KPMG

BT Denetim Standartları ve Uygulamaları

Araştırma Raporu

Eylül 2017

kpmg.com.tr

İçindekiler

Araştırma hakkında

Bu araştırma raporu, Bilgi Teknolojileri (BT) denetimi kavramının ortaya çıkışı, zaman içerisinde gelişimi, standart ve düzenlemeleri ve denetim fonksiyonu içerisinde konumlanması konularını içermektedir. Söz konusu konular BT denetimi kapsamında yer alan yasal düzenlemeler ve standartlar baz alınarak detaylandırılmıştır. Araştırma raporu kapsamına alınan ülkeler, gelişmişlik düzeyleri baz alındığında ana aktörler olarak ortaya çıkan ülkeler arasından seçilmiş olmakla birlikte, Avrupa Birliği üyesi olmaları, denetim çalışmaları hakkında köklü ve kapsamlı yasal düzenlemelere sahip olmaları da dikkate alınan faktörlerden bazılarıdır.

Ülkelerin uygulamalarının yanısıra, BT denetimi kapsamında dünya çapında geçerli olan standartlar, çerçeveler ve diğer uygulamalar rapora konu edilmiştir.

Yasal düzenlemeler, lokal ve global standartlar, denetim raporu, denetim görüşü, denetçi yetkilendirmesi ve benzeri konu başlıkları altında BT denetimi uygulamaları geniş bir bakış açısı ile araştırılmıştır.

Araştırma raporu kapsamına alınan ülkeler ve ülkelerin seçilme kriterleri açısından öne çıkan başlıklara aşağıda yer verilmiştir:

Almanya: Avrupa Birliği standartlarına uyum adına, Türkiye için bir model teşkil edebileceği göz önüne alınarak, araştırma raporu kapsamına alınmıştır. Aynı zamanda denetim ve güvence uygulamaları çerçevesinde, Alman Denetçiler Enstitüsü (IDW) kurumunun bulunması, araştırma raporuna konu edilmesinde önemli bir rol oynamıştır.

Amerika Birleşik Devletleri: Yaşanan ekonomik ve finansal skandallar sonrası (Enron, Worldcom, vb), özellikle yönetim beyanı uygulamalarını ve Sarbanes Oxley Yasası (SOX) uygulamalarını yasal bir zorunluluk haline getirmiş ve diğer ülkelere denetim ve standartlar konusunda bir örnek teşkil etmiştir. Bu uygulamalar birçok ülke ve kurum için, düzenleme ve standartlara karar verilmesi açısından önemli bir etken olmuştur.

Birleşik Krallık: Finans sektörünün küresel çapta liderlerinden olan Birleşik Krallık, finans sektöründe önemli merkezlerden birisi konumunda yer almaktadır. Özellikle bankacılık sektöründe köklü ve kapsamlı yasal düzenlemelere ve uygulamalara sahip ülkelerden birisidir. BT denetimi ile ilgili düzenlemelere de sahip olması araştırma raporunda Birleşik Krallığın kapsama alınmasında önemli rol almıştır.

Güney Kore: Güney Kore, Birleşmiş Milletler, Dünya Ticaret Örgütü, Organization for Economic Cooperation and Development (OECD) ve G20 gibi örgütlere üye olması, gelişmekte olan ülkelerden birisi olması ve aynı zamanda Asia Pasific Economic Cooperation (APEC) ve Doğu Asya Zirvesi vb. yapıların kurucu üyelerinden olması nedeniyle önemli bir örnek teşkil etmektedir. Denetim anlamında düzenlenen yasalar ve hazırlanan standartlar rapora konu edilmesinde önemli bir rol oynamıştır.

Hollanda: Avrupa Birliği üyelerinden olan Hollanda, bilgi sistemleri denetçileri için ulusal düzeyde bir bilgi sistemleri denetimi meslek birliği ve yüksek öğrenim destekli yerel bir sertifikasyon programına sahiptir, bu alanda nadir örneklerden biri olarak öne çıkmaktadır. Söz konusu uygulamaların Türkiye için örnek teşkil edebileceği göz önüne alınarak, araştırma raporu kapsamına alınmıştır.

Japonya: Gayri safi yurtiçi hasıla ve ekonomik büyüklük olarak Japonya, ilk sıralarda bulunmaktadır. Birleşmiş Milletler, G7 ve APEC üyesidir. Gelişmişlik seviyesi ve SOX'a paralel bir düzenlemesinin (J-SOX) bulunması göz önüne alınarak araştırma raporu kapsamına alınmıştır.

Kanada: İşletmelerin bilgi sistemleri denetim faaliyetlerine ilişkin incelemeler gerçekleştirilirken International Standards on Auditing (ISA) standardı, Control Objectives for Information and Related Technologies (COBIT) ve CoCo baz alınarak hazırlanmış Information Technologies Control Guidelines (ITCG) kılavuzundan faydalanılarak gerçekleştirilmesinden dolayı Kanada'nın BT denetimi anlamında yol gösterici olabileceği göz önüne alınarak, araştırma raporu kapsamına alınmıştır.

Uluslararası bilgi teknolojileri denetim uygulamaları

1. Dünyada Bilgi Teknolojileri Denetimi Yönelimleri ve Tarihçesi

BT oluşumu ve sürekli gelişimi ile birlikte BT iş dünyasının önemli bir parçası haline gelmiştir. Bilgi teknolojileri artık iş süreçlerinin her noktasında karşımıza çıkmaktadır. Bu durum beraberinde birçok firma için teknoloji odaklı, teknoloji ile iç içe, teknolojiye bağlı iş süreçlerinin doğmasına neden olmuştur. Dolayısıyla teknolojilerden kaynaklı riskler önemli bir risk alanı haline gelmiştir.

Bilgi teknolojileri riskleri, bilgi sistemlerinin iş süreçlerinin önemli bir parçası olarak kullanıldığı sektörlerde kritik bir yönetim unsuru haline gelmiştir. Söz konusu unsurun yönetimi finansal odaklı bir yaklaşım ile ortaya çıkan denetim kavramının bilgi teknolojilerine yöneltilmesi ile mümkün hale gelmiştir. Bu doğrultuda ortaya bilgi teknolojilerinin denetimi kavramı çıkmıştır.

BT denetimi, bilgi teknolojileri altyapı ve süreçlerinin kendilerinden beklenen faydaları sağlayıp sağlayamayacaklarına dair güvence sağlamayı hedefler. Bu faydalar; etkililik, yani iş ihtiyaçlarını karşılama gücü; etkinlik, yani kaynakların verimli kullanımı; güvenlik, yani bilgi varlıklarının gizlilik, bütünlük ve sürekliliğinin korunması ve bu faydaların türevleri olan güvenilirlik ve yasalara uyumdur. Şirketler kendi iş hedeflerine ulaşabilmelerinin yanı sıra teknoloji kullanımının getirdiği riskleri de BT denetimi çerçevesinde gözetmek zorundadırlar.

BT denetimi ilk olarak elektronik veri işleme süreçleri kapsamında gerçekleştirilmeye başlanmıştır. Bu doğrultuda kavramın doğuşunu takiben zaman içerisinde çeşitli kurumlar tarafından BT denetimi kapsamında çerçeveler hazırlanmıştır. (İlgili çerçevelere ilişkin detaylara "Bilgi teknolojileri denetimi alanında kullanılan global standartlar ve çerçeveler" bölümü altında yer verilmiştir.)

BT denetiminin tarihçesini genel olarak ifade etmek gerekirse, denetim kavramı ile ilişkisini baz almak doğru olacaktır. Söz konusu bakış açısı ile incelendiği takdirde, karşımıza ilk olarak 1988 yılında yayımlanan çeşitli prensipler ve denetim rehberleri çıkmaktadır. Örnek olarak GAO Audit Guide, Wood's Principles verilebilir. Ancak denetim kavramının bütüncül ve detaylı bir şekilde ortaya konması 1994 ve takip eden yıllarda SAC, COSO, CoCo, GAPP çerçeveleri ile gerçekleştirilmiştir. 1998 yılında ITCG, FISCAM, GASSP, 2000'li yıllarda ise CobiT, SysTrust, SSAG, BS7799 (ISO17799-ISO27001) standart ve çerçeveleri ile denetim kavramı bilgi teknolojileri bazında detaylandırılmıştır.

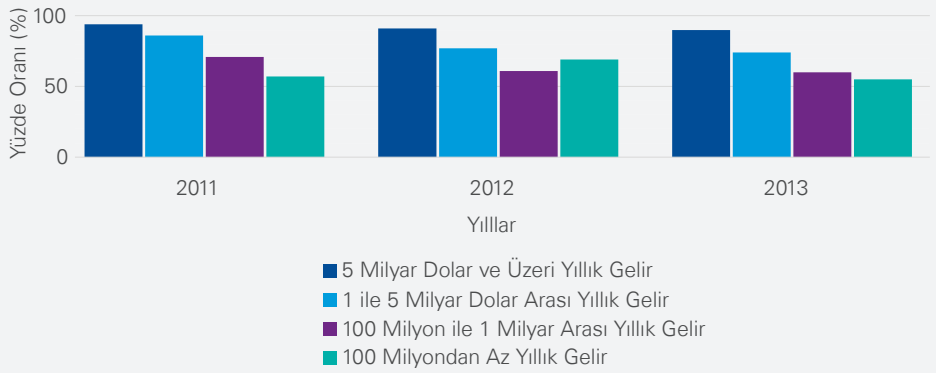
BT denetimi ortaya çıktığı tarihten itibaren teknolojinin gelişmesine paralel olarak içerik olarakda zenginleşmiş ve birçok ülke ve kurum tarafından önem verilen bir alan olmaya başlamıştır. Kazandığı önem doğrultusunda zaman içerisinde çeşitli düzenlemelere tabi olmuş ve yönlendirici standartlar hızla çoğalmıştır. Standartlar ve yasal düzenlemelerin etkisi ile firmaların denetim birimlerinde gittikçe daha önemli bir yere sahip olmuştur. Dolayısıyla teknolojik gelişmelerin son yıllarda iş süreçlerine fazlasıyla entegre olması ve hayatımızda çok yoğun bir etkiye sahip olması ile birlikte, BT denetimi kapsamındaki bütün bu gelişmelerin kazandığı hız artık açık bir şekilde görülebilmektedir. BT denetimi anlamında dünya çapında yönlendirici bir kurum olan Information Systems Audit and Control Association (ISACA) tarafından söz konusu değişimleri gözlemleyen ve ifade eden çalışmalar gerçekleştirilmiştir. Bu kapsamda ISACA tarafından yıllık olarak "BT Denetimi Değerlendirme Araştırması" (Annual IT Audit Benchmarking Survey) raporu hazırlanmaktadır.

Söz konusu rapor içerisinde BT denetimi fonksiyonunun kurumlar içerisindeki varlığı ve kurum organizasyonu içerisindeki konumu incelenmektedir. Bununla birlikte BT risk değerlendirme çalışmalarının yürütülmesi, yönetilmesi ve BT denetimi kapsamında kullanılan çerçeveler baz alınmaktadır.

ISACA'nın araştırma çalışmalarına göre, BT denetiminin kurum iç denetim fonksiyonu içindeki varlığı, kuruluş büyüklüklerine ve yıllara göre aşağıdaki şekilde değişiklik göstermektedir.

Bu kapsamda ISACA tarafından Proviti işbirliği ile yıllık olarak "BT Denetimi Değerlendirme Araştırması" (Annual IT Audit Benchmarking Survey) raporu hazırlanmaktadır.

BT Denetim Fonsiyonunun İç Denetim Fonksiyonu İçindeki Varlığı (%)

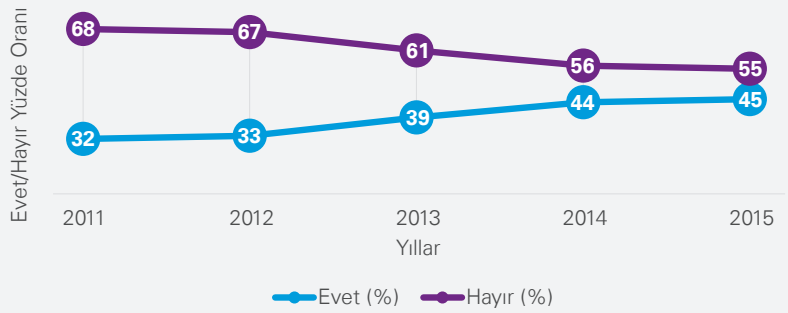


Kaynak: Proviti (2013). Yıllık Rapor. www.proviti.com, (2013). Third Annual IT Audit Benchmarking Survey. USA: Proviti Insights.

Firma yıllık geliri ile BT denetim fonksiyonunun varlığının ise birbiri ile doğru orantılı olduğu, yıllık gelirin artması ile fonksiyonunun varlığının arttığı görülmektedir.

ISACA'nın gerçekleştirdiği BT denetimine yönelik araştırmalar doğrultusunda BT denetimi direktör pozisyonunun kuruluşlar içindeki varlığı yıllara göre aşağıdaki şekilde değişiklik göstermektedir.

BT Denetim Direktörü Pozisyonunun Varlığı (%)

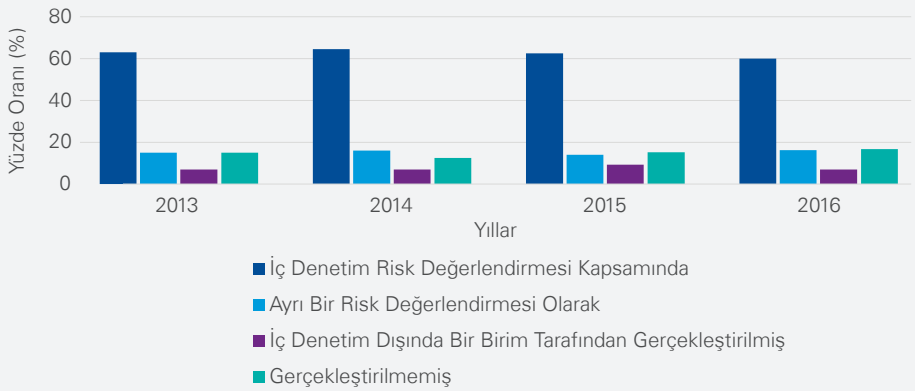


Kaynak: Proviti (2013). Yıllık Rapor. www.proviti.com, (2013). Third Annual IT Audit Benchmarking Survey. USA: Proviti Insights.

Yıllara göre BT denetim direktörü pozisyonunun varlığı incelendiğinde, düzenli olarak oranın arttığı görülmektedir. Dolayısıyla organizasyonel olarak BT denetim fonksiyonuna üst seviyede verilen önemin arttığı, kurum organizasyon yapısı içerisinde BT denetimi kavramının önem kazandığı görülmektedir.

BT kapsamındaki risk değerlendirme çalışmalarının yıllar içerisindeki değişimi yandaki grafikte görülmektedir. Grafik incelendiğinde, BT risk değerlendirme çalışmalarının büyük bir oranda iç denetim risk değerlendirme çalışmaları kapsamında gerçekleştirildiği görülüyor. Söz konusu durum yıllar içerisinde küçük bir miktarda azalma göstermiş olmakla birlikte, ayrı bir risk değerlendirmesi olarak yapılmasına oranla çok daha fazla bir hacme sahip. Ancak büyük resme bakıldığında BT risk değerlendirme çalışmalarının kuruluşlarda büyük oranda gerçekleştirildiği görülmektedir.

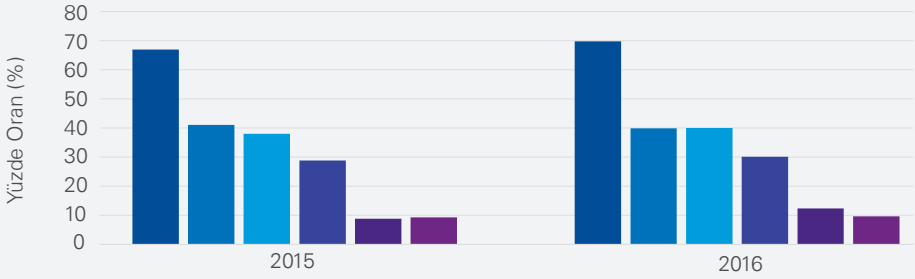
BT Risk Değerlendirme Çalışmaları (%)



Kaynak: Proviti (2013). Yıllık Rapor. www.proviti.com, (2013). Third Annual IT Audit Benchmarking Survey. USA: Proviti Insights.

Söz konusu risk değerlendirme çalışmaları ve BT denetim çalışmalarında baz alınan standartlar da ISACA'nın araştırmalarına konu olmuştur. Bu doğrultuda yıllar içerisindeki değişim aşağıdaki grafik üzerinde ifade edilmektedir.

BT Risk Değerlendirmesi Kapsamında Kullanılan Standartlar & Çerçeveler (%)



	2015	2016
COBIT	67	70
COSO	41	40
ISO	38	40
ITIL	29	30
NIST CSF	9	12
Basel III	9	10

Kaynak: Proviti (2013). Yıllık Rapor. www.proviti.com, (2013). Third Annual IT Audit Benchmarking Survey. USA: Proviti Insights.

Araştırma sonuçları incelendiğinde BT risk değerlendirme çalışmalarında ağırlıklı olarak COBIT ve COSO çerçevelerinin baz alındığı görülmektedir. Bununla birlikte ISO ve ITIL çerçeveleri de oldukça yüksek bir orana sahiptir.

