



T.C.
ÇANKIRI KARATEKİN ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
BİLGİ VE BELGE YÖNETİMİ ANABİLİM DALI

**Kurum ve Kuruluşlarda Elektronik Belge Yönetim
Sistemi Risk Unsurları ve Eğitimi: Çankırı Karatekin
Üniversitesi Örneği**

Nagihan Gönül EROĞLU

DOKTORA TEZİ

Danışman
Prof. Dr. Coşkun POLAT

Çankırı – 2025

T.C.
ÇANKIRI KARATEKİN ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
BİLGİ VE BELGE YÖNETİMİ ANABİLİM DALI

**Kurum ve Kuruluşlarda Elektronik Belge Yönetim
Sistemi Risk Unsurları ve Eğitimi: Çankırı Karatekin
Üniversitesi Örneği**

Nagihan Gönül EROĞLU
ORCID: 0000-0003-2215-5073

DOKTORA TEZİ

Danışman
Prof. Dr. Coşkun POLAT

Çankırı – 2025

İÇİNDEKİLER

Sayfa

BİLİMSEL ETİK BİLDİRİMİ.....	iv
TEZ KABUL VE ONAY	v
ÖNSÖZ	vi
ÖZET.....	viii
ABSTRACT.....	ix
KISALTMALAR	x
TABLO LİSTESİ.....	xii
ŞEKİL LİSTESİ.....	xiv
1. GİRİŞ.....	1
1.1. Araştırmanın Konusu	1
1.2. Araştırmanın Amacı ve Önemi.....	3
1.3. Araştırma Soruları ve Hipotez.....	4
1.4. Literatür Özeti	5
1.5. Araştırmanın Yöntemi	12
1.5.1. Yöntem	12
1.5.2. Araştırmanın Sınırlılıkları	15
1.5.3. Araştırmanın Örneklemi.....	16
2. EBYS'DE RİSK YÖNETİM SÜRECİ	19
2.1. Risk Değerlendirmesi	22
2.1.1. Risk Tanımlaması.....	24
2.1.1.1. Dış Etkenlere Bağlı Riskler	26
2.1.1.1.1. Siyasi-Toplumsal Bağlamdaki Değişiklikler.....	27
2.1.1.1.2. Makro Ekonomik ve Teknolojik Çevre.....	29
2.1.1.1.3. Fiziksel Çevre ve Altyapı	31
2.1.1.1.4. Dış Güvenlik Tehditleri.....	31
2.1.1.2. İç Etkenlere Bağlı Riskler	32
2.1.1.2.1. Organizasyonel Değişim	33
2.1.1.2.2. Teknolojik Değişim	34
2.1.1.2.3. İnsan Kaynakları, Yetkinlikler ve Finansman	35
2.1.1.3. Sistem Faktörüne Bağlı Riskler.....	37
2.1.1.3.1. EBYS Tasarımı.....	39
2.1.1.3.2. EBYS Bakımı	40
2.1.1.3.3. Sürdürülebilirlik ve Süreklilik.....	42
2.1.1.3.4. Birlikte Çalışabilirlik	43
2.1.1.3.5. Güvenlik	45
2.1.1.4. Elektronik Belge Yönetim Süreçlerindeki Riskler	49
2.1.1.4.1. Elektronik Belgenin Oluşturulması	52
2.1.1.4.2. Elektronik Belgenin Kullanımı	52
2.1.1.4.3. Kullanılabilirliğin Sürdürülmesi.....	53
2.1.1.4.4. Elektronik Belgenin Düzenlenmesi.....	53

2.1.1.4.5. Elektronik Belge Kontrolleri	54
2.1.1.4.6. Elektronik Belgeye Erişim	59
2.1.1.4.7. Elektronik Belgenin Saklanması	62
2.1.1.4.8. Elektronik Belgelerde Ayıklama ve İmha	63
2.1.1.5. EBYS ve Süreçlerine İlişkin Risk Tanımlamaları Kontrol Listesi.....	65
2.1.2. Risk Analizi	76
2.1.2.1. İş Etki Analizi (Business Impact Analysis).....	77
2.1.2.2. İnsan Güvenilirliği Analizi (Human Reliability Analysis).....	78
2.1.2.3. Papyon Analizi	79
2.1.3. Risk Değerlendirme ve Teknikleri	83
2.1.3.1. Makul Olarak Uygulanabilir En Düşük Seviye (As Low As Reasonably Practicable) (ALARP).....	83
2.1.3.2. Güvenilirlik Merkezli Bakım (Reliability Centred Maintenance)	85
2.1.3.3. Risk Değerlendirme Matrisleri	87
2.1.3.4. Fayda-Maliyet Analizi.....	91
2.2. Risk Müdahalesi (Risklerin Tedavi Edilmesi/Risk İyileştirmesi)	92
2.3. İzleme ve Gözden Geçirme	94
2.4. İletişim ve Danışma.....	97
2.5. Kaydetme ve Raporlama	98

3. BULGULAR 100

3.1. Risk Yönetimi Süreçlerinde Karşılaşılan Temel Sorunlara İlişkin Elde Edilen Verilerin Analize Hazırlanması.....	100
3.2. Risk Yönetimi Süreçlerinde Karşılaşılan Temel Sorunlara İlişkin Bulgular .	104
3.2.1. EBYS Kapsamında Risk Unsurlarının Tematik Dağılımı.....	104
3.2.1.1. Dış Faktörlere Bağlı Riskler	104
3.2.1.1.1. Beklenmedik Olayların Oluşturduğu Riskler	104
3.2.1.1.2. Yasal Düzenlemeler ve Politik Riskler	108
3.2.1.1.3. Yeni Teknolojilerin Riskleri.....	111
3.2.1.2. İç Faktörlere Bağlı Riskler	117
3.2.1.2.1. Elektronik Belgenin Kurum Kültüründeki Yeri	117
3.2.1.2.2. Organizasyonel Değişiklikler	119
3.2.1.2.3. Personel ve Eğitim Riskleri	121
3.2.1.2.4. Politika ve Prosedür Eksikliği	126
3.2.1.2.5. Yönetim Desteği.....	127
3.2.1.3. Sistem Faktörüne Bağlı Riskler.....	129
3.2.1.3.1. Sistem Tasarım ve Yapılandırma	129
3.2.1.3.2. Sürdürülebilirlik ve Süreklilik.....	131
3.2.1.3.3. Tedarikçi İlişkilerindeki Riskler.....	132
3.2.1.3.4. Teknik Riskler	133
3.2.1.3.5. Mevzuat/Standartlarla Uyum ve Hukuki Riskler	134
3.2.1.3.6. Bakım ve Güvenlik Riskleri	137
3.2.1.3.7. Saklama Gereksinimlerinin Yetersizliği.....	139
3.2.1.4. Belge Yönetim Sürecine Bağlı Riskler	140
3.2.1.4.1. Belge Üretim Sürecindeki Riskler.....	140
3.2.1.4.2. Belge Gönderme/Dağıtım Sorunları.....	145
3.2.1.4.3. Saklama ve Erişilebilirlik	148
3.2.1.4.4. Saklama Süreli Belgelerin Yönetimi ve İmha İşlemleri.....	150
3.2.1.4.5. Kâğıt ve Elektronik Belge Süreçlerinde Entegrasyon.....	154

3.2.1.4.6. Dijitalleştirme Sürecindeki Riskler	155
3.2.1.4.7. E-Arşiv Modülünün Olmama Riskleri	157
3.2.2. EBYS’de Karşılaşılan Riskler	160
3.2.3. Risklerin Tespiti ve Yönetimine Yönelik Öneriler	162
3.3. Eğitim Materyalinin Geliştirilmesi.....	165
3.4. Eğitim Materyalinin Etkinliğine İlişkin Bulgular.....	170
3.4.1. Normal Dağılım Analizi	172
3.4.2. Eğitimin Etkinliği	174
3.4.3. Eğitim Materyalinin Konularına Göre Performans Değerlendirmesi	175
3.4.4. Katılımcı Özelliklerine Göre Performans Değerlendirmesi	176
3.5. Tartışma.....	178
4. SONUÇ VE ÖNERİLER	186
5. KAYNAKÇA	197
EKLER.....	212
EK 1: Görüşmeler İçin Etik Kurul İzni	212
EK 2: Eğitim Materyalinin Etkinliği Testi İçin Etik Kurul İzni	213
EK 3: Kurumlar İçin Soru Formu	214
EK 4: Akademisyenler/Uzmanlar İçin Soru Formu	217
EK 5: Firmalar İçin Soru Formu	220
EK 6: Sekreterler İçin Soru Formu	223
EK 7: Eğitim Materyali	227
ÖZGEÇMİŞ.....	383

BİLİMSEL ETİK BİLDİRİMİ

Doktora tezi olarak hazırladığım *Kurum ve Kuruluşlarda Elektronik Belge Yönetim Sistemi Risk Unsurları ve Eğitimi: Çankırı Karatekin Üniversitesi Örneği* adlı çalışmanın öneri aşamasından sonuçlanmasına kadar geçen süreçte bilimsel etiğe ve akademik kurallara özenle uyduğumu, tez içindeki tüm bilgileri bilimsel ahlak ve gelenek çerçevesinde elde ettiğimi, tez yazım kurallarına uygun olarak hazırladığım bu çalışmamda doğrudan veya dolaylı olarak yaptığım her alıntıya kaynak gösterdiğimi ve yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu beyan ederim.

