BİLİŞİM SİSTEMLERİ DENETİMİ VE SAYIŞTAY

Özcan Rıza YILDIZ*

Giriş

Son on yıl içerisinde bilgi ve iletişim teknolojilerinde yaşanan hızlı değişim dünyamızı yeni bir çağa taşırken, kamu ve özel sektördeki tüm kurumları da bu değişime ayak uydurmak zorunda bırakmıştır.

Verilere kolay ulaşım, kolay ve rahat iletişim, verimlilik ve etkinliği arttırma gibi konularda sunduğu yeni imkânlar nedeniyle başta finans, medya, eğitim olmak üzere hemen her alanda bilişim teknolojisinin kullanımı giderek yaygınlaşmaktadır. Bugün geldiğimiz noktada bir kurumun varlığını sürdürmesinin artık büyük ölçüde bilişim teknolojilerinden yararlanmasına bağlı olduğu bir gerçekliktir.

Bilişim teknolojilerinin kullanımı, görevleri kamu kaynaklarının yürürlükteki mevzuata uygun olarak tutumlu, verimli ve etkin şekilde kullanılıp kullanılmadıklarını denetlemek olan yüksek denetim kurumlarının gerek yürüttükleri denetimler üzerinde, gerekse bu denetimlerin yürütülmesi sırasında kullandığı yapı ve araçlar üzerinde doğrudan bir etkiye sahiptir.

Bu çalışmada, bilişim teknolojilerindeki gelişmelerin denetim mesleğine ve denetime olan etkileri, elektronik bilgi ortamlarındaki denetim yaklaşımları ve bu denetimlere ilişkin uluslararası düzenlemeler dikkate alınarak, Sayıştay'da bilişim sistemleri denetimi alanında yapılan çalışmalar hakkında bilgi verilecektir.

Bilişim Teknolojileri

Bilginin toplanmasında, işlenmesinde, depolanmasında, ağlar aracılığıyla bir yerden bir yere iletilmesinde ve kullanıcıların hizmetine sunulmasında yararlanılan ve iletişim ve bilgisayar teknolojilerini de kapsayan bütün teknolojiler "bilişim teknolojisi" olarak adlandırılabilir.

Kurumlar bilişim teknolojilerini, bilgi varlıklarının değerini arttırarak kurum amaçlarının yakalanmasına yönelik stratejilerinin bütünleyici parçası

* Sayıştay Uzman Denetçisi

olarak görmektedir. İşletim sistemleri, ağ sunucuları veya diğer uygulamaların amaçlandığı gibi işlememesi, hem kurum çalışanlarını, hem de hizmetten yararlananları etkilemektedir. Kurum birçok rutin veya kritik faaliyetleri yürütemez duruma gelebilmektedir.

Bilişim teknolojilerindeki gelişme, kamu hizmetlerine yönelik beklentilerin de düzeyini etkilemektedir. Artık teknolojiyi yenilemek yetmemekte, iş yapma anlayışında ve iş süreçlerinde çağın gereklerine uygun yapısal değişikliklerin benimsenmesi gerekmektedir. E-devlet uygulamasının gerçekleştirilmesi, saymanlıkların tek bir merkezden otomasyonunun (Say2000i) sağlanması, kurum hizmetlerinin bir kısmının web tabanlı uygulamalar üzerinden verilmesi gibi çalışmalar bu kapsamda değerlendirilmelidir.

Günümüzde, hem bireysel hem de kurumsal açıdan bilişim teknolojilerine bağımlılık giderek artmaktadır. Ancak, bilişim sistemlerine olan bireysel ve toplumsal bağımlılık arttıkça, bu sistemlerde meydana gelebilecek arıza ve saldırılara karşı duyarlılık da artmaktadır. Bilgisayar sistemlerine ve ağlarına yönelik saldırılar veya bu sistemlerde meydana gelebilecek aksaklıklar ciddi miktarda para, zaman, itibar ve değerli bilgi kaybına neden olabilmektedir.

On yıl kadar önce, bilişim teknolojilerinin ve bu teknolojiler aracılığıyla işlenen, tutulan bilginin güvenliğine yönelik tehditler, bunların merkezi olarak kilitli odalarda tutulmasıyla önlenebilen, sadece basit hırsızlık veya donanım bozuklukları gibi tehlikeler iken, bugün bilişim teknolojilerinin ve hizmetlerinin hızlı gelişmesi, yaygınlaşması ve yönetimlerinin uzaktan yapılabilmesi, çok değişik güvenlik tehditlerini gündeme getirmektedir.

Başka bir deyişle, bilişim teknolojilerine ilişkin alt yapı hizmetlerinin ucuzlaması ve internet kullanımının yaygınlaşması ile kurum açısından hassas olan bilişim sistemlerinin, bu sistem aracılığıyla verilen hizmetlerin ve bu sistemde tutulan her türlü ortamdaki (disket, CD, DVD, bilgisayar, ağ, internet vb.) bilginin güvenliğini sağlamak, bütünlüğünü korumak ve erişimi denetleyerek gizliliği ve sistem devamlılığını sağlamak, giderek daha karmaşık bir hal almaktadır.