Uluslararası Ödemeler Bankası (Bank of International Settlements) (BIS) birçok ülkenin merkez bankasının üye olduğu bir kuruluştur. Söz konusu kuruluş tarafından 2013 yılında "Etkin Risk Veri Toplama ve Raporlama İlkeleri" adı altında bir rehber yayımlanmıştır. Rehber içeriğinde veri mimarisi ve BT altyapısının risk veri toplama sürecini kriz durumları ve normal işleyiş sürecinde tamamen desteklemesi gerektiği belirtilmektedir. Ek olarak BT stratejisinin risk veri toplama ve raporlama süreçlerini iyileştirici bir bakış açısını içermesi gerektiği ifade edilmektedir. Ayrıca veri doğruluğu, bütünlüğü ve tamlığı söz konusu rehberin üçüncü ve dördüncü ilkelerine konu olmaktadır. Dolayısıyla risk değerlendirme süreci kapsamında BT kaynaklarının strateji ve altyapı olmak üzere birçok açıdan dikkate alınması gerektiği açık bir şekilde belirtilmektedir.

Söz konusu araştırmalar ve rehberler ışığında BT risk değerlendirmesi ve BT denetimi kavramlarının teknolojinin gelişimi ile birlikte hızla gündeme girdiği ve zaman içerisinde hızla önem kazandığı görülmektedir. BT denetimi tarihin büyük resmine bakıldığında resme son zamanlarda girmiş olmasına rağmen, kısa sürede oldukça önemli ve büyük bir yer edinmeye başladığı uygulamalar, standartlar ve yasal düzenlemeler bazında açıkça ortaya çıkmaktadır.

2. Türkiye'deki Bilgi Teknolojileri Denetimi Yönelimleri ve Tarihçesi

İş hayatında bilgi teknolojilerinin kullanımının artması Türkiye'de de dünyaya paralel olarak artmıştır. Ülkemizde kamu kuruluşları ve özel sektördeki kuruluşlar, teknolojideki gelişmelere bağlı hızlı bir dönüşüm süreci içinde bulunmakta, faaliyetlerinin büyük bir kısmını gerçekleştirirken sistemlerden ve uygulamalardan yararlanmaktadırlar. Türkiye'de, Bankacılık Düzenleme ve Denetleme Kurumu'nun, Bankacılık Kanunu ve 6493 sayılı Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun ışığında yaptığı düzenlemeler ile finans sektörü bilgi teknolojileri kapsamında zorunlu denetimlerden geçmektedir. Ayrıca, Enerji Piyasası Düzenleme Kurumu (EPDK), Bilgi Teknolojileri ve İletişim Kurumu (BTK) ve Gümrük ve Ticaret Bakanlığı'nın da BT kontrollerinin tesisi üzerine düzenlemeleri mevcuttur. Bununla beraber, Türkiye'de yerleşik yabancı ortaklı kuruluşların, ABD borsalarında kote olanları da, belirli şart ve şekil çerçevesinde SOX çevresinde BT denetimlerine tabidir. Bunlara ek olarak, Sermaye Piyasası Kurulu (SPK), aracı kurumlarda uygulanacak iç denetim sistemine ilişkin esaslar hakkında bir tebliğ çıkarmış olup, Gelirler İdaresi Başkanlığı da yeni nesil Ödeme Kaydedici Cihazlar için Güvenilen Servis Sağlayıcılarda (TSM) BT denetimlerini zorunlu hale getirmiştir.

Tarihsel olarak Türkiye'de Kurumlar Bazında Bilgi Sistemlerine Yönelik Çıkarılan Mevzuatlar

Kurum	Düzenleme	Tarih
SPK	Aracı Kurumlarda Uygulanacak İç Denetim Sistemine İlişkin Esaslar Hakkında Tebliğ	2003
BDDK	Bankalarda Bağımsız Bilgi Sistemleri Denetimi Hakkında Yönetmelik	2006
	Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ	2008
	Bankalarda Bağımsız Bilgi Sistemleri ve Bankacılık Süreçleri Denetimi Hakkında Yönetmelik	2010
Sayıştay	Bilişim Sistemleri Denetim Rehberi	2013
Gümrük ve Ticaret Bakanlığı	Gümrük İşlemlerini Kolaylaştırma Yönetmeliği kapsamında ihracatçı firmaların lisans almasında ISO27001 Zorunluluğu	2013
BDDK	Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ	2014
Gelir İdaresi Başkanlığı	Yeni Nesil ÖKC'lere Ait ÖKC TSM Merkezlerinin Bilgi Sistemleri Denetimi Adımları Teknik Kılavuzu	2015
Türkiye Bankalar Birliği Risk Merkezi	Risk Merkezi Üyelerinin Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Denetimi ve Raporlanması Hakkında Genelge	2016
EPDK	Lisans sahiplerine Türk Akreditasyon Kurumu'ndan (TÜRKAK) akredite bir belgelendirme kuruluşundan ISO27001 belgeli olma zorunluluğu	2016

3. Bilgi Teknolojileri Risk ve Güvence Düzenlemeleri

Almanya

Almanya German Federal Supervisory Authority (BaFin) Almanya Federal Gözetim Otoritesidir. BaFin'in başlıca görevi; bankaların, sigorta şirketlerinin ve menkul kıymetlerin ticaretinin denetlenmesi ve Alman finans sisteminin uygulanabilirliği, bütünlüğü ve istikrarını sağlamaktır. Yasal işlem yürütme yetkisine sahip bağımsız bir kuruluştur. Denetim unsuru kapsamında, BaFin tarafından yayımlanan Bankacılık Kanunu içerisinde beşinci bölüm altında denetim raporu ve altıncı bölüm altında denetçi ve denetim kapsamı hakkında tanımlamalar yapılmıştır. Özellikle BT denetimine yönelik bir referans bulunmamaktadır. Ancak BaFin tarafından "Risk Yönetimi için Minimum Gereksinimler" adı altında bir ek düzenleme yayımlanmıştır. Bu düzenlemeye "Bankacılık Kanunu" Madde 25.a altında atıf yapılmaktadır. Düzenleme içerisinde başlık 7.2'nin altında bilgi teknolojilerine yönelik tanımlamalar bulunmaktadır. Söz konusu bölümde bilgi teknolojileri yönetiminde erişim hakları, verinin bütünlüğü, gizliliği, erişilebilirliği ve sistemlerdeki değişiklikler konularına değinilmiştir. Yasada özellikle belirli bir standart veya çerçeve baz alınmamaktadır. Bundesamt für Sicherheit in der Informationstechnik, Federal Office for Information Security (BSI) ve ISO standartlarının baz alınabileceğini belirtmekle birlikte sadece söz konusu standartların bilgi güvenliğinin sağlanmasında yeterli olmayabileceğini, organizasyonun yapısı doğrultusunda hareket etmesi gerektiğini belirtmektedir. Dolayısıyla organizasyonların gereksinimlerini kendilerinin belirlemesi gerektiği ifade edilmektedir.

BSI Almanya hükümeti için bilgisayar ve iletişim güvenliği yönetiminden sorumlu olan Alman üst düzey federal ajansıdır. Uzmanlık alanı ve sorumluluk alanları, bilgisayar uygulamalarının güvenliği, kritik altyapının korunması, İnternet güvenliği, kriptografi, sayaç dinleme, güvenlik ürünlerinin sertifikasyonu ve güvenlik test laboratuvarlarının akreditasyonunu içermektedir. Ağustos 2009'da "Federal Bilgi Teknolojilerinin Güvenliği" (Act to Strengthen the Security of Federal Information Technology) adı altında bir yasa yayımlanmıştır. Bu yasa doğrultusunda bilgi güvenliği ile ilgili gereksinimler tanımlanmıştır. Ek olarak BSI tarafından "BSI Standart 100-1: Bilgi Güvenliği Yönetimi Sistemi", "BSI Standart 100-2: IT Grundschutz", "BSI Standart 100-3: Risk Analizi" standartları yayımlanmıştır. Söz konusu standartların ISO27001 ile paralel olduğu belirtilmektedir. Dolayısıyla Almanya'da BSI kapsamında hükümet tarafından ISO27000 standartlarının baz alındığı görülmektedir. IDW Almanya'daki denetçiler ve denetim firmalarına hizmet eden, yasalardan ziyade gönüllülük esaslı bir kuruluştur. Söz konusu kuruluş tarafından denetim çalışmalarına yönelik birçok standart yayımlanmaktadır. Bilgi teknolojileri denetimi kapsamında ise IDW RS FAIT 1, FAIT 2, FAIT 3, GoBS ve GDPdU ile uyumlu bir şekilde IDW PS 330 adlı standart yayımlanmıştır. İlgili standart ile bilgi teknolojileri denetiminde BT çevresi, BT Stratejisi, BT Altyapısı, uygulamaları, izleme sistemleri ve dış kaynak kullanımı gibi konular dikkate alınmaktadır. Standart içeriğinde BT kontrollerinin test edilmesi, bilgisayar destekli denetim teknikleri, dokümantasyon, raporlama ve ISA çerçevesi ile uyum başlıkları bulunmaktadır.

Almanya'daki yasal mevzuatta yukarıda belirtildiği üzere bilgi teknolojilerine yönelik gerçekleştirilecek denetime ilişkin unsurlara yer verilmekle birlikte; denetim faaliyetlerinin nasıl gerçekleştirileceğine ilişkin detaylı hükümler bulunmamaktadır. Ancak bilgi teknolojilerine ve denetimine yönelik BSI ve IDW tarafından tavsiye niteliğinde standartlar yayımlanmıştır.

Amerika Birleşik Devletleri

Amerika Birleşik Devletleri'nde BT denetimi kapsamında düzenleyici yasa olarak karşımıza en üst düzeyde SOX çıkmaktadır. SOX, 2002 yılında kongre tarafından onaylanarak yürürlüğe girmiştir. Public Company Accounting Oversight Board (PCAOB) tarafından gözetimi gerçekleştirilen SOX da yer alan kurallar, U.S. Securities and Exchange Commission (SEC) üyesi bilgi sistemleri özelinde bir düzenleme getirmemekte; ancak "finansal raporlama süreçleri üzerindeki iç kontrol ortamı"na hem iç denetçi, hem de bağımsız denetçi tarafından güvence verilmesi, bilgi sistemlerine ilişkin genel kontrollerin ve iş süreçlerindeki otomatik kontrollerin değerlendirilmesini gerektirmektedir. Özellikle Bölüm 404 olarak adlandırılan bu bölüm, kuruluşların finansal raporlara üzerindeki iç kontrol ortamına yönelik değerlendirmeleri ve dolayısıyla BT ve otomatik süreç kontrollerinin denetimini gerektirmektedir. SOX denetimi kapsamında PCAOB tarafından aşağıdaki standartlar bilgi sistemlerine ilişkin AS 2100 (Denetim Planlaması ve Risk Değerlendirme), AS 2200 (Finansal Raporlama Süreçleri Üzerindeki İç Kontrol Ortamının Denetimi), AS 2300 (Riskin Doğası, Zamanlaması ve Boyutuna Yönelik Denetim Prosedürleri) detaylarını içermektedir.

Ek olarak PCAOB tarafından Ağustos 2010 tarihinde yayımlanmış olan "Denetçinin Değerlendirmesi ile ilgili Denetim Standartları" dokümanında "Bilgi ve İletişim" başlığı altında finansal raporlama ile ilgili bilgi sistemlerine yönelik ek tanımlamalar bulunmaktadır. Söz konusu tanımlamalara göre denetçiler finansal raporlama süreçleri ile ilgili bilgi sistemlerini anlamaları gerekmektedir. Bu kapsamda bilgi sistemlerinin firmanın iş akışlarını ne ölçüde ve nasıl etkilediğinin belirlenmesi gerektiğini belirtmektedir. Risk ve kontrollerin değerlendirilmesi çalışmalarında bilgi sistemlerinin değerlendirme kapsamında dâhil edilmesi gerektiği belirtilmektedir. Manüel ve otomatik kontrollerin yanısıra BT genel kontrollerinin risklerin değerlendirilmesinde dikkate alınması gerektiği ifade edilmektedir.

ABD'de Federal Devletin Standart Enstitüsü olarak Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) bulunmaktadır. NIST tarafından "Security and Privacy Controls for Federal Information Systems" standardı yayımlanmıştır. Söz konusu standart Kongre tarafından 2002 yılında yayımlanan "Federal Information Security Management Act" (FISMA) yasası doğrultusunda hazırlanmıştır. Yasa içeriğinde bilgi güvenliği, bilgi teknolojilerinin yönetimi konularına değinmektedir. Aynı yasa içerisinde NIST'e standart düzenleme yetkisi verilmektedir. NIST tarafından standart içerisinde ise risk yönetimi, güvenlik kontrol mekanizması, tasarımı, güvenlik kontrol kataloğu, bilgi güvenliği programı konularına ilişkin detaylı tanımlamalar yer almaktadır. Ek olarak küresel standartlara bazı göndermeler yapılmaktadır. Kontrol başlıkları bazında ISO27001 ile eşleşmelere ilişkin detaylı tablolar bulunmaktadır. Ana hatlarıyla erişim yönetimi, farkındalık ve eğitim, denetim izi, güvenlik değerlendirmesi, konfigürasyon yönetimi, acil durum yönetimi, olay yönetimi, bakım, medya yönetimi, fiziksel güvenlik, personel güvenliği, risk değerlendirme, sistem ve servis edinimi ve güvenliği konularını içermektedir. Bu standardın ISO27001 standardı ile oldukça paralel olduğu görülmektedir.

NIST tarafından ayrıca, "Generally Accepted Principles and Practices for Securing Information Technology Systems" (GAPP) adında bir standart yayımlanmıştır. Standart içeriğinde sistem güvenliği prensipleri, genel BT güvenliği prensipleri, politikalar, program yönetimi, risk yönetimi, değişiklik yaşam döngüsü, kullanıcı yönetimi, iş sürekliliği, olay yönetimi, farkındalık ve eğitim, fiziksel ve çevresel güvenlik, erişim yönetimi, denetim izleri, kriptografi başlıkları yer almaktadır. Denetçiler tarafından bir rehber olarak kullanılmak üzere yayımlandığı belirtilmektedir.

NIST tarafından denetim rehberi niteliğinde "Guide to Auditing for Controls and Security: A System Development Life Cycle Approach" dokümanı yayımlanmıştır. Doküman içeriğinde sistem geliştirme yaşam döngüsü kapsamında yer alan kontrol hedefleri ve denetim metodolojisi, daha detayda ise her bir süreç aşamasında denetimin nasıl dâhil olacağı hakkında bilgiler bulunmaktadır. Sistem geliştirme yaşam döngüsü kapsamında denetim fonksiyonunun rolü, uygulamaları hakkında oldukça detaylı açıklamalar yer almaktadır. "Ek olarak NIST tarafından "Security Self-Assessment Guide for Information Technology Systems" (SSAG) ve "Risk Management Guide for Information Technology Systems" standartları yayımlanmıştır. Söz konusu standartlar kapsamında bilgi güvenliği çerçevesinde uygulama ve tasarım anlamında tamamlayıcı ve yol gösterici tanımlamalar bulunmaktadır. Detayda ise risk yönetimi, güvenlik kontrollerinin gözden geçirilmesi, yaşam döngüsü, yetkilendirme işlemleri, sistem güvenlik planı, personel güvenliği, fiziksel ve çevresel güvenlik, üretim kontrolleri, acil durum planlaması, donanım ve sistem yazılımı bakımı, veri bütünlüğü, güvenlik farkındalığı ve eğitimi, olay tepki kapasitesi, mantıksal erişim kontrolleri, denetim izleri başlıklarını içermektedir.

The Financial Industry Regulatory Authority ("FINRA"), Amerika finansal endüstrisinde yatırımcıları korumayı hedefleyen sistemsel düzenlemeler yapan bir kurumdur. FINRA tarafından denetim kavramı kapsamında "Rule 418" ve "Rule 4140" bulunmaktadır. Söz konusu yönetmelikler içeriğinde denetim doğrultusunda tanımlamalar bulunmakla birlikte tanımlamalar BT denetimi özelinde değildir.

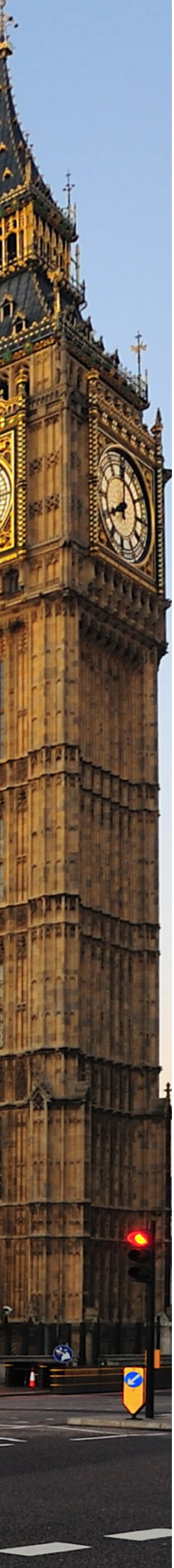
Government Accountability Office ("GAO") kongre için çalışan bir fonksiyondur. Düzenleme ve yönetmelikler kapsamında destek olmak amacıyla çalışmaktadır. 2011 yılında GAO tarafından "Government Auditing Standarts" (GAGAS) dokümanı yayımlanmıştır. Doküman içeriğinde "Information Systems Control" başlığı altında BT denetimine yönelik detaylı tanımlamalar bulunmaktadır. İç kontrollerin bilgi sistemleri kontrolleri ile bağlantısı ile ilişkilendirilmesi kapsamında genel kontroller, uygulama kontrolleri ve kullanıcı kontrolleri ele alınmaktadır. Güvenlik yönetimi, erişim yönetimi, konfigürasyon yönetimi, görevler ayrılığı, acil durum planlaması konuları BT kontrolleri kapsamında belirtilmektedir. Ek olarak GAO tarafından 2009 yılında "Federal Information System Controls Audit Manual" (FISCAM) dokümanı yayımlanmıştır. Rehber kapsamında ele alınan konu başlıkları GAGAS ile paralel olarak güvenlik yönetimi, erişim kontrolleri, konfigürasyon yönetimi, görevler ayrılığı ve acil durum planlaması olarak karşımıza çıkmaktadır.

