef Belirleme	5.Hedefler ve Performans Göstergeleri
8.Çok Yıllı Programlama	5.Hedefler ve Performans Göstergeleri
9.Yıllık Yönetim Planı	5.Hedefler ve Performans Göstergeleri
10.Performansın Hedefler ve Göstergeler Temelinde İzlenmesi	5.Hedefler ve Performans Göstergeleri
11.Risk Analizi ve Yönetimi	6.Risk Yönetim Süreçleri
12.Yeterli Yönetim Bilgileri	12.Bilgi ve İletişim
13.E-Posta Yoluyla Kayıt ve Raporlama Sistemleri	11. Belge Yönetimi
14.Raporlama Uygunsuzlukları	2.Etik ve Kurumsal Değerler
15.Prosedürlerin Belgelendirilmesi	8. Süreç ve Prosedürler
16.Görevler Ayrılığı	8. Süreç ve Prosedürler
17.Gözetim	9.Yönetim Tarafından Yapılan Gözetim
18.Raporlama İstisnaları	8. Süreç ve Prosedürler
19.İşlemlerin Sürekliliği	10. İş Sürekliliği
20.İç Kontrol Zayıflıklarının Raporlanması ve Düzeltilmesi	12. Bilgi ve İletişim
21.Denetim Raporları	9.Yönetim Tarafından Yapılan Gözetim
22.İç Denetim Kapasitesi	16. İç Denetim Kapasitesi
23.Değerlendirme	14.Faaliyet Değerlendirmeleri
24.İç Kontrol Yıllık Gözden Geçirmesi	15.İç Kontrol Sistemlerinin Değerlendirmesi

Bilgi Notu

ARAŞTIRMA VE TASNİF GRUBU 11.03.2002

ABD Sayıştayı Tarafından Yayımlanan

"Federal Devlette İç Kontrol Standartları"

İsimli Doküman Hk.

Federal Hükümette
İç Kontrol Standartları

Çeviri

Baran Özeren

Uzman Denetçi

Araştırma ve Tasnif Grubu

Mart 2002

Eserin Özgün Adı

Standarts for lnternal Control in the Federal Government

Washington DC, Kasım 1999

Önsöz

Federal politikaları oluşturanlar ve program yöneticileri kurumların misyonlarını daha etkin biçimde yerine getirmeleri ve daha başarılı program sonuçları elde etmeleri için sürekli olarak yöntemler ararlar; başka bir deyişle hesapverme sorumluluğunu geliştirme metotları bulmaya çalışırlar. Başarılı sonuçlar alınmasına ve faaliyetlere ilişkin problemlerin azaltılmasına katkıda bulunan en önemli faktör iç kontrolün uygun biçimde yapılmasıdır. Etkin iç kontrol değişen çevre koşullarının, çeşitlenen taleplerin ve önceliklerin üstesinden gelmek üzere değişimin yönetilmesine de yardımcı olur. Kurumların operasyonel süreçlerini geliştirmek ve yeni teknolojik gelişmeleri uygulamaya koymak üzere çaba sarf etmelerinden ve programların değişmesinden dolayı, yönetimlerin, kontrol faaliyetlerinin etkinliğinden ve gerekiyorsa güncelliğinden emin olmak için iç kontrollerının niteliğini ve değerini süreklilik temelinde saptayıp değerlendirmeleri gerekir.

1982 tarihli Federal Yöneticilerin Malî Güvenilirliği Yasası (The Federal Manager's Financial Integrity Act) kamuda iç kontrol standartları yayımlama görevini ABD Sayıştayına vermektedir. Bu standartlar iç kontrolün oluşturulup sürdürülmesine ve yolsuzluk, israf, suiistimal ve kötü yönetim riskinin en yüksek olduğu önemli performans ve yönetim sorunlarını ve alanlarını belirleyip bunlara dikkat çekilmesine dönük genel bir çerçeve sunar. Yönetim ve Bütçe Ofisinin 21 Haziran 1995 tarihinde gözden geçirip değiştirdiği ***"Yönetimin Hesapverme Sorumluluğu ve Kontrol"*** hakkındaki A-123 no'lu Genelgesi kontrollerla ilgili olarak değerlendirme yapmaya ve rapor hazırlamaya yönelik özel hükümler getirmektedir. Bu dokümandaki iç kontrol terimi yönetim kontrolü terimiyle eşanlamlı kullanılmakta olup bir kurumun faaliyetlerinin bütün boyutlarını (program amaçlı, finansal ve uygunluk) içermektedir.

Son yıllarda, başka yasalar iç kontrole yeniden odaklanmayı teşvik etmektedir. 1993 tarihli Kamusal Performans ve Sonuçlar Yasası (Government Performance and Results Act) kurumların misyonlarını belirgin hale getirmelerini, stratejik ve yıllık performans hedeflerini oluşturmalarını ve bu hedefler doğrultusunda performanslarını ölçüp raporlamalarını hükme bağlamaktadır. İç kontrol yöneticilerin hedeflerine ulaşmalarında önemli bir rol oynar. Keza, 1990 tarihli Malî İşlerden Sorumlu Üst Düzey Yöneticiler Yasası (Chief Financial Officers Act) malî yönetim sistemlerinin iç kontrol standartlarıyla uyumlu olmasını gerektirmekte; 1996 tarihli Malî Yönetimi Geliştirme Yasası da iç kontrolü malî yönetim sistemlerinin geliştirilmesinin ayrılmaz bir parçası olarak tanımlamaktadır.

Bilişim teknolojisindeki süratli gelişmeler modern bilgisayar sistemleriyle ilgili iç kontrol rehberinin güncellenme ihtiyacını vurgulamaktadır. Beşerî sermayenin yönetimi iç kontrolün önemli bir parçası olarak kabul edilmektedir. Ayrıca, Treadway Komisyonunu Destekleyen Kuruluşlar Komitesi (Committee of

Sponsoring Organizations of the Treadway Commission- COSO) tarafından yayımlanan ***"İç Kontrol-Bütünleşik Sistemi"*** dokümanı aracılığıyla özel sektör iç kontrol rehberini güncelleştirmiş bulunmaktadır. Sonuç olarak, hazırladığımız bu güncel standartlar daha önce yayınladığımız "Federal Devlette İç Kontrol Standartları"nın yerine geçmektedir.

Bu güncelleştirme önemli kamusal işlemlerinin yürütülmesi amacıyla bilişim teknolojisinden giderek artan biçimde yararlanılması için daha dikkat çekici fırsatlar yaratmakta, beşerî sermayenin değerini öne çıkarmakta ve yeri geldiğinde, özel sektör için hazırlanmış söz konusu modern iç kontrol rehberini kapsamaktadır. Bu standartlar 2000 malî yılının başlangıcından itibaren yürürlüğe konulacak ve Federal Yöneticilerin Malî Güvenilirliği Yasası da bu yılı kapsayan bilgileri sunacaktır.

Bu standartların geliştirilmesinde değerli katkılarını esirgemeyen kamu görevlilerinin devlet muhasebe uzmanlarının, malî sektör mensuplarının ve akademisyenlerin çabalarını takdirle karşılıyoruz.

David M.Walker
ABD Sayıştay Başkanı

Giriş

Aşağıdaki tanım, hedefler ve temel kavramlar iç kontrol standartlarının esasını teşkil eder.

Tanım ve Hedefler

İç Kontrol

Bir örgüt yönetiminin ayrılmaz öğesi olup;

2. Faaliyetlerde etkinlik ve verimlilik,
3. Finansal raporlamada güvenilirlik,
4. Yürürlükteki yasalara ve düzenlemelere uygunluk,

amaçlarının gerçekleşmesi konusunda makul güvence sağlar.

İç kontrol bir örgütü yönetmenin önemli bir parçasıdır. İç kontrol görevleri, amaçları ve hedefleri gerçekleştirmede yararlanılan planları, metotları ve prosedürleri kapsar ve bu suretle, performansa dayalı yönetime katkıda bulunur. İç kontrol, ayrıca, varlıkları korumada ve hataları ve yolsuzlukları önlemede ve ortaya çıkarmada ilk savunma hattı olarak işlev görür. Kısacası, yönetim kontrolü ile eş anlamlı olarak kullanılan iç kontrol, kamu kaynaklarının etkin idaresi aracılığıyla kamu program yöneticilerinin arzulanan sonuçları elde etmesine yardımcı olur.

İç kontrol, kuruluş hedeflerinin başarılabilmesi için şu hususlarda güvence sağlar:

- Kurum kaynaklarının kullanımı dahil olmak üzere faaliyetlerin etkinliği ve verimliliği,
- Bütçenin uygulanması, finansal tablolar ile ilgili raporlar dahil olmak üzere finansal raporlama ve iç ve dış kullanıma ilişkin diğer raporların güvenilirliği,

- Yürürlükteki yasalara ve düzenlemelere uygunluk.

Bu hedeflerin alt kümesini varlıkların korunması oluşturur. İç kontrol yetkisiz elde etmenin, kullanmanın veya bir kuruluşun varlıklarını elden çıkarmanın önlenmesi veya derhal ortaya çıkarılması bakımından makul güvence sağlamak üzere tasarlanmalıdır.

Temel Kavramlar

İç Kontrol

- **Faaliyetlerin sürekli biçimde ayrılmaz bir öğesini oluşturur.**
- **Kişiler tarafından hayata geçirilir.**
- **Mutlak güvence değil, makul güvence sağlar.**

Standartların tasarlanmasına ve yaşama geçirilmesine yarayan bir çerçeveyi sözü edilen bu temel kavramlar sağlar.

İç kontrol faaliyetlerin sürekli biçimde ayrılmaz bir öğesini oluşturur

İç kontrol tekil bir olay değil, bütün bir örgüt faaliyetlerinde ve devamlılık temelinde oluşan bir seri eylem ve aktivitedir. İç kontrol, kuruluş içinde ayrı bir sistem olmaktan çok, yönetimin faaliyetlerini düzenlemede ve yönlendirmede yararlandığı sistemlerin ayrılmaz bir parçası olarak kabul edilmelidir. Bu bakımdan iç kontrol, yöneticilerin kurumu çalıştırmalarına ve amaçlarını süreklilik temelinde gerçekleştirmelerine yardımcı olmak üzere alt yapının bir parçası olarak inşa edilen bir yönetim kontrolüdür.

İç kontrol kişiler tarafından hayata geçirilir

İç kontrolü çalıştıranlar kişilerdir. Başarılı bir iç kontrolün sorumluluğu bütün yöneticilere düşmektedir. Yönetim amaçları belirler, kontrol mekanizmalarını oluşturur ve faaliyetleri uygulamaya koyar ve kontrolü izler ve değerlendirir. Ancak örgüt içindeki bütün personel bunun gerçekleşmesinde önemli rol oynar.

İç kontrol mutlak güvence değil, makul güvence sağlar.

Yönetim iç kontrolü maliyet ve faydaları ile bağlantılı olarak tasarlamak ve uygulamalıdır. Ne kadar güzel tasarlanıp uygulanırsa uygulansın, bütün kuruluş amaçlarının gerçekleşmesi konusunda mutlak güvence

sağlayamaz. Kontrol dışındaki faktörler veya yönetimin nüfuzu kurumun hedeflerinin tümünü gerçekleştirme gücünü olumsuz
etkileyebilir. Örneğin; insan hataları, karar ya da yorum hataları ve kontroldan kaçınmak üzere gizli anlaşmalar yapma kuruluş amaçlarının gerçekleşmesini etkileyebilir. Bu nedenle, konulduğu her yerde iç kontroller kuruluş amaçlarını gerçekleştirmenin mutlak değil makul güvencesini sağlar.

İç Kontrol Standartları

Standartların Sunumu

İç Kontrolün Beş Standardı

- **Kontrol Ortamı**
- **Risk Değerlendirmesi**
- **Kontrol Faaliyetleri**
- **Bilgi ve İletişimler**
- **İzleme**

Bu standartlar iç kontrolün kamuda kabul edilebilir asgari kalite düzeyini belirler ve iç kontrolün değerlendirilebileceği bir temel oluşturur. Bu standartlar bir kuruluşun faaliyetlerinin bütün cephelerine (program amaçlı, finansal ve uygunluk) uygulanabilir. Bununla birlikte, standartların yasa hazırlama, kural koyma ya da diğer takdirî politika üretme ile ilgili olarak bir kuruluş içinde usulüne uygun biçimde devredilmiş yetkiye sınırlama getirmeleri ya da bu yetkiyle çalışmaları istenmez. Bu standartlar genel bir çerçeve sağlar. Bu standartların uygulanması açısından, yönetim kuruluş faaliyetlerine uygun olacak ve faaliyetlerin ayrılmaz bir parçası olarak tesis edilecek ayrıntı politikalar, prosedürler ve pratikler geliştirmekten sorumludur.

