IJMA International Journal of Management and Administration

Year:2, Volume:2, Number:3 / Yıl:2, Cilt:2, Sayı:3, 2018

DOI Number: 10.29064/ijma.409421

COBIT VE COSO İÇ KONTROL YAKLAŞIMLARININ KARŞILAŞTIRILMASI

COMPARISON OF COBIT AND COSO INTERNAL CONTROL APPROACHES

Kadir GÖKOĞLAN[1]

ÖZET

COSO tarafından geliştirilen yaklaşım, iç kontrol ve işletmelerin yönetim konularına odaklanarak finansal raporlamaların kalitesini arttırma amacını taşımaktadır. Bu yaklaşımların en önemlisi olarak görülen COBIT iç kontrolün tanımlanması, raporlanması, geliştirilmesi alanlarında bilgi teknolojilerinin yönetişimini ifade etmektedir. COBIT, uygulayıcıların odağında görünmesine rağmen, genellikle akademik olmayan araştırmalarda kullanılmaktadır. Çünkü akademik araştırmacılar tarafından yoğun inceleme alanları arasında yer almamaktadır. Bu nedenle mevcut literatürde yer alma ihtiyacı doğmaktadır (Bernrioder ve Ivanov, 2011: 325). COBIT'in kontrol tanımını ve kaynak dokümanlarını COSO'dan aldığı bilinmektedir. Çalışma sonucunda COBIT, COSO iç kontrol çerçevesinin bir yedeği değil ama bugünün bilgi teknoloji merkezli dünyasında iç kontrolleri belirlemek için farklı bir yol olarak kullanıldığını ve COBIT ve COSO iç kontrol çerçevelerini belgeleme ve anlaşılmaları için önemli bir destek aracı olarak görüldüğü belirlenmiştir. Bu çalışmada iç kontrol alanındaki yaklaşımlardan COBIT ile COSO arasındaki benzerlik ve farklılıklar incelenmiştir. Bu amaçla yapılan bu çalışma akademik olarak literatürde yer alması ve gelecekte yapılacak akademik çalışmalara ışık tutmak amacıyla yapılmaktadır.

Anahtar Kelimeler: COBIT, COSO

Jel Kodu: M40, M42, M49

ABSTRACT

The approach developed by COSO is aimed at increasing the quality of financial reporting by focusing on internal control and management issues of enterprises. COBIT, seen as the most important of these approaches, represents the governance of information technologies in the areas of identification, reporting and development of internal control.

COBIT, Although it does appear in the focus of practitioners, it is often used in non-academic research. This is because it is not among the areas of intensive investigation by academic researchers. For this reason, there is a need to take part in the current literature (Bernrioder and Ivanov, 2011: 325). It is known that COBIT received control descriptions and source documents from COSO. As a result of the study, COBIT is not a supplement to the COSO internal control framework, but is used as a different way to identify internal controls in today's IT-centric world and COBIT and COSO have been identified as important support understanding internal control frameworks.

[1] Öğr. Gör. Dicle Üniversitesi, Sosyal Bilimler Meslek Yüksekokulu, Muhasebe ve Vergi Uygulamaları Bölümü, kadir.gokoglan@dicle.edu.tr

In this study, the similarities and differences between COBIT and COSO were examined from the approaches in the field of internal control. This study for this purpose has been done academically to take place in the literature and to shed light on academic studies to be done in the future.

Keywords: COBIT, COSO

Jel Codes: M40, M42, M49

1. GİRİŞ

Son zamanlarda dünyanın birçok ülkesinde merkezi kontrol yaklaşımından iç kontrol yaklaşımına ağırlık verilmeye başlanılmış ve iç kontrol kavramının önemi artmıştır. İlk olarak özel sektörde kullanılmaya başlanılan ve daha sonra kamu sektöründe de bir yönetim aracı olarak uygulanılmaya başlanılan COSO iç kontrol yaklaşımı zamanla gelişmiştir. İlerleyen dönemlerde teknoloji ve diğer faktörlerin gelişimiyle birlikte bilgi teknolojilerin öneminin artmasına neden olmuş ve bu kavram araştırmacıların dikkatini çekmeye başlamıştır. COSO iç kontrol yaklaşımına ek olarak hem bilgi teknolojileri odaklı denetim yaklaşımı ve hem de iş odaklı kontrol modeli arasında köprü görevi yapacak olan COBIT modeli geliştirilmiştir (Grembergen, 1997: 17-18).

İç kontrol sistemi, giderek daha önemli bir kurumsal yönetişim, operasyonları destekleme mekanizması, stratejileri ve kurumsal performansın başarılı süreçleri desteklemesi ve gerçekleştirmesi için temeller belirlemektedir (Sarens ve De Beelde, 2006: 5). Aynı zamanda iç kontrol sistemleri kapsamı geniş iş ve kurumsal risk kontrolü dahil yüksek kalitede finansal raporlamanın sağlanmasında önemli bir rol almaktadır (Brown vd., 2014: 1). İç kontrol çerçeveleri, bir işletmenin denetimlerini anlamak ve kontrollerin etkinliği hakkında yargıda bulunmak için temel sağlamaktadır (Cereola ve Cereola, 2011: 521). En etkili bilgi teknolojileri kontrol çerçevelerinden birisi olarak bilinen COBIT, organizasyon ile bilgi teknolojilerinin uyumlaştırması temel amacı ile bilgi sistemleri ile teknoloji yönetişimi ve kontrol süreçleri için önerilen en iyi uygulamaları sağlamaktır (Rubino ve Vitolla, 2014: 737).

