INTOSAI:

Kamu Kesimi İç Kontrol Standartları Rehberi

Çeviren
Baran Özeren
Uzman Denetçi
12. Gr.

10 Temmuz 2006

İçindekiler

Önsöz

1992 tarihli INTOSAI İç Kontrol Standartları Kılavuzu[*]; iç kontrolu 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 kararları 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

[*] Sözü edilen Kılavuz Sayıştayın "135. Kuruluş Yıldönümü Yayınları" içinde dilimize kazandırılmıştır. (Çevirenin Notu)

[1] COSO, Enterprise Risk Yönetimi- Integrated Framework, www.coso.org. 2004

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[2] bu yana, kamu sektöründeki sahteciliğin ve yolsuzluğun önlenmesi ve ortaya çıkarılması kadar, etik tutum ve davranışların öneminin daha fazla vurgulanması iç kontrol hedeflerinin 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 kontrolun geleneksel bakış açısıyla tam olarak sınırlandırılmadığından ve daha kapsamlı yönetim kontrolu kavramını tam

[2] XVI. Uluslararası Sayıştaylar Birliği Kongresi; 1998, Montevideo

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 kontrolları giderek önemli hale gelmiştir. Bilişim teknolojisi kontrolları; 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 kontrolun tesis edilmesine ve bunun sürdürülmesine rehberlik etmektir. Bu nedenle, kamu yönetimi (government management), rehberin önemli bir yararlanıcısıdır. kamu yönetimi, bu rehberden kendi organizasyonlarında iç kontrolu geliştirme ve uygulamaya koyma temelinde yararlanabilir.

Kkamu denetiminde; iç kontrolun değerlendirilmesi genel kabul görmüş bir çalışma standardı[3] olduğundan, denetçiler bu Rehberden bir denetim gereci olarak yararlanabilirler. COSO Modelini ihtiva eden iç kontrol standartları, bu nedenle, hem devlet yönetimi[4] tarafından organizasyonlarının güçlü iç kontrol yapısı bakımından bir örnek, hem de denetçiler tarafından iç kontrolu 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 hedefler; kullandıkları kamu fonları; bütçe çevriminin önemi; performanslarının karmaşıklığı (bu kanunlara uygunluk, güvenilirlik ve şeffaflık 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 kontrolun geliştirilmesine yönelik ayrıntılı politikalar, prosedürler ve uygulamalar tesis etmez, bununla birlikte, kurumların içinde bu türden kontrolları

[3] INTOSAI Denetim Standartları

[4] Sözü edilen grup spesifik olarak faaliyetleri yürüten personel değildir. Faaliyetleri yürüten personel iç kontroldan ve kontrolun 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.

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. 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 kontrolun maliyeti artırma bakımından önemli etkileri de vardır. Mevcut prosedürlerden ayrı yeni kontrol prosedürleri eklenmesi maliyetleri arttırır. Mevcut faaliyetlere ve etkili iç kontrolun katkısına odaklanmak ve kontrolları sürdürülen temel faaliyetlerle bütünleştirmek suretiyle, bir organizasyon, çoğunlukla, gereksiz prosedürleri ve maliyetleri azaltabilir.

Yönetim ve Diğer Personel Tarafından Hayata Geçirilme

İç kontrolu çalıştıranlar kişilerdir. Bu, yaptıkları ve söyledikleriyle, organizasyonun içindeki kişilerle başarılır. 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 hedeflerini de belirler ve iç kontrol sisteminin tümünden sorumludur. İç kontrol kurumun hedefleri bağlamında riskleri kavrayabilmek üzere gerekli mekanizmaları oluşturduğundan, yönetim iç kontrol faaliyetlerini uygulamaya koyacak, bunları izleyip değerlendirecektir. İç kontrolun uygulanması önemli yönetim inisiyatifini ve yönetimle diğer personel arasında yoğun bir iletişimi gerektirir. Bu nedenle, iç kontrol yönetimin yararlandığı bir araçtır ve kurumun hedefleriyle doğrudan bağlantılıdır. O kadar ki, yönetim iç kontrolun önemli bir unsurudur. Ancak, organizasyon içindeki bütün personel iç kontrolun 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 kontrolu 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 hedeflerin gerçekleştirilmesi konusunda sadece makul güvence oluşturur.

