BİLGİ DÜNYASI
INFORMATION WORLD

e-ISSN: 2148-354X

Kurum ve Kuruluşlarda Elektronik Belge Yönetim Sistemi Risk Unsurları: Paydaş Görüşlerine Dayalı Nitel Bir İnceleme

Risks Elements of Electronic Records Management Systems in Institutions and Organizations: A Qualitative Review Based on Stakeholder Views

Nagihan Gönül EROĞLU, Coşkun POLAT

Makale Bilgisi / *Article Information*
Bu makaleye atıf yapmak için / *To cite this article:*
Eroğlu, N. G. ve Polat, C. (2025). Kurum ve kuruluşlarda elektronik belge yönetim sistemi risk unsurları: Paydaş görüşlerine dayalı nitel bir inceleme. *Bilgi Dünyası, 26*(2), 485-518. doi: 10.15612/BD.2025.862

Makale türü / *Paper type:* Araştırma Makalesi / *Research Article*

DOI: 10.15612/BD.2025.862

Geliş Tarihi / *Received*: 08.08.2025
Kabul Tarihi / *Accepted*: 15.11.2025
Elektronik Yayınlanma Tarihi / *Online Published*: 22.12.2025

İletişim / Communication
Üniversite ve Araştırma Kütüphanecileri Derneği / University and Research Librarians Association
Posta Adresi / Postal Address: Marmara Sok. No:38/17 06420 Yenişehir, Ankara, Türkiye.
Tel: +90 312 430 03 61; Faks / Fax: +90 312 430 03 61; E-posta / E-mail: bilgi@bd.org.tr
Web: https://bd.org.tr

Araştırma Makalesi

Kurum ve Kuruluşlarda Elektronik Belge Yönetim Sistemi Risk Unsurları: Paydaş Görüşlerine Dayalı Nitel Bir İnceleme*

*Nagihan Gönül EROĞLU*** , *Coşkun POLAT****

Öz

Fiziki ortamda yürütülen belge yönetimi uygulamalarının elektronik ortama taşınması çeşitli risk unsurlarını beraberinde getirmiştir. Önlem alınmadığı takdirde organizasyonlara hukuki yaptırımlar, ekonomik sorunlar, prestij kaybı gibi ciddi zararlar verebilecek bu risklerin yönetimi önemli bir konu haline gelmiştir. Bu çalışma, Türkiye'deki kurum ve kuruluşlarda Elektronik Belge Yönetim Sistemleri (EBYS) ve süreçlerinde karşılaşılan risk unsurlarını ortaya koymak amacıyla gerçekleştirilmiştir. Araştırmanın, EBYS'lerdeki potansiyel risk unsurlarının tespit edilmesine ve daha etkin bir şekilde yönetilmesine yardımcı olacağı öngörülmüştür. Bu kapsamda öncelikle, başta standartlar ve rehberler olmak üzere literatürde konuyla ilgili çalışmalar değerlendirilmiştir. Ardından yarı yapılandırılmış görüşme tekniği kullanılarak 13 kurum ve kuruluşta görev yapan EBYS'den sorumlu personel, belge yönetimi alanında sekiz uzman/akademisyen ve EBYS yazılımı geliştiren üç firma ile gerçekleştirilen görüşmelerle uygulamada karşılan riskler belirlenmiştir. Görüşmelerden elde edilen veriler MAXQDA yazılımı kullanılarak değerlendirilmiştir. Yapılan analizler sonucunda, EBYS ve süreçlerinde kullanıcı hataları, mevzuat belirsizliği/yetersizliği, beklenmedik olaylara hazır olmama, teknoloji değişimi, organizasyonel değişiklik, kurumsal analiz eksikliği, firma bağımlılığı, güvenlik, teknik yetersizlik gibi başlıca risk unsurlarının olduğu anlaşılmıştır. Elde edilen bulgular, ülkemizdeki kurum ve kuruluşlarda EBYS ve süreçlerine ilişkin karşılaşılan risklerin yalnızca yazılım kaynaklı olmadığını, insan kaynaklı, kurumsal ve ulusal boyutlarıyla birlikte çok yönlü olduğunu göstermiştir. Çalışma, EBYS ve süreçlerinin daha sağlıklı işlemesi adına kurumsal farkındalığın ve risk yönetimine olan ilginin güçlendirilmesine yönelik öneriler sunmaktadır.

Anahtar sözcükler: *EBYS, elektronik belge yönetimi, elektronik belge yönetim sistemi, risk, risk yönetimi, elektronik belge yönetiminde risk.*

* Bu çalışma, Nagihan Gönül Eroğlu'nun Prof. Dr. Coşkun Polat danışmanlığında 2025 yılında tamamladığı "Kurum ve Kuruluşlarda Elektronik Belge Yönetim Sistemi Risk Unsurları ve Eğitimi: Çankırı Karatekin Üniversitesi Örneği" başlıklı doktora tezine dayanmaktadır.

** Öğr. Gör. Dr., Çankırı Karatekin Üniversitesi, nagihangonulboso@gmail.com

*** Prof. Dr., Çankırı Karatekin Üniversitesi, polatcoskun@gmail.com

INFORMATION WORLD, 2025, 26 (2), *485-518* *DOI: 10.15612/BD.2025.862*

Research Article

Risks Elements of Electronic Records Management Systems in Institutions and Organizations: A Qualitative Review Based on Stakeholder Views*

*Nagihan Gönül EROĞLU*** , *Coşkun POLAT****

Abstract

The transition from physical records management practices to electronic media has introduced various risks. Managing these risks, which, if left unchecked, can cause significant harm to organizations, including legal penalties, financial hardship, and loss of prestige, has become a crucial issue.This study was conducted to identify the risk factors encountered in Electronic Records Management Systems (ERMS) and their processes in institutions and organizations in Türkiye. It is anticipated that the research will help identify potential risk factors in ERMS and manage them more effectively. To this end, relevant literature studies, particularly standards and guidelines, were reviewed. Then, using a semi-structured interview technique, interviews were conducted with ERMS personnel responsible from 13 institutions and organizations, eight experts/academics in the field of records management, and three companies that developed ERMS software, and the risks encountered in practice were determined. Data obtained from the interviews were analyzed using MAXQDA software. The analyzes revealed that ERMS and processes face significant risks, including user errors, regulatory uncertainty/inadequacy, unpreparedness for unexpected events, technological change, organizational change, lack of institutional analysis, company dependency, security, and technical inadequacy. The findings demonstrate that the risks faced by institutions and organizations in our country related to ERMS and its processes are not solely software-related, but are multifaceted, with human, institutional, and national dimensions. The study offers recommendations for strengthening institutional awareness and interest in risk management to ensure the smooth operation of ERMS and processes.

Keywords: *ERMS, electronic records management, electronic records management system, risk, risk management, risk in electronic records management.*

* This study is based on Nagihan Gönül Eroğlu's doctoral thesis entitled "Electronic Records Management System Risk Elements and Training in Institutions and Organizations: Çankırı Karatekin University Example," supervised by Prof. Dr. Coşkun Polat.

** Lecturer Dr., Cankiri Karatekin University, nagihangonulboso@gmail.com

*** Prof. Dr., Cankiri Karatekin University, polatcoskun@gmail.com

Giriş

İnsanların yaşamında her daim öncelikli bir yeri olan risk, bireylerin kendi ölüm olasılığını düşünmeye başladığı ve tehlikeli durumlardan kaçınmak için eylemlerde bulunması gerektiğini anladığından bu yana önemli bir çalışma alanı olmuştur (Renn, 1998, s. 50). Yalnızca bireylere özgü bir durum olmayan, hemen her alan ve oluşum için geçerli olan risk kavramının birbirine benzer birçok tanımı bulunmaktadır. Oxford Languages'te gelecekte herhangi bir zamanda kötü bir şey olma olasılığı, zarara uğrama tehlikesi olarak tanımlanan risk (Oxford University Press, 2023), Türk Dil Kurumu (TDK) Güncel Türkçe Sözlüğü'nde de benzer şekilde zarara uğrama tehlikesi olarak açıklanmaktadır (2024). "Belirsizliğin amaçlara etkisi" olarak da ifade edilen bu kavram, kurum ve kuruluşların beklenilen durumdan sapmasına işaret etmektedir (International Organization for Standardization [ISO], 2018, s. 1). Bu etki, koşullara ve yönetim yaklaşımına bağlı olarak olumlu (fırsat) veya olumsuz (tehdit) sonuçlar doğurabildiği gibi her iki yönü birden içeren karmaşık bir etkileşim de yaratabilir. Faaliyet alanı veya büyüklüğü ne olursa olsun kurum ve kuruluşlar amaçlarına ulaşma sürecinde belirsizlik oluşturan iç ve dış etkenlerle karşılaşmaktadır. Bu belirsizliklerin giderilerek olası risklerin yönetilmesi, bir organizasyonun hedeflerine ulaşabilmesi için izleyeceği stratejilerin geliştirilmesine önayak olmaktadır (ISO, 2018).

Risk yönetimi, risklerin tanımlanması, analizi, değerlendirmesi, kontrolü ve izlenmesine odaklanan yapılandırılmış bir süreçtir (Salgotra vd., 2025, ss. 1-2). Risklerin belirlenmesinin ardından risk azaltma seçeneklerinden en uygun olan tedavi yöntemi uygulanır (Laine vd., 2021, s. 4). Buradaki amaç, riskleri yönetmek için girdileri bu tür girişimlerden elde edilen faydalarla dengeleyerek maliyet, zaman ve kalite açısından en iyi değeri elde etmektir (Srinivas, 2018).

Kurumlarda risk yönetimi için geliştirilmiş, uluslararası bir standart olan ISO 31000:2018, riskleri belirleme, değerlendirme, takip etme ve yönetme süreçlerini içermektedir. Söz konusu standart içerisinde yer alan ilke, çerçeve ve süreçler sayesinde kurumlar, risklerine daha etkin çözümler üretebilmekte ve hedeflerine ulaşma olasılıklarını artırabilmektedir. Amacı değer yaratmak ve değerleri korumak olan risk yönetimi, kurumlarda performansın artmasına, yeniliğin teşvik edilmesine ve belirlenen hedeflere ulaşılmasına destek vermektedir. Risk yönetimi sürecinde, üst yönetimin de desteğiyle tüm paydaşların dâhil olduğu, kurumun stratejik hedefleriyle uyumlu bir risk kültürünün oluşturulması hedeflenmektedir. Bu hedef doğrultusunda tasarlama, uygulama, değerlendirme ve sürekli iyileştirme aşamalarını içeren bir süreç metodolojisi benimsenmelidir. Bu sürecin gereksinim duyduğu politika, strateji, plan ve prosedürlerin oluşturularak risklerin belirlenmesi, analiz edilmesi, değerlendirilmesi, gerektiğinde müdahale edilmesi, kaydedilmesi ve raporlanması adımlarının sistematik olarak izlenmesi önemlidir (Barnawi, 2013, s. 67; ISO, 2018).

Hayatın hemen her alanına etki eden bilgi ve iletişim teknolojilerindeki gelişmeler kurumların iş süreçlerini dönüştürerek klasik belge yönetimi faaliyetlerinin elektronik ortama taşınmasına zemin hazırlamıştır (Dişli ve Külcü, 2020, s. 57). Elektronik belge yönetimi kurumların belgeye dayalı iş süreçlerine yönelik önemli avantajlar sunmuştur. Kurumlar bu sayede, kâğıt yükünü azaltarak önemli ölçüde zaman ve kâğıttan tasarruf sağlamıştır. Belgelerin merkezi bir yerde depolanması ve kolay erişilebilir hale gelmesi hem iş süreçlerini hızlandırmış hem de ekipler arası iş birliğini artırmıştır. Bu türden avantajlar kurumlara elektronik belge yönetimi konusunda önemli sorumluluklar da yüklemektedir. Elektronik ortamda belgeleri yönetmek amacıyla geliştirilen uygulamalar, sistem ve iş süreçlerinde teknolojinin doğasından kaynaklı birtakım riskleri de beraberinde getirmiştir. Bu riskler, teknolojik altyapı yetersizlikleri, siber saldırılar, veri kaybı/sızıntısı, uyumsuzlukla ilgili sorunlar, insan hatası, kötü niyetli kullanım vb. gibi pek çok farklı unsurdan kaynaklanabilmektedir. Çeşitli alanlarda risklerin yönetilmesi için programlanan risk planlarının, organizasyonlardaki belge yönetim süreçlerine titizlikle ve sistematik biçimde dâhil edilmesi önemli bir konu haline gelmiştir. Bu planlar, risklerin önceden belirlenmesine, analiz edilmesine, değerlendirilmesine ve uygun önlemlerin alınmasına yardımcı olma amacı taşımaktadır. Bu bağlamda çalışmanın odak noktasını kurumların Elektronik Belge Yönetim Sistemi (EBYS) ve süreçlerinde karşılaşabilecekleri potansiyel risklerin belirlenmesi, değerlendirilmesi ve yönetilmesi oluşturmaktadır. Araştırmada, kurumsal iletişimin sağlanmasında kullanılan elektronik belge yönetim sürecinde risk potansiyeli barındıran pek çok tehdit unsuru incelenmektedir. EBYS için teknolojik donanım, yazılım, güvenlik ve gizlilik gibi tahmin edilebilir risk unsurlarının yanı sıra kurumsal iş süreçlerinde öngörülemeyen risk tehditlerinin belirlenmesi ve uygun bir plan çerçevesinde yönetilmesi ayrıntılı bir şekilde değerlendirilmektedir. Araştırma bulguları, kurumların EBYS'lerindeki olası risklerin ve sebeplerinin belirlenmesi, ortaya çıkaracağı olumsuzluğu ortadan kaldırmaya yönelik önlemlerin alınması konusunda değerlendirmeler yapmaya olanak sağlamıştır. Bu değerlendirmeler ışığında kurumlar, çoğu ortak olan bu risklere yönelik alınacak önlemlerle potansiyel zararları en aza indirebilir ve elektronik belge yönetimi uygulamalarını daha güvenli hale getirebilirler.

