Bilgi Notu

ARAŞTIRMA VE TASNİF GRUBU **11.03.2002**

ABD Sayıştayı Tarafından Yayımlanan

"Federal Devlette İç Kontrol Standartları"

İsimli Doküman Hk.

Federal Hükümette İç Kontrol Standartları

Çeviri

Baran Özeren
Uzman Denetçi
Araştırma ve Tasnif Grubu

Mart 2002

Eserin Özgün Adı
Standarts for Internal Control in the Federal Government
Washington DC, Kasım 1999

Önsöz

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

1982 tarihli Federal Yöneticilerin Malî Güvenilirliği Yasası (The Federal Manager's Financial Integrity Act) kamuda iç kontrol standartları yayımlama görevini ABD Sayıştayına vermektedir. Bu standartlar iç kontrolun oluşturulup sürdürülmesine ve yolsuzluk, israf, suiistimal ve kötü yönetim riskinin en yüksek olduğu önemli performans ve

yönetim sorunlarını ve alanlarını belirleyip bunlara dikkat çekilmesine dönük genel bir çerçeve sunar. Yönetim ve Bütçe Ofisinin 21 Haziran 1995 tarihinde gözden geçirip değiştirdiği ***"Yönetimin Hesapverme Sorumluluğu ve Kontrol"*** hakkındaki A-123 no'lu Genelgesi kontrollarla ilgili olarak değerlendirme yapmaya ve rapor hazırlamaya yönelik özel hükümler getirmektedir. Bu dokümandaki iç kontrol terimi yönetim kontrolu terimiyle eşanlamlı kullanılmakta olup bir kurumun faaliyetlerinin bütün boyutlarını (program amaçlı, finansal ve uygunluk) içermektedir.

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

Bilişim teknolojisindeki süratli gelişmeler modern bilgisayar sistemleriyle ilgili iç kontrol rehberinin güncellenme ihtiyacını

vurgulamaktadır. Beşerî sermayenin yönetimi iç kontrolun önemli bir parçası olarak kabul edilmektedir. Ayrıca, Treadway Komisyonunu Destekleyen Kuruluşlar Komitesi (Committee of Sponsoring Organizations of the Treadway Commission- COSO) tarafından yayımlanan ***"İç Kontrol-Bütünleşik Sistemi"*** dokümanı aracılığıyla özel sektör iç kontrol rehberini güncelleştirmiş bulunmaktadır. Sonuç olarak, hazırladığımız bu güncel standartlar daha önce yayınladığımız "Federal Devlette İç Kontrol Standartları"nın yerine geçmektedir.

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

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

David M. Walker
ABD Sayıştay Başkanı

Giriş

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

Tanım ve Hedefler

İç Kontrol

Bir örgüt yönetiminin ayrılmaz öğesi olup;

- faaliyetlerde etkinlik ve verimlilik,
- finansal raporlamada güvenilirlik,
- yürürlükteki yasalara ve düzenlemelere uygunluk

amaçlarının gerçekleşmesi konusunda makul güvence sağlar.

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

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

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

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

Temel Kavramlar

İç Kontrol

- faaliyetlerin sürekli biçimde ayrılmaz bir öğesini oluşturur.
- kişiler tarafından hayata geçirilir.
- mutlak güvence değil, makul güvence sağlar.

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

İç kontrol faaliyetlerin sürekli biçimde ayrılmaz bir öğesini oluşturur	İç kontrol tekil bir olay değil, bütün bir örgüt faaliyetlerinde ve devamlılık temelinde oluşan bir seri eylem ve aktivitedir. İç kontrol, kuruluş içinde ayrı bir sistem olmaktan çok, yönetimin faaliyetlerini düzenlemede ve yönlendirmede yararlandığı sistemlerin ayrılmaz bir parçası olarak kabul edilmelidir. Bu bakımdan iç kontrol, yöneticilerin kurumu çalıştırmalarına ve amaçlarını süreklilik temelinde gerçekleştirmelerine yardımcı olmak üzere alt yapının bir parçası olarak inşa edilen bir yönetim kontroludur.
İç kontrol kişiler tarafından hayata geçirilir	İç kontrolu çalıştıranlar kişilerdir. Başarılı bir iç kontrolun sorumluluğu bütün yöneticilere düşmektedir. Yönetim amaçları belirler, kontrol mekanizmalarını oluşturur ve faaliyetleri uygulamaya koyar ve kontrolu izler ve değerlendirir. Ancak örgüt içindeki bütün personel bunun gerçekleşmesinde önemli rol oynar.
İç kontrol mutlak güvence değil, makul güvence sağlar	Yönetim iç kontrolu maliyet ve faydaları ile bağlantılı olarak tasarlamalı ve uygulamalıdır. Ne kadar güzel tasarlanıp uygulanırsa uygulansın, bütün kuruluş amaçlarının gerçekleşmesi konusunda mutlak güvence sağlayamaz. Kontrol dışındaki faktörler veya yönetimin nüfuzu kurumun hedeflerinin tümünü gerçekleştirme gücünü olumsuz

