ELEKTRONİK BELGE YÖNETİM SİSTEMLERİ VE DENETİM

Özcan Rıza YILDIZ*

ÖZET

Bilişim teknolojilerinin kamu kurumlarında yoğun şekilde kullanılmaya başlanmasıyla birlikte, belge tutma ve saklama faaliyetleri elektronik ortamda yürütülmeye başlanmıştır. Ancak elektronik belge yönetim sistemlerinin bilişim teknolojileriyle gelen riskler dikkate alınmadan oluşturulması güvenilir veriler üretilmesini, dolayısıyla kurum üst yönetiminin hesap verebilmesini zorlaştıracaktır. Bu nedenle, bu sistemlerin güvenli olarak çalıştırılması ve güvenilir veriler üretmesi için belirli kontrollerin kurulması ve bunların etkin olarak çalıştığının tespit edilmesi gerekmektedir. Bu sistemleri kullanan kurumların denetimleri yürütülürken, sistemlere özgü bir yaklaşım gösterilmesi, yapılan denetimin kalitesi ve elde edilen bulguların kanıt niteliğini koruması açısından önemli olacaktır.

Anahtar Kelimeler: Belge, Elektronik Belge Yönetimi, Denetim, e-imza.

ELECTRONIC RECORDS MANAGEMENT SYSTEMS AND AUDITING

ABSTRACT

With intensive use of information technologies in public organizations, the record retention and storage activities have led to the execution of electronic media. However, unless the risks emanated from information technologies are taken into account, electronic record management systems will fail in providing reliable data and in consequence severe difficulties in rendering accounts will be experienced by managers. Therefore, founding of specific controls and determination of the efficiency of their operations are needed to run these systems safely and to produce reliable data. During the conduction of the audits of these institutions, a peculiar approach to these systems holds key for the quality of the audit and for maintenance of the findings' proof quality.

Keywords: Record, Electronic Record Management Systems, Audit, e-signature.

* Sayıştay Uzman Denetçisi

I. GİRİŞ

Kamu veya özel tüm kurumlar, faaliyetlerine ilişkin bilgi ve belgeleri, işlemlerinin kanıtı olarak belirli bir süre saklamakla yükümlüdürler. Hukuki, idari veya mali, her ne saikle olursa olsun, kurumlarda işlem gören belge sayısı giderek artmaktadır. Bu artış, bir yandan kurumların üst yöneticilerini belge imzalamaya daha fazla zaman ayırmak zorunda bırakırken, diğer yandan mevcut belge yığını içerisinde ihtiyaç duyulanların bulunup çıkarılmasına ve istendiği şekilde kullanılmasına ilişkin süreçlerin yönetimi de güçleşmektedir. Bunlara ek olarak, bilişim teknolojilerinde son yıllarda kaydedilen gelişmeler ve bunların uygulamaya yansıtılması sonucu hızlanan e-devlet uygulamaları da, kurumları kendilerine ait bilgileri diğer kurumlarla ve/veya kamuoyuyla paylaşmaya yöneltmiştir. Buna göre, kurumların bilgi ve belgelerini hukuka uygun, güvenilir, paylaşılabilir, ulaşılabilir ve hesap verilebilir yapılar içerisinde tutmaları gerekmektedir. Bu durum, hem belge artışını sınırlamak hem de yönetimde basitleşme, hızlılık, kullanım kolaylığı ile zaman ve para tasarrufu sağlamak için belgelerin bir sistem dâhilinde yönetilmesine büyük bir önem kazandırmaktadır.

Belge yönetiminde amaç, kurumun aldığı karar ve yürüttüğü işlemlerin kanıtlayıcı bilgisini içeren belgelerin üretilmesi, dağıtılması, saklanması, paylaşılması ve imha edilmesi süreçlerinin iyi yönetilmesidir. Burada insan kaynakları, taşınır ve taşınmaz mallar, muhasebe ve diğer mali işlemler gibi değişik birimlerdeki tüm süreçlerin bir bütünün parçaları gibi yönetilmesi ve belgelerinin bir sistem dâhilinde tutulması esastır. Bu ihtiyaç başlangıçta belgelerin tasnif edilmesi ve kaliteli bir arşivcilik çalışmasıyla giderilmeye çalışılmış, ancak günümüzde bilişim teknolojilerinde meydana gelen hızlı gelişme, belge yönetiminin daha etkin bir şekilde yerine getirilmesini kolaylaştırmıştır.

Bilişim teknolojilerinin hayatımızın her alanında varlığını artırması, sunduğu imkanlarla birlikte birçok dezavantajı da gündemimize getirmiştir. Bu durum kamu kurumları açısından da geçerlidir. Zira bilişim sistemlerinin yaygınlaşması sonucu kamu hizmetleri daha ucuz, daha nitelikli ve kaliteli bir şekilde sunulurken, bu sistemlerin karmaşık yapısı ve beklentileri tam olarak karşılamasındaki belirsizlikler, sürdürülebilirlik ve güvenlik endişelerini de beraberinde getirmektedir. Dolayısıyla klasik anlamdaki belge yönetimi sorunlarına, günümüzde bilişim sistemlerinin olası sorunları da eklenmiş

bulunmaktadır. Çünkü bilişim teknolojileri doğası gereği riskli araçlar olup, riskleri önceden belirlenmez ve önlemleri alınmazsa, telafisi zor kayıplarla karşılaşılması kaçınılmaz olabilmektedir.

Bu çalışmada, kurumların en önemli varlıklarını oluşturan ve bilişim ortamında bulunan bilgi ve belgelerin yönetimi için oluşturulmuş olan sistemlerin belirli kriterler çerçevesinde yeterli ve etkin şekilde yönetilip yönetilmediği konusunda yürütülecek bir denetimde dikkate alınması gereken hususlara değinilecektir. Bundan önce, elektronik belge yönetim sistemine genel olarak yakından bakmak yararlı olacaktır.

2. BELGE VE BELGE YÖNETİMİ

2.1. Belge Kavramı ve Niteliği

Belge, "herhangi bir bireysel veya kurumsal fonksiyonun yerine getirilmesi için alınmış ya da fonksiyonun sonucunda üretilmiş, içerik, ilişki ve formatı ile ait olduğu fonksiyon için delil teşkil eden kayıtlı bilgi" (TS 13298) olarak tanımlanmaktadır. Bir başka tanım da, "fiziksel şekline, özelliğine ve hangi araç üzerinde olduğuna bakılmaksızın herhangi bir kuruluş tarafından üretilen, alınan, sahip olunan ve kullanılan her türlü yazışma, harita, sunu, manyetik veya kağıt kaydı, fotoğrafik film, çıktı ve benzeri dokümandır" (California, 2002) şeklindedir.

Genel olarak bir belge, üretilmesi ve/veya alınması, ilgili birimlere iletilmesi, işlemler sonrası tasnif edilerek ilgili dosyasında saklanması ve belirli dönem sonrasında da genel arşive gönderilmesi veya imha edilmesi gibi süreçlerden geçmektedir. Tüm bu safhalarda, üretilen bilginin hem kalitesinin hem de miktarının kontrol altına alınabilmesi, korunması ve gerek duyulduğunda etkili bir şekilde hizmete sunulabilmesi, değerini yitirdikten sonra da uygun bir şekilde elden çıkarılabilmesi için bilgi ve belgelerin yeterli ve etkin bir şekilde yönetilmesi gerekmektedir. Belge yönetimi ise, "kurumsal faaliyetler içerisinde üretilen belgelerin üretiminden uygun bir biçimde dağıtılmasına, erişilmesine, dosyalanmasına, ayıklanmasına ve/veya imha edilmesine kadar sürdürülen her türlü işlemin kontrol altına alınmasını sağlayan ilke ve uygulamalar" (Odabaş, 2008:123) şeklinde tanımlanmaktadır.

Teknolojideki hızlı gelişme, tüm dünyada e-devlet uygulamalarının aldığı mesafe ve kurumların iş süreçlerini bilişim ortamına giderek daha fazla

aktarmaları karşısında belge yönetimi konusunda yapılan düzenlemeler ve çalışmalar 'elektronik belge yönetimi'ne doğru yönelmiş bulunmaktadır. Belgelerin tutulması ve saklanması için gerekli olacak depolama alanlarından tasarruf edilerek, belgeler, bir ana bellek, sunucu, CD ya da DVD gibi yer kaplamayan araçlarda tutulabilmekte, istenen bilgi ve belgeye daha hızlı şekilde erişim sağlanabilmekte ve başka kullanıcılarla da paylaşılabilmektedir. Ancak, elektronik belgelerin neler olacağı, nasıl yönetileceği, nasıl saklanacağı ve nasıl imha edileceği, yeni teknolojilere uyumun nasıl gerçekleştirileceği gibi sorular da cevap beklemektedir. Bu cevapların önemli bir kısmı teknolojideki gelişmelerle karşılanmışsa da, halen cevap bekleyen sorular da yok değildir.