Makul güvence sağlama

İç kontrol ne kadar iyi tasarlanırsa tasarlansın ve ne kadar iyi işlerse işlesin, genel hedeflerin 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 kontrolu veya etkisi dışındaki faktörlerin onun hedeflerini 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 kontrolların bir maliyeti olduğu gerçeğine işaret eder. Bu tür sınırlamalar yönetimi hedeflerin gerçekleşmesine için mutlak güvence oluşturmaktan alıkoyar.

Makul güvence; iç kontrolun maliyetinin ondan elde edilen yararı aşmaması gerektiği şeklinde tanımlanır. Risklere yanıt verme ve kontrolları 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 kontrolların tasarlanması, yöneticilerin gerçekleştirilmesi gereken genel hedefleri açık ve net bir biçimde anlamalarını gerektirir. Başka bir deyişle, kamu yöneticileri faaliyetlerinin bir alanındaki sistemlerini, başka faaliyetlerini olumsuz biçimde etkileyecek şekildeki aşırı kontrollarla 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 masrafları türünden yüksek riskli/düşük parasal miktarlar içeren işlemler üzerinde uygun kontrolların bulunması önemli olabilir. Genel

yönetim harcamaları ile alakalı parasal tutarlar üzerindeki uygun kontrollar 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 hedefler 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, kontrollar 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.

1.2. İç Kontrolun Etkinliği ile İlgili Sınırlar[5]

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

Etkin bir iç kontrol sistemi, ne kadar iyi tasarlanırsa tasarlansın ve ne kadar iyi işlerse işlesin, kurum hedeflerini gerçekleştirmesi veya kurumun varlığını sürdürmesi konusunda, yönetime sadece makul -mutlak değil- güvence sağlayabilir. Hedeflerin 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 kontrolunun sınırları dışında olup yöneticilerin kontrolları yeniden tasarlamasını veya kabul edilebilir risk düzeyini bu duruma göre ayarlamasını gerektirebilir.

Etkin bir iç kontrol sistemi hedefleri başaramama olasılığını azaltır. Bununla birlikte, iç kontrolun 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. Kontrolların 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 kontrolun etkinliği ve sistemi çalıştıran personeli derinden etkiler. Yönetimin, bu nedenle, kontrolları süreklilik temelinde gözden geçirmesi ve güncelleştirmesi, değişiklikleri personele duyurması ve kontrollara uyarak örnek oluşturması gerekir.

[5] İç kontrolun halihazırdaki anlamının yanlış anlaşılması yüzünden abartılı beklentileri önlemek amacıyla iç kontrolun etkinliği ile ilgili sınırlamaların vurgulanmasına ihtiyaç duyulmuştur.

2. İç Kontrolun Unsurları

İç kontrol birbiriyle bağlantılı beş unsurdan meydana gelir:

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

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

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

Açık hedefler belirlemek ve etkin bir kontrol ortamı tesis etmek suretiyle, kurum misyonunun ve hedeflerinin 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. Hedefleri 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. Hedeflerini 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 kontrolun değişen hedeflere, 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.

