COBIT
(Control OBjectives for Information and related Technology)

Vildan UZUNAY
İç Kontrol Merkezi Uyumlaştırma Dairesi

Ankara,2007

Giriş

Son yıllarda Avrupa Birliğinde ve birçok ülkede kamu mali yönetim ve kontrolü anlayışında önemli değişiklikler yaşanmış, merkezi kontrolden iç kontrole geçiş olmuştur. Yeni kontrol anlayışı kapsamında, iç kontrol kavramı önem kazanmıştır.

Avrupa Birliği tarafından benimsenen kamu iç mali kontrol sistemi, iç kontrol kavramını esas almaktadır. COSO[1], önce özel sektörde kullanılan daha sonra kamu sektöründe de bir yönetim aracı olarak uygulanan iç kontrol anlayışını geliştirmiştir. Bu nedenle iç kontrol modeli COSO modeli olarak bilinmektedir. COSO modeli, Avrupa Birliği ve Uluslar arası Sayıştaylar Birliği INTOSAI[2] tarafından kabul edilen ve uygulanan bir iç kontrol modelidir.

COSO tarafından iç kontrol kavramı geliştirilmiş, iç kontrolün unsurları sayılmıştır. COSO modeli dışında diğer ülkeler tarafından uygulanan farklı iç kontrol modelleri de vardır. Kanada'da CoCo, İngiltere'de Turnbull Report, Güney Afrika'da King Report, Fransa'da Vienot Report gibi iç kontrol yöntem ve prosedürleri hakkında çalışmalar yapılmıştır. İç kontrolün tanımlanması, raporlanması, geliştirilmesi alanlarında COBIT, SAC, SAS55, SAS78 gibi başka yaklaşımlar da vardır.

Bu çalışmada iç kontrol alanındaki yaklaşımlardan COBIT incelenecektir.

[1] The Committee on Sponsoring Organizations of the Treadway Commission
[2] The International Organisation of Supreme Audit Institutions

1. İç Kontrol

Avrupa Birliği iç kontrol modeli olarak COSO modelini esas almıştır. COSO modeline göre iç kontrol; risklerin tespit edilmesi ve işlemlerin düzenli, etik, ekonomik, etkin ve etkili bir şekilde gerçekleştirilmesi, hesap verebilirlik sorumluluğunun yerine getirilmesi, yürürlükteki kanun ve yönetmeliklere uyumun sağlanması, kaynakların kayıp, kötü kullanım ve zararlara karşı korunması gibi hedeflere ulaşıldığına dair makul güvence sağlamak üzere tasarlanmış olan ve bir işletmenin yönetim kurulu, yöneticileri ve diğer personeli tarafından uygulanan bir süreçtir. İç kontrol, kurumun hedeflerinin gerçekleştirilmesi, mali raporların güvenilirliğinin sağlanması ve mevzuat ve düzenlemelere uyumun sağlanması konusunda makul güvence sağlamayı amaçlar.

COSO modeline göre iç kontrolün 5 bileşeni vardır. COSO modelinde iç kontrol bileşenleri; kontrol ortamı, risk değerlendirme, kontrol faaliyetleri, bilgi ve iletişim ile gözetimdir. Modelin etkilerinin nasıl tanımlandığı, uygulandığı, değerlendirildiğidir. Hedeflerin elde edilmesine yöneliktir. İç kontrol bir süreçtir.

Son yıllarda, iç kontrol konusunun önemi artmıştır. İç kontrolün tanımlanması, raporlanması, geliştirilmesi alanlarında 5 önemli doküman vardır. COBIT, COSO, SAC, SAS55 ve 78.

2. COBIT (Control OBjectives for Information and related Technology)

COBIT, ilk olarak 1996'da Information Systems Audit and Control Foundation (ISACF) tarafından yayımlanmıştır. Günümüzdeki başlıca yayımcısı Information Systems Audit and Control Association (ISACA) tarafından 1998'de kurulan IT Governance Enstitüsüdür. COBIT; ISO teknik standartları, ISACA ve AB tarafından yayınlanan yönetim kanunları, COSO, AICPA[3], GAO[4] tarafından yayınlanan profesyonel iç kontrol ve denetim standartları tarafından biçimlendirilmiştir. Bu kaynaklar COBIT 'in organizasyona adapte edilen bilgi teknolojisinden bağımsız olmasını sağlarken aynı zamanda pratik, işletmenin ihtiyaçlarına cevap vermeye hazır olmasını sağlayacak şekilde tanımlar.

COBIT (Bilgi ve İlgili Teknoloji için Kontrol Amaçları), Bilgi Sistemleri Denetim ve Kontrol Birliği[5] tarafından bir denetim aracı olarak tasarlanmıştır ama bilgi işlem ve iş

[3] The American Institute of Certified PublicAccounts
[4] The US General Accounting Office
[5] Information Systems Audit and Control Association- ISACA

yönetiminde de kullanılan bir araçtır. COBIT, bilgi ve ilgili teknoloji için kontrol amaçları yaklaşımıdır ve ulaşılmak istenen kontrol amaçları ve bu amaçlara ulaşmak için gerekli yollar tarafından tasarlanan kontroller olarak tanımlanan iç kontrol odaklı bir yaklaşımdır. İşletmenin iş hedefleri doğrultusunda hizmet vermesini sağlamak amacıyla bilgi işlem kaynaklarını kullanmasını amaçlar ve verilen hizmetlerin, istenilen kalite, güvenlik ve hukuksal ihtiyaçlara cevap vermesini sağlar. COBIT süreç değil kontrol esaslıdır. Şirketlerin neler yapması gerektiği ile ilgilidir ama bunların nasıl yapmaları gerektiği ile ilgilenmez.