Bu standartların her biri aşağıda kısa ve özlü bir ifadeyle sunulmuştur. Yöneticilerin bu standartları kendi günlük faaliyetleriyle bütünleştirmelerine yardımcı olmak üzere ek bilgi sağlanacaktır.

Kontrol Ortamı

Yönetim ve çalışanlar, bütün bir örgüt içinde, iç kontrole ve dikkatli bir yönetime yönelik olarak pozitif ve destekleyici bir tavrı geliştiren ortamı oluşturmalı ve sürdürmelidirler.

Pozitif bir kontrol ortamı diğer bütün standartlar için temel oluşturur. Disiplin ve yapılanma getirir ve iç kontrol kalitesini etkileyen iklimi yaratır. Birçok faktör kontrol ortamını etkiler.

Faktörlerden biri, yönetim ve çalışanlar tarafından dürüstlüğün ve etik değerlerin korunması ve sergilenmesidir. Kuruluş yönetimi bu alanda önderlik ederek özellikle, örgütün etik üslubunun oluşturulmasında ve sürdürülmesinde, uygun davranışa yönelinmesinde, etik olmayan davranışlara karşı konulmasında ve gerektiğinde, disiplin sağlanmasında önemli rol oynar.

Bir diğer faktör, yönetimin uzmanlığa olan bağlılığıdır. Bütün personelin kendilerine verilen görevi başarması kadar başarılı bir iç kontrolü geliştirmesinin ve uygulamanın önemini kavramasına imkân veren bir uzmanlık seviyesine sahip olması ve bunu sürdürmesi gerekir. Yönetim farklı görevler için gereksinim duyulan elverişli bilgi ve becerileri tespit etmeli ve eğitim sağlamanın yanı sıra dürüst ve yapıcı tavsiyelerde bulunup personelin performansını değerlendirmelidir.

Yönetimin felsefesi ve iş görme tarzı da ortamı etkiler. Bu faktör kuruluşun risk üstlenmeye isteklilik derecesi ile yönetimin performans esaslı yönetime ilişkin felsefesini belirler. Ayrıca yönetimin bilişim sistemlerine, muhasebeye, personel fonksiyonlarına, izlemeye, denetimlere ve değerlendirmelere yönelik yaklaşımı iç kontrol üzerinde derin bir etki yaratabilir.

Ortamı etkileyen bir başka faktör kuruluşun organizasyonel yapısıdır. Organizasyonel yapı kuruluşun amaçlarını gerçekleştirmek üzere planlama, yol gösterme ve kontrol faaliyetlerine yönelik bir yönetim çerçevesi sağlar. Başarılı bir iç kontrol ortamı; kuruluşun organizasyonel yapısının önemli yetki ve sorumluluk alanlarını açıkça tanımlamasını ve elverişli bir raporlama hattı oluşturmasını gerektirir.

Ortam, ayrıca, kuruluşun organizasyon içinde yetkilerin ve sorumlulukların devredilme tarzından etkilenir. Yetki devri faaliyetlerin yapılmasına, ilişkilerin raporlanmasına yönelik onay ve yükümlülükler ile anlaşma iznini kapsar.

Etkili beşeri sermaye politikaları ve uygulamaları önemli bir diğer çevresel faktördür. Etkili beşeri sermaye politikaları ve uygulamaları işe alma, oryantasyon, eğitim, değerlendirme, tavsiyelerde bulunma, teşvik etme, ücret ödeme ile personelin disipline edilmesine yönelik iyi uygulamaların tesis edilmesini içerir. Ayrıca gerektiği kadar inceleme yapılmasını da kapsar.

Ortamı etkileyen son bir faktör kuruluşun Kongreyle ve Yönetim ve Bütçe Dairesi türünden gözetim kuruluşlarıyla olan ilişkileridir. Kongre kuruluşların üstlendikleri programlara onay verir ve bunların seyrini izler, merkezî kuruluşlar ise çok farklı sorun hakkında politika üretir ve rehberlik eder. Ayrıca Genel Müfettiş ve kurum içi üst düzey yönetim konseyleri etkin bir genel kontrol ortamına katkıda bulunabilir.

Risk Değerlendirmesi

İç kontrol, kuruluşun hem dış hem de iç nedenler dolayısıyla karşılaştığı risklerin bir değerlendirmesini yapmalıdır.

Risk değerlendirmesinin ön koşulu, kuruluş amaçlarının açık-seçik ve tutarlı biçimde belirlenmesidir. Risk değerlendirmesi Kamusal Performans ve Sonuçlar Yasası gereğince stratejik ve yıllık performans planlarında tespit edilmiş amaçlar gibi açıklanan amaçların gerçekleştirilmesiyle bağlantılı risklerin

tanımlanması, analiz edilmesi ve bu risklerin nasıl
yönetilmesi gerektiği hakkında bir esas oluşturulmasıdır.

Yönetimin riskleri kapsamlı biçimde tanımlaması gerekir ve yönetim hem kurum çapındaki hem de faaliyet düzeyindeki iç faktörler kadar kurum ile diğer taraflar arasındaki önemli bütün etkileşimleri dikkate almalıdır. Risk tanımlama metotları arasında kantitatif ve kalitatif değerlendirme faaliyetleri, yönetim konferansları, tahminî ve stratejik planlama, denetimler ve diğer değerlendirmelerden elde edilen bulguların dikkate alınması yer alabilir.

Riskler tanımlandığında, bunların muhtemel etkileri analiz edilmelidir. Risk analizi genel olarak riskin öneminin tahmin edilmesini, onun meydana gelme olasılığının değerlendirilmesini, riskin nasıl yönetilmesi ve hangi önlemlerin alınması gerektiğine karar verilmesini kapsar. Kuruluşların misyonlarında farklılıklar olmasından ve risk düzeylerinin kalitatif ve kantitatif olarak tespit edilmesindeki güçlük yüzünden yararlanılan spesifik risk analiz metotları kuruluşça sürekli olarak değiştirilebilir.

Kamusal, ekonomik, endüstriyel, yasal ve faaliyetlerle ilgili koşullar devamlı suretle değiştiğinden mekanizmaların bu tür değişikliklere yol açan herhangi bir spesifik riski tanımlaması ve bu riski önleyebilmesi gerekir.

Kontrol Faaliyetleri

İç kontrol faaliyetleri yönetimin direktiflerinin uygulanmakta olduğuna dair güvence sağlamaya yardımcı olur. Kontrol faaliyetleri, kuruluşun kontrol amaçlarının gerçekleşmesi bakımından etkin ve verimli olmalıdır.

Kontrol faaliyetleri politikalar, prosedürler, teknikler ile bütçenin hazırlanmasına ve uygulanmasına yönelik gereksinimleri destekleyen süreçler türünden yönetimin direktiflerini güçlendiren mekanizmalardır. Bu mekanizmalar riskleri karşılamak üzere önlemler alınmasına yardımcı olur. Kontrol faaliyetleri bir kurumun planlamasının, uygulamasının, gözden geçirmesinin ve kamu kaynaklarının idaresine yönelik hesap verme sorumluluğunun ve etkin sonuçlara ulaşmanın ayrılmaz bir parçasıdır.

Kontrol faaliyetleri kurumun bütün kademelerinde ve fonksiyonlarında oluşturulur. Bu faaliyetler arasında onaylamalar (resmî izinler, muvaffakatlar), yetkilendirmeler (izinler, yetkiler, salahiyetler), teyitler, mutabakatlar, performans incelemeleri, güvenlik sağlama ile uygun dokümantasyonun yanı sıra bu faaliyetlerin gerçekleşme kanıtı olan ilgili kayıtların yapılması ve muhafazası gibi çok geniş alanı içine alan muhtelif aktiviteler yer alır. Kontrol faaliyetleri bilgisayarlı bir bilişim sistemi ortamında ya da elle gerçekleştirilen (manual) süreçler aracılığıyla uygulanabilir.

Faaliyetler, bilgi işlemenin doğruluğunu ve tamlığını sağlama gibi, spesifik kontrol amaçlarına
göre tasnif edilebilir.

Kontrol faaliyetlerinden örnekler

Fiili performansın üst düzeyde incelenmesi,
Yönetim tarafından fonksiyonel düzeyde ya da faaliyet düzeyinde yapılan incelemeler,
Beşeri sermayenin yönetimi,
Bilgi işleme üzerindeki kontroller,
Hassas varlıklar üzerinde fiziki kontrol,
Performans ölçülerinin ve göstergelerinin oluşturulması ve gözden geçirilmesi,
Görevlerin ayrılması,
İşlemlerin ve işlerin gerektiği şekilde icrası,
İşlemlerin ve işlerin eksiksiz ve vaktinde kaydedilmesi,
Kaynaklara ve kayıtlara erişim sınırlandırmaları ve bunlarla ilgili hesap verme sorumluluğu,
İşlemlerin ve iç kontrolün uygun biçimde dokümante edilmesi.

Bütün kuruluşlar için ortak olan belirli kontrol faaliyet kategorileri bulunmaktadır.
Bunlara ilişkin örnekler aşağıda gösterilmiştir:

Fiilî Performansın Üst Düzeyde İncelenmesi

Yönetim, kuruluşun önemli başarılarının izini sürmeli ve bunları, Kamusal Performans ve Sonuçlar Yasasına göre oluşturulan planlar, ana amaçlar ve hedeflerle kıyaslamalıdır.

Yönetimce Fonksiyonel ve Organizasyonel Düzeyde Yapılan İncelemeler

Yöneticilerin, fiilî performansı örgüt genelinde planlananla ya da arzulanan sonuçlarla kıyaslaması ve önemli farklılıkları da analiz etmesi gerekir.

Beşerî Sermayenin Yönetimi

Bir örgütün işgücünün -ki beşerî sermayesidir etkin biçimde yönetimi sonuçlara ulaşılması açısından yaşamsal önemde olup iç kontrolün ayrılmaz bir parçasıdır. Yönetim beşerî sermayeye bir maliyet olarak değil bir varlık olarak bakmalıdır. Faaliyetlerin başarısı, yalnızca, işe doğru personel alınmasıyla, doğru eğitim, araçlar, sistem ve teşvikler sağlanmasıyla ve doğru sorumluluklar verilmesiyle mümkündür. Yönetim ihtiyaç duyulan becerileri süreklilik temelinde değerlendirmeli ve örgütün ana amaçlarını gerçekleştirebilmesi için gerekli becerilerle donatılmış işgücünü temin edebilmelidir. Eğitim, çalışanların beceri düzeylerini, örgütün değişen ihtiyaçlarını karşılayacak şekilde geliştirmeyi ve sürdürmeyi hedeflemelidir. İç kontrol hedeflerine ulaşılabilmesi bakımından süreklilik temelinde ve nitelikli bir gözetim gerçekleştirilmelidir. Örgütün

başarısıyla kendi performansları arasındaki bağlantıyı anlamalarına yardımcı olmak üzere, çalışanların etkin bir ödül sistemiyle desteklendiği bir performans değerleme ve tepki alma (feed back) sistemi tasarlanmalıdır.

Beşerî sermayeyi planlamanın bir parçası olarak, yönetim, ayrıca, değerli çalışanlarını en iyi ne şekilde elinde tutacağını, nihayetinde, birbiri ardısıra göreve gelmelerini nasıl planlayacağını ve gerekli becerilerin ve yeteneklerin sürekliliğini en iyi ne şekilde sağlayacağını göz önünde bulundurmalıdır.

Bilgi İşleme Üzerindeki Kontroller

Bilgi işleme sürecinde çeşitli kontrol faaliyetlerinden yararlanılır. Örneğin; bilgisayara girişi yapılan verilerin kullanıma hazır olup olmadıklarının test edilmesi, işlemlerin rakamsal olarak muhasebeleştirilmesi, kontrol hesaplarıyla dosya toplamlarının karşılaştırılması ve verilere, dosyalara, programlara erişimin kontrol edilmesi. Bilgi işlemeye dönük kontrol faaliyetleri hakkında "Bilgi Sistemlerinin Spesifik Kontrol Faaliyetleri" bölümünden daha fazla bilgi sağlanabilir.

Hassas Varlıklar Üzerindeki Fiziksel Kontrol

Bir kurum hassas varlıkları muhafaza etmek ve güvenliğini sağlamak üzere fiziksel kontrol tesis etmelidir. Örneğin; nakit, teminatlar, stoklar ile kaybolma riskine ve yetkisiz kullanıma karşı hassas olabilecek nitelikteki araç-gereçler türünden varlıkların, güvenliğinin sağlanması ve bunlara erişimin sınırlandırılması bu kontroller arasında sayılabilir. Bu tür varlıklar düzenli aralıklarla sayılmalı ve kontrol kayıtlarıyla karşılaştırılmalıdır.