American Institute of Chartered Public Accountants ("AICPA") ve Canadian Institute of Chartered Accountants ("CICA") tarafından "SysTrust Principles and Criteria for System Reliability" hazırlanmıştır. Standart kapsamında CIA modeli baz alınmakla birlikte ulaşılabilirlik, gizlilik, güvenlik, bütünlük ve bakım prensipleri yer almaktadır.

The Federal Financial Institutions Examination Council ("FFIEC"), tarafından yayınlanan "Supervision of Technology Service Providers ("TSP") Booklet" dokümanında teknoloji hizmeti sunan firmaların risk yönetimi kapsamında denetim sorumlulukları belirtilmiştir. Doküman kapsamında finansal kuruluşlar ve servis sağlayıcıların bilgi teknolojilerinin edinimi, kurulumu ve kullanımı kapsamında iç kontrol ortamının ve risklerin değerlendirilmesinin beklendiği vurgulanmıştır.

Ülkede, American Institute of CPAs ("AICPA") tarafından hazırlanmış ve ISAE 3402 tabanlı bir denetim ve güvence standardı olan SSAE 16 yaygın olarak kullanılmaktadır.

İç Denetim Enstitüsü Araştırma Vakfı tarafından "Electronic Systems Assurance and Control" (eSAC Model) dokümanı yayımlanmıştır. Teknolojideki değişikliklerden kaynaklı iş risklerinin değerlendirilmesi, sistemlerin kapasitesi, ulaşılabilirliği, işlevselliği, korunabilirliği, izlenebilirliği ve denetlenebilirliği kapsamında geliştirilmiştir.



Birleşik Krallık

Financial Services Authority (FSA), finansal piyasalarda hizmet veren şirketler ve borsa için standartları belirlemek ve denetlemek amacıyla kurulmuş bağımsız bir kuruluştur. BT denetimi ile ilgili FSA tarafından yayımlanan ilkeler, Senior Management Arrangements, Systems and Controls (SYSC13) adlı kılavuzda bulunmaktadır.

FSA, bilgi teknolojileri ile ilgili değerlendirmesini ilgili kılavuz içerisinde "Bir firma süreçlerindeki ve sistemlerindeki yetersizliklerden veya arızalardan doğabilecek operasyonel riskler için uygun sistemleri kurmalı ve kontrol etmelidir." şeklinde tanımlamaktadır. Bu tanımlamaya ek olarak, uygulama, işletim sistemi, ağ altyapısı, sunucu gibi BT sistemleri süreçlerin otomasyonu için gerekli olan bilgi ve donanımı içermektedir. Otomasyon iş süreçlerindeki insan riskini azaltmakta, ancak BT sistemlerinin güvenilirliğine bağımlılık artmaktadır. Bu kapsamda artan BT sisteminin önemi için firmaların BT sistemi risklerini yönetmesi için aşağıda belirtilen maddelere uygun sistemleri ve kontrolleri oluşturmalı ve sürdürmelidir;

- Teknoloji operasyonları için organizasyon ve raporlama yapısı
- Teknoloji gereksinimlerinin iş stratejilerine uyumluluğu
- Sistemlerinin edinimi, geliştirme ve bakım faaliyetlerinin uygunluğu
- BT sistemlerinin işletilmesini destekleyen faaliyetlerinin uygunluğu

FSA tarafından yayınlanan ilgili kılavuz kapsamında ayrıca bilgi güvenliğine de değinilmiştir. Bilgilerin işlenmesindeki başarısızlıklar veya bilginin korunmasını sağlayan sistemlerdeki güvenlik açığı firmadaki önemli bir iş sürecinin aksamasına veya durmasına neden olabilir. Bu kapsamda bilgi güvenliği risklerinin yönetilmesi uygun sistemler ve kontrolleri kurulmalıdır. İlgili riskleri yönetirken firmalar aşağıda belirtilen maddeleri göz önünde bulundurmalılar;

Gizlilik; bilginin yetkisiz kişilerin eline geçmemesi, Bütünlük; Bilginin yetkisiz kişiler tarafından değiştirilmesi, silinmesi ya da herhangi birşekilde tahrip edilmesi tehditlerine karşı içeriğinin korunması,

Kullanılabilirlik ve kimlik doğrulama; bilginin herihtiyaç duyulduğunda kimliği doğrulanmış ilgiliya da yetkili kişilerce ulaşılabilir ve kullanılabilir durumda olması,

Hesap verilebilirlik ve sorumluluk; bilgiyi işleyen kişinin veya sistemin eylemlerini inkar edememesi.

Bilginin işlenmesini ve güvenliğini korumak için kullanılan sistemlerin ve kontrollerin yeterliliğini sağlamalıdır ve BS17799 (Bilgi Güvenliği Yönetimi) gibi belirlenmiş güvenlik standartlarını dikkate almalıdır.

Ayrıca, ilgili kılavuz kapsamında firmaların süreçlerinin ve sistemlerinin farklı lokasyonlarda olması ve özellikle sistemlerinin farklı ülkelerde yer alması durumunda, o ülkelerdeki yerel regülasyonların, verinin korunması ve transferi konusundaki yasaların, siyasi aksaklıklar veya kültürel farklılıkların hizmet sunumundaki olasılığı ve etkisinin değerlendirilmesi gerektiği belirtilmiştir. Belirtilen ilgili maddelerin yanı sıra SYSC7 adlı kılavuzda firmaların risk yönetimi gerçekleştirmesi gerektiği ve risk yönetimi hakkında bilgilere yer verilmiştir.

Güney Kore

Güney Kore'de bilgi teknolojileri denetimi özelinde bir düzenleme bulunmamakla birlikte, denetim çalışmaları kapsamında çeşitli ve detaylı düzenlemeler bulunmaktadır. Bu doğrultuda karşımıza "Board of Audit and Inspection Act", "Act on External Audit of Stock Companies" ve "Act on Public Sector Audits" düzenlemeleri çıkmaktadır. Bahsi geçen düzenlemeler finansal denetim çalışmaları çerçevesinde hazırlanmış olup, bu doğrultuda denetim planlanması, yürütülmesi ve raporlanması unsurlarını barındırmaktadır. "Act on External Audit of Stock Companies" düzenlemesi içerisinde anonim şirketlere yönelik dış denetim çalışmalarının düzenlenmesi unsurları bulunmakta, bilgi teknolojileri bağlamında ise muhasebe verisinin tanımlanması, üretilmesi, sınıflandırılması, raporlanması kapsamında tanımlamalar yer almaktadır.

Güney Kore'de 1954 yılında "Korean Institute of Certified Public Accountants" (KICPA) kurulmuştur. KICPA tarafından muhasebe ve denetim standartları yayımlanmıştır. "Kore Denetim Standartları" (Korean Standards on Auditing) dokümanı beraberinde standart uygulama rehberi ile birlikte KICPA tarafından düzenlenmiştir. Söz konusu standart ve uygulama rehberi içerisinde "Bilgisayar ve Bilgi Sistemleri Denetimi" başlığı altında planlama, risk değerlendirme ve denetim prosedürleri alt başlıkları içerisinde BT denetimine ilişkin düzenlemeler yer almaktadır. Detaylı olarak ise log kayıtları, görevler ayrılığı, bilgisayar destekli denetim teknikleri, verinin erişilebilirliği, bütünlüğü konuları bulunmaktadır.

Güney Kore'de BT denetimine yönelik detaylı düzenlemeler bulunmamaktadır. Ancak bilgi teknolojileri risklerinin değerlendirilmesi ve denetim çalışmaları kapsamına dâhil edilmesine yönelik farkındalık KICPA tarafından yayımlanan denetim standartları ile sağlanmaktadır.

Hollanda

Autoriteit Financiële Markten (AFM) Hollanda finansal hizmetler düzenleyici otoritesidir. Ayrıca AFM, Hollanda'daki ihtiyati tedbir düzenlemesinden sorumlu olan De Nederlandsche Bank (DNB) ile birlikte çalışmaktadır. Devlet makamları finansal kurumları (bankalar ve sigorta şirketleri gibi) ve finansal sistemi bir bütün olarak denetlemektedir. DNB ve AFM bu denetimleri yürütür. AFM, Hollanda'daki finansal piyasalar üzerindeki davranışların düzenlenmesinden sorumlu otorite olarak karşımıza çıkmaktadır. Bu, tasarruf, kredi, yatırım ve sigorta piyasaları ile ilgili tüm tarafların davranışlarının düzenlenmesini içerir. Bu düzenlemeler mali ürünler sunan tüm kuruluşları ve borsalar da dahil olmak tüm finansal kuruluşları kapsamaktadır. Kamu, işletme sektörü ve hükümet, birçok faaliyetleri için çeşitli pazarlarda sunulan finansal ürünlere bağımlıdır. Bu nedenle, bu pazarların düzenli ve dürüst çalışması konusundaki güveni sağlamakta da AFM görevlidir.

AFM dışında Hollanda'da denetim standartlarını belirleyen kuruluşlardan biri de Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA) kurumudur. NBA; kamuda, işletme sektöründe ve devlet nezdinde muhasebeciler ve denetçilerden oluşan Royal NIVRA ve üyeleri öncelikle muhasebeciler olan NOvAA organizasyonlarının birleşmesiyle 2013'te oluşmuştur.

Aralık 2012'de, Hollanda Denetim Mesleği Yasası NBA'in hukuki statüsünü oluşturmuş ve enstitünün görevini teşvik ederek mesleğin tanıtımını ve üyelerine hizmet etmeyi, mesleki standartları oluşturmayı ve üyelerin ilgili kurallara ve düzenlemelere uymasını sağlama görevini vermiştir. NBA, Türkiye'de SMMMO'nun olduğu gibi Hollanda'daki muhasebecilerin mesleki kurumudur. NBA üyeliği tüm denetçiler için zorunludur.

Hollanda'da denetim standartlarını belirleyen NBA, aynı zamanda IFAC üyesidir. IAASB tarafından ulusal standartlar olarak çıkartılan standartları, gerektiğinde yasal ve düzenleyici faktörlere uygun hale getirmek için bazı değişiklikler yaparak benimser ve ülkesine uyarlar. NBA yönetmelikleri, uluslararası standartların (ISA, ISRE, ISAE, ISARS, vb.) doğrudan çevirilerini içermektedir. ISQC 1 gereksinimleri Denetim Firmaları Denetim Yasası ve NBA düzenlemelerinde yer almaktadır.

Hollanda'daki BT denetçilerinin profesyonel derneği ise Nederlandse Orde van Register EDP-Auditors'dür (NOREA). NOREA üyeliği, BT denetimi alanında yüksek lisans veya doktora derslerini başarıyla tamamlayan ve meslekte en az üç yıllık tecrübesi olan adaylara açıktır. Söz konusu adayın uzmanlığı olumlu değerlendirildikten ve meslek kurallarına uymayı kabul ettikten sonra adları kamu defterine eklenebilir. Bu akreditasyon, profesyönellerin isimlerinin ardındaki "RE", yani Register EDP-Auditors harflerini, kendi uzmanlık düzeylerini belirten korumalı unvanının bir göstergesi olarak yerleştirmelerini sağlar. RE olmaya hak kazandıktan sonra, BT denetçilerinin her yıl belli bir sürelerin eğitime ayırması gerekir. NOREA da ayrıca IFAC üyesi bir kuruluştur ve IFAC'ın uluslararası standardını tanır.

Japonya

Japonya'da bankacılık, sigortacılık, menkul kıymetler ve borsa kapsamında gözetim ve düzenleme yetkisine sahip Finansal Servisler Kurumu (Financial Services Agency, "FSA) bulunmaktadır. Japonya'nın finansal sisteminin istikrarını sağlamakla yükümlüdür. FSA tarafından "Comprehensive Guidelines for Supervision of Financial Instruments" dokümanı yayımlanmıştır. Söz konusu doküman içerisinde "Control Environment for Managing Information Technology Risk" başlığı altında BT kapsamında kontrol ortamına ilişkin detaylı tanımlamalar yer almaktadır. Bilgi teknolojileri risklerinin üst yönetim tarafından tanınması, risk yönetimi için uygun kontrol ortamının tanımlanması, bilgi teknolojileri risklerinin değerlendirilmesi, bilgi güvenliğinin yönetimi, siber güvenliğin yönetilmesi, sistem geliştirme ve yönetimi, bilgisayar sistemleri denetimi, destek hizmetlerinin yönetimi, acil durum planı, sistem entegrasyon riskleri, sistem hatalarına yönelik aksiyonlar başlıkları altında detaylı bilgilere yer verilmiştir.

Kanada

Kanada Yeminli Mali Müşavirler Enstitüsü (CICA), Kanada'nın Yeminli Mali Müşavirliği mesleğini hem ulusal hem de uluslararası düzeyde temsil etmektedir. CICA, Uluslararası Muhasebeciler Federasyonu (IFAC) ve Global Accounting Alliance'ın (GAA) kurucu üyelerinden biridir.

Kanada'da CoCo iç kontrol model yaklaşımıkullanılmaktadır. İlgili model kapsamında BTdenetimi de ele alınmaktadır. CoCo modeliKanada Mali Müşavirler Odası tarafından içkontrol yapısının değerlendirilmesi amacıyla1995 yılında geliştirilmiştir. COSO modelinegöre daha pratik ve anlaşılırdır fakat etkisi yerelseviyede kalmıştır. Bu anlamda COSO İç Kontrolmodelinin üstlendiği uluslararası düzenlemestandartlarına ikame olacak bir model halinialamamıştır. COSO iç kontrol yapısının aksine,CoCo modelinde "iç kontrol" değil, sadece"kontrol" kavramı kullanılmıştır. CoCo, kontrolü,organizasyon amaçlarına ulaşılması için çalışanlarıdestekleyen ve bir arada tutan kaynaklar,sistemler, süreçler, kurum kültürü, kurumsal yapıve görevler gibi organizasyon unsurlarından biriolarak tanımlamıştır.

Ayrıca, Kanada Ontario eyaleti tarafından yayınlanan bilgi teknolojileri standartları bulunmaktadır. İlgili standartlar çerçevesinde bilgi teknolojileri kontrollerine yer verilmiş olup, standartlara ilişkin başlıklar aşağıda belirtilmiştir;

- Teknik Standartlar
- Mimari Standartlar
- Bilgi Standartları
- Bilgi Teknolojileri Servis Yönetimi
- Bilgi Teknolojileri Standartları
- Ağ Standartları
- Güvenlik Standartları

Yukarıda yer alan standartlar altında bilgi teknolojilerine ilişkin uyulması gereken bazı alt maddeler aşağıda belirtilmiştir;

- Uygulama Geliştirme Standardı
- Değişiklik Yönetimi Standardı
- Olay Yönetim Standardı
- Problem Yönetim Standardı
- Sürüm Yönetimi
- Genel Güvenlik Gereksinimleri
- Bulut Hizmetleri için Güvenlik Hizmetleri
- Veri Merkezi Fiziksel Güvenlik Standardı
- İşletim Sistemi ve Veritabanı YönetimSistemi Standardı

4. Seçilen Ülkeler Bazında Özet Bilgi

Dünya'da BT denetimine yönelik ülke düzenlemeleri incelendiğinde genel olarak düzenlemelerin iç kontrol/ iç denetim kapsamında ele alındığı, detaylı içerikten ziyade konu başlıklarının belirtildiği görülmektedir. Ülkelerde yer alan söz konusu düzenlemelerin içeriğinde ise aşağıdaki başlıkların karşımıza çıktığı görülmektedir;

Ülkeler Bazında BT Denetim Konuları

BT Denetim Konu Başlığı	İlgili Ülkeler
Erişim Yönetimi ve Görevler Ayrılığı	Almanya, Amerika, Birleşik Krallık, Güney Kore, Kanada
Verinin Bütünlüğü, Gizliliği, Erişilebilirliği	Almanya, Amerika, Birleşik Krallık, Güney Kore
Değişiklik Yönetimi	Almanya, Amerika, Birleşik Krallık, Kanada
BT Stratejisi ve Politikası	Almanya, Amerika, Birleşik Krallık
Farkındalık ve Eğitim	Almanya, Amerika, Birleşik Krallık
Denetim izi, Log Yönetimi	Almanya, Amerika, Birleşik Krallık, Güney Kore
BT Güvenliği	Almanya, Amerika, Birleşik Krallık, Japonya, Kanada
Konfigürasyon Yönetimi	Almanya, Amerika, Birleşik Krallık
Acil Durum Yönetimi, İş Sürekliliği Planı	Almanya, Amerika, Birleşik Krallık, Japonya
Olay yönetimi	Almanya, Amerika, Birleşik Krallık, Kanada
Fiziksel ve Çevresel Güvenlik	Almanya, Amerika, Birleşik Krallık, Kanada
Bilgi Sistemleri Risk Yönetimi	Almanya, Amerika, Birleşik Krallık, Güney Kore, Japonya
Bilgi Sistemleri Edinimi	Almanya, Amerika, Birleşik Krallık, Kanada
Geliştirilmesi ve Bakımı	Almanya, Amerika, Birleşik Krallık, Japonya, Kanada