COBIT yöneticinin, kontrol gereksinimleri, teknik konular ve iş riskleri arasındaki boşluklar arasında köprü kurmasına yardımcı olan yönetişim çatısı ve destekleyici araçlardır. COBIT, organizasyon genelinde bilgi teknolojisi kontrolü için saydam politika geliştirilmesine ve başarıyla uygulanmasına imkan vermektedir. Bilgi teknolojisinin işletmenin gereksinimlerini yerine getirmek konusunda başarılı olabilmesi için, yönetim iç kontrol modeli oluşturmaktadır. COBIT kontrol çerçevesi bu ihtiyaca cevap verir. İşletmenin gereksinimleri ile bağlantı kurar. Bilgi teknolojisi faaliyetlerini genel kabul görmüş bir süreç modeli şeklinde örgütler. Ana bilgi teknolojisi kaynaklarını tanımlar. İşletme kontrol hedeflerini açıklar.

İşletme yönelimli COBIT; işletmenin amaçlarının bilgi teknolojisi amaçlarına odaklanması, başarıyı değerlendirmek için vade modellerinin oluşturulması, işletme ve bilgi teknolojisi süreç sahiplerinin birleşik sorumluluklarının teşhis edilmesi faaliyetlerinden oluşur.

COBIT, iş süreç sahiplerinin bilgi sistem kontrol sorumluluklarını etkin ve verimli bir şekilde yerine getirmelerini sağlayan bir çerçevedir. SAC, iç denetçilere bilgi sistem ve teknolojisinin kontrol ve denetiminde yardım sağlar. SAS55 ve SAS78 dış denetçilere organizasyonun finansal tablolarının denetiminin planlanması ve gerçekleştirilmesi ile ilgili iç kontrol alanında rehberlik sağlar.

COBIT kaynak dokümanlarını COSO ve SAC ’dan sağlar. COBIT kontrolün tanımını COSO ’dan ve bilgi teknolojisi kontrol amaçlarının tanımını SAC ’dan alır. COBIT kontrol iş hedeflerinin gerçekleştirilmesi ve beklenmeyen olayların önlenmesi, düzeltilmesi için makul güvence sağlamak amacıyla tasarlanan kurallar, usuller, uygulamalar ve organizasyon yapıları olarak tanımlanmıştır.

İç kontrol, ulaşılmak istenen kontrol amaçları ve bu amaçlara ulaşmak için gerekli yollar tarafından tasarlanan kontrollerdir. COBIT anahtar iç kontrol gereksinimleri olan sistemleştirme, belgelendirme, standartlar ve tanımlanan beklentiler, değerlendirmeler, uygun

risk değerlendirmeleri, tanımlanmış operasyonel hedefler ve kontrol hedefleri, uygun kontroller, yetkili ve güvenilir insanlar, kontrol etme ve değerlendirmeyi birleştirir.

COBİT 'in misyonu; işletme yöneticileri ve denetçiler tarafından günlük kullanılan, yeterli, geçerli, modern, uluslararası genel kabul görmüş bilgi teknolojisi kontrol amaçlarını araştırmak, geliştirmek, tanıtmak ve ilerletmektir.

COBİT 'in amacı, kar maksimizasyonu, fırsat optimizasyonu, rekabetçi avantaj sağlamak için iş riski, kontrol gerekleri ve teknik konular arasındaki boşluklar arasında köprü kurmak için bir çatı oluşturmaktır.

2.1. COBIT 'in Unsurları:

COBIT beş unsurdan oluşan bir modeldir. Bunlar; yönetici özeti, çerçeve, kontrol amaçları, denetim ilkeleri ve yönetim ilkeleridir.

Yönetici özeti, COBIT 'in amaçlarını ve süreçlerini özetler.

Çerçeve; denetçiler, yöneticiler, işletme ve iş süreç sahipleri için kapsamlı rehberlik sağlar.

Kontrol amaçları, sürecin uygulanmasını kolaylaştırmak için üst düzey yönetici ihtiyaçlarını tanımlar.

Denetim ilkeleri, kapsamlı kontrol değerlendirmesi için gerekli bilgilerin elde edilmesi, değerlendirilmesi amacıyla oluşturulan bir modeldir.

Yönetim ilkeleri, yöneticinin aşağıdaki soruları yanıtlamasını sağlamak için faaliyete yönelik ilkelerdir:

1)Fayda maliyetten fazla mı?

2)İyi bir performansın göstergeleri nelerdir?

3)Kritik başarı faktörleri nelerdir?

4) Amaçları gerçekleştirememenin riskleri nelerdir?

5) Diğerleri ne yapıyor?

6) Nasıl karşılaştırma ve değerlendirme yapabiliriz?

2.1.1. COBİT Çerçevesi

COBIT unsurlarından çerçeve, bir iş süreç akım şemasıdır. Organizasyonun elindeki kaynaklardan elde ettiği mevcut bilgilerden iş süreçleri sonucunda ihtiyaç duyulan bilgilerin elde edilmesini sağlayan bir yapıdır. COBIT çerçevesi; işletme odaklı, süreç yönelimli,

kontrol esaslı ve ölçmeye dayalı olarak düzenlenmiştir. COBIT çerçevesi, işletmenin hedeflerini gerçekleştirmesi için gerekli bilgiyi sağlamak, kuruluşların gerekli bilgi hizmetlerini sunması için yapısal süreçlerde kullanılan bilgi teknolojisi kaynaklarını yönetmek ve kontrol etmek esaslıdır.

COBIT çerçevesi üç unsurdan oluşur. Bunlar bilgi için işletme gereksinimleri, bilgi teknolojisi kaynakları ve bilgi teknolojisi süreçleridir.