EBYS Kapsamında Risk Unsurlarının Tematik Dağılımı

Bu çalışmada, EBYS ve süreçlerindeki risk unsurları literatür ve görüşmelerden elde edilen veriler ışığında "dış faktörlere bağlı riskler, iç faktörlere bağlı riskler, sisteme özgü riskler ve belge yönetim süreçlerine ilişkin riskler" olarak dört ana tema çerçevesinde sınıflandırılmıştır.

Dış faktörlere bağlı riskler, kurumun dış çevresinden kaynaklanan, genellikle kontrol edilemeyen veya sınırlı müdahale imkânı bulunan unsurları içermektedir. Siyasi, sosyal, ekonomik ve teknolojik çevredeki değişimler, yasal düzenlemeler gibi kurumun faaliyet gösterdiği alanda meydana gelecek değişiklikler ile doğal afetler ve

EBYS yazılımını tehdit eden siber saldırılar, veri sızıntısı gibi unsurlar dış faktörlere bağlı riskleri oluşturmaktadır. Bu riskler kurumun prestijini, mali yapısını, stratejik hedeflerini ve yapısını doğrudan etkileyebilir. Bu bağlamda risklerin belirlenerek yönetilmesi, önlemler alınması önem arz etmektedir. Dış faktörlerden kaynaklanan riskleri tamamen yok etmek mümkün olmamakla birlikte risk yönetim sisteminin işletilmesi bu tür durumlara karşı daha etkili kararlar alınmasını ve risklerin etkisini en aza indirmesini sağlayabilmektedir (Usman ve Kaygusuz, 2019, s. 115).

İç faktörlere bağlı riskler, kurum içi yönetim, kullanıcı davranışları ve organizasyonel süreçlerden kaynaklanan riskleri kapsamaktadır. Kurumu tam anlamıyla anlamak ve başarılı bir risk yönetimi uygulamak için öncelikle kurumun kültürü, iç ve dış paydaşları, organizasyonel yapısı, mevcut kaynakları, hedefleri, misyonu gibi iç faktörlerin kapsamlı bir şekilde değerlendirilmesi gerekmektedir. Çünkü risk yönetimi kurumun amaç ve hedefleri bağlamında gerçekleşmekte, kurumsal politika, prosedür ve hedefler risk politikasının tanımlanmasında yardımcı olmaktadır. Belge yönetiminin başarısı potansiyel riskler ve fırsatlar dikkate alınarak belirlenmektedir (Australian/New Zealand Standards [AS/NZS], 2004).

Sisteme özgü yapısal riskler, EBYS'nin teknik altyapısı, yazılım ve donanım bileşenleri, güvenlik protokolleri ve teknoloji ile ilişkilidir. EBYS, kurum ve kuruluşlarda işleyişi desteklemeye, karar verme süreçlerini iyileştirmeye ve yasal uyumluluğu sağlamaya yarayan önemli bir araçtır. İyi bir belge yönetim sistemi, kurumsal hafızayı korur, bilgi paylaşımını kolaylaştırarak iş süreçlerini verimli hale getirir (ISO, 2020, ss. 4-5). Birçok faydasının olmasının yanı sıra bu sistemlerin tasarımı, konfigürasyonu, uygulaması ve kullanımı süreçlerindeki hatalar, teknolojik gelişmeler, veri güvenliği riskleri, personel hataları, siber saldırılar gibi çeşitli faktörler sistemin güvenliğini ve performansını olumsuz etkileyebilmektedir.

Belge yönetim süreçlerine ilişkin riskler, belgelerin oluşturulması, sınıflandırılması, saklanması, erişimi ve arşivlenmesi gibi süreçlerde ortaya çıkan hatalar ve eksiklikleri içermektedir. Bir kuruluşun işleyişinde hayati önem taşıyan ve tüm belgelerin kontrolünü, dağıtımını, erişimini, dosyalanmasını ve imha edilmesini sağlayan kapsamlı bir sistem olan elektronik belge yönetimi birçok kurumda belge yönetiminin iyileştirilmesi için geliştirilmiş yeni bir teknoloji gibi görülmektedir. Bu teknoloji belgelerin üretiminden tasfiyesine kadar tüm yönetim sürecinin bilgisayar sistemleri aracılığıyla yürütülebilmesi için geliştirilmiştir. Dolayısıyla sistem fonksiyonları belge yönetimi faaliyetlerini yerine getirebilmelidir. Belgenin oluşturulduğu andan itibaren değerlerine bağlı olarak saklanması veya imha edilmesi noktasına kadar belgenin yaşam döngüsü denilen bu süreçlerin bir yol haritası olarak uygulanması sağlanmalıdır (Marutha, 2022; Odabaş, 2005, s. 37).

Bu tematik yapı, EBYS'deki risklerin farklı boyutlarıyla detaylıca incelenmesine olanak tanımakta, böylece kurumların karşı karşıya olduğu riskler bütüncül bir bakış açısıyla değerlendirilebilmektedir. Birbirleriyle etkileşim içinde olan bu temalar, EBYS süreçlerinin başarısını doğrudan etkilemektedir. Çalışmada, katılımcıların ifadelerinden örnekler sunularak temalar somutlaştırılmakta ve risklerin etkileri ile yönetimine ilişkin öneriler üzerine değerlendirmeler yapılmaktadır. Bu yaklaşım, EBYS süreçlerindeki riskleri kapsamlı şekilde anlamayı sağlamaktadır.

Önceki Çalışmalar

Literatürde EBYS uygulamalarındaki risk yönetimi konusuna dair çalışmaların sınırlı olduğu, özellikle farklı sektörlerde sıkça incelenen risk yönetiminin EBYS bağlamında daha az ele alındığı görülmektedir. Ülkemizdeki literatür, genel anlamda elektronik belge yönetimi üzerine yoğunlaşırken elektronik belge yönetimi uygulamalarının beraberinde getirdiği risk faktörlerine dair analizler oldukça azdır.

Çiçek (2021), sistemin kullanılmasında yüklü miktarda kaynak ayrılmasına rağmen elektronik belgelerin yaşam döngüsü içerisinde birçok riskle karşı karşıya kaldığını belirtmektedir. Araştırmacı, bu risklerin önceden belirlenip çözüm üretilmesi gerektiğine dikkat çekmektedir. Aksi takdirde belgelerin yok olması gibi geri dönüşü mümkün olmayan risklerin ortaya çıkabileceğini vurgulamaktadır. Yalçınkaya (2015) ise EBYS uygulamalarındaki başarının yalnızca kullanılan yazılıma bağlı olmadığını, organizasyonların belge yönetiminde başarı sağlayabilmesi için gerekli olan teknik ve yönetimsel konuları ortaya koyarak risk faktörleri bağlamında değerlendirmesi gerektiğini vurgulamaktadır. Bu nedenle kurumlarda EBYS uygulamalarının başarısı sadece yazılımsal unsurların değil, ilgili yönetimsel süreçlerin de detaylı analizini gerektirmektedir.

Yıldız (2010), bilişim teknolojilerinin kurumlar üzerindeki etkisinin, belge yönetiminin güvenliği ve geçerliliği ile ilgili endişeleri artırdığını belirtmektedir. Bu endişeler, geçerli belge yönetim sistemleriyle ilgili risklerin belirlenmesi ve önceden önlem alınmasını zorunlu kılmaktadır. Sağlık (2021) ise kurumların EBYS'lerinde saklanan e-imzalı belgelerin zamanla özgünlüklerini kaybetme riskiyle karşı karşıya olduğuna dikkat çekmektedir.

Lin (2020) Tayvan'daki devlet kurumlarına yönelik risk yönetiminin teorik çerçevesine uygun olarak elektronik belgelere yönelik bir risk yönetimi modeli oluşturmayı amaçlamaktadır. Gibson (2011) ise İngiltere'deki küçük ve orta ölçekli işletmelerde (KOBİ) elektronik ortamda yürütülen belge yönetimindeki riskleri irdelemektedir.

International Council on Archives (ICA) tarafından geliştirilen Principles and Functional Requirements for Records in Electronic Office Environments (ICA-Req) standardı, belge yönetimindeki riskleri belirlemek ve bunlarla başa çıkmak için önemli bir referans oluşturmakta ve bu alanda yapılan çalışmaların değerini artırmaktadır (ICA, 2008). ISO'nun (2014) "Information and Documentation- Risk Assessment for Records Processes and Systems Technical Report" isimli raporu, 2024 yılında geliştirilerek kapsamlı bir risk yönetim çerçevesi sunmaktadır. Hazine ve Maliye Bakanlığı tarafından hazırlanan Kamu Kurumsal Risk Yönetimi Rehberi (2024), ülkemizdeki kurumların etkin risk yönetimi süreçlerine rehberlik etmek amacıyla kapsamlı bir yöntem ve uygulama adımları sunmaktadır.

Araştırmanın Amacı ve Soruları

Dijitalleşmenin hız kazanmasıyla bilgi ve belge yönetimi alanında önemli bir dönüşüm yaşanmış, kurum ve kuruluşlar belge yönetimini elektronik ortama taşıyarak EBYS'yi zorunlu olarak kullanmaya başlamıştır. Ülkemizde bilgi toplumuna dönüşüm sürecinin bir parçası olarak yürütülen e-Yazışma Projesi kapsamında, kamu kurumlarının 31.07.2017 tarihine kadar EBYS'ye geçmeleri talimatlandırılmış ve sistemin kullanımı yasal bir zorunluluk hâline gelmiştir (e-Yazışma Projesi, 2017). Bu nedenle kurumlar elektronik belge yönetimine ilişkin altyapı çalışmalarına başlamıştır.

EBYS'lerin etkili ve güvenli biçimde işletilebilmesi yalnızca teknik altyapıya bağlı değildir. Bu sistemler bir yazılımdan ibaret olmadığı gibi yalnızca bir paket program da değildir. EBYS, kurum bilgi sistemlerinin omurgasını oluşturmaktadır. Sistemin yönetimi, kullanıcı davranışları, mevzuat yeterliliği ve kurumsal işleyiş gibi çok boyutlu unsurlarla doğrudan ilişkilidir (Özdemirci, 2019, s. 5). EBYS'lerin sahip olduğu bu kompleks yapı, çeşitli kaynaklardan ortaya çıkabilecek çok çeşitli risk türlerini beraberinde getirmektedir. Bu nedenle araştırma, kurum ve kuruluşlarda EBYS süreçlerindeki veya potansiyel risk unsurlarını belirlemeyi, bu riskleri oluşturan etkenleri analiz etmeyi ve sistemin güvenli, tutarlı ve sürdürülebilir şekilde işlemesine engel teşkil eden unsurlar hakkında veri temelli değerlendirmeler sunmayı amaçlamaktadır. Çalışma, EBYS ve süreçlerinde karşılaşılan risklerin anlaşılmasıyla bu risklere yönelik daha bilinçli kararların alınmasına katkıda bulunması bakımından önemli görülmüştür. Bu bağlamda kurum ve kuruluşların risk yönetimi faaliyetleri ve bu etkinliklerdeki eksik yönleri incelenmiştir.

Çalışma kapsamında aşağıdaki sorulara yanıt aranmıştır:

- Kurumlarda EBYS'ye yönelik politikalar oluşturulmuş mudur ve risk yönetim mekanizmaları hayata geçirilmiş midir?
- Kurumlarda EBYS'deki risklerin yönetimine ilişkin yapılması gerekenler nelerdir?
- EBYS ile ilgili mevcut mevzuat ve standartlar yeterli midir?

Yöntem

Araştırma sorularının yanıtlanabilmesi amacıyla nitel yöntem benimsenmiş ve veriler gerçekleştirilen görüşmelerden elde edilmiştir. Bu aşama, EBYS ile doğrudan ilişkili üç farklı paydaş grubuyla gerçekleştirilmiştir. Bu gruplar; kurum ve kuruluşlarda görev yapan EBYS profesyonelleri, EBYS yazılım geliştiren firma temsilcileri ve belge yönetimi alanında çalışmalar yapan uzman/akademisyenlerden oluşmaktadır. Katılımcı profillerindeki çeşitlilik nedeniyle görüşmelerde her bir grup için ayrı hazırlanmış yarı yapılandırılmış görüşme formları kullanılmıştır. Formlar, hem temel temalara ilişkin standart soruları hem de katılımcıların kendi deneyimlerini aktarmasına olanak sağlayacak açık uçlu soruları içermektedir. Her grubun süreçlere dair farklı bakış açılarının olması, çalışmada risklerin çok yönlü olarak ele almasını sağlamıştır.