Daha açık bir ifade ile bilişim teknolojilerin bir çok alanda kullanılmaya başlanmasıyla, bilginin bilişim sistemleri aracılığıyla işlenip saklanması büyük avantajlar sağlamakla birlikte, kurumları, tedbir alınmaması durumunda sistemlerinde zaafiyetlere yol açabilecek, yeni riskler ve tehditlerle karşı karşıya bırakmaktadır. Kullanılan bilişim sistemi, münferit hataların sistematik hatalara dönüşmesi, hataların birbirini beslemesi, mantıksız işlemler

meydana gelmesi, verilerin doğru girilmemesi, kanıtlayıcı belgelerin bulunamaması, yetkili kullanıcılar tarafından sistemin yanlış kullanılması, sisteme yetkisiz erişimlerin kontrol edilememesi, işlem yapan kişinin belirlenememesi gibi riskleri de beraberinde getirmektedir.[1]

Bu risklerin önlenmesi veya kabul edilebilir bir seviyeye düşürülebilmesi, kurum bilişim sistemlerinin hedeflendiği gibi çalışmasının temin edilebilmesi ve güvenli ve güvenilir bir bilişim ortamının oluşturulması için, kurum yönetiminin belirli kontrol mekanizmalarını kurması gerekmektedir. Örneğin, bilişim ortamında verilerin doğru olarak elde edilmesini sağlamak için bilişim ortamına özgü sistematik hataları önleyecek bir kontrol mekanizmasının kurulması gerekir.

Bilişim Sistemleri Denetimi

Bazı alanlarda tanım yapmak oldukça zor bir uğraştır. Tanımı yapılan şeyin ne olup olmadığını tanımdan belirlemek her zaman mümkün olamayabilmektedir. Bu durum bilişim sistemleri denetimi için de geçerlidir. Ancak, yine de bir tanım vermek gerekirse, bilişim sistemleri denetimi, "bir bilişim sisteminin, kurum amaçlarına etkin bir şekilde ulaşılmasını, kaynakların verimli kullanılmasını, varlıkların korunmasını ve veri bütünlüğünün sürdürülmesini sağlayacak şekilde tasarlanıp tasarlanmadığını tespit etmeye yönelik kanıt toplama ve değerlendirme süreci"[2] olarak tanımlanabilir.

Yapılan denetimin amacına göre de bir tanım yapmak mümkündür. Örneğin, bir mali denetim esnasında bilişim sistemleri ile karşılaşıldığı ve bilişim ortamında tutulan veriler denetimin önemli bir parçasını oluşturduğu durumda, bilişim sistemleri denetimi, denetlenen kurumlarda kullanılan bilişim sistemlerinin işlem ve uygulamalarının güvenlik ve güvenilirliğini sağlayan iç kontrolleri incelemek ve değerlendirmektir.

Bilişim sistemleri denetimi, bilişim teknolojisinin gelişimine ve kurumlarda kullanım düzeyine paralel olarak üç şekilde yapılabilmektedir:[3] Bilgisayar çevresinde denetim, bilgisayarlı denetim, bilgisayarın içinde denetim.

---

[1] Özkul, Davut, "Bilişim Sistemleri Denetimi", Yayımlanmamış Yüksek Lisans Tezi, G.Ü. Sosyal Bilimler Enstitüsü, Ankara, 2002, s. 42.

[2] Weber, R., Information Systems Control and Audit, 1999, Akt. ASOSAI, IT Audit Guidelines, ASOSAI Research Project, Eylül 2003.

[3] INTOSAI Geliştirme Girişimi (IDI), Intorduction of IT Audit e-learning Course Notes, 2007, s. 5. http://idi.cliksonline.com.

Bilgisayar çevresinde denetim; bilişim teknolojilerinin kurumlar tarafından kullanılmaya başlandığı ilk yıllarda, birçok işlem bilişim teknolojileri ile birlikte manuel olarak da yapılmaktadır. Burada denetçiler denetim izini, bilgisayara giren kaynak dokümanlardan elde edip bilgisayardan çıkan dokümanla karşılaştırarak, kayıtları takip ederek ihtiyaç duyulan kanıtları manuel olarak elde etmektedir. Bu yöntemde, denetçiler bilgisayara girilen veriler ve ürettiği çıktılarla ilgilendiği halde, bilgisayarın kendisi ile ilgilenmemektedir.