İşletmenin hedeflerini gerçekleştirmesi için bilginin COBIT 'in kullandığı kontrol kriterlerine uyumlu olması gerekir. Bilgi kriterleri etkililik, verimlilik, gizlilik, bütünlük, kullanırlık, uyum ve güvenirliktir.

Bilgi teknolojisi kaynakları bilgi, uygulama sistemleri, teknoloji, olanaklar ve insanlardır. Bilgi teknolojisi süreçleri planlama ve organizasyon, kazanım ve uygulama, teslim ve destekleme, izleme olmak üzere dört alandan oluşur. Bu alanlar, bilgi teknolojisi geleneksel sorumluluk alanları olan planlama, yapılanma, işleme, izleme ile eşleşir.

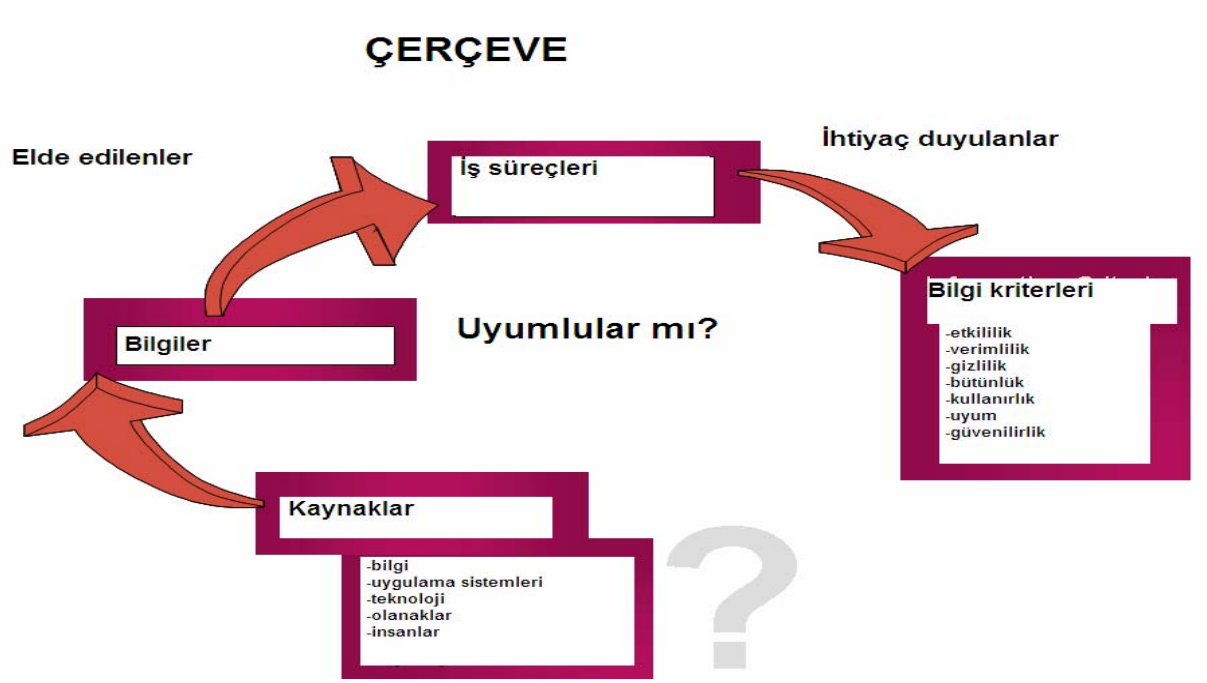
Planlama ve organizasyon süreci strateji ve taktikleri içerir, bilgi teknolojisinin iş hedeflerini gerçekleştirmesi adına en iyi katkıyı sağlamasının yollarını belirtir. Planlama ve organizasyon süreci; bilgi teknolojisi için stratejiler ve taktiksel planlar oluşturma, bilgi teknolojisinin iş hedeflerini en iyi şekilde gerçekleştirmesini sağlayacak yolları tanımlama, stratejik vizyonun gerçekleştirilmesini sağlama, planlama, bildirme, bilgi teknolojisi organizasyonunu kurma, bilgi yönetimi ve teknoloji altyapısı için alan oluşturma faaliyetlerinden oluşmaktadır.

Kazanım ve uygulama süreci; tanımlanan, geliştirilen, uygulanan, iş sürecine adapte edilen bilgi teknolojisi çözümleri, var olan sistemlerin değiştirilmesi ve sürdürülmesi faaliyetlerinden oluşmaktadır.