2.2. Elektronik Belge Yönetim Sistemi (EBYS)

Elektronik belge (e-belge) çeşitli şekillerde ortaya çıkabilmektedir. Örneğin, bilişim teknolojileri araçları tarafından okunabilir bir form içinde tutulan tüm belgeler e-belge olabileceği gibi, bilişim teknolojileri araçları tarafından yazdırılan, üretilen, kaydedilen, iletilen her türlü belge de e-belge olarak kabul edilmektedir. Nitekim elektronik belge, "bilişim teknolojileri aracılığıyla oluşturulan, iletilen ve korunan belgeler" şeklinde tanımlanmaktadır. Bu tür belgeler giderek el ile atılan (ıslak) imzalarla geçerlik kazanan kağıt belgelerin yerini almaktadır. Elektronik belgeler bilişim teknolojileri kullanılarak üretildiği gibi, orijinal formatından (örneğin kağıt dokümanların taranması suretiyle) elektronik ortama alınanları da olabilmektedir. Kurumlar, çeşitli şekilde kelime işlemci dokümanlar, tablolar, multimedya sunumlar, e-postalar, web sayfaları ve online işlemler gibi birçok elektronik belge üretmekte ve saklamaktadırlar (NAA, 2004: 13).

Burada öncelikli konu, elektronik belgenin, belge olarak kabul edilip edilemeyeceği hususudur. Belge olarak kabul edilebilmesi için, bir takım kriterlere göre oluşturulması ve belli özellikleri taşıması gerekmektedir. Kağıtlı ortamlarda bir belgenin yasa ve/veya diğer düzenlemelerde belirtilen şekle uygun olmasına, içerisinde olması gereken bilgilerin bulunmasına ve nihayetinde imzalanmış veya mühürlenmiş olmasına bakılmaktadır. Bu durum elektronik belgeler için de değişmemekte; ancak, e-belgelerde, değiştirilmesine imkân verilmeden ilk haliyle saklanıp saklanmadığı, yasa koyucu veya düzenleme yapma yetkisi bulunanlar tarafından belirlenen kriterler ve ilkeler çerçevesinde üretilmiş olup olmadığı, taşıması gereken

bilgileri içerip içermediği ve gelecekteki teknolojik gelişmelere uyumlu olarak her durumda kullanılabilir olup olmadığına bakılmaktadır. Başka bir deyişle, "elektronik belgelerin yasal, yönetsel ve kanıtsal olarak belge kimliği taşıyabilmesi için **özgünlük** (belgenin ilk halinin sahip olduğu bütün özellikleri koruması), **güvenilirlik** (belgenin sahip olması gereken özellikleri ve bunların işleme konma biçimini gösteren başta yasalar olmak üzere bütün politikalar, programlar, rehberler ve standartlarla bütünüyle uyumlu olması), **bütünlük** (belgenin içerik, bağlam, yapı ve sunumdan oluşan dört unsurundan tümüne sahip olması) ve **kullanılabilirlik** (belgenin e-devlet uygulamaları da dahil ortaya konan her türlü bilişim sistemi ile günümüzde ve gelecekte uyumlu olması) olarak ifade edilen dört temel özelliğe sahip olması gerekmektedir" (Odabaş, 2008: 129). Bu özellikleri taşıyan elektronik belgelerin, yaşam döngüsünü doldurması ve kurum beklentilerini karşılaması için etkin ve güvenilir bir sistem içerisinde yönetilip yönetilmediği de göz önünde tutulmaktadır. Bu sistem, elektronik belge yönetim sistemi (EBYS) olarak adlandırılmaktadır.

EBYS, "kurumların gündelik işlerini yerine getirirken oluşturdukları her türlü dokümantasyonun içerisinden kurum faaliyetlerinin delili olabilecek belgelerin ayıklanarak bunların içerik, format ve ilişkisel özelliklerini korumak ve bu belgeleri üretimden nihai tasfiyeye kadar olan süreç içerisinde yönetmek" (TS 13298) şeklinde tanımlanmıştır.

Aynı şeyin iki farklı ifadesi olarak görülen elektronik doküman ve belge kavramlarına ilişkin ayırımın yapılması gerekmektedir. Çalışmamızın konusunu oluşturan elektronik belge de nihayetinde bir doküman olmakla birlikte, oluşturulması, paylaşılması, saklanması ve imha edilmesine ilişkin özel düzenlemelerin olması ve hesap verebilirliğe katkıda bulunması açılarından dokümandan ayrılmaktadır. Bir diğer ifade ile belge, hesap verebilirliği göstermeye hizmet eden faaliyet ve kararların kanıtlarını içeren bir doküman türüdür. Ancak belgelerin kurumun günlük işlerinin yapılması sırasında üretilmesi ve belge üretmek için kurulan sistemin sürekli olarak doğru belgeleri oluşturabilmesi ve koruyabilmesi de gerekir. Bu durum, kurumun faaliyetlerini sürekli bir şekilde, normal iş süreçlerinin olağan bir ürünü olarak doğru belgelerle sonuçlandırıp sonuçlandırmadığı konusunda güvence almak durumunda olan denetim elemanlarının da dikkatinde olacaktır (EUROSAI, 2006a: 6).

Doküman ise, "kurumsal faaliyetlerin yerine getirilmesinde üretilen ya da toplanan, henüz belge vasfı kazanmamış her türlü kayıtlı bilgi" olarak tanımlanmaktadır (TS 13298). Bu nedenle, kurum faaliyetlerinin oluşturulması süreci içerisinde meydana gelen gelişmeleri yansıtmakla birlikte, henüz bu faaliyetlerin kanıtını oluşturacak belge vasfına ulaşmayanlar doküman olarak kabul edilmektedir. Örneğin her türlü taslak çalışma doküman niteliğinde olup, bu taslaklar, yetkili makamlarca onaylanması veya onaylanması anlamına gelecek işaretlerin konulması durumunda bir daha değiştirilmemek üzere belge niteliği kazanmış olacaktır. Daha açık bir ifadeyle, kurumlarda her türlü doküman genel bir belgeyi oluşturmakta, ancak, uygulamada, son kullanıcılar hepsini değil, önceden belirlenmiş kurallara göre bazılarını belge olarak belirlemektedir. Bu yönüyle bu işlemlerin elektronik ortamlarda yürütülmesinin, idari işleyiş açısından kolaylaştırıcı ve tasarruf sağlayıcı bir boyutu bulunmaktadır. Belge sayısındaki artış dikkate alındığında, bir o kadar, hatta ondan daha fazla dokümanın üretilmekte olduğu ve bunların da bir yönetim sistemi içerisinde ele alınmasına ihtiyaç duyulduğu açıktır. Elektronik doküman yönetim sistemleri (EDYS) olarak isimlendirilen bu sistemler, kuruma ait bilgilerin daha etkin şekilde kullanılmasına yardım eder ve saklanan bilgiye daha iyi ve hızlı erişim sağlanmasına imkan verir. Çoğu zaman da bu sistemlerin belge yönetim sistemiyle birbirinden ayrılmaz şekilde tek bir uygulamada birlikte çalıştığı görülmektedir.

Temelde kurumun günlük işlerini daha etkin ve hızlı yapmasına yönelik olarak tasarlanan elektronik doküman yönetimi sistemlerinde, dokümanların üzerinde değişiklik yapılmasına izin verilmekte veya dokümanların sistem içerisinde birden fazla versiyonu bulunabilmektedir. Ayrıca, doküman, üreticisi tarafından silinebilmekte, bazı saklama kriterleri ve planları içerebilmekte ve dokümanların saklanmasına ilişkin kontrol, kullanıcılar tarafından sağlanmaktadır. Bu özellikleri itibariyle doküman yönetim sistemi, elektronik belge yönetim sistemlerinden ayrılmaktadır (EUROSAI, 2006b: 14).

Günlük işlerin yapılmasının yanı sıra kurumsal hafızanın korunması ve kurumsal faaliyetlere delil teşkil eden belgelerin güvenilirliğinin sağlanmasına yönelik olarak oluşturulan elektronik belge yönetim sistemi (EBYS), doküman yönetim sisteminden farklı olarak, belgelerin değiştirilmesine kesinlikle izin

vermez, belli güçlü kurallarla kontrol edilen ortamları dışında belgelerin imha edilmesini önler, kesinlikle saklama planları içerir ve atanmış bir yönetici tarafından yönetilen güçlü bir belge düzenleme yapısı içerir. Bunun yanında sistem, belgelerin içeriği, yapısı ve bağlamı ile kayıt edildiklerine ve yetkilendirilmiş prosedürlerin ve denetim izlerinin yerinde olduğuna güvence verir. Bu durum, belgelerin yasal bir kanıt olarak kullanılması, kurum hesap verebilirliğinin geliştirilmesi ve iç ve dış denetim gereksinimlerinin karşılanması için kurumlara yardım eder (EUROSAI, 2006b: 14).

2.3. Elektronik Belge Yönetiminde Üstveri (Metadata)

Üstveri, elektronik belge gibi bir bilgi kaynağının biçimi ve içeriğinin bir özetidir. En genel tanımıyla veri hakkındaki bilgidir. Örneğin bir kütüphane kataloğu, yazarı, yayıncısı, başlığı gibi kitaplara ilişkin üstverileri içerir. Üstveri araştırıcıya ve bilgi yöneticilerine, konu, anahtar kelimeler, oluşturulan tarih ve belgenin muhatabı gibi kaynağın kendisinde her zaman bulunamayacak bilgileri ihtiva ederek yardım eder. Çoğu zaman kaynağın kendisinden çok üstverileriyle araştırmak daha etkin olmaktadır (EUROSAI, 2006b: 15).