Performans Ölçülerinin ve Göstergelerinin Oluşturulması ve Gözden Geçirilmesi

Faaliyetlerin performans ölçülerini ve göstergelerini izlemek üzere tesis edilmeleri gerekir. Bu faaliyetler, ilişkilerin analiz edilebilmesi ve uygun önlemlerin alınabilmesi bakımından farklı veri setlerinin diğerleriyle karşılaştırılmasını ve değerlendirme yapılmasını gerektirir. Kontroller, ayrıca, örgütsel ve bireysel performans ölçüleri ile göstergelerinin doğruluğunun ve güvenilirliğinin teyit edilmesini de hedeflemelidir.

Görevlerin Ayrılması

Hata ya da sahtecilik riskinin azaltılması bakımından, önemli görevlerin ve sorumlulukların farklı kişiler arasında bölüşülmesine veya birbirinden ayrılmasına ihtiyaç duyulur. Bu ise işlemlere onay verilmesine, bunların gerçekleştirilmesine ve kaydedilmesine, gözden geçirilmesine ve söz konusu varlıkların yönetilmesine dönük sorumlulukları kapsar. Bir işlemin ya da bir olayın bütün önemli boyutlarını tek bir kişi kontrol etmemelidir.

İşlemlerin ve İşlerin Gerektiği Şekilde İcrası

İşlemler ve diğer önemli işler yalnızca bunlara yetkili kişilerce onaylanmalı ve icra edilmelidir. Satın almaya, transfere, kullanıma yönelik geçerli işlemlere başlandığı veya tahsis edilen kaynakların veya diğer işlerin harekete geçirildiği konusunda güvence sağlamanın esas yolu budur. Yetkilendirmeler yöneticilere ve çalışanlara açık bir biçimde duyurulmalıdır.

İşlemlerin ve İşlerin Eksiksiz ve Vaktinde Kaydedilmesi

Faaliyetlerin kontrol edilmesi ve kararların alınması sırasında yönetim nezdinde ilgisini ve önemini sürdürmesi bakımından işlemlerin doğru şekilde kaydedilmesi gerekir. Söz konusu kaydetme faaliyeti, hesap özetlerinin nihaî sınıflaması aracılığıyla, bir işlemin veya işin başlangıcından ve onaylanmasından o işlemin veya işin tamamlanmasına kadar bütün süreç veya süre boyunca uygulanır. Kontrol faaliyetleri bütün işlemlerin tam ve doğru biçimde kayıt altına alındığından emin olunmasına da yardımcı olur.

Kaynaklara ve Kayıtlara Erişim Sınırlandırmaları ve Bunlarla İlgili Hesap verme Sorumluluğu

Kaynaklara ve kayıtlara erişim yetkili kişilerle sınırlandırılmalı, gözetime ve kullanıma yönelik olarak bu kişilere hesap verme sorumluluğu tevdi edilmeli ve bu görev sürdürülmelidir. Kaydedilenlerle kaynakların periyodik olarak mukayesesine yönelik hesap verme sorumluluğu hataların, yolsuzluğun, suiistimal riskinin veya yetkisiz görev değişikliğinin en aza indirilmesine yardımcı olmalıdır.

İşlemlerin ve İç Kontrolün Uygun Biçimde Dokümante Edilmesi

İç kontrolün, diğer işlemlerin ve başka önemli işlerin açık biçimde dokümante edilmesi gerekir; incelemelerde kolayca belgelere ulaşılmalıdır. Dokümantasyon yönetimin direktiflerinde, idarî politikalarda veya çalışma rehberlerinde açık ve net biçimde görünmeli; hem kağıt üstünde hem de elektronik ortamda tutulabilmelidir. Belgelerin ve kayıtların tümü doğru biçimde yönetilip muhafaza edilmelidir.

Bu örnekler sadece, faydalı olabilecek, çok çeşitli ve değişik kontrol faaliyetlerinin kurum yöneticilerine gösterilmesi anlamına gelir. Bu örnekler herşeyi kapsamaz ve bir kurumun ihtiyaç duyabileceği özel kontrol faaliyetlerini içermeyebilir.

Ayrıca bir kurumun iç kontrolü, o kurumun spesifik ihtiyaçlarını karşılamak bakımından kontrol faaliyetlerinin tasarlanmasına olanak sağlayan esneklikte olmalıdır. Belirli bir kurum tarafından kullanılan spesifik kontrol faaliyetleri çok sayıda faktöre bağlı olarak başka kuruluşlar tarafından kullanılanlardan farklı olabilir. Bu faktörler arasında kurumların karşılaştığı spesifik tehlikeler ve maruz kaldıkları riskler, amaçlardaki farklılıklar; yönetsel kararlar, organizasyonun büyüklüğü ve karmaşıklığı, faaliyetlere ilişkin çevre koşulları, verilerin gizliliği ve önemi ile sistemin güvenilirliğine, yararlılığına ve performansına yönelik gereklilikler sayılabilir.

Bilişim Sistemlerine Yönelik Spesifik Kontrol Faaliyetleri

·Genel Kontrol
·Uygulama Kontrolü

Bilişim sistemlerine özgü kontrol iki ana başlık altında toplanmaktadır: Genel kontrol ve uygulama kontrolü. Genel kontroldan bütün bilişim sistemlerinde -ana bilgisayar, kişisel bilgisayar, ağ sistemi ve nihai kullanıcılı ortamlarda- yararlanılır. Uygulama kontrolü ise uygulama yazılımı içindeki veri işlemesini kapsayacak şekilde tasarlanır.

Genel Kontrol

Bu tür kontrol kurum ölçekli güvenlik programının planlamasını, yönetimini, merkezi veri işlemleri aracılığıyla kontrolünü, sistem yazılımının teminini ve muhafazasını, güvenlik erişimini ve uygulama sistemi oluşturup bunu sürdürmeyi kapsar.

Özellikle de;

- Veri merkezi ve müşteri-sunucu faaliyetlerine yönelik kontrol; yedekleme ve veri kurtarma (recovery) prosedürleri ile iş devamlılığının sürdürülmesini ve afet planlamasını kapsar. Veri merkezinin faaliyetlerine yönelik kontroller, ayrıca, iş-düzenini (job-setup) ve veri operatörünün faaliyetleri üzerindeki prosedürlerin ve kontrollerın tasarlanmasını da içerir.

- Sistem yazılım kontrolü şu hususları kapsar: veri işleme sistemi, veri tabanı yönetim sistemleri, telekomünikasyon, güvenlik yazılımı ve ortak programlar dahil olmak üzere bütün sistem yazılımlarının temini, uygulaması ve muhafazası üzerindeki kontroller.

- Sistemleri ve ağ sistemini "bilgisayar-korsanların (hackers) ve diğer saldırganların (trespassers) yetkisiz erişiminden ve uygunsuz kullanımdan veya personelin amaca aykırı kullanımlarından erişim güvenlik kontrolü korur. Spesifik kontrol faaliyetlerine şu hususlar dahildir: Bağlantı numaralarının değişme sıklığı, geri-çağırma (dial-back) erişiminden yararlanma, kullanıcıların yalnızca ihtiyaç duydukları sistem fonksiyonlarına ulaşmalarına olanak veren sınırlamalar, kurum dışındaki kişilerin varlıklara, bilgisayarlara ve ağ sistemlerine erişimini engelleyen "güvenlik kalkanı" (firewalls) yazılımı ve donanımı, şifre değişim sıklığı ile kurumda daha önce çalışanlarca kullanılan şifrelerin iptal edilmesi.

- Uygulama sistemi oluşturma ve bunu sürdürmeye yönelik kontroller; yeni

sistemlerin güvenli biçimde oluşturulmasına ve mevcut sistemlerde değişiklik yapılmasına dönük bir düzen sağlar. Bu kontrollera şu konular dahildir: dokümantasyon düzeninin gereksinimleri, yürütülen projeler için yetkilendirmeler, incelemeler, testler ve faaliyetin sistemler içine yerleştirilmesinden önce hazırlık ve değişiklik faaliyetlerinin onaylanması. Kurum içindeki alternatif bir hazırlık faaliyeti ticari yazılımın satın alınması olabilir; yine de, seçilen yazılımın kullanıcı ihtiyaçlarını karşılamasını ve bunun faaliyet içine düzgün olarak yerleştirilmesini sağlamak üzere kontrol gereklidir.

Uygulama Kontrolleri

Bu kategorideki kontrolleri eksiksizliği, doğruluğu, yetkilendirmeyi ve bütün işlemlerin uygulama işlemi boyunca geçerliliğini sağlayabilmek üzere tasarlanır. Kontrolleri bütün girdilerin elde edilmesini ve geçerli olmasını, çıktıların doğru ve uygun biçimde dağılmasını sağlayacak şekilde uygulamanın diğer sistemlerle bağlantılı olan ara yüzlerine yerleştirilir. Verinin biçimini, mevcudiyetini ve uygunluğunu gözden geçiren bir sisteme bilgisayar imlâ kontrollerinin yerleştirilmesi buna örnek olarak gösterilebilir.

Bilgisayar sistemleri üzerindeki genel ve uygulamaya dönük kontroller birbirleriyle bağlantılıdır. Genel kontrol uygulama kontrolünün çalışmasını destekler; eksiksiz ve doğru bilgi işlemenin sağlanması için iki tür kontrole da ihtiyaç duyulmaktadır. Genel kontrolün yetersiz olması durumunda uygulama kontrolü muhtemelen düzgün çalışmaz ve göz ardı edilebilir.

Bilişim teknolojisindeki hızlı değişiklikler dolayısıyla, etkinliklerinin sürdürülmesi bakımından kontrollerin geliştirilmeleri gerekmektedir. Teknolojideki değişiklikler ve bunun elektronik ticaret alanına uygulanması ve Internet uygulamalarının yaygınlaşması yararlanılabilen ve uygulanması gereken spesifik kontrol faaliyetlerini değiştirmekteyse de, kontrole duyulan temel gereksinimler önemini korumaktadır. Nihai kullanıcıların eline daha güçlü bilgisayarlar geçtikçe veri işleme sorumluluğu için ihtiyaç duyulan kontroller da tanımlanıp uygulamaya konulacaktır.

Bilgi ve İletişimler

Bilgi kaydedilmeli, yönetime ve kuruluş bünyesinde ona ihtiyaç duyanlara kendi iç kontrollermı ve diğer sorumluluklarını yerine getirebilecekleri bir formatta ve zaman dilimi içinde iletilmelidir.

Bir kurumun, çalışması ve faaliyetlerini kontrol etmesi bakımından kurum içi işler kadar kurum dışı işlerle ilgili olarak amaca uygun, güvenilir ve vaktinde iletişimlere sahip olması gerekir. Amaçlarının tümünü başarması için kurum genelinde bilgiye ihtiyaç duyulur.

Program yöneticileri, kurumlarının stratejik ve yıllık performans planlarının gerçekleşip gerçekleşmediğini ve kaynaklarının etkin ve verimli kullanılmasına yönelik hesap verme sorumluluğu amaçlarının karşılanıp karşılanmadığını tespit etmek bakımından hem finansal hem de faaliyetlerle ilgili olan verilere ihtiyaç duyarlar. Örneğin; işlenmiş bilgi finansal raporların hazırlanmasını gerektirir. Bu ise satın almalar, finansal yardımlar, sabit varlıklar ve stoklar hakkındaki verilere dayalı diğer işlemler ile tahsilatlardan elde edilen bir dizi geniş veriyi kapsar. İşlenmiş bilgi, kurumun çeşitli yasalar ve mevzuat uyarınca hukuka uygun davranıp davranmadığının tespit edilmesini de gerektirir. Finansal bilgiye hem kurum içinde hem de dışında ihtiyaç duyulur. Faaliyetler hakkında karar vermek, performansı izlemek ve kaynakları tahsis etmek bakımından dışa dönük olarak düzenli biçimde rapor ve günlük bazda finansal tablo hazırlamak gerekir. Kalıcı nitelikteki bilgi tanımlanmalı, bu bilgi muhafaza edilmeli ve kişilerin görevlerini etkin olarak yapabilmelerine imkan verecek biçimde ve zaman dilimi içinde duyurulmalıdır.

Etkin iletişim, en geniş anlamıyla, bilginin örgüt içinde aşağıya, yukarıya ve yatay olarak akışıyla meydana gelir. Ayrıca kurum içi iletişimler bakımından yönetim, kurumun amaçlarına ulaşmasında önemli etkiye sahip paydaşlarla iletişim kurmaya ve onlardan bilgi edinmeye dönük elverişli araçlar bulunduğunu garanti etmelidir. Dahası, etkin bilgi teknolojisi yönetimi yararlı ve güvenilir olana ulaşılması, kayıtların süreklilik temelinde yapılması ve bilginin iletilmesi bakımlarından yaşamsal önemdedir.

İzleme

İç kontrol izlemesi; performansın belli bir zaman içindeki kalitesini değerlendirmeli ve denetimlerin ya da diğer incelemelerin bulgularının derhal çözüme bağlanmasını güvence altına almalıdır.