21/07/2025

İmza

Nagihan Gönül EROĞLU

TEZ KABUL VE ONAY

ÇANKIRI KARATEKİN ÜNİVERSİTESİ SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Nagihan Gönül EROĞLU tarafından hazırlanan *Kurum ve Kuruluşlarda Elektronik Belge Yönetim Sistemi Risk Unsurları ve Eğitimi: Çankırı Karatekin Üniversitesi Örneği* başlıklı bu çalışma, 21.07.2025 tarihinde yapılan tez savunma sınavı sonucunda *oybirliğiyle* başarılı bulunarak jürimiz tarafından *Bilgi ve Belge Yönetimi* Anabilim Dalı'nda Doktora tezi olarak kabul edilmiştir.

TEZ JÜRİSİ ÜYELERİ (Unvanı, Adı ve Soyadı)

Danışman	: Prof. Dr. Coşkun POLAT	İmza:
Üye	: Prof. Dr. Hüseyin ODABAŞ	İmza:
Üye	: Prof. Dr. Mehmet Ali AKKAYA	İmza:
Üye	: Prof. Dr. Fahrettin ÖZDEMİRCİ	İmza:
Üye	: Doç. Dr. Bahattin YALÇINKAYA	İmza:

ONAY

Bu Tez, Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Yönetim Kurulunun 02/07/2025 tarih ve 2025/27-01 sayılı oturumunda belirlenen jüri tarafından kabul edilmiştir.

Prof. Dr. Ersoy YILMAZ

Enstitü Müdürü

ÖNSÖZ

Kurum ve kuruluşların yapmış olduğu faaliyetlerin delili niteliğindeki belgelerin yönetimi günümüzde elektronik ortamda gerçekleşmektedir. Elektronik Belge Yönetim Sistemlerinin (EBYS) kullanımını zorunlu hâle getiren bu durum, sistemi kurumsal bilgi yönetim süreçlerinin merkezinde konumlandırmaktadır. Bu sistemler birçok fayda sağlarken çeşitli risk faktörlerini de beraberinde getirmektedir. Bu doktora tezinde, kurum ve kuruluşlarda EBYS’de karşılaşılabilecek risklerin belirlenmesi, değerlendirilmesi ve bu risklerin yönetimine yönelik eğitim materyali geliştirilmesi amaçlanmaktadır. Örneklem olarak belirlenen Çankırı Karatekin Üniversitesinde (ÇAKÜ) gerçekleştirilen eğitimin kurumsal risk farkındalığı artırmada etkili olduğu görülmektedir. Farklı kurumlarda uygulanabilir ve geliştirilebilir olan bu eğitim, belge yönetimi alanında önemli bir uygulama olduğu düşünülmektedir.

Uzun ve meşakkatli bu süreçte motive edici yaklaşımıyla birlikte çalışmaktan onur duyduğum, bilimsel rehberliği ve desteğiyle tezin ortaya çıkmasını sağlayan çok kıymetli tez danışmanın Prof. Dr. Coşkun POLAT’a içtenlikle teşekkür etmek isterim.

Tez sürecinin yalnızca değerlendirme aşamasında değil, planlama ve geliştirme evrelerinde de yol gösterici katkılarıyla çalışmanın şekillenmesine destek olan çok değerli jüri üyeleri Prof. Dr. Hüseyin ODABAŞ, Prof. Dr. Mehmet Ali AKKAYA, Prof. Dr. Fahrettin ÖZDEMİRCİ ve Doç. Dr. Bahattin YALÇINKAYA’ya teşekkürlerimi borç bilirim.

Bu çalışmanın hazırlanma sürecine katkı sunan tüm kişi ve kurumlara içtenlikle teşekkür ederim. Saha araştırmaları kapsamında görüşme isteğini kabul ederek zamanını bana ayıran ve yöneltile sorulara içtenlikle cevap veren tüm katılımcılara ve ÇAKÜ’de eğitime katılım sağlayan personele katkılarından dolayı teşekkür ederim.

Tezin istatistiksel kurgusunun geliştirilmesinde görüşlerini aldığım çok kıymetli akademisyen arkadaşlarıma teşekkür ederim.

Bu tez yolculuğunda kimi zaman durakladığım, kimi zaman tıklandığım, kimi zaman da pes etme noktasına geldiğim anlarda motivasyon kaynağım olan kardeşlerime ve dostlarıma teşekkür ederim.

Hayatım boyunca maddi ve manevi destekleriyle her daim yanımda olan kıymetli annem ve babama sonsuz teşekkürler...

Doktora sürecinin her aşamasında yanımda olan en büyük motivasyon kaynağım ve hayat arkadaşım Ertuğrul Burak EROĞLU'na ve "Tezin daha bitmedi mi anne?" sorusuyla beni hem gülümseten hem destekleyen hem de duygulandıran biricik oğlum Oğuz Kağan EROĞLU'na gönülden teşekkür ederim.

21/07/2025

Nagihan Gönül EROĞLU



ÖZET

Tezin Başlığı : Kurum ve Kuruluşlarda Elektronik Belge Yönetim Sistemi Risk Unsurları ve Eğitimi: Çankırı Karatekin Üniversitesi Örneği
Tezin Yazarı : Nagihan Gönül EROĞLU
Danışman : Prof. Dr. Coşkun POLAT
Anabilim Dalı : Bilgi ve Belge Yönetimi
Tezin Türü : Doktora
Kabul Tarihi : 21/07/2025

Bu çalışmada, Türkiye'deki kurum ve kuruluşlarda Elektronik Belge Yönetim Sisteminde (EBYS) risk yönetimi konusu irdelenmiştir. Çalışmanın temel amacı, elektronik belge yönetim sistem ve süreçlerindeki risklerin belirlenmesi, analiz edilmesi ve bunların azaltılmasına yönelik bir eğitim materyalinin geliştirilmesidir. Bu amaç doğrultusunda öncelikle literatürde yer alan kaynaklardan (rehberler, standartlar, akademik çalışmalar vb.) taslak bir eğitim materyali oluşturulmuştur. Ardından belge yönetimi alanında çalışmaları olan uzman/akademisyenlerden 8 kişi, örneklem olarak seçilen 13 kurum ve kuruluşta görev yapan EBYS temsilcileri ve EBYS yazılımı geliştiren 3 firma ile görüşmeler gerçekleştirilmiştir. Yarı yapılandırılmış mülakat tekniğinin kullanıldığı bu süreçte katılımcılardan elde edilen veriler MaxQDA yazılımı aracılığı ile değerlendirilmiştir. Yapılan değerlendirmeler sonucunda risklerin yönetilmesine katkı sağlayacak bir eğitim materyali geliştirilmiştir. Bu materyal, deneysel bir model çerçevesinde Çankırı Karatekin Üniversitesinde görev yapan yazışma personeline (sekreter) uygulanmıştır. Eğitimin etkinliğinin ve başarısının ölçülmesine yönelik eğitim öncesinde ve sonrasında test uygulanmıştır. Eğitime katılanların son testteki %36,8'lik genel puan artışı istatistiksel açıdan anlamlıdır. EBYS risk unsuruna yönelik konular düzeyinde yapılan değerlendirmede de son testteki başarı puanları istatistiksel olarak anlamlıdır. Eğitim sonrası bu puan artışında demografik özellikler farklılığa neden olmamakla birlikte yalnızca hizmet süresinin anlamlı olduğu anlaşılmıştır. Geliştirilen eğitim materyalinin farklı kurumlarda uygulanabilir ve geliştirilebilir olduğu sonucuna varılmıştır.

Anahtar Kelimeler: Elektronik belge, elektronik belge yönetim sistemi, risk yönetimi, belge yönetim süreçleri

ABSTRACT

Thesis Title : Electronic Records Management System Risk Elements and Training in Institutions and Organizations: Çankırı Karatekin University Example
Author : Nagihan Gönül EROĞLU
Supervisor : Prof. Dr. Coşkun POLAT
Department : Information and Records Management
Thesis Type : Ph.D
Date : 21/07/2025

This study examines the risk management in Electronic Records Management System (ERMS) in institutions and organizations in Turkey. The main purpose of the study is to develop a training material to identify, analyze and reduce risks in electronic records management systems and processes. For this purpose, a draft training material was first created from sources in the literature (guides, standards, academic studies, etc.). Then, interviews were conducted with eight experts/academics working in the field of records management, ERMS representatives working in thirteen institutions and organizations selected as a sample, and three companies developing ERMS software. In this process, where the semi-structured interview technique was used, the data obtained from the participants were evaluated through MaxQDA software. As a result of the evaluations, a training material that will contribute to the management of risks was developed. This material was applied to correspondence personnel (secretaries) working at Çankırı Karatekin University within the framework of an experimental model. A test was applied before and after the training to measure the effectiveness and success of the training. The 36.8% general score increase of the participants in the post-test is statistically significant. In the evaluation made at the level of subjects regarding the ERMS risk element, the success scores in the post-test are statistically significant. It was understood that demographic characteristics did not cause a difference in this score increase after the training, but only the service period was significant. It was concluded that the developed training material could be applied and improved in different institutions.