Bilgisayarlı denetim; bilişim sistemlerini yaygın olarak kullanan ve işlemlerini daha az manuel olarak yürüten kurumlarda, bu sistemdeki verileri araştırmak, karşılaştırmak, analiz etmek ve değişik test türlerini uygulamak veya veriler üzerinde matematiksel hesaplamalar yapmak için bilgisayar kullanılmaktadır. Denetimde etkinliği ve verimliliği önemli ölçüde arttırmak için kullanılan bu tekniklere sıklıkla bilgisayar destekli denetim teknikleri (BDDT) denmektedir.

Bilgisayarın içinde denetim; manuel olarak üretilen çıktıların minimuma indiği, kurumun bütün bilgileri ve iletişiminin bilişim teknolojileri aracılığıyla sağlandığı karmaşık ve büyük sistemlerin denetimine ilişkin olarak kullanılan bu yöntemde, bilgisayar, sistem içinde var olan işlem mantığını, var olan kontrol mekanizmalarını ve sistem tarafından üretilen kayıtları test etmek için kullanılmaktadır. Denetçi, sistem tasarımı ve sistemin geliştirilmesinde de belli görevler üstlenmektedir.

Bilişim teknolojisindeki gelişmeye ve denetçilerin çalışma ortamları ve bilgisayar ile ilişkilerine göre bu denetimin isimlendirilmesi de zamanla değişmiştir. Önceleri bu denetim, "Bilgisayar Denetimi" (Computer Audit), "Elektronik Veri İşleme Denetimi" (Electronic Data Processing (EDP) Audit) olarak adlandırılırken, daha sonra "Bilgi Teknolojilerinin Denetimi" (Information Technology (IT) Audit) ve "Bilişim Sistemlerinin Denetimi" (Information Systems (IS) Audit) olarak adlandırılmaya başlanmıştır. [4]

Bilişim sistemlerine ilişkin kontrollerin değerlendirilmesinin bilişim teknolojisinin kendine özgü özellikleri nedeniyle, bu konuda belirli düzeyde bilgi birikimi olan kişiler eliyle yerine getirilmesi gerektiği açıktır. Geçmişte ve hatta günümüzde bazı kurumlarda böyle uzmanlar, bilgisayar denetçisi (computer auditor), bilgi işlem denetçisi (EDP auditor) olarak

[4] Menkus, Belden and Gallegos, Frederick, "An Introduction to the IT Auditing", EDP Auditing, Auerbach Publications, 2001, s.12/2.

adlandırılmaktadır. Ancak günümüzde birçok kurumda bu uzmanlar bilişim sistemleri denetçisi (IT or IS auditor) olarak nitelendirilmektedir.[5]

Yüksek Denetim Kurumları ve Bilişim Sistemleri Denetimi

Bilişim teknolojisindeki gelişim, denetim birimleri üzerinde iki yönlü etkide bulunmaktadır. Birincisi denetim elemanlarının denetim işini kolaylaştırmak için bizzat bilişim teknolojisinden faydalanmaları (bilgisayar destekli denetim tekniklerini kullanmaları), ikincisi de denetlenen kurumların bilişim teknolojisine geçmeleri dolayısıyla bilişim ortamında denetim yapmak zorunda kalmalarıdır.[6]

Bilişim sistemlerinin varlığı temel denetim amaçlarını değiştirmemekle birlikte, denetim kanıtını, denetim izini ve iç kontrol ortamını değiştirmesi, yeni suç ve hata yapma mekanizmaları ve fırsatları[7] ortaya çıkarması gibi denetçinin riskler hakkındaki görüşleri üzerinde etkili olabilecek bir özelliğe sahip olduğundan, denetim sürecinde, tekniğinde, kanıtlarında ve en önemlisi denetim anlayışında değişimlerin yaşanmasına neden olabilmektedir. Bu değişim, denetçinin yeni duruma uyum sağlamasını ve elektronik bilgi ortamlarının denetim sürecini nasıl etkileyebileceğini dikkate almasını gerektirmektedir.[8] Bugün bilişim teknolojilerinin denetlenen kurumlarda yoğun şekilde kullanılmasının beraberinde getirdiği riskleri makul seviyeye düşürecek kontrol mekanizmalarının kurulması ve belirli standartlar çerçevesinde bu kontrollerin kurulup kurulmadığının denetlenmesi gerekliliği bulunmaktadır.

Bu çerçevede yüksek denetim kurumları, bu gelişmeleri yakından takip ederek bilişim teknolojilerinin getirdiği yeni durumlara ayak uydurmaya çalışmış, özellikle bu konudaki çalışmalarını daha önceden başlatan Sayıştayların ürettiği raporlar ve denetim rehberleri diğer tüm Sayıştaylarca paylaşılmıştır. Bu arada başta INTOSAI olmak üzere uluslararası meslek kuruluşlarının da bilişim sistemleri denetimine yönelik standartların

---

[5] Özkul, Davut, a.g.e. s.42.

[6] Özkul, Davut, "Bilişim Sistemi Kavramı ve Bilişim Sistemlerinin Denetimi", Sayıştay Dergisi, Sayı: 44-45, Ocak-Haziran 2002, s.19.