Üstverinin diğer bir özelliği bilgi kaynağının kendisinden ayrılabilmesi ve gerçek kaynak bulunmazsa bile kendisinin kullanılabilir olmasıdır. Örneğin, kütüphanedeki fiziksel bir kitaba ilişkin elektronik form içindeki üstverilere dünyanın her yerinden erişim sağlanabilir, böylece kitabın kendisi sadece kütüphane raflarındayken, bir konuyu araştıran olası okuyuculara onun hakkında bilgi verilir (EUROSAI, 2006a: 15).

Bu özellikleri nedeniyle, elektronik belge yönetim sistemlerinde belgelerin üstverileriyle birlikte tutulması gerektiği ifade edilmektedir. Özellikle değişik uluslararası çalışmalarda, üst verilere ilişkin düzenlemelerin, sistemin tasarımı aşamasında düşünülmesi gerektiği vurgulanmaktadır (Odabaş, 2008:135). Bu nedenle, doğru üst veriyi alma ve koruma, giderek artan şekilde sayısal nesnelerin yeniden kullanımı ve korunmasını kolaylaştırmakta olduğundan, çok sayıda üstveri şeması ve standardı geliştirilmiş durumdadır (Day, 2009: 1).

Bazen veri ve üstveri arasındaki ayırım çok açık olmayabilir. Örneğin bir belgenin indeksleme bilgilerinin (adı, tarihi gibi), bu belgenin üstverisinin parçası olduğu açık olmakla birlikte, bir belgenin denetim izleri ve saklama

listesi ise ya veri ya da üstveri olarak dikkate alınabilmektedir. İndeksleme, koruma, iade etme gibi üstverinin farklı türleri için farklı tanımlamalar yapılmaktadır. EBYS uygulamasının olası tüm üstveri gereksinimlerini burada tanımlamak olası değildir. Kurum ve uygulamalar farklı ihtiyaç ve geleneklere sahip olduğundan, hesap adlarına ve işlem tarihlerine odaklanan bazı kurumlar indekslemeye ihtiyaç duyarken, diğerleri katı hiyerarşik numaralamayı tercih edebilir (Cornwell, 2001: 87).

2.4. Elektronik Belge Yönetim Sisteminde e-imza ve Güvenlik

Elektronik belge yönetimi sistemleri aracılığıyla oluşturulan belgelerin güvenli bir şekilde bir yerden bir yere iletilmesi durumunda gönderenin gerçekten gönderip göndermediği, alıcının da alıp almadığı ve bu gönderme ve alma sırasında belgenin içeriğinin yetkisiz kişilerce görülmediği ve değiştirilmediğinin güvence altına alınması önemli bir konudur. Günümüzde tüm dünyada olduğu şekliyle bu güvence, yine teknolojik gelişmelerin yardımıyla güvenli şekilde oluşturulmuş elektronik imzalarla sağlanmaktadır.

Belgeler, farklı şekillerde olsa bile, imzalanabilmeleri durumunda hepsinin aynı şekilde hukuki geçerliliğinin ve doğacak sorumlulukların taşınacağının bir göstergesidir. Bu açıdan, güvenli şekilde oluşturulmuş elektronik imza, nitelik olarak, tükenmez kalemle bir kağıda atılan bildiğimiz imzadan farklı değildir. Aralarındaki tek fark birinin bir kağıt üzerinde olması, diğerinin de elektronik ortamda bulunmasıdır (Ahi, 2004).

Elektronik imzaya ihtiyaç duyulmasının en önemli sebebi, hukuki işlemlerde güvenlik, kimlik tespiti, inkâr edilmeme gibi özelliklerin sağlanmak istenmesidir. Ancak, elektronik imza genel bir ifade olup, birçok yöntemi bulunmaktadır. Bilgisayar ekranına kalemle atılan imza, biyometrik imza (göz retina taraması, parmak izi taraması ve sesli), el yazısıyla imzanın tarayıcıdan geçirilerek elektronik belgelere eklenmesi ve güvenli sayısal imza gibi farklı uygulamaları bulunmaktadır. Bununla birlikte, elektronik belge yönetim sistemi içerisinde oluşturulacak ve yaşam süreci içerisinde varlığını sürdürecek olan belgelerin kanıt niteliğini koruması için kabul edilen yöntem, bilginin bütünlüğünü ve tarafların kimliklerinin doğruluğunu sağlayan güvenli şekilde oluşturulmuş elektronik imza, sayısal imzadır (Erturgut, 2003: 68).

Farklı tanımlamalar bulunsa da, elektronik imza, "başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik

doğrulama amacıyla kullanılan elektronik veri" (EİK, 2. md.) olarak tanımlanmaktadır. Bu tanım gereği, oluşturulması gereken güvenli elektronik imza, değişik ülkelerde kabul edilen farklı kriterler bulunsa da; münhasıran imza sahibine bağlı olan, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan ve imzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan elektronik imzadır (EİK, 4. md.).

Bu çerçevede, güvenli oluşturulmuş elektronik imza ile sadece gönderenin kimliği sorununun yanında belgenin iletim esnasında değiştirilmeden orijinal haliyle ulaştığına ve alıcının da aldığını inkar edemeyeceğine ilişkin bir güvence verilmektedir. Bu nedenle de, güvenli, iyi ve yeterli şekilde yönetilen elektronik sistemlerde tutulan belgeler, denetim elemanları ve/veya diğer hukuki makamlar açısından geçerli ve güvenilir bir kanıt oluşturmaktadır. Ancak, elektronik belge yönetim sistemi içerisinde tutulan ve elektronik imzalı bulunan bu belgelerin saklanmasında özgünlüğün korunması için e-imzaların sürekliliğinin sağlanması gerekir. Bu konuda sertifika sağlayıcılara belirli kriterler çerçevesinde görevler verilmişse de esas olarak kurum, elektronik imzalı belgeleri belgenin yaşam süreci boyunca saklamalı ve zamanla meydana gelebilecek kriptografik zayıflıklar da düzenli olarak takip edilmelidir. Bu nedenle, elektronik belge yönetim sistemleri kurulmadan önce tasarım aşamasında e-imza kullanımına ilişkin düzenlemelerin planlaması yapılmalıdır (Cornwell, 2001: 68).

2.5. Yeterli ve Etkin Bir Belge Yönetimi İçin Genel Esaslar

Belge tutma ve bunların belirli bir sistem yardımı ve sorumlu bir yönetici eliyle yönetilmesi; uygun politikaların oluşturulması; politikaların uygulanmasına ilişkin stratejilerin geliştirilmesi ve uygulama için prosedürlerin belirlenmesi gibi hususlar, etkin bir belge yönetimi için genel esaslar olarak sayılmaktadır. Ayrıca, tüm bu esasların gerçekleştirilmesini sağlayan bir elektronik belge yönetimi uygulama yazılımının bulunması ve belirlenen ilkelere ve/veya tabi olunan diğer mevzuata uygun olarak işletilmesi de bu esaslara dahil edilmelidir.

İş süreçlerini belgelemek için, öncelikle hem elektronik belgelerin yapısı hem de belge olarak sisteme alınacak olan bilginin açık bir şekilde

anlaşılması gerekir. Burada, strateji ve prosedürleri geliştirecek ve uygulayacak, bunların uyumluluğunu izleyecek ve gerekli uzmanlığı sağlayacak olan tecrübeli ve yeterli bilgi ve birikime sahip belge yöneticisinin atanması önemlidir. Bununla birlikte, kurum üst yönetimi, kurum belgeleri gibi tüm elektronik kanıtları korumak için resmi bir politikayı da benimsemelidir. Bu politika, elektronik belge yönetim prosedürleri ve uygulamalarının geliştirilmesi ve korunması için bir çerçeve oluşturmaya hizmet etmeli ve zaman içinde iş ihtiyaçlarında ve sistemlerde meydana gelecek değişiklikleri ve gelişmeleri izlemek için rehberlik edecek ilkeleri de sağlamalıdır (EUROSAI, 2006b: 9-10).

Kurum belgelerinin ihtiyaç duyulduğu sürece hem erişilebilir hem de kullanılabilir kalmasının sağlanması için bir strateji de benimsenmeli, uygulanmalı ve izlenmelidir. Anlaşılması ve kullanılması kolay olan prosedürler, tasarım süreci içerisinde belirlenen esaslar çerçevesinde elektronik belgeleri üreten her elektronik sistemi kapsamalıdır.

Elektronik belge yönetim sistemleri de, geçerli ve güvenilir belgeleri yönetmek ve gerektiğinde onların geçerliliğinin kolaylıkla doğrulanabilir olmasını sağlamak için tasarlanmalıdır. Sistemde bulunan bilgi ve belgelere uygulanacak uygun değerlendirme, listeleme ve imha faaliyetleri için gerekli olan politika ve prosedürlere göre koruma yeterliliği sağlanmalıdır. Daha önemlisi, iş süresince en iyi belge tutma uygulamasına ilişkin kültürün geliştirilmesi esas olup, bu ve bütün diğer gerekliliklerin temelini oluşturmak için de personelin bu konuda eğitimi zorunludur.