İç kontrol, genellikle, normal faaliyetlerin akışı içinde sürekli izleme yapılmasını güvence altına almak üzere tasarlanır. İzleme süreklilik temelinde gerçekleştirilir ve kurum faaliyetlerinin ayrılmaz bir parçasıdır. Düzenli yönetimi ve faaliyetlerin gözetimini, karşılaştırmaları, uzlaşmaları ve kişilerin görevlerini yerine getirirken almış oldukları diğer önlemleri kapsar.

Belirli zamanlarda kontrollerın etkinliği üzerine yoğunlaşmak suretiyle ayrı ayrı kontrol değerlendirmeleri yapılması da yararlı olabilir. Tekil kontrol değerlendirmelerinin kapsamı ve sıklığı öncelikle, risk değerlendirmesine ve süregelen izleme prosedürlerinin etkinliğine bağlıdır. Tekil değerlendirmeler kontrol tasarımını gözden geçirme ve iç kontrolün doğrudan test edilmesi kadar öz-değerlendirme anket formunu da dikkate alabilir. Tekil değerlendirmeler, ayrıca, Kurumun Teftiş Kurulu veya bir dış denetçi tarafından yürütülebilir. Sürekli izleme sırasında veya tekil değerlendirmeler aracılığıyla tespit edilen yetersizlikler ve eksiklikler o işten sorumlu olan kişiye ve o kişinin en azından hemen bir üst yönetim kademesine de bildirilmelidir. Önemli sorunlar üst yönetime duyurulmalıdır.

Denetimlerin ve diğer incelemelerin bulgularının gerektiği şekilde çözüme kavuşturulmasına yönelik politikalar ve prosedürler iç kontrolün izlenmesi meselesinin içinde yer alır. Yöneticiler;

(1) Denetimlerden ve başka incelemelerden elde edilen bulguları doğru biçimde değerlendirmeli, -ki söz konusu bulgular arasında denetçiler ve kurum faaliyetlerini değerlendirenler tarafından gösterilen eksiklikler ve tavsiyeler de bulunur.

(2) Denetimlerden ve incelemelerden elde edilen bulgulara ve bunlar aracılığıyla yapılan tavsiyelere cevaben alınacak gerekli önlemleri tespit etmeli,

(3) Kendisine sunulan düzeltici önlemlerin veya başka bir şekilde çözüm aranan meselelerin tümünü belirlenen bir takvim içinde tamamlamalıdır.

Denetim veya diğer inceleme sonuçları yönetime bildirildiğinde çözüm süreci başlar ve bu süreç ancak;

(1) tespit edilen yetersizlikleri düzelten,
(2) iyileşmeler sağlayan,
(3) yönetimin tedbir almasını gerektirmeyen bulguları ve tavsiyeleri sergileyen,

adımlar atıldıktan sonra tamamlanır.

Kamu Sektörü İç Kontrol Standartları Rehberi
Kurum Risk Yönetimi Hakkında Tamamlayıcı Ek Bilgiler

Çev.Sacit YÖRÜKLER

Sayıştay Uzman Denetçisi

Önsöz

1992 tarihli INTOSAI İç Kontrol Standartları Rehberi iç kontrolün planlanmasının, uygulanmasının ve değerlendirilmesinin teşvik edilmesi gerektiği düşüncesini yansıtan canlı bir doküman olarak tasarlanmıştı. Bu düşünce rehberi sürekli güncel tutma çabasını gerekli kılmaktadır.

17'nci INTOSAI Kongresi (Seoul, 2001) 1992 tarihli rehberin artan güncellenme ihtiyacını saptamış ve Treadway Komisyonu Sponsor Organizasyonlar Komitesi (COSO) iç kontrol bütünleşik çerçevesinden bir model olarak yararlanmada mutabakatını belirtmiştir. Sonradan, güncellenmiş rehber etik değerleri ve bilgi işlenmesine ilişkin kontrol aktivitelerinin genel prensiplerini içerecek şekilde genişletilmiştir.

Güncellenmiş İç Kontrol Rehberi 2004 yılında yayımlanmıştır. Bu rehber de zaman içinde yeni gelişmelerin etkisini, örneğin COSO İşletme Risk Yönetim çerçevesini1 içerecek şekilde geliştirilecek ve rafine edilecek yaşayan bir doküman olarak görülmelidir. Dolayısıyla, Rehbere yapılan iş bu ekleme, COSO İşletme Risk Yönetim Modelinde belirtildiği gibi, risk yönetimi alanındaki güncel gelişmeleri yansıtmayı amaçlamaktadır. Bu doküman esas itibariyle kamu kesimindeki okurlara seslendiği için daha çok özel sektör bağlantısına sahip "işletme" (enterprise) terimi yerine "kurum" (entity) terimi kullanmıştır.

Burada sağlanan ek bilgiler INTOSAI İç Kontrol Standartları Alt Komitesi üyelerinin ortak çabalarının ürünüdür. Bu güncelleme, Fransa, Macaristan Bengaldeş, Litvanya, Hollanda, Oman, Ukrayna, Romanya, Birleşik Krallık, Amerika Birleşik Devletleri ve Belçika (Başkan) Sayıştaylarının temsilcileri arasından oluşturulan bir çalışma grubu tarafından koordine edilmiştir.

Franki VANSTAPEL *Belçika Sayıştayı*
Birinci Başkanı INTOSAI İç Kontrol
Standartları Alt Komitesi Başkanı

Giriş

COSO Kurum Risk Yönetimi temel varsayımına göre, her kurum paydaşlarına değer katmak için vardır. Kamu sektöründe, kamu görevlileri dürüstlük içinde kamu yararına hizmet etmeli ve kamu kaynaklarını doğru şekilde yönetmelidirler. Uygulamada paydaşlar, vatandaşlar ve onların seçilmiş temsilcileridir.

Bütün kurumlar belirsizlikle karşı karşıyadır. Yönetim bakımından temel zorluk, paydaşlara en fazla değeri sağlamaya çalışırken ne miktarda belirsizliğin kabul edileceğini belirlemektir. Ayrıca belirtmek gerekir ki, belirsizlik hem risk hem de fırsat kaynağıdır ve değeri aşındırma veya güçlendirme veyahut kamu sektörü terimiyle kamu yararına daha çok veya daha az hizmet etme potansiyeline sahiptir. Risk yönetiminin amacı, yönetime belirsizlikle ve bununla bağlantılı risklerle ve fırsatlarla etkili şekilde ilgilenme imkânı vermek, değer yaratma kapasitesini güçlendirmek, daha etkili hizmetleri eşitlik ve adalet gibi değerleri dikkate alarak daha verimli ve daha ekonomik şekilde sunmaktır.

INTOSAI Kamu Sektörü İç Kontrol Standartları Rehberi iç kontrolü bir kurumun amaçlarını gerçekleştirmesine imkân veren genel kapsamlı kavramsal bir çerçeve olarak görmektedir. COSO Kurum Risk Yönetim modeli ve benzeri diğer modeller daha uzağa gitmekte ve kurumun potansiyel riskleri ve fırsatları belirlemek suretiyle, amaçlarını netleştirerek ve riskleri en aza indirmek ve fırsatları en üste çıkarmak amacıyla iç kontrolleri oluşturarak yönetilebileceğini ileri sürmektedir.

Kurum risk yönetimi yalnızca kurumsal yönetişim rejiminin kavradığı fonksiyonların tanımını genişletmemekte, ama aynı zamanda organizasyonların amaçlarını gerçekleştirmeyi düşünme tarzında bir değişikliği gerekli kılmaktadır. Bu nedenle etkili olmak için kurum risk yönetimi, strateji belirlenmesinde dikkate alınan, organizasyonun her kademesinde ve her biriminde uygulamaya konan ve organizasyonun amaçlarını gerçekleştirme kapasitesini etkileyebilecek bütün olayları belirlemeyi hedefeyen sürekli bir prosestir.

Bu doküman kamu sektöründe kurum risk yönetiminin uygulanması için tavsiye edilen bir çerçevenin ana hatlarını çizmekte ve kendisine kıyasen kurum risk yönetiminin değerlendirilebilmesi amacıyla bir temel sağlamaktadır. Ancak, doküman Kamu Sektörü İç Kontrol Standartları Rehberinin yerine geçmeyi veya onun yerini doldurmayı amaçlamamakta; ama üye devletlerin uygun gördüğü hallerde bu standartların yanı sıra yararlanabilecekleri tamamlayıcı ek bilgiler sağlamayı hedefemektedir. Ayrıca, iş bu doküman, yetkili makamların organizasyon bünyesinde mevzuat hazırlama, kural koyma veya siyasa belirleme yetkilerini sınırlamayı veya bu yetkilere müdahaleyi öngörmemektedir.

Sonuç olarak, açıkça belirtmek gerekir ki, bu dokümanın amacı kurumsal yönetişim standartları hakkında ilave yönlendirici ilkeler sunmaktır. Bu yönlendirici ilkeler bir en iyi kurumsal yönetişim rejimi pratiğinin uygulamaya geçirilmesi için detaylı siyasalar, prosedürler ve pratikler getirmediği gibi, bütün hukukî ortamlarda bütün organizasyonlar bakımından uygun değildir. Ne var ki, bu ek kurumların paydaşlara sağlanan hizmetleri en üst düzeye çıkarmalarına yardımcı olacak sistemleri geliştirebilecekleri bir genel çerçeve sağlamaktadır.

Bu dokümanın yapılanması nasıldır?

Bu ekin yapısı INTOSAI Kamu Sektörü İç Kontrol Standartları Rehberininkine benzerdir. Birinci bölümde kurum risk yönetimi tanımlanmakta ve kapsamı resmedilmektedir. İkinci bölümde kurum risk yönetiminin öğeleri sunulmakta ve iç kontrol standartlarına ekler vurgulanmaktadır.

1. Bölüm

Kurum Risk Yönetiminin Tasviri

1.1 Tanım

1.1.1 COSO'nun “Kurum Risk Yönetimi: Bütünleşik Çerçeve” modeline göre, kurum risk yönetimi değer

yaratmayı ve değer korumayı etkileyen riskleri ve fırsatları ele alıp işlemekte ve şu şekilde tanımlanmaktadır: "Kurum risk yönetimi; yönetim kurulu, yöneticiler ve diğer personel tarafından uygulamaya geçirilen; strateji hazırlanmasında ve organizasyonun bütün aktivitelerinde dikkate alınan; kurumu etkileyebilecek potansiyel olayları belirlemek ve risk iştahı sınırları içinde riskleri yönetmek için tasarlanan ve organizasyonun amaçlarına ulaşma konusunda makul güvence sağlayan bir prosestir" (COSO KRY modeli 2004)

1.1.2. Kamu sektöründe "değer yaratma" ve "değer koruma" terimleri özel sektördeki gibi doğrudan doğruya ilgili olma özelliğine sahip değildir. Ancak, bu tanım, olabildiği kadar çok sektörü ve organizasyon türünü kapsamak amacıyla bilerek geniş tutulmuştur. Aslında tanımın kamu sektörü kurumlarına bütünüyle uygulanabilmesi için, "değer yaratma" ve "değer koruma" terimlerini "hizmet yaratma" "hizmet sürdürme" terimleri ile değiştirmek mümkündür.

1.2 Misyonun Belirlenmesi

1.2.1 Kurum risk yönetimi için hareket noktası kurum tarafından belirlenen misyon veya vizyondur. Bu misyon çerçevesinde yönetim stratejik amaçları saptamalı, bu amaçları gerçekleştirecek stratejileri seçmeli ve bütün organizasyon kademelerine yayılan ikincil amaçları belirlemelidir.

1.3 Amaçların Saptanması

1.3.1 INTOSAI İç Kontrol Standartları Rehberine göre, amaçlar aşağıdaki dört kategoride (amaçların çoğu birden fazla kategoriye giriyor olsa da) sınıflandırılabilir.

- **Stratejik-** organizasyonun misyonuna hizmet eden amaçlar
- **Operasyonel-** operasyonların düzenli, etik, ekonomik, verimli ve etkili şekilde uygulanması ve kaynakların kayıplara, kötüye kullanımlara ve hasarlara karşı korunması ile ilgili amaçlar.
- **Raporlama-** hesap verme sorumluluğu ile ilgili yükümlülüklerin yerine getirilmesi dâhil olmak üzere raporlamanın güvenilirliğine ilişkin amaçlar
- **Uygunluk-** yürürlükteki yasalara ve yönetmeliklere uygunlukla ilgili ve hükümet siyasalarına uygun davranma kapasitesi ile ilişkili amaçlar

5. İlk iki kategorideki amaçlar tamamıyla kurumun kontrolünde değildir. Bu nedenle, risk yönetim sistemi, bu risklerin tatmin edici bir şekilde yönetildiği hakkında ancak makul güvence sağlayabilirse de yönetime bu amaçların ne ölçüde zamanında karşılanacağının farkında olma imkânını vermelidir. Buna karşılık, raporlamanın güvenilirliği ve uygunluk ile ilgili amaçlar kurumun kontrolü içindedir ve dolayısıyla etkili risk yönetimi, genellikle, bu amaçların karşılanmakta olduğu konusunda yönetime güvence verecektir.

