BİLGİ MERKEZLERİNDE RİSK VE KRİZ YÖNETİMİ

Editörler

Alpaslan Hamdi KUZUCUOĞLU

Yasin ŞEŞEN

hiperyayın

Hiperyayın 722
Araştırma-İnceleme

Editörler
Alpaslan Hamdi KUZUCUOĞLU-Yasin ŞEŞEN

Genel Yayın Editörü
Hatice BAHTİYAR

Mizanpaj
Senem ILGIN

Kapak Tasarım
Kenan TEMİZEL

Yayıncı Sertifika No: 16680

ISBN: 978-625-7280-02-0
e- ISBN: 978-625-7280-03-7

1. Baskı: İstanbul, 2020

Bilgi merkezlerinde risk ve kriz yönetimi / ed. Alpaslan Hamdi Kuzucuoğlu, Yasin Şeşen. - İstanbul: Hiperyayın, 2020.
342 s.: fotoğ., tbl., şkl.; 21 cm. — (Hiperyayın; 722)
Kaynakça bölüm sonlarındadır.
ISBN: 978-625-7280-02-0 e-ISBN: 978-625-7280-03-7
1. Kütüphaneler—Risk yönetimi 2. Kütüphane binaları I. Eser adı II. Dizi
Z679.7.T87. B55 2020 025.82 BİL 2020

Baskı-Cilt: Yalın Yayıncılık-**Sertifika No:** 44154

GENEL SATIŞ PAZARLAMA VE YAYINEVİ
Hiperlink Eğt İlet. Yay. Gıda San. ve Paz. Tic. Ltd. Şti
Tozkoparan Mah. Haldun Taner Sok. Alparslan İş Merkezi
No: 27 Kat: 6 D: 21 Merter- Güngören / İstanbul
Telefon: 0212 293 07 05-06 Faks: 0212 293 56 58
www.hiperlink.com.tr / info@hiperlink.com.tr

İÇİNDEKİLER

2. BÖLÜM

KRİZ YÖNETİMİ

1.2. ELEKTRONİK ARŞİVLERDE DİJİTAL KORUMA VE BİLGİ GÜVENLİĞİ RİSK DEĞERLENDİRMESİ

Digital Preservation and Information Security Risk Assessment in Electronic Archives

Tolga ÇAKMAK

Doç. Dr., Hacettepe Üniversitesi Edebiyat Fakültesi, Bilgi ve Belge Yönetimi Bölümü, tcakmak@hacettepe.edu.tr, ORCID: 0000-0002-7700-6609

Şahika EROĞLU

Dr., Hacettepe Üniversitesi Edebiyat Fakültesi, Bilgi ve Belge Yönetimi Bölümü, sahikaeroglu@hacettepe.edu.tr, ORCID: 0000-0001-5724-1970

Giriş

Dijital dönüşüm, yetkili bir kurum olarak arşivlerin geleneksel sınırlarını değiştirmiş ve arşivler kendilerine emanet edilen belge ve verilerin korunmasında yeni zorluklarla karşılaşmışlardır. Hızla değişen kayıt tutma ortamında, tüm ilgili riskleri anlamak ve etkili bir şekilde yönetmek arşiv yönetiminin merkezinde yer almaktadır. Bu bağlamda modern bilgi teknolojileri ile dönüşen arşivlerde dijital arşiv sistemleri geliştirmek, bu sistemlerin güvenliğini ve güvenirliğini sağlamak önemli bir iş süreci olarak karşımıza çıkmıştır. Elbette arşiv yönetiminde güvenirlik ve güvenlik yeni bir kavram değildir fakat elektronik ortamın yoğun bir şekilde kullanımıyla konuya yönelik süreçlerin dijital ortamda kurgulanması ve işletilmesi gerekliliği ortaya çıkmıştır. Bu süreçlerden biri elektronik ortamda üretilen içeriklerin arşivlenmesidir. Tanım olarak değerlendirdiğimizde elektronik arşivleme elektronik biçimde ortaya çıkan veya kağıt biçiminden uygun şekilde dijitalleştirilmiş elektronik kayıtların korunmasını ifade eder. Klasik arşivleme tek seferlik bir eylemken, elektronik arşivleme sürekli bir süreci temsil eder ve belgenin oluşturulmasından imha edilmesine kadar tüm

belge yaşam döngüsüyle bağlantılıdır. Elektronik bir belge, arşivleme sürecine dahil olan herhangi bir sorumlu tarafından kolaylıkla manipüle edebilebilmektedir. Bu nedenle de elektronik belgelerin arşivleme dönemi boyunca bütünlüğünü ve özgünlüğünü korumak önem taşımaktadır. Elektronik arşivleme sürecinde gelen belgenin seçimi, sağlanması ve dijitalleştirilmesi, elektronik depolama, bütünlüğünün ve özgünlüğünün korunması ile erişim gibi aşamalar bulunmaktadır. Dijital nesnelerin elektronik belgeler olarak güvenilir bir şekilde korunması, elektronik kayıtlara dayalı iş yapan kuruluşların veya bireylerin hesap verebilirliğini sağlamada kritik bir unsurdur (Jerman Blažič, Klobučar ve Jerman, 2007).

Elektronik arşivlerde hem sistemin yapısal olarak hem de bu arşivlerdeki içeriğin güvenliğinin sağlanması sistemin kurumsal işleyişte aktif olarak kullanılmasında, sistem içeriğinin özgünlüğünde ve bu içeriğin kanıt olarak değer taşımasında etkili olmaktadır. Teknolojideki gelişmelerle birlikte elektronik ortamda oluşturulan içeriğin format ve depolandığı ortam olarak ömrünün değişkenlik göstermesi, eskimesi, tahribata uğraması bu içeriğe erişimin sürekliliğini sağlamak için önlemlerin alınmasını ve korunmasını gerektirmektedir. Konuyla ilgili literatür incelendiğinde dijital koruma kavramının elektronik ortamda oluşturulan ya da dijitalleştirme gibi uygulamalarla sonradan elektronik ortama aktarılan birçok bilgi kaynağı türünde olduğu gibi belgeler için de kullanıldığı görülmektedir (Cloonan ve Sanett, 2000; Siew Lin, Ramaiah ve Kuan Wal, 2003). Dijital koruma, elektronik sistemlerde belgelerin özgünlüğünün sağlanması üzerine gerçekleştirilen uluslararası bir araştırma projesi olan InterPARES projesi terminolojisinde de bulunduğu ortama bakılmaksızın, teknolojinin farklı evreleri sırasında dijital materyalleri korumaya yönelik olarak gerçekleştirilen bir süreç olarak tanımlanmaktadır (Pearce-Moses, 2018).

Genel olarak teknolojideki yenilikler çerçevesinde şekillenen

koruma süreçlerinde kurumların belgeler de dahil olmak üzere elektronik ortamda yapılandırdıkları sistemleri, geliştirdikleri içerikleri ve teknolojiyi takip etmeleri önem taşımaktadır. Nitekim literatürde kurumların elektronik ortamdaki varlıklarına yönelik uygulamaları açısından olgunluk düzeylerini belirlemeyi hedefleyen çalışmaların yayınlandığı görülmektedir (ARMA, 2013). Bunun yanı sıra koruma uygulamalarını bir risk yönetimi bileşeni olarak değerlendiren yaklaşımların da olduğu dikkati çekmektedir. Bu yaklaşım çerçevesinde koruma, bir kurumdaki belgelerin zaman içerisinde yok olmasına ya da zarar görmesine neden olabilecek herhangi bir tehditten korunması şeklinde de yorumlanmaktadır (Ismail ve Bullah Affandy, 2018). Dijital koruma uygulamaları değerlendirildiğinde ise konunun fiziksel koruma uygulamalarında da olduğu gibi risk yönetimi bağlamında ele alınan yönlerinin olduğu ve elektronik kaynaklarla ilgili risklerin çeşitlilik gösterdiği Dijital Koruma Koalisyonu (Digital Preservation Coalition) tarafından yayınlanan Dijital Koruma El Kitabı'nda (Digital Preservation Handbook) belirtilmektedir (Digital Preservation Coalition, 2015). Diğer yandan dijital koruma ile ilgili tehditlerin belirlenmesi çerçevesinde çeşitli risk değerlendirme araçları ve modelleri geliştirilmiştir (Digital Curation Center ve DigitalPreservationEurope, 2010; The Center for Research Libraries ve NARA Task Force on Digital Repository and Certification, 2007; Vermaaten, Lavoie ve Caplan, 2012). Söz konusu araç ve modeller kurumların elektronik ortamdaki varlıkları ile ilgili tehditleri belirlemekten başlayarak alınacak önlemler ve uygulanacak stratejiler konusunda yönlendirici bir rol üstlenmektedir. Dijital koruma uygulamalarının risk yönetimi ile bağlantısından hareketle, bu süreçler daha geniş ve kurumsal ölçekte bir kurumun bilgi varlıkları ile ilgili riskleri gidermesine yönelik bilgi güvenliği uygulamaları kapsamında da ele alınabilmektedir. Nitekim, bilgi güvenliğinin bilgiye uygulanan teknolojinin riskleri de yarattığı için gerekli olduğu ve bu risklerin içerisinde bilginin bütünlüğünün kaybolması, yok olması ya da kullanımının mümkün olmaması gibi durumların yer aldığı belirtilmektedir (Blakley, McDermott ve Geer, 2001). Bu ifadenin genel

olarak bilgi güvenliği, risk yönetimi ve dijital koruma arasındaki bağlantıyı ortaya koyduğunu söylemek mümkündür.