Sistemin hem içeride belirlenen politika ve ilkelere, hem de dışarıdan düzenleme yetkisi bulunan otoriteler tarafından belirlenen standart, iyi uygulama örneği veya mevzuat düzenlemesine uygun olarak çalışmasının sağlanması için düzenli olarak izlenmesi gerekmektedir. Belge yöneticisinin bu yolla üst yönetime uygunluk güvencesi vermesi de sağlanmalıdır.

Bu esaslar çerçevesinde, kurulacak olan elektronik belge yönetim sistemlerinin güvenilir, geçerli ve hukuka uygun belge üretebilmesi ve bu yolla kurumun yükümlülüklerini yerine getirerek hesap verebilirliğini güçlendirmek için, kurulması gereken kontrollerin değerlendirilmesi gerekmektedir. Bu değerlendirmenin esas olarak kurumların kendi iç yönetim süreçlerinin bir parçası olarak yapılması gerekmekle birlikte, elektronik belge yönetim sisteminin ürettiği/muhafaza ettiği belgeler üzerinden kurumu

denetlemekle yükümlü olan dış denetçilerin de bu değerlendirmeyi yapması ya da yapılan değerlendirmeleri gözden geçirmesi, sağlıklı sonuçlara ulaşabilmesi için önem arzetmektedir.

3. ELEKTRONİK BELGE YÖNETİM SİSTEMLERİNİN DENETİMİ

Denetim, denetim amacına uygun olarak, önceden belirlenmiş standartlar, ilkeler ve/veya mevzuat çerçevesinde kanıt toplama ve değerlendirme sürecidir. Bilişim sistemleri denetimi de, "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" (Weber, 1999) olarak tanımlanmaktadır. Elektronik belge yönetim sistemleri (EBYS) uygulamalarının denetiminde de amaç, bu sistemlerin belirlenen standartlara, ilgili politika ve prosedürlere ve/veya mevzuatta öngörülen esaslara uygun olarak yeterli ve etkin bir şekilde çalışıp çalışmadığı ve sistemin kurumun hesap verebilirliğine yönelik bir yapı içerisinde yönetilip yönetilmediğinin incelenmesidir. Bir başka deyişle bu denetimde, elektronik belge yönetim sistemlerinin güvenli çalışması ve güvenilir veri üretmesi için kurulması gereken kontroller risk tabanlı bir yaklaşımla incelenmekte ve değerlendirilmektedir.

Risk tabanlı denetim yaklaşımında, öncelikle bilişim sisteminden kaynaklanabilecek riskler belirlenmekte; bu riskleri minimize edecek kontrol mekanizmaları tespit edilmekte; bu kontrol mekanizmalarının kurum tarafından oluşturulup oluşturulmadığı, oluşturulmuş ise etkin çalışıp çalışmadığı incelenmekte; inceleme sonrası kontrollerdeki zayıflıklar değerlendirilmekte ve elde edilen bulgular belli bir prosedüre göre raporlanmaktadır.

Bu denetimin sonuçları, hem bir kurumun mali karar ve işlemlerine dayalı olarak üretilen mali tabloların ve raporların doğruluğu ve güvenilirliği (mali denetim) hem de kaynakların ekonomik, verimli ve etkin olarak kullanılıp kullanılmadığının (performans denetimi) tespit edilmesi için yapılacak denetimlerde dikkate alınmaktadır. Performans denetimi yaklaşımında, elektronik belge yönetim sisteminin kurulması ve geliştirilmesi süreçlerinde ekonomi ilkesine riayet edilmesi, sistemin verimli işletilmesi,

kurumun amaçlarını en iyi şekilde gerçekleştirmesi ve hesap verebilirliğini güçlendirmesine en azami katkıyı sağlayacak şekilde tasarlanması ve yönetilmesi gibi açılardan sistemin değerlendirilmesi hedeflenmektedir. Mali denetim açısından da, muhasebe sisteminin neredeyse tümüyle elektronik kayıt sistemi üzerinden işletildiği dikkate alındığında, elektronik belge yönetim sisteminin güvenilirliği ve ürettiği bilginin doğruluğu büyük önem taşımaktadır.

Bu nedenle de gerek denetimlerin yürütülmesi sırasında yapılacak testler ve analizler açısından, gerekse denetim sonucu elde edilen bulgu ve değerlendirmelerin isabetlilik düzeyi ve kalite güvencesi açısından, elektronik belge yönetim sistemlerinin kendisinden beklenenleri yerine getirmesine zarar verebilecek olan temel risklerin neler olabileceğinin iyi bilinmesi gerekmektedir.

3.1. Elektronik Belge Yönetim Sistemlerinde Riskler ve Denetim Açısından Önemi

Bilişim teknolojileri araçları ve bunların oluşturduğu sistemler, doğası gereği riskli alanlar olduğundan, elektronik belge yönetim sisteminin iyi ve yeterli şekilde çalışması sağlanmadığı durumlarda, bu sistemlerde tutulan belgelere olan güven sarsılacak, geçerlilikleri ve güvenilirlikleri konusunda şüphe oluşacaktır. Ayrıca, kurumun iş süreçleri içinde alınan karar ve yürütülen işlemlerin kanıtı olarak tutulan, saklanan, paylaşılan belgeler zarar görecektir. Kurumun yaşayacağı itibar kaybı yanında, yasal yükümlülüklerinin yerine getirilmesinde aksaklıklara sebep olunarak olası para ve idari cezalarla karşılaşılması muhtemel olacaktır. Dolayısıyla elektronik belge yönetim sisteminin etkin ve güvenilir olup olmadığı, yürütülecek her tür denetim için üzerinde titizlikle durulması gereken bir konudur.

Sisteme alınması, ilgili yerlere iletilmesi, işi bitenlerin saklanması ve saklama süresi dolanların belirlenen prosedürler çerçevesinde imha edilmesi süreçlerinden geçen belgeler, bilişim sistemleri yardımıyla sürdürülen bu safhaların her birinde belirli risklerle karşı karşıya kalacaktır. Bu nedenle, elektronik belge yönetim sistemlerinin, bu risklerin etkilerini kabul edilebilir bir düzeye çekecek kontrollerle birlikte oluşturulması gerekmektedir. Özellikle, bilişim sistemlerinde saklanması gereken belgelerin kolaylıkla kaybolabildiği, silinebildiği, kopyalanabildiği, bozulabildiği veya herhangi bir

iz bırakmadan değiştirilebildiği unutulmamalıdır. Bu çerçevede, belgenin yaşam sürecinde karşı karşıya olduğu temel risklerin bir kısmı şunlardır:

- Belgenin sisteme tam olarak alınamaması,
- Sisteme alınması sırasında belgenin bütünlüğünün kaybolması,
- Sisteme alımının hemen akabinde belgede değişikliklerin yapılması veya kasıtlı olarak tahrif edilmesi,
- Belgelerin yanlış klasör ve üst verilerle ilişkilendirilmesi,
- Belgelere teknolojik değişiklikler nedeniyle erişim sağlanamaması,
- Belgelerin ve ihtiva ettiği bilgilerin yetkisiz kişilerce açıklanması, değiştirilmesi veya bozulması,
- Belgelerin doğru şekilde sınıflandırılmaması,
- Belgelerin üst verilerinde değişiklikler yapılması,
- Belgelerin zamanından önce veya yetkisiz kişilerce imha edilmesi veya etkin şekilde imha edilememesi.

Doğrudan belge yönetim sisteminin etkin ve güvenilir olup olmadığını inceleme konusu yapan bir denetim kadar, bu sistemin ürettiği belgeler üzerinden yürütülen bir denetimde de, sistemin sahip olduğu risklerin sağlıklı bir şekilde tespiti ve analizi büyük önem taşımaktadır. Risklerin değerlendirilmesi konusundaki muhtemel zaaflar, denetim elemanları ve kurumları için de ciddi güvenilirlik ve itibar sorunlarına yol açabilecektir.

3.2. Bilişim Sistemleri Denetimi ve EBYS

Bilişim sistemleri denetimi, planlama, sistem kontrollerinin değerlendirilmesi ve raporlama safhalarından oluşmaktadır.

Sistem kontrollerinin değerlendirilmesi, kuruma ait tüm bilişim sistemleri faaliyetlerinin sürekliliğinin sağlanmasına yönelik yapı, yöntem ve prosedürlere ilişkin kontrollerden oluşan ve uygulama yazılımları ve bunlara ilişkin kontroller için güvenli bir ortam oluşturan *genel kontroller* ile kurumun iş süreçlerinin bir kısmının veya tamamının bilgisayar ortamında yapılmasını sağlayan elektronik belge yönetimi, muhasebe gibi yazılımların, kurum işlemlerinin ve verilerinin tamlığını, kullanılabilirliğini ve makul bir ölçüye kadar güvenilirliğini güvence altına alan *uygulama kontrolleri* başlıkları altında yapılmaktadır.