1.4 Hadiselerin- Risklerin ve Fırsatların Belirlenmesi

1.4.1 Amaçların saptanmasının hemen ardından organizasyonun kurum risk yönetimi çerçevesinde, bu amaçların gerçekleşmesi üzerinde etkide bulunabilecek hadiseleri (events) belirlemesi gerekir. Hadiseler olumsuz ya da olumlu bir etki doğurabileceği gibi her iki yönden etki yaratabilir. Olumsuz etki doğuran hadiseler kurumun amaçlarını gerçekleştirme kapasitesini engelleyebilen risklerdir. Bu riskler içsel ve dışsal etkenlerden kaynaklanabilir. Aşağıdaki 1 no'lu şema kamu kurumlarının karşı-laştığı risklerden pek çoğunu

göstermekte ise de, belirli kurumları ilgilendiren başka riskler de söz konusu olabilir.

1.4.2 Olumlu etki doğuran hadiseler olumsuz etkileri telafi edebilir veya fırsatlar oluşturabilir. Fırsatlar; meydana gelecek hadisenin kurumun amaçlarını gerçekleştirme kapasitesini artırma veyahut kuruma amaçlara daha verimli ulaşma imkânı verme olasılığıdır. Yönetim sadece riskleri en aza indirmeyi araştırmakla kalmamalı, fırsatları kavrayan planlar hazırlamalıdır.

1.5 İletişim ve Öğrenme

1.5.1 Bir kurumun risk yönetiminin "arzulanan etkiye sahip" olup olmadığının belirlenmesi sürecinin çok önemli bir öğesidir. Yönetimin, kurum risk yönetiminin öğelerinin uygulamaya konulup konulmadığını ve etkili şekilde işleyip işlemediğini, yani önemli yetersizlikler bulunup bulunmadığını ve bütün risklerin, kurum risk iştahı sınırları içinde kabul edilebilir parametrelere indirilip indirilmediğini değerlendirmesi gerekir. Kurum risk yönetiminin arzulanan etkiye sahip yönetim olduğu ahvalde, kurum yönetimi, dört kategorideki amaçların misyona ne ölçüde uygun düştüğünü ve amaçlara ne derecede ulaşıldığını anlayacaktır. Bütün kurumda dikine ve enine etkili bir iletişim bu süreci kolaylaştırmak için elzemdir.

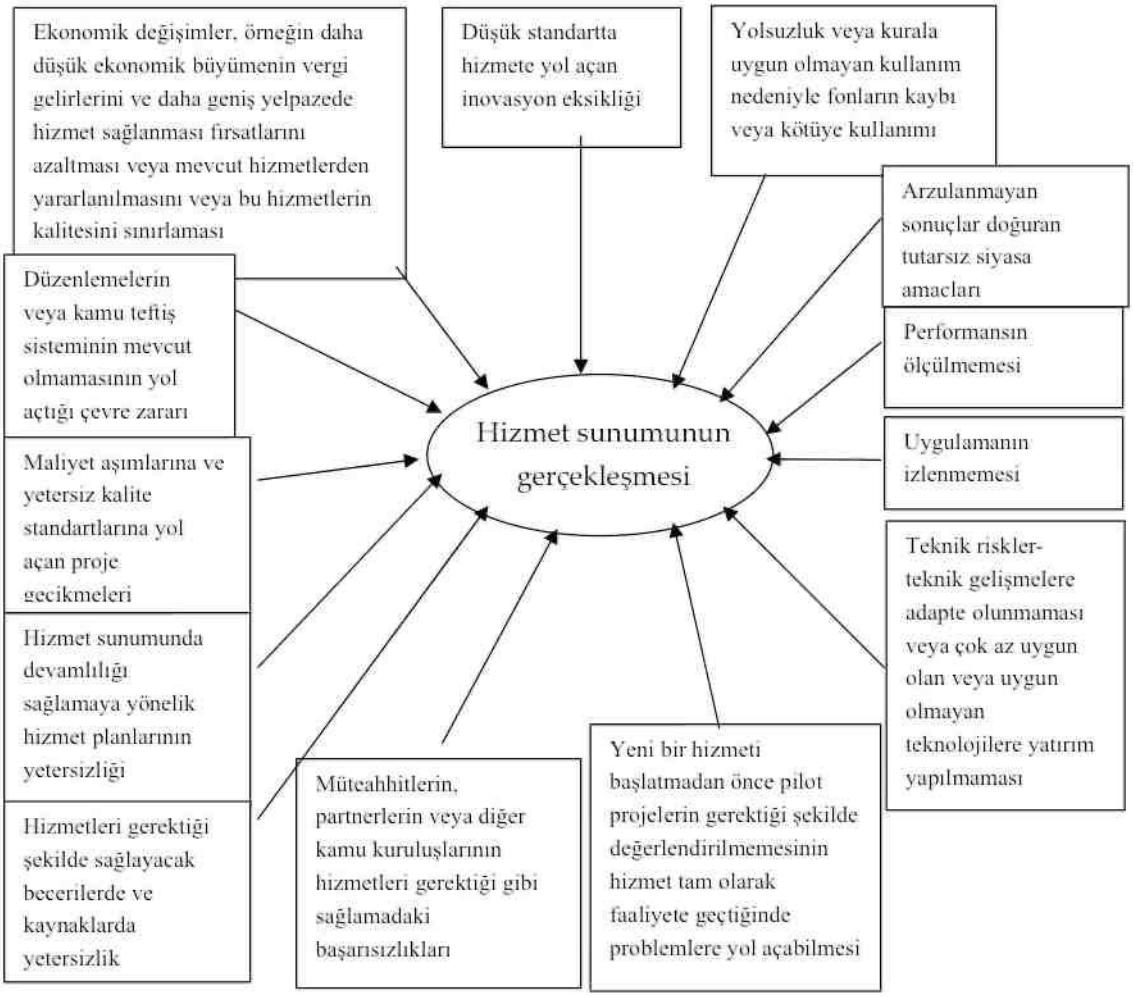
1.6 Sınırlamalar

1.6.1 Sistem ne kadar iyi tasarlanıp işlerse işlesin kurum risk yönetimi yöneticilere genel amaçlara ulaşıldığı hakkında mutlak güvence sağlayamaz. Bu nedenle iş bu doküman ancak makul bir güvence düzeyine ulaşılabileceğini kabul etmektedir.

1.6.2 Makul güvence; amaçlara ulaşılması veyahut amaçlara ulaşılması olası değilse yönetimin zamanında bilgi sahibi olması hakkında tatmin edici bir güven düzeyine tekabül etmektedir. Tatmin edici güven düzeyine erişmek için ne kadar güvence gerektiğinin belirlenmesi bir değer hükmü meselesidir. Bu değer hükmünü verirken yöneticilerin kurumun risk iştahını ve amaçlara ulaşılma üzerinde etkisi olabilecek hadiseleri değerlendirmeleri gerekir.

1.6.3 Makul güvence; belirsizliğin ve riskin gelecekle ilgili olduğu, bunu da kimsenin kesinlikle tahmin edemeyeceği düşüncesini yansıtmaktadır. Ayrıca, kurumun kontrolü veya etkisi dışındaki faktörler, örneğin siyasi faktörler, amaçlara ulaşma üzerinde etkide bulunabilir. Kamu sektöründe kurumun kontrolü dışındaki faktörler çok kısa sürede temel amaçları bile değiştirebilir. Diğer sınırlamalar şu gerçeklerin sonucu olabilir: karar alırken verilen değer hükmünün hatalı olması, aksaklıkların beşerî kusurlar örneğin hatalar veya yanılmalar nedeniyle vuku bulması, risklere karşı alınan kararların ve belirlenen kontrollerin maliyetleri ve faydaları dikkate alma zorunluluğu, iki veya daha fazla kişinin hileli anlaşması yoluyla kontrollerden sıyrılınması ve üst yöneticilerin iç kontrol sistemini umursamaması. Bu sınırlamalar yönetimin amaçlara ulaşma konusunda mutlak güvence elde etmesini engellemektedir. 1 no'lu şemada karşılaşılabilecek tipik risklerden bazıları gösterilmektedir. Şema açıklayıcı olmayı amaç edinmiş olup sınırlayıcı değildir.

Şema1: Kamu Kurumlarının Karşılaştıkları Bazı Tipik Riskler



1.7 İç kontrol ile Kurum Risk Yönetimi Arasındaki İlişki

1.7.1 Pek çok bakımdan kurum risk yönetimi iç kontrol modelinin doğal bir evrimi olarak görülebilir. Organizasyonların çoğu kurum risk yönetimiyle bütünleşik konseptleri uygulamaya koymadan önce iç kontrol modelini eksiksiz olarak uygulamaya yönelmektedirler. İç kontrol, kurum risk yönetiminin

bütünleşik bir parçasıdır. Kurum risk yönetimi modeli iç kontrolü kapsamakla kalmaz, kurum işletim kararlarının nasıl ana misyondan ve bağlantılı amaçlardan akıp geldiği hakkında daha sağlam bir kavramlaştırma oluşturur ve belirli hadise karşısındaki doğru cevabın ne olması gerektiğini belirlemede yönetime yardımcı olacak bir araç sağlar. Kurum Risk Yönetim Modeli, özellikle aşağıda belirtilen alanlarda, INTOSAI İç Kontrol Rehberinden daha ileri gider:

- Amaç kategorileri daha geniştir ve ayrıca daha eksiksiz raporlamayı, finansal olmayan bilgileri, stratejik amaçları içerir;

- Risk değerlendirme öğesini kapsar ve risk iştahı, risk toleransı, risk cevabı gibi değişik risk konseptlerini ortaya getirir; Yönetim kurulunda bağımsız yöneticilerin önemine vurgu yapar ve onların rollerini ve sorumluluklarını ayrıntıları ile açıklar.

2. Bölüm

Kurum Risk Yönetiminin Öğeleri

Kurum risk yönetimi birbiriyle karşılıklı ilişkili sekiz öğeden oluşmaktadır. Bu öğeler organizasyonun yönetilme biçiminden kaynaklanmakta olup yönetim süreciyle bütünleşmişlerdir. Bu öğeler şunlardır:

- Kontrol ortamı,
- Amaç belirlenmesi,
- Hadiselerin (event) tanımlaması,
- Risklerin değerlendirilmesi,
- Risk cevabı,
- Kontrol faaliyetleri,
- Bilgi ve iletişim,
- İzleme.

Risk yönetiminin öğelerini uygularken kurum, organizasyonun tüm kademelerindeki faaliyetlerinin bütününü dikkate almalıdır. Yönetim, ayrıca, risk yönetim modelini uygularken yeni projeleri ve girişimleri incelemelidir.

Risk Yönetiminin Kurumun Bütününe Uygulanması

Yönetimin bütünsel bir risk yaklaşımına sahip olması gerekir. Pratikte bütün yönetim kademeleri, kendi faaliyet alanlarını etkileyebilecek hadiseleri değerlendirmeli ve bu konuda üst düzey yöneticileri bilgilendirmelidirler. Bu değerlendirme nitel ya da nicel olabilir. Üst yönetim, organizasyon bütününde global bir risk değerlendirmesi oluşturmak amacıyla kurumun bütün faaliyet kademelerini ve alanlarını kapsayan bu değerlendirmelerden yararlanmalıdır.

İnsanın Önemi

Kurum risk yönetimi yönetim ve diğer personel tarafından uygulamaya konulur ve etkili şekilde işletilir. Kurum risk yönetimi organizasyon bünyesindeki bireylerin yaptıklarıyla ve söylediklerileriyle gerçekleşir.

Benzer şekilde, kurum risk yönetimi bireylerin eylemlerini etkiler. Her çalışan, farklı ustalıklara ve farklı anlama yetilerine sahip bir bireydir. Kurum risk yönetimi, personele kurumun amaçları bağlamında riskleri kavrama imkânı verecek mekanizmaları yaratmaya yönelir.

Personelin sorumluluklarını ve yetki sınırlarını bilmeleri gerekir. Bu nedenle, kişinin görevleri ile bu görevleri yerine getirme tarzı arasında açık ve doğrudan bir ilişki bulunmalıdır. Üst düzey yönetim esas itibariyle gözetimle yükümlüdür. Böyle olmakla birlikte, üst düzey yöneticiler, ayrıca, gidilecek yönü belirler, stratejileri, belirli işlemleri ve siyasaları onaylar ve dolayısıyla organizasyon kültürüne uyulmasını sağlamada yaşamsal bir rol oynar.