2. COBIT KAVRAMI

COBIT, işletmelerin ihtiyacı olan bilgi ve ilgili teknolojiler için kontrol hedefleri ve bilgi teknolojileri yönetiminde ulaşılması gereken hedefleri ortaya koymak olarak tanımlanmaktadır (Işkın, 2012: 77; Peker, 2008: 7; Akyol, 2013: 57; Hacısüleymanoğlu, 2010: 16; Topkaya, 2011: 27; Güneş vd., 2013: 2; Üvey, 2009; Pekel vd., 2008: 21). COBIT başlangıçta iyi uygulamalardan oluşan bilgi teknolojileri için yeterli güvenlik ve kontrol kriterleri olarak geliştirilmiş ve daha sonra bir çerçeve haline geliştirilmiştir (Khadra vd., 2009: 311-312; Tuttle ve Vandervelde, 2007: 243). Aynı zamanda bilgi teknolojileri yönetişiminin iyileştirilmesi, risklerin azaltılması, bilgi teknolojileri değer teslimi ve stratejik uyum olgunluk değerlendirmelerinde çok iyi bilinen bir çerçevedir (Guldentops, 2004; Ridley vd., 2004: 1; Simonsson ve Jhonson, 2006: 7; Sallé ve Rosenthal, 2005: 3-4; Simonsson vd., 2007: 1279).

COBIT özellikle mevcut bilgi teknolojileri yönetişim sorunlarını çözmek için tanınmış uluslararası denetim çerçevesini temsil etmektedir. (Bernrioder ve Ivanov, 2011: 326). Ayrıca, beklenilmeyen durumların önlenebilinmesi ve düzenlenmesi için makul bir

güvence sağlama, iş hedeflerinin geliştirilmesi ve uygulanabilirliğinin arttırılması amacıyla oluşturulan kurallar ve uygulamalar çerçevesi olarak tanımlanmak mümkündür (Artinyan, 2009: 1; Işkın, 2012: 79).

Bir değerlendirme çerçevesi olarak ISACA tarafından tasarlanmış ve oluşturulmuş (Bowen vd., 2007: 193; Simonsson vd., 2007: 1279), ilk olarak ISACF (Guldentops, 2004: 277; Khadra vd., 2009: 312) ve ITGI tarafından yayımlanmış olan (Pederiva, 2003: 1; Simonsson vd., 2007: 1279) COBIT, daha sonra bilgi işlem ve iş yönetiminde de kullanılmaya başlanılmıştır. COBIT, ulaşılmak istenen kontrol amaçları ve bu amaçlara ulaşmak için gerekli yollar tarafından tasarlanan kontroller olarak tanımlanan iç kontrol odaklı bir yaklaşımdır. Ayrıca pek çok ülkede bilgi teknolojileri kontrol siteminin değerlendirilmesi, yönetimi ve kuruluşların güvenliğini sağlamak amacıyla yöneticiler, iç ve dış denetçiler tarafından kullanılmaktadır (Kerr ve Murthy, 2011: 591; Ridley vd., 2004: 2; Uzunay, 2007: 3).

COBIT, bilgi teknolojileri yönetişim üzerinde belirli bir odak noktası sağlayan en olgun modellerden biridir (Pederiva, 2003: 1-2; Huang vd., 2011: 406). Süreç esaslı olarak çalışmayıp kontrol esaslı olarak işletme faaliyetlerine katkı sağlamaktadır. Bununla birlikte işletmelerin başarılı olması için yapması gereken faaliyetler üzerinde dururken, bu faaliyetleri nasıl yapacağı konusuyla ilgilenmemektedir (Uzunay, 2007: 3). İşletme yöneticileri ve denetçiler ön plvea olmak üzere bilgi teknolojileri kullanıcılarına ihtiyaçlarını karşılayacak, modern bilgi teknolojileri kontrol araçlarını araştırmak, geliştirmek ve ilerletmeyi misyon edinmiştir (Uzunay, 2007: 5; Akyol, 2013: 57).

1996'da ilk kez yayınlanan COBIT, birçok ülkede yayınlanmakta denetim, kontrol, yönetim ve nihayetinde yönetişim kavramlarını kapsamakta ve (Pekel vd., 2008: 21; Işkın, 2012: 80; Ridley vd., 2004: 2), güncellenerek 1998'da 2., 2000 yılında 3., 2005 yılında 4., 2005 yılında ise 4.1. (Peker, 2008: 7; Akyol, 2013: 58; Artinyan, 2009: 2; Hacısüleymanoğlu, 2010: 17; Özcan, 2009: 61; Topkaya, 2011: 28; Üvey, 2009; Kutsikos ve Bekiaris, 2007: 38) ve son olarak da 5. versiyonuna ulaşmış olan bir stvearttır. COBIT 5 çerçevesi beş prensip ve yedi sağlayıcı ile yönetişimin zorluklarını kolay hale getirmektedir. Ayrıca COBIT çerçevesi, özellikle COBIT 5 versiyonu ile birlikte, Bilgi Teknolojileri yönetişim ve yönetim süreçleri ile ilgili net bir ayrıma gitmiştir. Bu husus iç denetçinin kontrollerin niteliğini doğru algılayabilmesi açısından önem arz etmektedir (Hatipoğlu, 2014: 21). COBIT 5; COSO, ITIL, Sarbanes-Oxley Mevzuatı ve Basel III gibi birçok yaklaşım ve stveartları dikkate alarak çerçevesini oluşturmaktadır (Meadows, 2014; Ridley vd., 2004: 2).

COBIT, bilgi teknolojilerini profesyoneller ve şirket yöneticilerinin kaynak kullanımını (Bowen vd., 2007: 193) optimize etmede ve ileride meydana gelebilecek muhtemel olan olumlu (yarar) veya olumsuz (riskler) durumlar arasında bir denge sağlamayı amaçlamaktadır. Basit bir denetim aracı olarak ortaya çıkarılmış, COBİT 1 ve COBİT 2 kontrol temelli, COBİT 3 yönetim temelli ve COBİT 4 bilgi teknolojileri yönetişim temeline dayanılarak hazırlanmış olup, COBİT 5 ile kurumsal bilgi sistemleri yönetimin bir aracı haline gelmiştir (Rubino ve Vitolla, 2014: 750). Ayrıca, işletmeler için değer yaratmak, bilgi ve teknoloji merkezi rolünü yansıtan yönetim ve kurumsal bilgi teknolojileri yönetiminin varlığını ortaya çıkarmış (Verew, 2012: 1) ve risk odaklı bileşenler için bir rehber olarak COBIT 5 risk görünümünü geliştirmeyi amaçlamaktadır (Steven, 2012).