Elektronik arşivlerde kayıt altına alınan belgelerin ve diğer içeriklerin erişilebilirliğinin güvenirliğinin sağlanması bu içeriklerin kanıt niteliği taşıması ve yeniden kullanılabilirliği açısından değerlidir. Söz konusu belge ve içeriklerin güvenirliğinin sağlanmasında kullanılan çeşitli koruma ve güvenlik süreçleri bulunmaktadır. Bu çerçevede ilgili koruma ve güvenlik stratejileri uygulamalarında izlenen strateji ve yaklaşımlar ise hizmet sunumunun sürekliliği açısından önem taşımaktadır. Bu doğrultuda çalışmada elektronik belge ve arşiv sistemlerinde koruma uygulamaları çerçevesinde kurumsal farkındalığın ve olgunlaşmanın önemi vurgulanmaktadır. Bununla birlikte bilgi güvenliği, risk yönetimi ve dijital koruma kavramları arasındaki bağlantıdan hareketle elektronik belge ve arşiv sistemlerinde dijital korumaya yönelik risklerin literatür bağlamında açıklanması, uygulanabilecek stratejilerin betimlenmesi ve risk yönetiminde kullanılabilecek araçların tanıtılması amaçlanmıştır. Belirtilen amaç doğrultusunda elektronik belge ve arşiv sistemlerinde koruma konusu öncelikli olarak ele alınmıştır. Bu konuyu söz konusu sistemlerdeki stratejiler ve riskler takip etmiştir. Çalışmada ayrıca bu sistemlerde risk değerlendirmesi ve risk değerlendirme araçları anlatılarak konuya yönelik sonuç ve değerlendirmelere yer verilmiştir.

1. Elektronik Belge ve Arşiv Sistemlerinde Koruma

Günümüzde kurumsal işleyişin büyük bir bölümü bilgi sistemleri aracılığıyla elektronik ortam üzerinden gerçekleştirilmektedir. Kurumların gerek kendi içlerindeki iletişim gerekse diğer paydaşlarıyla olan iletişimi elektronik ortam üzerinden yürütülmekte, bu ortamda oluşturulan saklama alanlarında depolanmakta ve kayıt altına alınmaktadır. Bu ortamda kayıt altına alınan ve saklanan bilgi ve belgelerin yeniden kullanımında, istendiğinde zamandan ve mekândan bağımsız olarak erişilebilirliğinin sağlanmasında

elektronik arşivlerin önemli bir rolü bulunmaktadır. Elektronik arşivler sonradan dijitalleştirilmiş içerikler veya doğrudan dijital ortamda oluşturulmuş içerikleri kapsamaktadır. 1990'lardan itibaren arşiv biliminde yerini alan elektronik arşivlerin düzenlenmesi, işletilmesi, saklanması ve korunmasına yönelik bir çok kurallar dizini oluşturulmuştur. Özellikle internetin ve ağ ortamının da gelişmesiyle birlikte elektronik arşivler, kanıt niteliği de taşıyan, ayırt edici nitelikleri sunan ve elektronik belgelerin yönetiminde kullanılan platformlar olarak nitelendirilmektedir (Hedstrom, 1995). Bununla birlikte Uluslararası Arşivler Konseyinin (International Council on Archives - ICA) elektronik belge tanımında kullandığı unsurlarının elektronik arşiv sistemlerinin genel özellikleri hakkında fikir verici olduğunu söylemek mümkündür. ICA'nın yayımlamış olduğu rehberde yer alan elektronik belge tanımında manipüle edilebilirlik, taşınabilirlik ve işlenebilirlik özellikleri bulunmaktadır (International Council on Archives, 1997, s. 22). Dolayısıyla elektronik arşiv sistemlerinin de bu özellikleri taşıyabileceklerini söylemek mümkündür. Bir diğer tanımda ise elektronik belgeler, bu belgelerin kuruluşlar veya kişiler tarafından oluşturulan, alınan veya yönetilen ve faaliyetlerin kanıtı olarak saklanan elektronik dosya ve elektronik ortamlarda bulunan bilgiler olarak tanımlanmaktadır (Sutanto ve Nuryani, 2020, s. 83). Bu noktada elektronik ortamda oluşturulan belge ve içeriklerden oluşan elektronik arşivlerde çeşitli zorluklarla da karşılaşılabilemektedir. Hedstrom (1995) çalışmasında elektronik arşivlerde yaşanan en büyük zorluklardan birinin belgelerin güvenilirlik, özgünlük ve fayda sağlamaya dönük niteliklerinin korunması olduğunu belirtmektedir. The Commission on Preservation and Access and Research Libraries Group tarafından yayımlanan bir raporda da dijital (elektronik) arşivlerin bir ulusun dijital ortamda bulunan sosyal, ekonomik, kültürel ve ekonomik mirasının uzun süreli olarak erişiminin ve bütünlüğünün sağlanmasından sorumlu oldukları ifade edilmektedir (Task Force on Archiving of Digital Information, Commission on Preservation and Access ve Research Libraries Group, 1996, s. iii). Elektronik arşivlerle ilgili

olarak yukarıda verilen açıklamalardan bu arşivlerin sundukları içeriklerin bütünlüğünü ve güvenliğini sağlama ile korumaya yönelik amaçlarının ön plana çıktığını söylemek mümkündür. Bu kapsamda konunun elektronik belge yönetimiyle de yakınlaştığı dikkat çekmekle birlikte elektronik belgelerin sistemlerde güvenilir bir şekilde yaşatımının sağlanması gerektiği vurgulanmaktadır. Elektronik belgelerin depolandığıı sistemler olan belge koruma sistemlerinin güvenilirliğinin ve yapısının yasal ve yönetimsel gereklilikleri karşılayacak bir nitelikte olması beklenmektedir (Brown University Archives, t.y.).

Güven kavramı her zaman arşivlerin (elektronik veya fiziki) merkezi olmuştur. Bununla birlikte, belgelerin ve arşivlerin hızlı gelişimi güven kavramını daha da öne çıkarmakla birlikte birçok arşiv çalışmasının da temelinde bu kavramın sıklıkla kullanıldığı bilinmektedir. Kavram elektronik arşivler bağlamında incelendiğinde ise konunun arşivlerin elde ettikleri, korudukları, bağlamsallaştırdıkları veya sundukları dijital içeriklere verdikleri meşruiyeti nasıl korudukları odağında geliştiği anlaşılmaktadır. Bu bağlamda karşılaşılabilecek risklerin tespiti elektronik arşivlerin ve elektronik belgeleri içerik unsuru olarak kullanan sistemlerin güvenilirliğinin sürekliliği açısından önem taşımaktadır. Elektronik belgelerle ilgili risklerin belge yaşam döngüsünün hemen her aşamasında (elde etme, yaşatım, sisteme dahil etme, erişim, ayıklama ve koruma gibi) oluşabildiği dile getirilmektedir (Bearman, 2006). Bununla birlikte belgelere yönelik güvenin sağlanması, gelişime yönelik amaçlara ulaşmada kritik bir altyapı sağlayan belge sistemlerinde farklı bağlamlarda ihtiyaç duyulan bir gerekliliktir (Lemieux, 2016). Lemieux (2016) ayrıca sistemlere güvenin (trustworthiness) literatürde birbiriyle bağlantılı iki kavram olan güvenilirlik ve özgünlük ile bütünlük, kimlik ve provenans kavramları bağlamında tartışıldığını ifade etmektedir. Diğer taraftan Association of Records Managers and Administrators (ARMA, Belge Yöneticileri Derneği) genel olarak kabul edilen belge koruma ilkelerini aşağıdaki gibi belirlemiştir (ARMA, 2017):

- Hesap verilebilirlik
- Şeffaflık
- Bütünlük
- Koruma
- Uyumluluk
- Elde edilebilirlik
- Ayıklama
- İmha.