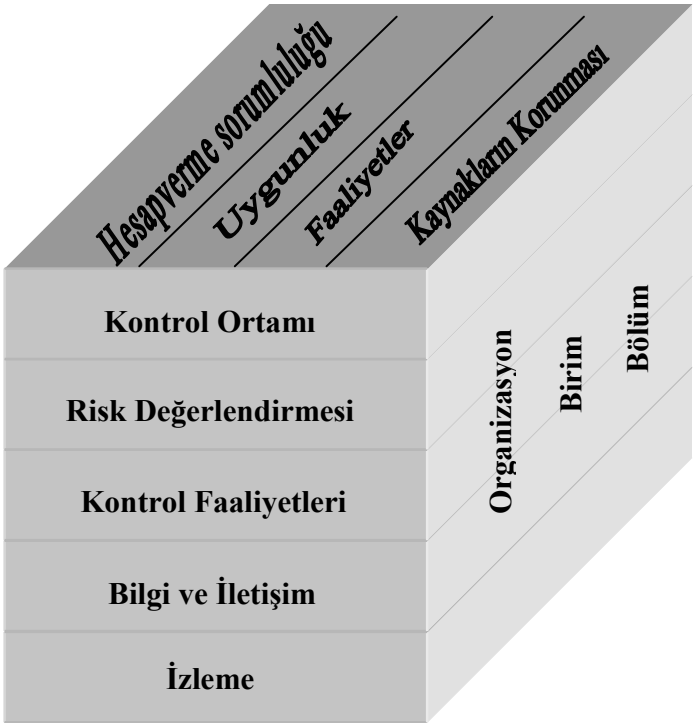
Bu rehber genel bir çerçeve sunmaktadır. Bu unsurlar uygulamaya konduğunda, organizasyonun faaliyetlerine uygun düşecek kapsamlı politikalar, prosedürler ve uygulamalar geliştirmekten, unsurların faaliyetlerin içine yerleştirilmesini ve faaliyetlerin ayrılmaz bir parçası olmasını sağlamaktan yönetim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



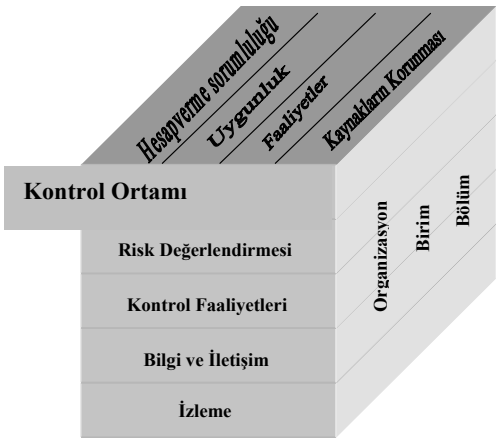
Benzer şekilde genel hedeflere bakıldığında, beş unsurun tümü de hedeflerin her biriyle ilgilidir. Faaliyetlerin etkinliği ve verimliliği gibi tek bir hedef ele alındığında, açıktır ki beş unsurun tümü verimliliğin ve etkinliğin gerçekleşmesine uygulanabilir ve bunların başarılması bakımından önemlidir.

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 kontrolu uygun şekilde geliştirmenin, uygulamaya koymanın ve sürdürmenin önemini anlamalarına genel iç kontrol hedeflerini 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 hedefleri ve özellikle de etiği ilgilendiren davranışların hedefi konusundaki farkındalıklarını arttırabilir, onların iç kontrol hedeflerini anlamalarına ve etik açmazlarla baş etme becerilerini geliştirmelerine yardımcı olur.

Üst Yönetimin Tavrı

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

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

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

Sonuç olarak, yönetimin etik davranışlar sergileyip bu konuda kararlılık göstermesi iç kontrol hedefleri bakımından yaşamsal önemdedir, özellikle de "etikle ilgili davranışlar"ın 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 kaynakları 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 kontrolun en önemli boyutu personeldir. Etkin kontrolun 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

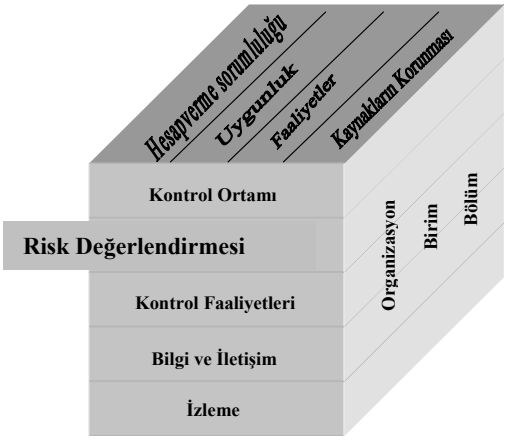
alma ve çalıştırma kararları; bu nedenle, kişilerin dürüstlüğünün, görevlerini yerine getirebilmelerine yetecek eğitime ve deneyime sahip olduklarının ve zorunlu formel, işbaşı ve etik eğitim göreceklerinin güvencesini içermelidir. Etkili bir iç kontrol için doğru iç kontrol anlayışına sahip ve sorumluluk 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 hedeflerini gerçekleştirebilmesi konusunda iç kontrol sadece makul güvence verebilir. İç kontrolun bir unsuru olarak risk değerlendirmesi garantiyi sağlayacak uygun kontrol faaliyetlerinin seçilmesinde kilit rol oynar. İç kontrol kurumun hedeflerini gerçekleştirmesini engelleyen riskleri tespit ve analiz etme, bunlara verilecek uygun yanıtları belirleme sürecidir.