[7] INTOSAI EDP Committee, IT Controls Student Notes, March 2007 s.3 -5, http://www.nao.org.uk/intosai/edp/trainingindex.html.

[8] Selvi, Yakup, Türel, Ahmet ve Şenyiğit, Bora,., "Elektronik Bilgi Ortamlarında Muhasebe Denetimi", 7. Muhasebe Denetimi Sempozyumu, Nisan 2005, İstanbul, s.1.

benimsenmesi ve iyi uygulama örneklerinin yaygınlaştırılmasına yönelik çalışmaları önemli katkılar sağlamıştır.

Uluslararası Standartlar ve Bilişim Sistemleri Denetimi

Denetim standartları, denetimin başlangıcından bitimine kadar izlenecek yol ve usulleri tarif eden kurallardır. Sayıştaylar ve denetçiler için denetim standartları yaptıkları işlerin kalite güvencesidir. Sayıştaylar açısından referans olarak kabul edilen uluslararası denetim standartları Uluslararası Sayıştaylar Birliği (INTOSAI) ve Uluslararası Muhasebeciler Federasyonu (IFAC) tarafından oluşturulan standartlardır. Ayrıca bazı ülkelerde Uluslararası Denetim Standartları (UDS) ve kendi iç mevzuatları esas alınarak ulusal denetim standartları oluşturulmaktadır. Bilişim sistemlerine ilişkin olarak ISO 27001 Bilgi Güvenliği Yönetimi ve Bilgi Sistemleri Denetim ve Kontrol Birliği (ISACA) standartları gibi bir dizi başka kurum ve kuruluş tarafından oluşturulmuş olan standartlar da vardır.

INTOSAI Denetim Standartlarında; denetçi ve Sayıştayın işlerini yeterli kalitede yürütebilmesi için gerekli yeterliliğe sahip olması ve Sayıştayın kendisini, iç kontrol mekanizmalarının güvenilirliğine dayalı denetim tekniklerini (sistem tabanlı teknikler), mali tablo analiz metodlarını, istatistiki örneklemeyi ve bilişim sistemlerinin denetimini içeren tüm güncel denetim metodolojileriyle donatması gerektiği belirtilmektedir. Ayrıca, muhasebe veya diğer bilgi sistemlerinin bilgisayarlaştırıldığı ortamlarda denetçi, denetlenen kurumun verilerinin doğruluk, tamlık ve güvenilirliğini sağlayan iç kontrollerin uygun çalışıp çalışmadığını belirlemelidir.

IFAC tarafından oluşturulan Uluslararası Denetim Standartlarına göre de; denetçi denetlediği kurumun, mali raporlama ve iş yönetim süreci içerisinde kullanılan bilişim sistemi ve bu sistemden kaynaklanacak risklere kurumun nasıl cevap verdiği hakkında yeterli düzeyde bilgi sahibi olmalıdır.

5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanununun "Dış Denetim" başlıklı 68 inci maddesinde, dış denetimin, isimleri sayılmamış olmakla birlikte, genel kabul görmüş uluslararası denetim standartları dikkate alınarak Sayıştay'ın Anayasal ve yasal yetki ve sorumluluklarına göre yürütülmesi esası benimsenmiştir. Buna göre, 5018 sayılı Kanunun yürürlüğe girmesi ile uluslararası genel kabul görmüş denetim standartlarının gerektirdiği tarzda denetim yapılması Sayıştay için kanuni bir zorunluluk haline gelmiştir.

Uluslararası Kuruluşların Bilişim Sistemleri Denetimine İlişkin Çalışmaları

Bilişim teknolojilerinin denetlenen kurumlarda hızla yaygınlaşması ve bu teknolojilere yönelik denetim metodolojisinin Sayıştaylarca geliştirilmeye çalışılması, yüksek denetimin konusu olan her alanda, elde edilen birikimi üyesi bulunduğu ülkelerle paylaşma platformu olarak görülen başta INTOSAI olmak üzere, birçok uluslararası kuruluşu bu konuda harekete geçirmiş ve bilişim sistemleri denetimine yönelik daimi çalışma grupları kurma yoluna yöneltmiştir.

INTOSAI Bilişim Sistemleri Denetimi Daimi Çalışma Grubu 1992 yılından beri bu konudaki gelişmeleri yakından izleyerek, elde ettiği birikimi üyelerine aktarmaya çalışmaktadır. Bu çalışma grubu, bilişim sistemleri denetimine ilişkin eğitim notlarını ve iyi uygulama örneklerini web sayfası aracılığıyla paylaşıma sunmaktadır. Burada yer alan ve düzenli olarak teknolojik gelişmelere göre güncellenen eğitim notları, birçok Sayıştay için bilişim sistemleri denetimine ilk adımın atılmasında önemli bir kaynak niteliğindedir. Ayrıca tüm üye kurumlara gönderilen ve web ortamında da paylaşılan "IntoIT Journal" adlı dergiyi yayımlamaktadır. Bu dergide, bu alandaki gelişmeler, yapılan toplantılarda alınan kararlar ve gelecekteki işbirliği alanlarına ilişkin konular işlenerek gelişmeler hakkında bilgi verilmektedir.

