BİLGİ TEKNOLOJİLERİ DENETİMİ VE ULUSLARARASI STANDARTLAR

İzzet Gökhan ÖZBİLGİN
Sermaye Piyasası Kurulu
Sistem Mühendisi

Günümüz iletişim ve bilişim teknolojisinde ortaya çıkan gelişmeler, özellikle de internetin gelişip büyümesi tüm kamu kesimini ve özel sektörü önemli bir biçimde etkilemektedir. Bu gelişmelerle birlikte, ülkeler arasındaki sınırlar giderek ortadan kalkmakta ve oluşan ekonomik bütünleşmeler, verilen hizmetlerin niteliğini ve yapısını da önemli bir şekilde değiştirmektedir.

Ülkemizde de kamu kesimi ve özel sektör, teknolojideki bu gelişmelere bağlı hızlı bir dönüşüm süreci içinde bulunmakta, faaliyetlerinin büyük bir kısmını gerçekleştirirken bilgisayarlardan yararlanmaktadırlar. Bu gelişim, işlemlerin daha hızlı ve etkin bir şekilde yapılmasına imkân tanımaktadır. Ancak, teknolojide yaşanan bu hızlı değişimin yararları yanında neden olduğu bazı olumsuzluklar da söz konusudur. Bunların başında, önceden yazılı olarak gerçekleştirilen işlemlerin sanal ortama taşındıktan sonra izlenme, kontrol altına alınma ve denetlenmesinin güçleşmesi gelmektedir. Öte yandan, sistemlerin daha karmaşık bir yapıya dönüşmesi, işletmelerin bilgi teknolojileri ile ilgili risklerinin türleri ve bunların içerikleri üzerinde olumsuz etkiler doğurmakta, yeni risk faktörleri oluşturmaktadır.

Yaşanan tüm bu gelişmeler, sadece bu sistemlerden elde edilen verilerin değil, aynı zamanda bu verileri üreten sistemlerin de önemli olduğunu göstermiştir. Dolayısıyla, işlemlerini böyle sanal ortamda gerçekleştirmeye başlayan kuruluşların denetiminde elde edilen verilerin daha anlamlı olabilmesi için bu verileri oluşturan bilgisayar sistemlerinin ve bu sistemler üzerindeki işlem ve uygulamaların düzgün ve güvenilir bir şekilde çalışması gerekmektedir.

Denetim mesleği ve denetim uygulamaları, teknolojik gelişmelere paralel olarak birçok değişikliğe uğramış, günümüzde geldiği noktaya kadar da pek çok evreler geçirmiştir. Özellikle, Yirminci Yüzyılda yatırımcıların bilgilendirilmesi ve toplum-kamu çıkarlarının korunması açısından denetim mesleği ve uygulamaları ile ilgili olarak standartların oluşturulması ve yasal düzenlemelere gidilmesi söz konusu olmuştur. Bu noktada, oluşturulacak standartlar ile yapılacak yasal düzenlemelerde bilgi teknolojilerindeki yeniliklere yer verilmesi ve kuruluşların

denetimleri sırasında bilgi teknolojileri ortamlarının dikkate alınması da zorunluluk haline gelmiştir.

Oluşturulan bu standartlar, denetim çalışmasının nasıl olması ve karşılaşılan durumlarda nasıl davranılması gerektiği konularında denetçiye yol gösterici olup, denetim uygulamalarında birlik sağlamaktadır. Bunun yanında, bağımsız denetimin kamu çıkarını koruyup kollama işlevi göz önünde tutulursa, standartlar denetim çalışmalarında kaliteyi sağlayarak veya mevcut kaliteyi artırarak denetimin sonucuna olan güveni artıracaktır.