Belge koruma dijital ortamdaki belgeler de dahil olmak üzere birçok işlemden oluşmaktadır. Dijital belgelerin korunmasına yönelik uygulamalar kurumların stratejik ve işletimsel amaçlarına, önceliklerine, gelişimsel hedeflerine ulaşmalarına, bilginin temel bir kaynak olarak yönetilmesine, hesap verilebilirlikle ilgili yaptırımlar ile bilgi edinme özgürlüğü, açık devlet, açık veri gibi konulardaki gerekliliklerin yerine getirilmesine olanak sağlamaktadır. Bu doğrultuda ICA, dijital belge korumayı Dijital Koruma Koalisyonunun da tanımından hareketle dijital kayıtlara ihtiyaç duyulduğu sürece sürekli erişim sağlamak için gerekli olan ve yönetilen faaliyetler dizisi şeklinde tanımlamaktadır (International Council on Archives, 2016, s. 13).

ARMA tarafından belirlenen ilkeler genel olarak değerlendirildiğinde elektronik belge koruma sistemlerinin belgeleri depolamanın yanı sıra hem işlev olarak hem de süreçlere yönelik özelliklerine değinildiği görülmektedir. Bununla birlikte bu ilkelere yönelik olarak beş farklı düzeyi içeren bir olgunlaşma modeli yayınlayan ARMA, söz konusu ilkeler arasında yer alan koruma ilkesi ile ilgili olarak özel, ayrıcalıklı, gizli, sınıflandırılmış olan, iş süreçlerini devam ettirmek ya da başka bir nedenle koruma gerektiren belgelere makul düzeyde koruma sağlamak için bir bilgi yönetişim programının oluşturulmasına işaret etmektedir. Bu programa yönelik uygulamaların da kurumların olgunluk düzeylerine göre farklılık gösterdiği ve kurumların belge koruma uygulamalarına yönelik beş düzeyin bulunduğu görülmektedir. Bunlar (ARMA, 2013);

Birinci düzey (alt standart - sub-standard): Bu düzeyde bilginin korunmasına yönelik önem düzeyi çok düşüktür. Belgeler rastgele bir düzende saklanırken, erişim denetimi ve yetkilendirmeler çeşitli gruplar ve bölümler tarafından gerçekleştirilir. Merkezi bir erişim yönetimi uygulaması yoktur. Kontroller bilgiyi veya belgeyi üretenler tarafından gerçekleştirilir.

İkinci düzey (geliştirme - in development): Bilgi varlıklarına ilişkin bazı koruma uygulamaları gerçekleştirilir. Personel kayıtları gibi belirli bir düzeyde koruma gerektiren belge ve bilgilere yönelik yazılı bir politika vardır. Ancak bu politika bütün ortam türlerindeki bilgiler için yönlendirmeleri içermemektedir. Çalışanlar için rehberlik düzeyi değişkenlik göstermektedir ve sistemlere yönelik bir personel eğitimi gerçekleştirilmemiştir. Politika kurum içi ve dışı paydaşlarla bilgi değişiminin nasıl yapılacağını göstermemektedir. Erişim denetimi de bireysel içerik sahipleri tarafından gerçekleştirilmektedir.

Üçüncü düzey (temel - essential): Bu düzeydeki bir kurumda belge yöneticisi rolü tanımlanmıştır. Belge yöneticisi kurumun bütününde yürütülen belge yönetimi programının işletiminden sorumludur. Kurum elektronik belgeleri mevcut belge yönetim programının bir parçası olarak değerlendirir. Belge yöneticisi aktif olarak kurumdaki diğer yetkililerle birlikte stratejik bilgi ve belge yönetimi girişimlerinin içerisinde bulunur. Üst yönetimi belge yönetimi programına yönelik bir farkındalıkla hareket eder. Kurumda bilgi odaklı süreçlerin yönetimine dönük geniş kapsamlı bir bilgi yönetişim programının yapılandırılması görüşü hakimdir. Bu düzeydeki bir kurumda ayrıca hesap verilebilirlik ile ilgili spesifik amaçların olduğu görülmektedir.

Dördüncü düzey (proaktif - proactive): Bu aşamada kurum bir bilgi yönetişim profesyoneline sahiptir. Belge yöneticisi de bilgi yönetişim programının bir parçası olan belge yönetim programının stratejik ve uygulamaya dönük bütün yönlerinden sorumlu bir üst yönetici rolündedir. Bu düzeyde bütün işlevsel alanları kapsa-

yan ve paydaşlara yönelik olarak oluşturulan bir komisyon belge yönetimi ile ilgili konuları ve imha politikasını periyodik olarak değerlendirmek üzere toplantılar yapar.

Beşinci düzey (dönüşümsel - transformational): Olgunlaşma modelinin koruma prensibi ile ilgili son düzeyi olan bu düzeyde kurumun üst yönetimi ve yönetim kurulu bilgi yönetişim programına büyük önem gösterir. Belge yöneticisi belge yönetim programını yöneterek üst yönetime raporlama yapar. Bilgi yönetişim sorumlusu ve belge yöneticisi kurumun yönetim kademesinin temel üyeleri rolündedir. Kurumun hesap verilebilirlikle ilgili ilk amaçları karşılanmıştır ve kurum hesap verilebilirlik amaçlarına yönelik rutin olarak değerlendirilen ve gözden geçirilen süreçlere sahiptir.

Yukarıda belirtilen aşamalardan hareketle elektronik belge ve belge koruma sistemlerine yönelik prensiplerden biri olan koruma prensibi kapsamında kurumsal olgunlaşmanın ilk aşamalarında basit düzeylerde gerçekleştirilen ya da gerçekleştirilmesi adına bireysel veya kısa vadeli çözümlerin geliştirilmesi söz konusudur. Özellikle proaktif ve dönüşümsel süreçlere bakıldığında ise kurumun belge yönetimi uygulamalarının süreklilik ve sürdürülebilirliği ile ilgili adımların atıldığı dikkati çekmektedir. Bu düzeylerdeki kurumlarda elektronik belge yönetimi ve belge koruma uygulamalarının belirli dönemlerde gözden geçirilmesi ve güncellenmesi bu uygulamalara ilişkin koruma süreçlerinin değişkenlik göstereceğine işaret etmektedir. Bu doğrultuda kurumlardaki olgunlaşma düzeyiyle de bağlantılı olarak elektronik belge yönetimi ve belge koruma uygulamalarına yönelik risklerin periyodik olarak tespit edilmesi ve ilgili önlemlerin alınması bu uygulamaların sürekliliğini sağlamada etkili olmaktadır.

2. Elektronik Belge ve Arşiv Sistemlerinde Koruma Stratejileri ve Riskler

Bilginin elektronik ortamda oluşturulması, dağıtımı, kullanımı ve saklanması ile kurumsal işleyişte yoğun olarak kullanılan elektronik belgeler iş süreçlerinin hızlı bir şekilde gerçekleştirilmesinde etkili olmuştur. Diğer yandan elektronik ortamın sürekli olarak değişkenlik gösteren yapısı ve kullanılan formatlardaki değişiklikler de elektronik belgelerin uzun süreli olarak korunması ve erişilebilirliğinin sağlanmasına ilişkin ihtiyaçları ortaya çıkarmıştır. Literatürde birçok tanımı bulunan dijital koruma kavramsal olarak elektronik belgelerle de bağlantılı olarak kullanılabilmektedir. Bu doğrultuda konuyla ilgili bir çalışmada dijital koruma yeniden biçimlendirilmiş ya da dijital ortamda oluşturulmuş elektronik materyalleri zaman içerisinde erişilebilir, okunabilir ve kullanılabilir formlarda tutan ve koruyan süreçler ve etkinlikler olarak tanımlanmıştır (Cloonan ve Sanett, 2002, s. 95). ICA'nın Elektronik Belge Konseyi tarafından hazırlanan 1997 yılında yayımlamış olduğu ve elektronik belgelerin yönetimine dönük yönlendirmeleri içeren rehberde belirtilen ilkelerden dördüncüsünde arşivlerin elektronik belgelerin erişilebilir, elde edilebilir ve anlaşılabilir şekilde kalmasını sağlamak için koruma ve erişim gerekliliklerini belirlemelerine işaret etmektedir (International Council on Archives, 1997). Rehberdeki bu ilkeyi elektronik belgelerin teknolojideki gelişmelere bağlılığından kaynaklanabilecek sorunlara vurgu yapıldığını söylemek mümkündür. Rehber ayrıca elektronik belgelere yönelik koruma ve erişim uygulamalarının birbiriyle bağlantılı olduğunu ifade etmekte; elde edilebilirlik ile fiziksel olarak bozulmamışlığı, tanımlanmışlığı ve okunabilirliği, erişilebilirlik ile arama stratejileriyle seçilebilirliği, anlaşılabilirlik ile de tarihi değeri ve kanıt olarak kullanılabilmeyi öne çıkarmaktadır.