Keywords: Electronic records, electronic records management system, risk management, records management processes

KISALTMALAR

ALARP	As Low As Reasonably Practicable (Makul Olarak Uygulanabilir En Düşük Seviye)
AS/NZS	Australian/New Zealand Standards (Avustralya/Yeni Zelanda Standartları)
BGYS	Bilgi Güvenliği Yönetim Sistemi
BIA	Business Impact Analysis (İş Etki Analizi)
BEYAS	Ankara Üniversitesi Belge Yönetimi ve Arşiv Sistemi Koordinatörlüğü
ÇAKÜ	Çankırı Karatekin Üniversitesi
DAB	Devlet Arşivleri Başkanlığı
DETSİS	Devlet Teşkilatı Merkezi Kayıt Sistemi
e-Arşiv	Elektronik Arşiv
e-Belge	Elektronik Belge
EBY	Elektronik Belge Yönetimi
EBYS	Elektronik Belge Yönetim Sistemi
FERMA	Federation of European Risk Management Associations (Avrupa Risk Yönetimi Dernekleri Federasyonu)
FMEA	Failure Mode Effect Analysis - Hata Türü ve Etkileri Analizi
ELAS/RM	Elektronik Arşivleme Sistemi Referans Modeli
EYP	Elektronik Yazışma Paketi
FKM	Felaket Kurtarma Merkezi
HRA	Human Reliability Analysis (İnsan Güvenilirliği Analizi)
ICA	International Council of Archives (Uluslararası Arşivler Konseyi)
InterPARES	The International Research on Permanent Authentic Records in Electronic Systems (Elektronik Sistemlerde Belgelerin Özgünlüğünün Korunması Üzerine Uluslararası Araştırma Projesi)
IRMT	International Records Management Trust
ISO	International Organization for Standardization (Uluslararası Standartlar Teşkilâtı)
KAMU SM	Kamu Sertifikasyon Merkezi
KEP	Kayıtlı Elektronik Posta Sistemi
KVKK	Kişisel Verileri Koruması Kanunu
MR	Manyetik Rezonans Görüntüleme
NARA	The National Archives and Records Administration (Amerika Milli Arşivi ve Belge Yönetimi İdaresi)
OCR	Optical Character Recognition (Optik Karakter Tanıma)

ODM	Olağanüstü Durum Merkezi
PDF	Portable Document Format (Taşınabilir Doküman Formatı)
PDF/A	Portable Document Format Archive (Arşiv Taşınabilir Doküman Formatı)
PESTLE	Political (Politik), Economic (Ekonomik), Social (Sosyal), Technological (Teknolojik), Legal (Hukuki), Environmental (Çevresel)
RCM	Reliability Centred Maintenance (Güvenilirlik Merkezli Bakım)
SDP	Standart Dosya Planı
SHA	Secure Hashing Algorithm (Güvenli Özet Değeri Algoritması)
STEEPLE	Social (Sosyal), Technological (Teknolojik), Economic (Ekonomik), Environmental (Çevresel), Political (Politik), Legal (Hukuki), Ethical (Etik)
SWOT	Strengths, Weaknesses, Opportunities, Threats (Güçlü Yönler, Zayıf Yönler, Fırsatlar, Tehditler)
TBMM	Türkiye Büyük Millet Meclisi
T.C.	Türkiye Cumhuriyeti
TDK	Türk Dil Kurumu
TIFF	Tagged Image File Format (Etiketli Görüntü Dosya Biçimi)
TSE	Türk Standartları Enstitüsü
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
TÜSİAD	Türk Sanayicileri ve İş İnsanları Derneği
UDF	Universal Disk Format (Evrensel Disk Formatı)

TABLO LİSTESİ

<u>Tablo No:</u>	<u>Sayfa</u>
Tablo 2.1: EBYS’de risk yönetim süreci	19
Tablo 2.2: Risk tanımlaması	20
Tablo 2.3: Risk analizi	21
Tablo 2.4: Risklerin değerlendirilmesi	21
Tablo 2.5: Elektronik belge risklerinin kaynaklarına ilişkin örnekleri içeren kontrol listesi	66
Tablo 2.6: Risklerin etki düzeylerinin değerlendirilmesi ölçeği	80
Tablo 2.7: Risklerin gerçekleşme ihtimallerinin değerlendirilmesi	80
Tablo 2.8: Risk analizi tablosu örneği.....	81
Tablo 2.9: ALARP modeli örneği.....	84
Tablo 2.10: GMB tekniği uygulanarak bakım görevleri listesine örnek.....	86
Tablo 2.11: Risk değerlendirme tablosu	88
Tablo 2.12: Sonucun kabul edilebilirlik değerleri.....	88
Tablo 2.13: Bileşik puanlama kullanan risk indeksi sistemi örneği	89
Tablo 2.14: Maliyet/fayda seçenekleri analizi örneği	91
Tablo 3.1: Beklenmedik olaylara bağlı risk tetikleyicileri.....	105
Tablo 3.2: Beklenmedik olaylar sonucu ortaya çıkabilecek riskler	106
Tablo 3.3: Hükümet politikaları ve yasal düzenlemelerin oluşturabileceği riskler .	108
Tablo 3.4: Yeni teknolojilerin riskleri.....	112
Tablo 3.5: Teknolojik değişim riskleri.....	115
Tablo 3.6: Elektronik belgenin kurum kültüründeki yeri.....	117
Tablo 3.7: Organizasyonel değişiklik riskleri	119
Tablo 3.8: Eğitimin başarısını etkileyen risk unsurları	122
Tablo 3.9: Eğitim eksikliğinin riskleri	123
Tablo 3.10: Personel devir hızının oluşturduğu riskler.....	124
Tablo 3.11: Politika ve prosedür eksikliği riskleri	126
Tablo 3.12: Yönetim desteğine bağlı riskler	127
Tablo 3.13: Sistem tasarım ve yapılandırma riskleri	129
Tablo 3.14: Sürdürülebilirlik ve sürekliliğe ait riskler.....	131
Tablo 3.15: EBYS tedarikçi ilişkilerindeki riskler.....	132

Tablo 3.16: Yaşanan teknik riskler	133
Tablo 3.17: Hukuki riskler	134
Tablo 3.18: Bakım ve güvenlik riskleri.....	138
Tablo 3.19: Sistem saklama gereksinimleri yetersizliğinin oluşturduğu riskler	139
Tablo 3.20: Üstveri riskleri	141
Tablo 3.21: SDP hata riskleri	141
Tablo 3.22: SDP hata nedenleri	142
Tablo 3.23: Saklama ve erişilebilirlik risklerine neden olan etmenler.....	148
Tablo 3.24: Saklama ve erişilebilirlik riskleri.....	149
Tablo 3.25: Tasfiye işlem belirsizliği riskleri	151
Tablo 3.26: Kâğıt ve elektronik belge süreçlerinde entegrasyon riskleri.....	154
Tablo 3.27: Dijitalleştirme sürecindeki riskler.....	156
Tablo 3.28: E-arşiv modülünün olmama riskleri	159
Tablo 3.29: EBYS’de karşılaşılan riskler.....	160
Tablo 3.30: Risklerin tespiti ve yönetimine yönelik öneriler.....	162
Tablo 3.31: Eğitim materyalinin sunulmasının faydaları.....	164
Tablo 3.32: Katılımcıların Özellikleri.....	171
Tablo 3.33: Çarpıklık ve basıklık analizi	173
Tablo 3.34: Normallik testi	173
Tablo 3.35: Bağımlı örneklem t-testi sonuçları	175
Tablo 3.36: Konu bazında bağımlı örneklem t-testi sonuçları.....	176
Tablo 3.37: Bağımsız gruplar t-testi analizi sonuçları	177
Tablo 3.38: Tek yönlü ANOVA analizi sonuçları	178

ŞEKİL LİSTESİ

<u>Şekil No:</u>	<u>Sayfa</u>
Şekil 1.1: Risk yönetimi	2
Şekil 1.2: Araştırma süreci	15
Şekil 2.1: Risk yönetim süreci	23
Şekil 3.1: MaxQDA kodlama.....	102
Şekil 3.2: MaxQDA kod sistemi	103
Şekil 3.3: E-arşiv modülü.....	157
Şekil 3.4: Risk yönetimi yaklaşımı	163
Şekil 3.5: Q-Q Grafiği.....	174

1. GİRİŞ

1.1. Araştırmanın Konusu

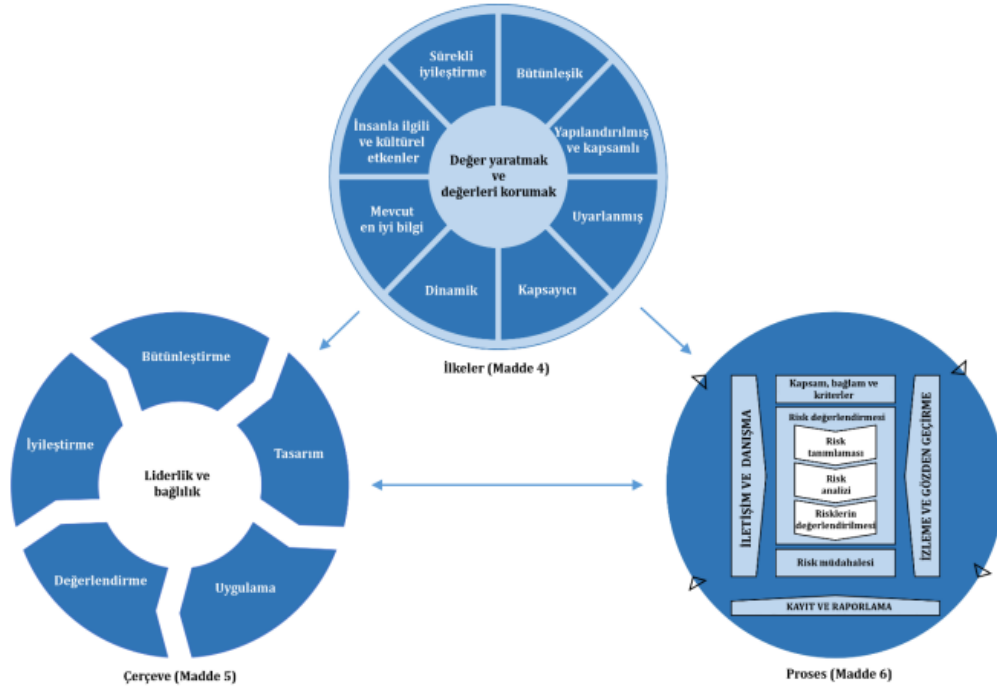
İnsanların yaşamında her daim öncelikli bir yeri olan risk, bireylerin kendi ölüm olasılığını düşünmeye başladığı ve tehlikeli durumlardan kaçınmak için eylemlerde bulunması gerektiğini anladığından bu yana önemli bir çalışma alanı olmuştur (Renn, 1998, s. 50). Yalnızca bireylere özgü bir durum olmayan, 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 beklenen durumdan sapmasına işaret etmektedir (International Organization for Standardization (ISO) 31000, 2018b, 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 31000, 2018b).