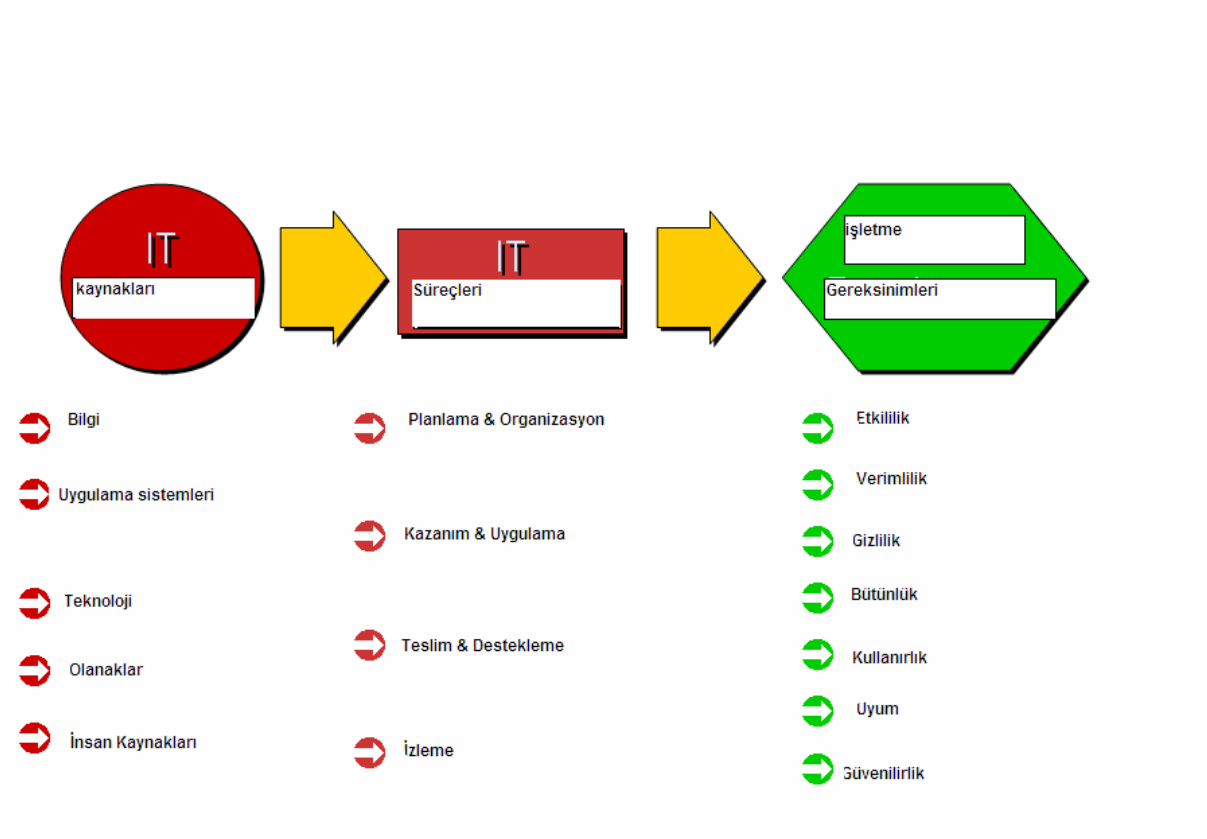
Teslim ve destekleme süreci; gerekli hizmetlerin yerine getirilmesi, hizmetlerin güvenliğinin ve devamlılığının sağlanması, eğitim ve stajı içeren destekleme sürecinin oluşturulması, uygulama kontrollerini içeren bilgi süreci faaliyetlerden oluşmaktadır.

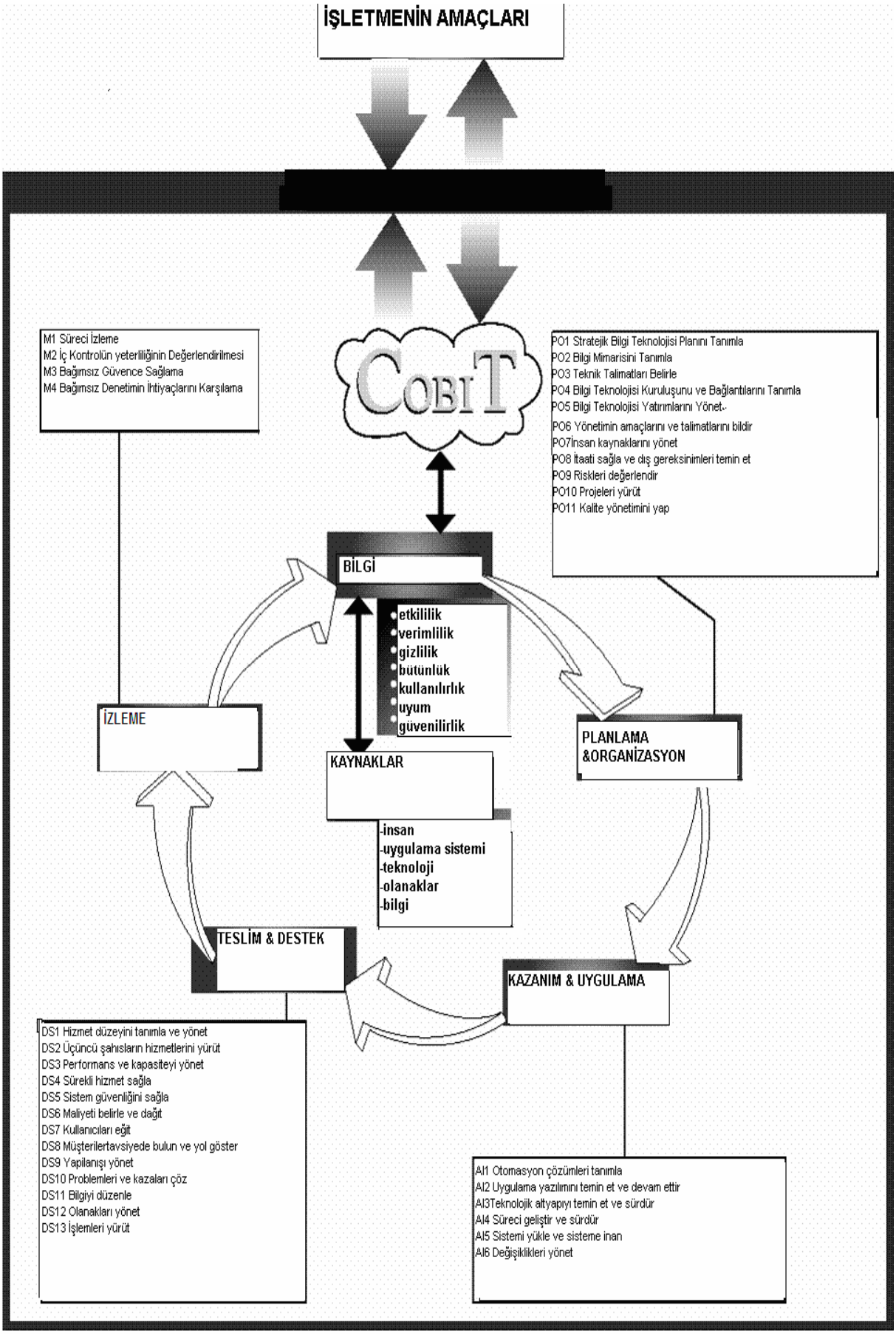
İzleme süreci; bütün bilgi teknolojisi süreçlerinin, kaliteleri ve kontrol gereksinimlerine uyumu açısından düzenli olarak gözden geçirilmesi faaliyetlerini gerektirmektedir. Bilgi teknolojisi sürecin kalitesi, kontrollerin uygunluğu, kontrol gereksinimlerine uyumunu düzenli olarak değerlendirilmesi, denetim fonksiyonunu gerçekleştirme faaliyetlerinden oluşmaktadır.