Elektronik belgelerin korunmasının literatürde özellikle 1990'lı yılların sonları ile 2000'li yılların başlarından itibaren tartışıldığını söylemek mümkündür. Bu kapsamda elektronik ortamda oluş-

turulan belgelerin erişilebilirliğinin sağlanması ve özgünlüğünün korunması ile ilgili stratejilerin geliştirildiği de görülmektedir. Bu stratejilerde beş uygulamanın öne çıktığı ifade edilmektedir. Bu uygulamalar (Siew Lin ve diğerleri, 2003).

- Belgelerin oluşturulduğu veya depolandığı teknolojinin korunması,
- Yeni platformlarda özgün teknolojinin öykünümünün oluşturulması,
- Belgelerin erişimi, dağıtımı ve kullanımı için gerekli yazılımın göç ettirilmesi,
- Belgerin güncel formatlara göç ettirilmesi,
- Belgelerin standart olarak kullanılan formatlara dönüştürülmesidir.

Birçok dijital koruma stratejisinde yer alan temel ilke materyalin en az zarar göreceği şekilde kalıcılığını sağlamaktır. Bunun nedeni de dijital bilginin uzun süreli korunmasına yönelik olarak deneyim eksikliği olarak değerlendirilebilir. Kurumlar bu noktada daha düşük düzeydeki koruma tekniklerini tercih edebilmekte; koruma tekniğinin uygulanışından kaynaklı hasarların da önüne geçebilmektedir (Waugh, Wilkinson, Hills ve Dell'oro, 2000). Literatürde ayrıca aşağıdaki adımların da koruma sürecinde uygulanabileceği önerilmektedir (Hunter ve Choudhury, 2003):

- Çoklu ortama yönelik nesneleri mümkün olduğunca yüksek kalitede, standardize edilmiş ve platformdan bağımsız formatlarda saklanması ve basit işaretleme dillerinde tüm nesnenin yapılandırılması,
- Nesneyi yorumlamak ve görüntülemek için tanımlayıcı, yönetimsel, yapısal ve teknik üstverilerin yeterli düzeyde kayıt altına alınması,
- Platform bağımsız bir formatta ve üstverileri hazırlanmış olan dijital nesnenin tam bir koruma paketinde bulunması için METS standardının kullanılması,
- Teknik ve yazılım gereklilikleri çerçevesinde bağlantıların güncellenmesi,
- Yalnızca talep doğrultusunda formatlarının yenilenmesi ya da bir değerden dolayı göç ettirilmesi gereken nesnelere bu işlemlerin uygulanması.

Bunun yanı sıra kurumlarda belgelerin korunması ile ilgili bir maliyet modelinin ve koruma politikasının oluşturulması da önemlidir (Cloonan ve Sanett, 2000). Elektronik belgelerin uzun süreli olarak erişilebilirliğinin sağlanması bu belgelere yönelik koruma uygulamalarının planlanması ve kurumsal stratejilerin oluşturulması açısından önem taşımaktadır. Konuyla ilgili bir çalışmada da literatürden hareketle elektronik belgelere yönelik dijital koruma stratejilerinin başlangıç ve uygulamaya yönelik adımlardan oluştuğu belirtilmiştir (Ismail ve Bullah Affandy, 2018). Bu adımlardan başlangıç aşamasında politika geliştirme, maliyet modellemesi, personel düzenlemeleri, işbirlikleri ve paydaşlar bulunmaktadır. Stratejinin uygulama aşamasında ise göç, öykünme, dijital arkeoloji, teknoloji koruması ve yenileme (refreshing) gibi koruma teknikleri yer almaktadır. Çalışmada ayrıca bu iki aşamanın teknolojik, organizasyonel ve yasal koşullar çerçevesinde şekillendiği savunulmaktadır.

Dijital koruma kurumlarda hemen her tür dijital nesnenin kalıcılığı açısından önem taşırken bu uygulamaların gerçekleştirilme sürecinde birçok sorunla karşılaşılabilmektedir. Bu doğrultuda karşılaşılan sorunların teknoloji eskimesi, farkındalık eksikliği, finansal sürdürülebilirlik, politika, yasal düzenleme, güvenlik ve mahremiyet konularında olduğu belirtilmektedir (Adu ve Ngulube, 2017). Bunun yanı sıra ICA'nın 2016 yılında yayımlamış olduğu bir eğitim dokümanında da dijital ortamdaki kayıt ve belgelere yönelik olarak şu sorunlarla karşılaşıldığı belirtilmektedir (International Council on Archives, 2016):

Medya Kırılganlığı (media fragilty): Dijital bilginin kaydedildiği ortamın (örneğin CD, DVD gibi) belirli bir süre sonra kullanılamaz hale gelmesi, bu ortama yönelik çevresel saklama koşullarının yetersizliği, kullanıma yönelik teknolojinin eksikliği ve dijital bilginin kayıt altına alındığı ortamın kalitesinin düşüklüğü gibi sorunlar

Yazılım ve Donanım Eskimesi (Software and Hardware Obsolescence): Bilgisayar donanımın ya da kayıt altına alınacak ortamın eskimesi

ile işletim sisteminin (sistem yazılımının), uygulama yazılımının ve kayıt formatlarının güncelliğini kaybetmesine ilişkin sorunlar

Üstveri Yetersizliği: Dijital kayıt ya da belgeye ilişkin bilgiyi bulamama, bilgiyi işleyememe ya da okuyamama, dijital bilginin anlamının ya da değerinin kaybolması ve bilginin veya belgenin özgünlüğünün doğrulanamaması ile ilgili sorunlar

Zayıf Hesap Verebilirlik: Kurumlarda dijital kayıt ve belgelerin bütünlüğünün sağlanmasından sorumlu birim ve kişilerin belirlenmemiş olması, birimlerin ya da kişilerin bu konuyla ilgili olarak kime ya da nereye raporlama yapacaklarına ilişkin süreçlerin tanımlanmamış olmasıyla bağlantılı sorunlar

Farkındalık: Kurum çalışanlarının ve yöneticilerin dijital ortamdaki bilgi ve belgelere yönelik tehditler ile dijital koruma işlemleri ile ilgili kavramlar konusundaki bilgi ve farkındalık eksiklikleri

Zayıf Mevzuat ve Politika: Dijital koruma işlemlerine yönelik politika oluşturmama, oluşturulan politikaların yetersizliği ya da mevzuat ile ilgili yetersizlikler

Riskleri Stratejik Olarak Değerlendirmeme: Dijital kayıtlara ya da belgelere yönelik olarak karşılaşılabilecek riskleri bütünleşik olarak değerlendirilmemesi, bir riski giderirken diğer alanlarda karşılaşılacak risklerin değerlendirilmemesi.

Yukarıda belirtilen çalışmalarda değinilen sorunların birbirine yakın olduğu görülürken bir yandan konunun dijital nesnenin kayıt altına alındığı ortama ve formata bir yandan da tanımlama, yönetim ve insan faktörüne ilişkin risklerin oluşabileceği anlaşılmaktadır. Ayrıca dijital kayıt ve belgelerle ilgili mahremiyet boyutunda da risklerin oluşabileceği de dikkat çekmektedir. Bu çerçevede bir kurumun dijital kayıtları ya da belgeleri iyi yönetildiğinde hesap verilebilirlik, yasal düzenleme ve politika uyumluluğu, kaynak yönetimi, hizmet sunumu, denetim, bilgiye erişim, bilgi güvenliği ve gizlilik konularını destekleyici stratejik bir varlık haline

gelmektedir. Kötü bir yönetim sergilendiğinde ise dijital kayıtlar ve belgeler eksik bir durumda olmakla birlikte, bulunması zor ya da doğrulanamamakta ve kolayca manipüle edilebilmekte, silinebilmekte, bozulabilmekte ya da kaybolabilmektedir.