Örneklem

Araştırmada, Türkiye'deki tüm kurum ve kuruluşlarla görüşme yapmanın zorluğu göz önünde bulundurularak evreni temsil edecek nitelikte 13 kamu kurumundan sistem ve işleyişten sorumlu toplam 27 personel, 3 ticari firma ve 8 alan uzmanı ile akademisyen örneklem olarak seçilmiştir. Veri toplama sürecinde seçilen kurumlardan daha kapsamlı bilgi edinebilmek amacıyla ihtiyaç duyulduğunda birden fazla çalışanla görüşülmüştür. Bu kurumlardan veri toplayabilmek için EBYS'den sorumlu kurum çalışanlarının araştırmacıyla görüşme yapmaya açık olması ön koşul olarak belirlenmiştir. Bunun yanı sıra kurum seçiminde çeşitli ek kriterler de göz önünde tutulmuştur. Bu kapsamda seçilen kurumlarda EBYS konusundaki deneyim düzeyinin yüksek olmasına ve veri toplama sürecinde çeşitliliğin sağlanmasına dikkat edilmiştir. Örneklemdeki Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı ve Cumhurbaşkanlığı Bilgi ve Belge Yönetimi Daire Başkanlığı gibi bazı kurumlar, ülkemizde belge yönetim sistemine geçişte öncü rol oynayıcı, politika ve standart belirleyici niteliktedir. Kurumların bir kısmı kamu tüzel kişiliğine sahipken (ör. Bağcılar Belediyesi), bir kısmı ise köklü geçmişleriyle öne çıkmaktadır (ör. Türkiye Kızılay Derneği). Ayrıca örneklemde diğer kamu teşkilatlarına benzer yapıda olan kurumlar da (ör. Başkent Üniversitesi) yer almaktadır. Yapı ve işleyiş bakımından farklı özelliklere sahip bu kurumlar aşağıda listelenmiştir:

- Ankara Üniversitesi Belge Yönetimi ve Arşiv Sistemi (BEYAS) Koordinatörlüğü
- Atatürk Kültür, Dil ve Tarih Yüksek Kurumu
- Bağcılar Belediyesi
- Başkent Üniversitesi
- Cumhurbaşkanlığı Bilgi ve Belge Yönetimi Daire Başkanlığı
- Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı

- Çalışma ve Sosyal Güvenlik Bakanlığı
- Çankırı Karatekin Üniversitesi (ÇAKÜ)
- Kadıköy Belediyesi
- Tapu ve Kadastro Genel Müdürlüğü
- Türkiye Kızılay Derneği
- Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK)
- Türkiye Büyük Millet Meclisi (TBMM)

Bunların yanı sıra EBYS yazılımı geliştiren firmalarla da görüşme yapıldığı daha önce ifade edilmişti. Özellikle EBYS yazılımına yönelik risk değerlendirmelerinin yapıldığı bu görüşmeler için sektörde öncü ve deneyimli olduğu bilinen üç ticari firma seçilmiştir. Bununla birlikte elektronik belge yönetimi alanında risk yönetimi konusunda bilimsel çalışmalar gerçekleştirmiş veya uygulamada etkin rol oynamış sekiz akademisyen ve uzmanın görüşlerine başvurulmuştur.

Verinin Toplanması, Hazırlanması ve Analizi

Araştırma kapsamında yapılan görüşmeler, 04.01.2025 - 13.03.2025 tarihleri arasında katılımcıların tercihine göre yüz yüze veya çevrim içi (Zoom, Microsoft Teams) ortamda gerçekleştirilmiştir. Görüşmelerden 9'u yüz yüze ve 15'i çevrim içi ortamda gerçekleştirilmiştir. Görüşme öncesinde katılımcılara çalışma hakkında bilgi verilmiş, görüşme formu ve ön değerlendirme materyalleri paylaşılmıştır. Yüz yüze yapılan görüşmeler, katılımcılardan izin alınarak ses kayıt cihazı ile kaydedilmiş ve gerekli durumlarda notlar alınmıştır. Çevrim içi görüşmelerde ise çevrim içi platformun kayıt özelliği kullanılmıştır. Buradaki kayıtlar, Microsoft Word yazılımı aracılığıyla otomatik olarak metne çevrilmiştir. Yüz yüze gerçekleştirilen görüşmelerde tutulan kayıtlar ise Microsoft Word'ün "dikte" özelliği kullanılarak metne dönüştürülmüştür. Otomatik dönüştürme sürecinde ortaya çıkabilecek yazım ve anlam hatalarının önüne geçebilmek amacıyla tüm dökümler, orijinal ses kayıtlarıyla karşılaştırılarak manuel olarak kontrol edilmiş ve hatalı kısımlar düzeltilmiştir. Böylece metin analizi için hazır duruma getirilen görüşmelerden toplam 253 sayfadan oluşan kapsamlı bir nitel veri kümesi elde edilmiştir. Elde edilen veriler, nitel veri analizi yazılımı olan MAXQDA kullanılarak içerik analizi yöntemiyle değerlendirilmiş ve temalar altında sınıflandırılarak analiz edilmiştir.

Nitel araştırmalarda elde edilen verilerin sistematik bir biçimde analiz edilerek araştırma sorularına yanıt üretilmesi, yapılandırılmış ve aşamalı bir çözümleme sürecini takip etmeyi gerektirmektedir. Bu sürecin temel adımlarından biri olan kodlama, araştırmacının ham verilerdeki karmaşayı düzenleyerek temel kavramları ve aralarındaki ilişkileri ortaya çıkarmasına olanak tanır (Miles vd., 2014, s. 79). Kodlama,

verilerin sınıflandırılması, tematik desenlerin belirlenmesi ve ilişkili kavramların açığa çıkarılması için önemli bir analitik çerçeve sağlamaktadır (Yıldırım ve Şimşek, 2018, s. 228). Bu doğrultuda çalışmada veri analizinin ilk aşaması olan kodlamayla veriler sistemli bir biçimde erişilebilir hale getirilmiş, içeriklerin işlenebilirliği artırılmış ve analiz sürecinin güvenilirliği güçlendirilmiştir. Ayrıca kodların sıklıkları ve dağılımları belirli ölçülerde nicel göstergelere dönüştürülerek analiz süreci hem nitel hem de nicel boyutta desteklenmiştir.

Kodlama sürecinin ardından nitel veri analizinin ikinci aşaması olan tema oluşturma aşamasına geçilmiştir. Bu süreçte elde edilen tüm kodlar, kavramsal benzerlikleri ve içeriksel ilişkileri doğrultusunda daha üst düzeyde anlam taşıyan temalar altında gruplandırılmıştır. Temalar, kodlar arasındaki benzerlikler, farklılıklar ve karşılıklı ilişkiler dikkate alınarak yapılandırılmıştır. Kodlama süreci boyunca katılımcılardan elde edilen farklı yanıtlar, belirli tematik kategoriler altında birleştirilmiş ve temaların tanımlanması sağlanmıştır. Yorumlayıcı ve sınıflayıcı nitelikte olan bu süreç, veri analizinin en yoğun ve zorlu aşamalarından biridir. Her bir görüşme metni analiz edilirken yeni kodlar ve temalar ortaya çıkmıştır. Daha önce analiz edilen metinler, bu yeni tematik yapılar doğrultusunda yeniden incelenerek gerektiğinde revize edilmiştir.

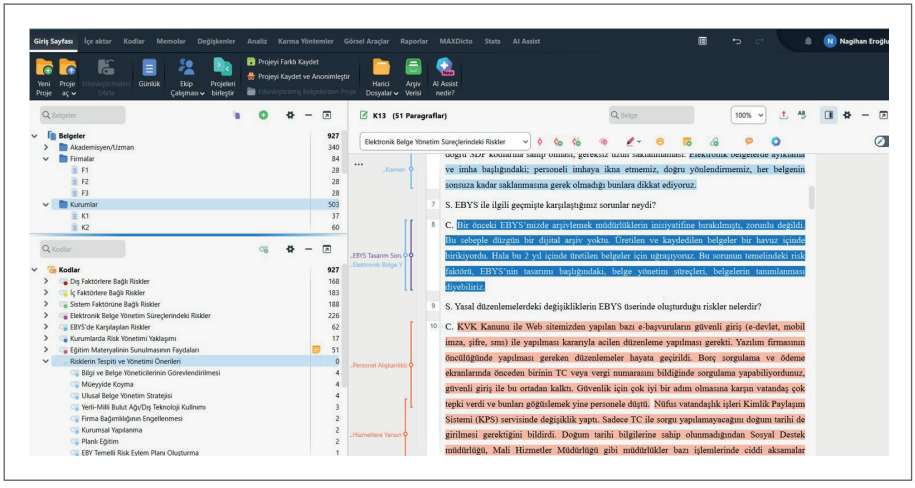
Tüm kodlama işlemlerinin tamamlanmasının ardından yazılım üzerinde "Kod İstatistikleri" modülü altında yer alan "Alt Kodların İstatistiği" özelliği kullanılarak kodlara, temalara ve alt temalara ilişkin frekans verileri elde edilmiştir. Bu özellik sayesinde nicel verilerin yanı sıra ilgili kod ve temaların yer aldığı metin parçalarına da doğrudan erişim sağlanmıştır. Ayrıca yazılımın sunduğu kod modeli aracı kullanılarak "Kod-Alt Kod-Bölümler Modeli" ve "Hiyerarşik Kod-Alt Kod Modeli" gibi hiyerarşik yapılar oluşturulmuştur. Bu yapılar bölümler arasındaki ilişkileri görselleştirerek verilerdeki örüntülerin daha sistematik bir şekilde analiz edilmesine yardımcı olmuştur.

Verilerin analize hazırlanmasının son aşamasında araştırmaya katılan kişilerin kimlik bilgilerinin ve çalıştıkları kurumların gizliliğini sağlamak amacıyla tüm veriler kişisel verilerin korunmasına ilişkin etik ilkelere uygun biçimde anonimleştirilmiştir. Bu doğrultuda akademisyen ve uzmanlar AU1-AU8 arasında; firma temsilcileri F1-F3 arasında; kurum/kuruluş temsilcileri ise K1-K13 arasında kodlanmıştır.

Araştırmada iç geçerliliği artırmak amacıyla konunun derinlemesine irdelenebilmesi için her bir görüşmede yeterince süre ayrılmasına özen gösterilmiştir. Bununla birlikte katılımcıların gerçek deneyimlerini doğru bir şekilde aktarmalarını sağlamak amacıyla anlaşılması güç yanıtların açıklanması istenmiş ve anlaşıldığı şekliyle katılımcıya teyit ettirilmiştir. Veri analizi sürecinin güvenirliğini sağlamak amacıyla ise ham veriden başlayarak kodlara ve temalara ilişkin detaylı bir kodlama şeması oluşturulmuştur (Bkz. Şekil 1). Bunun yanı sıra bulgular bölümde, katılımcılardan doğrudan ve ayrıntılı alıntılar sunularak bulguların inandırıcılığının güçlendirilmesi hedeflenmiştir.

Şekil 1

MAXQDA kod sistemi



Bulgular

Çalışmanın bu bölümünde araştırma verilerinin analizi sonucu ulaşılan bulgulara yer verilmektedir. Okunabilirliği ve takibi kolaylaştırmak amacıyla araştırma bulguları 6 grup altında yapılandırılmıştır. Bu gruplar sırasıyla "Dış Faktörlere Bağlı Riskler", "İç Faktörlere Bağlı Riskler", "Sistem Faktörüne Bağlı Riskler", "Belge Yönetim Sürecine Bağlı Riskler", "EBYS'de Karşılaşılan Temel Riskler" ve "Risklerin Tespiti ve Yönetimine Yönelik Öneriler"dir.

Dış Faktörlere Bağlı Riskler

Sistem dışında gelişmesine rağmen EBYS'yi etkileyen doğal afetler, siber saldırılar, ekonomik krizler gibi beklenmedik olayların oluşturduğu riskler, yeni teknolojinin beraberinde getirdiği riskler bu temada yer almaktadır.

Katılımcılar umulmadık zamanda gerçekleşerek geniş etki yaratan beklenmedik olayları, EBYS'yi tehdit eden önemli bir alan olarak görmektedir. Beklenmedik olaylara bağlı risk tetikleyicileri ve ortaya çıkabilecek riskler Tablo 1'de gösterilmektedir:

Tablo 1

Beklenmedik Olaylara Bağlı Risk Tetikleyicileri ve Ortaya Çıkabilecek Riskler

Risk Tetikleyicileri (N=30)	**Katılımcılar**
Önlem Eksikliği (N=14)	AU1-AU8, F1, K2, K5, K10, K12, K13
Ekonomik Krizler (N=9)	AU1-AU3, AU5, AU7, AU8, F1, K5, K9
Bilgi Eksikliği (N=7)	AU1, AU5, AU7, F2, K8, K10, K13
Risk Unsurları (N=34)	**Katılımcılar**
Veri Kaybı (N=12)	AU1, AU5, F1-F3, K1, K3-K5, K7, K10, K13
Veri Güvenliği (N=7)	AU2, AU5, F1, K5, K7, K9, K13
Fiziksel Hasar (N=5)	F3, K5, K10, K12, K13
Erişim (N=3)	AU2, K5, K13
Verilerin Bozulması (N=3)	K5, K7, K9
Hizmet Kesintisi (N=2)	F1, K2
İş Sürecinin Aksaması (N=2)	K2, K3

Tablo 1 incelendiğinde, beklenmedik olayların meydana getireceği risk etmenleri hususunda katılımcıların 14'ünün önlem eksikliği, 9'unun ekonomik krizler ve 7'sinin bilgi eksikliğini belirttiği görülmektedir. Buna göre, en yaygın risk kategorisinin önlem eksikliği olduğu anlaşılmaktadır.

Tabloda ayrıca beklenmedik olayların sonucunda meydana gelebilecek risklere yer verilmektedir. Bu risklerin başında veri kaybının (N=12) geldiği görülmektedir. Bunu veri güvenliği (N=7) ve fiziksel hasar (N=5) risklerinin takip ettiği anlaşılmaktadır. Beklenmedik olayların oluşturabileceği risklerden olan erişim (N=3) ve verilerin bozulması (N=3) faktörlerinin de EBYS ve süreçlerini tehdit eden önemli unsurlar olduğu gözlemlenmektedir.