COBIT çerçeve içerisinde 34 kontrol amacı ve 318 ayrıntılı kontrol amacı yer almaktadır.


ÇERÇEVE
Elde edilenler
İş süreçleri
İhtiyaç duyulanlar
Bilgi kriterleri
-etkililik
-verimlilik
-gizlilik
-bütünlük
-kullanırlık
-uyum
-güvenilirlik
Bilgiler
Uyumlular mı?
Kaynaklar
-bilgi
-uygulama sistemleri
-teknoloji
-olanaklar
-insanlar
?

Bilgi teknolojisi süreçleri




İŞLETMENİN AMAÇLARI
M1 Süreci İzleme
M2 İç Kontrolün yeterliliğinin Değerlendirilmesi
M3 Bağımsız Güvence Sağlama
M4 Bağımsız Denetimin İhtiyaçlarını Karşılama
COBIT
PO1 Stratejik Bilgi Teknolojisi Planını Tanımla
PO2 Bilgi Mimarisini Tanımla
PO3 Teknik Talimatları Belirle
PO4 Bilgi Teknolojisi Kuruluşunu ve Bağlantılarını Tanımla
PO5 Bilgi Teknolojisi Yatırımlarını Yönet
PO6 Yönetimin amaçlarını ve talimatlarını bildir
PO7İnsan kaynaklarını yönet
PO8 İtaati sağla ve dış gereksinimleri temin et
PO9 Riskleri değerlendir
PO10 Projeleri yürüt
PO11 Kalite yönetimini yap
BİLGİ
etkililik
verimlilik
gizlilik
bütünlük
kullanılırlık
uyum
güvenilirlik
İZLEME
KAYNAKLAR
-insan
-uygulama sistemi
-teknoloji
-olanaklar
-bilgi
PLANLAMA &ORGANİZASYON
TESLİM & DESTEK
KAZANIM & UYGULAMA
DS1 Hizmet düzeyini tanımla ve yönet
DS2 Üçüncü şahısların hizmetlerini yürüt
DS3 Performans ve kapasiteyi yönet
DS4 Sürekli hizmet sağla
DS5 Sistem güvenliğini sağla
DS6 Maliyeti belirle ve dağıt
DS7 Kullanıcıları eğit
DS8 Müşterilertavsiyede bulun ve yol göster
DS9 Yapılanışı yönet
DS10 Problemleri ve kazaları çöz
DS11 Bilgiyi düzenle
DS12 Olanakları yönet
DS13 İşlemleri yürüt
AI1 Otomasyon çözümleri tanımla
AI2 Uygulama yazılımını temin et ve devam ettir
AI3Teknolojik altyapıyı temin et ve sürdür
AI4 Süreci geliştir ve sürdür
AI5 Sistemi yükle ve sisteme inan
AI6 Değişiklikleri yönet

COBIT denetim ilkeleri; anlamayı sağlama, kontrol değerlendirmesi, uyum değerlendirmesi ve teşvik riski olmak üzere dört unsurdan oluşur. COBIT yönetim ilkeleri; kritik başarı faktörleri, kilit hedef göstergeleri, kilit performans göstergeleri, vade modelleri olmak üzere dört unsurdan oluşur. COBIT bu süreçler sonucunda işletme hedeflerinin gerçekleştirilmesini amaçlar.

3. COBIT Bilgi Güvenliği

Bilgi güvenliği, Bilgi teknolojisi yönetişiminin en önemli unsurudur ve bütün bilgi kullanıcıları için bunu anlamak ve uygulamak önemlidir. Bilgisayar sistemleri işten eve kadar hayatın her alanında yaygınlaştıkça, güvenlik riskleri de artmaktadır. İnternet, portatif bilgisayar gereçleri, mobil teknolojinin yaygın kullanımı artık tüm bilgilere daha çabuk ulaşmamızı sağlamaktadır. Ancak diğer taraftan bilgi teknolojisindeki bu gelişmeler, bilgi hırsızlığı, virüslerle kasıtlı saldırı, bilgisayar korsanlığı gibi bilgi teknolojisi ile ilgili problemlerin ortaya çıkmasına sebep olmaktadır. Bu riskler, dikkatsiz hatalar, ciddi finansal zararlara sebep olur. COBIT Güvenlik Dayanağı daha iyi güvenlik sağlama ihtiyacı üzerine tasarlanmış ve bilgi kullanıcılarını risklerden korumak için önemli tavsiyeler ve pratik araçlar içeren bir modeldir.