2.1 Risk Ortamı/Bağlamı

2.1.1 Risk ortamı/bağlamı, organizasyondaki bütün bireylerin risk bilincini etkilediği için organizasyonunun kültürünü yansıtır ve bir disiplin ve yapı getirmek suretiyle kurum risk yönetiminin diğer bütün öğeleri için bir temel oluşturur. Kurumun risk yönetim felsefesi, risk iştahı, yönetim kurulunca yapılan gözetim, dürüstlük ve etik değerler, personelin uzmanlıkları ve yönetimin yetkileri ve sorumlulukları dağıtma ve personeli organize etme ve geliştirme tarzı iç ortam faktörleri arasındadır.

2.1.2 Bir kurumun risk yönetim felsefesi, kurumun strateji saptamasından günlük operasyonel aktivitelere kadarki her şeyde riski nasıl değerlendirdiğini belirleyen ortak inançlar ve tutumlar setidir. Risk yönetim felsefesi; kültür ve faaliyet tarzı ve özellikle risklerin nasıl belirlendiği, kabul edilen risklerin türü ve risklerin nasıl yönetildiği üzerinde etki yapar. Bir kurumun risk yönetim felsefesi siyasa bildirimlerinde, paydaşlara ve personele yönelik sözlü ve yazılı iletimlerde ve alınan kararlarda belli edilmelidir. İletim yöntemi ne olursa olsun, üst yönetimin sadece iletim siyasaları yoluyla değil, ama aynı zamanda gündelik eylemleri aracılığıyla felsefeyi güçlendirmesi son derecede önemlidir.

2.1.3 Risk iştahı, bir kurumun amaçlarına ulaşmak için kabul etmeye hazır olduğu risk düzeyine tekabül etmektedir. Risk iştahı, risk yönetim felsefesini yansıtır; kurumun kültürünü ve faaliyet tarzını etkiler. Risk iştahı nicel veya nitel olarak tahmin edilebilir. Risk iştahı strateji belirlemede dikkate alınmalıdır ki, bu durumda bir stratejinin tahmin edilen yararı ile risk iştahı yani riski kabul veya tolere etme arasında bir paralellik bulunmalıdır.

2.1.4 Öte yandan, risk ortamının kimliğini saptarken ve uygun risk iştahını seçerken kamu sektöründeki kurumların "genişletilmiş kurum" kavramını dikkate almaları gerekir. Diğer kamu organları veya yasama organları söz konusu olsun sponsorluk yapan veya sponsorluk edilen kuruluşların görüşleri ve beklentileri ve partner konumundaki kuruluşların düşünceleri uygun risk yönetme felsefesi ve risk iştahı konusunda doğrultuyu net bir şekilde gösterebilir.

2.1.5 Bir kurumun üst yönetimi iç ortamın yaşamsal bir parçasıdır ve iç ortamın öğelerini önemli derecede etkiler. Organizasyon kültürünün "üst yönetimin anlayışı" tarafından belirlendiği veya tersine altının oyulduğu malumun ilâmıdır. Üst yönetimin icra yönetiminden bağımsızlığı, üyelerinin deneyimi ve çapı, müdahil olma ve denetleme dereceleri ve faaliyetlerinin isabetliliği gibi hususlar bir rol oynar. Üst icra yönetiminin üyeleri üst yönetimin parçası olabilirse de, iç ortamın etkili olmasını sağlamak için üst yönetim ekibi içinde kurum dışından bağımsız birkaç üyenin bulunması uygun olur. Bunun nedeni, üst yönetimin faaliyetlerini sorgulayarak ve denetleyerek icra yönetimini hesap vermeyle yükümlü tutmaya ve alternatif görüşler sunmaya hazır olması gerektiğidir.

2.1.6 Yönetimin dürüstlüğü ve etik değerleri stratejinin ve amaçların uygulamaya konulmasını etkiler. Kurumun iyi bir şöhrete sahip olması o kadar değerlidir ki, davranış standartlarının asgarî yasal gerekliliklere basitçe bir uymanın ötesine geçmesi gerekir. Etik davranış ve yönetimin dürüstlüğü; etik ve davranış

standartlarını ve bu standartların iletilmesini ve bunlara uyulmasını içeren kurum kültürünün yan ürünüdür. Üst yönetim kurum kültürünün belirlenmesinde kilit rol oynar. Genel misyonun gerçekleştirilmesi yerine kısa vadeli sonuçlara gereksiz önem verilmesi uygun olmayan bir iç ortamı güçlendirebilir.

2.1.7 Formel davranış kuralları önemlidir ve uygun etik anlayışın temelidir. Çalışanların yönetim kuruluna uygun bilgileri iletme imkânı veren aşağıdan yukarı iletim kanalları (veya formel ihbar prosedürleri) da önemlidir. Ne var ki, yazılı bir davranış kurallarının varlığı, bütün çalışanlar kendilerinden beklenen davranışlar hakkında bilgilendirildiklerini beyan etmiş olsalar bile, kendi başına prosedürlere uyulmasını güven altına almaz. Kuralları ihlal eden çalışanlar için yaptırımların mevcudiyeti de aynı derecede önemlidir. Üst yönetim tarafından gönderilen mesajlar çabucak kurum kültürüyle bütünleşir, öyle ki kompleks yönetim kararlarıyla karşılaşıldığında sahip olunacak "doğru tepkiler" kurum bütününe yerleşir.

2.1.8 Uzmanlık, verilen görevlerin yerine getirilmesi için ihtiyaç duyulan bilgileri ve becerileri ifade eder. Uzmanlık; uygun kişilerin işe alınmasına ve yükseltilmesine, bu kişilerin görevlere tahsislerine ve eğitilmelerine ve yetersiz performanslara çözüm bulunmasına ilişkin insan kaynakları pratikleri aracılığıyla desteklenmelidir. Yönetim, belirli görevler için spesifik uzmanlık düzeylerini belirlemeli ve bunları spesifik kadrolarla ilgili uygun görev tanımlarına dönüştürmelidir. Uzmanlık ile maliyet arasında bir denge bulunabileceğinin kabul edilmesi işin önemli bir yönüdür.

2.1.9 Bir kurumun organizasyonel yapısı kuruma faaliyetlerini planlama, uygulama, kontrol etme ve izleme imkânını sağlayan çerçeveyi verir. Organizasyonel yapı işletim ihtiyaçlarına uygun olacaktır. Bazı kurumların merkezîleştirilmiş olmasına karşılık diğerleri adem-î merkeziyetçi yapıdadır. Bazı kurumlar coğrafî mahalle göre organize edilmiş oldukları halde diğerlerinin organizasyonu fonksiyona göredir. Yapı ne olursa olsun, bir kurum, riskleri etkili olarak yönetmesine ve amaçlarına ulaşmak üzere faaliyetlerini yürütmesine imkân verecek şekilde organize edilmelidir.

2.1.10 Yetkilerin ve sorumlulukların sınırlarının çizilmesi kişilerin ve ekiplerin sorunları ele almak ve problemleri çözmek için inisiyatif kullanmada yetkili olma ve desteklenme derecesini ve yetkilerinin sınırlarını ilgilendirmektedir. Temel zorluklar bütün personelin kurumun amaçlarını anlaması,kendi eylemlerinin bu amaçların gerçekleşmesine nasıl katkıda bulunacağı ve sadece bu amaçlara ulaşma gerektirdiği ölçüde bu sorumlulukların devredilmesidir. Sorumluluk yetki kadar önemlidir. İç ortam, bireylerin hesap vermekle yükümlü olacaklarının bilincinde olma derecesinden büyük ölçüde etkilenir. Bu, icra başkanı dâhil olmak üzere bütün kademeler için geçerlidir.

2.2 Amaçların Belirlenmesi

2.2.1 Amaçlar stratejik düzeyde belirlenir ve daha alt düzeydeki operasyonlar, raporlar ve uygunluk ile ilgili amaçlar için bir temel oluşturur. Her kurum iç ve dış kaynaklı çeşitli risklerle karşılaşır ve amaçların belirlenmesi, hadiselerin etkili şekilde tanımlanmasının, risklerin değerlendirilmesinin ve risk cevabının hazırlanmasının bir ön koşuludur. Amaçlar yönetimin bu amaçların gerçekleşmesine yönelik riskleri belirleyebilmesi ve değerlendirebilmesi ve bu risklerin azaltılması için gerekli girişimlerde bulunulabilmesi amacıyla belirlenmelidir. Amaçlar, kurum risk tolerans düzeylerini saptayan kurum risk iştahına paraleldir.

2.2.2 Kurumun misyon bildirimi, kalın hatlarıyla, kurumun nelere ulaşmayı arzu ettiğini belirler. Yönetim; stratejik amaçları saptar, stratejiyi formüle eder ve tekabül eden faaliyetleri tespit eder. Stratejik amaçlar, kurumun misyonuna paralel olan ve bu misyonu destekleyen üst düzey hedeferdir. Misyonu ve ilişkili amaçları gerçekleştirmek için uygulanan strateji misyondan daha dinamiktir ve koşullardaki değişikliği yansıtmak üzere ayarlanır.

2.2.3 Kurumların amaçları çeşitlilik göstermekte ise de bazı genel kategoriler uygulanabilir. Bütün amaçlar aşağıdaki kategorilerden birisiyle veya daha fazlasıyla ilişkili olmaktadır:

- **Operasyonel amaçlar-** Bu amaçlar, performans hedeferi ve kaynakların kayıplara karşı korunması dâhil olmak üzere, kurumun faaliyetlerinin etkililiği ve verimliliği ile ilişkilidir. Hesapların kamuoyuna raporlanması bağlamında "kaynakların/varlıkların korunması" tanımı şu şekilde genişletilebilir: kamu fonlarının zimmete geçirilmesinin önlenmesi veyahut ortaya çıkarılması ve düzeltilmesi. Operasyonel amaçların içinde kurumun faaliyet gösterdiği belirli bir ortamı yansıtması gerekir. Operasyonel amaçlar tahsis edilen kaynakların yönetilmesinde odak noktaları olduğu için, operasyonel amaçlar net değilse veya iyi kavranmamışsa, bu kaynaklar iyi yönetilmeyebilir.

- **Raporlamayla ilgili amaçlar-** Bu amaçlar raporlamanın güvenilirliği ile ilişkili olup hem malî hem de malî olmayan verileri içerebilir. Raporlamayla ilgili amaçlar üçüncü kişiler için hazırlanan bilgilerle ilişkili olsa da güvenilir raporlamanın temel amacı, yönetime tespit edilen hedefe uygun, doğru ve eksiksiz bilgiler sağlamaktır. Doğru ve eksiksiz bilgiler olmaksızın iyi kararlar vermek yönetim açısından son derecede zordur.

- **Uygunlukla ilgili amaçlar-** Bu amaçlar yasalara ve yönetmeliklere uygunlukla ilgili amaçlardır. Piyasalarla, çevreyle, çalışanların refahıyla ve benzeri konularla ilgili kurallar söz konusu olabilir. Bazı kurumların uluslararası uygunluk amaçlarına uyum göstermeleri de gerekebilir.

2.2.4 Etkili risk yönetimi, bir kurumun operasyonel, raporlama ve uygunluk ile ilgili amaçlarının gerçekleşmekte olduğu konusunda makul güvence sağlar.

2.2.5 Yönetim ve yönetim kurulu tarafından belirlenen risk iştahı, strateji saptamada ve amaçların göreli önemini değerlendirmede bir yönlendirici işarettir. Gerçekte, risk iştahı, bir kurumun paydaşlar için değer (kamu hizmetleri biçiminde) yaratmada kabul etmeye hazır olduğu risk seviyesidir. Genellikle, hedefenen misyonu gerçekleştirmek üzere her biri farklı risklere sahip bir çok strateji tasarlanabilir. Yönetim, risk iştahı ile en çok uyuşan stratejiyi ve bağlantılı amaçları seçmelidir.

2.2.6 Risk toleransı, amaçların gerçekleşmesiyle ilgili olarak kabul edilebilir fark düzeyidir. Risk toleransı performans hedeferi yardımıyla ölçülebilir. Performans hedeferi; çoğu kez, amaçların ilişkili olduğu aynı birimlerde ölçülür. Risk toleransları çerçevesinde faaliyet göstermek yönetime kurumun risk iştahı içinde kaldığı ve amaçlarını gerçekleştirdiği konusunda çok daha fazla güvence sağlar.

2.3 Hadiselerin Tanımlanması (Event Identification)

2.3.1 Yönetim, vuku bulunca, kurumu etkileyecek potansiyel hadiseleri (events) tanımlar. Fırsatları temsil eden hadiseleri, kurumun stratejiyi başarılı şekilde uygulama ve amaçları gerçekleştirme kabiliyetini olumsuz şekilde etkileyen hadiselerden (risklerden) ayırmak gerekir. Hadiseleri tanımlamak için yönetim, kurumun bütünü bağlamında risklere ve fırsatlara yol açabilen iç ve dış faktörler dizisini dikkate alır.