etkileyebilir. Örneğin; insan hataları, karar ya da yorum hataları ve kontroldan kaçınmak üzere gizli anlaşmalar yapma kuruluş amaçlarının gerçekleşmesini etkileyebilir. Bu nedenle, konulduğu her yerde iç kontrollar kuruluş amaçlarını gerçekleştirmenin mutlak değil makul güvencesini sağlar.

İç Kontrol Standartları

Standartların Sunumu

İç Kontrolun Beş Standardı

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

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

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

Kontrol Ortamı

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

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

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

Bir diğer faktör, yönetimin uzmanlığa olan bağlılığıdır. Bütün personelin kendilerine verilen görevi başarması kadar başarılı bir iç kontrolu geliştirmesinin ve uygulamanın önemini kavramasına imkân veren bir uzmanlık

seviyesine sahip olması ve bunu sürdürmesi gerekir. Yönetim farklı görevler için gereksinim duyulan elverişli bilgi ve becerileri tespit etmeli ve eğitim sağlamanın yanı sıra dürüst ve yapıcı tavsiyelerde bulunup personelin performansını değerlendirmelidir.

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

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

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

Etkili beşeri sermaye politikaları ve uygulamaları önemli bir diğer çevresel faktördür. Etkili beşeri sermaye politikaları ve uygulamaları işe alma, oryantasyon, eğitim, değerlendirme, tavsiyelerde bulunma, teşvik

etme, ücret ödeme ile personelin disipline edilmesine yönelik iyi uygulamaların tesis edilmesini içerir. Ayrıca gerektiği kadar inceleme yapılmasını da kapsar.

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

Risk Değerlendirmesi

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

Risk değerlendirmesinin ön koşulu, kuruluş amaçlarının açık-seçik ve tutarlı biçimde belirlenmesidir. Risk değerlendirmesi Kamusal Performans ve Sonuçlar Yasası gereğince stratejik ve yıllık performans planlarında tespit edilmiş amaçlar gibi açıklanan amaçların gerçekleştirilmesiyle bağlantılı risklerin tanımlanması, analiz edilmesi ve bu risklerin nasıl yönetilmesi gerektiği hakkında bir esas oluşturulmasıdır.

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

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

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

Kontrol Faaliyetleri

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

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

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

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

Kontrol Faaliyetlerinden Örnekler

- fiili performansın üst düzeyde incelenmesi,
- yönetim tarafından fonksiyonel düzeyde ya da faaliyet düzeyinde yapılan incelemeler,
- beşeri sermayenin yönetimi,
- bilgi işleme üzerindeki kontrollar,
- hassas varlıklar üzerinde fiziki kontrol,
- performans ölçülerinin ve göstergelerinin oluşturulması ve gözden geçirilmesi,
- görevlerin ayrılması,
- işlemlerin ve işlerin gerektiği şekilde icrası,
- işlemlerin ve işlerin eksiksiz ve vaktinde kaydedilmesi,
- kaynaklara ve kayıtlara erişim sınırlandırmaları ve bunlarla ilgili hesap verme sorumluluğu,
- işlemlerin ve iç kontrolun uygun biçimde dokümante edilmesi.