EUROSAI Bilişim Sistemleri Denetimi Çalışma Grubu da, üye ülke birikimlerinin paylaşımını daha ileri noktalara taşımak ve bilişim sistemleri denetimi alanında ortak faaliyetlerin yürütülmesini desteklemek amacıyla 2002 yılında kurulmuştur. Kuruluşunun hemen sonrasında, Sayıştayların kendi bilişim sistemlerini değerlendirebilmesi amacıyla bir metodoloji geliştirilmesi için "Sayıştaylarda Bilişim Sistemlerinin Kontrolü" konusunda bir çalışma yapılmasına ve eğitim faaliyetlerinin organize edilmesine yönelik bir proje geliştirilmiştir. Bu projedeki metodoloji ve uygulama, Sayıştay'ın mevcut durumunun bir takım standartlar çerçevesinde kontrol edilerek, güçlü ve geliştirilmesi gereken yönlerinin tespitini sağlayan ve eylem planı ile sonuçlanan bir faaliyettir. Şu ana kadar hemen hemen tüm üye Sayıştaylar bu metodolojiyi kendi bünyelerinde uygulamışlardır. Geride kalan birkaç üye Sayıştayın da verilen teşvik ve gerekli destekle uygulamayı gerçekleştireceği görülmektedir. Sayıştay da bu metodolojinin uygulanmasına yönelik çalışmaları başlatmış ve önemli mesafeler almış bulunmaktadır.

Çalışma grubu, düzenli toplantılar yaparak üye ülke birikimlerinin düzenlenen seminerlerde tartışılmasına ve iyi uygulama örneklerinin yaygınlaştırılmasına katkı sağlamaktadır. Bu seminerlerden bir tanesi, 2006 yılının Mayıs ayında İsviçre'de gerçekleştirilen, İngiltere Sayıştayı tecrübesi temelinde Elektronik Kayıt Sistemlerinin Kurulması ve Denetimi semineridir. Bundan başka, diğer konuların yanında e-devlet ve e-ihale uygulamalarının oluşturacağı risklerin neler olabileceği ve denetimlerinin nasıl yapılacağı konularında da çalışmalar yapılmış bulunmaktadır.

ASOSAI de, Hindistan Sayıştayının önderliğinde bilişim sistemleri denetimi konusunda eğitimler yapılması, eğiticilerin yetiştirilmesi ve kurs materyallerinin geliştirilmesine yönelik çalışmalar yapmaktadır. Bu çalışmalarda geliştirilen kurs materyalleri değişik ülke Sayıştaylarında düzenlenen bilişim sistemleri denetimi kurslarında kullanılmaktadır. Tüm bu eğitim notlarından ve diğer ülke Sayıştayların rehberlerinden yararlanılarak hazırlanan Bilişim Sistemleri Denetimi Rehberi bu alandaki çalışmaların derlenmesi açısından önemli bir kaynak niteliğindedir.

INTOSAI Geliştirme Girişiminin (IDI) de, bölgesel Sayıştay birlikleri ile işbirliği halinde değişik ülkelerde bilişim sistemleri denetimi alanında başarısı kanıtlanmış metodolojisine uygun eğitim kurslarının düzenlenmesi ve eğiticilerin yetiştirilmesine yönelik faaliyetleri bulunmaktadır. Ayrıca internet üzerinden uzaktan eğitimin ilk uygulama konusu da bilişim sistemleri denetimi olmuştur. Bu çalışmaya Sayıştaydan da meslek mensubu katılarak sertifika almaya hak kazanmıştır.

Bilişim sistemleri denetimi alanında uluslararası kuruluşların çalışmalarına değinilirken bu konuda uluslararası bir otorite olarak kabul edilen Bilgi Sistemleri Denetim ve Kontrol Birliği'ne (ISACA) değinmemek bir eksiklik olacaktır. Bu Birliğin, denetçiler için mesleki ahlak kurallarını da içeren ve sürekli olarak geliştirilen denetim standartları bulunmaktadır. Ayrıca, bilişim sistemleri konusunda uzmanlığın bir göstergesi olan Uluslararası Bilişim Sistemleri Denetçi Sertifikası'nın (CISA) da bu birlik tarafından verilmesi, bu kurumun çalışmalarına özel önem verilmesini gerektirmektedir. Bu sertifika olmadan da bilişim sistemleri denetimlerinin yürütülebilme imkanı bulunmakla birlikte, sertifikası olmayan denetçinin yapacağı denetimlerde yetki ve nitelik tartışmasının yaşanması tüm ülkelerde olasıdır. Günümüzde bu sertifika, bilişim sistemleri denetimi alanında yüksek denetim kurumlarının yaptığı işlerin kalite güvencesinin teminatı olarak görülmektedir.