2.3.2 Hadiseler; stratejinin uygulanmasını veya amaçların gerçekleşmesini etkileyen iç veya dış orijinli olaylar (incidents) veya vakalardır (occurences). Hadiseler olumlu veya olumsuz veyahut da hem olumlu hem de olumsuz etkiye sahip olabilir. Bazı hadiseler apaçık görülür iken bazıları belirsizdir ve hadiseler önemsiz veya hatırı sayılır etkilere sahip olabilir. Hadiselerin gözden kaçmasını önlemek için hadiselerin tanımlanması ile hadiselerin vuku ihtimalinin ve etkilerinin değerlendirilmesinin birbirinden ayrı olarak yapılması uygun olur.

2.3.3 Yönetimin hadiseleri belirleyen iç ve dış faktörlerin temel kategorilerini anlaması gerekir. Dış faktörler; özellikle, politik, sosyal ve teknolojik ortamdaki değişikliklerden ve kurumu veya tedarikçileri etkileyen ekonomik sorunlardan kaynaklanan faktörlerdir. İç faktörler, yönetimin işleyiş tarzı ile ilgili olarak yaptığı tercihlerden kaynaklanır. İç faktörler, kurumun alt yapısı, kurumun kaç mahalde faaliyet gösterdiği, personelin becerileri ve uzmanlıkları, kurum bilgi sistemlerinin nasıl işlediği gibi hususları içerir.

2.3.4 Hadiselerin tanımlanması teknikleri hem geçmişe hem de geleceğe dönüktür. Geçmiş hadiselere odaklanan teknikler, yıllık raporlar ve hesaplar, hatalı ödemelerle ilgili açıklamalar, iç raporlar gibi öğeleri değerlendirebilir. Gelecekteki hadiselere odaklanan teknikler, nüfus değişikliği, yeni piyasa koşulları ve siyasal ortamda beklenen değişiklikler gibi faktörlerle ilgilenebilir. Bu teknikler karmaşıklık ve otomasyon düzeyleri bakımından çok değişkenlik gösterir ve hadiselere yukarıdan aşağıya veyahut da aşağıdan yukarıya bakış açısıyla odaklanabilir.

2.3.5 Hadiselerin soyutlanmış şekilde vuku bulması az rastlanan bir durumdur. Bir hadise diğerini tetikleyebilir ve hadiseler eş zamanlı olarak vuku bulabilir. Yönetim, hadiselerin karşılıklı olarak birbirleriyle nasıl bağlantılı olduklarını anlamalıdır. İlişkileri değerlendirmek suretiyle risk yönetim çabalarının nerelere yönlendirileceğini belirlemek mümkün olabilir.

2.3.6 Potansiyel hadiseleri kategoriler içinde gruplandırmak da yararlı olabilir. Hadiselerin yatay olarak bütün kurum bünyesinde, dikine olarak da faaliyet birimleri bünyesinde toplanması yönetime hadiseler arasındaki ilişkileri kavrama imkânı verir. Hadiselerin gruplandırılması, ayrıca, en maliyet etkin cevapların neler olduğu konusunda işaretler verebilir. Her kurum hadise gruplandırmasında kendi metodunu oluşturabilirse de, standart araçlara örneğin "PEST" Piyasa Analizi2 metoduna dayanabilir.

2.4 Risklerin Değerlendirilmesi

2.4.1 Risklerin değerlendirilmesi, kuruma, potansiyel hadiselerin amaçların gerçekleşmesi üzerinde ne derecede bir etkiye sahip olduğunu değerlendirme imkânı verir. Yönetim, hadiseleri, nicel ve nitel tekniklerin bir kombinasyonundan yararlanmak suretiyle iki perspektiften -etki ve olasılık değerlendirmelidir. Hadiselerin olumlu ve olumsuz etkileri ya bireysel olarak ya da kurum bütününü kavrayan kategori itibariyle değerlendirebilir. Risk değerlendirmesi hem bireysel riskler hem de artık riskler temelinde yapılmalıdır.

2.4.2 "Risklerin değerlendirmesi" terimi zaman zaman tek bir aktiviteyi belirtmek için kullanılmakta ise de, kurum risk yönetimi bağlamında risk değerlendirme öğesi daha çok kurumun bütününde gerçekleşen devamlı ve tekrarlanan etkileşimli eylemler olarak kabul edilir. Risk değerlendirmesinin amacı hangi hadiselerin yönetimin dikkatinin odaklanacağı kadar önemli ve anlamlı olduğunu belirlemektir.

2.4.3 Potansiyel olaylara ilişkin belirsizliklerin olasılık ve etki perspektiferinden değerlendirilmesi gerekir. Olasılık (likelihood), bir hadisenin belirli bir zaman periyodu içinde vuku bulma ihtimalini (possibility) ifade etmesine karşılık, etki (impact)q hadisenin kurumun kendi amaçlarını gerçekleştirme kabiliyeti üzerindeki tesir (effect) derecesi anlamına gelmektedir. Yönetimin süresince olasılığı değerlendirdiği zaman süresi, ilgili strateji ve amaçların zaman ufkuna tekabül etmelidir. En önemli riskler vuku olasılığı ve etkisi yüksek olan risklerdir. Bunun tersine en az önem taşıyan riskler vuku olasılığı ve etkisi düşük olan risklerdir. Yönetim çabalarını yüksek olasılıklı ve yüksek etkili risklere odaklamalıdır. (Aşağıdaki 2 numaralı şemaya bakın.) Sürecin nihaî neticesi her bir riski olasılık ve etki açısından derecelendirmek olacaktır. Bazı kurumlar "yüksek düşük" şeklindeki derecelendirmeyi kullandıkları halde, diğer bazı kurumlar "trafik ışığı" sisteminde olduğu gibi kırmızı, sarımsı kahverengi ve yeşil renkleri ve

başkaları nicel bir ölçüyü, örneğin yüzde oranını kullanmaktadırlar.

2.4.4 Risk değerlendirme metodolojisi nicel veya nitel olabilir; objektif ya da sübjektif metotlara dayanabilir. Ayrıca, bir kurumun bütün faaliyet alanlarında klasik değerlendirme tekniklerini kullanması gerekmez. Ancak, yönetimin riskleri değerlendirirken insanî faktörlerin farkında olması ve ilgili bütün personelin bu değerlendirme için kullanılan derecelendirme sisteminin anlamını kavramalarını sağlaması gerekir. Bu gerçekleşmezse, üst yönetimin çeşitli risklerin her birinin önemini belirlemesi zor olacaktır.

2.4.5 Risk değerlendirmesi tamamlanır tamamlanmaz, kurumun risk öncelikleri belli olmalıdır. Eğer riske maruz olma kurumun risk iştahı çerçevesinde kabul edilemez ise, risk "yüksek öncelikli" veya "kilit risk" olarak sınışandırılmalıdır. Kilit risklere kurumun en üst kademesinde düzenli olarak dikkat gösterilmelidir. Kurum başka amaçlar belirledikçe, risk ortamı değiştikçe ve temel risklere cevap verildikçe spesifik risk öncelikleri zaman içinde değişiklik gösterecektir.

2.4.6 Yukarıda ana hatlarıyla açıklanan risk değerlendirmesi "bünyesel risk" ile ilişkilidir. Bünyesel risk, yönetimin hadisenin vuku ihtimalini veya etkisini değiştirmek üzere yapacağı eylemlerinin yokluğunda kurumun karşılaşacağı risktir. Artık risk, aşağıdaki paragrafta ana hatlarıyla açıklanan yönetim risk cevabının (karşılığının) dikkate alınmasından sonra geriye kalan risktir. Bu metodun avantajı, kurumlara diğer sorunları çözmek için daha iyi harcanabilecek iken yönetim tarafından bu zaman kendilerine ayrılan riskleri belirleme imkânı vermesidir. (Örneğin, bünyesel riskin vuku ihtimalinin düşük olması nedeniyle böyledir.)

2.5 Riske Cevap (Risk Response)

2.5.1 İlgili riski değerlendirdikten sonrayönetim bu riske nasıl cevap verileceğini kararlaştırır. Tanımlanmış riske cevap verme biçimleri arasında riskin transferi, riskin iyileştirilmesi, faaliyetlerin sona erdirilmesi ve riske katlanılması yöntemleri yer almaktadır. Kendi cevap türünü belirlerken, arzulanan risk toleransı çerçevesinde artık riski taşıyacak cevabı seçmek amacıyla, yönetim olasılık ve etki üzerindeki tesiri değerlendirir ve her bir cevabın maliyetini ve faydasını dikkate alır. Yönetim, ayrıca, yararlanılabilir bütün fırsatları belirlemeli ve global risk vizyonu elde edilmesine imkân sağlamalıdır.

2.5.2 Risk cevapları aşağıdaki kategorilerde dizilmektedir:

- **Paylaşma/Riskin Transferi-** Riskin bir bölümünün transfer edilmesi veya paylaşılması suretiyle bu risk olasılığının veya etkisinin azaltılması. Bu, klasik sigorta yoluyla veyahut üçüncü kişiye riski bir başka şekilde üstlenmesi için ödeme yapılması suretiyle gerçekleştirebilir. Bu seçenek, özellikle, finansal riskleri, varlıklarla ve dışarıya yaptırılan faaliyetlerle ilgili riskleri azaltmada yararlıdır. Ne var ki, risklerin çoğu bütünüyle transfer edilemez. Özellikle, hizmet dışarıdan sağlanmış olsa bile, tanınmışlıkla ilgili riskin transferi genellikle mümkün değildir.

- **Azaltma/Riskin İyileştirilmesi-** Risklerin büyük çoğunluğu bu şekilde çözümlenir. Risk olasılığını veya etkisini veyahut her ikisini azaltmak için önlemler alınır. Bu tür bir cevap; detaylı şekilde 2.6 numaralı bölümde ve

- **İç Kontrol-** Bütünleşik Çerçevede ele alınan kontrol prosedürleri dâhil olmak üzere, genellikle, çok sayıda günlük yönetsel kararları kapsar.

- **Kaçınma/Faaliyetin Sona Erdirilmesi-** Bu tür cevapta riske yol açan aktivitelere son verilir. Kamu sektörü kurumlarının bir ana program unsurunun sağlanmasından vazgeçmeleri çok seyrek bir durum olmakla birlikte, yeni bir hizmet sunum metodunun uygun olup olmadığının değerlendirilmesi veyahut spesifik bir projeye devam etmenin yerinde olup olmadığının belirlenmesi söz konusu olduğunda kaçınma (vazgeçme) yararlı bir cevap olabilir.

- **Kabul/Katlanma-** Risk olasılığını veya risk etkisini azaltmak için hiçbir önlem alınmaz. Bu cevap; etkiyi veya olasılığı kabul edilebilir bir düzeye indirmek için verimli bir metot belirlenmemiş olduğunu veyahut bünyesel riskin zaten kabul edilebilir düzeyde bulunduğunu varsaymaktadır. Kuşkusuz, riske katlanılması, eğer risk gerçekleşirse doğacak etkileri ele alan müdahale önlemleri ile desteklenebilir.

2.5.3 "Kurum Risk Yönetim" modeli sadece riskleri önceden tahmin edip yönetmeye değil, ama aynı zamanda, aynı yaklaşım çerçevesinde fırsatları belirlemeye vurgu yapmaktadır. Hangi durumla karşılaşırsa karşılaşsın, yönetim sadece olumsuz etkileri olan riskleri veya hadiseleri değil, olumlu etkiler barındıran fırsatları veya hadiseleri dikkate almalıdır. Bu konuda iki husus söz konusudur. İlkin, tehditlerin azalmasına paralel olarak, olumlu etkiden yararlanmaya yönelik bir fırsatın ortaya çıkıp çıkmadığını; ikinci olarak da tehditler doğurmaksızın olumlu fırsatlar yaratan koşulların ortaya çıkıp çıkmadığını incelemek gerekir.

2.5.4 Yönetim; riski ele alan çeşitli metotların etkilerini değerlendirmenin ardından risk tolerans sınırları çerçevesinde hem risk olasılığına hem de risk etkisine yönelik olarak tasarlanmış bir cevabı veya cevap kombinasyonunu seçmek suretiyle riskin en iyi nasıl yönetileceğine karar vermelidir. Seçilen cevabın zorunlu olarak, en az miktarda artık risk sonucunu doğurması gerekmez. Ancak, eğer cevap yine de risk tolerans derecesini aşıyorsa, yönetimin ya cevabı ya da risk tolerans düzeyini yeniden incelemesi gerekecektir.