Digital Preservation Europe tarafından yayımlanan araştırma yol haritasında dijital koruma aynı zamanda bir risk yönetimi problemi olarak da değerlendirilmekte; dijital korumaya yönelik belirsizliklerin ölçülebilir değişkenlerle tespit edilmesine ve buna yönelik araçlara ihtiyaç duyulduğu belirtilmektedir (Digital Preservation Europe (DPE), 2007, s. 26). Diğer taraftan Dijital Koruma Koalisyonu (Digital Preservation Coalition) tarafından yayımlanan Dijital Koruma El Kitabında dijital korumanın sadece risklerle ilgili olmadığı aynı zamanda dijital nesnelerden değer üretimine katkı sağlamaya yönelik süreçler olduğu dile getirilmektedir (Digital Preservation Coalition, 2015).

Risk yönetimi kapsamında yapılan bir çalışmada da dijital koruma ile ilgili karşılaşılabilecek tehditler ve oluşabilecek güvenlik açıkları şu şekilde sınıflanmıştır (Barateiro, Antunes, Freitas ve Borbinha, 2010).

Tablo 1. Dijital korumaya yönelik güvenlik açıklarının ve tehditlerinin sınıflandırılması (Barateiro ve diğerleri, 2010, s. 9)

Güvenlik açıkları	Süreç	Yazılım hataları
		Yazılım eskimesi
	Veri	Ortam hataları
		Ortam eskimesi
	Altyapı	Donanım hataları
		Donanım eskimesi
		İletişim hataları
		Ağ servisi yetersizlikleri
Tehditler	Felaketler	Doğal felaketler
		İnsan işlemlerinden kaynaklı hatalar
	Saldırılar	İç saldırılar
		Dış saldırılar
	Yönetim	Ekonomik yetersizlikler
		Kurumsal yetersizlikler
	Yasal düzenleme	Yasal değişiklikler
		Yasal yükümlülükler

Tablo 1'de yer alan sınıflamadan da hareketle dijital kaynakların yönetiminde karşılaşılan risklerin çeşitlilik gösterdiğini söylemek mümkündür. Bu risklerin bazıları aşağıda sıralanmaktadır (Digital Preservation Coalition, 2015):

- Kurumlar arasında işlevlerin aktarımı, birleştirilmesi ya da yakınlaştırılması
- Kurumda stratejik eğilimlerin ya da bütçe ve işlevlerdeki değişiklikler
- Bireysel lider ya da uzmanlardaki büyük değişiklikler
- Gelecekteki koruma ihtiyaçları dikkate alınmadan dış kaynak kullanımı
- Dosya formatının eskimesi bu nedenle verileri işlemenin mali-

yetli veya imkânsız hale gelmesi
- Medyanın eskimesi, bu nedenle verilerin kurtarılmasını maliyetli veya imkânsız hale gelmesi
- Ortam bozulması, bu nedenle verilerin hasar görmesi veya değişmesi
- Anlam kaybıyla sonuçlanan bağlamsal bilgi kaybı
- Haklar ve yükümlülükler üzerinde belirsizliğe neden olan telif hakkı veya diğer yasal bilgilerin kaybı
- Orijinallik kaybıyla sonuçlanan bir belge hakkında kaynak bilgisinin veya sabitliğin kaybı
- Bağlamsal bilgi kaybı
- Bir belgenin yetkili örneklerini tanımlamayı zorlaştıran sürüm kontrolünün bozulması
- Yanlışlıkla silinmeye yol açan insan hatası
- Binaları veya altyapıyı etkileyen doğal afetler.

Sıralanan risklere ek olarak 2020 yılında T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yayımlanan Bilgi ve İletişim Güvenliği Rehberi'nde dijital kayıt tutulan sistemlerde depolama alanlarının doluluk oranlarının izlenmesine yönelik bir öneri bulunmaktadır. Bu öneriden hareketle depolama alanının doluluğunun da bir risk olarak yorumlamak mümkündür (Türkiye Cumhuriyeti Cumhurbaşkanlığı, Dijital Dönüşüm Ofisi, 2020).

Risk yönetiminin dijital koruma stratejisinin temel boyutlarından biri olduğunu ifade eden bir diğer çalışmada dijital koruma uygulamalarında görev alacak personelin dijital içeriğin oluşturulması aşamasından itibaren sürecin içerisinde yer alması, açık ve iyi dokümante edilmiş standartların ve sistemlerin yapılandırılması, iyi bilgilendirilmiş kararların verilmesi ve bu kararların kayıt altına alınması, kabul görmüş üstveri şemalarının kullanılması, başarı kriterlerinin ve sonlandırma süreçlerinin planlanmasının dijital koruma stratejilerinde bulunması gerektiği vurgulanmıştır (Corrado ve Sandy, 2017).

3. Elektronik Belge ve Arşiv Sistemlerinde Risk Değerlendirmesi ve Risk Değerlendirmesi Süreçlerine Yönelik Standart ve Araçlar

Elektronik belge ve arşiv sistemleri fiziksel arşivlerle kıyaslandığında erişim ve kullanıma yönelik avantajlarının olduğunu söylemek mümkündür. Ancak avantajlar beraberinde bir takım zorlukları da getirebilmektedir. Söz konusu zorluklardan biri içeriklerin güvenirliğini, özgünlüğünü ve erişilebilirliğini yalnızca yasal anlamda değil aynı zamanda ağ ortamında da koruyarak kanıt niteliklerini belirleyen özelliklerin korunmasını sağlamaktır. Bu çerçevede elektronik belge ve arşiv sistemlerinde bilgi güvenliği uygulamaları önem kazanmaktadır. Herhangi bir önlem alınmamış sistemler saldırılara karşı savunmasız kalmaktadır. Bu noktada bilgi güvenliği uygulamaları yönetilen içeriğin kalıcı güvenliğini sağlamaya yönelik uygulamaları barındırmaktadır. Bilgi güvenliği riskleri ise, güvenlik olaylarının olasılıkları ve etkileri anlamına gelmektedir. Dolayısıyla riskler, güvenlik olaylarının olasılıkları ve etkilerinden oluşan iki endeksle ölçülmektedir. Bilgi güvenliği, bir bilgi güvenliği politikasının oluşturulmasına yönelik ve güvenlik risk yönetimine dayalı olması gereken bir süreçtir. En uygun bilgi güvenliği politikası ise, optimize edilmiş bir karşı önlem olarak tanımlanmaktadır (Wangen, Hallstensen ve Snekkenes, 2018). Bilgi güvenliği ve risk yönetimi, güvenlik risklerini azaltmak için devam eden bir süreç olarak görülebilir, burada nihai amaç genellikle güvenlik risklerini kabul edilebilir bir düzeye düşürmektir (Wang ve Xiang, 2008). Bu çerçevede ilgili sistemleri güvenli hale getirmenin temeli riskleri önceden belirlemek, saldırıların verimli bir şekilde analizi ve sistem güvenlik açıklarının objektif bir şekilde analizine dayanmaktadır (Ionita, 2013). Bu bağlamda dijital sistemlerde karşılaşılabilecek risklerin değerlendirilmesi önem kazanmaktadır.

Bilgi güvenliği risk değerlendirmesi kurumun değerli bilgi varlıklarına yönelik potansiyel riskleri ve bunları ele alacak araçları anlamasını sağlayan sürekli bir süreçtir. Bu süreç risk yönetimi

teorilerine dayanır, internetten gelebilecek olası saldırıları sistematik olarak analiz eder ve bilimsel yöntemlerle bilgi sisteminin zafiyetini değerlendirir. Böylelikle, güvenlikle ilgili bir olay (hacklenme, sızdırma gibi) meydana geldiğinde bunların kötü etkilerinin seviyeleri bilinmekte ve risklere karşı bazı koruyucu ve iyileştirici önlemler alınabilmektedir. Bir diğer ifadeyle güvenlik açığı meydana gelmeden farkedilemeyen açıkların ve tehditlerin olabileceği de göz önünde bulundurulmalıdır. Bunun yanı sıra ağların ve bilgi güvenliği sistemlerinin korunmasını en üst düzeye çıkarmak için bilimsel bir temel sağlamak amacıyla riskleri kabul edilebilir bir düzeye indirilebilmektedir (Blakley ve diğerleri, 2001; Hulitt ve Vaughn, 2010; Saleh, Refai ve Mashhour, 2011).