Yeni teknolojilerin (yapay zekâ, nesnelerin interneti vb.) kurumsal sistemlere entegrasyonu, iş süreçlerinin hızlanması ve verimliliğin artması açısından önemli fırsatlar sunduğu gibi birçok riski de beraberinde getirmektedir. Söz konusu teknolojilere entegrasyonla birlikte EBYS'de karşılaşılabilecek risklere yönelik katılımcı görüşlerine ilişkin veriler Tablo 2'de verilmektedir:

Tablo 2

Yeni teknolojilerin ve teknolojik değişimin beraberinde getirdiği riskler

Yeni Teknoloji Riskleri (N=56)	**Katılımcılar**
Güvenlik/Gizlilik (N=17)	AU1-AU8, F1, F3, K1, K4, K5, K7, K9, K11, K12
Teknolojik Altyapı Yetersizliği (N=10)	AU1-AU8, K3, K10
Yapay Zekâ İçin Veri Seti Riskleri (N=10)	AU4-AU7, F1-F3, K2, K4, K11
Personel Yetkinliği (N=7)	AU1, AU2, AU7, K2, K4, K11, K13
Dış Kaynaklı Teknoloji Kullanımı (N=5)	AU1, AU4, AU6, AU7, K2
Mevzuat Eksikliği (N=4)	AU1, AU4, K1, K5
Bilinçsiz Kullanım (N=3)	K1, K2, K5
Teknolojik Değişim Riskleri (N=9)	**Katılımcılar**
Güvenlik (N=5)	AU1, AU3-AU5, AU8
Belgenin Delil Değerinin Bozulması (N=2)	AU1, AU7
Erişim (N=2)	AU3, AU5

Tablo 2 incelendiğinde hem yeni teknolojilerin hem de teknolojik değişimin beraberinde getirdiği risklerin başında "güvenlik" geldiği görülmektedir. Katılımcılar ayrıca yeni teknolojilerin entegrasyonu konusunda teknolojik altyapı yetersizliklerine (N=10) ve yapay zekâ için hazırlanan veri setinin beraberinde getireceği risklere (N=10) değinmiştir. Ayrıca personel yetkinliği (N=7), dış kaynaklı teknoloji kullanımı (N=5), mevzuat eksikliği (N=4) ve yeni teknolojilerin bilinçsiz kullanımının (N=3) dikkate değer risk unsurları arasında olduğu gözlemlenmektedir.

Yapay zekâ, makine öğrenmesi ve nesnelerin interneti gibi yeni teknolojilerin EBYS'leri tehdit etmesinin yanı sıra kullanılan teknolojinin kendisindeki değişim ve dönüşüm de sistemsel risklere neden olmaktadır. Teknolojik altyapının sürekli değişmesi/gelişmesine paralel olarak güvenliğin yanı sıra erişim (N=2) ve belgenin delil değeri (N=2) üzerinde riskler meydana getirmektedir.

Katılımcıların teknolojinin EBYS üzerindeki güvenlik riskleri konusuna daha çok değindiği anlaşılmıştır. Konuyla ilgili olarak AU4, "Teknolojiyi transfer edenler aynı şekilde sistem güvenliğini de transfer etmeli. Özellikle dış kaynaklı hizmet alımlarında

hukuki altyapısı çok iyi oluşturulmuş akıllı sözleşmeler hazırlanmalı" ifadeleriyle, teknolojik dönüşüm süreçlerinde güvenlik tedbirlerinin yasal ve teknik boyutlarının eş zamanlı ele alınması gerektiğini vurgulamıştır.

İç Faktörlere Bağlı Riskler

Kurum ve kuruluşların bünyesinde, iç yapıdan, süreçlerden ya da personelden kaynaklanan riskler bu tema altında yer almaktadır.

Tablo 3

İç Faktörlere Bağlı Riskler

Organizasyonel Değişim Riskleri (N= 24)	**Katılımcılar**
Erişim (N=5)	AU8, K1, K9, K10, K12
İş Yükü (N=5)	AU6, AU8, K1, K2, K9
Veri Kaybı (N=4)	AU1, AU6, F3, K1
Yönetsel Karmaşıklık (N=4)	AU1, K5, K6, K13
Firma Değişikliği (N=3)	AU4, AU6, AU8
İş Sürecinin Aksaması (N=3)	F1, F3, K1
Personel Devir Hızının Oluşturduğu Riskler (N=13)	**Katılımcılar**
İş Sürecinin Aksaması (N=5)	AU1, K2, K11-K13
Yetkisiz Erişim (N=4)	AU1, K2, K3, K11
Geçmiş Belgelere Erişim Sorunu (N=2)	K5, K10
Uzmanlaşmanın Sağlanamaması (N=2)	AU1, K10

Tablo 3'te yer alan organizasyonel değişikliklerin oluşturabileceği riskler incelendiğinde, 5 katılımcının kurumlarda belgeye erişim riski üzerinde durduğu görülmektedir. Ayrıca değişikliklerin personele iş yükü artışı olarak yansıyacağını aktaran aynı sayıda (N=5) katılımcı bulunmaktadır. Bununla birlikte katılımcılardan 4'ü değişiklikler sırasında veri kaybının meydana gelebileceğine dikkat çekmektedir. Ayrıca yönetsel karmaşıkların oluşabileceğini ifade eden 4 katılımcının olduğu gözlemlenmektedir.

Tablo 3 ayrıca EBYS başarısını olumsuz etkileyen bir diğer iç faktörün sık yaşanan personel değişimi ve buna bağlı olarak sistemde görev tanımlarının sürekli değiştirilmesi/güncellenmesi olduğunu göstermektedir. Buna göre iş sürecinin aksamasının (N=5) katılımcılar tarafından en çok vurgulanan risk olduğu, bunu yetkisiz erişimin (N=4) takip ettiği anlaşılmaktadır. Geçmiş belgelere erişim sorunu (N=2) ve uzmanlaşmanın sağlanamaması (N=2) katılımcılar tarafından dile getirilen önemli diğer riskler arasındadır.

Sistem Faktörüne Bağlı Riskler

EBYS, belge yaşam döngüsündeki süreçlerin işletileceği bir yazılım sistemidir. Bu sistemler belirli yazılımlar, donanımlar, veri tabanları, ağ bağlantıları gibi etkenlerden oluşmaktadır. Sistemin işletilmesinde pek çok risk unsuru bulunmaktadır. Görüşmelerden elde edilen bulgularda, sistem tasarım ve yapılandırma, sürdürülebilirlik ve süreklilik, bakım ve güvenlik uygulamaları, tedarikçi bağımlılığı, hukuki riskler, teknik riskler gibi risklerin olduğu görülmektedir.

Elde edilen bulgular, özellikle bakım ve güvenlik konusuna dikkat çekmektedir. EBYS'lerin güncelliğini ve performansını etkileyen bakım ile sistemdeki bilgi ve belgelere yetkisiz erişime yol açabilecek güvenlik riskleri katılımcılardan elde edilen veriler doğrultusunda Tablo 4'te sunulmaktadır:

Tablo 4

Bakım ve güvenlik riskleri

Riskler (N=26)	Katılımcılar
Veri Güvenliği (N=10)	F1, F2, K2-K5, K7-K9, K12
Yedekleme ve Geri Yükleme Riskleri (N=8)	
Veri Kaybı (N=3)	AU5, K2, K12
Hizmet Kesintisi (N=3)	K2, K3, K12
Fiziksel Cihazların Deforme Olması (N=2)	K3, K9
Alt Yapı (N=4)	AU1, AU4, AU5, AU7
Teknik Şartname (N=2)	F1, AU8
İnsan Faktörü (N=2)	F1, AU3

Tablo 4'e göre, bakım ve güvenlik risklerinin başında veri güvenliği (N=10) gelmektedir. Katılımcılar veri güvenliği riskini, özellikle elektronik belgelerin yetkisiz erişim tehdidine karşı korunma ihtiyacı bağlamında en önemli risk unsuru olarak vurgulamaktadır. Bu riskin yanı sıra altyapı (N=4) sorunları ile yedekleme ve geri yüklemeyle ilgili risklerin (N=8) ön plana çıktığı görülmektedir. Yedekleme ve geri yükleme kategorisinin altında ise veri kaybı (N=3), hizmet kesintisi (N=3) ve fiziksel cihazların deforme olması (N=2) unsurlarının yer aldığı izlenmektedir. İnsan faktörü (N=2) ise ayrı bir risk unsuru olarak ele alınmaktadır. Katılımcı görüşleri, veri güvenliğinin daha çok teknik, dışsal veya yetkilendirme unsurlarına odaklandığını gösterirken insan faktörü riskleri içsel ve davranışsal sorunlara işaret etmektedir. Katılımcı ifadelerinde insan faktörü riskinin güvenlik zafiyetine yol açtığı şu şekilde ifade edilmektedir: "Genel olarak kullanıcı dikkatsizliği, eğitimsizliği ve liyakatsizliği nedeniyle yaşadığımız sorunlar. Bu durumları da tespit ettikçe gerekli önlemleri alıyoruz. Örneğin kullanıcının hesabını bilgisayarında

açık bırakıp ayrılması gibi." ve "En önemli güvenlik sorunu şimdilik yine insan unsurudur. Eğitimler, katmanlı denetimler ve kontrol sistemleri ile bu süreçler sürekli gözetilebilmelidir."

Sistem faktörlerine bağlı risk alanlarından biri mevzuat/standartlara uyum ve hukuki risklerdir. EBYS'nin tasarım ve yapılandırma sürecinde akademisyenler/uzmanlar ve firma temsilcileriyle gerçekleştirilen görüşmelerden elde edilen risklere ilişkin veriler Tablo 5'te verilmektedir:

Tablo 5

Hukuki riskler

Riskler (N=19)	Katılımcılar
Uluslararası Belge Yönetim Standartlarına Uyum ve Uygulamadaki Yetersizlikler (N=7)	AU1-AU5, AU7, AU8
Belgenin Delil Değeri (N=5)	AU1, AU4, AU5, AU7, AU8
E-İmza Güvenliği (N=3)	AU5-AU7
Mevzuat Takibi (N=2)	AU1, AU2
Uzman Personel Eksikliği (N=2)	AU1-AU3

Tablo 5'te en sık dile getirilen riskin uluslararası belge yönetim standartlarına uyum ve uygulamadaki yetersizlikler (N=7) ilgili olduğu görülmektedir. Ülkemizde kullanılan EBYS'lerin TS 13298 ile uyumlu olma zorunluluğuna rağmen katılımcıların risk olarak algıladığı temel sorun, bu standartların pratikte benimsenme, uygulama ve uluslararası belge yönetim mevzuatlarına göre eksik yanlarının olduğu yönündedir. Katılımcılar, Türkiye'deki kurumların bu standartlara uyum sağlayamadığını, böyle bir çabalarının da genellikle olmadığını belirtmiştir. Ayrıca, belgenin delil değeri (N=5), e-imza güvenliği (N=3), mevzuat takibinin yapılmaması (N=2), uzman personel eksikliği (N=2) gibi unsurların da hukuki riskler arasında olduğu gözlemlenmektedir.

Katılımcılar tarafından sıklıkla vurgulanan uluslararası belge yönetim standartlarına uyum ve uygulamadaki yetersizlikler konusunda katılımcılardan AU5, "Mesela 13298'i ele alırsak 13298 daha çok aslında yazılımcıların ve sistemlerin işine yarayan bir standart işte belge süreç nasıl olması gerektiğine dair ama mesela ICA'nın (Uluslararası Arşiv Konseyi) çıkardığı standartlar var. Bunların tam uygulanmadığını düşünüyorum. Bunların benimsenmesi için mutlaka bunların Türkçeye çevrilip her kurumlara böyle rehber niteliğinde resmi tebliğlerle desteklenmesi lazım." şeklinde açıklamaktadır. AU7 ise uluslararası belge yönetim standartlarının ayna komiteler aracılığıyla tüm dünyadaki gelişmelerin (örn. Blockchainde belge yönetimi) ışığında oluşturulduğunu, bu standartları takip etmeninin verilen hizmetin düzeyini olumlu etkilediğini, aslında

bunların bir zorunluluk olması gerektiğini ve ülkemiz standartlarının bu yönde güncellenmesi gerektiğini vurgulamaktadır.

Katılımcılar tarafından sıklıkla vurgulanan uluslararası belge yönetim standartlarının uyarlanması konusunda katılımcılardan AU8 ise bu standartların ülkemizde uluslararası alandaki kadar değer görmediği görüşündedir. Katılımcı, bunun acı bir gerçek olduğunu ve buna uygun adımlar atılması gerektiğini belirtmiştir. Belgeyi elektronik ortamda imzalayıp elektronik karar defteri tutmalarına rağmen, denetim mercilerinin hâlen fiziki defterleri sormasının, standartların tam anlamıyla yakalanamadığını gösterdiğini ifade etmiştir.