Elektronik belge yönetim sistemleri, bilişim sistemleri denetimi açısından

önemli bir uygulama alanı olup, uygulama kontrollerinin konusunu oluşturmaktadır. Ancak bu uygulamanın genel çalışma ortamının güvenli olması için, uygulamaya özgü genel kontrollerin de dikkate alınması gerekmektedir.

Elektronik belge yönetim sistemleri denetiminde genel kontroller, sistemin güvenli çalışması için kurulması gereken üst düzey kontrolleri içermektedir. Bu denetimlerde, genellikle sisteme yönelik oluşturulması ve oluşturulduktan sonra titizlikle takip edilmesi gereken strateji, politika ve prosedürler gibi genel esasları düzenleyen kontroller ile güvenli çalışan bir sistemdeki beklentilere yönelik kontrollerin olup olmadığı, varsa etkin çalışıp çalışmadığı, yoksa başka telafi edici düzenlemelerin bulunup bulunmadığı gibi hususlar incelenmektedir. Bu inceleme esnasında elektronik belge yönetim sisteminin içinde çalıştığı kurumun bilişim sistemlerinin de güvenli ve güvenilir çalışmasının bir gereklilik olduğu unutulmamalıdır.

Denetim sırasında gerçekleştirilen uygulama kontrolleri ise, girdi, işlem ve çıktı kontrollerinden oluşmakta olup, belgenin sisteme dahil edilmesi, belge olarak tanımlanması, işlem göreceği yerlere iletilmesi, beklendiği şekilde işlem görmesi, belirlenen biçim, içerik ve bağlamı ile kabul edilmesi ve saklanması süreçlerine ilişkin belirlenen kontroller veya telafi edici düzenlemeleri içermektedir.

Elektronik belge yönetim sistemlerine yönelik bilişim sistemleri denetimleri, EBYS standartları (TS 13298 veya ISO 15489), (TS) ISO/IEC 27001-2 Bilgi güvenliği yönetimi standardı, kendisi bir standart olmamakla birlikte, birçok iyi uygulama örneğini birleştiren COBIT (Control Objectives for Information and Related Technology-Bilgi ve İlgili Teknoloji için Kontrol Amaçları), ülke düzeyinde düzenleme yapma yetkisi tanınan kurumlarca belirlenen ilkeler veya mevzuat ile denetim birimleri tarafından uluslararası denetim standartları dikkate alınarak oluşturulan denetim rehberleri çerçevesinde gerçekleştirilmektedir. Bu çalışmada da, Avrupa Sayıştaylar Birliği-EUROSAI Bilişim Sistemleri Çalışma Grubu tarafından hazırlanan "Electronic Record Management, *An Audit Guide* - Elektronik Belge Yönetimi, *Bir Denetim Rehberi*" adlı çalışma ile Sayıştay Başkanlığı Taslak Bilişim Sistemleri Denetim Rehberi ve ülkemiz elektronik belge yönetim standardı (TS 13298) esas alınmıştır.

3.3. EBYS Kontrolleri ve Denetim

Etkin işleyen bir elektronik belge yönetim sisteminde bulunması ve denetim elemanlarının da yürüttükleri denetimler sırasında güvence alması gereken kontrollerin bir kısmı aşağıdaki gibidir:

Politika ve Prosedürlere İlişkin Kontroller

- Üst yönetim tarafından onaylanmış yazılı bir elektronik belge yönetimi politikası bulunmalı ve uygulanması izlenmelidir. Bu politika belgesinde, politikanın uygulanmasında görevli personel ve sorumluluklar belirlenmiş olmalıdır. Ayrıca, sistem kurumun tümünde etkili olacağından, politikanın bütün personelin kolaylıkla kavrayabileceği ve yapılan işlerle uyumlu olacak şekilde yazılması sağlanmalıdır. Politika belgesi gerektiğinde güncellenmelidir.

- Elektronik belge yönetimi politikasının uygulanmasına ilişkin olarak yazılı güncel bir stratejik plan olmalıdır. Bu stratejinin hedefi, üst düzey politika hedeflerini, kaynaklı ve zamanlı bir eylem planına dönüştürmek ve kurumun, üst düzey riskleri ile teknik ve diğer standartları karşılaması gereken belge tutma gereksinimlerini belirlemektir. Hedeflerin gerçekleştirilmesini gözden geçirmek, ilerlemeleri raporlamak ve teknolojideki değişiklikler ile iş gereksinimlerindeki değişiklikleri izlemek ve güncellemek için, uygulama planının bir yönetim çerçevesiyle desteklenmesi gerekir.

- Elektronik belge yönetiminin etkin ve güvenli yürütülebilmesi için yeterli sorumluluklarla yetkilendirilmiş bir yönetim birimi oluşturulmalıdır. Bu işlemlerin sağlıklı yürütülmesi için bu sistemin en kilit görevi, gerekli birikimlere sahip belge yöneticisidir. Belge yönetimine ilişkin faaliyetler, bu birimin desteğiyle iyi bir şekilde koordine edilmeli, görev ve sorumluluklar açıkça belirlenmelidir.

- Belge yönetimi sistemlerine ilişkin tüm bilgi ve varlıkları koruyacak, işlevlerini düzenli ve sürekli bir şekilde yerine getirmelerini sağlayacak etkin bir varlık yönetimi için gerekli tedbirler alınmalıdır. Bunun için;

  - belge yönetim sisteminde kullanılan varlıkların envanteri yapılmalı;
  - kullanım kuralları belirlenmeli;

- kullanımdan çıkartılması veya imhası belirli bir prosedüre bağlanmalı;
- kurum verileri uygun bir şekilde sınıflandırılmalı ve sistemde yürütülen bütün iş ve işlemler belgelendirilmelidir.

Bu çerçevede, elektronik belge yönetimine ilişkin politikaları, düzenlemeleri, standartları ve prosedürleri açıklayan uygulanabilir güncel doküman sağlanmalıdır. Bu doküman;

- veri tarama ve girme metotlarının bir tanımını;
- belgelerin nasıl gözden geçirileceği, güncelleneceği ve silineceğine ilişkin tanımlamaları;
- belgelerin nasıl indeksleneceğine ilişkin tanımlamaları;
- dosya isimlendirme düzenleri ve hiyerarşisini;
- belgelerin okunabilirliğini test etme prosedürlerini;
- yedekleme prosedürlerini ve yetkilendirilmiş belge tutma ve değerlendirme cetvellerini içermelidir.

▪ Kurum sistemlerine zarar verebilecek insan kaynaklı hata, ihmal ve suiistimalleri önleyecek tedbirleri almalıdır. Bunun için, sisteme yönelik politikalara uygun şekilde personelin rol ve sorumlulukları yazılı olarak belirlenmeli ve yeni ve değişen süreçleri kapsayacak şekilde güncellenen rollerine uygun eğitimler verilmelidir. Ayrıca sistemde, hassas noktalarda çalıştırılacak personelin seçiminde gereken özen gösterilmelidir. Bu konuda yönetim, personele ilişkin gözetim görevini etkin şekilde yerine getirmelidir. Personelin düzenli olarak belge yönetim sistemine ilişkin eğitim ve bilgi güncelleme programlarına katılması ve işten ayrılan personelin kullanımında olan varlıkları kuruma teslim etmesi ve kurum bilgilerine ulaşma yetkilerinin derhal kaldırılması sağlanmalıdır.

▪ Elektronik belge yönetiminin, belirlenen politika ve stratejiye uygun olarak işleyip işlemediği izlenmelidir. Yasal denetim, izleme sürecinin önemli bir aşamasını oluşturur. Elektronik belge yönetiminin kalitesi üzerindeki idari kontroller, hem kalite kontrol (iş süreçlerinin düzenli şekilde uygulanmasını sağlamak için gerçek zamanlı inceleme) hem de kalite güvencesi (iş süreçlerinin tasarlandığı gibi çalışıp çalışmadığını veya

değişikliklere ihtiyaç duyulup duyulmadığını değerlendirmek için süreç sonrası inceleme) açısından izleme sürecinin dayanak noktasını oluşturabilir.

- Elektronik ortamdaki varlıkların bütünlüğünü (varlıkların doğruluğunun ve tamlığının korunması), kullanılabilirliğini (yetkisi olanlar tarafından talep edildiğinde erişilebilir ve kullanılabilir olması) ve gizliliğini (bilginin yetkisiz kişiler, varlıklar ya da süreçlerce kullanılmaması ya da açıklanmaması) korumak için gerekli önlemler alınmalıdır. Bu konuda kurum, bilişim sistemlerinin güvenli ortamda çalışması için bilgi güvenliği standartları, ilkeleri ve iyi uygulama örnekleri çerçevesinde bilişim teknolojileri risklerine karşı gerekli önlemleri almalıdır (ISO 27001 ve COBIT).

Belgenin Sisteme Alınmasına İlişkin Kontroller

- Elektronik belge yönetim sistemi, mevcut elektronik belge oluşturma uygulamalarını, yeni belge oluşturma sistemlerini ve hem yeni olarak içeride oluşturulan belgelerin hem de kurum dışından alınanların sisteme alınmasını, yönetimini ve erişimini kapsamalıdır.