Sonuçta, hedeflerin belirlenmesi risk değerlendirmesinin önkoşuludur. Yönetim; başarısını engelleyecek riskleri tespit etmeden ve onlarla başetmeye yönelik önlemleri almadan önce hedeflerini 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 hedeflere yönelik risklerin tespit edilmesine dayanır. Bu hedeflerle 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 hedeflerinin açıklanmasıyla ortaya çıkan risk profilindeki[6] değişimlerin tespitini kolaylaştırır.

[6] Bir kurumun ya da alt birimlerinin karşı karşıya kaldığı önemli risklere genel bir bakış ya da bunların matrisidir; olayların meydana gelme olasılığı ya da ihtimaliyle birlikte, etki düzeylerini (örneğin, yüksek, orta, düşük) ihtiva eder..

Risk tespiti için uygun araçları benimsemek gerekir. Yaygın biçimde en fazla yararlanılan araçlardan ikisi risk incelemesi yaptırılması ve risk özdeğerlendirmesidir.[7]

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 finansal riskler) pek çoğunu nitelendirmek çoğunlukla zor olduğundan (örneğin; saygınlık riski), riskleri analiz etme metodolojileri farklılık gösterir. Sözü edilen bu ikinci risk, subjektif 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 hafifletir.

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 sınıflandıran 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

---

[7] *Risk İncelemesi Yaptırılması*

Yukarıdan aşağıya doğru işleyen bir prosedürdür. Organizasyonun hedefleriyle bağlantılı faaliyetlerini ve eylemlerini gözden geçirmek ve bunlarla bağlantılı risklerini tespit etmek üzere bir ekip oluşturulur. Ekip, özellikle riske duyarlı olan politika alanları, eylemleri ve fonksiyonları (sahtecilik ve yolsuzluk riskleri dahil olmak üzere) belirlemek suretiyle, faaliyetlerin tümünün bir risk profilini çıkarmak için organizasyonun her kademesindeki kilit personelle bir dizi mülakat yapar.

Risk Özdeğerlendirmesi

Aşağıdan yukarıya doğru işleyen bir prosedürdür. Organizasyonun her kademesi ve her bölümü faaliyetlerini gözden geçirmeye ve karşı karşıya kaldıkları yükselen risklerini teşhis etmeye davet edilir. Çalışma, dokümantasyon yaklaşımı yoluyla (anket soruları yoluyla konulan teşhise yönelik bir çerçeve), ya da kolaylaştırılmış bir atölye yaklaşımı vasıtasıyla yapılabilir.

Her iki yaklaşım birbirinden ayrı düşünülmemelidir; yukarıdan aşağıya ve aşağıdan yukarıya elde edilen risk değerlendirme süreci girdilerinin bileşiminin hem kurum ölçeğinde hem de faaliyet düzeyinde riskleri tespit edebilmesi arzulanır.

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 subjektif 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 hedeflerini gerçekleştirmesi konusunda iç kontrolun 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 kontrolu dizayn etmek, normal koşullarda, yeterlidir. Her kontrolun bir maliyeti vardır ve kontrol faaliyetinin göğüslediği riskle bağlantılı maliyet değerini karşılaması gerekir.

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

[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.

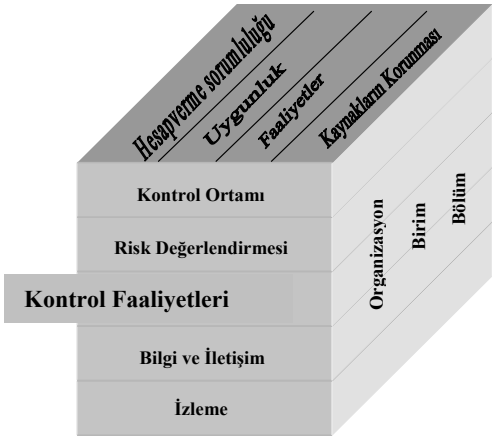
hedeflerin öncelikleri ve bunlara eşlik eden risklerin önemi farklı yöne kayıp değişikliğe uğrar.