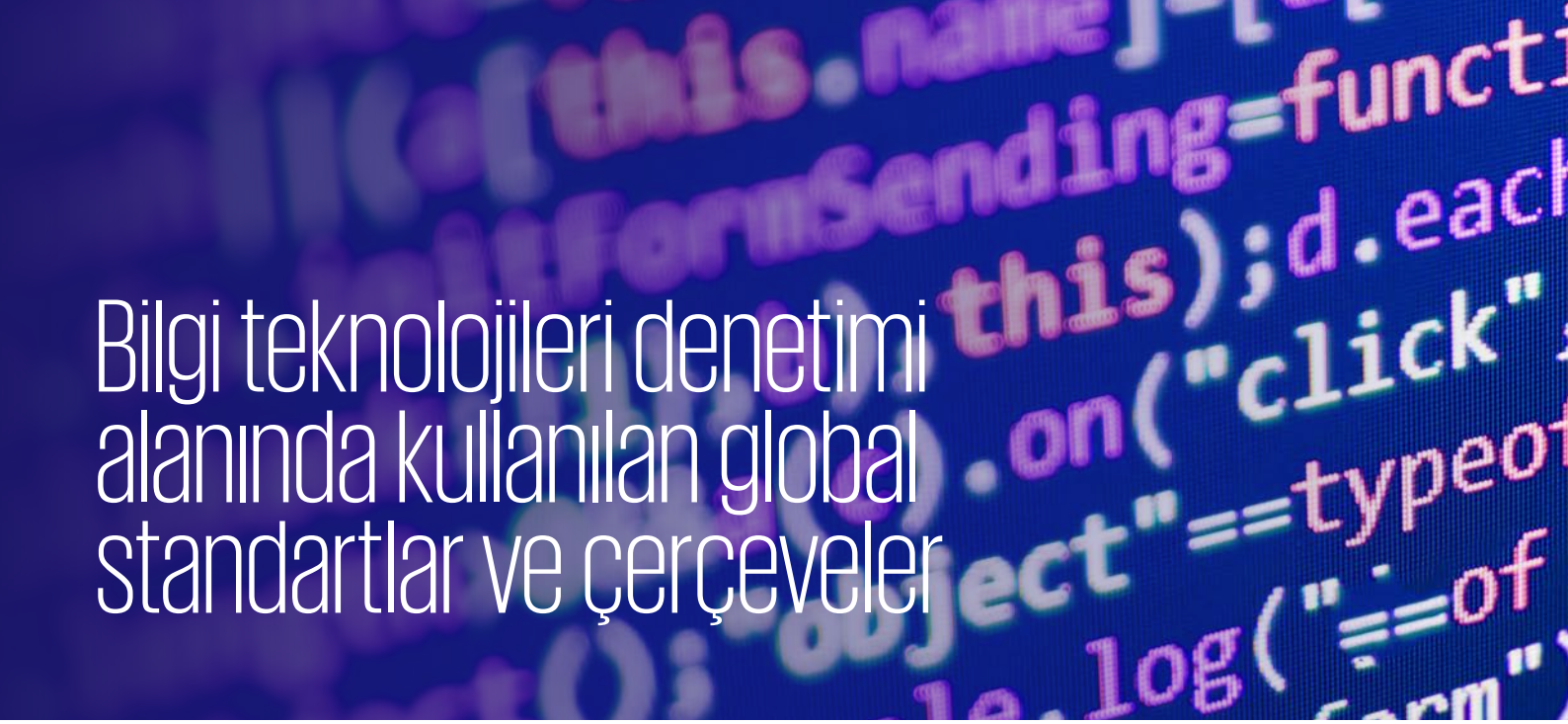
Söz konusu başlıklar, BT denetimi kavramı kapsamında dikkate alınan temel konular olarak belirlenmekle birlikte, seçilen ülkelerde risk değerlendirme ve denetim çalışmalarının kapsamını ve içeriğini oluşturmaktadır.

Bilgi Teknolojileri Denetimi ile ilgili Düzenlemeler ve Standartlar

Rapor kapsamında seçilen ülkeler ve söz konusu ülkelerde düzenleyici otoriteler ve bu düzenleyici otoriteler tarafından yayınlanmış ve bilgi teknolojileri kapsamında denetim ve risk değerlendirme çalışmaları ile ilgili yasal düzenlemeler ve standartlara ilişkin özet bilgi ülke bazında aşağıdaki tabloda sunulmuştur.

Ülke	İlgili Otorite	Düzenleme ve Standartlar
Almanya	• German Federal Supervisory Authority (BaFin) • Federal Office for Information Security (BSI)	• Bankacılık Kanunu (25a) • MaRisk (7.2) • Federal Bilgi Teknolojisinin Güvenliğini Güçlendirme Kanunu
Amerika Birleşik Devletleri	• National Institute of Standards and Technology (NIST) • The Financial Industry Regulatory Authority (FINRA) • Government Accountability Office (GAO) • Public Company Accounting Oversight Board (PCAOB) • The Institute of Internal Auditors (IIA) • American Institute of Chartered Public Accountants (AICPA)	• Sarbanes Oxley Kanunu (SOX) • Federal Bilgi Sistemleri için Güvenlik ve Gizlilik Kontrolleri • Federal Bilgi Güvenliği Yönetim Kanunu (FISMA) • Bilgi Teknolojileri Sistemlerinin Güvenliği İçin Genel Olarak Kabul Edilen İlkeler ve Uygulamalar (GAPP) • Kontroller ve Güvenlik Denetim Rehberi: Sistem Geliştirme Yaşam Döngüsü Yaklaşımı • Bilgi Teknolojisi Sistemleri için Güvenlik Öz-Değerlendirme Kılavuzu (SSAG) • Devlet Denetim Standartları (GAGAS) • Federal Bilgi Sistemi Kontrol Denetim Kılavuzu (FISCAM) • Elektronik Sistemler Güvencesi ve Kontrolü (eSAC) • Sistem Güvenilirliği için SysTrust İlke ve Kriterleri
Birleşik Krallık	• Financial Services Authority (FSA)	• Kıdemli Yönetim Düzenlemeleri, Sistemler ve Kontroller (SYSC13)
Güney Kore	• Korean Institute of Certified Public Accountants (KICPA) • Board of Audit and Inspection of Korea	• Standartlar için Uygulama Rehberiyle Denetim Üzerindeki Kore Standartları • Denetim ve Teftiş Kurulu Kanunu • Kamu Sektörü Denetimleri Hakkında Kanun • Hisse Senedi Şirketlerinin Dış Denetimi Hakkında Kanun
Hollanda	• Autoriteit Financiële Markten (AFM) • De Nederlandsche Bank (DNB)	• IAASB tarafından ulusal standartlar olarak çıkartılan standartları, gerektiğinde yasal ve düzenleyici faktörlere uygun hale getirmek için bazı değişiklikler yaparak benimsenir ve ülkeye uyarlanır.
Japonya	• Financial Services Agency (FSA)	• Finansal Araçların Denetimi için Kapsamlı Kılavuz • Finansal Enstrümanlar İş Süreçleri Teftiş Kılavuzu
Kanada	• Chartered Professional Accounts of Canada (CICA) • Canadian Public Accountability Board (CAASB)	• CoCo İç Kontrol Modeli • ISA Standartları

Bu ülkelerde BT kapsamında risk değerlendirme ve denetim unsurları doğrultusunda hükümler barındıran yasal düzenlemeler ve standartların detaylı içeriğine "3. Bilgi Teknolojileri Risk ve Güvence Düzenlemeleri" başlığı altında yer verilmiştir.



Bilgi teknolojileri denetimi alanında kullanılan global standartlar ve çerçeveler

1. COSO İç Kontrol Modeli

İç kontrol kurumların hedeflerine ulaşması ve misyonlarını gerçekleştirmesi; bu yolda ilerlerken önlerine çıkabilecek belirsizliklerin en aza indirilmesi amacıyla uygulanan süreçtir. İç kontrol, kurumların sürekli değişen çevre koşulları, hizmet alanların talepleri ve öncelikleri ile gelecekte ortaya çıkabilecek tehdit unsuru olan veya fırsatlar yaratabilecek risklerle başa çıkabilmeleri için yönetimi güçlendirir. Diğer bir ifadeyle iç kontrol, kurumun, yönetimi ve personeli tarafından hayata geçirilen, belirlenmiş hedeflere ulaşmasında ve misyonunu gerçekleştirmesinde makul bir güvence sağlamak üzere tasarlanmış ve kurumun genelini etkileyen bütünleşmiş bir süreçtir. İç kontrol standartları, iç kontrol sisteminin uygulama esnasında başvurduğu temel ilkelerdir.

Teknolojik gelişmeler ve küreselleşmenin etkisiyle 1980'lerle birlikte işletme yönetimi çok karmaşık bir yapıya bürünmüştür. Bu karmaşık yönetim sistemleri işletme yönetimine ve denetim organlarına bilgi sağlamak için standartları belirlenmiş iç kontrol yapılarının oluşturulmasına zemin hazırlamıştır. Bu amaçla çalışmalarına başlayan muhasebe ve denetim örgütleri, ABD'de COSO, SAC ve COBIT iç kontrol modellerini, Kanada'da CoCo modellerini ortaya koymuşlardır. Bu çalışmalar etkin bir iç kontrol yapısının oluşturulması amacıyla tasarlanmış olmakla birlikte farklı kuruluşlar tarafından hazırlandığından tasarlandığı dönem ve öncelikleri dikkate alınarak oluşturulmuş modelleridir.

COSO, iç kontrol sistemini beş katman veya birbiri ile bağlantılı bileşenlerden oluşan bir piramit olarak tanımlamaktadır. Bu bileşenler:

Risk değerlendirme süreci ileriye yönelik bir süreçtir ve birçok işletme çeşitli seviyelerdeki riskleri değerlendirmek için en uygun zamanın yıllık veya belirli aralıklarla yapılan planlama süreçleri olduğunu düşünmektedir. COSO risk değerlendirme sürecini üç adımda tanımlamaktadır.

- Riskin öneminin tahmin edilmesi,
- Riskin gerçekleşme ihtimalinin veya sıklığının değerlendirilmesi,
- Riskin nasıl yönetilmesi gerektiğinin belirlenmesi ve ne gibi önlemler alınması gerektiğine karar verilmesidir.

Kontrol faaliyetleri, işletmenin amaçlarına ulaşması için olası riskleri önlemek amacıyla gerekli eylemlerin yapılmasını sağlayan politika ve yöntemlerdir. Kontrol faaliyetlerinde yönetim, kullandığı yöntemlerle çalışanlarına işletme amaçlarını ve bu amaçlara ulaşma yollarını göstererek, ortaya çıkan sonuçları değerleme yoluna gider. Kontrol faaliyetleri, kontrol ortamının zayıf olduğu durumlarda, zayıflığın etkisini hafifletmektedir.

Tüm işletmede veya bir işlev ya da bölüm seviyesinde uygulanabilen kontrol faaliyetleri, aşağıdaki unsurları içerir:

Performans değerlendirmesi,

- Görev ayrımı,
- Fiziksel kontroller,
- Bilgi isleme kontrolleri,
- Kontrol prosedürlerinin anlaşılmış olması.

COSO, çeşitli kişi ve gruplar ve bunların beklentileri söz konusu olduğunda iletişimin daha geniş kapsamlı bir şekilde ele alınması gerektiğini vurgulamıştır. COSO'ya göre, iletişimin belki de en önemli bileşeni üst yönetim tarafından çalışanlara belirli aralıklarla iç kontrol sorumluluklarının çok önemsenmesi gerektiğini hatırlatan mesajlar göndermesidir. Gönderilen bu mesajların açık olması işletmenin etkin iç kontrol ilkelerini takip edebilmesi açısından önem taşımaktadır.

İç kontrol yapılarının zaman içindeki performans ve kalitesinin değerlendirilmesi gerekmektedir. İzlemenin amacı, işletmelerdeki mevcut iç kontrol yapısının uygun biçimde tasarlanıp tasarlanmadığı, doğru şekilde uygulanıp uygulanmadığı ve etkili olup olmadığına karar vermektir.

2. CoCo İç Kontrol Modeli

CoCo çerçevesi, CICA tarafından 1995 yılında "Kontrol Rehberi" (Guidance on Control) ismiyle yayımlanmıştır. Kısaca "CoCo Raporu" olarak da isimlendirilen çalışmada, iç kontrol sisteminin etkinliğini ölçmeye yönelik çeşitli ölçütler ele alınmaktadır. CoCo, kontrolü işletmenin amaçlarına ulaşması için çalışanları destekleyen ve bir arada tutan kaynaklar, sistemler, süreçler, kurum kültürü, kurumsal yapı ve görevler gibi işletme unsurlarından biri olarak kabul etmiştir.

CoCo modelinde kontrol rehberinin oluşturulmasına üç gerekçe gösterilmektedir.

- Kuruluşun denetim etkinliğinin arttırılması için genel raporlamaya ihtiyaç vardır.
- Kuruluşların pek çoğunda artan rekabet ortamı ve küresel rekabet ortamı nedeniyle kontrol sistemleri değişikliğine ihtiyaç vardır.
- Kuruluşların değerlerin paylaşımı ve açık iletişim kanalları gibi farklı kontrol mekanizmalarına ihtiyacı vardır.

CoCo, kontrol rehberinde iç kontrol amaçlarının değerlendirilmesinde kullanılabilecek yirmi tane spesifik kriter belirlemiş ve bunları 5 kriterden oluşan amaç (purpose), 4 kriterden oluşan sorumluluk (commitment), 5 kriterden oluşan yeterlilik (capability), 6 kriterden oluşan izleme ve öğrenme (monitoring and learning) olarak dört ana başlık altında toplamıştır. CoCo, belirlediği 20 kriteri, iç kontrolün herhangi bir bileşeninin değerlendirilmesinde her çeşit spesifik amaca uygulanabileceğini savunmaktadır. CoCo, kurumun amaçlarına ulaşmasında kontrolün vereceği makul güvencenin, kontrolün etkinliğiyle doğru orantılı olduğunu belirtmektedir.

CoCo modelindeki amaç bölümü, kurumun yönünü tayin etmektedir. Kurumun amaçları, risk yönetimi, planlar ve performans hedefleri bulunmakta olup, belirlenen amaçlar tüm işletme çalışanlarına iletilmelidir. Amaçlara ulaşılmasını engelleyeceği düşünülen bütün önemli iç ve dış riskler belirlenmeli ve incelenmelidir.

CoCo modelindeki sorumluluk bölümü, kurum kimliğini ve ahlaki değerlerini, insan kaynakları politikalarını, yetki ve sorumlulukları ve karşılıklı güveni kapsamaktadır. İlk önce dürüstlük olmak üzere, ahlaki değerler belirlenmeli, çalışanlara iletilmeli ve tüm şirket içinde uygulanmalıdır. İnsan kaynakları yöntemleri ve uygulamaları, şirketin ahlaki değerleriyle ve amaçlarıyla uyumlu olmalıdır. İşletmenin amaçlarına ulaşılmasına yönelik performansı artırmak ve işletme çalışanları arasındaki bilgi alış verişini güçlendirmek için karşılıklı güven ortamı oluşturulmalıdır.

CoCo modelindeki yeterlilik bölümü, çalışanların, bilgi sistemlerinin ve kontrol faaliyetlerinin sahip olması gereken nitelikleri belirlemektedir. İşletme çalışanlarının, işletmenin amaçlarına ulaşmasına yardımcı olabilmeleri için gerekli bilgi, beceri ve donanıma sahip olmaları gerekir. Bilgi iletişim sistemi, firma değerlerini ve amaçlara ulaşılmasını desteklemelidir. Kontrol faaliyetleri, amaçlar, riskler ve kontrol unsurları arasındaki iç bağlantı dikkate alınmalı ve örgütün bütüncül bir parçası olarak tasarlanmalıdır.

CoCo modelindeki izleme ve öğrenme bölümü, kurumsal gelişmenin ve çevresel değişimin sürekli olarak izlenmesini sağlar. Performansın, bilgi sistemlerinin ve kontrolün etkinliğinin değerlendirilmesini ve iş takip yöntemlerini içermektedir.

3. SOX Kapsamında Gerçekleştirilen BT ve Süreç Denetimleri

ABD'de meydana gelen Enron, Worldcom ve Xerox gibi büyük şirketlerin finansal skandallarından sonra 2002 yılında yürürlüğe giren SOX ile halka açık şirketlerin denetiminin izlenmesi, denetçi bağımsızlığının güçlendirilmesi, şirket sorumluluğunun ve üst yönetim düzeyinde açıklama sorumluluğunun artırılması, halka açık şirketlerin finansal raporlama sürecindeki kalite ve şeffaflığın artırılması ve kurumsal yönetimin arttırılması konu başlıklarında düzenlemeler getirilmiştir. SOX yasası, ilk etapta PCAOB adında bir kamusal kurum kurulmasını hüküm altına almıştır. Bu kurumu halka açık şirketleri denetlemekle görevli şirketleri gözetim altında tutmak, denetlemek, disipline etmek ve gerekli mevzuatı oluşturmak üzere yetkilendirmiştir. Yasa denetim olgusu üzerinde hassasiyetle durmakta ve denetçinin bağımsızlığı, kurumsal yönetişim, iç kontrol sisteminin değerlendirilmesi, geliştirilmiş kamu aydınlatma sistemi gibi konuları da içermektedir.

Bağımsız denetimle ilgili temel düzenlemeler bu yasanın 4 numaralı, "Gelişmiş Finansal Bilgi Açıklamaları" başlıklı kısmında bulunan 404 numaralı, "Yönetimin İç Kontrole İlişkin Değerlendirmesi" alt başlık altında yer almaktadır. 404 numaralı alt başlık altındaki hükümler genel olarak halka açık şirketlerin yönetimine ve bağımsız denetçilere bazı sorumluluklar yüklemektedir. Örneğin, şirketin finansal raporlamasına yönelik iç kontrol sürecinin yeterliliğinin raporlanması; şirket yönetiminin yıllık faaliyet raporunda bir iç denetim raporuna da yer vermesi; finansal raporlama için uygun bir iç denetim yapısının oluşturulması ve bunun devam ettirilmesinin şirket yönetiminin sorumluluğunda olduğunun belirtilmesi, yılsonu itibariyle şirketin iç denetim yapısının ve denetime ilişkin prosedürlerinin etkinliğin değerlendirilmesi vb. Finansal bilginin bilgi sistemleri kapsamında işlenmesi, üretilmesi ve saklanması nedeniyle bilgi teknolojileri SOX 404 kapsamında iç kontrol ortamı içerisinde önemli bir parça olarak tanımlanmaktadır.