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

Fiilî Performansın Üst Düzeyde İncelenmesi	Yönetim, kuruluşun önemli başarılarının izini sürmeli ve bunları, Kamusal Performans ve Sonuçlar Yasasına göre oluşturulan planlar, ana amaçlar ve hedeflerle kıyaslamalıdır.
Yönetimce Fonksiyonel ve Organizasyonel Düzeyde Yapılan İncelemeler	Yöneticilerin, fiilî performansı örgüt genelinde planlananla ya da arzulanan sonuçlarla kıyaslaması ve önemli farklılıkları da analiz etmesi gerekir.
Beşerî Sermayenin Yönetimi	Bir örgütün işgücünün –ki beşerî sermayesidir- etkin biçimde yönetimi sonuçlara ulaşılması açısından yaşamsal önemde olup iç kontrolun ayrılmaz bir parçasıdır. Yönetim beşerî sermayeye bir maliyet olarak değil bir varlık olarak bakmalıdır. Faaliyetlerin başarısı, yalnızca, işe doğru personel alınmasıyla, doğru eğitim, araçlar, sistem ve teşvikler sağlanmasıyla ve doğru sorumluluklar verilmesiyle mümkündür. Yönetim ihtiyaç duyulan becerileri süreklilik temelinde değerlendirmeli ve örgütün ana amaçlarını gerçekleştirebilmesi için gerekli becerilerle donatılmış işgücünü temin edebilmelidir. Eğitim çalışanların beceri düzeylerini, örgütün değişen ihtiyaçlarını karşılayacak şekilde geliştirmeyi ve sürdürmeyi hedeflemelidir. İç kontrol hedeflerine ulaşılabilmesi bakımından süreklilik temelinde ve nitelikli bir gözetim gerçekleştirilmelidir. Örgütün başarısıyla kendi performansları arasındaki bağlantıyı anlamalarına yardımcı olmak üzere, çalışanların etkin bir ödül sistemiyle desteklendiği bir performans değerleme ve tepki alma (feed back) sistemi tasarlanmalıdır.

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

Bilgi İşleme Üzerindeki Kontrollar

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

Hassas Varlıklar Üzerindeki Fiziksel Kontrol

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

Performans Ölçülerinin ve Göstergelerinin Oluşturulması ve Gözden Geçirilmesi	Faaliyetlerin performans ölçülerini ve göstergelerini izlemek üzere tesis edilmeleri gerekir. Bu faaliyetler, ilişkilerin analiz edilebilmesi ve uygun önlemlerin alınabilmesi bakımından farklı veri setlerinin diğerleriyle karşılaştırılmasını ve değerlendirme yapılmasını gerektirir. Kontrollar, ayrıca, örgütsel ve bireysel performans ölçüleri ile göstergelerinin doğruluğunun ve güvenilirliğinin teyit edilmesini de hedeflemelidir.
Görevlerin Ayrılması	Hata ya da sahtecilik riskinin azaltılması bakımından, önemli görevlerin ve sorumlulukların farklı kişiler arasında bölüşülmesine veya birbirinden ayrılmasına ihtiyaç duyulur. Bu ise işlemlere onay verilmesine, bunların gerçekleştirilmesine ve kaydedilmesine, gözden geçirilmesine ve söz konusu varlıkların yönetilmesine dönük sorumlulukları kapsar. Bir işlemin ya da bir olayın bütün önemli boyutlarını tek bir kişi kontrol etmemelidir.
İşlemlerin ve İşlerin Gerektiği Şekilde İcrası	İşlemler ve diğer önemli işler yalnızca bunlara yetkili kişilerce onaylanmalı ve icra edilmelidir. Satın almaya, transfere, kullanıma yönelik geçerli işlemlere başlandığı veya tahsis edilen kaynakların veya diğer işlerin harekete geçirildiği konusunda güvence sağlamanın esas yolu budur. Yetkilendirmeler yöneticilere ve çalışanlara açık bir biçimde duyurulmalıdır.