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.

2.3 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) 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 eğitme),

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, kontrolun uygulamaya konma maliyetinin ondan elde edilecek yararları aşmaması),
- kapsamlı, makul ve kontrol hedefleriyle 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 direktifler 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 kontrolu eksiksiz biçimde uygulamaya koymaya yetecek sayıda personeli bulunmayabilir.Bu tür durumlarda yönetim risklere karşı uyanık olmalı ve bu riskleri diğer kontrollarla 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 kontrollar

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 direktiflerine 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) İşgörme performansına yönelik incelemeler

Etkinlik ve verimlilik değerlendirilmek suretiyle faaliyet performansı bir dizi standarda göre düzenli olarak gözden geçirilir. Performans incelemeleri fiili başarıların saptanmış hedefleri veya standartları karşılamadığı sonucuna varmışsa, iyileştirmeye ihtiyaç duyulup duyulmadığını tespit etmek bakımından hedefleri 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 işletimleriyle 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 hedeflerinin 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 direktiflerinin 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 kontrolların özel dezavantajlarını telafi etmek için karma kontrollardan 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 kontrolun bir unsuru olarak biçimlendirildiğinin açık olması gerekir. Kontrol faaliyetleri iç kontrolun diğer dört unsuru ile bütünleştirilmelidir.

Örnekler

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

2.3.1 Bilişim Teknoloji Kontrol Faaliyetleri

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

(1) Genel Kontrollar

Genel kontrollar 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 kontrolların işlediği bir ortam yaratır.

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

(2) Uygulama Kontrolları

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

Genel kontrollar ve uygulama kontrolları birbirleriyle bağlantılıdır; her ikisi de bilişim süreçlerinin eksiksiz ve doğru olmasını sağlamaya yardım etmelidir. Bilişim teknolojilerinin hızla değişmesi yüzünden, bağlantılı kontrolların 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, 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 kontrolları kendi sistemleri tarafından işlenmiş bilgilerin eksiksizlik, vaktindelik, verilerin doğruluğu ve güvenilirliğinin korunması gibi, arzu edilen kontrol hedeflerini karşılaması bakımından yönetime makul güvence sağlar.

Bilişim teknolojisi kontrolları genel kontrollar ve uygulama kontrolları olmak üzere iki ana gruptan oluşur.

Genel Kontrollar

Genel kontrollar; 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 kontrollar içinde uygulama sistemleri ve kontrolların çalıştığı bir ortam yaratır.

Genel kontrolların ana kategorileri şunlardır:

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

(2) *Erişim kontrolları*; 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 kontrollar;* izinsiz programları ve mevcut programların değiştirilmelesini önler.

(4) *Sistem yazılımının kontrolları*; 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 kontrolları;* istenmeyen olaylar meydana geldiğinde kritik faaliyetlerin kesilmeden devam etmesini veya derhal başlatılıp, önemli ve hassas verilerin korunmasını sağlamaya yardımcı olur.

Uygulama Kontrolları

Uygulama kontrolları 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 kontrollar, genellikle, bilişim sistemleri içinde bilgi akışı olurken hataları ve düzensizlikleri önlemek, ortaya çıkarmak ve düzeltmek amacıyla dizayn edilir.

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

Uygulama kontrolları 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 kontrollar ve uygulama kontrolları birbirleriyle bağlantılıdır.

Uygulama kontrollarının etkinliğine karar verirken genel kontrolların etkinliği önemli bir faktördür. Genel kontrollar zayıf olduğu takdirde, özel uygulamalarla bağlantılı kontrolların güvenilirliği önemli ölçüde azalır. Etkin genel kontrollar olmadan uygulama kontrolları 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 kontrolu olabilir. Ancak, genel kontrollar yazım denetiminden muaf tutulmuş bazı işlemleri engelleyemiyen yetkisiz program değişikliklerine izin veriyorsa, bu kontrola güven duyulmayabilir.