Söz konusu durumlar birlikte değerlendirildiğinde, ortaya SOX bazlı BT denetimi kavramı çıkmaktadır. Yasanın yukarıda belirtilen 404 numaralı bölümünde ifade edilen amaçların sağlanabilmesi çerçevesinde PCAOB tarafından belirli standartlar hazırlanmış olup, bu doğrultudaki BT ve süreç denetim çalışmalarında ise söz konusu standartlar baz alınmaktadır.

4. PCAOB Denetim Standartları

SOX yasasının bir önceki maddede belirtilen 404 numaralı bölümünde ifade edilen amaçların sağlanabilmesi çerçevesinde PCAOB tarafından belirli standartlar hazırlanmış olup, SEC onayı sonrasında bu standartlar kullanılmaya başlanmıştır. Bu denetim standartlarına "SEC Onaylı Denetim Standartları" da denilmektedir. Ayrıca, söz konusu standartların dışında "Geçici Standartlar" denilen bir başka grup denetim standardı daha bulunmaktadır. Bu standartlara ise "Genel Kabul Görmüş Denetim Standartları" denilmekte olup, değiştirilmediği veya yürürlükten kaldırılmadığı sürece ABD'de yapılacak bağımsız denetim çalışmalarında uygulanmaları zorunludur. Dolayısıyla ABD'de geçerli bağımsız denetim anlayışı SOX yasası çerçevesinde denetimle ilgili olarak ortaya konulan mevcut standartların yanı sıra "Genel Kabul Görmüş Denetim Standartları" da kullanmaktadır.

Söz konusu standartlar BT denetimi açısından incelenecek olursa karşımıza AS2201 (An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements) standardı karşımıza çıkmaktadır. Finansal raporlama üzerindeki iç kontrolün etkinliğinin değerlendirilmesi kapsamında bilgi teknolojileri ele alınmaktadır. Madde 27 içerisinde bilgi teknolojilerinin finansal raporlama sürecindeki yerinin denetçi tarafından değerlendirilmesi gerektiği, madde 36 içerisinde denetçinin bilgi teknolojilerinin iş süreçlerini nasıl etkilediğinin anlaşılması gerektiği, finansal raporlamaya ilişkin iç kontrollere etkisinin değerlendirilmesi gerektiği belirtilmektedir. Ek olarak madde 47 içerisinde kontroller kapsamında bilgi teknolojileri kontrolleri ele alınmakta, söz konusu kontrollerin etkinliğinin değerlendirilmesi gerekliliği belirtilmektedir. Dolayısıyla iç kontrolün değerlendirmesi kapsamına bilgi teknolojileri kontrolleri dahil edilmekte, BT denetim çalışmaları iç kontrolün değerlendirilmesi çalışmaları kapsamında yürütülmektedir. Bu doğrultuda PCAOB tarafından yayımlanan denetim raporu, denetim planlanması, denetim görüşü ve denetçi yetkilendirmesi kapsamında AS standartları bilgi teknolojileri denetim çalışmaları için de geçerli olmaktadır.

5. IFAC / IAASB Denetim Standartları

IFAC bünyesinde yer alan IAASB tarafından yayınlanmış olan denetim ve güvence standartlarında bilgi teknolojilerine özel olarak bir bölümde veya standartta değinilmemesine rağmen; bağımsız denetim şirketleri tarafından bu standartların uygulanmasında, denetim çalışmalarına bilgi sistemleri denetimi bileşenlerinin de dâhil edildiği bilinmektedir.

IFAC tarafından yayınlanmış olan ISA bilgi sistemleri denetimine ilişkin kontroller; ISA 300, ISA 315, ISA 330 ve ISA 402 standartlarında belirtilmiştir. Bu standartlar içerisinde özellikle, mali denetimler içerisinde bilgi sistemleri uzmanlığına sahip kişilerin görevlendirilmesinden; süreçlerdeki otomatik kontrollerin değerlendirilmesi gerektiğinden ve genel denetim metodolojisinin oluşturulmasında bilgi sistemleri yapısındaki değişikliklerin de dikkate alınması gerektiğinden bahsedilmektedir.

Söz konusu ISA denetim standartları yandaki gibidir;

- ISA 300 (Planning an Audit of Financial Statements)
- ISA 315 (Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and Its Environment) madde 18 içerisinde iş süreçleri ve finansal raporlar kapsamında bilgi sistemlerinin anlaşılması gerekliliği belirtilmektedir. Ek olarak madde A54, A55, A56 ve A81 içerisinde bilgi sistemleri iç kontrol ilişkisi ifade edilmektedir. A95 ve A96 içerisinde ise bilgi sistemlerin kaynaklanan risk unsurları ve risk grupları tanımlanmaktadır. (Sistem odası, yazılım edinimi, değişiklik yönetimi, bakım, erişim güvenliği, uygulama sistemleri edinimi, geliştirilmesi ve bakımı vb.)
- ISA 330 (The Auditor's Responses to Assessed Risks) içerisinde madde 42 içerisinde genel BT kontrollerinin etkinliğinin değerlendirilmesi kavramına değinilmektedir.
- ISA 402 (Audit Considerations Relating to An Entity Using A Service Organization)

6. COBIT

COBIT, ilk olarak 1996'da Information Systems Audit and Control Foundation (ISACF) tarafından yayımlanmıştır. Günümüzdeki başlıca yayımcısı ISACA tarafından 1998'de kurulan BT Yönetişim Enstitüsüdür (ITGI). COBIT; ISO teknik standartları, ISACA ve AB tarafından yayınlanan yönetim kanunları, COSO, AICPA3, GAO4 tarafından yayınlanan profesyonel iç kontrol ve denetim standartları tarafından biçimlendirilmiştir.

COBIT'in temel amacı süreç performans metriklerini ve olgunluk modellerini belirleyerek ve BT'nin iş sorumluluklarını tayin ederek, iş hedefleriyle BT hedeflerini bağdaştırmaktır. Birçok kurum için bilgi ve bilgi teknolojileri en değerli fakat en az anlaşılan varlıktır.

BT yönetişimi; değer, risk ve kontrol üzerine kuruludur. COBIT BT yönetişimi için temel hedefleri ve bileşenleri sunmaktadır.

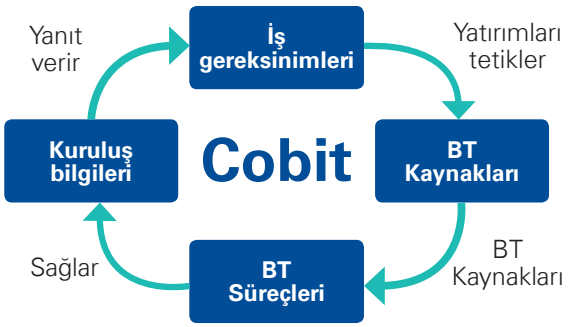
COBIT, aşağıda belirtilen maddeler kapsamında hedefe ulaşmayı amaçlar;İş gereksinimlerine bağlantı kurarak,

1. BT aktivitelerini genel kabul görmüş süreç modelleriyle organize ederek,
2. Esas gerekli BT kaynaklarını ayırt ederek,
3. Yönetim kontrol hedeflerini tanımlayarak.

COBIT, genel anlamda dört ana başlık altında öneriler getirir ve kontrol noktaları belirler:

- Planlama ve Organizasyon (PO)
- Tedarik ve Uygulama (AI)
- Teslimat ve Destek (DS)
- İzleme ve Değerlendirme (ME)

COBIT, bazı ülkelerde çeşitli sektörler için yasal düzenleme olarak da kullanılmakta olup, ülkemizdeki en somut örneği ise bankacılık sektörü için Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) tarafından regüle edilmiş olmasıdır.



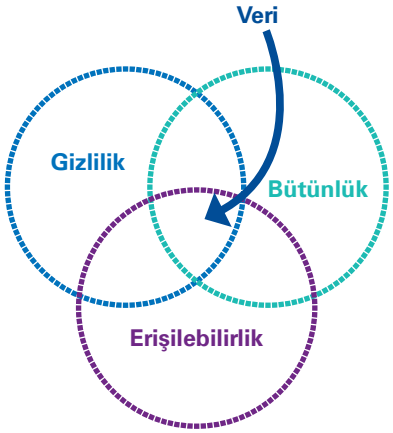
7. ISO 27001 Bilgi Güvenliği Yönetim Sistemi

ISO 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) kuruluşların gelişen teknolojiyle beraber her geçen gün daha fazla iş yüklediği ve ihtiyaç duyduğu bilgi sistemlerinin güvenliğini sağlamaya yönelik oluşturulmuş bir modeldir.

ISO 27001 kuruluşların risk yönetimi ve risk işleme planlarını, görev ve sorumlulukları, iş devamlılığı planlarını, acil durum olay yönetimi prosedürleri hazırlamasını ve uygulamada bunların kayıtlarını tutmasını gerektirir.

Kuruluş tüm bu faaliyetlerin de içinde yer aldığı bir bilgi güvenliği politikası yayınlamalı ve personelini bilgi güvenliği ve tehditler hakkında bilinçlendirmelidir. Seçilen kontrol hedeflerinin ölçülmesi ve kontrollerin amacına uygunluğunun ve performansının sürekli takip edildiği yaşayan bir süreç olarak bilgi güvenliği yönetimi ancak yönetimin aktif desteği ve personelin katılımcılığıyla başarılabilir.

BGYS sayesinde kuruluşlar bilgi sistemleri altyapısında belirledikleri varlıklara yönelik olası tehlikeleri analiz ederek, bu risklerin oluşması durumunda hangi kontrolleri uygulayacaklarına ve hangi kontrolleri uygulamayacaklarına karar verirler. ISO 27001 standardının amacı bilginin gizliliğini, erişilebilirliğini ve bütünlüğünü korumaktır.



8. Bilgi Sistemleri ve Ağlarının Güvenliği Rehberi

Bilgi Sistemleri ve Ağlarının Güvenliği Rehberi (Guidelines For The Security of Information Systems and Networks), OECD tarafından hazırlanmış olup, 2002 yılında yayımlanmıştır. Standart içerisinde temel olarak dokuz farklı prensip yer almaktadır. Söz konusu prensipler;

- Sorumluluk,
- Farkındalık,
- Etik,
- Multidisipliner,
- Orantılılık,
- Entegrasyon,
- Dönemsellik,
- Yeniden Değerlendirme,
- Demokrasidir.

Bu doğrultuda bilgi sistemlerinin güvenliğine ilişkin sorumluluklar, bilgi sistemlerinin güvenlik gereksinimlerine ilişkin farkındalık, paydaşların gereksinimlerinin dikkate alındığı etik yaklaşım, demokratiklik değerleri ile uyumluluk, kontrollerin maliyeti ile risklerin maliyetinin dengelendiği orantılılık, periyodik gözden geçirme unsurları rehber kapsamında yer alınmaktadır.

9. GASSP

GASSP International Information Security Foundation (I2SF) tarafından hazırlanmış olup, 1998 yılında yayımlanmıştır. GASSP kapsamında OECD tarafından hazırlanan "Information Security Principles" baz alınmıştır. Dolayısıyla sorumluluk, farkındalık, etik, çok disiplinli yaklaşım, orantılılık, entegrasyon, dönemsellik, yeniden değerlendirme ve demokrasi prensipleri GASSP içinde geçerlidir.

Standart içerisinde yer alan fonksiyonel prensipler ise aşağıda yer almaktadır;

- Bilgi Güvenliği Politikası,
- Eğitim ve Farkındalık,
- İzlenebilirlik,
- Veri Yönetimi,
- Çevre Yönetimi,
- Personel Nitelikleri,
- Sistem Bütünlüğü,
- Bilgi Sistemleri Yaşam Döngüsü,
- Erişim Kontrolü,
- Operasyonel Sürekliliği ve Acil Durum Planlaması,
- Bilgi Sistemleri Risk Yönetimi,
- Ağ ve Altyapı Güvenliği,
- Bilgi Güvenliği Kapsamında Yasal ve Sözleşmesel Gereksinimler,
- Etik Prosedürler.

10. Standart ve Çerçeve İçerikleri Hakkında Özet Bilgi

Dünya'da BT denetimine yönelik global standartlar incelendiğinde belirli ana başlıklar karşımıza çıkmaktadır. Odaklanan unsur doğrultusunda içeriklerin detayları farklılık göstermekle birlikte, BT denetimi ve risk değerlendirmesi doğrultusunda temel olarak ele alınan konular aşağıdaki gibi gruplanabilir:

- Verinin Gizliliği, Bütünlüğü, Erişilebilirliği
- Bilgi Sistemleri Risk Yönetimi
- İş Sürekliliği ve Acil Durum Planlaması
- Değişiklik Yönetimi
- Erişim, Kullanıcı Hakları Yönetimi
- Problem ve Olay Yönetimi
- Program Yönetimi
- Fiziksel ve Çevresel Güvenlik
- Log Yönetimi
- BT Güvenliği (Politika, Farkındalık, Eğitim, Prosedür, Plan)
- BT Operasyonlarının Yönetimi

Söz konusu konu başlıkları ile birlikte küresel çerçeveler ve iç kontrol modelleri ile BT denetimi ve risk değerlendirilmesi süreçlerini düzenleyen denetim başlığı altında ifade edilmiş çeşitli tanımlamalar bulunmaktadır.

Çalışma çıktıları, yetkilendirme, BT denetiminin denetim çalışmaları içerisindeki konumu vb. konular bu tanımlamalar dâhilinde yer almaktadır.

Bilgi teknolojileri denetimi süreci

1. Bilgi Teknolojileri Denetim Sertifikaları

Denetime ilişkin mevzuatın önemli bir bileşeni de denetim kuruluşlarının ve denetçilerinin yetkilendirilmesi olarak karşımıza çıkıyor.

Türkiye'de BDDK'nın uygulamalarına benzer olarak birçok ülkenin, denetçiler için; CISA ve benzeri sertifikasyona ve belirli bir mesleki tecrübeye sahip olunmasını ön koşul olarak belirlediğini görüyoruz.

CISA sertifikasyon programı ISACA tarafından yürütülen bir program olup, bilgi sistemleri denetimi alanında dünya genelinde kabul görmektedir. CISA sertifikasyon sınavı bilgi sistemleri denetçilerinin sahip olması gereken denetim nosyonu, temel bilgi teknolojileri altyapısı ve kontrolleri bilgisini sınamaya yönelik bir sınavdır. Sınavı geçmenin yanı sıra deneyim koşuluyla birlikte bu teorik bilginin pratik deneyimle desteklenmesi sertifikasyon için ön koşuldur.

Diğer bir taraftan Hollanda'da ise global sertifikasyon programlarının yanı sıra, bilgi sistemleri denetçileri; serbest muhasebeci mali müşavirlik akreditasyonuna benzer şekilde; ulusal düzeyde bir bilgi sistemleri denetimi meslek birliği ve yüksek öğrenim destekli yerel bir sertifikasyon programına sahip:

NOREA BT denetçilerinin profesyonel derneğidir.

NOREA üyeliği, BT denetimi alanında yüksek öğrenim derslerini başarıyla tamamlayan ve meslekte en az üç yıllık tecrübesi olan adaylara açıktır. Hollanda'da yaklaşık olarak 1000 kişi RE sertifikasına sahiptir.

IFAC üyesi bir kuruluştur ve uluslararası denetim ve güvence standartlarını tanımaktadır.

Regülasyonların öngördüğü ayrı bir BT denetimi raporu ve bireysel olarak denetçi yetkilendirmesi söz konusu olmadığı için, RE sertifikasyonu herhangi bir sektörde BT denetimi gerçekleştirebilmek için bir zorunluluk olarak tutulmuyor.

Hollanda örneğine kıyasla, incelenen çoğu ülkede, BT denetçileri için ayrı bir oda, meslek birliği veya ISACA haricinde farklı bir dernek bulunmadığı görülmektedir.

Fakat, örnek seçilen ülkelerde, IFAC ve PCAOB kuralları doğrultusunda finansal denetim raporlarından ayrı bir BT Denetim Raporu'nun bir zorunluluk olmadığı, bu nedenle mevzuat nezdinde BT denetiminin "sorumluluk" atamasının ayrı olarak yapılmadığı göz önüne alındığında, bağımsız denetim kuruluşlarının gözetim kuruluşları tarafından "mali denetim" yapmak üzere yetkilendirildiği, ancak genel olarak BT denetimi yapmak üzere ayrı bir kuruluş veya denetçi yetkilendirmesi bulunmadığı görülmektedir.

Bu durumun istisnası olarak ise, Türkiye'de BDDK tarafından "Bankalarda Bilgi Sistemleri Denetimi Yapmaya Yetkili Bağımsız Denetim Kuruluşları"nın ve bu kuruluşlar nezdinde yetkilendirilen BS denetçilerinin bulunması sayılabilir. BDDK tarafından yayınlanmış olan "Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik" uyarınca, Bilgi Sistemleri Bağımsız Başdenetçisi'nin bilgi sistemleri ve bankacılık süreçleri raporuyla ilgili sorumluluğu üstlendiği ve bu ünvana sahip olabilmek için asgari 10 yıllık tecrübeyle birlikte CISA sertifikasının ön koşul olarak bulunduğu görülmektedir.

Kişiler BT Denetçisi Olarak Yetkilendiriliyor mu?	
BDDK (Türkiye)	Evet (CISA sertifikası ve asgari 10 yıl tecrübe)
PCAOB (ABD)	Hayır
IFAC (Global)	Hayır
Hollanda	Hayır (RE sertifikası herhangi bir sektörde BT denetimi gerçekleştirmek için zorunlu tutulmuyor)

2. Bilgi Teknolojileri Denetim Kapsamı

Türk Ticaret Kanunu'nun 397. Maddesinde açıklandığı üzere; denetime tabi olan anonim şirketlerin ve şirketler topluluğunun finansal tabloları denetçi tarafından, "Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumu"nca yayımlanan uluslararası denetim standartlarıyla uyumlu Türkiye Denetim Standartları'na göre denetlenir.