COBIT, yönetim ve kontrol çerçevesi için kritik bilgiler sağlayan ve bilgi teknolojileri yönetişimi kontrolleri ve güvenilirliği için bir kontrol sistemidir (Huang vd., 2011: 411). Tuttle ve Vandervelde (2007) tarafından oluşturulan COBIT çerçevesinin kavramsal modelini ve bilgi teknoloji kontrollerini değerlendirirken denetçilere yararlı olabilecek modeli ortaya çıkarmıştır. Ayrıca Rozek (2008) bilgi teknolojileri kontrolleri ve iç kontrol durumunu kaydetmek için standart bir yol sağlayarak COBIT'in genel tutum değerlendirmesinde denetçilere yardımcı olabileceğini savunmuştur. Yine gerçekleştirilen bazı araştırmalarda COBIT ile SOX'un uygunluk amacıyla geçerli bir çerçeve oluşturduğu belirlenmiştir (Rubino ve Vitolla, 2014: 754; Abu-Musa, 2008: 444).

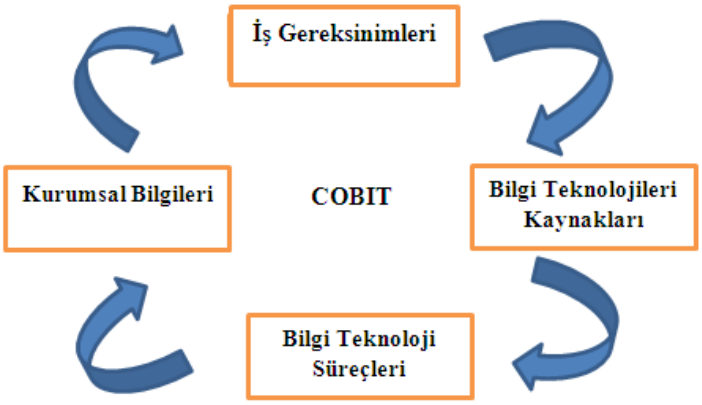
Proje yönetimi, performans değerlendirme ve ampirik doğrulama için model geliştirme ve performans göstergelerinin daha kapsamlı bir model sunmasının yanında (Bryde, 2003: 229) bazı ek parametreleri de sağladığı yapılan araştırmalarla kanıtlanmıştır. Ayrıca Henderson ve Lee'nin 1992 yılında yapmış olduğu bir çalışmada yönetim kontrolü ve proje yönetimi performansının benimsenmesi oranları arasında pozitif bir ilişkinin olduğu saptanmıştır (Bernrioder ve Ivanov, 2011: 325).

ITIL ve COBIT en yoğun çalışılan şirketler tarafından bilgi teknolojileri yönetişim sürücüleri olduğu belirtilmiştir. Bilgi teknolojileri altyapısının yönetimi için özel olarak geliştirilen ve birçok şirket de bilgi teknolojileri yönetişim uygulanması için bir rehber olarak bu iki model kullanıldığı belirtilmiştir. COBIT dört büyük etki alanlarıyla (planlama ve organizasyon, satın alma ve uygulama, teslimat ve destek ve izleme) farklı süreçlerin kontrolünü vurgulamaktadır. COBIT ve ITIL gibi bilgi teknolojileri yönetişim mekanizmaları işletmeleri izleme ve iç kontrol faaliyetlerinde yardımcı olmakla birlikte bilgi teknolojilerin altyapısı, verimliliğini ve iç, dış kalitesini arttırmaktadır (Guldentops vd., 2004: 27; Lunardi, 2015: 74). Bilgi teknolojileri işletmelerin faaliyet giderlerine karşı almış olduğu önlemlerle maliyeti düşürmeye yol açmaktadır. Bununla birlikte, istatistiksel olarak bu avantajları doğrulamak mümkün değildir (Lunardi, 2015: 77).

3. COBIT ÇERÇEVESİ

COBIT iç kontrol çerçevesi; kurumsal bilgi teknolojilerinin üzerinde durularak iç kontrolleri değerlendiren anlama ve rehberlik görevlerini yapmaktadır. Bilgi teknolojileri yönetiminin anahtarı olan COBIT'in konsepti SOX'tan önce elementlerinin önemi daha az vurgulanmaktayken, bugün ise ITGI'nın güçlü liderlik rolünün sayesinde önemi artmıştır. COBIT tanımlamasının en basit şekli stratejik işbirliğinde hem risk hem de performans ölçümü bilgi teknolojilerinin önemli bir anahtarını oluşturmaktadır (Moeller, 2009: 114).

Şekil 1: Basit COBIT Formatı



Kaynak: (Moeller 2008: 123; Moeller, 2009: 93; Ak, 2012: 41)

COBIT'in temel prensipleri, Şekil 1'de görüldüğü üzere dörde ayrılmaktadır. Bu prensipler; iş gereksinimleri, bilgi teknolojileri kaynakları, bilgi teknoloji süreçleri ve kurumsal bilgilerden oluşmaktadır. İş gereksinimleri prensibinin oluşmasında etkinlik, verimlilik, gizlilik, bütünlük, erişebilirlik, uyumluluk ve güvenilirlik ölçüleri önemli bir yer almaktadır (Tuttle ve Vveervelde, 2007: 243). Bilgi teknoloji kaynaklarını uygulama, bilgi, altyapı (teknoloji) ve insan (olanaklar) oluşturmaktadır. Bilgi teknoloji süreçlerini ise etki alanları, süreçler ve faaliyetler oluşturmaktadır (Moeller, 2008: 124; Moeller, 2009: 94).

Öncelikle bu süreçlerde bilgi teknolojileri kullanımı ile risk ve kaynak optimizasyonu sağlamaktadır. Bu süreçler, bilgi teknolojilerini kullanan şirketlerin başarılı bir yönetim için gerekli olan şirketin misyonu, amaç ve hedeflerine ulaşmak için sorumlulukların net ve etkili bir şekilde belirlenmesini sağlayan ilke, süreç ve uygulamaları korumayı ifade etmektedir. Bu etki sayesinde COBIT, kontrol ortamına, kontrol faaliyetlerine ve risk değerlemesi bileşenlerini destekleyen bazı faaliyetler, ölçüler ve ayrıntılı bilgi teknolojileri kontrol hedeflerini geliştirmeyi gerektirmektedir (Rubino ve Vitolla, 2014: 755).