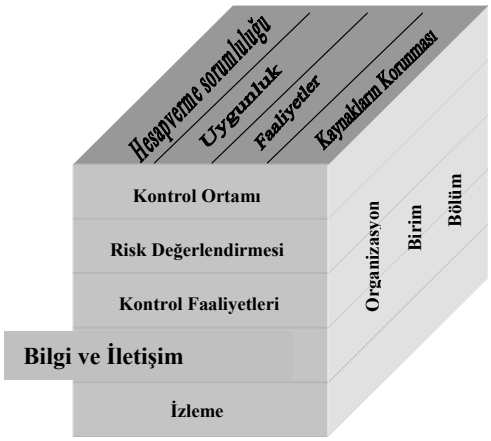
Bilişim teknolojisinde meydana gelen hızlı değişiklikler, kontrol hedeflerinin esasını değiştirmemekle birlikte, etkin kalabilmeleri bakımından kontrolların mükemmelleştirilmesini gerektirir. Ağ sistemine giderek artan oranda güven duyulması, son kullanıcıların ellerindeki veri işlemcisine sorumluluk 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.

Örnekler

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

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 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 sınıflandırılmasıdır.

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 sınıflandırılması gerekir. Bunun anlamı hazırlanan raporlar, çizelgeler ve finansal tablolardan elde edilen bilgilerin düzenlenmesi, tasnif edilmesi ve biçimlendirilmesidir.

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 taraflarca 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 hedeflerinin ve kontrol prosedürlerinin tanımlamalarını kapsamalıdır. Organizasyonun hedefleri 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.

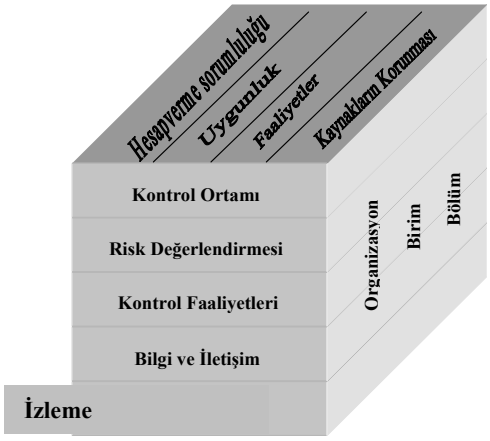
Kurum içi iletişimlere ek olarak yönetim, kurum dışı iletişimler organizasyonun hedeflerine ulaşma derecesi üzerinde çok önemli etki yaratabilecek girdiler sağlayabildiğinde, üçüncü kişilerle iletişim kurmaya ve onlardan bilgi edinmeye yarayan araçlar temin etmelidir.

Yönetim; kurum içi ve kurum dışı iletişimlerden elde edilen girdilere dayalı olarak gerekli önlemleri zamanında almak ve bu önlemleri izlemek zorundadır.

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 sonuçları 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 kontrolun 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 kontrolları uygulayan personelin ehliyetine ve deneyimine ve sürekli izleme faaliyetinin sonuçlarını göz önünde bulundurmalıdır. Tekil kontrol değerlendirmeleri, spesifik bir zamanda, kontrolların etkinliğine doğrudan odaklanmak suretiyle de yararlı olabilir. Özel değerlendirmeler kontrol tasarım incelemesinin ve iç kontrolların 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 kontrolun 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 hedeflerini başarma gücünü olumsuz etkileyen bir durum demektir. Eksiklik, bu yüzden, muhtemel veya gerçek bir kusuru veya kurumun genel hedeflerini başarma olasılığını artırmak bakımından iç kontrolu güçlendirme potansiyelini ifade eder.

İç kontrolun eksikliği hakkındaki gerekli bilginin doğru taraflara 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 hedefleri 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 kontrolun izlenmesi; denetimlerin ve diğer incelemelerin bulgularının yeterli şekilde ve hemen çözüme kavuşturulmasını hedefleyen 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 sonuçları 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.