19 Mart 2016 tarihli Resmi Gazete'de 2016/8549 sayılı "Bağımsız Denetime Tabi Olacak Şirketlerin Belirlenmesine Dair Kararda Değişiklik Yapılması Hakkında Karar" da ve aşağıdaki şartlardan en az ikisini art arda iki hesap döneminde aşan şirketler bağımsız denetime tabi olacakları belirlenmiştir.

- Aktif toplamı 40 milyon ve üstü Türk Lirası
- Yıllık net satış hasılatı 80 milyon ve üstü Türk Lirası
- Çalışan sayısı 200 ve üstü

Denetim kapsamına giren firma denetimlerinde Uluslararası Finansal Raporlama Standartları'na (UFRS) uyumlu Türkiye Finansal Raporlama Standartları'na (TFRS) göre hazırlanan mali tabloların denetimi yapılmaktadır. Türkiye'de yukarıda belirtilen şirketlere yönelik olarak gerçekleştirilecek bağımsız denetimin çalışmalarının, IFAC tarafından yayımlanan uluslararası standartları referans alarak hazırlanmış olan Uluslararası Bağımsız Denetim Standartları (BDS) çerçevesinde yürütülmesi gerekmektedir.

IFAC dünya genelinde birçok ülkeden farklı kurumların üyeliği ile oluşmaktadır. Uluslararası Muhasebeciler Federasyonu'nun misyonu, kamu çıkarına hizmet etmek, dünya genelinde muhasebe mesleğini güçlendirmek, yüksek kaliteli uluslararası standartlar ve kılavuzluk geliştirilmesi, benimsenmesi ve uygulamaya konmasına katkı sağlayarak; güçlü muhasebe meslek organizasyonları ve muhasebe firmalarının gelişimine ve muhasebe meslek mensupları tarafından yüksek kaliteli uygulamalara katkı sağlayarak; dünya genelinde muhasebe meslek mensuplarının değerini artırarak; muhasebe mesleğinin uzmanlığının en alakalı olduğu yerlerde kamu çıkarı meseleleri hakkında görüş bildirerek, kamu çıkarına hizmet etmektir. IFAC'ın yayınladığı standartlar içerisinde bilgi sistemleri denetimine ilişkin kontrolleri tanımlamıştır.

Ayrıca, Türkiye'deki Bankalar BDDK tarafından yetkilendirilmiş bağımsız denetim kuruluşlarınca her yıl süreç denetimi, her iki yılda bir ise bilgi sistemleri denetimine tabi tutulmaktadır. Yetkilendirilen bağımsız denetim kuruluşlarınca gerçekleştirilen denetimde COBIT standardı baz alınmaktadır.

Diğer bir taraftan SEC'e yıllık bazda raporlama yapma zorunluluğu bulunan tüm kuruluşlar SOX denetimine tabi tutulmaktadır. SOX kapsamında bilgi sistemleri özelinde bir düzenleme bulunmamakla birlikte, "finansal raporlara süreçleri üzerindeki iç kontrol ortamı"na hem iç denetçi hem de bağımsız denetçi tarafından güvence verilmesi, bilgi sistemlerine ilişkin genel kontrollerin ve iş süreçlerindeki otomatik kontrollerin değerlendirilmesi gerekmektedir.

BT Denetim Zorunluluğu Var mı?		Kapsam Bilgisi
BDDK (Türkiye)	Bankalar özelinde her yıl süreç denetimi, iki yılda bir ise zorunlu BT denetimi gerçekleştirilmektedir.	BDDK düzenlemeleri ve COBIT 4.1 çerçevesi baz alınmaktadır
PCAOB (ABD)	BS denetimi özelinde bir düzenleme bulunmamaktadır.	Standartlar içerisinde BS kontrollerine değinilmiştir.
IFAC (Global)	BS denetimi özelinde bir düzenleme bulunmamaktadır.	Standartlar içerisinde BS kontrollerine değinilmiştir.

3. BT Denetim Raporu ve Görüş

Ülke düzenlemeleri ve global yetkili kurumlar tarafından yayımlanan standartlar, çerçeveler incelendiğinde bilgi teknolojileri ve denetim çalışmalarının iç kontrollerin bir bütün olarak değerlendirildiği süreç içerisinde yer aldığı görülmektedir. Dolayısıyla bilgi sistemleri denetimine ilişkin çalışma kağıtları ve raporlar aynı sürecin kapsamına girmektedir. Bu noktada dünyada IFAC/IAASB, PCAOB (SOX) ve Türkiye'de KGK tarafından yayımlanan standartlar ve düzenlemeler belirleyici olmaktadır.

SOX yasasının etkisi ile PCAOB tarafından hazırlanan standartlar doğrultusunda bilgi teknolojileri kontrolleri iç kontrollerin değerlendirilmesi kapsamında ele alınmaktadır. Finansal Tabloların Denetimi ile Bütünleşik bir Finansal Raporlama Süreçlerinin Üzerindeki İç Kontrol Ortamının Denetimi standardı olan AS2201 madde 85 içerisinde denetim raporunun içermesi gereken unsurlardan bazıları aşağıdaki şekilde tanımlanmaktadır;

- "Bağımsız" kelimesini içeren başlık,
- Yönetimin finansal raporlama üzerinde iç kontrol ortamının sağlanmasından ve etkinliğinin değerlendirilmesinden sorumlu olduğu ifadesi,
- Denetçinin sorumluluğunun finansal raporlama üzerindeki iç kontrol ortamının etkinliğine yönelik görüş verilmesi olduğu ifadesi,
- Finansal raporlama üzerindeki iç kontrol ortamı kavramının tanımı,
- Denetim çalışmalarının PCAOB standartlarına göre gerçekleştirildiğine dair ifade,
- İç kontrol ortamının anlaşılması, risklerin değerlendirilmesi ve söz konusu risk değerlendirme doğrultusunda kontrollerin tasarım ve operasyonel etkinliğinin değerlendirildiği ifadesi,
- Denetçi firmasının imzası,
- Denetim raporu tarihi.

Söz konusu unsurlar ile birlikte önemli kontrol zayıflıklarının ve eksikliklerin ifade edilmesi gerekliliği de çeşitli maddeler içerisinde atıf ile belirtilmektedir.

Denetim çalışmaları sonucunda iç kontrol ortamının etkinliğine yönelik denetçi tarafından görüş verilmektedir. Bu görüş bilgi teknolojileri veya otomatik kontroller özelinde verilmiş bir görüş değildir. Standart kapsamında iç kontrol ortamının etkinliğine yönelik olumlu veya olumsuz görüş verildiği belirtilmektedir. Bir veya daha fazla önemli kontrol zayıflığının bulunması direkt olarak olumsuz görüş ortaya çıkmasına neden olmakla birlikte, görüşün denetçi tarafından denetim çalışmalarının sonuçlarının bir bütün olarak değerlendirilmesi sonucunda verildiği ifade edilmektedir.

78'den 84'e kadar yer alan maddeler içerisinde tebliğlere yönelik (Belirli Hususların İletişimi) tanımlamalar yer almaktadır. Denetim Komitesi ve Yönetim Kurulu'na bildirim yapılması gerektiği belirtilmektedir. IFAC tarafından yayımlanan "Finansal Tabloların Denetiminin Planlanması", "Kuruluş ve Ortamının Anlaşılması Yoluyla Önemli Hata Riskinin Belirlenmesi ve Değerlendirilmesi", "Denetçi'nin Değerlendirilen Risklere Yanıtı", "Bir Hizmet Kuruluşu Kullanan Kuruluşlar için Denetim Gereksinimleri", "Bağımsız Denetçinin Genel Hedefleri ve Uluslararası Denetim Standartlarıyla Uyumlu bir Denetim Gerçekleştirilmesi" standartları BT denetimi kapsamında düzenleyici unsurlar olarak karşımıza çıkmakla birlikte, raporlama ve görüş konularına ilişkin ayrı bir standart olan "Finansal Tablolar Üzerinde Görüş Verilmesi ve Raporlama" standardı içerisinde denetçi görüşüne ilişkin ibareler ve denetim raporunun içermesi beklenen unsurları tanımlanmıştır. Standarda göre denetim raporunda bulunması gereken başlıklardan bazılarını aşağıdaki şekilde belirtilebiliriz;

- Raporun bağımsız denetçi tarafından hazırlandığına ilişkin açık ifade
- Yönetim sorumluluğu
- Denetçi sorumluluğu
- Denetim çalışmalarının ISA standartları doğrultusunda gerçekleştirildiğine dair ibare
- Denetim kanıtlarının çalışma kapsamında ve denetim görüşü verilmesi noktasında yeterli olduğuna dair ibare
- Denetçi görüşü
- Görüşün dayanağı
- Rapor tarihi ve denetim periyodu
- Denetçi imzası ve adresi

	Finansal Denetim Sonucu Denetim Raporu Hazırlanıyor mu?	Gerçekleştirilen BT ve Süreç Denetimi Çalışmaları için Ayrı bir BT/Süreç Denetim Raporu Hazırlanması Gerekiyor mu?
BDDK (Türkiye)	Evet	Evet
PCAOB (ABD)	Evet	Hayır
IFAC (Global)	Evet	Hayır

ISA standartlarına göre denetim çalışmaları kapsamında olumlu görüş, sınırlı olumlu görüş (şartlı görüş), olumsuz görüş verilebilmekte veya görüşten kaçınılabilmektedir. Raporlama ve görüş noktasında söz konusu tanımlamalar bilgi teknolojileri denetimi kapsamında da geçerli olmakla birlikte, bilgi teknolojileri denetimi özelinde raporlama süreci ISA standartları içerisinde tanımlanmamaktadır.

Türkiye'de ise denetim standartları kapsamında üst kurum olarak Kamu Gözetim Kurumu bulunmakta¬dır. Ek olarak bankacılık sektörü düzenlemelerini gerçek¬leştiren BDDK, sermaye piyasası kurumlarına ve araçlarına ilişkin usul ve esasları düzenlemek ve bunları denetlemekle yükümlü SPK bulunmaktadır. Söz konusu iki Kurum KGK'nın düzenlemelerine tabi olmaktadır. KGK tarafından söz konusu kurumlar için de geçerli olan Türkiye Denetim Standartları hazırlanmış ve yayımlanmıştır. Söz konusu standartlar hazırlanırken IFAC tarafından yayımlanan uluslararası standartlar referans alınmıştır. KGK tarafından 26 Aralık 2012 tarihli Bağımsız Denetim Yönetmeliği'nde Türkiye Denetim Standartları, 660 sayılı KHK uyarınca yürürlüğe konan, bilgi sistemleri denetimi dâhil olmak üzere, bağımsız denetim alanında uluslararası standartlarla uyumlu eğitim, etik, kalite kontrol ve denetim standartları ile bu alana ilişkin diğer düzenlemeler olarak tanımlandığı ifade edilmektedir. Bu ifade ile bilgi sistemleri denetimi de söz konusu standartlar dâhilinde düzenlendiği görülmektedir. Daha detayda belirtilecek olursa; IFAC çatısı altında bulunan IAASB tarafından hazırlanan ISA standartlarının baz alındığı belirtilmektedir. Dolayısıyla Türkiye'de bilgi sistemleri denetimi çalışmaları özelinde KGK tarafından hazırlanmış ayrıca bir düzenleme mevcut olmamakla birlikte, yürürlüğe aldığı düzenlemeler ile IFAC çatısı altında yer alan yapının benimsendiği görülmektedir.

KGK tarafından bağımsız denetimin sonuçları ve raporlama kapsamında "BDS 700 Finansal Tablolara İlişkin Görüş Oluşturma ve Raporlama", "BDS705 Bağımsız Denetçi Raporunda Olumlu Görüş Dışında Bir Görüş Verilmesi", "BDS706 Bağımsız Denetçi Raporunda Yer Alan Dikkat Çekilen Hususlar ve Diğer Hususlar Paragrafları", "BDS710 Önceki Dönemlere Ait Karşılık Gelen Bilgiler ve Karşılaştırmalı Finansal Tablolar", "BDS720 Bağımsız Denetçinin Denetlenmiş Finansal Tabloları İçeren Dokümanlardaki Diğer Bilgilere İlişkin Sorumlulukları" standartları yayımlanmıştır. IFAC tarafından yayımlanan ISA 700 ile paralel olarak yayımlanan BDS 700 standardı içerisinde denetçi görüşüne ilişkin ibareler ve denetim raporunun içermesi beklenen unsurları tanımlanmıştır. Standarda göre denetim raporunda bulunması gereken başlıklardan bazıları aşağıdaki şekildedir;

- "Bağımsız Denetçi Raporu" başlığı,
- Denetçi görüşü,
- Görüşün dayanağı,
- Kilit denetim konuları,
- Yönetim sorumluluğu,
- Denetçi sorumluluğu,
- Rapor tarihi ve denetim periyodu,
- Denetçi imzası, adresi.

KGK'nın düzenlemeleri kapsamında denetim çalışmaları sonucunda IFAC ile paralel olarak olumlu görüş, sınırlı olumlu görüş (şartlı görüş), olumsuz görüş verilebilmekte veya görüşten kaçınılabilmektedir.

BDDK tarafından bilgi sistemleri denetimine yönelik düzenlemeler gerçekleştirilmiştir. Bu doğrultuda BDDK tarafından yayımlanan "Bankaların Bağımsız Denetimi Hakkında Yönetmelik" ikinci bölüm madde 4 üçüncü fıkrası içerisinde "Bağımsız denetim raporu, TDS'de öngörülen hususlara ilave olarak bankanın iç kontrol sisteminin; finansal tabloların "Bankaların Muhasebe Uygulamalarına ve Belgelerin Saklanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik" ve TMS hükümleri ile Kurul tarafından bankaların hesap ve kayıt düzenine ilişkin yayımlanan diğer düzenlemelere, Kurum genelge ve açıklamalarına uygun olarak, tüm önemli yönleriyle gerçeğe uygun bir biçimde hazırlanmasını ve sunulmasını sağlayacak nitelikte olduğu, uygun muhasebe politikalarının seçildiği ve uygulandığına ilişkin ibareleri de içerecek şekilde düzenlenir." ibaresi bulunmaktadır. Denetim çalışmaları kapsamında ortaya çıkarılan rapor formatı ve içeriği değerlendirildiğinde global olarak belirli bir metodolojinin uygulandığı görülmektedir. Bununla birlikte bilgi teknolojileri denetimine özgü raporlama metodolojileri çeşitli standartlar (ISO 27001, ISAE 3402 vb.) kapsamında bulunmaktadır. Ancak global ölçekte uygulamalar ağırlıklı olarak değerlendirildiğinde BT denetiminin bütünleşik bir şekilde değerlendirildiği söylenebilir.

4. BT Denetim Çalışmaları Yetkilendirme

Global ölçekte bilgi teknolojilerine yönelik denetim çalışmalarının yetkilendirilmesi kapsamında
özerk bir düzenleme bulunmamakta, bilgi teknolojileri denetimi finansal denetim içerisinde değerlendirilmekte, dolayısıyla yetkilendirme süreci de finansal denetim yetkilendirme süreci kapsamında yönetilmektedir.

Bu doğrultuda değerlendirildiği takdirde global kapsamda IFAC ve PCAOB (SOX) düzenlemeleri ve Türkiye'deki mevcut düzenlemeler kaşımıza çıkmaktadır.

IFAC tarafından düzenlenen standartlar kapsamında iç denetim birimi tarafından tanımlandığı kapsamda denetim çalışmaları gerçekleştirilmektedir. Bununla birlikte denetim çalışmaları bağımsız denetim ekipleri tarafından gerçekleştirilebilmektedir. Dolayısıyla bilgi teknolojileri denetimi çalışmaları finansal denetimin bir parçası olarak bağımsız denetçiler tarafından ve iç denetim birimleri tarafından gerçekleştirilmektedir. Bağımsız denetçiler kapsamında ek olarak IFAC tarafından
"Overall Objectives of the Independent Auditor and the Conduct of an Audit In Accordance With International Standards on Auditing" standardı yayımlanmıştır. Standart içerisinde bağımsız denetçinin sorumlulukları, denetim planlaması, yürütülmesi ve raporlanması ile ilgili uyumlu olmakla yükümlü olduğu unsurlar belirtilmektedir.

SOX kapsamında ise PCAOB tarafından "An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements" standardı bulunmaktadır. Finansal raporlama üzerindeki iç kontrolün etkinliğinin değerlendirilmesi kapsamında bilgi teknolojileri ele alınmaktadır. İç kontrolün etkinliğinin değerlendirilmesi çalışmalarında iç denetim birimi ve bağımsız denetçi tanımları
yer almaktadır. Dolayısıyla IFAC standartlarında da karşılaşıldığı üzere bilgi teknolojileri denetimi çalışmaları finansal denetimin bir parçası olarak bağımsız denetçiler tarafından ve iç denetim birimleri tarafından gerçekleştirilmektedir. Bu doğrultuda "Responsibilities and Functions of the Independent Auditor", "Training and Proficiency of the Independent Auditor", "Part of the Audit Performed by Other Independent Auditors" standartları bulunmaktadır. Bağımsız denetçinin sorumlulukları, yetkinlikleri, bağımsız denetim çalışmalarına referans verilmesi, bağımsız denetim çalışmalarının raporlanması vb. unsurlar tanımlanmaktadır. Bağımsız denetçilere ilişkin yetkilendirme resmi olarak PCAOB tarafından gerçekleştirilmekte olup, kurumun internet sitesinde yetkili denetçiler yayımlanmaktadır.