- Sisteme alınacak belge veya bilgiler tam olarak alınmalıdır. Elektronik belgeler kurumsal fonksiyonların yerine getirilmesi sırasında üretilir veya alınırlar. Kurum içinde üretilenler yanında kurum dışı kaynaklardan da belge akışı söz konusudur. Bu belgeler farklı kişi ve kurumlar tarafından üretilmiş farklı formatlarda olabilir. Belgeler tek doküman şeklinde olabileceği gibi belge grupları şeklinde de olabilir. Yerel veya geniş alan ağları, elektronik posta veya faks gibi elektronik araçlarla iletilebildikleri gibi sayısallaştırma yöntemiyle de elektronik ortama aktarılmış olabilir.

Bu konuda, öncelikle belirlenmiş prosedürler çerçevesinde yazılı hale getirilmiş süreçler bulunmalıdır. Bu prosedürlerin uygulamaları yönetim düzeyinde izlenmeli ve personele bu konuda eğitimler verilmelidir. Bunun yanında, iş sürecinin yakından gözlenmesinde de iç kontrol süreçlerinin kurulu olması gerekmektedir. Yönetimin de gözetim yükümlülüğünü gerçekleştirmesi sağlanmalıdır. Özellikle kağıt belgelerin taranarak sisteme alınmasında tarayıcı kalitesine ve tarama işlemlerinin gerektiği gibi yürütülmesine dikkat edilmesi gerekir. Ayrıca tarama sonrası kalite kontrolünün de yapılması yerinde olur. Taranacak belgelerin bir listesi bulunmalı ve tarama sonrası toplamları karşılaştırılmalıdır.

▪ Belgelerin elektronik belge yönetim sistemine alımı sırasında bütünlüğü kaybolmamalıdır. Sisteme alınacak belgelerin elektronik imzalı olması en önemli kontroldür. Bu noktada kurum bilişim sistemlerinin kötü niyetli yazılımlar için alınmış olan önlemler, elektronik belge yönetimi sistemlerini de kapsamalıdır.

▪ Elektronik belge yönetim sistemi, üretilen elektronik belgelerin bütün türlerinin içerik ve yapısını sisteme almalıdır. Sisteme alınan belgelerin, orijinal kağıt kopyalarının sistemdeki belge ve bilgilerin doğrulanabilmesine kadar korumak önemlidir. Aynı durumlarda, kanunun gerektirdiği yerlerde orijinalini tutmak gerekli olabilir.

▪ Sistem içerisine belgelerin alımı sırasında kasıtlı olarak tahrif edilmesi engellenmelidir (girdide sahtecilik). Zaman zaman belge oluşturma süreçleri geriye dönük olarak kontrol edilmelidir. Bunun yanında, belirlenen roller itibariyle varlıklara hem fiziksel hem de mantıksal olarak erişim kontrolleri oluşturulmalıdır. Bu kontrollerin iyi uygulanması için sistemin kilit aşamalarında belirli rollerin verilmesi gerekmektedir. Burada ayrıca bilişim sistemleri destek işlevlerinde de bu rollerin ayrılması yerinde olacaktır.

▪ Elektronik belge yönetimi, elektronik belgeyi üreten kişiyi, oluşturulan zamanı ve üzerindeki müteakip faaliyetleri konusundaki bilgisini de sisteme almalıdır. Denetim izi, bir belgeye ilişkin tüm faaliyet ve olayların kim, ne, ne zaman ve niçin gibi soruları cevaplayan belgelerdir. Denetim izi, denetim elemanlarına veya kanıt durumunda mahkemeye sunulabilen sorumluluk zincirini göstermede önemli, kilit bir unsurdur. Denetim izi, üreticisini, alıcısını, içeriğini, oluşturma tarihini, düzeltme yapma tarihini, gönderme tarihini, her türlü değişiklikleri ve tek bir belgeyle bağlantılı yetkilendirmeleri belgeleyecektir.

▪ Elektronik belge yönetimi, belgeyle bağlantılı olan standart üstveriyi de sisteme almalıdır. Yeni belge, içeriği, yapısı ve bağlamı ile birlikte, bir belgeyi oluşturan bütün elektronik bilgi kaynakları belgenin kendisiyle birlikte alınmalı ve korunmalıdır. Ancak üstveri oluşturma durumu karmaşıktır. İndeksleme ile birlikte, belgelerin parçası olarak sisteme alınması ve korunması gereken;

- **erişilebilirlik** (bir belgeye uygulanacak yasal sınırlamalar hakkındaki bilgiyi içerir),

- **saklama ve imha** (bir belgenin ne kadar süre tutulacağı ve hangi kriterler (tarih, yılsonu, vs.) itibariyle imhasına geçileceği hakkında bilgiyi içerir),
- **güvenlik bilgisi** (verilerin nasıl şifreleneceği konusundaki bilgi ve bu bilgi üzerine sınırlamaları içerir),
- **denetim izi** (belge üzerinde gerçekleştirilen bütün faaliyetleri dokümante eden bilgiyi içerir) ve,
- **göç ettirme** (belgeyi oluşturacak ve saklayacak yazılım versiyonları ve teknoloji platformları konusundaki bilgiyi içerir)

gibi diğer üst veri türlerini de içermelidir. Bu üstverinin tümü elektronik form içinde olmayabilir. Örneğin, göç ettirme üst verisi, sistemle ilgili donanım ve yazılım belgeleme rehberlerini içerecektir.

Dosya Tasnif Planına İlişkin Kontroller

▪ Elektronik belge yönetimi, belgelerin düzenlenmesine yönelik mantıksal yapıyı destekleyebilmelidir. Burada roman, biyografi, tarih ve benzeri bölümler altında organize edilen bir kütüphanedeki kitaplarla bir analoji kurulabilir. Buna göre dosya tasnif planları çerçevesinde bir mantıksal yapı oluşturulmalıdır. Bu plan hiyerarşik bir yapıda olmalı ve en az üç seviyeden oluşmasına imkan sağlanmalıdır. Ayrıca, dosya tasnif planının kurulum aşaması sonrasında doğabilecek güncelleme ihtiyaçlarına da imkan tanınmalıdır. Ancak, bir elemanın başka bir yere taşınması, o elemana ait referans numarası ve ad bilgisi gibi çeşitli üst verilerde değişiklik yapılması gerekebilir. Tüm bu işlemler, elektronik belge yöneticisi kontrolünde ve yetkisinde olmalıdır.

▪ Elektronik belge yönetimi, belgelerin bütünüyle yönetimini etkileyen olayların bir denetim izini tutmalıdır. Denetim izi, iki açıdan izlenmelidir: her bir belgeyi doğrudan etkileyen olaylar ve elektronik belge yönetimi politika ve stratejilerinin uygulamayla uyumlu olduğu güvencesini sağlayan faaliyetler. Bu tür belgeler denetim elemanlarına elektronik belge yönetimi sürecinin doğru ve sürekli şekilde işlediğinin kanıtını sağlar. Kağıtsız ortamlarda, belgelerin kağıt orjinalleriyle karşılaştırılamadığı yerde, tam, kapsamlı ve uygun şekilde yetkilendirilmiş süreç kontrol kayıtlarının yokluğu, kaçınılmaz olarak elektronik belge yönetim sistemi içerisinde tutulan belgelerin geçerliliğine şüphe oluşturacaktır.

▪ Elektronik belge yönetim sistemi içerisindeki tüm belgeler indekslenmeli ve gerektiğinde görülebilmelidir. İndeks bir belgeyi düzeltmenin anahtarıdır. Bir dosyayı indeksleme, üreticisine faydalı bir anahtar sağlar. Herkesin anladığı istikrarlı bir yaklaşım sağlamak için, kurumun bir indeksleme standardı bulunmalıdır. Ayrıca, indeksleme standardının, sistemin dokümantasyonun kolaylıkla erişilebilir bir parçası olması gerekir (bazı elektronik belge yönetimi sistemleri dosya yönetim yazılımı içinde indekslemeyi otomatikleştirir). Genelde, elektronik indekslemeler belgenin özelliklerine dayalı olmalıdır, tarih, konu, gönderici, alıcı ve sayısı(dosya, sözleşme, satın alma emri, proje, tazminat, sosyal güvenlik, vs.).

▪ Elektronik belgelerin belirlenen dosya tasnif planları ve varlık yönetimi çerçevesinde tanımlanan sınıflandırmalara uygun olarak doğru şekilde sınıflandırılması sağlanmalıdır. Elektronik belge yönetiminin kilit safhalarından biri de belgelerin sınıflandırılmasıdır. Doğru olmayan sınıflandırma sonucunda, bir daha belgeye erişim sağlanamayabileceği gibi, yetkisiz kişilerin belgeyi görmesine, bozmasına, kopyalamasına veya değiştirmesine yol açabilmektedir. Bu nedenle, sınıflandırma listelerinin hazır bulunması gerekir. Sınıflandırma işlemlerinin de belirli prosedürlere bağlı yürütülmesi sağlanmalıdır. Sistem, sınıflandırmayı otomatik şekilde yapabilmelidir. Bu konuda belge yöneticisinin önemli görevleri bulunmaktadır.