Muhasebecilik alanında en büyük mesleki birlik olan IFAC (International Federation of Accountants), denetime yönelik koyduğu standartlar ve bunların sürekli olarak geliştirilmesiyle ilgili olarak faaliyet gösteren en büyük kuruluştur. IFAC'ın bünyesinde bulunan IAASB (International Auditing and Assurance Standarts Board) de uluslararası denetim standartları ve uygulamaları ile ilgili çalışmaları yürütmektedir. Bu Kurul tarafından hazırlanan düzenlemelerden özellikle ISA (International Standards on Auditing) ve IAP (International Auditing Practice Statement), denetim uygulamaları konusunda birlik sağlanması bakımından son derece önemlidir.

ISA 10 konu başlığı altında 52 adet standarttan oluşmaktadır ve bu standartlar mali tabloların denetiminde kullanılmaktadır. Bu standartlar diğer bilgilerin ve ilgili hizmetlerin denetiminde de kullanılabilir ve gerekli görülürse bunlara da uyarlanabilir. Bu düzenlemede yer alan standartlar, açıklama şeklindeki diğer açıklayıcı rehber bilgilerle birlikte asli ilkeleri ve önemli prosedürleri içermektedir.

IFAC tarafından tasnif edilen bu standartlardan ISA 401 no'lu standart ("Auditing in a Computer Information Systems Environment") bilgi teknolojileri ortamında denetimin asli ilkeleri ve önemli prosedürlerini belirtmektedir. Aynı zamanda bu ilke ve prosedürler, uygulamaya yönelik rehber niteliğindeki IAP 1001, IAP 1002, IAP 1003, IAP 1008, IAP 1009 ve IAP 1013[1] no'lu standartlardaki diğer açıklayıcı bilgilerle beraber yorumlanmalıdır.

---

[1]IAP 1001 IT Environments - Stand-Alone Personal Computers
IAP 1002 IT Environments - On-Line Computer Systems
IAP 1003 IT Environments - Database Systems
IAP 1008 Risk Assessments and Internal Controls
IAP 1009 Computer-Assisted Audit Techniques
IAP 1013 Electronic Commerce

ISA 401 no'lu "Bilgi Teknolojileri Ortamında Denetim" adlı standart ile ilgili asli ilkeler ve önemli prosedürler şunlardır:

1. Bu uluslararası standardın amacı, bilgi teknolojileri ortamlarında yürütülecek bir denetimin standartlarını ortaya koymak ve izlenilmesi gerekli prosedürlerle ilgili rehber olmaktır.

2. Denetçi bilgi teknolojileri ortamının, denetimi nasıl etkileyeceğini dikkate almalıdır.

3. Denetimin genel amacı ve alanı, bilgi teknolojileri ortamına göre değişmez. Buna rağmen, bir bilgisayarın kullanımı; mali bilgilerin işlenmesini, depolanmasını ve paylaşımını değiştirebilir ve firma tarafından uygulanan muhasebe ve iç kontrol sistemlerini etkileyebilir.

4. Denetçi gerçekleştirilen bir işi planlamak, yönetmek, yürütmek ve gözden geçirebilmek için bilgi teknolojileri sistemleriyle ilgili yeterli bilgi birikimine sahip olmalıdır. Denetçi, denetim sırasında bilgi teknolojileri sistemleriyle ilgili özel bir beceriye ihtiyaç duyup duymadığını belirlemelidir. Eğer böyle bir beceriye ihtiyaç duyulursa denetçi, ya kendi denetim ekibinden bir personelin ya da bu becerilere sahip dışarıdan bir profesyonelin yardımına başvurabilir. Eğer böyle bir profesyonelin kullanımı planlandıysa, denetçi, ISA 620 "Using the Work of an Expert" standardına göre, bu işlemin denetlemenin amacı açısından yeterli olunduğuna dair uygun bir kanıt temin etmelidir.

5. ISA 400 Risk Assessments and Internal Control standardına göre; denetçi, yeterli bir denetim planlayabilmek ve etkili bir denetim yaklaşımı geliştirebilmek için, muhasebe ve iç kontrol sistemlerini iyi değerlendirmeli ve anlamalıdır.