İşlemlerin ve İşlerin Eksiksiz ve Vaktinde Kaydedilmesi	Faaliyetlerin kontrol edilmesi ve kararların alınması sırasında yönetim nezdinde ilgisini ve önemini sürdürmesi bakımından işlemlerin doğru şekilde kaydedilmesi gerekir. Söz konusu kaydetme faaliyeti, hesap özetlerinin nihaî sınıflaması aracılığıyla, bir işlemin veya işin başlangıcından ve onaylanmasından o işlemin veya işin tamamlanmasına kadar bütün süreç veya süre boyunca uygulanır. Kontrol faaliyetleri bütün işlemlerin tam ve doğru biçimde kayıt altına alındığından emin olunmasına da yardımcı olur.
Kaynaklara ve Kayıtlara Erişim Sınırlandırmaları ve Bunlarla İlgili Hesapverme Sorumluluğu	Kaynaklara ve kayıtlara erişim yetkili kişilerle sınırlandırılmalı, gözetime ve kullanıma yönelik olarak bu kişilere hesapverme sorumluluğu tevdi edilmeli ve bu görev sürdürülmelidir. Kaydedilenlerle kaynakların periyodik olarak mukayesesine yönelik hesapverme sorumluluğu hataların, yolsuzluğun, suiistimal riskinin veya yetkisiz görev değişikliğinin en aza indirilmesine yardımcı olmalıdır.
İşlemlerin ve İç Kontrolun Uygun Biçimde Dokümante Edilmesi	İç kontrolun, diğer işlemlerin ve başka önemli işlerin açık biçimde dokümante edilmesi gerekir; incelemelerde kolayca belgelere ulaşılmalıdır. Dokümantasyon yönetimin direktiflerinde, idarî politikalarda veya çalışma rehberlerinde açık ve net biçimde görünmeli; hem kağıt üstünde hem de elektronik ortamda tutulabilmelidir. Belgelerin ve kayıtların tümü doğru biçimde yönetilip muhafaza edilmelidir.

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

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

Bilişim Sistemlerine Yönelik Spesifik Kontrol Faaliyetleri

- Genel Kontrol
- Uygulama Kontrolu

Bilişim sistemlerine özgü kontrol iki ana başlık altında toplanmaktadır: Genel kontrol ve uygulama kontrolu. Genel kontroldan bütün

bilişim sistemlerinde –ana bilgisayar, kişisel bilgisayar, ağ sistemi ve nihai kullanıcılı ortamlarda- yararlanılır. Uygulama kontrolu ise uygulama yazılımı içindeki veri işlemesini kapsayacak şekilde tasarlanır.

Genel Kontrol

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

Özellikle de;

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

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

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

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

Uygulama Kontrolları

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

Bilgisayar sistemleri üzerindeki genel ve uygulamaya dönük kontrollar birbirleriyle bağlantılıdır. Genel kontrol uygulama kontrolunun çalışmasını destekler; eksiksiz ve doğru bilgi işlemenin sağlanması için iki tür kontrola da ihtiyaç duyulmaktadır. Genel kontrolun yetersiz olması durumunda uygulama kontrolu muhtemelen düzgün çalışmaz ve göz ardı edilebilir.

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

Bilgi ve İletişimler

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

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

Program yöneticileri, kurumlarının stratejik ve yıllık performans planlarının gerçekleşip gerçekleşmediğini ve kaynaklarının etkin ve verimli kullanılmasına yönelik hesap verme sorumluluğu amaçlarının karşılanıp karşılanmadığını tespit etmek bakımından hem finansal hem de faaliyetlerle ilgili olan verilere ihtiyaç duyarlar. Örneğin; işlenmiş bilgi finansal raporların hazırlanmasını gerektirir. Bu ise satın almalar, finansal yardımlar, sabit varlıklar ve stoklar hakkındaki verilere dayalı diğer işlemler ile tahsilatlardan elde edilen bir dizi geniş veriyi kapsar. İşlenmiş bilgi, kurumun çeşitli yasalar ve mevzuat uyarınca hukuka uygun davranıp davranmadığının tespit edilmesini de gerektirir. Finansal bilgiye hem kurum içinde hem de dışında ihtiyaç duyulur. Faaliyetler hakkında karar vermek, performansı

izlemek ve kaynakları tahsis etmek bakımından dışa dönük olarak düzenli biçimde rapor ve günlük bazda finansal tablo hazırlamak gerekir. Kalıcı nitelikteki bilgi tanımlanmalı, bu bilgi muhafaza edilmeli ve kişilerin görevlerini etkin olarak yapabilmelerine imkan verecek biçimde ve zaman dilimi içinde duyurulmalıdır.

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

İzleme

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

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

görevlerini yerine getirirken almış oldukları diğer önlemleri kapsar.

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

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

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

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

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

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

(1) tespit edilen yetersizlikleri düzelten,

(2) iyileşmeler sağlayan,

(3) yönetimin tedbir almasını gerektirmeyen bulguları ve tavsiyeleri sergileyen

adımlar atıldıktan sonra tamamlanır.