Bilgi teknolojileriyle ilgili bir dizi çerçeveler, standartlar ve belgeler varken, COBIT'in birincil odak noktası örgütsel hedeflere ulaşmada bilgi teknolojilerini kullanımıdır (Lainhart, 2000: 21-22). Kontrol hedefleri iş ve bilgi teknolojilerinin uyum sağlamada yardımcı olmak için tasarlanmıştır. Çerçevede bilgi ve bilgi teknolojilerini desteklemeyi tüm yönleriyle dikkate aldığı gibi, yönetimin bilgi teknolojileri için uygun bir kontrol sistemi sağlamaya yardımcı olmak için COBIT kullanılmaktadır (Ridley vd., 2004: 2).

COBIT modeli spesifik ve detaylı kontrol hedefleriyle ilişkili 32 bilgi teknolojisi süreçlerine sahipken (Grembergen, 1997: 22) günümüzde 34 bilgi teknolojisi süreçlerine ve 4 etki alanına sahiptir (Solm, 2005; Peker, 2008: 9; Akyol, 2013: 70; Hacısüleymanoğlu, 2010: 17; Özcan, 2009: 65; Uzunay, 2007: 6; Topkaya, 2011: 28; Güneş vd., 2013: 3; Herz vd., 2013: 239; Üvey, 2009; Bowen vd., 2007: 193; Guldentops, 2004: 278; Simonsson ve Jhonson, 2006: 7; Sallé ve Rosenthal, 2005: 4; Simonsson vd., 2007: 1279; Hardy, 2006: 59; Lainhart, 2000: 22; Guldentops vd., 2004: 13). Bu etki alanları; Planlama ve Organizasyon, Tedarik ve Uygulama, Hizmet ve

Destek ile İzleme ve Değerlendirme ve alt başlıklarından oluşmaktadır. Özellikle bu 34 bilgi teknolojileri süreçleri ve 4 etki alanlarına odaklanarak bilgi teknolojileri kontrol ve güvenlik süreçleri dahilinde güvenilir finansal raporlama yapılabilmektedir (Kerr ve Murthy, 2011: 591).

Planlama ve organizasyon süreci; işletmelerin hedeflerine ulaşmada ihtiyacı olan strateji ve taktikler ile bilgi teknolojisinin iş hedeflerini gerçekleştirmesi amacına maksimum katkıyı sağlamasının yollarını belirtmektedir (Özcan, 2009: 69; Ak, 2012: 42; Güneş vd., 2013: 4). Tedarik ve uygulama süreci; tanımlanan, geliştirilen, uygulanan, iş sürecine adapte edilen bilgi teknolojisi çözümleri, var olan sistemlerin değiştirilmesi ve sürdürülmesi faaliyetlerinden oluşmaktadır. Hizmet 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 ve değerlendirme süreci; bütün bilgi teknolojisi süreçlerinin, kaliteleri ve kontrol gereksinimlerine uyumu açısından düzenli olarak gözden geçirilmesi faaliyetlerini gerektirmektedir (Özcan, 2009: 69-72; Ak, 2012: 42-50; Güneş vd., 2013: 4).

4. COSO VE COBIT YAKLAŞIMLARININ KARŞILAŞTIRMALARI

Bilgi teknoloji kontrollerinin kullanımı ve izlemesini sağlayarak, bilgisayar vb araçlara bağımlılığıyla başa çıkma ile ilgili çerçevenin etkinliği ve geçerliliği çok çeşitli çalışma ve araştırmalarla ispatlanmıştır Bu yapısal çerçeve sayesinde yöneticilerin ayrıntılı bilgi teknolojileri denetim testleri sağlamamıza olanak tanımaktadır. Bu şekilde COBIT, COSO tarafından sağlanan sınırlı rehberlik ve yöneticiler ve denetçilerin bilgi teknolojileri ile SOX'un uyumluluğu (Hardy, 2006: 58) için kontrol değerlendirmelerine yardımcı olmaktadır (Rubino ve Vitolla, 2014: 754).

COSO çerçevesi iç kontrol için genel bir değerlendirme çerçevesi olarak kabul edilirken (Protoviti, 2014), COBIT genellikle teknoloji üzerinde belirli kontrolleri dikkate alan ve aynı zamvea yararlı rehberlik ve arka plana malzeme sağlamaya yöneliktir. Kısacası COBIT, bilgi sistemlerinin yönetimi üzerinde durmaktadır. Sonuç olarak, öncelikle bilgi teknolojileri ile ilgili finansal raporlama sorunlarını azaltmayı hedeflemektedir. Yani, COSO gibi belirli bir iç kontrol çerçevesine entegre fakat, bilgi teknolojileri sorunlarını azaltma veya ortadan kaldırmaya yönelik değerli bir araç olarak görülmektedir (Rubino ve Vitolla, 2014: 754-755).

COSO bileşenleri küpün dikey kısmından oluştuğunu, COBIT bileşenleri ise yatay kısmını oluşturduğu görülmektedir. Yatay kısımda COBIT bileşenleri olan bilgi teknolojileri süreçleri, iş hedefleri, kontrol açıklamaları ve kontrol süreçleri yer almaktadır. Dikey kısımda ise COSO bileşenleri olan kontrol çevresi, risk değerlendirme, kontrol faaliyetleri, bilgi ve iletişim ile izleme yer almaktadır.