Bu Birliğin denetim standartları geliştirme ve uluslararası sertifika verme çalışmalarının yanında, kurumların sağlıklı ve güvenilir bir bilişim alt yapısının kurulmasına yönelik önemli çalışmaları da vardır. Bilişim teknolojilerinin yönetişim çerçevesi olarak görülen ve kurum bilişim sistemlerinin denetiminde, yönetiminde ve kontrolünde önemli bir araç olarak oluşturulan ve 4. sürümü yapılan COBIT (Control Objectives for Information and Related Technology) tüm dünyada, sistem değerlendirme yöntemlerinde temel başvuru ve uygulama rehberi niteliğindedir. COBIT, standartları dikkate alan, uygulamalar içerisinde sürekli geliştirilen ve denetçiler ile idareciler tarafından bilinmesi gereken bir kaynaktır. Bu nedenle hem denetim hem de uygulayıcı birimler açısından yoğun şekilde istifade edilmektedir.[9]

Sayıştay ve Bilişim Sistemleri Denetimi

Kamu kurumlarının bilişim sistemlerine artan bağımlılığı ve özellikle Türkiye'de bankacılık sisteminde meydana gelen sorunlar, denetim birimlerini bu sistemlerin kendine özgü riskleri konusunda daha dikkatli davranmaya yöneltmiştir. Daha açık bir ifade ile, kurum bilişim sistemlerinin güvenli ve güvenilir bir ortamda çalışıp çalışmadığına ve güvenilir veriler üretip üretmediğine ilişkin kontrollerin değerlendirilmesi ya da bir başka deyişle bilişim sistemlerinin denetiminin yapılması gerektiği ortaya çıkmıştır.

Bugün gelinen noktada, yüksek denetimin, gerek kapsamı ve niteliği, gerekse amaçları, işlevleri ve toplumsal etkileri açısından yeni boyutlar kazanmasının kendisine yüklediği sorumluluklar dikkate alındığında, Sayıştay, bilişim teknolojilerindeki hızlı gelişmenin yakından takip edilmesi gerektiğinin farkındadır.

Sayıştay, Türkiye'de bir bilgi işlem birimine sahip ilk kurumlar arasındadır. Günümüzde de yaygın ve güçlü bir bilişim alt yapısına sahiptir. Ancak, bilişim teknolojilerinin denetimde kullanılması veya bilişim teknolojilerinin imkanlarından yoğun şekilde yararlanan kurumların sistemlerinin denetlenmesine yönelik çalışmalar yeni başlamış bulunmaktadır. Özellikle 2003 yılı içerisinde Hazine Müsteşarlığında yürütülen ilk uygulamalar sonucu elde edilen başarı, kurumumuz açısından bu alanda yapılan çalışmaları daha ileriye götürme konusunda cesaret verici bir gelişme

[9] ISACA, CISA ve COBIT hakkında daha fazla bilgi için bakınız, www.isaca.org.

olmuştur.[10] Nitekim İngiltere ve kısmen de İspanya Sayıştayı ile yürütülen "Sayıştay'ın Denetim Kapasitesinin Güçlendirilmesi" Eşleştirme Projesinde, mali denetim ve performans denetimi ekiplerinden ayrı bir bilişim sistemleri denetim ekibi oluşturularak, bu konudaki bilgi birikimine uluslararası standartlar ve AB uygulamaları bağlamında önemli katkı sağlanmış ve bir metodoloji geliştirilmesinin önü açılmıştır.

Eşleştirme Projesi çerçevesinde yürütülen bu çalışmalarla, bilişim sistemlerinin denetimi alanında uluslararası standartların benimsenmesi ve denetim metodolojisi geliştirilmesi ile bu denetimleri uygulamak ve sürdürmek üzere denetçilerin yeterli bilgi ve deneyim sahibi olması ve gerekli örgütsel yapının oluşturulması hedeflenmiştir.

Bilişim sistemleri denetimi alanında proje bünyesindeki çalışmalar iki kademeli olarak yürütülmüştür. Birinci kademedeki çalışmalar, bilişim sistemleri ile ilgili başlangıç düzeyindeki bilgilerle sınırlandırılmıştır. Bu çalışmanın hedefi, bütün mali denetçilerin bilişim sistemleri ile ilgili temel riskleri belirleyebilecek şekilde eğitilmesidir. Bu kapsamda mali denetim rehberine bilişim sistemlerinin değerlendirilmesiyle ilgili bölümler eklenmiştir.