COBIT Güvenlik Dayanağı, COBIT ’e dayandırılmaktadır. COBIT, bilgi kuruluşlarının Bilgi Teknolojisi yönetişimine ve kontrol çerçevelerine uyum sağlamaları için gerekli olan kapsamlı kaynakları içeren bir modeldir. COBIT, bilgi teknolojisi kullanımından doğan riskleri tespit eder. Bu model, bilgi teknolojisi güvenliğindeki önemli risklere karşı ana kullanıcıların, küçük ve orta ölçekli işletmelerin, idarecilerin ve büyük kuruluşların yönetim kurulu üyelerinin kolaylıkla uygulayıp, takip edilebilecekleri işlemlerin üzerinde yoğunlaşır.

3.1. COBIT Bilgi Güvenliği Unsurları:

COBIT Bilgi Güvenliği; arka planın başarıyla okunması, COBIT esaslı güvenlik dayanağı, teknolojik güvenlik risklerinin özetini içeren ek olmak üzere üç unsurdan oluşmaktadır.

Yüzde yüz güvenlik diye bir şey yoktur ama modeldeki tavsiyeleri takip ederek, güvenlikle ilgili riskler hakkında bilinci arttırarak çok etkili seviyede güvenlik sağlanabilir.

Bilgi teknolojisi ortamı değişmeye devam etmektedir ve dolayısıyla yeni güvenlik riskleri ortaya çıkmaktadır. İyi bir güvenlik sağlamak büyük miktarlarda zaman ve para

harcamakla gerçekleştirilmez. Bilgi teknolojisi kullanılırken bilincin arttırılması, gerçekleşebilecek risklerin belirlenmesi ve hassas önlemlerin alınması çok az gayretle gerçekleştirilebilir. Bu model, kontrolün her safhasında ortaya çıkabilecek tüm riskleri teşhis etmez ama ne yapılması gerektiğini ve nasıl yapılması gerektiğini anlama yeteneğini geliştirir.

İyi bir bilgi güvenliği sadece riskleri azaltmaz. İyi güvenlik, işletmenin bağlantıda bulunduğu diğer işletmeler üzerindeki itibarı, güveni de arttırır, zaman kaybını önleyerek etkinliği arttırır.

3.2 Bilgi Güvenliğinin Tanımı:

Bilgi güvenliği, değerli varlıkların kaybedilmesi, yanlış kullanılması, ifşa edilmesi ve zarar görmesini önlemekle ilgilidir. Değerli varlıklar; kaydedilen, işlenen, saklanan, paylaşılan, elektronik ortamda gönderilen bilgilerdir. Bu bilgiler tehditlere karşı korunmalıdır. Bilgi güvenliğinin amacı; bilgiyle ilgili olanları ve kullanılırlık, gizlilik, bütünlük unsurları ile ilgili başarısızlıklardan zarar görebilecek sistemleri bağlantıları korumaktadır.

İnternetin etkisi, internet üzerinden ekonominin büyümesi elektronik işlemlere güvenme ihtiyacını doğurmuştur.

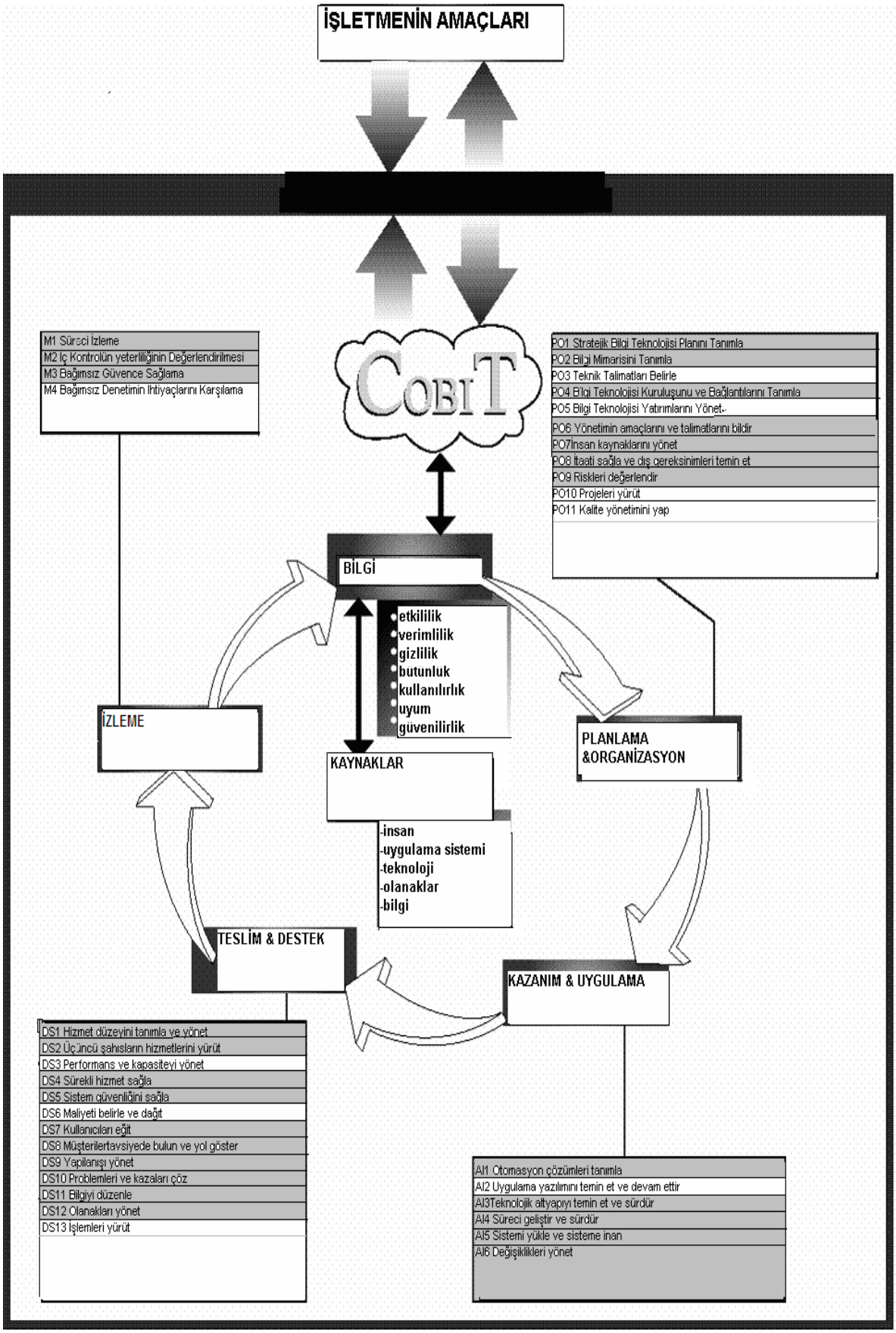
4.3 Bilgi Güvenliği Neden Önemlidir?