Risk değerlendirmesinin amacı, risk seviyesiyle eşleşen koruma politikası ve önlemleri geliştirmeye rehberlik edilmesidir. Bilgi güvenliği risk değerlendirmesi, tüm güvence sisteminin temel ve önemli bir parçasıdır ve bilgi sistemi tasarımı, uygulaması, bakımı ve kullanılması gibi tüm süreç boyunca kullanılması beklenmektedir (Wangen ve diğerleri, 2018). Risk değerlendirmenin en temel aşaması sistem güvenlik açıklarının açıkça tanımlanması olarak belirtilmektedir. Sistem güvenlik açıkları ise sistem yeteneğini azaltan ve sınırlayan hata veya zayıflık olarak tanımlanmaktadır (Stoneburner, Goguen ve Feringa, 2002). Risk değerlendirme, amacı ve kapsamına bağlı olarak üç türe ayrılmaktadır. Bunlar:

Yüksek düzey değerlendirme: Uygulama öncesinde güvenlik risklerini belirlemek için tasarım aşamasında sistem için uygulanabilen değerlendirmedir.

Kapsamlı değerlendirme: Mevcut bir sistemde iyileştirme tavsiyesi sağlamak için güvenlik riskini değerlendirmek için kullanılabilen değerlendirmedir.

Uygulama öncesi değerlendirme: Yeni bilgi sistemi yayınlanmadan önce veya büyük bir işlevsel değişiklik olduktan sonra yapılan sistem sunulmadan önce yapılan değerlendirmedir (Bajpai, Sachdeva ve Gupta, 2010).

The National Archives tarafından yayımlanan "Risk Assessment Handbook" çalışmasında risk değerlendirme dijital süreklilik bağlamında irdelenmiştir. Buna göre dijital süreklilik "bilgilerinizi ihtiyaç duyduğunuz şekilde, ihtiyaç duyduğunuz sürece kullanma yeteneği" olarak tanımlanırken dijital süreklilik için riskleri değerlendirmenin iş yapmak için gerekli olan bilgileri korumada önemli olduğu vurgulanmaktadır (The National Archives, 2017, s. 5). Bunun yanı sıra iş süreçlerinde şeffaf, hesap verebilir, yasal ve verimli bir şekilde çalışmayı sağladığı, kurum itibarının korunmasına destek sağladığı, bilinçli kararların alınmasına, maliyetlerin azaltılmasına ve daha iyi kamu hizmetlerinin sunulmasına yardımcı olduğu belirtilmektedir. Yine aynı kaynağa göre dijital süreklilik bağlamında risk değerlendirmesi çerçevesi belirlenmiştir. Buna göre elektronik arşiv ve belge sistemlerinde risk değerlendirmesi sürecinde yer alan aşamalar şu şekilde sıralanmıştır (The National Archives, 2017, s. 9):

- Dijital sürekliliğe yönelik riskleri yönetmek için rollerin ve sorumlulukların belirlenmesi
- Süreç için hedefler ve başarı kriterlerinin tanımlanması
- Risk değerlendirmelerinin kapsamının tanımlanması
- Risklerin nasıl tanımlanacağı, analiz edileceği, kontrol edileceği, kaydedileceği, izleneceği sürecininin tanımlanması ve incelenmesi
- Bu süreçler için güvence ve süreklilik sağlanması.

Genel olarak değerlendirildiğinde risk değerlendirme sürecinin öncelikle iyi bir süreç yönetimi planlaması ile başladığı ve her bir ayrıntının doğru politikalarla önceden netleştirilmesi gerekliliği anlaşılmaktadır. Bu çerçevede elektronik belge ve arşiv sistemlerine yönelik risk değerlendirme süreçlerinde birçok kurum ve oluşumun risk değerlendirme süreçlerine yönelik metodolojiler ve araçlar geliştirdiği bilinmektedir. Bu çerçevede karşımıza çıkan standartlardan biri ISO/IEC 27001:2013 Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri - Gereksinim-

ler (Information technology-Security techniques - Information security management systems - Requirements) başlığını taşıyan standarttır. Bu standart, bir bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için gereksinimleri belirtmektedir. Gereksinimler geneldir ve tüm kuruluşlar için geçerli olması amaçlanmıştır (ISO, 2019).

Temel olarak kullanılabilecek bu uluslararası standartın dışında kütüphaneler, arşivler ve diğer kültürel kurumlardaki dijital koruma programlarından sorumlu olan veya olacak yöneticiler için The National Endowment for the Humanities ve Cornell Üniversitesi ortaklığında gerçekleştirilen çalıştayların çıktısı olan Dijital İçerik için Afete Hazırlık (Disaster Preparedness for Digital Content) çalışmasından bahsedilebilir. Önerilen dört belgeyi (afet planı politikası, iletişim planı, eğitim planı, roller ve sorumluluklar) birbirine bağlayan bir Dijital Koruma Yönetimi çalıştayı web sayfası olan çalışmada kümülatif olarak kapsamlı belgelere yer verilemekte ve afete hazırlık için mevcut uygulamaları yansıtacak şekilde güncellemeler yapılmaktadır ("Disaster preparedness for digital content", 2016).

Birleşik Krallık Ulusal Arşivleri de konuya yönelik değerlendirme araçları üretmektedir. Bu kaynaklar değerlendirildiğinde dijital süreklilik kapsamında risk değerlendirmesi içeren iki öz değerlendirme aracının sunulduğu görülmektedir. Bu öz değerlendirme araçlarından biri risk değerlendirmesini üç bölüme ayırmaktadır: Bunlar; 1) dijital sürekliliği ve roller ile sorumlulukları anlama, 2) bilgi gereksinimleri ve teknik bağımlılıklar, 3) yönetimdir. Bilgi varlığı risk değerlendirme aracı ise herhangi bir belirli dijital bilgi varlığının sürekliliğine yönelik risklerin belirlenmesine yardımcı olan ve sürekliliğin halihazırda kaybolduğu yerleri tanımlanmasını sağlayan bir araç olarak sunulmuştur. Kaynakta bir dijital süreklilik eylem planının geliştirilmesine yardımcı olmak için sürekliliği koruma veya geri yükleme konusunda önerilerde bulunulmaktadır (The National Archives, 2017).

Risk değerlendirmesi sürecinde kullanılabilecek bir diğer araç Dijital Kürasyon Merkezi (Digital Curation Center-DCC) ve Av-

rupa Dijital Koruma Merkezi (DigitalPreservationEurope-DPE) tarafından geliştirilen DRAMBORA, Risk Değerlendirmesi Tabanlı Dijital Arşiv Değerlendirme Yönetimi Modeli (Dijital Repository Audit Method Based on Risk Assessment - DRAMBORA) aracıdır. DRAMBORA dijital depo risk değerlendirmesi için bir metodoloji ve bir araç seti sunmaktadır. Araç, arşivlerin değerlendirmeyi kurum içinde yürütmesini (öz değerlendirme) veya süreci dış kaynak olarak kullanmasını sağlamaktadır. DRAMBORA risk değerlendirme sürecini altı aşamada düzenlemektedir. Yetki ve rollerin tanımlanması, varlık tabanının kategorizasyonu, risklerin belirlenmesi, Risklerin olasılık ve potansiye etkisinin değerlendirilmesi gibi aşamalardan oluşmaktadır. DRAMBORA araçları, denetimin amacını ve kapsamını tanımlamadan arşivdeki riskleri belirlemeye ve ele almaya kadar denetim süreci boyunca kullanıcılara rehberlik etmektedir. DRAMBORA, olası sonuçlar açısından çerçevelenmiş, dijital havuzlara yönelik 80'den fazla potansiyel risk örneğinin bir listesini ssunmaktadır (Digital Curation Center ve DigitalPreservationEurope, 2010).