Risk yönetimi riskleri belirlemek, sınıflandırmak, ölçmek ve daha sonra bunları yöneterek kontrol altına almak için doğru zamanda doğru kararın verilmesine yardımcı olmayı amaçlayan planlı ve yapılandırılmış bir süreçtir. 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).

Kuruluşların risklerini belirleme, değerlendirme, takip etme ve yönetme süreçlerini kapsayan, uluslararası kabul görmüş bir risk yönetimi standardı olan ISO 31000:2018b içerisinde yer alan ilke, çerçeve ve süreçler sayesinde kurumlar, risklerine daha etkin çözümler üretebilmekte ve hedeflerine ulaşma olasılıklarını artırabilmektedir (Şekil 1.1). Amacı değer yaratmak ve değerleri korumak olan risk yönetimi, kurumlarda performansın artmasına, yeniliğin teşvik edilmesine ve belirlenen hedeflere

ulaşılmasına destek vermektedir. Şekil 1.1’de özetlenen ilkeler etkili ve verimli bir risk yönetiminin amacını ve değerini açıklamaktadır. Buna göre 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, 67; ISO 31000, 2018b).

Şekil 1.1: Risk yönetimi



Kaynak: ISO 31000, 2018b

Bilgi ve iletişim teknolojilerindeki gelişmeler, klasik belge yönetimi faaliyetlerinin elektronik ortamda yürütülmesine zemin hazırlamıştır. 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 (ör. EBYS), 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 kaynaklanabilir. 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 yönetimi sistem ve süreçlerinde karşılaşılabilecekleri potansiyel risklerin belirlenmesi, değerlendirilmesi ve yönetilmesi oluşturmaktadır. Araştırmada, kurumsal iletişimin sağlanmasında kullanılan elektronik belge yönetim sürecinde risk potansiyeli barındıran pek çok tehdit unsuru incelenmektedir. Elektronik belge yönetim sistemi (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.

1.2. Araştırmanın Amacı ve Önemi

Kurumların elektronik belge yönetimi sürecinde büyük bir tehdit oluşturan riskler, dış ve iç etkenlere bağlı riskler ile belge yönetim sistemine ve süreçlerine bağlı riskler olarak gruplandırılmaktadır (Yalçınkaya, 2014). Belge yönetim süreçlerine ve sistemlerine yönelik risk olaylarının sonucunda kurumlar için hayati öneme sahip belgelerin güvenilirliğine, geçerliliğine, bütünlüğüne veya erişilebilirliğine zarar gelmesi muhtemeldir (ISO 18128, 2014). Bu zararın bertaraf edilebilmesi için kurumların belge yönetimi sistem ve süreçlerinde karşılaşılabileceği risk unsurlarını tespit edebilmesi, karşılaşılabileceği zararın farkında olması ve bunlara ilişkin önlem

alabilmesi gerekmektedir. Bu nedenle başta yöneticiler olmak üzere kurum çalışanlarının, belge yönetim sisteminden ve iş süreçlerinde yapılan hatalı işlemlerden doğabilecek risklerin bilincinde olmaları gerekmektedir. Böylelikle kurumlar, bu risklerden doğabilecek zararı en aza indirebilecektir. Bu doğrultuda çalışmada kurum ve kuruluşlara rehberlik edebilecek gelişmiş bir risk yönetimi eğitim materyalinin ortaya çıkarılması amaçlanmıştır. EBYS'yi ve iş süreçlerini tehdit eden risklerin ve bu risk unsurlarının ortadan kaldırılabilmesi için nelere dikkat edilmesi gerektiğinin detaylıca açıklandığı bu materyal ile eğitilen kurum çalışanları, belge yönetim sistem ve süreçlerinde gerçekleştirdikleri işlemlerden doğabilecek riskleri tespit ederek bunlardan doğabilecek zararın önüne geçebilecektir.

Kurum ve kuruluşlarda risk yönetiminin birincil muhatabı çalışanlardır. Kurum çalışanları günlük işlerini yürütürken pek çok riskle karşılaşmaktadır. Bu risklerin yönetilebilmesi, çalışanların bu konudaki bilgi ve farkındalık eksikliğinin giderilmesiyle mümkündür. Bu çalışma kapsamında geliştirilen eğitim materyalinin, kurum ve kuruluşların risk bağışıklığını güçlendireceği öngörülmektedir.

Çalışmada kişilerin, organizasyonların ve devletlerin hukukunu koruyan, delil niteliğindeki belgelerin yönetiminde potansiyel risklerin tanınması ve bunların yönetilmesinde en uygun koşulların belirlenerek özgünlüğüne zarar gelmeden erişilebilir kılınmasına yönelik bir programın geliştirilmesi üzerinde durulmuştur. Bu programın elektronik belgelerin yönetim sürecinde risklerin belirlenerek ortadan kaldırılması hususunda organizasyonlar için önemli bir kaynak olacağı öngörülmektedir. Araştırma bulgularına dayalı olarak geliştirilen eğitim materyalinin belge yönetimi alanındaki uygulamacılara, yöneticilere ve ileride konu üzerinde çalışma yapacak araştırmacılara ilham vereceği, yol göstereceği ve organizasyonlarda sağlam temeller üzerine kurulmuş risk organizasyonunun oluşmasına katkı sağlayacağı savunusu bu çalışmayı önemli kılmaktadır.

1.3. Araştırma Soruları ve Hipotez

Türkiye'deki kurum ve kuruluşlarda elektronik belge yönetimi risklerini yönetme konusunda kullanılan yöntemlerin incelenmesi ve literatürden derlenen bilgiler ışığında hazırlanan bir eğitim materyalinin risk yönetimi üzerindeki etkinliğinin değerlendirilmesi amacıyla gerçekleştirilen bu çalışmada doğrulanması istenen hipotez şu şekildedir:

- *“EBYS risk yönetimi eğitim programının, kullanıcıların bilgi ve farkındalık düzeylerini artırmada ve elektronik belge yönetimi sistem ve süreçlerinde karşılaşılabilecek risk unsurlarını azaltmada anlamlı bir etkisi vardır.”*

Bu hipotezi doğrulamak için yanıtı aranan araştırma soruları ise şunlardır:

- a) Kurumlarda EBYS'ye yönelik kurumsal risk yönetim planları oluşturulmuş mudur?*
- b) EBYS sorumluları, belge yönetimi uzmanları ve akademisyenler ile EBYS yazılım firmaları, gelişmiş bir eğitim materyalinin kurumların risk yönetim planlarına katkı sağlayacağını düşünmekte midir?*
- c) EBYS risk yönetimi eğitimi alan ÇAKÜ personelinin, eğitim öncesi ve sonrası bilgi düzeyleri arasında anlamlı bir fark oluşmuş mudur?*

1.4. Literatür Özeti

Elektronik belge yönetimi konusunda Türkiye’de özellikle son yıllarda pek çok çalışma yapılmasına karşın, farklı sektörlerde sıklıkla çalışılan bir konu olan risk yönetiminin elektronik belge yönetim sistem ve süreçlerinde kullanılmasını konu alan çalışma sayısı oldukça azdır. Alandaki bu boşluğu doldurulması beklenen bu çalışmanın kapsamını ortaya koyabilme adına yurt içi ve yurt dışında yapılmış ilgili çalışmaların saptanması ve değerlendirilmesi önemlidir. Bu bağlamda öncelikle araştırma kapsamında bir literatür özeti sunmanın faydalı olacağı düşünülmektedir.

Çalışma kapsamında araştırma konusuna paralel olarak Türkçe kaynaklarda “elektronik belge yönetimi, elektronik belge yönetim sistemi, risk yönetimi, risk ve belge yönetimi, risk ve elektronik belge yönetim sistemi”, İngilizce kaynaklarda ise “electronic records management, electronic records management system, risk management, risk and records management, risk and records management system” anahtar kelimelerle taramalar gerçekleştirilmiştir. Bu anahtar kelimeler ile Google Akademik, YÖK Tez Merkezi, kütüphane katalogları ve veri tabanları, Açık Anahtar, Dergipark, Türkiye Akademik Arşivi, Türk Kütüphaneciliği, Bilgi Dünyası, Bilgi Yönetimi, TR Dizin, arama ve harmanlama motorları ile açık erişim sistemleri taranmıştır. Kitap, tez, makale, bildiri, rapor, rehber, standart gibi farklı türlerden kaynaklara erişilmiştir.

ISO 15489-1 (2016) standardı belge yönetimini; kurumsal faaliyetler ile ilgili bilgi ve belge formundaki işlemlerin kanıtını tutma ve saklamaya yönelik işlemler dâhil olmak üzere belgelerin üretimi, alınması, saklanması, kullanımı ve tasfiyesinin etkili ve sistemli kontrolünden sorumlu yönetim alanı olarak tanımlamaktadır. Standart, belge yönetim sistemini ise belgeleri toplayan, yöneten ve bunlara erişim sağlayan bilgi sistemi olarak açıklamaktadır. Yapılan faaliyetlerin kanıtlarına yönelik gereksinimlerin karşılanmasında belgelerin oluşturulması ve kayıt altına alınması görevlerini gerçekleştiren belge yönetim sistemleri, belgelerin yönetimine yönelik iş bağlamlarının ve yönetim gereksinimlerinin zaman içerisinde değişmesine paralel olarak özgünlük, güvenilirlik, bütünlük ve kullanılabilirlik özelliklerini korumak için en uygun önlemleri almak zorundadır. Uluslararası kabul gören ISO 15489-1, belge yönetimi için stratejiler geliştirmede risk yönetiminin önemine ve başlı başına bir risk yönetimi stratejisi olarak da belgelerin yönetimine dikkat çekmektedir (ISO 15489-1, 2016).