Bilgi teknolojisi günlük yaşamın ve iş hayatının ayrılmaz bir parçasıdır ve bilgi teknolojisine bağımlılık giderek artmaktadır. Yeni teknolojiler işlevselliği arttırırken, yeni riskler kontrol edilmesi güç sonuçlar doğurur. İnternet ağının yaygın kullanılması, bireylerin kişisel bilgileri ve şirketlerin gizli bilgilerinin güvenliği hakkında daha fazla endişelenmelerine neden olmaktadır.

4.4. COBIT Güvenlik Dayanağı: Güvenlik İçin 39 Adım

Bilgi güvenliği teknik önlemlerden ziyade davranışlarla ilgilidir. Kurumların güvenlik alanında gerekli adımları atmasına yardımcı olmak için COBIT bir güvenlik dayanağı tasarlanmıştır. Bu dayanak, güvenlikle ilgili en önemli hedefleri COBIT ’den almaktadır. Dayanak, 34 kontrol sürecinin planlama-organizasyon, kazanım-uygulama, teslim-destek, izleme olmak üzere dört gruba ayrıldığı COBIT çerçeve kontrol modelini kullanılır. Kilit

kontrol amaçlarını, gerekli minimum kontrol adımlarını, COBIT sürecini ve detaylı COBIT kontrol amaçlarını içerir. Daha güvenli kontrol için 39 adım içerir. Dayanakta, ISO17799'daki kontrol amaçları da kullanılır. COBIT, ISO 17799'dan daha üst düzeydedir.



Koyu renkli olan kontrol amaçları güvenlikle ilgili kontrol amaçlarıdır.

Bu model, COBIT ’in güvenlikle ilgili kontrol amaçlarının her biri için oluşabilecek riskleri ve güvenliği sağlamak için gerekli önlemleri belirtilir. Model, kontrol amaçlarının her biriyle ilgili güvenliğin sağlanması amacıyla 39 adımdan oluşur:

1) Bilgi, hizmet ve işlemlerin doğruluğunun ve uygunluğunun tespiti, güvenlik gereksinimlerinin göz önünde bulundurulması,
2) Güvenlik yönetimi için spesifik sorumlulukların tanımlanması,
3) Sürekli iletişim halinde bulunulması, güvenlik gereksinimlerinin yerine getirilmesi için gerekli kuralların düzenli olarak görüşülmesi,
4) Personeli işe alırken referans bilgilerin doğruluğunun kontrol edilmesi,
5) Kuruluşların güvenlik gereksinimlerini yerine getirmek için gerekli kalifiye elemanların işe alınması ve yetiştirilmesi,
6) Ana güvenlik hizmetlerinin tek bir kaynağa bağlı olmamasının garanti edilmesi,
7) Gizliliğe, fikir haklarına, diğer yasal, düzenleyici sözleşmeye dayalı ve sigorta gereksinimlerine uyulması için gerekli güvenlik yükümlülüklerine ilişkin yapılmasına ihtiyaç duyulan şeylerin belirlenmesi,
8) İşletmenin başarısı için gerekli bilgi, hizmet ve işlemlerin güvenliğinin sağlanması, en önemli riskleri belirten risk yönetimi faaliyet planının hazırlanması,
9) Tanımlanmış güvenlik risklerinin yönetimi için gerekli maliyet-etkin araçlara olan ihtiyacın, tüm personel tarafından anlaşılmasının sağlanması,
10) Otomasyon çözümlerin etkinliğinin, fonksiyonelliğinin değerlendirilmesi,
11) Teknolojik altyapının otomasyon güvenlik uygulamalarını desteklemesinin sağlaması,
12) Teknolojik altyapıyı korumak için gerekli ilave güvenlik gereksinimlerinin göz önünde bulundurulması,
13) Kaynakların güncelliğinin korunması için tanımlanması ve kontrol edilmesi,
14) Güvenliği bütünleştirmek için uygulanması gereken günlük prosedürün tüm çalışanlar tarafından bilinmesinin sağlanması,
15) Fonksiyonel ve operasyonel güvenlik gereksinimlerine karşı sistemin test edilmesi,
16) İşletmenin amaçları ve güvenlik gereksinimlerine karşı test sonuçlarının değerlendirilmesi ve güvenlik onayının verilmesi,
17) Tüm değişikliklerin değerlendirilmesi,
18) Tüm değişikliklerin kaydedilmesi,
19) İşletmenin güvenlik gereksinimlerini yerine getirmesinin sağlanması,