2007 yılında Uzay Veri Sistemleri Danışma Komitesi (CCSDS) ve OCLC'nin Araştırma Kütüphaneleri Grubu (RLG) ve Ulusal Arşivler ve Kayıtlar İdaresi (NARA) tarafından geliştirilen TRAC (Güvenilir Kurumsal Arşivler Denetim ve Belgelendirme Kriterleri ve Kontrol Listesi-Trustworthy Repositories Audit and Certification Criteria and Checklist) kurumsal bilgi depolarının güvenliği ve belgelerin uzun süreli korunmasına ilişkin değerlendirme kriterlerinden oluşmaktadır. TRAC, üç bölüm altında düzenlenmiştir. Bunlar; Organizasyonel Altyapı, Dijital Nesne Yönetimi ve Teknolojiler, Teknik Altyapı ve Güvenlik bölümleridir. TRAC Dijital arşivlerin denetimi, değerlendirilmesi ve potansiyel sertifikasyonu için araçlar sağlamakta ve denetim için gerekli dokümantasyon gereksinimlerini belirlemektedir. Bu çerçevede, sertifikasyon için süreci tanımlarken ve dijital depoların güvenirliğini ve sürdürülebilirliğini belirlemek için uygun metodolojileri oluşturmaktadır (The Center for Research Libraries ve NARA Task Force on Digital Repository and Certification, 2007).

Konuya yönelik kullanılabilecek bir diğer model SPOT (Basit Mülkiyet Odaklı Tehdit- Simple Property-Oriented Threat) modelidir. SPOT Dijital nesnelerin altı özelliğine (kullanılabilirlik, kimlik, kalıcılık, işlenebilirlik, anlaşılabilirlik ve özgünlük) yönelik tehditlere karşı korumaya odaklanan basit bir risk değerlendirmesi modeli sağlamaktadır. Model, tehditleri bu mülkler üzerindeki potansiyel etkileri açısından değerlendirmekte ve her biri için birkaç örnek sonuç sağlamaktadır (Vermaaten ve diğerleri, 2012).

Elektronik Belge ve Arşiv sistemlerinde risk değerlendirmesi genel olarak bilgi güvenliği uygulamalarına dayanan bir süreçtir. Bu bağlamda bu sistemlerde bilgi güvenliği ilkeleri çerçevesinde olası risklere karşı değerlendirme ve önlem alma süreçleri sürdürülebilir bir şekilde uygulanması önem kazanmaktadır. Bu noktada özellikle sunulan rehberlik kaynaklrı da değerlendirildiğinde risk değerlendirmesinin bir süreç yönetimi odağında geliştirilmesi gerekliliği, konuya yönelik öncelikle politikalar oluşturma, rollerin ve sorumlulukların belirlenmesi gibi aşamalardan oluştuğu anlaşılmaktadır. Bu bağlamda risk değerlendirmesi aşamalarında olası risklerin belirlenmesi ve bunlara yönelik önlemler alınarak bütüncül ve sürdürülebilir bir model çerçevesinde sürecin işletilmesi önem kazanmaktadır.

Sonuç ve Öneriler

Dijital dönüşüm kurumların uygulamalarını ve hizmetlerini yeniden yapılandırmalarını gerektiren bir süreçtir. Bu süreçte genellikle analog olarak gerçekleştirilen süreçlerin elektronik ortam üzerinden gerçekleştirilebilecek bir yapıya taşınması öne çıkmaktadır. Elektronik ortamın sağlamış olduğu avantajların kurumların kendi içlerindeki ve diğer kurumlarla olan iletişiminin yanı sıra hizmet sunduğu kitle ile olan etkileşimi de sağladığı bilinmektedir. Özellikle 1990'lı yılların sonlarından itibaren elektronik ortamın yoğun kullanımı ile iş süreçlerinin daha hızlı, zaman ve mekândan bağımsız bir şekilde gerçekleştirilmesine dönük

olanaklar kurumların da bu ortamda bilginin kullanımına ilişkin yatırımlarını artırmalarında etkili olmuştur. Bu yatırımlarla bilgi, birçok kurum için rekabet avantajı da sağlayan, ona sahip olanları güçlü kılan stratejik bir varlık olarak da görülmeye başlanmıştır. Elektronik ortamda oluşturulan belgeler de kurumların işleyişlerini etkinleştiren bilgi kaynaklarından biri olmuştur. Bilginin elektronik ortamda oluşturulması ve kullanımının yaygınlık kazanması sağladığı avantajların yanı sıra kötü niyetli kullanım, kolaylıkla yok edilebilme, değiştirilme gibi riskleri beraberinde getirmektedir. Bu noktada elektronik ortamda oluşturulan belgelerin özgünlüğünün ve güvenliğinin sağlanması öne çıkan konulardan biri olmuştur. Konuyla ilgili olarak da birçok çalışmanın yapıldığı ve kurumların belge yönetim uygulamaları ile ilgili olgunluk modellerinin geliştirildiği görülmektedir.

Kurumlarda elektronik belgelerin güvenliğinin sağlanmasına yönelik uygulamalar bilgi güvenliği uygulamaları çerçevesinde değerlendirilebilmektedir. Bu kapsamda kurumlarda bilgiye dayalı süreçlerde risklerin belirlenmesi ve bu risklere yönelik önlemlerin alınması ile ilgili uygulamalar yer almaktadır. Konuyla ilgili literatür incelendiğinde de bilgi ile teknolojinin bütünleştiği her noktada riskin bulunabileceği dile getirilmektedir. Bu doğrultuda kurumların risk yönetimi uygulamaları çerçevesinde koruma uygulamaları da bulunmaktadır. Literatürde de elektronik belge koruma ve dijital koruma kavramlarıyla ifade edilen koruma uygulamalarının kurumlarda süreklilik gösterecek bir yaklaşımla ele alınması önemli görülmektedir. Konuyla ilgili olarak ARMA tarafından geliştirilen olgunlaşma modelindeki koruma bileşeni incelendiğinde yüksek düzeylerdeki olgunluk seviyesinde bulunan kurumlarda koruma uygulamalarının periyodik olarak gözden geçirilen ve güncellenen bir strateji ve plan çerçevesinde yapılandırıldığı, bu süreçlerde yer alan profesyonellerin de kurumda bilgi yönetişim sistemi ile ilgili karar verici pozisyonlarda yer aldığı dikkati çekmektedir.

Koruma uygulamaları çerçevesinde kurumsal stratejiler kap-

samında yer alan risk değerlendirmelerinde elektronik ortamda oluşturulan ya da daha sonradan elektronik ortama aktarılan kaynaklara yönelik risklerin tanımlanması ilk aşamalardan biridir. Bu çalışmada da literatüre bağlı olarak açıklanması amaçlanan riskler değerlendirildiğinde bilginin kayıt altına alındığı ve sunulduğu ortamın, oluşturulduğu formatın kullanımı ile tahribatına yönelik riskler gibi teknik risklerin sıralandığı görülmektedir. Bunun yanı sıra üstveri ve bütçe yetersizliği, yönetici farkındalık eksikliği, insan hatalarından kaynaklanan kayıplar gibi yönetimsel riskler de dijital koruma uygulamaları için dikkate alınması gereken riskler arasında değerlendirilmektedir. Son olarak kullanım hakları, entellektüel mülkiyet hakları, mahremiyet ve yasal düzenlemeler gibi konunun hukukî yönü ile ilgili risklerin de bu çerçevede yer alabileceğini söylemek mümkündür.

Çalışmada bir diğer amaç doğrultusunda ele alınan dijital koruma stratejileri, risk yönetimi değerlendirme süreçleri, standartları ve araçları kurumların elektronik ortamdaki bilgi ve belge sistemleri ile bu sistemlerdeki içeriklerin kalıcı bir şekilde erişilebilirliğinin sağlanmasında gerekli önlemlerin alınmasında kullanılmaktadır. Bu tür araç, standart ve süreçlerle elektronik ortamdaki sistem ve içeriklerin düzenli aralıklarla değerlendirilmesi hem kurumun elektronik ortamdaki bilgi varlıklarını daha üst düzeyde konumlandırmasına bir başka deyişle kurumun olgunluk seviyesinin yükselmesine hem de gelişen teknoloji çerçevesinde elektronik bilgi ve belge ile ilgili süreçlerini güncelleyerek sistemin ve içeriğin yeniden kullanılmasına ve bu varlıklardan değer üretilmesine imkan tanıyacaktır. Pandemi gibi uzaktan yönetim gerektiren süreçlerde sistemin ek bir teknoloji yapılandırmasına ihtiyaç duyulmadan ve gerekli güvenlik önlemleri alınmış bir şekilde kullanımına olanak tanıyabilmektedir.

Kaynakça

Adu, K. K. ve Ngulube, P. (2017). Key threats and challenges to the preservation of digital records of public institutions in Ghana. *Information, Communication & Society*, *20*(8), 1127-1145. doi:10.1080/1369118X.2016.1218527

ARMA. (2013). The Principles maturity model. 28 Eylül 2020 tarihinde https://rim.ucsc.edu/management/images/ThePrinciplesMaturityModel.pdf adresinden erişildi.