Türkiye'de ise denetim standartları kapsamında üst kurum olarak Kamu Gözetim Kurumu bulunmaktadır. KGK tarafından Türkiye Denetim Standartları hazırlanmış olup, söz konusu standartlar hazırlanırken IFAC tarafından yayımlanan uluslararası standartlar referans alınmıştır. Dolayısıyla Türkiye'de bilgi sistemleri denetimi çalışmaları özelinde KGK tarafından hazırlanmış ayrıca bir düzenleme olmamakla birlikte, yürürlüğe aldığı düzenlemeler ile IFAC çatısı altında yer alan yapının benimsendiği görülmektedir. Ancak BDDK tarafından bilgi sistemleri denetimine yönelik düzenlemeler gerçekleştirilmiş olup, söz konusu çalışmaların yetkilendirilmiş bağımsız denetim kurumları tarafından ve teftiş birimleri tarafından yürütüldüğü görülmektedir. Bağımsız denetimin yetkilendirmesine yönelik BDDK tarafından yayımlanan "Bankaların Bağımsız Denetimi Hakkında Yönetmelik" üçüncü bölüm içerisinde bağımsız denetim kuruluşlarının listeye alınmasına, ortaklarına, kilit yöneticilerine ve bağımsız denetçilere ilişkin esaslar tanımlanmaktadır. Bölüm içerisinde kuruluş, ortak, yönetici ve denetçilere ilişkin aranan şartlar detaylı bir şekilde belirtilmektedir. Gerekli şartlar ve belgeler sağlanması durumunda kurumlar listeye alınarak denetleme yetkisine sahip olmaktadır. Söz konusu yetki resmi olarak KGK tarafından verilmektedir.

Ülkeler bazında bilgi teknolojileri denetim çalışmalarına yönelik yetkilendirme ile ilgili detay bilgiler ise aşağıdaki şekildedir:

Almanya: Almanya'da BT denetim çalışmaları iç denetim fonksiyonu ve bağımsız denetçiler tarafından gerçekleştirilmektedir. Düzenlemeler kapsamında finansalların denetlenmesi ve bu çalışma dâhilinde BT risklerinin de değerlendirilmesi gerektiği belirtilmektedir. Ancak BT denetimi ile ilgili özellikle ayrı bir yetkilendirme sistemi tanımlanmıştır. Almanya'da Alman Denetçiler Enstitüsü bulunmaktadır. Söz konusu enstitü tarafından BT kapsamında standartlar yayımlanmakla birlikte BT denetçilerine özgü bir sertifika programı bulunmamaktadır.

Amerika Birleşik Devletleri: Amerika'da BT denetim çalışmaları kurumların iç denetim fonksiyonları ve bağımsız denetçiler tarafından finansal denetim kapsamında gerçekleştirilmektedir. Ancak "Federal Bilgi Sistemleri Kontrolleri Denetim Rehberi" ve "Federal Bilgi Güvenliği Yönetimi Yasası" ile bilgi sistemleri kapsamında dış denetçi tarafından yıllık olarak söz konusu rehber ve yasa doğrultusunda BT değerlendirmesi gerçekleştirilebileceği belirtilmektedir. Amerika'da İç Denetçiler Enstitüsü (IIA) ve ISACA faaliyetleri bulunmakla birlikte ayrı bir BT denetçiler birliği veya ayrı bir yetkilendirme bulunmamaktadır.

Birleşik Krallık: İngiltere'de FSA, finansal piyasalarda hizmet veren şirketler ve borsa için standartları belirlemek amacıyla kurulmuş bağımsız bir kuruluştur. FSA tarafından yayınlanan düzenlemeler kapsamında denetleme sorumluluğu bağımsız kamu otoritesi FRC'ye verilmiştir. Bilgi sistemleri denetimi bağımsız finans denetim süreci kapsamında gerçekleştirilmektedir. Firmaların bağımsız denetimi kapsamında bilgi sistemlerini denetleyen kişilerde yasal bir gereksinim aranmamaktadır.

Güney Kore: Güney Kore'de denetim çalışmaları kapsamında "Board of Audit and Inspection Act" ve "Act on Public Sector Audits" başlıklı yasalar bulunmaktadır. Söz konusu yasalar denetim çalışmalarının kurumlar ve dış denetçiler tarafından yürütülmesine ilişkin tanımlamalar barındırmakla birlikte BT denetimi özelinde yetkilendirme mekanizmalarını tanımlamamaktadır. KICPA tarafından yayımlanan denetim standartları içerisinde bilgi teknolojileri riskleri ve denetimine yönelik tanımlamalar bulunmaktadır. Fakat Güney Kore'de BT denetimi özelinde bir enstitü ve ülke özelinde bir sertifika programı bulunmamaktadır

Hollanda: Hollanda'da, bilgi sistemleri denetçileri; ülkemizde serbest muhasebeci mali müşavirlik akreditasyonuna benzer şekilde; ulusal düzeyde bir bilgi sistemleri denetimi meslek birliği ve yüksek öğrenim destekli yerel bir sertifikasyon programına sahiptir. BT denetçilerinin profesyonel derneği olan NOREA, IT denetimi alanında yüksek öğrenim veya yüksek lisans derslerini başarıyla tamamlayan ve meslekte en az üç yıllık tecrübesi olan adaylara açıktır. Hollanda'da ortalama olarak 1000 kişi RE sertifikasına sahiptir.

Japonya: Japonya'da "Financial Instruments and Exchange Law" doğrultusunda iç denetim ve bağımsız denetim kuruluşları tarafından BT denetim çalışmaları gerçekleştirilmektedir. Düzenlemeler kapsamında BT risklerinin değerlendirilmesi ile ilgili tanımlamalar bulunmaktadır. Ancak BT denetimi ile ilgili özellikle ayrı bir yetkilendirme sistemi tanımlanmıştır. Japonya'da denetim sektörü kapsamında IFAC üyesi olan JICPA kurumu bulunmaktadır. Ancak BT denetçilerine özgü bir topluluk ve ülke özelinde bir sertifika programı bulunmamaktadır.

Kanada: Kanada'da bağımsız denetim kapsamında standartların yayınlanması Kanada Denetim ve Güvence Standartları Kurulu (CAASB) tarafından gerçekleştirilmektedir. Yayınlanan ilgili standartlar kapsamında işletmelerin bağımsız denetim faaliyetlerini düzenleyici ve denetleyici kurum ise Kanada Kamusal Hesap Verme Kurulu'dur (CPAB). İşletmelerin bilgi sistemleri denetim faaliyetlerine ilişkin incelemeler gerçekleştirilirken ISA standarlatı, COBIT ve CoCo baz alınarak hazırlanmış ITCG klavuzundan faydalanılmaktadır. Diğer yandan, Kanada'da BT denetimi özelinde bir enstitü ve ülke özelinde bir sertifika programı bulunmamaktadır.

	Bağımsız Denetim Kuruluşları Mali Denetim için Yetkilendiriliyor mu?	Bağımsız Denetim Kuruluşları BT Denetimi için Yetkilendiriliyor mu?
BDDK (Türkiye)	Evet	Evet
PCAOB (ABD)	Evet	Hayır
IFAC (Global)	Hayır (Kalite Kontrol Standartları ile Uyum Temel Alınıyor, Ülkeler Nezdinde Yetkilendirme Söz Konusu)	Hayır
Birleşik Krallık, Güney Kore, Hollanda, Japonya, Kanada	Evet	Hayır

Sonuç değerlendirmesi

Araştırma kapsamında bilgi teknolojileri denetiminin Dünya'da doğuşu ve gelişimi, Türkiye özelinde ortaya çıkışı ve zaman içerisindeki ilerleyişi ifade edilmiş olup, araştırmaya konu olan ülkeler bazında detaylı bir şekilde düzenlemeler, standartlar ve çerçeveler incelenmiştir. Bunlarla birlikte global düzeyde yetkin kurumlar tarafından yayımlanan standartlar yaşanan süreçler kapsamında incelemeye tabi tutulmuştur. Bütün araştırmalar neticesinde ortaya çıkan durumlar göz önünde bulundurularak aşağıda yer alan sonuçlar tespit edilmiş, sonuçlara ek olarak uygulamalar bazında önerilere yer verilmiştir.

Genel Değerlendirme

Dünya'da BT denetimine yönelik yasalar, yönetmelikler, rehber niteliğinde standartlar ve geniş kapsamlı çerçeveler incelendiğinde Bilgi Sistemleri Denetimi kavramı için çeşitli tanımlamalar ve uygulamalar görülmekle birlikte, bilgi sistemleri denetiminin ağırlıklı olarak özerk bir süreçten ziyade, bütünleşik denetim süreci dâhilinde değerlendirildiği görülmektedir.

Söz konusu durumun yanı sıra birçok çerçeve ve standart kapsamında bilgi teknolojileri denetimi ve risk değerlendirmesi bir kavram olarak tanımlanmıştır. Bilgi teknolojileri denetimi bahsi geçen standartlar ve çerçeveler ile içerik anlamında detaylandırılmıştır.

BT Denetiminin İçeriği

İçerikler incelendiğinde Dünya'da BT Denetimine içerik oluşturan ve BT denetim çalışmalarında dikkate alınan süreçleri aşağıdaki başlıklar altında gruplayabiliriz;

- Bilgi Sistemleri Risk Yönetimi Süreci
- Program, Değişiklik, Problem ve Olay Yönetimi Bütünleşik Süreci
- İş Sürekliliği Yönetimi Süreci
- BT Güvenlik (Fiziksel, Çevresel ve Yazılım) Yönetimi Süreci
- BT Operasyon (Erişim, Yedekleme vb.) Yönetimi Süreci

Bu doğrultuda, BT alanında önemli riskleri barındıran söz konusu süreçlerin, gelişmiş ülkeler ve rehber niteliğindeki standart ve çerçevelerde vurgulandığı üzere BT denetimine yönelik yasal düzenlemelerde görülmesi beklenebilir.

BT Denetimi Kapsamında Yer Alan Standartlar ve Mevzuatlar

Söz konusu içeriğe yönelik standartlar ve mevzuat küresel anlamda incelenmiş olup; küresel seviyede muhasebe, denetim ve güvence standartlarını belirleyen IFAC, ABD'de Sarbanes-Oxley Kanunu'yla ilişkili denetim standartlarını düzenleyen PCAOB, Türkiye'de ise muhasebe denetim standartları alanında KGK'nın düzenlemeleri öne çıkmıştır.

Ek olarak, bilgi teknolojileri denetimi anlamında müstakil ve detaylı bir çerçeve sunan BDDK'nın bankacılık sektörü için uyguladığı mevzuat detaylı olarak incelenmiştir.

IFAC, PCAOB, KGK ve BDDK tarafından yayımlanan standartlar ve düzenlemeler doğrultusunda denetim süreci detaylı bir şekilde tanımlanmış olup, bilgi teknolojileri bu sürecin kapsamına alınmıştır.

Ancak bilgi teknolojileri denetimi özelinde BDDK tarafından hazırlanan mevzuat haricinde, detaylı olarak hazırlanmış bir düzenleme bulunmamaktadır. Dolayısı ile bilgi teknolojileri denetiminde kapsam, raporlama, görüş, yetkilendirme konuları doğrultusunda detaylı ve yönlendirici tanımlamalara genel itibarıyla yer verilmemektedir. Bu noktada, bilgi teknolojileri denetimi için IFAC, PCAOB ve KGK tarafından yayımlanan standartların ve düzenlemelerin çatı olarak görülebileceği düşünülmektedir.

Diğer yandan, BDDK'nın Türkiye'de yayınladığı ve uygulamakta olduğu bilgi sistemleri ve bankacılık süreçleri denetiminin, farklı düzenleyiciler nezdinde tanındığı, bu düzenlemelere atıfta bulunulduğu ve uygulandığı görülmektedir.

Türkiye'deki farklı sektörler, kuruluşlar ve mevzuat uyum kültürüne bakıldığında, BT denetimi anlamında uluslararası standartlara nazaran daha detaylı ve yönlendirici bir düzenlemenin bulunmasının, mevzuatın uygulanmasındaki olası aksaklıkları ve görüş farklılıklarını azalttığı düşünülmektedir. Benzer bir bakış açısıyla, banka dışı sektörler ve kuruluşlar için de, KGK'nın mevcut düzenlemelerine ek olarak BT denetimi kurallarının ve standartlarının belirleneceği bir düzenlemenin, yönlendirici ve faydalı olacağı düşünülmektedir.

PCAOB'nin dolaylı olarak getirdiği BT denetimi ihtiyaçlarının halka açık şirketler için, IFAC'ın getirdiği gereksinimlerin üye ülkelerde yer alan yerel kurumlar tarafından uygulandığı ölçüde belirli sektörler ve bu sektörlerdeki kuruluşlar için, KGK düzenlemelerinin ise mevcutta Türk Ticaret Kanunu nezdinde bağımsız denetime tabi kuruluşlar için getirildiği söylenebilir. Bu bakış açısıyla, dünya genelinde hangi sektörlerdeki ve hangi boyutlardaki şirketlerin denetime tabi tutulduğuna dair bir fikir birliği bulunmadığı sonucuna varılabilir.

BT Denetimi Kapsamı

Genel itibarıyla kritik BT ortamlarına sahip olması beklenen halka açık şirketler, bankalar, finansal hizmetler, telekomünikasyon ve enerji, vb. sektörlerinde yer alan kuruluşlar veya ciro, aktif büyüklük, vb belirli bir finansal boyut açısından belirli bir eşiğin üzerinde yer alan kuruluşların BT denetimi uygulanması için en elzem kuruluşlar olacağı düşünülmektedir.

Bu anlamda, tüm sektör ve kuruluşlara yaygın olası bir BT denetimi mevzuatının; halihazırda bağımsız denetimin zorunlu tutulduğu kuruluşlara benzer bir şekilde ciro, personel adedi vb. kriterlere dayanarak firmalar için aşamalı bir şekilde devreye alınabileceği düşünülmektedir.

BT Denetimi Kapsamında Yer Alan Standartlar ve Mevzuatlar

Söz konusu içeriğe yönelik standartlar ve mevzuat küresel anlamda incelenmiş olup; küresel seviyede muhasebe, denetim ve güvence standartlarını belirleyen IFAC, ABD'de Sarbanes-Oxley Kanunu'yla ilişkili denetim standartlarını düzenleyen PCAOB, Türkiye'de ise muhasebe denetim standartları alanında KGK'nın düzenlemeleri öne çıkmıştır.

Ek olarak, bilgi teknolojileri denetimi anlamında müstakil ve detaylı bir çerçeve sunan BDDK'nın bankacılık sektörü için uyguladığı mevzuat detaylı olarak incelenmiştir.

IFAC, PCAOB, KGK ve BDDK tarafından yayımlanan standartlar ve düzenlemeler doğrultusunda denetim süreci detaylı bir şekilde tanımlanmış olup, bilgi teknolojileri bu sürecin kapsamına alınmıştır.

Ancak bilgi teknolojileri denetimi özelinde BDDK tarafından hazırlanan mevzuat haricinde, detaylı olarak hazırlanmış bir düzenleme bulunmamaktadır. Dolayısı ile bilgi teknolojileri denetiminde kapsam, raporlama, görüş, yetkilendirme konuları doğrultusunda detaylı ve yönlendirici tanımlamalara genel itibarıyla yer verilmemektedir. Bu noktada, bilgi teknolojileri denetimi için IFAC, PCAOB ve KGK tarafından yayımlanan standartların ve düzenlemelerin çatı olarak görülebileceği düşünülmektedir.

Diğer yandan, BDDK'nın Türkiye'de yayınladığı ve uygulamakta olduğu bilgi sistemleri ve bankacılık süreçleri denetiminin, farklı düzenleyiciler nezdinde tanındığı, bu düzenlemelere atıfta bulunulduğu ve uygulandığı görülmektedir.

Türkiye'deki farklı sektörler, kuruluşlar ve mevzuat uyum kültürüne bakıldığında, BT denetimi anlamında uluslararası standartlara nazaran daha detaylı ve yönlendirici bir düzenlemenin bulunmasının, mevzuatın uygulanmasındaki olası aksaklıkları ve görüş farklılıklarını azalttığı düşünülmektedir. Benzer bir bakış açısıyla, banka dışı sektörler ve kuruluşlar için de, KGK'nın mevcut düzenlemelerine ek olarak BT denetimi kurallarının ve standartlarının belirleneceği bir düzenlemenin, yönlendirici ve faydalı olacağı düşünülmektedir.

PCAOB'nin dolaylı olarak getirdiği BT denetimi ihtiyaçlarının halka açık şirketler için, IFAC'ın getirdiği gereksinimlerin üye ülkelerde yer alan yerel kurumlar tarafından uygulandığı ölçüde belirli sektörler ve bu sektörlerdeki kuruluşlar için, KGK düzenlemelerinin ise mevcutta Türk Ticaret Kanunu nezdinde bağımsız denetime tabi kuruluşlar için getirildiği söylenebilir. Bu bakış açısıyla, dünya genelinde hangi sektörlerdeki ve hangi boyutlardaki şirketlerin denetime tabi tutulduğuna dair bir fikir birliği bulunmadığı sonucuna varılabilir.

BT Denetimi Kapsamı

Genel itibarıyla kritik BT ortamlarına sahip olması beklenen halka açık şirketler, bankalar, finansal hizmetler, telekomünikasyon ve enerji, vb. sektörlerinde yer alan kuruluşlar veya ciro, aktif büyüklük, vb belirli bir finansal boyut açısından belirli bir eşiğin üzerinde yer alan kuruluşların BT denetimi uygulanması için en elzem kuruluşlar olacağı düşünülmektedir.