Hazine ve Maliye Bakanlığı tarafından hazırlanan Kamu Kurumsal Risk Yönetimi Rehberi (2024), kurumların etkin risk yönetimi süreçlerine rehberlik etmek amacıyla kapsamlı bir yöntem ve uygulama adımları sunmaktadır. Bu rehber, risk kavramını ve kurumsal risk yönetimini tanımlayarak söz konusu süreçlerin idarenin stratejik planları, misyon ve vizyonu ile entegrasyonu ve risk strateji belgelerinin oluşturulması gerekliliğini vurgulamaktadır. Ayrıca risklerin belirlenmesi aşamasında yasal uyum, hedef belirleme ve risk kapasitelerinin net bir biçimde tanımlanmasının önemine işaret eden rehber, risklerin etki ve olasılık değerlendirmesine dayalı önceliklendirilmesiyle alınacak kararların tespitine yönelik bir yol haritası sunmaktadır. İzleme ve raporlama süreçlerini de detaylandıran rehber, kurumsal risk yönetimi ile iç kontrol, kalite yönetimi, iç denetim ve dış denetim arasındaki ilişkileri açıklayarak kurum içindeki tüm birimlerin risk yönetimi sorumluluklarını yerine getirmesi için temel bir çerçeve sağlamaktadır.

Uluslararası Arşiv Konseyi (International Council of Archives-ICA) tarafından geliştirilen Principles and Functional Requirements for Records in Electronic Office Environments (ICA-Req) standardı, belge yönetimi için uluslararası standartları, ilkeleri ve işlevsel gereksinimleri uyumlu hale getirmeyi ve genişletmeyi amaçlamaktadır. Bu standart belge yönetimine yönelik riskleri; yazılımın seçimi ve

geliştirilmesi, kurumsal deęişim ve personel gibi çeşitli kategorilere ayırmıştır. Risk yönetim kavramını riskleri tanımlama, gerçekleşme olasılığını hesaplama, etkisini saptama ve bu etkiyi hafifletmeye yönelik stratejiler geliştirmeye yarayan bir mekanizma olarak tanımlayan ICA-Req, risklerin azaltılması amacıyla bir eylem planı geliştirilmesine alt yapı sağlamaktadır (ICA, 2008).

Akçakanat (2012), “Kurumsal Risk Yönetimi ve Kurumsal Risk Yönetim Süreci” adlı çalışmasında, organizasyonlardaki risklerin faydaya çevrilmesinin kurumsal risk yönetimi ile sağlanacağını vurgulamaktadır. Bu doğrultuda etkin bir kurumsal risk yönetimi oluşturabilmek adına gerekli olan süreçleri ele almaktadır.

Yalçinkaya (2015), “Elektronik Belge Yönetimi (EBY) Uygulamalarında Başarıyı Olumsuz Etkileyen Risk Unsurları” adlı çalışmasında, organizasyonların EBYS uygulamasında başarılı olabilmesinin yalnızca kullanılan yazılım ile mümkün olmadığını vurgulamaktadır. Organizasyonların belge yönetiminde başarı sağlayabilmesi için gerekli olan teknik ve yönetsel konuları ortaya koyarak risk faktörleri bağlamında değerlendirmektedir.

Public Record Office Victoria (2010) tarafından hazırlanan “Records & Risk Management” adlı kılavuz, Avustralya Standardı olan Australian/New Zealand Standards - Avustralya/Yeni Zelanda Standartları (AS/NZS) ISO 31000 2009, Risk Management - Principles and Guidelines (Risk yönetimi - ilkeler ve kılavuzlar) isimli standartta yer alan adımları ve ilkeleri izlemektedir. Risk yönetim stratejisinin geliştirilmesine ve uygulanmasına özel bir yaklaşım sunan kılavuz, belge yönetim politikasının risk yönetimi politikasıyla uyumlu olması gerektiğini savunmaktadır. Kılavuzda öncelikle risk yönetimine ilişkin kavramlar açıklanmakta ve risk yönetim süreçleri adım adım ele alınmaktadır.

Yalçinkaya (2014), “Belge Yönetim Sistemlerinde ve Süreçlerinde Risk Tanımları” adlı çalışmada kurumsal sorumluluğun bir parçası olarak belge yönetim sürecinde kurum ve kuruluşların yaşayabileceği riskleri “dış etkenlere, iç etkenlere, belge yönetim sistemine ve belge yönetim sürecine” bağlı olarak dört başlık altında incelemiştir.

Blake (2005), tarafından hazırlanan ve National Archives tarafından yayımlanan “Complying with the Records Management Code: Evaluation Workbook and Methodology” isimli eser, Ocak 2005’te Bilgi Edinme Özgürlüğü Yasası’nın

uygulamaya konmasıyla birlikte hazırlanmıştır. Bilgi Edinme Özgürlüğü Yasası'nın, resmi bilgilere erişim hakkını ortaya çıkarması ve kamu yetkililerine resmi belgeleri “yayın planlarına” uygun olarak yayınlama görevi yüklemesi resmi makamların belge yönetimi disiplinine gösterdiği önemi artırmıştır. Kamu yetkilileri tarafından belge yönetim sistemlerinin belge yönetim kurallarına uygunluğunun değerlendirilebilmesine yardımcı olmak amacıyla geliştirilen çalışma kitabında, belge yönetimi işlevi, politikaların oluşturulması, görev ve sorumluluklar, belge yönetim süreçleri, eğitim ve farkındalık gibi alanlara odaklanmaktadır. Ayrıca belge yönetimi kurallarına uyulmadığında kurumun maruz kaldığı risk düzeyini değerlendirmek için bir mekanizma sağlamak ve risk azaltma stratejilerini aktarmaktadır.

Yıldız (2010) “Elektronik Belge Yönetim Sistemleri ve Denetim” adlı çalışmasında, belge yönetiminin amacını, kurum ve kuruluşların yapmış olduğu faaliyetlerin ve almış oldukları kararların kanıtlayıcısı olan bilgileri içeren belgelerin üretimi, dağıtımını, saklanması, paylaşılması veya imha edilmesi süreçlerinde iyi yönetilmesini sağlamak olarak belirtmektedir. Bilişim teknolojilerinin gelişmesi ve kurumlarda yoğun olarak kullanılmasıyla belge yönetim faaliyetlerinin elektronik ortama taşındığını ama bilişim sistemlerinin karmaşık yapısı, beklentileri karşılamadaki belirsizlikler, güvenlik, sürdürülebilirlik gibi endişeleri yanında getirdiğini ve klasik belge yönetimi sorunlarına bilişim sistemlerinin sorunlarının da eklendiğini vurgulamaktadır. Kurumların en önemli varlığı olan ve bilişim ortamında bulunan belgelerin yönetilebilmesi için oluşturulan sistemlerin iyi ve yeterli şekilde çalışmadığı durumda belge geçerlilikleri ve güvenliği konusunda şüphelerin artacağını, kurumun itibar kaybedebileceğini, yasal yükümlülüklerin yerine getirilmesinde aksaklıklar yaşanabileceğini, idari veya maddi cezalar alınabileceğini vurgulamaktadır. Bu nedenler, elektronik belge yönetim sürecinin her aşamasında meydana gelebilecek her türlü risklerin belirlenmesi gerektiğini ve bir denetim çalışmasının olması gerektiğini ortaya koymaktadır.

Gibson (2011) “Risk and Records Management: Investigating Risk and Risk Management in the Context of Records and Information Management in the Electronic Environment” isimli doktora tez çalışmasında, İngiltere'deki küçük ve orta ölçekli işletmelerde (KOBİ) elektronik ortamda yürütülen belge yönetimi sürecinin risk yönetimine odaklanmaktadır. Araştırma, İngiltere'nin kuzeyinde bulunan üç KOBİ'de

ortaya çıkan vakalar üzerinde iki yıllık bir dönemde gerçekleştirilmiştir. Çalışmanın amacı, KOBİ’lerde elektronik bilgi ve belge yönetimi bağlamında riskleri araştırmak ve elektronik belgelere yönelik risk yönetimi konusunda kullanışlı bir kavramsal model veya teori geliştirmektir.

Sağlık (2021a) “Arşivlenen Elektronik Belgelerin Güvenilirliğini Tehdit Eden Riskler: Teknolojik Koşullar Açısından Bir İnceleme” adlı çalışmasında, müstakil olarak Türkiye’de elektronik belge yönetimi alanında belgeyi etkileyebilecek riskleri konu alan bildiri, makale, kitap gibi akademik çalışmaların olduğunu ama tez niteliğinde bir çalışma olmadığını belirtmiştir.

Çiçek (2021) ise “Türkiye’de Elektronik Belgelerin Geleceği İçin Ulusal Strateji İhtiyacı: Literatür Işığında Bir İnceleme” adlı makalesinde, organizasyonların elektronik belge yönetim sistemini iş süreçlerini hızlı, şeffaf ve verimli bir şekilde yönetebilmek amacıyla kullanıldığını hatta yüklü miktarda kaynak ayırdığını belirtmektedir. Buna karşın, elektronik belgenin uzun vadede kullanılabilir olmasını garanti edecek, erişilebilirliğini sağlayacak koşulların planlanmadığını, e-belgelerin yaşam döngüsü boyunca birçok riskle karşı karşıya kaldığını, riskleri önceden öngörüp çözümler üretilmesi gerektiğini, problem çıkmasını beklemenin uzun vadeli çözümleri geciktirebileceğini ifade etmektedir. Ayrıca ülke genelinde bir takım çalışmalara acil ihtiyaç olduğunu aksi takdirde bilginin varlığını kanıtlayan delil niteliğindeki belgelerin yok olması gibi geri dönüşü olmayan risklerin beklediğini vurgulamaktadır.