▪ Kaza veya isteyerek belgelerin kaybedilmesi engellenmelidir (yönetilen imha süreçlerinin dışında). Dosya yönetim sistemi, fiziksel olarak yaşamları boyunca belgeleri yöneten elektronik belge yönetim sistemi içindeki unsurdur. Dosya yönetim sistemi, ya silinemeyen depolama ortamının kullanımı ya da uygun koruma düzeyini sağlayan kontroller aracılığıyla belge bütünlüğünü korumalıdır. Bütün belgelerin, ilgili üst verileri, denetim izleri ve hem mantıksal hem de fiziksel araçları da dahil olacak şekilde yönetmesi gerekir. Dosya yönetim sistemi, aynı zamanda belgelerin, ortam değişimleri veya sistem değişiklikleri durumunda kopyalanmasını, yeniden biçimlendirilmesini ve transfer edilmesini desteklemelidir. Sistem bir felaket durumunda tüm belge yenilemeyi desteklemelidir. Bunun anlamı sistemin bütün hayati ve sürekli dosyaları ve onları göstermek için gerekli yazılımı çifte kayıt yapabilmesini sağlamasıdır.

Belgeye Erişim ve Güvenlik Kontrolleri

▪ Elektronik belge yönetim sistemi içerisinde uygun ve önceden belirlenen kriterlere göre korunan belgelere erişim kontrol edilmelidir. Sisteme erişim kontrolüne ilişkin düzenlemelere, bilgi güvenliği erişim politikasında yer verilmelidir. Genel erişim, kurum içinde bir kullanıcının statüsüne değil, rolleri ve gerçekleştirmeye ihtiyaç duydukları bilgiye bağlı olmalıdır. Benzer şekilde, sistem yönetimi olanaklarının (örneğin, diğer kullanıcılara erişim izinleri vermeye gerekli olanaklar ve silme belgeleri) da roller temelinde paylaştırılması gerekir. Belirli rollerin erişim türlerini gösteren bir erişim kontrol matrisi oluşturmak iyi bir uygulamadır. Denetim elemanları, zaman zaman bunun güncellendiğine ilişkin kanıt isteyebilirler.

▪ Elektronik belge yönetimi, bütün zamanlarda belgelerin içeriğindeki değişikliklere karşı korunmalıdır. Aktif iş ortamındaki yetkisiz değişime karşı belgeleri koruma, elektronik imzalama teknikleri, belgelerin şifrelenmesi, faaliyetlerin günlük kayıtları ve yetkilendirme, erişim kontrolleriyle sağlanabilir. Bu hayati ve teknik kontroller sistemde yer almalıdır ve belgenin bütün yaşam süreci içerisinde var olmalıdır. Burada, elektronik dokümanların değişebileceğini, ancak belgelerin asla değiştirilemez olduğunu hatırlamak gerekir. Sistem içindeki belgeler "sadece okuma ve asla üzerine yazılamama" prensibiyle korunmalıdır. Sonradan belgenin görünümü kopyaları üzerinden yapılmalıdır. Bu durum belgelerin yeni teknolojilere göç ettirilmesi sırasında da değişmemelidir. Ancak bir değişiklik yapılması gerekiyorsa, doğru değişikliklerin yapılması için yazılı prosedürlere uygun olması ve bu prosedürlerin doğru takip edilmesi için eğitimlerin alınması ve yönetimin de yakın takibi gerekir. Bu arada, yeni yazılımların veya güncellenen yazılım versiyonlarının uygulamaya doğrudan alınmadan önce gerekli testlerin yapılması gerekmektedir.

▪ Elektronik belge yönetim sistemi içerisinde belgelerin ve bilgilerin yetkisiz silinmesi önlenmelidir. Yetkisiz silinmesinin önlenmesi için erişim kontrollerinin uygulanması gerekir. Ayrıca, belgelerin sistem içerisinde silinmesi için yetkilendirilmiş yazılı prosedürlerin bulunması gerekir. Yönetim gözetiminin hiç bir safhada aksatılmaması sağlanmalıdır. Sistemde oluşturulan belge ve bilgiler periyodik süreçlerde gerçek zamanlı olarak yedeklenmeli, yedekleme sonrası etiketleme yapılmalı ve saklama

prosedürlerine göre gerekenlerin kurumdan uzak başka bir yerde tutulmasına ilişkin işlemlerin yürütülmesi sağlanmalıdır.

- Elektronik belge yönetim sisteminde yer alan üst verilerde doğru ve tam şekilde değişiklikler yapılmalıdır. Bu konuda değişimlerin önceden belirlenen prosedürler çerçevesinde yapılması için yönetimin yakın takibinin yanında sistem tarafından oluşturulan faaliyetlerin otomatik denetim izlerinin tutulması, düzenli olarak gözden geçirilmesi ve üst yönetime raporlanması gerekmektedir. Ayrıca belirlenen prosedürler çerçevesinde, değişikliklerin iki personel (değişikliği girecek biri, tatmin edici değişiklikleri gözden geçirecek ve teslim edecek biri) tarafından yerine getirilmesi kuralının uygulanması yerinde olacaktır. Burada, kalite kontrol ve süreç denetimlerinin yanında, yedekleme işlemlerinin de düzenli olarak yapılması sağlanmalıdır.

- Elektronik belge yönetim sistemi içerisinde tüm belgeler doğru ve uyumlu şekilde görüntülenmeli ve çıktısı alınabilmelidir. Bir belge sadece, yazıcı çıktısı veya bilgisayar ekranındaki görüntü gibi insan tarafından okunabilir bir form içinde olursa kullanılabilir. Belgeler üst verileri ve denetim izleri de dahil olarak, bütün yaşam süreçleri boyunca yetkilendirilmiş olanlar için erişilebilir olmalıdır. Bu, gerçek bir elektronik belge yönetimi stratejisinin önemini vurgular, uzun saklama periyotlarına sahip olan belgelerin gerçekliğini korumak için, onları orijinal olarak oluşturan yazılım ve donanım platformları kaçınılmaz şekilde değişir.

Belgenin Saklanmasına İlişkin Kontroller

- Elektronik belge yönetimi, belirlenmiş saklama kriterleri çerçevesinde belge saklama ve imha listelerini oluşturmalı, gerekli yerlerde sürecin gözden geçirilmesini desteklemeli ve bu listelerin uygulamasının gözden geçirilmesine imkan vermelidir. Gerektiğinde belgenin imhasını dondurmak veya bir yerde tutabilmek önemlidir.

- Elektronik belge yönetimi, belgelerin sistemde bağlantılı olduğu bütün üstverisiyle birlikte transfer edilmesine imkan vermelidir. Özellikle uzun dönemli saklamalarda, depolama ortamını yenilemek, kopyasını almak veya bir sistemden bir diğerine transfer etme durumlarında bu kaçınılmazdır. Genelde, uzun dönem korunacak belgeler için üç unsur bulunmaktadır: Yenileme, kopyalama ve transfer.

- Yenileme, bir ortamdan aynı tür bir başka ortama belgelerin kopyalanmasıdır; örneğin, 650 MB'lık bir CD'den diğerine belgeleri kopyalama. Belgelerin herhangi birinde değişim yoktur.
- Kopyalama, belgelerin bir ortamdan bir başkasına kopyalandığı veya yeniden biçimlendirildiğinde meydana gelir, belgelerin 650 MB'lık bir CD'den, kartuş bantlara transfer edilmesi bu duruma bir örnektir. Bu durumda, farklı depolama ortamlarında kayıtlı olan verilerden dolayı bir miktar değişim olabileceğinden, yeni ortamdaki belgelerin bir örneği ile eski ortamdaki eşleşen belgeler karşılaştırılarak bir değişikliğin olmadığı doğrulanmalıdır.
- Transfer (veya göç ettirme), dosya yönetim sisteminin tam bir değişimini öngörür, belgelerin bir yazılım/donanım platformundan bir diğerine taşınırken dosya formatlarındaki değişimi içerir. Her bir belgenin byte byte karşılaştırılması, verilerin bütünlüğünün korunması açısından gereklidir. Belgelerin kopyalanması ve transferi sadece içeriği taşımaya ihtiyaç duymaz aynı zamanda üst veri ve denetim izlerinin de taşınması gerekir. Her türlü bağlantı da korunmalı ve taşınmalıdır.

▪ Elektronik belge yönetim sistemi içerisinde bulunan verinin kaybolması önlenmelidir. Bunun için "bir kez yaz, birçok kez oku" teknolojilerinin kullanımına dikkat edilmelidir. Bunun yanında, acil durum ve iş sürekliliği planlamasına uygun olarak test prosedürleriyle birlikte yedeklemenin düzenli olarak yapılması gerekir. Yedeklenen unsurlar, saklama prosedürlerine uygun olarak değişik yerlerde saklanmalıdır. Sistemin büyüklüğü ve yeniden çalıştırılma zamanının kısa olması durumunda, gerçek zamanlı olarak sistemin aynısının başka bir yerde işletilmesi de sağlanabilir.