Katılımcılardan AU7 belgenin delil değeri riskine ilişkin olarak delil niteliğinin ait olduğu mevzuatın şartlarına göre değiştiğini belirtmiştir. E-fatura ile normal yazışma tipi belgelerde aradıkları kriterlerin birbirinden farklı olduğu örneğini vermiştir. Katılımcı, belge yönetimini süreç yönetimiyle ve mevzuatla ilişkilendirdiğini, farklı mevzuatlara tabi süreçlerin ortaya çıkardığı belgelerin niteliğinin değiştiğini vurgulamaktadır. Pratikte ise kurumların farklı belge grupları için aynı tür üst verileri kullandığını, oysa kanunun farklı üst veriler talep ettiğini dile getirmiştir. Katılımcı, kanun tipolojisine göre hareket ederek hangi mevzuatın hangi tür bilgiyi istediğinin tespit edilmesi gerektiğini ve üst verilerin buna uygun şekilde kurgulanması gerektiğini söylemiştir. Delil niteliğini etkileyen temel unsurlar arasında belgenin düzenleyicisi, belge sayısı, imzası ve belgenin PDF/A formatında hazırlanmasının yer aldığını ancak örnek olarak Adalet Bakanlığı'nın UYAP sistemi aracılığıyla UDF uzantılı belge oluşturduğunu, Birlikte Çalışabilirlik Esasları Rehberi'nin bu formatı içermediğini ve bu nedenle kamu tarafından resmî olarak tanınmadığını belirtmiştir. Katılımcı, bu durumun özellikle Devlet Arşivleri'ne intikal eden belgelerde delil niteliği açısından sorunlar yaratabileceğini, hukukun önerdiği formatları kullanmadıkları için format bazlı problemlerin ortaya çıkabileceğini öngörmektedir. Bu bağlamda belge formatları ile mevzuat uyumunun belgenin delil değeri açısından önemli risk unsurları arasında olduğunun altını çizmektedir.

Belge Yönetim Sürecine Bağlı Riskler

Belge yönetimi, kurumların iş faaliyetleri ve işlemleri hakkında kanıt niteliği taşıyan belgelerin oluşturulması, edinilmesi, bakımı, kullanımı, elden çıkarılması (tasfiyesi) ve saklama süreçlerinin etkin ve sistematik kontrolünden sorumlu yönetim alanıdır (ISO, 2016, s.3). Katılımcılardan elde edilen bulgular doğrultusunda, belge yönetim sürecinde karşılaşılan riskler bu bölümde verilmektedir.

Tablo 6

Belge Yönetim Sürecine Bağlı Riskler

SDP Hata Riskleri (N=48)	**Katılımcılar**
Belge Erişimi (N=14)	AU1, AU3-AU6, AU8, F2, K3, K4, K6, K8, K10, K11, K13
Tasfiye Sürecinde Zorluk (N=11)	AU8, K1, K2, K4-K7, K9, K11-K13
Yanlış İmha (N=8)	AU5, F2, K2, K6, K9, K11-K13
Hukuki Riskler (N=8)	AU1, K1, K2, K7, K9, K10, K12, K13
Gereksiz Saklama (N=4)	K2, K7, K9, K13
Yönetilemez Yapı (N=3)	AU1, AU6, F2
Tasfiye İşlem Belirsizlik Riskleri (N=26)	**Katılımcılar**
Belge/Veri Kaybı (N=7)	AU1, AU5, AU7, AU8, F1, F3, K5
Gereksiz Saklama (N=4)	K3, K4, K7, K9
Süreci İşletememe (N=4)	K1, K4, K7, K11
Yasal Riskler (N=4)	AU1, AU7, F1, F3
Yanlış İmha (N=3)	K7, K9, K13
Karbon Ayak İzi (N=2)	AU2, AU3
Yönetilemez Yapı (N=2)	AU1, AU8

Tablo 6'ya göre, en sık dile getirilen risk unsurunun belge erişimi (N=14) olduğu gözlemlenmektedir. Bunu tasfiye sürecinde yaşanan zorluklar (N=11)'ın izlediği anlaşılmaktadır. SDP'de yapılan hatanın yanlış imha işlemleri (N=8), hukuki riskler (N=8) gibi önemli sonuçlar doğurduğu görülmektedir. Dolayısıyla SDP'de yapılan hataların tasfiye işlemlerinde önemli sorunlara neden olduğu anlaşılmaktadır. Tabloda tasfiye işlem belirsizliklerinin ortaya çıkarabileceği riskler arasında en sık dile getirilen risk unsurunun belge/veri kaybı (N=7) olduğu görülmektedir. Gereksiz saklama (N=4), süreci işletememe (N=4), yasal riskler (N=4), yanlış imha (N=3) gibi durumların katılımcılar tarafından üzerinde önemli durulan riskler olduğu anlaşılmaktadır.

Katılımcılardan AU5 tasfiye sürecindeki riskler hakkında önemli bir konuya dikkat çekmiştir: "*Burada önemli olan şey bunların hataya yer verilmeden giderilmesi. Çünkü sistemde hem manuel imha var hem de tetikleyicilerin çalıştığı otomatik imhalar var. Siz bir belgeye beş (5) yıl sonra imha et diyorsunuz ama ilgili dosya kodu ne? Bu dosya kodunun içine önemli belgeler atanırsa bunlar otomatikman imha ediyor. Dolayısıyla bu hukuki ve arşivsel anlamda da değer kaybına yol açıyor*"

EBYS'de Karşılaşılan Temel Riskler ve Risklerin Yönetimi

Katılımcılardan elde edilen bulgular doğrultusunda, EBYS ile ilgili geçmişte yaşanılan veya karşılaşılması muhtemel riskler belirlenmiştir. Bu riskler, EBYS uygulamaları sırasında farklı düzeylerde ve çeşitli alanlarda karşılaşılan sorunları kapsamaktadır. Tablo 7'de EBYS uygulamalarında karşılaşılan temel risklere ve bunların etkili bir şekilde yönetilmesine ilişkin katılımcı görüşlerine yer verilmektedir.

Tablo 7

EBYS'de karşılaşılan temel riskler ve risklerin yönetimine yönelik öneriler

EBYS'de Karşılaşılan Temel Riskler (N=43)	**Katılımcılar**
Personel/Kullanıcı Kaynaklı Riskler (N=10)	AU1, AU3, AU5, AU6, AU8, F1, K2, K5, K8, K10
EBYS'nin Kurumsallaştırılamaması/Farkındalık Eksikliği (N=7)	AU1, AU2, AU6, AU8, K1, K9, K13
EBYS Yazılım Değişikliği (N=7)	AU1, AU4, F2, K1, K4, K6, K7
Organizasyonel Değişim (N=4)	F1, F3, K6, K7
E-imza Riskleri (N=3)	AU1, AU7, F2
EBYS Tasarım Sorunu (N=3)	F1, K10, K13
Güncelleme Sonrası Riskler (N=3)	AU1, K6, K12
Yönetici/İdareci/ Kullanıcı Talepleri (N=3)	AU2, F2, F3
Yetkilendirme (N=3)	AU1, AU2, K5
Risklerin Yönetimine Yönelik Öneriler (N=26)	**Katılımcılar**
Bilgi ve Belge Yöneticilerinin Görevlendirilmesi (N=5)	AU2, AU3, AU6, AU7, AU8
EBY Temelli Risk Eylem Planı Oluşturma (N=4)	AU1, AU5-AU7
Müeyyide Koyma (N=4)	AU1, AU2, AU5, AU7
Ulusal Belge Yönetim Stratejisi (N=4)	AU2-AU4, AU7
Yerli-Milli Bulut Ağı/Dış Teknoloji Kullanmama (N=3)	AU1, AU3, AU6
Firma Bağımlılığının Engellenmesi (N=2)	AU6, AU8
Kurumsal Yapılanma (N=2)	AU1, AU6
Planlı Eğitim (N=2)	AU4, AU5

Tablo 7'de EBYS'de karşılaşılan temel risklerin başında personel ve kullanıcı kaynaklı risklerin (N=10) olduğu görülmektedir. EBYS'nin kurumsallaştırılamaması/farkındalık eksikliği (N=7) ve EBYS yazılım değişikliği (N=7) de öne çıkan etmenler arasındadır. Ayrıca organizasyonel değişim (N=4), e-imza riskleri (N=3), EBYS tasarım sorunları (N=3), güncelleme sonrası riskler (N=3), yönetici, idareci veya kullanıcı talepleri (N=3), yetkilendirme sorunları (N=3) da sistemde karşılaşılan risklerdendir.

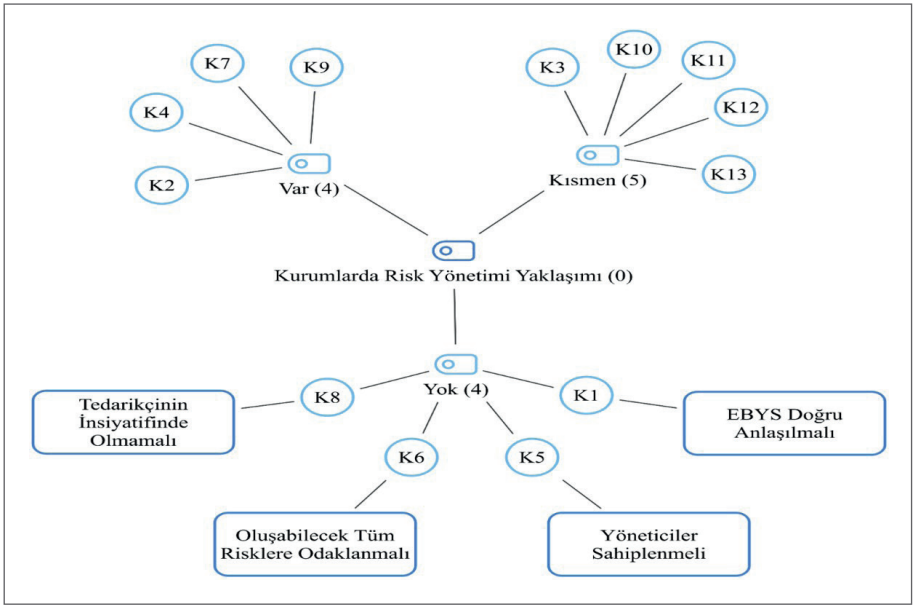
Katılımcılar, EBYS kapsamında en belirgin risk unsurlarından birinin insan faktörü olduğunu vurgulamıştır. Katılımcı AU6'ya göre, insanın dâhil olduğu her süreçte risk kaçınılmazdır ve bu nedenle sistemlerin mümkün olduğunca kullanıcıya sınırlı yetki verecek şekilde tasarlanması gerekmektedir. Benzer şekilde, AU8 kullanıcı alışkanlıklarının sisteme entegrasyon sürecini olumsuz etkilediğini, kullanıcıların eski kurumlardaki uygulamaları örnek göstererek yeni sistemlere uyum sağlama konusunda direnç gösterdiğini ifade etmiştir. AU1 ise özellikle yaşça büyük personelin, sistem güncellemeleri ve elektronik imza gibi teknik bileşenleri uygulamada zorluk yaşadığını, bu durumun belge akışını sekteye uğrattığını aktarmıştır. Ayrıca EBYS'lerin asgari şartlara uygun tasarlandığı halde, birçok önemli sürecin (örneğin belge oluşturma, dosya plan kodu seçimi) hâlen kullanıcı inisiyatifine bırakıldığını ve bunun hatalı işlem riskini artırdığını ifade etmiştir. K5 ve K10 ise kullanıcı bilgisizliğini ve alanında uzman personel eksikliğini temel risk faktörleri arasında saymıştır.

Tablo 7'de katılımcıların büyük çoğunluğunun (N=5) EBYS'de karşılaşılan temel risklerin yönetimi için bilgi ve belge yöneticilerinin görevlendirilmesi gerektiği önerisini sunduğu görülmektedir. Bunu EBY temelli risk eylem planı oluşturulması (N=4), müeyyide koyma (N=4) ve ulusal belge yönetim stratejisinin belirlenmesi (N=4) takip etmektedir. Yerli-milli bulut ağı kullanımı/dış teknoloji kullanmama (N=3), firma bağımlılığının engellenmesi (N=2), kurumsal yapılanma (N=2), planlı eğitim (N=2) gibi öneriler de dikkat çekmektedir.

Elektronik belge yönetim temelli risk eylem planlarının oluşturulmasının akademisyen/uzmanlar tarafından sıklıkla dile getirilen bir öneri olduğu görülmektedir. Kurumlarda buna yönelik çalışmaların varlığını ölçmek adına kurum EBYS temsilcilerine "Kurumlarının EBYS temelli bir risk yönetim yaklaşımının olup olmadığı" sorulmuştur. Alınan cevaplar Şekil 2'de gösterilmektedir.

Şekil 2

Risk yönetimi yaklaşımı



Şekil 2 incelendiğinde, risk yönetim yaklaşımına katılımcıların 4'ünün var, 5'inin kısmen ve 4'ünün yok olarak yanıt verdiği görülmektedir. Kısmen cevabını veren kurumlar mevcut mevzuat ve standartlar çerçevesinde bir risk yönetim yaklaşımı geliştirdiklerini ifade etmiştir. Risk yönetim yaklaşımına sahip olmayan 4 kurumun EBYS temsilcilerine, "böyle bir yaklaşım geliştirilmesi durumunda hangi alanlara odaklanılması gerektiği" sorusu yöneltilmiştir. Katılımcılardan K1, öncelikle EBYS'nin doğru anlaşılması gerektiğini, bu sistemin yalnızca yazı yazma ve dağıtım yapma fonksiyonunun ötesinde, süreç yönetiminin de etkin bir şekilde işletilebileceği bir yapıya kavuşturulması gerektiğini belirtmiştir. Katılımcı K5 ise, yalnızca personel eğitiminin sürecin sağlıklı bir şekilde işlemesini sağlamadığını, yöneticilerin de bu süreci sahiplenmesi gerektiğini ve böyle bir yaklaşımın en üst düzeyden başlaması gerektiğini vurgulamıştır.

Tartışma

EBYS, kurum ve kuruluşlarda resmi iletişimi sağlayan ve yapılan faaliyetleri sistematik bir şekilde yöneten önemli bir yapıdır. Kurumlardaki her birim tarafından kullanılan bu sistemlerde çeşitli faktörlerden kaynaklanan pek çok risk meydana gelebilmektedir.