“Risk Assessment Handbook” adlı çalışma, The National Archives (2017)’ın merkezi hükümet birimleriyle gerçekleştirilen istişareler neticesinde ortaya çıkmıştır. Hükümet için dijital süreklilik hizmetinin bir parçası olarak sunduğu kılavuzun bir kısmını oluşturmaktadır. Burada bahsi geçen dijital süreklilik, bilgi ve belgelerin ihtiyaç duyulduğu şekilde, ihtiyaç duyulan süre boyunca saklanabilmesi ve kullanılabilmesini ifade etmektedir. Kurum ve kuruluşlarda, yönetim süreçlerindeki değişimler veya teknolojiye gelişmeler dijital sürekliliği riske atabilen unsurlar olarak düşünülmektedir. Dijital sürekliliğe yönelik gerçekleştirilen risk yönetimi, iş ve işlemler için ihtiyaç duyulan bilgi ve belgeleri uzun vadeli korumayı hedeflemektedir. Şeffaf, hesap verilebilir, yasal ve verimlilik unsurlarını kapsayıcı nitelikte çalışmanın sağlanabilmesi için bu konu önemli görülmektedir. Kurumun itibarını koruması,

bilinçli kararlar vermesi, maliyetleri önlemesi, azaltması ve daha iyi kamu hizmetleri sunmasına önemli katkılar sağlayacaktır.

Barnawi (2013) “Risk Management of Electronic Health Record System in Hospitals” başlıklı doktora tezinde risk yönetiminin iş, sağlık ve proje başarısına önemli katkılar sağladığını vurgulamaktadır. Bu katkılar arasında zamandan tasarruf, maliyetin düşürülmesi ve potansiyel başarısızlıkların hasara neden olmadan önce çözüme kavuşturulabilmesi yer alır. Ayrıca risk yönetiminin uygun alternatif yolların belirlenmesini sağladığına, proje hedeflerine ulaşmada güveni artırdığına, başarının yükselirken şüphelerin ve tekrarlanan çabaların azaldığına dikkat çekmektedir. Tamamen risksiz bir ortamın garanti edilmesinin mümkün olmadığını ve her faaliyetin en az bir risk içerdiğini belirten araştırmacı, etkin bir risk analizi ve yönetimi stratejisi geliştirmenin olası risklerin değerlendirilmesi ve alınacak önlemlerin belirlenmesinde fayda sağlayacağını belirtmiştir. Bu nedenle büyüklükleri ne olursa olsun tüm organizasyonlarda gerçekleştirilen faaliyetlerin risk planlarına uygunluğu oldukça önem taşımaktadır. Bu bağlamda hastanelerdeki elektronik kayıt sistemlerinin kullanım düzeyi ve kapsamını araştıran Barnawi, sağlık hizmetlerinin performansını, güvenliğini ve kalitesini iyileştirmek adına risk tespiti ve yönetimi üzerinde durmuştur.

ISO’nun (2014) “Information and Documentation- Risk Assessment for Records Processes and Systems Technical Report” isimli raporunda, belge profesyonellerine ve kuruluşlarda belgelerden sorumlu kişilere, belge süreçleri ve sistemleriyle ilgili riskleri değerlendirmede yardımcı olan unsurlar yer almaktadır. Belge süreçleri ve sistemleri ile ilgili risklerin yönetilmesi için ISO 31000’de oluşturulan genel risk yönetimi sürecine dayalı rehber niteliği taşıyan ve örnekler sunan rapor: risk tanımlaması, risk analizi ve risk değerlendirmesi konularını içermektedir (ISO 18128, 2014). 2024 yılında yayımlanan ISO 18128 ise önceki 2014 raporunun yerine geçmiştir ve daha kapsamlı bir risk yönetimi çerçevesi sunmaktadır. Bu yeni sürüm, ISO 31000 ve IEC (International Electrotechnical Commission-Uluslararası Elektroteknik Komisyonu) 31010 gibi modern risk değerlendirme tekniklerini kullanarak daha gelişmiş araçlar ve yöntemler sunmaktadır. Risk tanımlama, analizi ve değerlendirmesi sürecinde daha derinlemesine rehberlik ve örnekler içerir. 2024 sürümünde, iş etki analizi (BIA), insan güvenilirliği analizi (HRA) ve papyon analizi gibi teknikler daha ayrıntılı şekilde ele alınmıştır. Ayrıca belirsizlik ve bağlamın daha

kapsamlı bir şekilde ele alınması, kuruluşların iç ve dış koşullarını daha iyi anlamalarına yardımcı olacak ek unsurlar eklenmiştir. Bu güncelleme, dijital kayıtların etkilerini de dikkate alarak daha uygun risk yönetimi stratejileri geliştirilmesini sağlamaktadır (ISO 18128, 2024).

Bir organizasyonun başarılı olabilmesi için risk yönetiminde beklenmedik durumları da hesaba katmak gerekmektedir. Bu nedenle risk yönetimi için geliştirilen ISO 31000:2018 Risk Management Guidelines, kurum ve kuruluşların karşılaştığı risklerin yönetimine ilişkin yönergeler sunmaktadır. Bir kuruma veya sektöre özgü olmayan kılavuz, organizasyonlar için ortak bir yaklaşım sağlamaktadır. Kurum ve kuruluşların ömrü boyunca tüm seviyelerdeki karar alma sürecine uyarlanabilmekte ve gerçekleştirilen tüm faaliyetlere uygulanabilmektedir.

Lin (2020) “Establishing The Risk Assessment Indicators of Electronic Records And Empirical Analysis of An Institution” adlı çalışmasında Tayvan’daki devlet kurumlarına yönelik risk yönetiminin teorik çerçevesine uygun olarak elektronik belgelere yönelik bir risk yönetimi modeli oluşturmayı amaçlamaktadır. Çalışma kapsamında, geniş bir literatür taraması yapılmış ve sekiz arşivcinin, bilgi bilimcinin ve kurumsal personelin risk faktörlerine ilişkin görüşlerinden faydalanılarak fikir birliğine dayalı risk değerlendirme göstergeleri oluşturulmuştur.

Sağlık’ın (2021b) “Elektronik Belge Yönetimi Uygulamalarındaki Koşullar Işığında E-İmzalı Belgelerin Delil Değerinin Arşivsel Güvenilirlik Açısından İncelenmesi” başlıklı doktora tezi, kurumların Elektronik Belge Yönetim Sistemleri’nde (EBYS) saklanan e-imzalı belgelerin zamanla özgünlüklerini kaybetme riskine odaklanmaktadır. Bu durumun belgelerin delil değerini ve güvenilirliğini olumsuz etkileyebileceğini vurgulayan bu çalışma, karma araştırma yöntemi (nitel ve nicel) kullanarak veriler toplamıştır. Nitel araştırma aşamasında uzman görüşlerine başvurulmuş ve saha uzmanlarının literatürdeki genel kanılarla örtüşen görüşlere sahip olduğu tespit edilmiştir. Nicel araştırma aşamasında ise Türkiye’nin en fazla kamu personeli çalıştıran bakanlıklarından altısının uygulamaları incelenmiştir. Araştırma bulguları, kurumların e-belge yönetiminde çeşitli risk unsurlarının bulunduğunu ve e-belge yönetiminin genellikle yalnızca bir yazılım uygulaması olarak algılandığı için sürecin bütünsel bir yaklaşımla ele alınmadığını ortaya koymuştur. Sonuç olarak çalışma, e-imzalı belgelerin delil değerinin korunabilmesi için uzun dönemli arşivleme

politikalarının geliştirilmesinin, uygun teknolojik altyapının sağlanmasının ve belge hiyerarşisinin korunarak arşivsel bağın muhafaza edilmesinin önemini vurgulamaktadır.

Bu çalışmada EBYS’de risk yönetimi için geliştirilmiş kapsamlı bir eğitim materyaliyle verilen seminerin etkinliği değerlendirilmiştir. Bu materyal aracılığıyla ÇAKÜ’de yazışma personeli olarak görev yapan personele eğitim verilmiştir. Hem eğitim öncesinde hem de sonrasında katılımcılara uygulanan testler, çalışanların risk yönetimi bilgi ve farkındalık düzeyinde önemli bir artış sağladığını ortaya koymuştur.

1.5. Araştırmanın Yöntemi

1.5.1. Yöntem

Bu çalışmada öncelikle belgesel tarama tekniğine başvurularak sistematik ve kapsamlı bir kaynak taraması yapılmıştır. Bu doğrultuda alan yazında konuyla ilgili önceki çalışmalar saptanmış, sentezlenmiş ve değerlendirilmiştir. Belgesel tarama ile elektronik belge yönetim sürecindeki risk unsurları ve bu süreci en iyi şekilde kontrol edebilmek amacıyla geliştirilen risk yönetimi ile ilgili daha önceden yapılmış çalışmalar tespit edilerek bu çalışmalardaki anlatılar, tartışmalar, sonuç ve değerlendirmeler anlaşılmıştır. Bununla birlikte konular arasındaki bağlantılar ve alanda gözlenen boşluklar da tespit edilmiştir.