6. Denetçi, denetlenecek kuruluşun bilgi teknolojileri ortamı tarafından etkilenecek denetim bölümlerini planlarken bilgi teknolojileri yapısının durumu ve verilerin anlamını iyi değerlendirmelidir.

7. Denetçi bilgi teknolojileri ortamının önemli olduğu durumlarda, bilgi teknolojileri ortamı ile bu ortamın iç kontrol risklerini nasıl etkilediğini anlamalıdır.

8. ISA 400 Risk Assessments and Internal Control standardına göre denetçi, maddi finansal beyanlar ile ilgili içsel risklerin ve kontrol risklerinin değerlendirmesini yapmalıdır.

9. ISA 400 Risk Assessments and Internal Control standardına göre denetçi, denetleme riskini kabul edilebilir derecede düşük bir seviyeye düşürmek

için denetleme usullerinin tasarımında bilgi teknolojileri ortamını göz önüne almalıdır.

10. Denetçinin özellikli denetleme amaçları, muhasebe verileri elle veya bilgisayar ile işlensin ya da işlenmesin değişmez. Ancak, kanıt toplamak için kullanılan denetim prosedürlerinin uygulanma yöntemleri, bilgisayar proses yöntemleri tarafından etkilenebilir. Denetçi, yeterli miktarda kanıt temin edebilmek için manuel denetleme usullerini, bilgisayar destekli denetleme tekniklerini ya da bunların birleşimini kullanabilir. Ancak, özel uygulamaları işleyen bazı muhasebe sistemlerinde, denetçi için bilgisayar olmaksızın belli teftiş verilerinin, talebini ya da teyidini temin etmek zor veya imkânsız olabilir.

Görüldüğü üzere IFAC tarafından bilgi teknolojileri denetimi ile ilgili standartlar belirlenmiştir. Bu standartların yanı sıra teknolojik alanlarda yapılmış diğer başka çalışmaların da dikkate alınması bilgi teknolojileri denetiminin daha etkin yapılmasını sağlayacaktır. Örneğin, ISO 17799 uluslararası kabul görmüş bir Bilgi Güvenliği Yönetim standardıdır. Bu standart, bilginin gizliliğinin ve bütünlüğünün nasıl korunacağına ve bilgiye sürekli erişimin nasıl sağlanacağı hakkında rehber bir çalışmadır.

Etkili bir bilgi teknolojileri denetiminden söz edebilmek için öncelikle uygulayıcıların, işletmelerin ve yasa koyucuların bilgi teknolojileri denetim kavramını anlamaları ve kabul etmeleri gerekmektedir. Bu konuya olan ihtiyacın tarafların görüş birliği ile kabul edilmesi, elde edilecek sonuçların etkinliği açısından son derece önemlidir. Bilgi teknolojileri denetimi bir lüks değil, ülkemizde acil olarak giderilmesi gereken önemli bir gereksinimdir. Devlet bu konuda öncü olmalı, yasal düzenlemelerle bilgi teknolojileri denetim uygulamalarına destek sağlayacak bir ortamı oluşturmalıdır.

Ülkemizde bağımsız denetime ilişkin standartların oluşumuna önemli katkıda bulunan düzenlemelerden biri de hiç kuşkusuz 2499 sayılı Sermaye Piyasası Kanunu'dur. Mali tabloların denetimine ilişkin olarak bu mevzuat ile getirilen ilke ve standartlar, uluslararası kabul görmüş denetim standartlarına en yakın olanıdır. Benzer şekilde Sermaye Piyasası Kurulu gene öncülük görevini üstlenmeli ve denetim uygulamaları ile ilgili mevzuatında bilgi teknolojileri hususlarına ve bilgi teknolojileri ortamında yapılacak denetim standartlarına değinmelidir. Özellikle, internet üzerinden hizmet veren aracı kurumlar ve halka açık şirketlerle ilgili olarak gerçekleştirdiği düzenlemelerinde mutlaka bilgi teknolojileri hususlarına da yer vermelidir.