COSO ve COBİT Piramidinin tabanını COBIT oluştururken, tepe kısmında ise COSO dikkate alınmaktadır. Ayrıca piramit üç aşamadan oluştuğu görülmektedir. Birinci aşamayı "Otomatik Uygulama Kontrolleri" oluştururken ve ayrıca piramidin tepe noktasında yer almaktadır. Birinci aşamada veri doğrulama, düzenli kontroller ve çıktı mutabakatı, ara yüz kontrolleri ve son kullanıcı güvenliği işlemleri yapılmaktadır. İkinci

aşamada "Genel Uygulama Kontrolleri" yapılmaktadır. Bu kontroller; sistem gelişimi, değişim kontrolü, veri kurtarma, veri tabanı yönetimi ve programlayıcı güvenliği başlıklarından oluşmaktadır. Son aşama olan üçüncü aşamada ise "Genel Bilgisayar Kontrolleri" yer almaktadır. Bu kontroller de; değişim ve yapılandırma yönetimi, ağ yönetimi, güvenlik yönetimi, veri merkezi operasyonları, veri tabanı yönetimi, olağanüstü durumlardan kurtulma ve 0/S yönetimi yer almaktadır. Kısacası piramidin tepe noktasını oluşturan COSO bileşenleri iç kontrolleri dikkate alırken, piramidin taban kısmını oluşturan COBIT bileşenleri bilgi teknolojilerinin işleyişini ifade etmektedir.

COSO ve COBIT kendi içerisinde bazı sınırlamaları mevcuttur. Bununla birlikte, bu sınırlamalar birbirlerini dengelemektedir. Birincisi, COBIT iyi sık sık uygulanması ve bilgi teknolojileri yönetişimi ve iç kontrol çerçeveleri yönetiminde zorluk küçük-orta büyüklükteki şirketlerinin yönetsel dinamiklerini yorumlamak için uygun olmadığını belirtmek gerekir. İkincisi, işletmeler yeni kontrol araçlarını kullanarak işletme sistemi üzerinde değişikliklere neden olmakla birlikte farkındalığın arttığı ve dolayısıyla işletme katma değerinin artışına neden olmaktadır (Rubino ve Vitolla, 2014: 754).

COSO bilgi teknolojilerine özgü riskleri ve karmaşıklığını ele olmamasına rağmen, bu COBIT tarafından ele alınmaktadır. COBIT bilgi teknolojilerinin varlığı içerisindeki süreçler iç kontrol sistemini güçlendirmeye yardımcı olmaktadır. Bununla birlikte, COSO'nun çerçevesini oluşturan beş bileşene dayalı olmak zorundadır. Bu nedenle COBIT, COSO'nun bir alternatifi değildir. Fakat finansal raporlamanın kalitesini arttıran, olumsuzlukları azaltan veya ortadan kaldıran tamamlayıcı bir çerçeve olarak görülmektedir (ITGI, 2005, 2007).

Bilgi teknolojileri genel kontrolleri literatürde (COSO'ya göre) en dar anlamıyla; uygulama sistemlerinin geliştirilmesi ve bakımına ilişkin kontroller, sistem yazılımı kontrolleri, erişim güvenliği kontrolleri ve veri merkezi operasyonlarına ilişkin kontrol unsurlarını kapsamaktayken (Hatipoğlu, 2014: 23), COBIT bütün bu kontroller ve diğer bilgi teknolojileri kontrollerini dikkate almaktadır.

İç denetçilere göre; SOX için bilgi teknolojileri kontrol hedeflerini COBIT daha fazla açıklamaktadır. Ayrıca bilgi teknolojilerin yüksek konsantrasyonu COSO'nun "kontrol faaliyetleri ile bilgi ve iletişim" bileşenleri etrafında işlemektedir (Hardy, 2006: 58; Abu-Musa, 2008: 443). COSO'nun beş anlamsal kategoriye göre yapılanmış bileşenlerin aksine COBIT çerçevesi dört ana alanlarını içeren bir sistem içinde yaşam döngüsü yaklaşımı etrafında organize bir süreç modeline dayanmaktadır (Tuttle ve Vveervelde, 2007: 242-243).

Hem COSO bileşenleri hem de COBIT bileşenlerinin birbirleriyle olan ilişkisini tablo 1'de açık bir şekilde görmek mümkündür.

Tablo 1: COSO ve COBIT Bileşenlerinin İlişkisi

	COSO BİLEŞENLERİ				
COBIT BİLEŞENLERİ	**Kontrol Faaliyetleri**	**Risk Değerleme**	**Kontrol Ortamı**	**Bilgi ve İletişim**	**İzleme Faaliyetleri**
Planlama ve Organizasyon					

Stratejik Bilgi Teknolojileri Planının Tanımlanması		X		X	X
Bilgi Mimarisinin Tanımlanması			X	X	
Teknolojik Yönün Belirlenmesi					
Bilgi Teknolojileri Organizasyonu ve İlişkilerinin Tanımlanması	X			X	X
Bilgi Teknolojileri Yatırımlarının Yönetimi					
Yönetimin Hedeflerinin ve Talimatlarının İletilmesi	X			X	X
İnsan Kaynakları Yönetimi	X			X	
Kalite Yönetimi	X		X	X	X
Risk Değerlendirme		X			
Proje Yönetimi					
Tedarik ve Uygulama					
Otomasyon Çözümlerinin Belirlenmesi					
Uygulama Yazılımı Tedarik Edilmesi ve Bakımı			X		
Teknoloji Altyapısının Tedarik Edilmesi ve Bakımı			X		
İş ve Kullanımın Etkin Kılınması			X	X	
Bilgi Teknolojileri Kaynaklarının Sağlanması					
Değişiklik Yönetimi			X		X
Çözüm ve Değişikliklerin			X		

Kurulması ve Kabul Edilmesi					
Teslimat ve Destek					
Hizmet Seviyelerinin Tanımlanması ve Yönetimi	X		X		X
Üçüncü Parti Hizmet Yönetimi	X	X	X		X
Performans ve Kapasite Yönetimi	X		X		
Hizmet Süreklinin Sağlanması	X		X		X
Sistem Güvenliğinin Sağlanması	X		X	X	X
Maliyetlerin Belirlenmesi ve Bütçelenmesi	X		X	X	X
Kullanıcı Eğitimi	X		X		
Kullanıcılara Yardım ve Danışmanlık					
Konfigürasyon Yönetimi	X		X	X	
Problem ve Olay Yönetimi			X	X	X
Veri Yönetimi			X	X	
Fiziksel Çevre Yönetimi			X		
Operasyon Yönetimi			X	X	
İzleme ve Değerlendirme					
Süreç İzleme			X		X
İç Kontrolün İzlenmesi ve Değerlendirilmesi					X
Yasal Mevzuat ve Yönetmeliklerle Uyumun Sağlanması	X				X
Bilgi Teknolojileri					