ARMA. (2017). The Principles®. 28 Eylül 2020 tarihinde https://www.arma.org/page/principles adresinden erişildi.

Bajpai, S., Sachdeva, A. ve Gupta, J. P. (2010). Security risk assessment: Applying the concepts of fuzzy logic. *Journal of Hazardous Materials*, *173*(1), 258-264. doi:10.1016/j.jhazmat.2009.08.078

Barateiro, J., Antunes, G., Freitas, F. ve Borbinha, J. (2010). Designing Digital Preservation Solutions: A Risk Management-Based Approach. *International Journal of Digital Curation*, *5*(1), 4-17. doi:10.2218/ijdc.v5i1.140

Bearman, D. A. (2006). Moments of risk: Identifying Threats to electronic records. *Archivaria*, *62*, 15-46.

Blakley, B., McDermott, E. ve Geer, D. (2001). Information security is information risk management. *Proceedings of the 2001 workshop on New security paradigms* içinde , NSPW '01 (ss. 97–104). New York, NY, USA: Association for Computing Machinery. doi:10.1145/508171.508187

Brown University Archives. (t.y.). Guide for managing electronic records. 17 Eylül 2020 tarihinde https://library.brown.edu/collections/archives/recmgt_guide_elecrec.php adresinden erişildi.

Cloonan, M. ve Sanett, S. (2002). Preservation Strategies for Electronic Records: Where We Are Now—Obliquity and Squint? *The American Archivist*, *65*(1), 70-106. doi:10.17723/aarc.65.1.ak0537t86l2715wv

Cloonan, M. V. ve Sanett, S. (2000). Comparing preservation strategies and practices for electronic records. *New Review of Academic Librarianship*, *6*(1), 205-216. doi:10.1080/13614530009516810

Corrado, E. M. ve Sandy, H. M. (2017). *Digital Preservation for Libraries, Archives, and Museums*. Rowman & Littlefield.

Digital Curation Center ve DigitalPreservationEurope. (2010). Welcome to DRAMBORA Interactive: Log in or Register to Use the Toolkit. *DRAMBORA interactive Digital Repository Audit Method Based on Risk Assessment*. 28 Eylül 2020 tarihinde http://www.repositoryaudit.eu/ adresinden erişildi.

Digital Preservation Coalition. (2015). *Digital Preservation Handbook* (2. basım.). Digital Preservation Coalition. https://www.dpconline.org/handbook adresinden erişildi.

DigitalPreservationEurope (DPE). (2007). Research roadmap. DigitalPreservationEurope (DPE). https://www.digitalpreservationeurope.info/publications/reports/dpe_research_roadmap_D72.pdf adresinden erişildi.

Disaster preparedness for digital content. (2016). 28 Eylül 2020 tarihinde http://dpworkshop.org/workshops/management-tools/disaster-preparedness adresinden erişildi.

Hedstrom, M. (1995). Electronic Archives: Integrity and Access in the Network Environment. *The American Archivist*, *58*(3), 312-324.

Hulitt, E. ve Vaughn, R. B. (2010). Information system security compliance to FISMA standard: A quantitative measure. *Telecommunication Systems*, *45*(2), 139-152. doi:10.1007/s11235-009-9248-8

Hunter, J. ve Choudhury, S. (2003). Implementing Preservation Strategies for Complex Multimedia Objects. T. Koch ve I. T. Sølvberg (Ed.), *Research and Advanced Technology for Digital Libraries* içinde , Lecture Notes in Computer Science (ss. 473-486). Berlin, Heidelberg: Springer. doi:10.1007/978-3-540-45175-4_43

International Council on Archives (Ed.). (1997). *Guide for managing electronic records from an archival perspective*. Studies / International Council on Archives. Paris: ICA.

International Council on Archives. (2016). Digital preservation in lower resource environments: A core curriculum :Understanding digital records preservation initiatives. International Concuil on Archives. https://www.ica.org/sites/default/files/Digital%20Preservation%20Initatives%20Module_0.pdf adresinden erişildi.

Ionita, D. (2013, 31 Temmuz). *Current established risk assessment methodologies and tools*. (Info:eu-repo/semantics/masterThesis). https://essay.utwente.nl/63830/ adresinden erişildi.

Ismail, A. ve Bullah Affandy, H. (2018). Conceptual Paper: Digital Preservation Strategies in Archival Institution. *MATEC Web of Conferences*, *150*, 05052. doi:10.1051/matecconf/201815005052

ISO. (2019). ISO/IEC 27001:2013 Information technology—Security techniques—Information security management systems—Requirements. ISO. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/45/54534.html adresinden erişildi.

Jerman Blažič, A., Klobučar, T. ve Jerman, B. D. (2007). Long-term trusted preservation service using service interaction protocol and evidence records. *Computer Standards & Interfaces*, *29*(3), 398-412. doi:10.1016/j.csi.2006.06.004

Lemieux, V. L. (2016). Trusting records: İs Blockchain technology the answer? *Records Management Journal*, *26*(2), 110-139. doi:10.1108/RMJ-12-2015-0042

Pearce-Moses, R. (Ed.). (2018). Digital preservation. https://interparestrust.org/terminology/term/digital%20preservation adresinden erişildi.

Saleh, Z. I., Refai, H. ve Mashhour, A. (2011). Proposed Framework for Security Risk Assessment. *Journal of Information Security*, *02*(02), 85-90. doi:10.4236/jis.2011.22008

Siew Lin, L., Ramaiah, C. K. ve Kuan Wal, P. (2003). Problems in the preservation of electronic records. *Library Review*, *52*(3), 117-125. doi:10.1108/00242530310465924

Stoneburner, G., Goguen, A. ve Feringa, A. (2002). *Risk management guide for information technology systems: Recommendations of the National Institute of Standards and Technology* (No: NIST SP 800-30) (0 bs., s. NIST SP 800-30). Gaithersburg, MD: National Institute of Standards and Technology. doi:10.6028/NIST.SP.800-30

Sutanto ve Nuryani, E. (2020). Management of the Electronic Archives for Optimizing Services at Banten Jaya University (ss. 82-86). 1st International Multidisciplinary Conference on Education, Technology, and Engineering (IMCETE 2019), sunulmuş bildiri, Atlantis Press. doi:10.2991/assehr.k.200303.021

Task Force on Archiving of Digital Information, Commission on Preservation and Access ve Research Libraries Group (Ed.). (1996). *Preserving digital information: Report of the Task Force on Archiving of Digital Information*. Washington, D.C: Commission on Preservation and Access.

The Center for Research Libraries ve NARA Task Force on Digital Repository and Certification. (2007). Trustworthy Repositories Audit & Certification: Criteria and Checklist. The Center for Research Libraries. https://www.crl.edu/sites/default/files/d6/attachments/pages/trac_0.pdf adresinden erişildi.

The National Archives. (2017). Risk assessment handbook. The National Archives. https://www.nationalarchives.gov.uk/documents/information-management/Risk-Assessment-Handbook.pdf adresinden erişildi.

Türkiye Cumhuriyeti Cumhurbaşkanlığı, Dijital Dönüşüm Ofisi. (2020). Bilgi ve iletişim güvenliği rehberi. Türkiye Cumhuriyeti Cumhurbaşkanlığı, Dijital Dönüşüm Ofisi. https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf adresinden erişildi.

Vermaaten, S., Lavoie, B. ve Caplan, P. (2012). Identifying threats to successful digital preservation: The SPOT model for Risk Assessment. *D-Lib Magazine*, *18*(9/10). doi:10.1045/september2012-vermaaten

Wang, Y. ve Xiang, W. (2008). Role of information security risk assessment in establishing electronic archives safeguard systems. *2008 IEEE International Conference on Networking, Sensing and Control* içinde (ss. 1320-1325). 2008 IEEE International Conference on Networking, Sensing and Control, sunulmuş bildiri. doi:10.1109/ICNSC.2008.4525422

Wangen, G., Hallstensen, C. ve Snekkenes, E. (2018). A framework for estimating information security risk assessment method completeness. *International Journal of Information Security*, *17*(6), 681-699. doi:10.1007/s10207-017-0382-0

Waugh, A., Wilkinson, R., Hills, B. ve Dell'oro, J. (2000). Preserving digital information forever. *Proceedings of the fifth ACM conference on Digital libraries* içinde , DL '00 (ss. 175–184). New York, NY, USA: Association for Computing Machinery. doi:10.1145/336597.336659