Bilgi teknolojileri denetimi oldukça ayrıntılı ve önemli süreçleri içermektedir. Bu süreçlerin eksiksiz ve doğru bir şekilde yürütülebilmesi için, denetim teknolojik anlamda yeterli düzeyde bilgi birikimine sahip denetçiler tarafından yürütülmeli ya da denetim sırasında bilgi teknolojileri konusunda uzman kişilerin yardımı alınmalıdır. Bu nedenle, bilgi teknolojileri denetim faaliyetlerinden söz edebilmek için öncelikle sektörde bilgi teknolojileri denetimi ile ilgili eğitim ve seminerlerin düzenlenmesi, "workshop"ların oluşturulması ve bilgi teknolojileri denetçilerinin yetiştirilmesi gerekmektedir.

Gerek dünyada 2001 yılında yaşanan "Enron Skandalı" gerekse ülkemizde 2003 yılında Bankacılık Düzenleme ve Denetleme Kurulu tarafından T.İmar Bankası T.A.Ş'e ait bankacılık işlemleri yapma ve mevduat kabul etme izninin kaldırılması ve bu bankanın Tasarruf Mevduatı Sigorta Fonuna intikaline sebep olan "çifte kayıt olayı" bilgi teknolojileri denetim kavramının öneminin her kesim tarafından iyice anlaşılması gerektiğini ortaya koymuştur.

Sonuç olarak, finans sektöründe bilgi teknolojileri denetim uygulamasının yeterli düzeyde olmaması, sektörün güvenilirliği açısından oldukça olumsuz bir etkendir ve bu durum bir an önce giderilmelidir. Ayrıca, bu sektördeki her aktör kendine ait iç kontrol sistemi oluşturmalı ve güvenlik politikaları belirlemelidir. Gerek kamu kesimi, gerekse özel sektör kendi sistemlerinin aksayan yönlerini tespit ederek bunları iyileştirmek için gerekli çabayı göstermeli, acil önlem planları düzenlemelidir. Devlet, bu konuda çalışmaları başlatmalı ve bilgi teknolojileri standartlarının geliştirilip uygulanmasını sağlamalıdır.

Eğer bir sistem kontrol edilemiyor, denetlenemiyorsa o sistemin güvenilirliliğinden, verimliliğinden bahsedilemez. Denetimden uzak bir bilgi teknolojileri sisteminin, ne kadar iyi kurulmuş olursa olsun ve ne kadar iyi çalışırsa çalışsın, kurumlara ve hatta tüm finans sektörüne verebileceği zararların büyüklüğü tahmin bile edilemeyecektir.

KAYNAKLAR

INTERNATIONAL FEDERATION OF ACCOUNTANTS (IFAC)

"International Standards on Auditing" , www.ifac.org

INTERNATIONAL FEDERATION OF ACCOUNTANTS (IFAC)

"International Auditing Practice Statement" , www.ifac.org

ERDEM, Mehmet Ali

"Uluslararası Standartların Mali Denetime Katkısı ve Kamu Denetimine İlişkin Yeni Düzenlemeler Global Muhasebe Standartlarına Doğru", Gazi Üniversitesi Muhasebe – Finansman Doktora Programı Seminer Notları, Aralık 2003

SAKA, Tamer

"Bankacılık Sektöründe Bilgi Teknolojileri Denetimi", 2001

BANKACILIK DÜZENLEME VE DENETLEME KURUMU TASARRUF MEVDUATI SİGORTA FONU

"İmar Bankası Olayı Raporu", Ekim 2003

T.C. SAYIŞTAY BAŞKANLIĞI

"Hazine Bilişim Sistemleri Denetim Raporu", Ekim 2003

www.bis.org

www.iso-17799.com

www.semor.com.tr

www.sayistay.gov.tr