Yönetişiminin Sağlanması					

Kaynak: (Moeller 2008: 145-146; Moeller, 2009: 115-116; Rubino ve Vitolla, 2014: 756-757)

Tablo 1 dikkate alındığında COBIT bileşenleri ile COSO "Kontrol Ortamı" bileşenin arasında yoğun bir ilişki olduğu dikkat çekmektedir. Kısacası "Kontrol Ortamında" yapılan faaliyetler genellikle COBIT çalışma alanını da kapsadığını söylemek doğru olacaktır. Yine "Bilgi ve İletişim "bileşeni COBIT'in faaliyet alanlarında önemli bir yer aldığı görülmektedir. Özellikle COBIT'in "Planlama ve Organizasyon" bileşeniyle çok fazla ortak noktalara sahiptir. Ayrıca COSO'nun "Kontrol Faaliyetleri" bileşeni ile COBIT'in "Teslimat ve Destek" bileşenlerinin ortak noktasının fazla olduğu görülmektedir. Fakat en dikkate çekici ilişki ise COBIT'in bütün bileşenleri neredeyse COSO'nun "Risk Değerleme" bileşeniyle fazla ortak noktasının olmadığıdır. Bunun en önemli sebebinin COBIT'in faaliyetleri daha çok bilgi teknolojilerin yönetişimi üzerine olmasından kaynaklanıyor olması ve COSO'nun aslında resmi bir risk yönetim modeli olarak kabul edilmesi bunu destekler niteliktedir. Yine tablo incelendiğinde COBIT'in bileşenlerinden "Teslimat ve Destek" bileşeni COSO ile aralarında en az ilişki olan ve "İzleme ve Değerlendirme Faaliyetleri" bileşeni en fazla ilişkili olan bileşen olarak görülmektedir. Son olarak bilgi teknolojilerin kontrolünün sağlandığı alanlarda COBIT ile COSO'nun ilişkisinin en az olduğu faaliyetler olarak görülmektedir. Çünkü COBIT için tekrarlamak gerekirse bilgi teknolojilerin denetimi, yönetişimi ve kontrollerinden oluşmaktadır. Sonuç olarak tablodaki belirlenen ilişkilerin yanı sıra her iki kontrol yaklaşımı birbirini destekler nitelikte olduğunu belirtmek doğru olacaktır.

5. SONUÇ

COSO çeşitli kuruluşlar tarafından resmi bir risk yönetim modeli olarak kabul edilmiştir. SOX ile birlikte önemi daha iyi anlaşılmaya başlanan dokümanlardan olan COBIT ise bir Bilişim Teknolojileri Yönetişimi çerçeve dokümanıdır ve yöneticilere, teknik konularla iş riskleri arasındaki ilişkileri anlamada yardımcı olmaktadır.

COBIT sadece bir denetim aracı değil aynı zamanda bir yönetişim aracı olma amacını da (Solms, 2005: 100) taşımaktadır. Bu nedenle yönetimden bilişim teknolojileri personeline kadar kurum içi ve dışında kurumun varlığı ve sağlıklı faaliyet göstermesi konusunda riskleri üstlenen çeşitli taraflara fayda sağlamayı da amaçları arasında gösterilmektedir. Aynı zamanda COBIT ile birlikte belirlenen iç kontroller ve güvenlik hedefleriyle işletmeler bu konulardaki farkındalıklarını arttırmıştır.

COBIT, COSO iç kontrol çerçevesinin bir yedeği değil ama bugünün bilgi teknoloji merkezli dünyasında iç kontrolleri belirlemek için farklı bir yol olarak bilinmektedir. Ayrıca, COBIT ve COSO iç kontrol çerçevelerini belgeleme ve anlaşılmaları için önemli bir destek aracı olarak görülmektedir. COBIT'in çerçevesi genellikle birbirine bağlı geniş beşgen şeklinde beş iç kontrol alanlarını tanımlarken, COBIT'in temel vurgulama alanı bilgi teknolojileri yönetiminin önemli temel kavramlarını oluşturmaktadır. Bu amaçla her iki kavram birbirine bağlı ve birbirini tamamlayan işlevlere sahiptir.

COBİT ve COSO yaklaşımları genel anlamda karşılaştırıldığında; COSO genellikle üst düzey hedefler, işletmenin misyonunu destekleyen bir uyum içerisinde stratejisini belirlerken, faaliyetler genellikle işletme kaynaklarının etkin ve verimli kullanılmasıyla oluşmaktadır. Aynı zamanda raporlamanın güvenliği ön planda tutulurken kanun ve yönetmeliklere tamamıyla uyum içerisinde olmaktadır. COBİT genellikle bilgi teknolojileri süreçlerinde kurulan ölçüm sonuçları tarafından oluşturulmaktadır. Etkin ve etkili iş faaliyetler, bilgi teknolojileri süreçlerinin yönetiminin ölçümü sonrasında oluşmakta, bilgi teknolojileri süreçlerin performans sonuçlarına göre operasyonlara odaklanmaktadır. Bilgi teknolojileri faaliyetlerinin ölçümleri sonucunda hedefler ortaya çıkarılmaktadır (Ivanyos ve Rooz, 2011: 5).

Yapılan araştırmalarda bugüne kadar bilgi teknolojileri özellikle operasyonel ve uygunluk denetimlerinde organizasyonlar tarafından yaygın bir şekilde kullanılmasına rağmen akademik olarak çok sınırlı ampirik ve teorik çalışmalarda yer almaktadır. Bu nedenle COBIT'de COSO iç kontrol yaklaşımı gibi literatürde akademik çalışmalarda yer alması gerekmektedir.