20) Üçüncü kişilerin profesyonel kapasitelerinin değerlendirilmesi ve işletmenin güvenlik gereksinimleri için gerekli temasın sağlanması,
21) Güvenlik gereksinimleri için işletme dışı tedarikçilere olan bağımlılığın dikkate alınması,
22) Kritik işletme fonksiyonlarının, bilgilerin ve kaynakların tanımlanması, hizmetlerin sürekliliğinin sağlanması için kaynakların kullanılırlığının arttırılması,
23) Bilgi teknolojisi hizmetlerinin korunması ve yeniden yapılandırılması için gerekli temel ilkelerin belirlenmesi,
24) İşletmenin gelişimini desteklemek için yedek kaynakların ayrılması, düzenli aralıklarla kontrol edilmesi, tamamlanması,
25) Müşterilerin, hizmet sunanların, tedarikçilerin bilgilere erişiminin gerçekleştirilmesi,
26) Bütün kullanıcı hesaplarının ve güvenlik işaretlerinin yönetimi için sorumlulukların dağıtılması,
27) Önemli güvenlik ihlallerinin günlük izlenmesi ve ortaya çıkarılması,
28) Karşı tarafın güvenilir olduğunun ve elektronik ortamda yapılan işlemlerin güvenilir olduğunun temin edilmesi,
29) İşletmenin altyapısında virüs koruma yazılımlarının kullanılmasının sağlanması,
30) Kuruluşa hangi bilgilerin gelebileceği ve kuruluştan hangi bilgilerin çıkabileceği hakkında politikaların tanımlanması, ağ güvenlik sistemlerinin yapılandırılması,
31) Bilgi teknolojisi donanım ve yazılım yapılanışında düzenli olarak güncellenmiş, eksiksiz envanter sağlanması,
32) Tesis edilmiş yazılımın ruhsatlı ve yetkili olup olmadığının düzenli olarak gözden geçirilmesi,
33) Bilginin doğruluğunun, eksiksizliğinin, geçerliliğinin, bütünlüğünün çeşitli kontrollere tabi tutulması,
34) Önemli bilgilerin sadece yetkili kişilere dağıtılması,
35) Girdi ve çıktı dokümanları, bilgi, yazılım için saklama süresinin, belgelere dayalı gereksinimlerin, depolama dönemlerinin tanımlanması,
36) Bilgi teknolojisi olanaklarının, varlıkların özellikle güvenlik tehdidi riskine karşı korunması,
37) Bilgisayar ağ sistemlerinin ve depolama teçhizatlarının çalınmaya, hasara, kaybolmaya karşı korunması,

38) Çalışanların düzenli aralıklarla güvenlik kontrollerinin yeterliliğini değerlendirmesi, güvenlik istisnalarını gözlemlemesi, güvenlik mekanizmalarının işlerliğini değerlendirmesi, önemli kontrollere uyumu sağlaması,

39) Bilgi güvenliği kontrol mekanizmalarının gözden geçirilmesi; bilgi güvenliği ile ilgili yasalara, düzenlemelere, sözleşme yükümlülüklerine uyumunun sağlanması için yetkili dış kaynakların sağlanması.

Bu 39 adımda bilgi teknolojisi güvenliğinin sağlanması amaçlanmaktadır.

5. Sonuç

COBIT, "bilgi ve ilgili teknoloji için kontrol amaçları" yaklaşımıdır ve ulaşılmak istenen kontrol amaçları ve bu amaçlara ulaşmak için gerekli yollar tarafından tasarlanan kontroller olarak tanımlanan iç kontrol odaklı bir yaklaşımdır. COBIT süreç değil kontrol esaslıdır. COBIT, iş süreç sahiplerinin bilgi sistem kontrol sorumluluklarını etkin ve etkili şekilde yerine getirmelerini sağlayan bir modeldir.

COBIT, bilgi teknolojisinin organizasyonun ayrılmaz parçası olduğunu, kontrol hedefleri üzerinde yoğunlaşmanın iç kontrolün kullanılması ve uygunluğunu güçlendirdiğini, değerlendirmenin iç kontrol için olmazsa olmaz önem taşıdığını, kontrol ve değerlendirmenin iç kontrol sisteminin ayrılmaz parçası olduğunu kabul eder.

COBIT, bilgi teknolojisi yönetişim hedeflerini destekler, bilgi teknolojisi süreçlerinin tanımlanmasını sağlar, kontrol hedefleri üzerinde yoğunlaşılmasını sağlar, maliyet etkinliği olan bilgi teknolojisi hizmetlerinin sunulmasını sağlar, işletmenin iç ve dış denetçilerden daha iyi yararlanmasını sağlar, bilgi teknolojisi yönetimi ve bilgi teknolojisi kontrolleri için en iyi uygulama noktalarını belirler. Organizasyonun kurallara, düzenlemelere, yükümlülüklerine uymasını sağlar. Uygun iç kontrollerin değerlendirme, algılama ve uygulamalarını kuvvetlendirir. Risk değerlendirmesi ve risk yönetimi için uygun bir çerçeve sağlar.

COBIT, başarıyla ve gereğiyle uygulandığı takdirde işletmenin hedeflerini en etkin ve yanlışsız şekilde ulaşmasına yardımcı olacak bir kontrol modelidir. Bilgi teknolojisinin işletmenin gereksinimlerini yerine getirmek konusunda başarılı olmasını amaçlar. Kamu kesiminde kullanılması için ciddi altyapı çalışmalarının yapılması gerekir ki bu oldukça maliyetli bir işlemdir ve tüm kamu kurumlarının katkısını sağlamak güç olabilir.

Kaynaklar

www.isaca.org

www.ITgovernance.org

www.sox-online.com

www.theiia.org/itaudit

www.kpmg.com

www.isaca.org/ COBIT Security Baseline