Çalışmanın diğer safhasında, risk yönetimine ilişkin literatürden elde edilen standartlar, rehberler, makaleler, kitaplar vb. bilgi kaynaklarından derlenen bilgiler ışığında elektronik belge yönetim sistem ve süreçleri için risk yönetimini konu edinen, risk değerlendirme kriterleri, risk tanımlama, tanımlanan risklerin analizi, risklerin değerlendirilmesi ve yönetilmesi başlıklarını içeren bir eğitim materyali taslağı hazırlanmıştır. Elektronik belge yönetimi alanındaki riskleri detaylı bir şekilde ele alan bu taslak, ülkemizdeki kurumların ihtiyaçlarına yönelik olarak geliştirilebilecek esneklikte hazırlanmıştır. Sonrasında, eğitim materyali taslağının etkinliğinin artırılabilmesi amacıyla kurum ve kuruluşlarda EBYS iş ve işlemlerinde çeşitli roller üstlenen personel, EBYS yazılımı geliştiren firmalar, alan uzmanları ve akademisyenlerle derinlemesine görüşmeler gerçekleştirilmiştir. Nitel araştırmalarda sıklıkla kullanılan ve görüşmeye katılan kişilerden kapsamlı veri toplamayı amaçlayan görüşme tekniğiyle (Yüksel, 2020), elektronik belge yönetimi sürecine ilişkin risk

yönetim mekanizmasına ait süreç ve unsurlar üzerinde derinlemesine bir inceleme yapılmıştır. Farklı paydaşlarla yapılan görüşmeler yeterli veriye ulaşana kadar sürdürülmüştür. Görüşmeler sonucunda elde edilen veriler nitel analiz yöntemlerine uygun olarak yorumlanmıştır. Elde edilen bilgiler doğrultusunda taslak, kurumların karşılaştığı ortak sorunlara çözüm önerilerini kapsayacak nitelikte bir kaynak haline getirilmiştir. Ayrıca önemli bulgular ayrıntılı olarak analiz edilmiştir.

Görüşme yapılan gruplar ve hedefler şu şekildedir:

1. Kurum çalışanları: Ülkemizdeki çeşitli kurumlarda elektronik belge yönetiminden sorumlu olan personelle görüşülerek uygulamalardaki riskler, ihtiyaçlar ve beklentiler hakkında veri toplanmıştır.
2. EBYS yazılım firmaları: Elektronik belge yönetim sistemlerinin tasarımı ve geliştirilmesi sürecinde ortaya çıkan riskler konusunda firmalarla görüşülerek sistemsal risklerin belirlenmesi ve bu risklerin azaltılmasına yönelik çözümler üzerinde durulmuştur.
3. Belge yönetimi uzmanları ve akademisyenler: Uzmanlar ve akademisyenlerle görüşülerek güncel literatür ve akademik çalışmalar ışığında eğitim materyalinin bilimsel bir temel üzerine oturtulması hedeflenmiştir.

Görüşmeler, katılımcıların istekleri doğrultusunda katılımcının bulunduğu ilde yüz yüze veya Zoom ve Microsoft Teams platformları üzerinden çevrimiçi olarak gerçekleştirilmiştir. Katılımcılar görüşme öncesinde araştırmanın amacı hakkında detaylı bir şekilde bilgilendirilmiştir. Görüşmeden on beş gün önce, eğitim materyali taslağı ve o gruba özel hazırlanmış görüşme formu¹ katılımcılarla paylaşarak ön değerlendirme yapabilmelerine imkân tanınmıştır.

Görüşmeler, önceden hazırlanmış yarı yapılandırılmış bir mülakat formu kullanılarak gerçekleştirilmiştir. Bu form, hem araştırmanın ana temalarına yönelik standart soruları hem de katılımcıların kendi deneyim ve görüşlerini paylaşabilecekleri açık uçlu sorulardan oluşmaktadır. Görüşme esnasında veri kaybının önlenmesi için ses kayıt cihazı kullanılmış ve gerekli durumlarda elle not alınmıştır. Katılımcılara ses kayıt cihazının kullanılacağı, görüşme sonunda katılımcıya dinletilebileceği ve

¹ Not: Görüşme formları, katılımcıların profiline göre (kurum çalışanları, firmalar, uzmanlar/akademisyenler) üç farklı şekilde hazırlanmıştır.

çalışma bitiminde istek doğrultusunda silinebileceği bilgisi verilmiştir. Görüşmeler yoluyla elde edilen veriler MaxQDA² yazılımı kullanılarak analiz edilmiştir. Eğitim materyalinin etkililiğini artırmak amacıyla yapılan görüşmeler, materyaldeki eksiklikleri ve riskleri belirleyerek daha etkili çözümler üretilmesine yönelik iyileştirmeye katkı sağlamıştır.

Hem uluslararası literatürden derlenen güncel bilgiler, hem de yapılan görüşmeler ışığında kapsamlı bir eğitim materyali hazırlanmıştır. Bu materyal aracılığıyla verilen seminerin ÇAKÜ’de farklı birimlerde görev yapan personelin EBYS’de risk yönetimi konusundaki bilgi ve farkındalık düzeylerinde ne gibi bir değişim yarattığı deneysel bir araştırma çerçevesinde incelenmiştir. Eğitim materyali her ne kadar kapsamı bakımından sekreterler, yöneticiler ve bilişim personeli için hazırlanmış olsa da bu gruplara ulaşmadaki zorluk nedeniyle eğitim materyalinin etkinliğinin değerlendirilmesi yalnızca yazışma personeliyle (sekreterler) sınırlı tutulmuştur. Bu nedenle hazırlanan eğitim materyalinden sekreterleri ilgilendiren konular seçilerek bu gruba özel bir sunum oluşturulmuştur.

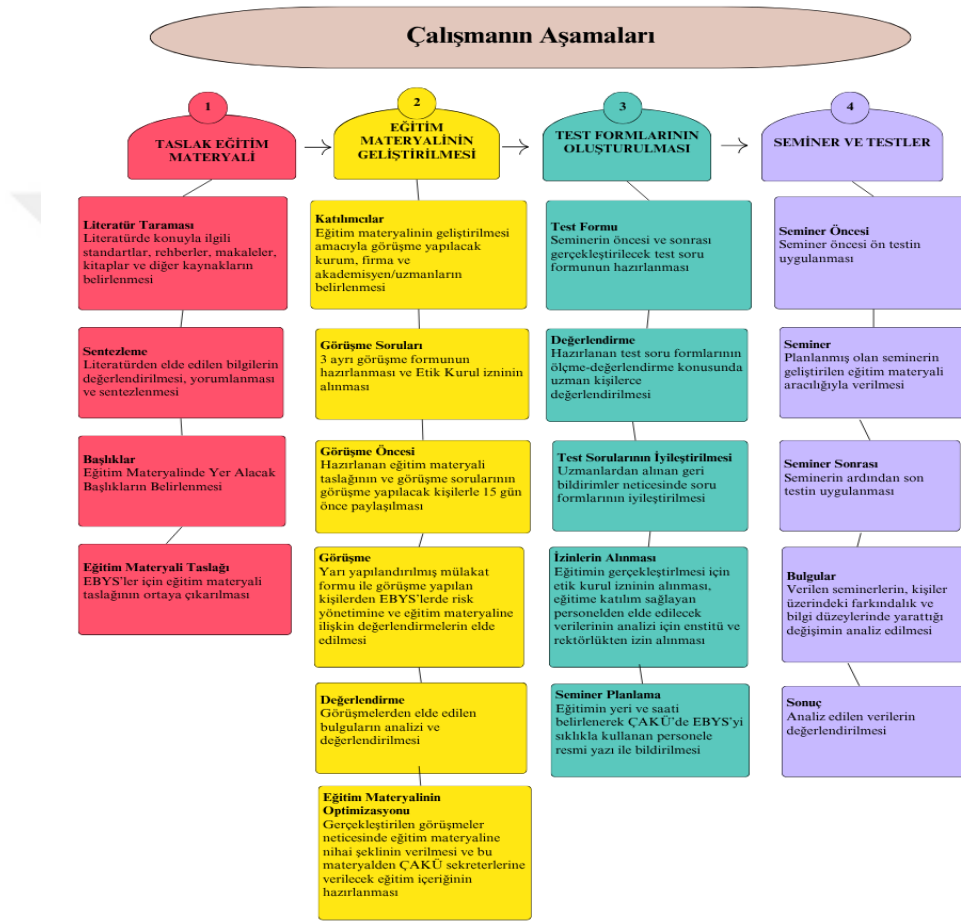
Eğitimin ÇAKÜ’de uygulanabilmesi için hem ÇAKÜ Sosyal Bilimler Enstitüsünden hem de Rektörlükten gerekli izinler alınmıştır. Bununla birlikte yeterli katılımcı sayısına ulaşmak için ÇAKÜ Rektörlüğü ile iletişime geçilerek eğitimin önemi ve gerekliliği anlatılmıştır. Bunun sonucunda Rektörlük, üniversitede yazışma personeli olarak görev yapan personeli resmi yazıyla eğitime davet etmiştir. Maliyet ve zaman faktörleri göz önüne alınarak ÇAKÜ’nün Çankırı’nın ilçelerindeki (Çerkeş, Kurşunlu gibi) birimleri bu davetin dışında tutulmuştur. 18 Haziran 2025 Çarşamba günü saat 14:00’te düzenlenen eğitime 26 katılımcı gelmiştir. Bu gruba yönelik düzenlenen “EBYS’de Risk Yönetimi” eğitiminin, katılımcıların elektronik belge yönetimi süreçlerindeki riskleri belirleme, değerlendirme ve yönetim becerilerini geliştirmedeki etkinliğini ölçmek amacıyla deneysel bir araştırma yürütülmüştür. Bu çalışmada özellikleri daha önce belirtilmiş olan gruba eğitim öncesi ve sonrası aynı içerikte ve formatta sorulardan oluşan bir soru formu yöneltilmiştir. Katılımcıların elektronik belge yönetimi risklerine dair bilgi ve farkındalık düzeylerini ölçmek üzere sorular, seminerde kullanılan sunuma sadık kalınarak hazırlanmıştır. Ayrıca hazırlanan soru formları, alan uzmanları ve ölçme-değerlendirme alanındaki öğretim üyelerinin

² Ayrıntılı bilgi için bkz. <https://www.MaxQDA.com/tr>

görüşleri doğrultusunda iyileştirilmiştir. Eğitim öncesi ve sonrası yöneltilen testi 26 katılımcıdan 25'i cevaplamış ve verilen yanıtlardan elde edilen verilerin istatistiksel analizi ile eğitim materyalinin etkililiği değerlendirilmiştir.