KAYNAKÇA

Abu-Musa, A.A. (2008), "Information technology ve its implications for internal auditing. An empirical study of Saudi organizations", Managerial Auditing Journal, Vol. 23 No. 5, pp. 438-466.

Ak, Mustafa, (2012), "(COBIT'in Yazılım Geliştirme Sürecinin İyileştirilmesine Uyarlanması", Gazi Üniversitesi, Bilişim Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, Mart, Ankara.

Akyol, Fatih, (2013), "COBIT (Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri) Uygulayan Şirketlerdeki Bilgi Güvenliği Politikalarının Şirket, Personel ve Süreçlere Etkileri", Beykent Üniversitesi Sosyal Bilimler Enstitüsü, İşletme Yönetimi Anabilim Dalı Yönetişim Bilişim Sistemleri Bilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, İstanbul.

Verew, Stekhoven, (2012), "Active Software Escrow's Usefulness for Companies Embracing COBIT 5", COBIT Focus, Vol. 2012 Issue 3, p4. http://www.isaca.org/Knowledge-Center/cobit/Documents/CF-Active-Software-Escrows-Usefulness-for-Companies-Embracing-COBIT-5.pdf.

Artinyan, Eliza Natasa. COBIT Çerçevesi, Deloitte /Makaleler, Çevrimiçi)http://www.denetimnetnet/UserFiles/Documents/Makaleler/ BT%20Denetim/COBIT%20%C3%87 er%C3%A7evesi.pdf. 23.11.2014.

Bernrioder, Edward W.N. ve Milen Ivanov, (2011), "IT Project management control ve the Control Objectives for IT ve Related Technology (CobiT) framework", International Journal of Project Management, 29, 325-336.

Bowen, P. L.,Cheung, May-Yin D., & Rohde, F. H. (2007), "Enhancing IT governance practices: A model ve case study of an organization's efforts", International Journal of Accounting Information Systems, 8, 191–221.

Brown, N.C.,Pott, C. ve Wömpener, A. (2014), "The effect of internal control ve risk management regulation on earnings quality: Evidence from Germany", Journal of Accounting ve Public Policy, Vol. 33 No. 1, pp. January–February 2014, Pages 1–31.

Bryde, D.J., 2003. Modelling Project management performance. International Journal of Quality&Reliability Management,20,2 ,229-254.

Cereola, S. ve Cereola, R.J. (2011), "Breach of Data at TJX: an instructional case used to study COSO ve COBIT, with a focus on computer controls, data security", Issues In Accounting Education, Vol. 26 No. 3, pp. 521-545.

Guldentops, E., W. V. Grembergen, ve S. De Haes, (2004), "Structures, Processes ve Relational Mechanisms for IT Governance", (Strategies for Information Technology Governance, Wim Van Grembergen, Idea Group Publishing), pp. 1-36.

Guldentops, E., (2004), "Governing Information Technology Through COBIT", IT Governance Institute, USA, (Strategies for Information Technology Governance, Wim Van Grembergen, Idea Group Publishing), pp. 269-309.

Grembergen, W. Van, (1997), "Millennium Conversion & COBIT", ComputerAudit Update l, July.

Güneş, Fatih, Kızıldeniz, S., Selçuk, S., Suna, B. ve Coşkun, S., (2013), "Bilgi Teknolojileri Denetimi ve COBIT' in Sektörel Uygulanabilirliği", http://ab.org.tr /ab13/bildiri/131.pdf

Hacısüleymanoğlu, Emine, (2010), "Bilgi Teknolojileri Yönetişim Yöntemleri ve COBIT ile Ulusal Bir Bankada Uygulaması", Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, İstanbul.

Hardy, Gary, (2006), "Using IT governance ve COBIT to deliver value with IT ve respond to legal, regulatory ve compliance challenges", Information Security Technical Report II, 55-61.

Hatipoğlu, İ. İlhan, (2014),"Kamu Bilgi Teknolojileri Denetim Rehberi", İç Denetim Koordinasyon Kurulu, Ankara, Ocak 2014. http://www.idkk.gov.tr/SiteDokumanlari/Mevzuat/Ucuncul%20Duzey%20Mevzuat/KamuBTDenetimiRehberi/KamuBTDenetimiRehberi.pdf

Henderson, J.C., Lee, S., 1992. Managing i/s design teams: a control theories perspective, Management Science, 38 (6), 757–777.

Herz, Thomas, Florian Hamel, Falk Uebernickel, Walter Brenner, (2013), "Toward a model of effective monitoring of IT application development ve maintenance suppliers in multisourced environments", International Journal of Accounting Information Systems, 14, (2013), 235-253.

Huang, S-M., Hung, W-H., Yen, D.C., Chang, I-C. ve Jiang, D., (2011), "Building the evaluation model of the IT general control for CPAs under enterprise risk management", Decision Support Systems, Volume 50, Issue 4, March, Pages 692-701

Işkın, Seyit A., (2012) "Elektronik Bankacılık Hizmetleri ve Denetimi", G.M. Matbaacılık ve Ticaret A.Ş., 2011, İstanbul.

IT Governance Institute, Cobit4.1" , 2005

IT Governance Institute, Cobit4.1", 2007

IT Governance Institute, "Cobit4.0", 2007

IT Governance Institute, "Cobit 5.0", 2014

Ivanyos, János ve József Roóz, (2011), "Using COSO ve COBIT Process Assessment Models", BPM GOSPEL, SPICE Assessors Workshop Community at the 18th EuroSPI Conference, Roskilde University, Denmark, 27-29 June. (BPM GOSPEL-Business Process Modelling for Governance SPICE ve Internal Financial Control)

Khadra, Husam Abu, Majdy Zuriekat, Nidal Alramhi, (2009), "An Empirical Examination of Maturity Model as Measurement of Information Technology Governance Implementation" The International Arab Journal of Information Technology, Vol. 6, No. 3, July.

Kerr, D.S. ve Murthy, U.S. (2013), "The importance of the CobiT framework IT processes for effective internal control over financial reporting in organizations: an international survey", Information & Management, Vol. 50, pp. 590-597.