Bu anlamda, tüm sektör ve kuruluşlara yaygın olası bir BT denetimi mevzuatının; halihazırda bağımsız denetimin zorunlu tutulduğu kuruluşlara benzer bir şekilde ciro, personel adedi vb. kriterlere dayanarak firmalar için aşamalı bir şekilde devreye alınabileceği düşünülmektedir.

BT Denetim Raporu

BT denetimi raporunun BDDK'nın düzenlemeleri özelinde ayrı olarak hazırlandığı bilinmekle birlikte, dünya genelinde BT genel kontrollerinin değerlendirilmesi kapsamında ayrı bir rapordan ziyade denetim raporunun bir parçası olarak hazırlandığı uygulamaların yüzdesel ağırlığının fazla olduğu görülmektedir.

Dünya'daki standartlarda yer alan genel geçer uygulama, ayrı bir BT denetim raporu oluşturulmasını gerektirmese de; Türkiye'de, örneğin BDDK tarafından BT denetimi raporlarıyla ilgili öngörülen detaylı ve yönlendirici yaklaşımın,

denetim kalitesine ve denetimin kuruluşlara kattığı değere katkısı olduğu düşünülmektedir.

Bilgi teknolojileri denetim çalışmaları baz alınan konunun doğası gereği denetlenen kuruluş hakkında teknik anlamda ciddi seviyede zafiyetleri açığa çıkaracak kritiklikte bilgiler içerebilir. Denetim esnasında ve denetim dokümantasyonu kapsamında söz konusu bilgiler denetçi, denetlenen kuruluş ve düzenleyici kuruluş arasında paylaşılmaktadır. Bahsi geçen kritik bilgilerin yalnızca bulgulara yönelik özet bilgi olması durumunda dahi kamu ile paylaşılması denetlenen kurum ve düzenlemelerin işleyişi ve yaptırım seviyesi açısından riskli bir durum olarak görülmektedir. Denetlenen kuruluşlar, genel kitle tarafından daha az bilinen karmaşık BT konularında birbirleriyle kıyas içerisinde girebilir, farklı denetçilerin görüş farkından ve doğası itibarıyla öznel bir değerlendirme yapılmasından kaynaklanan farklardan ötürü kuruluşlar belirli görüşlere ve yaklaşımlara sahip denetçilere yönlenebilir ve yalnızca görüşler veya yönetici özetinde finansal raporlama süreçlerinin etkinliği açısından belirtilmiş olan ve finansal denetime kıyasla daha az ölçülebilir olan eksiklikler, konunun uzmanı olmayan kişiler tarafından yanlış veya eksik bir biçimde yorumlanabilir.

Bu nedenle, **bilgi teknolojileri denetim raporlarının özel ve gizli raporlar olarak denetçi, denetlenen ve düzenleyici kuruluş dışında bir tarafla paylaşılmaması önem arz etmektedir.**

Bilgi teknolojileri denetim çalışmaları denetime tabi olunan alanda yeterli bilgi, tecrübe ve niteliklere sahip denetçi kimliğine sahip kişi ve kuruluşlar tarafından gerçekleştirildiği görülmekte ve uygulamada önerilmektedir. Ancak finansal denetimden farklı olarak bilgi teknolojileri denetimi sektörünün yakın geçmişte oluşumu ve sektördeki tecrübe ve yetkinlik oranlarının henüz yeterli olgunluğa erişmemesi sebebiyle yetkilendirme noktasında uygulamaların henüz başlangıç seviyesinde olduğu düşünülmektedir.

BT Denetim Çalışmaları Yetkilendirme ve Sertifikasyon

Global standartlarda, farklı bir BT denetimi raporunun veya BT denetçisi yetkilendirme uygulamalarının kısıtlı olduğu, denetimler için yetkinlik ve sertifikasyon gereksinimlerinin çok katı olmadığı görülmektedir.

Buna kıyasla, Türkiye'deki mevzuat ortamında, denetimlerin sıhhati için, kuruluşların ve denetçilerinin gerek finansal denetim gerekse de BT denetimi için yetkilendirilmelerinin, denetim kalitesi ve denetimin sağladığı faydaya katkıda bulunduğu düşünülmektedir. Bununla birlikte, BT denetimi için dünya genelinde geçerli olan çerçevelerin ve sertifikasyonların (ISACA tarafından düzenlenen COBIT çerçevesi ve CISA sertifikasyonu)'nun Türkiye bankacılık sektörü özelinde olumlu ve başarılı uygulamalarla sonuçlandığı görülebilir. Özetle, BT denetimi için kuruluşların ve kişilerin belirli kriterler ve ön koşullar esas alınarak yetkilendirilmesi Türkiye özelinde gerekli ve faydalı görülmektedir. Ancak bu yetkilendirme için halihazırdaki başarılı uygulamaların (örn. BDDK) ve uluslararası kabul gören sertifikaların (örn. ISACA) denk kabul edilmesi, BT denetimi mesleğinin gelişimini ve kalitesini destekleyecektir.

Önümüzdeki dönemde, kuruluş süreçlerinin teknoloji boyutunun ve bununla aynı doğrultuda, bilgi teknolojileri denetimlerinden beklenen verimlilik ve katma değerin artması kaçınılmazdır.

Genel Değerlendirme

Bu yönde, iş süreçlerinde BT'yi yoğun olarak kullanan sektörler ve şirketler için BT denetimi zorunluluğunun getirilmesi, BT denetimlerinin ve raporlamalarının finansal denetim çalışmalarıyla bütünleşik bir şekilde gerçekleştirilmesi ve BT denetimi mesleğinin ve kuruluşlarının bu yönde yetkilendirilerek gözetiminin gerçekleştirilmesi büyük önem arz etmektedir.

Referanslar

1. Bank of England (2006), "Financial markets and their supervision (Act on Financial Supervision)".http://www.bankofengland.co.uk/financialstability/Pages/fmis/default.aspx.
2. Bank of England (2016), "Internal Audit Charter", http://www.bankofengland.co.uk/about/Documents/iacharter.pdf, (21.05.2017)
3. Bank of England (2015), "Internal Governance", http://www.bankofengland.co.uk/pra/Pages/publications/ss/2017/ss2115update.aspx.
4. Bank of England (2016), "Increasing the relevance of Internal Audit", http://www.bankofengland.co.uk/publications/Pages/speeches/2016/952.aspx.
5. Financial Services Authority (FSA), "SYSC13". https://www.handbook.fca.org.uk/handbook/SYSC/13/?view=chapter.
6. Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) (2012), "Annotated text of the Minimum Requirements for Risk Management (Mindestanforderungen an das Risikomanagement)", https://www.bundesbank.de/Redaktion/EN/Downloads/Tasks/ Banking_supervision/PDF/minimum_requirements_for_risk_management_mindestanforderungen_an_das_risikomanagement_marisk.pdf?__blob=publicationFile.
7. Bundesamt für Sicherheit in der Informationstechnik (BSI) (2008), "BSI-Standard 100-1, Information Security Management Systems (ISMS)", https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile.
8. Bundesamt für Sicherheit in der Informationstechnik (BSI) (2008), "BSI-Standard 100-2, IT-Grundschutz Methodology", https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-2_e_pdf.pdf?__blob=publicationFile.
9. Bundesamt für Sicherheit in der Informationstechnik (BSI) (2009), "BSI-Standard 100-4, Business Continuity Management", https://www.efk.admin.ch/images/stories/efk_dokumente/publikationen/querschnittspruefungen/QP%20%2810%29/9217BE_Gesamtbericht_QP_BCM_publ.pdf.
10. Bundesamt für Sicherheit in der Informationstechnik (BSI) (2008), "BSI-Standard 100-3, Risk Analysis Based On IT-Grundschutz", https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-3_e_pdf.pdf?__blob=publicationFile.
11. Canadian Institute of Chartered Accountants' (CICA's), "Criteria of Control Framework (CoCo)", http://www.gfoa.org/canadian-institute-chartered-accountants.
12. Chartered Institute of Internal Auditors (2017), "Attribute standards", https://www.iia.org.uk/.
13. Chartered Institute of Internal Auditors (2016), "Code Of Ethics", https://www.iia.org.uk/.
14. FCA (2013), "Internal Audit Division", https://www.fca.org.uk/publication/corporate/ internal-audit-info-pack.pdf.
15. Financial Services Agency (FSA), "Comprehensive Guidelines for Supervision of Financial Instruments", www.fsa.go.jp/en/refer/guide/instruments.pdf.
16. Financial Services Agency (FSA), "Inspection Manual for Financial Instruments Business Operations", www.fsa.go.jp/sesc/kensa/manual/kinyusyouhin_en.pdf.
17. FRC (2017), "Developments In Audit", https://www.frc.org.uk/Our-Work/Publications/FRC-Board/Developments-in-Audit-%E2%80%93-February-2017-update.pdf.
18. FRC (2016), "Ethical and Auditing Standards", https://www.frc.org.uk/Our-Work/Audit/Audit-and-assurance/Standards-and-guidance/Standards-and-guidance-for-auditors/2016-Ethical-Standard.aspx.
19. FRC (2010), "International Standard on Auditing", https://www.frc.org.uk/Our-Work/Audit/Audit-and-assurance/Standards-and-guidance/Standards-and-guidance-for-auditors/2016-Auditing-Standards.aspx.
20. FRC (2016), "Glossary of Terms (Auditing and Ethics)", https://www.frc.org.uk/Our-Work/Publications/Audit-and-Assurance-Team/Glossary-of-Terms-(auditing-and-ethics)-June-2016.pdf.
21. FRC (2016), "Scope and Authority of Audit and Assurance Pronouncements", https://www.frc.org.uk/Our-Work/Publications/Audit-and-Assurance-Team/Scope-and-Authority-of-Audit-and-Assurance-Pronoun.pdf.
22. IFAC (2016), "ISQC International Standard on Quality Control", http://www.ifac.org/system/files/downloads/a007-2010-iaasb-handbook-isqc-1.pdf.
23. German Government (2009), "Act to Strengthen the Security of Federal Information Technology", https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act _ BSIG.pdf?__blob=publicationFile.
24. German Government (2014), "German Banking Act (Gesetz über das Kreditwesen)", https://www.bafin.de/SharedDocs/Downloads/EN/Aufsichtsrecht/dl_kwg_en.pdf?__blob=publicationFile.
25. German Government (2009), "German Federal Data Protection Act", https://www.gesetze-im-internet.de/englisch_bdsg/.
26. Government Accountability Office (GAO), "Government Auditing Standards (GAGAS)", http://www.gao.gov/products/GAO-12-331G.
27. Government Accountability Office (GAO), "Federal Information System Controls Audit Manual (FISCAM)", http://www.gao.gov/assets/80/77142.pdf.
28. Government of Canada, "Minister of Justice Information Processing Activities (Banks and Authorized Foreign Banks) Regulations", http://laws-lois.justice.gc.ca/eng/regulations/SOR-2001-391/page-1.html.
29. International Federation of Accountants (IFAC), "ISA 300: Planning an Audit of Financial Statements", www.ifac.org.
30. International Federation of Accountants (IFAC), "ISA 315: Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and Its Environment", www.ifac.org.
31. International Federation of Accountants (IFAC), "ISA 330: The Auditor's Responses to Assessed Risks", www.ifac.org.
32. International Federation of Accountants (IFAC), "ISA 402: Audit Considerations Relating to An Entity Using A Service Organization", www.ifac.org.
33. Information Systems Audit and Control Association (ISACA), "Control Objectives for Information and Related Technology", www.isaca.org.
34. International Information Security Foundation (I2SF), "Generally Accepted System Security Principles (GASSP)", www.infosectoday.com/Articles/gassp.pdf.
35. Korean Government, "Board of Audit and Inspection Act", www.english.bai.go.kr.
36. Korean Government, "Act On Public Sector Audits", www.english.bai.go.kr.
37. Korean Institute of Certified Public Accountants, "Korean Standards On Auditing with Application Guidance For The Standards", http://kicpa.or.kr/english/default.htm.
38. National Institute of Standards and Technology (NIST), "Generally Accepted Principles and Practices for Securing Information Technology Systems (GAPP)", http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf.
39. National Institute of Standards and Technology (NIST), "Guide to Auditing for Controls and Security: A System Development Life Cycle Approach", http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nbsspecialpublication500-153.pdf.
40. National Institute of Standards and Technology (NIST), "Security Self-Assessment Guide for Information Technology Systems (SSAG)", http://csrc.nist.gov/publications/nistbul/09-01.pdf.
41. Organization for Economic Cooperation and Development (OECD), "Guidelines for the Security of Information Systems and Networks", www.oecd.org.
42. Proviti (2011). Yıllık Rapor. www.proviti.com, (2011). 2011 IT Audit Benchmarking Survey. USA: Proviti Insights.
43. Proviti (2012). Yıllık Rapor. www.proviti.com, (2012). 2012 IT Audit Benchmarking Survey. USA: Proviti Insights.
44. Proviti (2013). Yıllık Rapor. www.proviti.com, (2013). Third Annual IT Audit Benchmarking Survey. USA: Proviti Insights.
45. Proviti & ISACA (2014). Yıllık Rapor. www.isaca.org, (2014). A Global Look at IT Audit Best Practices. USA: Proviti Insights/ISACA Research.
46. Proviti & ISACA (2015). Yıllık Rapor. www.isaca.org, (2015). A Global Look at IT Audit Best Practices. USA: Proviti Insights/ISACA Research.
47. Proviti & ISACA (2016). Yıllık Rapor. www.isaca.org, (2016). A Global Look at IT Audit Best Practices. USA: Proviti Insights/ISACA Research.
48. Public Company Accounting Oversight Board (PCAOB), "AS 2300: Audit Procedures in Response to Risks-Nature, Timing and Extent", https://pcaobus.org/Standards/Auditing/pages/default.aspx.
49. Public Company Accounting Oversight Board (PCAOB), "AS 2200: Auditing Internal Control Over Financial Reporting, https://pcaobus.org/Standards/Auditing/pages/default.aspx.
50. Public Company Accounting Oversight Board (PCAOB), "AS 2100: Audit Planning and Risk Assessment", https://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_12.aspx.
51. SEC (2002),"Sarbanes-Oxley Act", https://www.sec.gov/about/laws/soa2002.pdf.
52. The Committee of Sponsoring Organizations of the Treadway Commission's (COSO), "Internal Control–Integrated Framework", https://www.coso.org/Pages/default.aspx.

Kısaltmalar

AICPA	American Institute of Certified Public Accountants
AFM	Autoriteit Finaciele Markten
APEC	Asia-Pacific Economic Cooperation
APRA	The Australian Prudential Regulatory Auhtority
ASAE	Assurance Reports on Controls at a Service Organisation
AUASB	Auditing and Assurance Standards Board
BAFIN	German Federal Supervisory Authority
BDDK	Bankacılık Düzenleme ve Denetleme Kurumu
BGYS	Bilgi Güvenliği Yönetim Sistemi
BIS	Bank of International Settlements
BT	Bilgi Teknolojileri
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CAASB	Canadian Public Accountability Board
CICA	Canadian Institute of Chartered Accountants
COBIT	Control Objectives for Information and related Technology
COCO	Criteria of Control Framework
COSO	The Committee of Sponsoring Organizations of the Treadway Commission - Internal Control– Integrated Framework
DNB	De Nederlandsche Bank
EPDK	Enerji Piyasası Düzenleme Kurumu
ESAC	Electronic Systems Assurance and Control
FDIC	The Federal Deposit Insurance Corporation
FFIEC	The Federal Financial Institutions Examination Council
FINMA	Swiss Financial Market Supervisory Authority
FINRA	The Financial Industry Regulatory Authority
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
FSA	Financial Services Authority
GAO	Government Accountability Office
GAPP	Generally Accepted Principles and Practices for Securing Information Technology Systems
GAGAS	Government Auditing Standards
FSA	Financial Services Authority
ICAEW	Institute of Chartered Accountants in England and Wales
IDW	The Institut der Wirtschaftsprüfer in Deutschland
IFAC	Internatinal Federation of Accountants
IAASB	International Auditing and Assurance Standards Board
IESBA	International Ethics Standards Board for Accountants
IIA	The Institute of Internal Auditors
ISA	International Standards on Auditing
ISAE	International Standard on Assurance Engagements
ISACA	Information Systems Audit and Control Association
ITCG	Information Technology Controls Guidelines
I2SF	Information Security Foundation
KICPA	Korean Institute of Certified Public Accountants
NIST	National Institute of Standards and Technology
NIVRA	Nederlands Instituut van Registeraccountants
NOVAA	Nederlandse Orde Van Accountants
NOREA	Nederlandse Orde van Register EDP-Auditors
OECD	Organization for Economic Cooperation and Development
PCAOB	Public Company Accounting Oversight Board
SEC	U.S. Securities and Exchange Commission
SOC	Service Organization Control
SOX	Sarbanes Oxley Act
SPK	Sermaye Piyasası Kurulu
SSAG	Security Self-Assessment Guide for Information Technology Systems
SYSC13	Senior Management Arrangements. Systems and Controls
TSP	Supervision of Technology Service Providers


KPMG
Yayınlarımızı takip ediyor musunuz?
kpmg.com.tr

İletişim:

Detaylı bilgi için:
KPMG Türkiye
Kurumsal İletişim ve Pazarlama Bölümü
tr-fmmarkets@kpmg.com

İstanbul
İş kuleleri Kule 3 Kat 2-9 34330
Levent / Beşiktaş / İstanbul
T : +90 212 316 6000

Ankara
The Paragon İş Merkezi Kızılırmak Mah. Ufuk
Üniversitesi Cad. 1445 Sok. No:2 Kat:13
Çukurambar 06550 Ankara / Türkiye
T : +90 312 491 7231

İzmir
Heris Tower, Akdeniz Mah. Şehit Fethi Bey Cad.
No:55 Kat:21 Alsancak 35210 İzmir / Türkiye
T : +90 232 464 2045

kpmg.com.tr
kpmgvergi.com