Örnekler

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

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 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 kontrolunun 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 kontrolu yaşama geçirirler. Bunlar, genellikle, kontrolları yürüten, gözden geçiren ve yanlış uygulanan kontrolları düzelten ön cephedeki kişiler olup, günlük görevlendirmelerin gerçekleştirilmesinde kontrollar 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 hedeflerini gerçekleştirmesine katkıda bulunabilirler veya iç kontrolun 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:

- kontrolların değerlendirildiği riskin öneminin ve hassasiyetinin belirlenmesi,
- kaynakların kötüye kullanımının ortaya çıkaracağı duyarlılığın ve ahlak kuralları, ekonomiklik, verimlilik ve etkinlik konusunda hedeflere varmadaki başarısızlığın veya hesapverme sorumluluğunun gerektirdiği zorunluluklar bakımından yetersizliğin ve yasalara ve düzenlemelere aykırılığın değerlendirilmesi,
- ilgili kontrolların tespit edilmesi ve kavranması,

- kontrol etkinliği hakkında halihazırda bilinenlerin belirlenmesi,
- kontrol tasarımının yeterliliğinin değerlendirilmesi,
- kontrolların 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 kontrolun 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 hafifletip 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 hedeflerinin, özellikle, "hesapverme sorumluluğunun gereklerini yerine getirme"nin ve "kaynakları 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 kontrolun tanımı ve gerçekleştirilecek hedefleri 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 etmektedir.

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.	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 örneklerinin etkinliğinin ve verimliliğinin izlenmesine yardımcı olabilir.

Hesapverme sorumluluğunun gereklerinin yerine getirilmesi 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 veyahut da spor merkezlerinin veya spor klüplerinin sayısının %15 oranında 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 erişilebilmelidir.	Raporun tatmin edici olup olmadığı 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 akdî ilişkisi bulunmayan 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 geliştirmeli ve kamu ihaleleri ile ilgili bütün yasalara ve düzenlemelere göre davranılmalıdır.	Bu ihale şartnamesinin bütün koşullarının ilanı ile bağlantılı prosedürler, alınan tekliflerin değerlendirilmesi ve kazanan teklif sahibinin açıklanması yazılı olarak ve alınan önlemler ayrıntılarıyla dokümante edilmelidir. Teklifler değerlendirilirken, tekliflerin seçilme ve seçilememe nedenlerinin tümü belgelendirilmelidir.	İç denetim dosya incelemesi yapabilir ve itirazları takip edebilir.

Düzenli, ahlakî, 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 kontrolu 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, ahlakî, 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 niteliklerini çek etmek, - İnşaat işlerinin gelişimini arazi üzerinde görmek ve bunlar hakkındaki gelişme raporlarını gözden geçirmek, - Faturalarını inceleyerek birliklerin harcamalarını denetlemek ve sübvansiyonun (veya bir bölümünün) 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 edilmesini ve diğer benzer projelerle karşılaştırmalarını kapsar. Ayrıca, sulanan arazilerin hasılatlarının takibi de dikkate alınabilir.

Kaynakların korunması; örnek (1): Savunma bakanlığının ardiyeleri, askerî 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 beşerî sermaye politikaları yürürlüğe konmalıdır.	Kişilerin satmak ya da uygun olmayan biçimde kullanmak amacıyla silahları 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, yalnızca, 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 kontrollarının önemi küçümsenmekte ve bu yüzden de, Bilişim Teknolojisi kontrolunda 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 beşerî sermaye politikaları da önemli rol oynar.	Genel kontrollar düzeyinde, kuruluş; - kullanıcı erişimini sadece görevleri gereği bilgiye ihtiyaç duyan kullanıcılarla sınırlandırmamıştır. - programları ve hassas verileri korumak için sistem yazılım kontrollarını yeterince geliştirmemiştir. - yazılım değişikliklerini dokümante etmemiştir. - bağdaşmayan görevleri birbirinden ayırmamıştır. - hizmet devamlılığıyla ilgilenmemiştir. - ağ sistemini yetkisi bulunmayanlardan korumamıştır. Uygulama kontrolları 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 kontrollarını uygulamaya koyabilir. - uygulama kullanıcılarının işletim sistemine giriş yapabilmelerini engelleyebilir. - uygulamayı geliştirme personelinin üretim 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 faaliyetini 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.