Bilişim sistemleri ile ilgili çalışmaların ikinci kademesinde ise, bilişim sistemleri denetiminde uzmanlaşmış denetçilerin kullanacağı daha ayrıntılı bir metodolojinin belirlenmesi hedeflenmiştir. Söz konusu bilişim sistemleri denetim rehberi hazırlandıktan sonra pilot denetim uygulamalarıyla da test edilmiş ve tamamlanarak Sayıştay bünyesinde tartışmaya açılmıştır. Bilişim teknolojisinin hızlı bir şekilde değişmesi, bu rehberde yer alan sistem kontrollerinin de düzenli olarak gözden geçirilmesini, güncellenmesini ve geliştirilmesini gerekli kılmaktadır. Bu açıdan rehber, sürekli değişebilecek ve yenilenebilecek dinamik bir tarzda kurgulanmıştır.

Kurumların mali nitelikteki işlerini destekleyen bilişim sistemlerinin genel ve uygulama kontrollerinin değerlendirilmesi için tasarlanmış olan bu rehber, bilişim sistemleri denetimi alanında uzmanlaşmış denetçilere, karmaşık sistemlerin bilişim sistemleri denetiminin nasıl planlanacağı, yürütüleceği ve raporlanacağı konusunda yol göstermektedir.

---

[10] Sayıştay Genel Kurulunun 06.10.2003 tarih ve 5071/1sayılı kararı ile kabul edilerek Türkiye Büyük Millet Meclisine gönderilmesi uygun bulunan ve 2002 yılı Genel Uygunluk Bildirimi eki olan "Hazine Bilişim Sistemleri Denetimi Raporu" için bakınız, http://www.sayistay.gov.tr/rapor/hazine/diger/Hazine_Bilisim_Sistemleri_Raporu.pdf

Rehberin hazırlanmasında başta Uluslararası Sayıştaylar Birliği (INTOSAI), Bilgi Güvenliği Standartları (ISO (17799, 27001)) ve Bilgi Sistemleri Denetim ve Kontrol Birliği (ISACA) standartları olmak üzere uluslararası standartlardan ve diğer ülkelerin ve ilgili kuruluşların iyi uygulama örneklerinden yararlanılmış ve Sayıştay Mali Denetim Rehberinde belirtilen süreçler dikkate alınmıştır.

Rehbere göre, bilişim sistemleri denetiminin amacı, denetlenen kurumlarda kullanılan bilişim sistemlerinin işlem ve uygulamalarının güvenlik ve güvenilirliğini sağlayan iç kontrolleri incelemek ve değerlendirmektir.

Bilişim sistemleri denetimi, bir kurumun mali tablolarını etkileyen tüm sistemlerinde yürütülebileceği gibi, bu tabloları etkileyen sistemlerden risk değerlendirmesi sonucunda sadece yüksek riskli olarak görülen sistemlerde de yürütülebilir.

Rehber öncelikle mali denetim kapsamında kurum bazında karmaşık sistemlerin denetiminde kullanılmak amacıyla hazırlanmakla birlikte, gerek duyulması durumunda mali denetim sürecine bağlı olmadan belirlenen sistemlerin güvenilirliğine ilişkin görüş bildirmek amacıyla da kullanılabilir.

Bilişim sistemleri denetimi yürütülürken risk tabanlı denetim yaklaşımına uygun olarak;

- Öncelikle incelenen bilişim sisteminden kaynaklanabilecek riskler belirlenir,
- Bu riskleri minimize edecek kontrol mekanizmaları belirlenir,
- Bu kontrol mekanizmalarının kurum tarafından oluşturulup oluşturulmadığı, oluşturulmuş ise etkin çalışıp çalışmadığı incelenir,
- İnceleme sonrası, iç kontrollerdeki zayıflıklar değerlendirilir,
- Elde edilen bulgular belli bir prosedüre göre raporlanır.

Bu çerçevede rehber, üç ana bölümden oluşturulmuştur:

Birinci bölümde, bilişim sistemleri denetiminin planlanması sırasında denetçinin yapacağı işler sistematik bir şekilde anlatılmaktadır. Bu işler, kurumun ve kurum bilişim sistemlerinin tanınması, mali tabloları etkileyen sistemlerin belirlenmesi, sistem risk değerlendirmelerinin yapılması, denetim stratejisinin belirlenmesi ve denetim programlarının hazırlanmasından oluşmaktadır.

"Sistem Kontrollerinin Değerlendirilmesi" başlıklı ikinci bölümde, kontrol değerlendirmeleri kontrol alanı bazında ele alınmaktadır. Her bir kontrol alanı için, kontrol hedefi, o alana ilişkin riskler ve bu riskleri minimize edecek kontrol faaliyetleri açıklanacak şekilde düzenlenmiş ve o alandaki kontrollerin varlığı ve etkinliğinin nasıl değerlendirileceği kontrollerin değerlendirilmesi başlığı altında gösterilmiştir.

Denetim sonuçlarının raporlanmasını konu alan üçüncü bölümde, taslak raporun hazırlanması, kurum yöneticileriyle görüşme ve nihai raporun yazılması ve ilgili birimlere sunulması konuları açıklanmaktadır. Ayrıca raporda düzeltilmesi istenen hususların nasıl izleneceği ve denetim kalite kontrolünün nasıl yapılacağı konuları üzerinde durulmaktadır.