Risk yönetimi, EBYS'lerin başarısı için üzerinde yoğunlaşılması gereken konulardan biridir. Yetersiz bütçe, iletişim ve koordinasyon problemi, iş gücü eksikliği ve özensiz bir planlama EBYS projesinin sürdürülebilirliği üzerinde risk teşkil etmektedir. EBYS yazılımı ister bir firmadan tedarik edilmiş olsun isterse de kurum bünyesinde geliştirilmiş olsun organizasyonlar uyumluluk, verimlilik, dokümantasyon, organizasyonel iletişim, eğitim ve proje yönetimi gibi konularda risk etkenlerini konu edinen ve buna ilişkin önlemlere yer verilen detaylı bir risk yönetim planlamasına sahip olmalıdır (Yalçınkaya, 2016, ss. 76, 85-86). Araştırma kapsamında ülkemizdeki EBYS risk yönetimi uygulamalarının mevcut durumunu anlamak amacıyla görüşme yapılan katılımcılardan veri toplanmıştır. Elde edilen veriler, EBYS risk yönetimi uygulamaları konusunda kurumlar arasında önemli farklılıklar olduğunu ortaya koymaktadır. Çalışmanın "Bulgular" bölümündeki "Risklerin Tespiti ve Yönetimine Yönelik Öneriler" alt başlığında bulunan Şekil 2'ye göre, incelenen 13 kurumdan 4'ü risk yönetimi konusunda planlı-programlı bir şekilde hareket ederken 5 kurum kısmi ve düzensiz bir yaklaşım sergilemektedir. Diğer 4 kurumda ise EBYS'de risk yönetimine yönelik herhangi bir uygulama veya plan bulunmamaktadır. Bu nedenle Türkiye'deki kurumların önemli bir kısmının EBYS risk yönetimi konusunda yeterli plan ve programa sahip olmadığı ifade edilebilir. Risk yönetimi konusunda hiçbir çalışma yürütmeyen kurumların sayısının oldukça yüksek olması ise bu alanda ciddi bir iyileştirme yapılması gerektiğine işaret etmektedir. EBYS'leri destekleyici nitelikte, iyi tasarlanmış bir risk yönetim sisteminin, EBY sistem ve süreçlerine entegre edilmesi alandaki sorunların çözümüne katkı sağlayabilir. Bu uygulamayla her bir riskin meydana gelmesinden bertaraf edilmesine kadar olan (yaşam döngüsünün) sürecin yönetilmesi mümkün hale gelecektir (Kiedrowicz ve Stanik, 2015, s. 239).

Literatürde yer alan çalışmalar, başarılı bir belge yönetiminin etkin risk yönetimi uygulamaları sayesinde risklerin azaltılmasıyla oldukça güçlü bir bağı olduğuna dikkat çekmektedir (Tumuhairwe ve Ahimbisibwe, 2016, ss. 86-87). Bu bağlamda, ülkemizdeki kurumlarda planlı-programlı risk yönetimi çalışmalarının yetersiz olması (Bkz. Şekil 2), EBY uygulamalarının genel başarısının da düşük olmasıyla ilişkilendirilebilir. Ülkemizdeki kurumların belge yönetim sistem ve süreçlerinde ciddi sorunların olduğuna işaret eden bu durum, başta hukuki riskler olmak üzere pek çok önemli potansiyel riskin bulunduğu şeklinde yorumlanmaktadır. Araştırma bulguları (Bkz. Tablo 5), uluslararası belge yönetim standartlarının uyarlanmaması, belgenin delil değerinin ispatlanamaması, e-imza güvenliğinin sağlanamaması, kurumsal belge yönetimi için güncel mevzuatın takip edilmemesi ve uzman personel istihdamının yetersizliği gibi hususların ciddi hukuki riskleri beraberinde getirdiğini ortaya koymaktadır. Kurum ve kuruluşların yasal uyumluluğu sağlamak ve idari-mali yaptırımlarla karşılaşmamak adına söz konusu unsurlarda iyileştirme yapmaları son derece önemli görülmektedir.

Bilgi ve belge güvenliği için politikalar, talimatlar, prosedürler ve formlar oluşturmalı, risk analizleri yapılmalı, riskleri önlemek amacıyla tedbirler alınmalı ve bu önlemler sürekli gözden geçirilmelidir (Yılmaz ve Özdemirci, 2019, s. 57). Araştırma

bulguları beklenmedik olayların risk oluşturma sebebinin başında önlem eksikliği geldiğine işaret etmektedir (bkz. Tablo 1). Önlem eksikliği sonucunda beklenmedik olayların, en çok risk yaratacağı alanlar ise veri kaybı ve veri güvenliğidir. Bu durum kurumların önlem alma konusunda yetersiz olduğunu, EBYS'ye yönelik olağanüstü hâl senaryolarını geliştirmediğini göstermektedir. Bunun neticesinde sistemdeki çok değerli veriler kaybolabilir veya güvenliği tehlikeye düşebilir. Bu nedenle kurumlar beklenmedik olayların oluşturabileceği riskler dâhil olmak üzere her türlü riski ortaya çıkmadan bertaraf edebilmek ya da ortaya çıktığı takdirde en az zararla atlatabilmek amacıyla gerekli önlemleri almalıdır. Ayrıca bu önlemleri düzenli olarak gözden geçirmeli, gerektiği takdirde güncellemeli ve bunun için bir denetim mekanizması geliştirmelidir.

Araştırma bulguları (bkz. Tablo 2) teknolojik risklerin katılımcılar tarafından üzerinde önemle durulan bir konu olduğunu göstermektedir. Yeni teknolojilerin getireceği riskler arasında güvenlik/gizlilik, teknolojik altyapının yetersizliği ve yapay zekâ için hazırlanan veri seti riskleri ön plana çıkmaktadır. Özellikle günümüzün en popüler konusu, yapay zekâ teknolojisinin giderek daha fazla bilgi sistemine entegre edilme eğilimi, söz konusu teknolojinin EBYS'ye entegrasyonunda bilgi gizliliği ve veri ihlali gibi potansiyel birçok riski akıllara getirmektedir. Mooradian (vd., 2025, s. 157), kurum ve kuruluşların iş yapma biçimlerini iyileştirmek amacıyla yapay zekâyı giderek daha fazla benimsediğine dikkat çekmektedir. Yapay zekânın sağladığı pek çok fayda olsa da başta veri gizliliği olmak üzere birçok riski de beraberinde getirmektedir. Bu nedenle araştırmacılar, belgeler, iş zekâsı verileri, e-postalar, sözleşmeler, makine öğrenimi modellerinin eğitimi için kullanılan veriler ve dijital medya platformlarındaki veriler gibi tüm veri ve bilgi türlerini yönetmek için risk temelli bir yaklaşım sergilenmesi gerektiğini vurgulamaktadır. Uygulamacılar yapay zekâ araçlarını ve tekniklerini uygulamadan önce uygun araçları ve yöntemleri anlayarak kurum bilgi sistemine entegre etmelidir.

Giderek gelişen teknolojinin mevcut uygulamalara entegrasyonu, birçok risk unsurunu ortaya çıkarmaktadır. Araştırma bulguları (Tablo 2), teknolojik değişimin meydana getirebileceği risklerin yaratacağı etkiler arasında güvenlik, erişim, belgenin delil değerinin ve bütünlüğünün bozulması gibi önemli endişelerin olduğunu göstermektedir. Teknolojinin gelişimi ve yaygın kullanımıyla birlikte, bilgi güvenliğinin önemli bir konu haline geldiğini işaret eden Güler ve Furat (2022, s. 81), güvenlik eksikliğinin belgenin gizliliği, bütünlüğü ve kullanılabilirliği üzerinde ciddi tehditler yaratacağına değinmiştir. Bu durum teknolojik gelişmelere paralel olarak EBYS uygulamalarına yeni teknolojilerin entegrasyonunda risk yönetimine özen gösterilmesi gerektiği şeklinde yorumlanabilir. Aksi takdirde, sistemi derinden etkileyen potansiyel tehditlerin gün yüzüne çıkması kaçınılmaz olacaktır.

EBYS'lerde SDP kodlarının atanmasında yapılan hatalar, belge yaşam döngüsünde sorunlara neden olmaktadır (Binici, 2019, ss. 119-120). Genellikle personelin eğitim

eksikliği ya da dikkatsizliği nedeniyle gerçekleşen yanlış kod atamalarının beraberinde getirdiği risklerin başında (bkz. Tablo 6) belgelere erişimde yaşanan teknik sorunlar yer almaktadır. Bu durum ayrıca tasfiye ve imha süreçlerini olumsuz etkilemekte, yanlış imhaya ve yasal yükümlüklerin sağlanamamasına neden olmaktadır. Bu nedenle SDP kodlama hatalarının önüne geçebilmek amacıyla personele bilgi ve farkındalık eğitimlerinin verilmesi, belgelere doğru SDP numaralarının verilmesinde personeli yönlendirici bir takım sistemsel önlemler alınması (ör. makine öğrenmesi) önemli görülmektedir (Binici, 2019).

Belge yaşam döngüsünde, bir belgenin üretiminden tasfiyesine ve hatta arşiv yönetimine kadar birçok iş süreci vardır. Bu süreçte tasfiye işlemi yalnızca kurumları değil milli arşivi de ilgilendirmektedir. Çünkü kamu kurumları saklanması gereken belgelerin bir kısmını kendi bünyesinde muhafaza ederken diğer kısmını da milli arşivlere devretmektedir. Elektronik ortamda ise tasfiye sürecinin doğru işletilebilmesi için altyapı sorunları ve önemli belirsizlikler mevcuttur (Çiçek, 2021, s. 52) Araştırma bulguları (bkz. Tablo 6) tasfiye işlem belirsizliklerinin meydana getirebileceği risklerin, belge yaşam döngüsünün tamamlanmasının önünde büyük bir sorun teşkil ettiğini ortaya koymaktadır. Belge/veri kaybı, gereksiz saklama, süreci işletememe, yasal riskler ve yanlış imha tasfiye sürecinin doğru işletilememesinin ortaya çıkarabileceği önemli risklerdir. Tasfiye süreci için ülkemizde belge yönetimi alanında mevzuat geliştirici kurum olan Devlet Arşivleri Başkanlığının yol göstermesi gerekmektedir. Araştırma bulguları Başkanlığın pasif kaldığına ve yeterli alt yapıya sahip olmadığına işaret etmektedir. Bu durum EBYS standartlarını ortaya koyan Devlet Arşivleri Başkanlığının eksiklikleri tamamlamak ve belirsizlikleri çözmek adına daha aktif çalışması gerektiğini göstermektedir.

Sonuç ve Öneriler

Fiziksel ortamda sürdürülen belge yönetiminin elektronik ortama taşınmasıyla hem geleneksel ortamdan elektroniğe geçiş sürecinde hem de sonrasında yaşanan belirsizlikler, eksiklikler ve hatalar pek çok risk unsurunu beraberinde getirmiştir. Sistemin doğasından kaynaklanan riskler olduğu gibi kullanıcıdan kaynaklı risklerin de ciddi boyutta sistem işleyişini etkilediği görülmüştür. Ayrıca organizasyonel değişiklikler, mevzuat, politika eksikliği gibi kurumun iç yapısını etkileyen unsurlar ile insan müdahalesi dışında gerçekleşen olaylar da önemli derecede risk meydana getirmiştir. Elektronik belgenin üretiminden arşivlenmesine, erişiminden imhasına kadar tüm süreçlerde çeşitli riskler olduğu ortaya çıkmıştır. Bu doğrultuda çalışma ülkemizdeki kurum ve kuruluşların EBYS ve süreçlerinde karşılaşabileceği risk unsurlarını değerlendirmiş ve kategorize etmiştir. Bu kapsamda literatür değerlendirmesinden ve yapılan görüşmelerden aşağıdaki sonuçlara ulaşılmıştır:

- Araştırmada merak edilen ilk temel soru, Türkiye'deki kurumların EBYS'ye

yönelik politikalar oluşturup risk yönetim mekanizmalarını hayata geçirip geçirmediğidir. Bu inceleme, ülkemizdeki EBYS risk yönetimi uygulamalarının mevcut durumunu anlamak açısından önemli görülmüştür. Elde edilen veriler, kurumların pek çoğunda EBYS'ye yönelik politika ve prosedürlerin oluşturulmadığı, EBYS'de risk yönetimine yönelik kısmi çalışmaların yürütüldüğü ya da hiçbir uygulamanın bulunmadığı anlaşılmıştır.

- Bu araştırmanın temel gerekçelerinden biri EBYS'deki risklerin yönetimine ilişkin yapılması gerekenlerin tespit edilmesidir. Bu nedenle "*Kurumlarda EBYS'deki risklerin yönetimine ilişkin yapılması gerekenler nelerdir?*" sorusuna yanıt aranmıştır. Gerçekleştirilen görüşmeler neticesinde kurumlarda EBYS'deki risklerin yönetimine yönelik bilgi ve belge yöneticilerinin görevlendirilmesi, elektronik belge yönetimi temelli risk eylem planının oluşturulması, ulusal belge yönetim stratejisinin geliştirilmesi, müeyyide koyma, yerli-milli bulut ağı/dış teknoloji kullanmama, kurumsal yapılanmanın sağlanması gibi hem kurumsal hem de ulusal önlemlerin alınması gerektiği anlaşılmıştır.
- Araştırmada merak edilen bir diğer konu ise EBYS ile ilgili mevcut mevzuat ve standartların yeterli olup olmadığıdır. Kurumlar, akademisyenler, alan uzmanları ve EBYS firma temsilcileriyle gerçekleştirilen görüşmeler neticesinde uluslararası belge yönetim standartlarının uyarlanması konusunda ülkemizin yetersiz olduğu ve yurtdışı düzeyinde beklenen değeri taşımadığı anlaşılmıştır. Ayrıca tasfiye işlem tanımlarının belirsizliği, ayıklama ve imha çalışmalarının yapılmaması, elektronik belge transferinin gerçekleştirilmemesi gibi altyapı eksikliğinden kaynaklı risklerin oluştuğu tespit edilmiştir.