2.5.5 Bünyesel riske yönelik alternatif cevapların değerlendirilmesi, bir cevaptan kaynaklanabilen ilave risklerin dikkate alınmasını gerektirir. Bu durumda üst yönetimin cevapları global perspektiften değerlendirmesi yararlı olur. Bu değerlendirme, üst yönetime genel risk cevap profiline ilişkin genel bir bakış vereceği gibi varlığını sürdüren artık risklerin türlerinin ve niteliğinin genel misyona ve risk iştahına uygun düşüp düşmediğini inceleme imkânı sağlar.

2.5.6 Riskleri karşılamak için tercih edilen metotların seçiminin hemen ardından yönetimin bir uygulama planı hazırlaması gerekir. Her uygulama planının kritik kısmı kontrol faaliyetlerinin risk cevabının etkili

şekilde icra edilmesini sağlamasıdır.

2.6 Kontrol Faaliyetleri

2.6.1 Kontrol faaliyetleri; yönetimin risklere yönelik cevaplarının uygulanmakta olduğunu güven altına alan siyasalar ve prosedürler bütünüdür. Kontrol faaliyetleri bütün organizasyonda, bütün kademelerde ve bütün fonksiyonlarda cereyan eder. Kamu Sektörü İç Kontrol Standartları Rehberi etkili kontrolleri oluşturulmasıyla ilgili ayrıntılı bilgiler içermekte olduğundan, bu Ek iç kontrolleri kurum risk yönetimi bağlamı içine yerleştirmekten başka bir amaç taşımamaktadır.

2.6.2 Kurum risk yönetimi, kontrol faaliyetlerini, bir kurum tarafından yönetim amaçlarına ulaşmak için uygulanan prosesin önemli bir parçası olarak görmektedir. Kontrol faaliyetleri sadece kendi başına bir amaç olmadığı gibi "yapılacak doğru şey" olarak ortaya çıkmaz. Bu faaliyet, daha çok, yönetim amaçlarının gerçekleşmesini sağlamaya imkân veren mekanizmalar olarak hizmet görür.

2.6.3 Kontrol faaliyetleri, genellikle, risk cevaplarının gerektiği şekilde uygulanmalarını sağlamak üzere oluşturulmakta ise de bazı amaçlar bakımından bizatihî kontrol faaliyetleri risk cevabıdır. Kontrol faaliyetlerinin seçimi veya revizyonu işi bu faaliyetlerin risk cevabı ve ilişkili amaçlar yönünden uygunluklarının ve isabetliliklerinin incelenmesini içermelidir.

2.6.4 Her bir kurum kendine özgü amaçlara ve uygulama yaklaşımına sahip olduğu için risk cevaplarında ve bağlantılı kontrol faaliyetlerinde farklılıklar bulunmaktadır. İki kurum aynı amaçlara sahip olmuş ve bu amaçları gerçekleştirmek için benzer kararları almış olsa bile, sonuç olarak ortaya çıkan kontrol faaliyetleri farklı olabilecektir. Bunun nedeni iki farklı yönetim ekibinin farklı risk iştahına ve farklı risk toleransına sahip olmasıdır.

2.6.5 Ancak, risk yönetimi bağlamında bütün kontrol prosedürleri aşağıdaki dört kategoriden birine girmektedir:

- ***Önleyici kontroller*** riskin gelişmesi ve istenmeyen sonucun gerçekleşmesi olasılığını sınırlamak üzere tasarlanır. Kurumun amaçlarını gerçekleştirme kabiliyeti üzerindeki riskin etkisi ne kadar büyükse, uygun nitelikte önleyici kontrollerin uygulanması o kadar önemli hale gelir.
- ***Yönlendirici kontroller*** belirli bir sonuca ulaşılmasını sağlamak üzere tasarlanır. Bu kontroller arzu edilmeyen bir hadiseden (örneğin güvenlik ihlalinden) kaçınılması zorunlu olduğunda özellikle önemlidir ve dolayısıyla, çoğu kez, uygunluk amaçlarının gerçekleşmesini desteklemek amacıyla kullanılır.
- ***Ortaya çıkarıcı kontroller*** "hadiseden sonra" arzu edilmeyen sonuçların vuku bulmuş olup olmadığını belirlemeyi hedefler. Ne var ki, uygun nitelikte ortaya çıkarıcı kontrollerin mevcudiyeti, caydırıcı bir etki yaratmak suretiyle arzu edilmeyen sonuçların oluşması riskini de azaltabilir.
- **Düzeltici kontroller** ortaya çıkmış arzulanmayan sonuçları düzeltmeyi amaçlar. Bu kontroller, fonları ve servisleri kayıplara veya hasarlara karşı korumayı amaçlayan müdahale önlemi olarak da hizmet görebilir.

2.7 Bilgi ve İletişim

2.7.1 İç kontrol amaçlarını desteklemek üzere kullanılan verilerin kalite kriterleri ile kurum risk yönetimini desteklemek üzere kullanılan verilerin kalite kriterleri arasında çok küçük bir farklılık vardır. Kamu Sektörü İç Kontrol Standartları Rehberi bilgi ve iletişim hakkında ayrıntılı bilgiler içerdiğinden bu Ek kurum risk yönetim bağlamı içinde bu kriterlerden daha fazlasını vermeyi amaçlamamaktadır.

Bilgi

2.7.2 Kurum risk yönetimi, özellikle, iç kontrol amaçlarının gerçekleşmesi için gerekli olandan daha geniş kapsamda bilgi toplanmasını öngörmektedir: Örneğin, stratejik amaçlara odaklanmak daha çok çıktı ve sonuç bilgisine ihtiyaç göstermektedir. Ayrıca, içine bu verilerin yerleştirildiği kullanım biraz farklıdır. Geçmişle ilgili veriler; kuruma, fiilî performansı hedefere, planlara ve beklentilere kı-yasen izleme imkânı verir ve yönetimin dikkatini gerektiren potansiyel hadiselerle ilgili olarak önceden uyarılar getirebilir. Güncel veriler, yönetime, işletme biriminde/prosesinde mevcut riskler hakkında eş zamanlı bir fikir elde etme ve beklentilerden sapmalarıbelirleme imkânı verir. Kurum böylelikle faaliyetinin risk tolerans sınırları içinde olup olmadığını belirleyebilir.

2.7.3 Tutarlı bilgiler belirlenip toplanmalı ve personele, sorumluluklarını yerine getirmelerine imkân verecek bir formatta ve zamanda iletilmelidir. Etkili bir iletişim, ayrıca, bütün kurum içinde yukarıdan aşağıya, enine ve aşağıdan yukarıya gerçekleşmelidir. Bütün personel üst düzey yönetimden kurum risk yönetim sorumluluklarının ciddiyetle yerine getirilmesi gerektiği hususunda net bir mesaj almalıdır. Çalışanların kurum risk yönetim prosesi içinde kendilerine düşen rolleri ve bu rollerin diğer kişilerin çalışmalarıyla olan ilişkisini anlamaları gerekir. Personel önemli bilgileri yönetimin uygun kademesine iletme araçlarına sahip olmalıdır. Dış paydaşlarla da etkili bir iletişime ihtiyaç vardır.

2.7.4 Doğru bilgilerle donanmış kişilere, istenen zamanda ve uygun mahalde sahip olunması etkili kurum risk yönetimi bakımından gereklidir.

İletişim

2.7.5 İletişim, bilgi sistemlerinden ayrı düşünülemez. İlgili personele görevlerini yerine getirme imkânı veren bilgileri sağlamanın yanı sıra iletişim, kurum kültürünü yansıtan, beklentilere cevap veren, bireylerin ve grupların sorumluluklarını ve diğer önemli meseleleri kapsayan daha geniş bir anlamda düşünülmelidir.

2.7.6 Yönetim, personelden beklenen davranışlarla ve onların sorumluluklarıyla ilgili olarak spesifik ve hedefi bir iç iletişim sağlar. Bu iletişim kurumun risk yönetim felsefesinin ve yaklaşımının açık ve seçik bir beyanını içermelidir. Süreçlere ve prosedürlere ilişkin iletişim arzulanan kültüre paralel olmalı ve bu kültürün tesisine hizmet etmelidir. İletişim aşağıdaki hususlara duyarlı olmalıdır:

- Kurum risk yönetiminin önemi ve yerindeliği
- Kurumun amaçları
- Kurum risk iştahı ve risk tolerans derecesi
- Riskleri tanımlamada ve değerlendirmede kullanılan ortak dil
- Risk yönetim öğelerini uygulamaya geçirmede ve desteklemede personelin rolleri ve sorumlulukları

2.7.7 Bunun yanı sıra çalışanlar, risk temelli bilgileri operasyonel yönetime ve bütün organizasyona iletmek için araçlara sahip olmalıdırlar. İşleyiş problemleriyle her gün ilgilenmek durumunda olan ilk hat çalışanları, çoğu kez, problemler oluşur oluşmaz bu problemleri fark etmek bakımından çok iyi konumdadırlar. Raporlanacak bu tür bilgiler bakımından açık iletişim kanallarının ve belirgin dinleme iradesinin bulunması gerekir. Eğer kurum kültürü "mesajı iletenin öldürülmesi"ne imkân veriyorsa, çalışanlar problemleri üstlerine iletmeyecekler ve riskler zamanında belirlenmeyebilecektir.

2.7.8 Pek çok durumda normal raporlama kanalları raporların hiyerarşi içinde iletilmesi için uygundur. Ne var ki, bazı koşullarda alternatif iletişim kanalları gerekir (ihbar hatları örneğinde olduğu gibi). Önemi nedeniyle, etkili kurum risk yönetimi doğrudan üst yönetime bağlı bir alternatif iletişim kanalının bulunmasını ve bu kanalın geri tepme korkusu olmaksızın bütün personelin kullanı-mına hazır olmasını gerektirir.

2.7.9 Uygun iletişim yalnız kurumun içinde değil, kurumun dışında da bulunmalıdır. Kurumun beklentileri karşılayacağı ve bu beklentileri yöneteceği konusunda güvence vermek amacıyla kurumun riskleri yönetme tarzı hakkında dış paydaşlara bilgi verilmesi gerekir. Bu, özellikle, halkı etkileyen riskler söz konusu olduğunda ve halk hükümetin riskleri kendisi için yönetme kapasitesine bağımlı olduğunda önem taşımaktadır. Kurum dışı taraşarla iletişim ciddiyetle ve dürüstlükle gerçekleştirildiğinde, bu tür iletişim bütün kuruma önemli mesajlar gönderir ve örgüt kültürü üzerinde önemli bir etkiye sahip olabilir.

2.8 İzleme

2.8.1 Kurum risk yönetimi, kendi öğelerinin zaman zarfındaki işleyişini değerlendirmek amacıyla izlemeye konu olmalıdır. İzleme, rutin izleme faaliyetleri, ayrı değerlendirmeler (evaluations) ya da ikisinin kombinasyonu aracılığıyla gerçekleştirilebilir. Kurum risk yönetim sistemindeki yetersizlikler, kurumun süreçlerini iyileştirmesi amacıyla, yönetimin uygun kademesine iletilmeli, ciddi meseleler de üst yönetime veya kurula raporlanmalıdır.

2.8.2 Bir kurumun amaçları zaman içinde değişebilir. Risk portföyü ve bu portföydeki risklerin göreli önemi de zaman zarfında değişebilir. Eskiden etkili olan risk cevapları yetersiz veya uygulanamaz hale gelebilir ve kontrol faaliyetleri etkililiğini kaybedebilir veyahut tamamıyla terk edilebilir. Hâlâ uygun ve etkili olup olmadığını belirlemek amacıyla yönetimlerin kendi risk yönetim sistemlerinin etkililiğini sürekli olarak izlemeleri gerekir.

2.8.3 Risk yönetiminin etkililiğine ilişkin değerlendirmeler; risk gruplarının anlamlılığına, bu riskleri yönetmedeki risk cevaplarının ve bu cevaplarla ilişkili kontrollerin önemine bağlı olarak kapsam ve sıklık bakımından değişiklik gösterir. Yönetim, risk yönetim çerçevesinin bir kapsamlı değerlendirmesini yapma kararı aldığında, dikkat strateji belirlenmesi dâhil olmak üzere, sürecin bütün yönlerinin ele alınmasına yöneltilmelidir. Ancak, olağan yönetim aktiviteleri, örneğin risk kayıtlarının güncellenmesi ve organizasyonel veya fonksiyonel “periyodik kontroller” da risk yönetim sürecini izlemenin bir parçasını oluşturur.

Kaynakça

Australian Standard® for risk management (Standards Australia, 2004)

Entity Risk Management - Integrated Framework (COSO, 2004)

Integrated Risk Management Framework (Treasury Board of Canada Secretariat, 2001)

Internal Control - Integrated Framework (COSO, 1992)

Risk Management Standard (ARMIC, IRM&ALARM, 2002)

The Orange Book: Management of Risk - Principles and Concepts (HM Treasury, 2004)