Belgenin İmha Edilmesine İlişkin Kontroller

▪ Elektronik belge yönetim sistemi, imha listelerindeki belgeler için, belirlenen yazılı prosedürler çerçevesinde yönetilen bir imha süreci sağlamalıdır. Bunun için oluşturulan görev tanımlarına göre belirlenen rol ve sorumluluklar çerçevesinde imha edilecek varlıklara kimlerin nasıl erişeceği ve hangi yöntemlerle imha işleminin gerçekleştirileceği belirlenmelidir. Bu nedenle önceden belirlenen ve yetkili üst yöneticilerin onayını almış bulunan saklama ve imha listelerine uygun olarak ve tüm imha sürecinin kayıt altına

alınmasını da sağlayacak şekilde işlemlerin yürütülmesi gerekir. Burada da, imha işlemini gerçekleştirecek ve imhayı gözetleyerek doğrulayacak iki ayrı personel tarafından imha sürecinin gerçekleştirilmesi sağlanmalıdır.

- İmha, depolama ortamının türüne bağlı olarak mantıksal veya fiziksel olabilir:
  - **Mantıksal imha**, silinemeyen depolama ortamlarına uygulanır (örn. BYBO diskler). Bütün üst verileri, indeks noktaları, denetim izleri ve temizlenen bağlantılar, silinebilir ortamlarda tutulan her şeyi temizlemeyi içerir. Temizleme sonrası depoda belgeler kalmasına rağmen, bütün imha edilenlerin işaretleri erişilemez kılınır.
  - **Fiziksel imha**, yeniden oluşturulmasına imkan vermeyecek bir şekilde depolama ortamından belgeyi kaldırmayı içerir. Prosedürlerin, belgelerin toptan imhasını sağlamak amacıyla, yedeklemeler de dahil olmak üzere manyetik ortamlarda meydana gelen üzerine yazma sayılarını belirlemeleri gerekir.
- Yetkisiz imha işlemlerinin önlenmesi için, en az ayrıcalık prensibine uygun olarak rollerin belirlenmesi ve tüm faaliyetlerin otomatik olarak denetim izlerinin tutulması, izlenmesi ve üst yönetime raporlanması gerekmektedir.
- İmha işlemlerinin doğru şekilde yerine getirilmesi için uygun yazılımların temin edilmesi ve kullanılmasına ilişkin eğitimlerin alınması da gerekli olacaktır. "bir kez yaz, birçok kez oku" teknolojileriyle oluşturulan unsurların fiziksel imhası için de gerekli prosedürlerin yazılı olarak oluşturulması, işlemlerin prosedürler çerçevesinde yerine getirilmesinin sağlanması için izlenmesi ve işlem sonrası gerekli düzenlemelerin yapılması sağlanmalıdır.

SONUÇ

Kamu kurumlarında bilişim teknolojilerinin yoğun şekilde kullanılması, e-devlet uygulamalarının yaygınlaşması ve bilişim ortamlarında oluşturulan, tutulan, saklanan ve iletilen belgelerin geçerliliğine ilişkin düzenlemelerin de (elektronik imza kanunu ve ilgili düzenlemeler gibi) yürürlüğe girmesi ile birlikte, elektronik belge yönetim sistemlerinin ülkemizde kurulumu ve geliştirilmesi çalışmalarına hız verilmiş bulunmaktadır.

Bu sistemleri yoğun şekilde kullanan kurumlar da, idari, yasal, mali ve diğer nedenlerle iş ve eylemleri sırasında aldıkları karar ve işlemlerin kanıtı olarak belge tutmak, saklamak ve gerektiğinde bunları ilgililere sunmak durumundadır. Özellikle bu kurumların denetiminin yürütülmesi sırasında, bu sistem yoluyla üretilen belgelerin geçerliliği konusunda güvence elde edilmesi de bir zorunluluktur. Bu nedenle elektronik ortamda tutulan, saklanan, paylaşılan ve imha edilen belgelerin güvenlik ve güvenilirliğinin sağlanması ve kanıt niteliğinin kaybolmaması için bu sistemlerin yeterli ve etkin şekilde yönetilmesi gerekmektedir.

Yargı yetkisiyle donatılmış Yüksek Denetim Kurumu olarak Sayıştay, bir taraftan kurumların elektronik belge yönetim sistemlerinde üretilen mali işlem ve kararlarını gösteren mali tablolar ve eklerinin güvenilir olup olmadığına ilişkin güvence verirken; diğer yandan, bu güvence üzerine elektronik ortamlarda bulunan ve denetim kanıtı olarak elde edilen belgeler üzerinde bulunan hukuka aykırılıklar hususunda (sorumlular tarafından imzalanmış veya mühürlenmiş kağıt belge gibi), ilgilileri hakkında hüküm tesis edecektir. Ancak bu iki işlemin de yapılabilmesi için elektronik belge yönetim sistemleri içerisinde tutulan, saklanan belge ve bilgilerin üzerinde herhangi bir değişiklik yapılmadığının, işlerin yerine getirilmesi sırasında üretildiğinin ve kurumsal işlemlerin kanıtı olabilecek geçerlilikte bulunduğunun belirlenmesi gerekmektedir. Bunun için de bu sistemlerin bilişim sistemleri açısından belirli kontrollerin varlığına yönelik incelemeler yapılmalı ve elde edilen bulgular çerçevesinde belgelerin geçerliliği onaylanmalıdır.

Uygulanmasında bir takım sıkıntılar bulunsa da, 5070 sayılı Elektronik İmza Kanununa ilişkin yapılan düzenlemeler, elektronik belge yönetimine ilişkin belirlenen standartların (TS 13298) bu sisteme yönelik çalışmalar yapan kamu kurum ve kuruluşlarında esas olması gerektiğine yönelik idari düzenlemeler (2008/16 sayılı Başbakanlık Genelgesi) ve e-devlet uygulamalarının yaygınlaştırılması için yapılması düşünülen çeşitli mevzuattaki (Ticaret Kanunu, Borçlar Kanunu, HUMUK gibi) değişikliklere yönelik Kanun Tasarıları dikkate alındığında, elektronik belge yönetimi sistemleriyle daha sık karşılaşılacağı açıktır. Bu nedenle denetim kurumlarının bu sistemlere özel ilgi göstermesi ve bunların yeterli ve etkin şekilde yönetilmesi konusunda örnek uygulamaları denetimlerinde dikkate almaları gerekmektedir.

YARARLANILAN KAYNAKLAR

Ahi, Gökhan (2004), "Türk Hukuku'nda Yeni Bir Boyut: Elektronik İmza Kanunu", http://www.e-imza.gen.tr/index.php?Page=KoseYazisi&YaziNo=16&YazarNo=19, (Erişim Tarihi: 24.08.2010).

California Records and Information Management (2002), "Electronic Records Management Handbook: State of California Records Management Program", Akt. Odabaş, Hüseyin, "Bilgi Kaynaklarının İşletiminde Elektronik Doküman Yönetimi ve Elektronik Belge Yönetimi Sistemlerinin Rolü", http://ab.Org.Tr/Ab09/Bildiri/11.doc, (Erişim Tarihi: 17.05.2010)

Cornwell (2001), Model Requirements for the Management Of Electronic Records, Moreq Specification, *Cornwell Management Consultants plc (formerly Cornwell Affiliates* plc), Mart 2001, http://www.cornwell.co.uk/moreqdocs/moreq.pdf, (Erişim Tarihi: 18.07.2010).

Day, Michael (2009), "Metadata", http://www.dcc.ac.uk/resources/curation-reference-manual/completed-chapters/metadata, UKOLN, University of Bath, (Erişim Tarihi: 15.04.2010).

Erturgut, Mine (2004), "Elektronik İmza Kanunu Bakımından E-belge ve E-imza", Bankacılar Dergisi, Sayı 48, Mart, http://www.tbb.org.tr/Dosyalar/Dergiler/Dokumanlar/48.pdf , Erişim Tarihi: 26.08.2010).

EUROSAI (2006a), Electronic Record Management, An Audit Briefing, (version 1,2), EUROSAI IT Working Group.

EUROSAI (2006b), Electronic Record Management, An Audit Guide, (version 0,8), EUROSAI IT Working Group.

NAA (2004), "Digital Recordkeeping, Guidelines for Creating, Managing and Preserving Digital Records", National Archive of Australia, http://www.naa.gov.au/Images/Digital-recordkeeping-guidelines_tcm2-920.pdf, Australia, (Erişim Tarihi: 15.06.2010).

Odabaş, Hüseyin (2008), "Elektronik Belge Düzenleme Yaklaşımları ve Türkiye'de E-Devlet Uygulamalarında Elektronik Belge Yönetimi", Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Cilt 12, Sayı 2.

TS 13298, Elektronik Belge Yönetimi, Türk Standartları Enstitüsü, Haziran, 2009.

Weber, R. (1999), "Information Systems Control and Audit", Akt. ASOSAI, IT Audit Guidelines, ASOSAI Research Project, Eylül, 2003.

5070 sayılı Elektronik İmza Kanunu, 2005.