Araştırmada yanıtı aranan sorular cevap bulmuş ve araştırma kapsamında başka sonuçlara da ulaşılmıştır. Bunlar şu şekilde sıralanabilir:

- Deprem, yangın, sel gibi beklenmedik olaylara karşı kurumların hazır olmadığı, felaket kurtarma merkezlerinin kurulmadığı ve afet eylem planlarının oluşturulmadığı anlaşılmıştır.
- Kurumlarda EBYS güvenliğine yönelik yeterli önlemlerinin alınmadığı tespit edilmiştir.
- Yapay zekâ, makine öğrenmesi vb. yeni teknolojilerin ülkemizde henüz başlangıç düzeyinde olduğu, bu teknolojilerin EBYS'ye entegrasyonunun planlı bir şekilde gerçekleştirilmesi gerektiği ve bunun için mevzuata ihtiyaç duyulduğu saptanmıştır. Aksi takdirde gizlilik, güvenlik, mahremiyet gibi konularda risklerin ortaya çıkabileceği anlaşılmıştır.
- Organizasyonel değişiklikler ve EBYS yazılım değişikliğinin kurumlarda sıkça yaşandığı ve plansız bir şekilde gerçekleşen bu yapısal değişikliklerin veri kaybı,

erişim sorunları gibi risklere neden olduğu anlaşılmıştır.

- Personel devir hızı, başta iş süreçlerinin aksaması olmak üzere, birçok riski beraberinde getirmektedir. Görevlendirilen personelin hızlı bir şekilde değişmesi ayrıca yetkisiz erişim, geçmiş belgelere erişim sorunları, uzmanlaşma eksikliği ve yanlış uygulamalar gibi risklerin ortaya çıkmasına neden olmaktadır.
- EBYS'lerde risk yönetimine ilişkin kurumsal analizlerin etkin bir şekilde yapılmadığı ve risk yönetim mekanizmalarının işletilmediği anlaşılmıştır.
- EBYS ile ilgili mevcut mevzuatın ve standartların eksik bazı yanlarının olduğu anlaşılmıştır.
- Kurum çalışanlarının bir kısmının geleneksel (fiziksel) belge yönetiminden kalan alışkanlıklarına devam etmek istediği, yeniliklere karşı bir direnç gösterdiği anlaşılmıştır.
- Belgenin üretim aşamasında atanan Standart Dosya Plan kodlarının öneminin EBYS kullanıcıları tarafından yeterince anlaşılmadığı belirlenmiştir. Ayrıca bu konuda yanlış uygulamaların olduğu ve kontrollerinin yapılmadığı anlaşılmıştır.
- Tasfiye işlem belirsizliklerinin devam ettiği, bu belirsizliklerin belge kaybı, gereksiz belge saklama ve hatalı imha gibi pek çok ciddi riski tetiklediği anlaşılmıştır.
- Bakım aksaklıklarının ve güvenlik açıklarının beraberinde getireceği risklerin başında, veri güvenliği ve yedekleme/geri yükleme gelmektedir. Bu durumun veri kaybına, hizmet kesintilerine neden olabileceği anlaşılmaktadır.

Sonuç olarak, kurum ve kuruluşlarda EBYS ve süreçlerinde pek çok potansiyel risk unsuru mevcuttur. Önlem alınmadığı takdirde kurumlara ciddi zararlar verebilecek bu unsurlar, dış ve iç faktörlere, sisteme ve süreçlere bağlı olarak çeşitlilik göstermektedir. Bu bağlamda araştırma kapsamında aşağıdaki öneriler sunulmaktadır:

- Risk yönetiminin kurum kültürünün önemli bir parçası haline gelmesi önemlidir. Bunun için kurumun en üst amiri başta olmak üzere birim amirlerinin süreci sahiplenmesi ön koşuldur. Böylece kurumlarda risk yönetimi bilincinin gelişerek stratejik önem kazanması sağlanabilir.
- Görüşme yapılan kurumların önemli bir kısmında EBYS kapsamında risk yönetimi mekanizmalarının etkin işlemediği görülmüştür. Kurumların risklerden doğabilecek zararı en aza indirebilmesi için mevcut risk yönetimi mekanizmalarını yeniden değerlendirmeleri, bağımsız denetim mekanizmaları oluşturarak gerekli yapısal iyileştirmeleri yapmaları oldukça önemlidir.
- Kurumların riskleri etkin bir şekilde yönetebilmesi için bilgi ve belge yönetimi

bölümü mezunlarının EBYS ve arşivleme süreçlerinde görevlendirilmesi önerilmektedir. Araştırma bulguları alan uzmanlarının, bilgi ve belge yönetimi mezunlarının görevlendirilmesinin yanı sıra müeyyide uygulanması, kurumsal risk yapılanması, tedarikçi bağımlılığının azaltılması ve yazılım-donanım güncellemelerinin de risk yönetimine önemli katkılar sağlayacağını vurguladığını göstermektedir. Dolayısıyla kurumların risk stratejilerini belirlerken söz konusu unsurları göz önünde bulundurması gerekmektedir.

- EBYS'nin sürdürülebilirliğini ve sürekliliğini tehdit eden risklerin başında teknolojik altyapı sorunları ve kurumsal/yönetimsel sorumlulukların belirsizliği gelmektedir. Ayrıca, e-imza uygulamalarındaki riskler, tedarikçi firma bağımlılığı, yetkin personel eksikliği ve maliyet ciddi risk alanlarındandır. Bu nedenle kurumların teknolojik altyapısını iyileştirmeleri, gerekli güvenlik önlemlerini almaları oldukça önemlidir. Ayrıca kurum yönetiminin bu konuda gerekli desteği sağlaması, EBYS sorumlularının belirlenerek organizasyonel ve sistemsel yapılanmaya destek vermesi gerekmektedir. Bunların yanı sıra felaket kurtarma planları hazırlanmalı, düzenli güvenlik denetimleri ve veri güvenliği testleri periyodik olarak gerçekleştirilmelidir. Farklı lokasyonlarda felaket kurtarma merkezleri oluşturularak afetlerden etkilenme düzeyleri minimuma indirilmelidir.
- Kurumlar belge yönetim sistemlerinin güvenliğini incelemek için risk değerlendirmesi, erişim kontrolü, şifreleme gibi çeşitli güvenlik kontrollerini içeren ISO 27000 standart serisine başvurmalıdır. Bu standartlar, fiziksel güvenliğin yanı sıra veri gizliliği, bütünlüğü, kullanılabilirliği gibi alanları kapsamaktadır. Ayrıca bulut bilişim ve mobil cihazların yaygınlaşmasıyla birlikte gelen riskler ile siber güvenlik konularını içeren bu standartların kurumlar tarafından değerlendirilmesi önemlidir.
- Ulusal ölçekte belge yönetimine ilişkin risk yönetim stratejilerinin belirlenmesi büyük önem taşımaktadır. Araştırma bulguları, ulusal belge yönetim stratejisinin oluşturulması, yerli-milli bulut ağının kullanılması ve standartların uygulanmasının sağlanması konularında ülke çapında önlemler alınması gerektiğini ortaya koymaktadır. Bu bağlamda ülkemiz belge yönetimi alanında yetkili kurumların başında gelen Devlet Arşivleri Başkanlığı'nın Cumhurbaşkanlığı'nın ilgili birimleri (Belge Yönetim Daire Başkanlığı, Dijital Dönüşüm Ofisi gibi), Sanayi ve Teknoloji Bakanlığı, Bilgi Teknolojileri ve İletişim Kurumu gibi kurumlarla iş birliği yapması gerekmektedir. Bu iş birliği neticesinde yerli-milli teknolojinin geliştirilerek elektronik belge yönetim sürecinin güvenli ve etkili bir şekilde işletilmesi sağlanmalıdır.
- EBYS risk yönetimini konu edinen politika ve rehberler oluşturulmalıdır. Bu süreçte öncelikle mevcut durum analiz edilmeli, ihtiyaçlar ve eksiklikler tespit edilmelidir. Söz konusu belgeler ilgili mevzuata uygun olmalı, çalışanlar sürece

dâhil edilmeli ve herkes tarafından kolayca anlaşılabilir şekilde hazırlanmalıdır. Tablo, akış şemaları ve örneklerle desteklenmelidir. Sistem ve süreçlerdeki değişikliklere göre güncellenmelidir. Belge yönetimi süreçleri, belgenin oluşturulmasından imhasına kadar adım adım açıklanmalı, yetkilendirme, erişim, veri güvenliği ve yedekleme gibi konuları içeren kapsamlı bir güvenlik planı hazırlanmalıdır. Bu plan Bilgi Güvenliği Yönetim Sistemi (BGYS) yaklaşımı ile Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Rehberi dikkate alınarak oluşturulmalı ve yöneticiler tarafından benimsenmelidir.

- Her belge türü için saklama süreleri açıkça belirlenmelidir. Birimlerin ve çalışanların sorumlulukları ayrıntılı bir şekilde tanımlanmalıdır. Personel hatalarının tespit edilebilmesi için düzenli denetimler ve sistem kontrolleri yapılmalıdır. Denetimler sonucu başarılı uygulamalar ödüllendirilmeli, sorun teşkil eden uygulamalar ise soruşturmaya tabi tutulmalıdır. Risk oluşturan eylemler için kurumun yönerge veya yönetmeliği doğrultusunda yaptırımlar uygulanmalıdır.
- EBYS kullanıcılarına uzaktan yardım sağlamak için sıkça sorulan sorular, arama motoru, eğitim materyalleri ve canlı destek gibi geleneksel yöntemler kullanılmaktadır. Bu tür hizmetlerin birim üzerindeki iş yükünü artırdığı göz önünde bulundurulduğunda daha yenilikçi çözümlerin uygulanması önemli görülmektedir. Yapay zekâ, veri analitiği ve bulut teknolojileri gibi yenilikçi çözümler, bir taraftan sistemin kullanıcı dostu hale gelmesine diğer taraftan da destek ekibinin iş yükünün azalmasına yardımcı olacaktır. Özellikle 7/24 hizmet verebilen, kişiselleştirilmiş destek sunabilen ve kullanıcıların soru/sorunlarına hızlı yanıt üretebilen bir sohbet robotunun kullanıcı deneyimini iyileştirebileceği düşünülmektedir. Bu robot gelen sorular doğrultusunda sürekli geliştirilmeli, gerektiğinde kullanıcıları uzman personele yönlendirebilecek şekilde tasarlanmalıdır. Bunun yanı sıra kullanıcıların sistemle etkileşimlerini analiz ederek öneriler sunabilmeli, otomatik hata tespiti yapabilmelidir. Bu sayede destek birimine ihtiyaç duyulmadan birçok problemin çözülmesi mümkün hale gelebilir.
- Kurumlarda, Ankara Üniversitesi BEYAS Koordinatörlüğü veya Cumhurbaşkanlığı Bilgi ve Belge Yönetim Daire Başkanlığı örneklerinde olduğu gibi en az müdürlük seviyesinde elektronik belge yönetimi birimi kurulmalıdır. Ayrıca her birim için belge yöneticileri atanmalı ve bu kişilere gerekli yetkiler tanımlanmalıdır. Belge yöneticilerinin EBYS ve risk yönetimi konusunda kapsamlı eğitimler alması sağlanmalıdır. Ayrıca belge oluşturma, güncelleme ve imha gibi süreçler için iş akışları oluşturulmalıdır. Belgelere erişim yetki matrisleri üzerinden kontrol edilerek güvenli bir yönetim tasarlanmalıdır.
- EBYS'de dosyalama yapılırken özellikle SDP kodunun verilmesi aşamasında sıkça hata yapıldığı gözlemlenmektedir. Bu durum belgelerin yaşam döngüsünün

tamamlanamamasına neden olmaktadır. Her ne kadar gizlilik, güvenlik, mahremiyet gibi riskleri beraberinde getirse de yapılan bilimsel çalışmalar makine öğrenmesi tekniklerinin, belgelere otomatik standart dosya planı atanması konusunda başarılı olduğunu göstermektedir. Bu amaçla oluşturulan bir makine öğrenmesi uygulamasının EBYS ile entegrasyonu, aynı konulardaki belgelere verilen dosya plan kodlarında standartlaşmayı sağlayacağı gibi kodların doğruluğunu da artırabilir. Bu entegrasyon sürecinde söz konusu risklerin gözetilmesi, uygulama tasarımında ve EBYS entegrasyonunda kontrollü davranılması, sonraki süreçte sürekli izlenmesi ve risk oluşturan alanlara müdahalede bulunulması alandaki sorunların çözümüne katkı sağlayacağı gibi risklerin azaltılmasına da yardımcı olacaktır.