Kutsikos, K., ve Bekiaris, M. G., (2007), "IT Governance Auditing in Virtual Organizations", Transactions on Line, Vol 1, Issue 1, Autumn, Management of International Business & Economic Systems.

Lainhart, J.W. (2000), "COBIT: A Methodology for Managing ve controlling information ve information technology risks ve vulnerabilities", Journal of Information Systems, Vol. 14, pp. 21 - 25.

Lunardi, G. L., João L. B., Antonio C. G. M. ve Pietro C. D., (2014), "The impact of adopting IT governance on Financial performance: An empirical analysis among Brazilian firms" International Journal of Accounting Information Systems, 15, 66–81.

Meadows, Rolling, "Control Objectives of Information ve Related Technology (CobiT)", Third Edition. Copyright _c 1996, 1998, 2000, the IT Governance Institute, http://isaca.org ve http://itgi.org, IL 60008, USA. Reprinted by permission.

Moeller, Robert R., (2009), "Brink's Modern Internal Auditing: A Common Body of Knowledge", John Wiley&Sons, Inc., Hoboken, New Jersey, Seventh Edition.

Moeller, Robert R., (2008), "Sarbanes-Oxley Internal Controls: Effective Auditing with AS5, CobiT, ve ITIL, John Wiley&Sons, Inc., Hoboken, New Jersey.

Özcan, Bilal, (2009), "Kurumsal Bilgi Güvenliği & COBIT", Haliç Üniversitesi Fen Bilimleri Enstitüsü Yönetim Bilişim Sistemleri, Yayınlanmamış Yüksek Lisans Tezi, Haziran, İstanbul.

Pederiva, Verea, (2003), The COBIT maturity model in the vendor evaluation case. Available online at. Information Systems Control Journal, http://www.isaca.org

Pekel, Ahmet, Zaim, Ü.Ü, Cumurcu, T. Ve Peker, D., (2008), "Bilişim Teknolojilerinde Yönetişim, Türkiye Bilişim Derneği Çalışma Grubu Raporu",http://www.tbd.org.tr/usr_img/cd/kamubib12/RaporlarPDF/RP1 -2008.pdf

Peker, Deniz, (2008), "Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri", Türkiye Bilişim Derneği Çalışına Grubu Raporu,TBD/Kamu-BIB/2008-ÇGR, http://www.tbd.org.tr /usr_img/cd/kamubib12/raporlar PDF/RP1-CobiT-2008.pdf.

Protoviti (2014), The Updated COSO Internal Control Framework. Frequently Asked Questions, 3rd ed., Protoviti, http://www.protiviti.com/en-US/Documents/Resource-Guides/Updated-COSO-Internal-Control-Framework-FAQs-Third-EditionProtiviti.pdf

Ridley G., J. Young, P. Carroll, (2004), "CobiT ve its utilization: a framework from the literature in Proceedings of the 37th Hawaii International Conference on System Sciences".

Rozek, P. (2008), "Putting IT governance into action", Internal Auditor, Vol. 65 No. 3, pp. 29-31.

Rubino, Michele ve Vitolla, Filippo, (2014), "Internal control over Financial reporting: opportunities using the COBIT framework", Managerial Auditing Journal, Vol. 29 Iss 8 pp. 736 – 771.

Sallé, M. ve S. Rosenthal (2005), "Formulating ve Implementing an HP IT Program Strategy Using Cobit ve HP ITSM", Proceedings of the 38th Hawaii International Conference on System Sciences, Hawaii.

Sarens, G. ve De Beelde, I. (2006), "Internal auditors" perception about their role in risk management. A comparison between US ve Belgian companies", Managerial Auditing Journal, Vol. 21 No. 1, pp. 63-80.

Simonsson, M. ve P. Johnson, (2006), "Assessment of IT Governance – A Prioritization of Cobit." Proceedings of the Conference on Systems Engineering Research. Los Angeles, USA. http://pdf.aminer.org/000/248/744/attemptingtodefineitgovernance wisdom_or folly.pdf.

Simonsson, M. ve P. Johnson, Wijkström H., (2007), "Model-Based IT Governance Maturity Assessments with Cobit", ECIS 2007, Proceedings. Paper 77. European Conference on Information Systems, http://aisel.aisnet.org/ecis2007/77

Solms, Basie von, (2005), "Information Security Governance: COBIT or ISO 17799 or both?", Computers & Security (2005) 24, 99-104.

Steven, Bab, (2012)," COBIT 5 for Risk Progress Report", COBIT Focus; Oct 2012, Vol. 2012 Issue 4, p5. http://www.isaca.org /Knowledge-Center/cobit/cobit-focus/Documents/COBIT-Focus-Vol-4-2012.pdf.

Tuttle, B. ve Vveervelde, S.D. (2007), "An empirical examination of CobiT as an internal control framework for information technology", International Journal of Accounting Information Systems, Vol. 8 No. 4, pp. 240-263.

Topkaya, Ahmet, (2011), "Bilgi Teknolojileri Yönetimi ve Denetim İlkeleri", Dış Denetim Dergisi, Temmuz – Ağustos - Eylül. http://www.sayder.org.tr/e-dergi-bilgi-teknolojileri-yonetimi-ve-denetim-ilkeleri-13-3.pdf.

Uzunay, Vildan, (2007), COBIT (Control Objectives for Information ve related Technology), İç Kontrol Merkezi Uyumlaştırma Dairesi, Mesleki Yeterlilik Tezi, Ankara, S.3

Üvey, M. Cüneyt, (2009), "Orkestra Şefiniz: COBIT", http://www.isaca.org/Knowledge-Center/cobit/Documents/COBITarticle-turkish.pdf

http://wildlaw.wordpress.com/case-study-1

https://cobitonline.isaca.org/

http://www.cozumpark.com/blogs/cobit-itil/archive/2010/11/21/cobit-nedir.aspx

http://tr.wikipedia.org/wiki/Cobit

http://www.itgovernance.co.uk/cobit.aspx