Oluşturulan Sayıştay Bilişim Sistemleri Denetim Rehberi bu alandaki metodoloji geliştirme çalışmalarının önemli bir adımını oluşturmaktadır. Ancak bu adımın, uluslararası kuruluşların ve diğer Sayıştayların çalışmalarının yakından takip edilerek ve bu alanda yurt içindeki kurum ve kuruluşlarla işbirliği olanakları araştırılarak, düzenli ve sürekli çalışmalarla gelecekte hızlı yürümeye dönüştürülmesi kaçınılmazdır. Çünkü bilişim sistemleri denetimi, yukarıda açıklanan nedenlerle bir zorunluluk haline gelmiş; zaman içerisinde bilişim teknolojilerinde hızlı değişimlerin yaşanması ve denetim metodolojisinde meydana gelecek yeni yaklaşımların yakından izlenmesinin gerekmesi gibi nedenlerle göz ardı edilemeyecek bir olgu olarak Sayıştayın önünde durmaktadır.

Sonuç

Bilişim teknolojilerine yönelik yasal alt yapının sürekli olarak geliştirilmekte olması, kurumların bu teknolojilere yaptıkları yatırımların boyutlarının giderek büyümesi ve nihayet kurumların iş ve işlemlerini yürütürken artık bilişim teknolojilerine bağımlı hale gelmesi, görevleri kamu kaynaklarının yürürlükteki mevzuata uygun olarak tutumlu, verimli ve etkin şekilde kullanılıp kullanılmadıklarını denetlemek olan yüksek denetim kurumlarının bilişim sistemleri denetimine ağırlık vermeleri gerektiğini açıkça ortaya koymaktadır. Bu çerçevede tüm dünyadaki gelişmelere paralel olarak Sayıştayın da son yıllarda elde ettiği birikimleri hem kendi denetim çalışmalarındaki kalitenin arttırılması için kullanması, hem de bu birikimden yararlanacak kurumların denetiminde değer katan bir yaklaşımın benimsemesi kaçınılmazdır.

İki yıllık yoğun bir çalışma ile üretilen bilişim sistemleri denetim rehberi, eğitim materyalleri ve elde edilen birikim, kurumumuzdan beklenen hizmetlerin layıkıyla yerine getirilmesine önemli katkılar sağlayacaktır. Nitekim bu birikimin bir sonucu olarak, Sayıştay ile Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) arasında bilişim sistemleri denetimi, eğitimi, rehber ve yazılım geliştirilmesi ile ilgili konularda işbirliği yapılmasına ilişkin bir protokol imzalanmıştır. Buna göre, Sayıştayın kamu kurumlarında yürüteceği bilişim sistemleri denetimlerinde, 1995 yılından itibaren çalışmalarını bilgi güvenliği alanında yoğunlaştırmış ve bilgi güvenliği alanında Türkiye'deki en yetkin ve tecrübe sahibi kurum olan TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) ile işbirliği yapılacaktır. Bu işbirliği ile bir yandan Sayıştayın bilişim sistemlerine yönelik denetim işlerinin kalite güvencesini arttırması bir yandan da Devlet Planlama Teşkilatı tarafından geniş katılımla hazırlanan 2006-2010 yıllarını kapsayan ve eylem planlarıyla desteklenen Türkiye Bilgi Toplumu Stratejisinde öngörülen kamusal alanda bilgi güvenliği yönetim sistemlerinin oluşturulması ve geliştirilmesi amaçlarına da katkıda bulunulacaktır.

YARARLANILAN KAYNAKLAR

ASOSAI, IT Audit Guidelines, ASOSAI Research Project, Eylül 2003.

IDI, Introduction of IT Audit, e-learning Course Notes, 2007, http://idi.cliksonline.com.

INTOSAI EDP Committee, IT Controls Student Notes, March 2007. http://www.nao.org.uk/intosai/edp/trainingindex.html

Menkus, Belden and Gallegos, Frederick, " An Introduction to the IT Auditing", EDP Auditing, Auerbach Publications, CRC Pres LLC, 2001.

Özkul, Davut, "Bilişim Sistemleri Denetimi", Yayımlanmamış Yüksek Lisans Tezi, G.Ü. Sosyal Bilimler Enstitüsü, Ankara, 2002.

Özkul, Davut, "Bilişim Sistemi Kavramı ve Bilişim Sistemlerinin Denetimi", Sayıştay Dergisi, Sayı: 44-45, Ocak-Haziran 2002.

Selvi, Yakup, Türel, Ahmet ve Şenyiğit, Bora, "Elektronik Bilgi Ortamlarında Muhasebe Denetimi", 7. Muhasebe Denetimi Sempozyumu Nisan 2005, İstanbul.