- Kurumlarda halen üretilen elektronik belgenin fiziki çıktısı alınarak dosyalandığı görülmektedir. Bu durum bir taraftan israfa neden olurken diğer taraftan Cumhurbaşkanlığının 19.03.2024 tarihli, E-67915368-805.01-213492 sayılı ve Elektronik Ortamda Üretilen Belgelerin Çıktısının Alınmaması ve e-İmza Kullanımı konulu yazısına aykırı uygulama yapılması anlamına gelmektedir. Verimliliği artırmak ve kaynakları daha etkin kullanmak amacıyla kurum yönetimi tarafından tüm birimlere duyurulacak bir karar ile fiziki belge kullanımının en aza indirilmesi hedeflenmelidir. Bu hedef doğrultusunda caydırıcılığın sağlanması için yaptırımlar belirlenmeli ve uygulanmalıdır.
- Alanda gözlemlenen bir diğer önemli sorun da birçok kurumda dosya tasnif planı ile sisteme dâhil edilen her bir eleman için saklama planında bir saklama süresi ve tasfiye işleminin tanımlanmamış olmasıdır. TS 13298 Standardında belirtilmesine rağmen uygulamada gözlemlenen bu eksiklikler belge yönetimini önemli ölçüde sekteye uğratmaktadır. Bu nedenle saklama planları EBYS'ye entegre edilerek saklama süreleri ile tasfiye işlem tanımları yapılmalıdır. EBYS bünyesinde tanımlanan saklama planları, sistemdeki tüm verilerin saklama sürelerini belirleyen, bu sürelerin düzenli olarak raporlanmasını sağlayan ve saklama süresi dolan verilerin otomatik olarak inceleme, değerlendirme ve imha/arşivleme süreçlerine dâhil edilmesini sağlayan kapsamlı bir yapıya sahip olmalıdır.
- EBYS'ler TS 13298 standardına uygun olarak geliştirilmektedir. Sistemler standardın gereksinimlerini karşılayacak teknik yapıda olmasına rağmen kurumların büyük bir kısmında EBYS ile bütünleşik çalışan bir elektronik arşivleme modülünün temin edilmediği ya da var olan modülü aktif bir şekilde kullanmadığı gözlemlenmektedir. Bu durum ihtiyaç duyulduğunda belgelere erişimi zorlaştıracağı gibi tasfiye işlemlerinin düzgün bir biçimde yapılamamasına neden olmaktadır. EBYS ile bütünleşik çalışan bir elektronik arşiv modülü, kurumların belge yönetimi süreçlerini iyileştirir, verimliliği artırır ve yasal uyumluluk sağlar. Bu modül sayesinde kurumlar önemli belgelerini

güvenli bir şekilde saklayabilir, ihtiyaç duyduklarında belgelere hızlıca erişebilir ve depolama maliyetlerini düşürebilirler. Bu bağlamda Devlet Arşivleri Başkanlığı, elektronik belgelerde tasfiye işlemlerinin nasıl yapılacağına dair bir rehber hazırlamalı, kurumlarda saklama süresi dolmuş arşiv belgesi niteliğindeki belgelerin milli arşive kazandırılmasını sağlamalı ve elektronik arşiv modülü kullanımı için bir talimat yayınlamalıdır.

Araştırma sonuçları kurum ve kuruluşlardaki EBYS uygulamalarının ciddi riskler barındırdığını ortaya koymaktadır. EBYS'lerde bulunması gereken özelliklere ilişkin talimatlar ve standartlar mevcut olmasına rağmen uzun yıllardır devam eden sorunların yoğun olarak uygulamadan kaynaklandığı anlaşılmaktadır. Kurumlar, EBYS uygulamalarını mevzuata ve standartlara uygun şekilde gerçekleştirmeli, iç denetim mekanizmalarını hayata geçirerek sorunların ve risklerin tespiti ve tedavisi üzerine çalışmaları ivedilikle başlatmalıdır. Aksi takdirde sorunlu uygulamaların tetikleyeceği riskler ve bunların sonuçlarıyla yüzleşmek zorunda kalacaklardır.

EBYS ekiplerinde ve birim bazında belge yöneticilerinin görevlendirilmesi, uygulamadaki eksikliklerin/hataların giderilmesi ve mevzuat-uygulama uyumsuzluğunun engellenmesi için etkili bir yöntem olarak değerlendirilmektedir. Bununla birlikte mevzuat düzenleyici ve politika geliştirici kurumların da tasfiye işlem belirsizlikleri gibi hususlarda üzerine düşen sorumlulukları yerine getirmesi, gerekli yönlendirmeleri yapması, özellikle arşiv belgesi niteliğindeki belgeler için transfer işleminin nasıl yapılacağını belirtmesi ve kurumların elektronik ortamdaki belge transferi için gerekli altyapıyı sağlaması önemli görülmektedir.

Çıkar Çatışması

Yazarlar arasında çıkar çatışması bulunmamaktadır.

Maddi Destek

Araştırmada herhangi bir maddi destek alınmamıştır.

Yazarlık Katkısı

Yazarlar makale için eşit oranda katkıda bulunmuştur.

Etik Kurul Kararları ve İzinler

Çankırı Karatekin Üniversitesi Fen, Matematik ve Sosyal Bilimler Etik Kurulu'ndan 20.12.2024 tarihli ve 49 nolu toplantıda etik kurul izni alınmıştır.

Kaynakça

Australian/New Zealand Standard [AS/NZS]. (2004). *Risk management* (AS/NZS 4360:200https://mkidn.gov.pl/media/docs/pol_obronna/20150309_3-NZ-AUST-2004.pdf

Barnawi, A. O. (2013). *Risk management of electronic health record system in hospitals* [Yayımlanmamış doktora tezi]. De Montfort Üniversitesi.

Binici, K. (2019). Makine öğrenmesi yaklaşımıyla e-belgelere standart dosya plan numaralarının otomatik olarak atanması üzerine bir çalışma. *Bilgi Yönetimi, 2*(2), 116-126. https://doi.org/10.33721/by.654464

Çiçek, N. (2021). Türkiye'de elektronik belgelerin geleceği için ulusal strateji ihtiyacı: Literatür ışığında bir inceleme. *Bilgi ve Belge Araştırmaları Dergisi,* (15), 33-57. https://doi.org/10.26650/bba.2021.15.02

Dişli, M. ve Külcü, Ö. (2020). Üniversitelerde elektronik belge yönetim sistemlerinin birlikte çalışabilirlik açısından değerlendirilmesi. *Bilgi Dünyası, 21*(1), 35-63. https://doi.org/10.15612/BD.2020.781

e-Yazışma Projesi (2017, 14 Ekim). *T.C. Resmî Gazete* (No: 30210). https://www.resmigazete.gov.tr/eskiler/2017/10/20171014-11.pdf

Gibson, N. (2011). *Risk and records management: Investigating risk and risk management in the context of records and information management in the electronic environment* [Yayımlanmamış doktora tezi]. University of Northumbria at Newcastle.

Güler, C. ve Furat, F. (2022). Belge yönetimi ve arşiv uygulamalarının bilgi güvenliği ilkelerine katkısı: Kavramsal bir değerlendirme. *Türk Kütüphaneciliği, 36*(1), 74-89. https://doi.org/10.24146/tk.1012325

Hazine ve Maliye Bakanlığı. (2024). *Kamu kurumsal risk yönetimi rehberi*. https://ms.hmb.gov.tr/uploads/2024/04/Kamu-Kurumsal-Risk-Yonetimi-Rehberi-2024.pdf

International Council on Archives [ICA]. (2008). *Principles and functional requirements for records in electronic office environments: Module 1-Overview and statement of principles*. https://www.naa.gov.au/sites/default/files/2019-09/m1-ica-overview-principle-and-functional-requirements_tcm16-95418.pdf

International Organization for Standardization [ISO]. (2014). *Information and documentation - Risk assessment for records processes and systems technical report* (ISO Standard No. 18128:2014).

International Organization for Standardization [ISO]. (2016). Information and documentation —Records management — Part 1: Concepts and principles (ISO Standard No. 15489-1:2016).

International Organization for Standardization [ISO]. (2018). *Risk management guidelines* (ISO Standard No. 31000:2018).

International Organization for Standardization [ISO]. (2020). *Information and documentation - Processes and functional requirements for software for managing records* (ISO Standard No. 16175-1:2020).

Kiedrowicz, M. ve Stanik, J. (2015). Selected aspects of risk management in respect of security of the document lifecycle management system with multiple levels of sensitivity. B. F. Kubiak ve J. Maślankowski (Ed.) *Information management in practice* içinde (ss. 231-249).

Laine, V., Goerlandt, F., Banda, O. V., Baldauf, M., Koldenhof, Y. ve Rytkönen, J. (2021). A risk management framework for maritime pollution preparedness and response: Concepts, processes and tools. *Marine Pollution Bulletin*, *171*, 2-22. https://doi.org/10.1016/j.marpolbul.2021.112724

Lin, C. M. (2020). Establishing the risk assessment indicators of electronic records and empirical analysis of an institution. *Journal of Library and Information Studies, 18*(1), 69-96. https://doi.org/10.6182/jlis.202006_18(1).069

Marutha, N. (2022). Rethinking the movement to get moving: Archives and records in the era of disruptions. *Mousaion: South African Journal of Information Studies, 40*(3). https://doi.org/10.25159/2663-659X/13490

Miles, M. B., Huberman, A. M. ve Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3. bs.). SAGE Publications. https://www.metodos.work/wp-content/uploads/2024/01/Qualitative-Data-Analysis.pdf

Mooradian, N., Franks, P.C. and Srivastav, A. (2025), The impact of artificial intelligence on data privacy: A risk management perspective. *Records Management Journal, 35*(2), 147-159. https://doi.org/10.1108/RMJ-06-2024-0013

Odabaş, H. (2005). Belge yönetimi ve Türkiye'de belge yönetimi gereksinimi. *Bilgi Dünyası, 6*(1), 36-57. https://doi.org/10.15612/BD.2005.446

Oxford University Press. (2023). Risk. *Oxford Learner's Dictionaries*. https://www.oxfordlearnersdictionaries.com/definition/english/risk_1?q=risk

Özdemirci, F. (2019). Kurumlar için EBYS ve e-arşiv sistemi idari yapılanma ve yönetim süreci: Bileşenler ve entegrasyonlar. B. Yalçınkaya, M.A. Ünal, B. Yılmaz ve F. Özdemirci (Ed.) *Bilgi yönetimi ve bilgi güvenliği: ebelge-earşiv-edevlet-bulut bilişim-büyük veri-yapay zekâ* içinde (ss. 3-9). Ankara Üniversitesi Bilgi Yönetim Sistemleri Belgelendirme ve Bilgi Güvenliği Merkezi.

Renn, O. (1998). Three decades of risk research: Accomplishments and new challenges. *Journal of Risk Research*, *1*(1), 49-71. https://doi.org/10.1080/136698798377321

Sağlık, Ö. (2021). *Elektronik belge yönetimi uygulamalarındaki koşullar ışığında e-imzalı belgelerin delil değerinin arşivsel güvenilirlik açısından incelenmesi* [Yayımlanmamış doktora tezi]. İstanbul Üniversitesi.

Salgotra, P., Nirupama, E., L. B., M, Srivastava, A., Lourens, M. ve Sable, A. (2025, Ağustos 22-23). *Machine learning for risk management: Identifying and mitigating business risks*. [Tam Metin]. World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS), Indore, India, 1-6, https://doi.org/10.1109/WorldSUAS66815.2025.11199089

Srinivas, K. (2018). Process of risk management. A. G. Hessami (Ed.), *Perspectives on risk, assessment and management paradigms* içinde. IntechOpen. https://doi.org/10.5772/intechopen.80804

Tumuhairwe, R. ve Ahimbisibwe, A. (2016). Procurement records compliance, effective risk management and records management performance: Evidence from Ugandan public procuring and disposing entities. *Records Management Journal, 26*(1), 83-101. https://doi.org/10.1108/RMJ-06-2015-0024

Türk Dil Kurumu. (2024). Risk. *Güncel Türkçe Sözlük*. https://sozluk.gov.tr/

Usman, Ö. ve Kaygusuz, S. Y. (2019). Kurumsal risk yönetiminde uygulanması gereken adımlar. *Muhasebe ve Denetime Bakış,* (56),109-128. https://dergipark.org.tr/tr/pub/mdbakis/issue/63889/967151

Yalçınkaya, B. (2015). Elektronik belge yönetimi (EBY) uygulamalarında başarıyı olumsuz etkileyen risk unsurları. *Bilgi ve Belge Araştırmaları Dergisi,* (4), 20-40. https://dergipark.org.tr/tr/pub/bel/issue/25183/413405

Yalçınkaya, B. (2016). Elektronik belge yönetim sistemi (EBYS) uygulamalarında başarı faktörü ve fayda analizi. *AJIT-e: Online Academic Journal of Information Technology,* (7), 23. https://doi.org/10.5824/1309-1581.2016.2.006.x

Yıldırım, A. ve Şimşek, H. (2018). *Sosyal bilimlerde nitel araştırma yöntemleri*. Seçkin Yayıncılık.

Yıldız, Ö. R. (2010). Elektronik belge yönetim sistemleri ve denetim. *Sayıştay Dergisi*, (78), 3-29. https://dergipark.org.tr/tr/pub/sayistay/issue/61533/919015

Yılmaz, B. ve Özdemirci, F. (2019). Bilgi güvenliği yönetim sistemi (BGYS) sürecinde bilgi güvenliği temelli EBYS yönetimi. B. Yalçınkaya, M. A. Ünal, B. Yılmaz, F. Özdemirci (Ed.), *Bilgi yönetimi ve bilgi güvenliği: ebelge-earşiv-edevlet-bulut bilişim-büyük veri-yapay zekâ* içinde (ss. 45-59). Ankara Üniversitesi Bilgi Yönetim Sistemleri Belgelendirme ve Bilgi Güvenliği Merkezi.