Bu kapsamlı çalışmanın amacına ulaşabilmesi amacıyla çeşitli süreç adımları izlenmiştir. Araştırma süreci ve aşamaları özetle Şekil 1.2'de gösterilmektedir.

Şekil 1.2: Araştırma süreci



1.5.2. Araştırmanın Sınırlılıkları

Eğitim materyalinin geliştirilmesi aşamasında 13 kamu kurumu, 10 uzman/akademisyen ve 3 EBYS yazılım firmasıyla görüşmeler yapılmıştır. Geliştirilen materyalin etkililiğinin değerlendirilmesi ise ÇAKÜ ile sınırlı tutulmuştur. Bunun nedeni materyalin etkinliğini ölçmek için gerekli olan eğitimin ÇAKÜ tarafından sağlanabilmesidir. Bu eğitimi gerçekleştirebilmek ve personelin eğitime katılmasını sağlamak amacıyla başta kurumsal izin, hedef kitlenin eğitime yönlendirilmesi, maliyet ve zaman gibi unsurlar çalışmanın sınırlandırılmasına neden

olmuştur. Ayrıca kapsamı oldukça geniş olan eğitim materyali her ne kadar yöneticiler (dekan, dekan yardımcıları, daire başkanları vb.), bilgi işlem personeli (EBYS yazılım yöneticileri) ve yazışma yapan personel (sekreterler) gibi geniş bir kitleye hitap etse de yönetici ve bilgi işlem personeli gruplarına ulaşmadaki zorluklar nedeniyle materyalin etkinliği yalnızca yazışma yapan personel grubuyla (sekreterler) kısıtlanmıştır. Bu kısıt nedeniyle eğitim materyalinde özellikle yazışma yapan personelin ilgi alanlarına giren konular seçilmiş ve eğitim bu doğrultuda verilmiştir. Ayrıca yazışma yapan personele uygulanan test de bu grup için hazırlanan eğitim sunumu içerisindeki konular temel alınarak hazırlanmıştır. Bu grup üzerinde yapılan değerlendirmeler ile ortaya çıkarılan eğitim materyalinin etkinliği analiz edilmiştir.

1.5.3. Araştırmanın Örneklemi

Çalışmada EBYS’de risk yönetimi eğitim materyalinin taslak hali literatüre dayalı olarak oluşturulmuştur. Daha sonra bu taslağın iyileştirebilmesi amacıyla elektronik belge yönetimi alanında çalışan uzmanlar/akademisyenler, çeşitli kurumlarda EBYS sorumluları ve EBYS yazılım firmalarından temsilcilerden görüş alınmıştır. Bu sayede eğitim materyalinin hem teorik zeminin güçlendirilmesi hem de pratik açıdan örneklerle zenginleştirilerek ülkemizdeki elektronik belge yönetimi uygulamalarına daha etkin bir şekilde katkı sunması sağlanmıştır. Bu doğrultuda Türkiye’deki tüm kurum ve kuruluşlarla görüşme yapmanın zorluğu göz önünde bulundurularak evreni temsil edecek nitelikte 13 kamu kurumundan sistem ve işleyişten sorumlu personel, üç ticari firma ve 10 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 önkoşul olarak belirlenmiştir. Bunun yanı sıra kurum seçiminde çeşitli ek kriterler de göz önünde tutulmuştur. 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*
- *Türk Kızılay,*
- *Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK),*
- *Türkiye Büyük Millet Meclisi (TBMM)*

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 3 ticari firma seçilmiştir. Bununla birlikte elektronik belge yönetimi alanında risk yönetimi konusunda bilimsel çalışmalar gerçekleştirmiş veya uygulamada etkin rol oynamış 8 akademisyen ve uzmanın görüşlerine başvurulmuştur.

Çalışmanın “Yöntem” başlığında da ifade edildiği gibi yapılan görüşmelerin ardından nihai alan eğitim materyaliyle seminer verilmiş ve bu materyalin etkinliği ölçülmüştür. Bu doğrultuda ÇAKÜ’de gerçekleştirilen “EBYS’de risk yönetimi” temalı seminere, EBYS süreçlerinde aktif görev alan ve yoğun işlemler yürüten başlıca grup olan yazışma yapan personel (sekreterler) davet edilmiştir. ÇAKÜ Rektörlüğü tarafından resmi yazı aracılığıyla davet edilen bu özellikteki personelden 26 kişi eğitime katılmıştır. Eğitim materyalinin etkinliğini değerlendirmek amacıyla katılımcılara eğitim öncesi ve sonrası uygulanan testi ise 25 katılımcı yanıtlamış ve elde edilen bulgular uygun istatistiksel yöntemler kullanılarak titizlikle analiz edilmiştir. Bu

analizler sonucunda eğitim materyalinin katılımcıların bilgi ve becerileri üzerindeki etkisi somut bir şekilde ortaya konmuştur.



2. EBYS'DE RİSK YÖNETİM SÜRECİ

EBYS, kurumların dijital dönüşümü için önemli bir bileşendir. Belge iş akışlarını iyileştirerek kurumlara önemli avantajlar sağlayan EBYS'ler, aynı zamanda kişisel veriler ve finansal bilgiler gibi hassas verilerin de merkezi haline gelmiştir. Bu hassas verilerin siber saldırılar ve yetkisiz erişim gibi risklere karşı korunması için EBYS'lerde güçlü bir risk yönetimi altyapısının kurulması elzem olmuştur. Sistemin güvenliği, işlevselliği ve yasal düzenlemelere uygunluğu sürecin temel unsurlarıdır. Bu bölümde, EBYS'ye özgü bir risk yönetimi uygulama süreci ilgili standart ve rehberler ile literatüre dayalı olarak sunulmaktadır. Bahsedilen adımların sayısı ve sıralaması kurumların yapılarına göre değişiklik gösterebilse de temel prensipler ve hedefler her kurum için aynıdır.

Risk yönetim sürecinin beş adımda ele alındığı bu bölümde öncelikle belirtilmesi gereken husus, bu adımların uygulanabilmesi için kurumsal bir risk kültürünün oluşması gerektiğidir. EBYS'nin önemi ve risk yönetimi bilincinin tüm çalışanlara aşılması, risk yönetimi politikası ve prosedürlerinin belirlenmesi ve paydaşlarla paylaşılması, risk yönetimi faaliyetlerine yönelik sorumlulukların ve yetkilerin tanımlanması sürecin uygulanması için gerekli zemini oluşturmaktadır. Çalışmanın bu bölümünde ele alınan aşamalı yaklaşım, kurumların belge yönetim sistemlerindeki riskleri belirlemelerine ve bu risklere karşı etkili çözümler geliştirmelerine yardımcı olacaktır. Bu bölümde işlenen ana konu başlıkları Tablo 2.1'de sunulmaktadır:

Tablo 2.1: EBYS'de risk yönetim süreci

Süreç	Açıklama
<i>Risk Değerlendirmesi</i>	Risklerin tanımlanması, analizi ve değerlendirilmesi süreçlerini içerir. Potansiyel riskler belirlenir, olasılık ve etki değerleri analiz edilir, riskler önceliklendirilerek kabul edilebilirliği değerlendirilir.
<i>Risk Müdahalesi</i>	Belirlenen risklere yönelik aksiyonların alınmasıdır.
<i>İzleme ve Gözden Geçirme</i>	Risklerin sürekli olarak izlenmesidir.
<i>İletişim ve Danışma</i>	Risk yönetim süreçlerine dair bilgilendirme ve danışma faaliyetlerinin yürütülmesidir.
<i>Kaydetme ve Raporlama</i>	Risk yönetim süreçlerinin belgelenmesi ve raporlanmasıdır.

Risk yönetiminin çekirdeğinde ‘Risk Değerlendirmesi’ bulunmakta ve bu değerlendirme süreci ‘Risk Tanımlaması’, ‘Risk Analizi’ ve ‘Risklerin Değerlendirmesi’ aşamalarını içermektedir. Değerlendirme sürecinin ilk basamağını oluşturan ‘Risk Tanımlaması’ EBYS’yi etkileyebilecek tüm potansiyel risklerin sistematik bir şekilde belirlenmesi anlamına gelmektedir. Tablo 2.2, çalışmanın ‘Risk Tanımlaması’ bölümünde ele alınan konu başlıklarını özetlemektedir.

Tablo 2.2: Risk tanımlaması

Risk Tanımlaması	<i>Dış Etkenlere Bağlı Riskler</i>	Siyasi-Toplumsal Bağlamdaki Değişiklikler
		Makro Ekonomik ve Teknolojik Çevre
		Fiziksel Çevre ve Altyapı
		Dış Güvenlik Tehditleri
	<i>İç Etkenlere Bağlı Riskler</i>	Organizasyonel Değişim
		Teknolojik Değişim
		İnsan Kaynakları, Yetkinlikler ve Finansman
	<i>Elektronik Belge Yönetim Sistemine Bağlı Riskler</i>	EBYS Tasarımı
		EBYS Bakımı
		Sürdürülebilirlik ve Süreklilik
		Birlikte Çalışabilirlik
		Güvenlik
	<i>Elektronik Belge Yönetim Süreçlerindeki Riskler</i>	Elektronik Belgenin Oluşturulması
		Elektronik Belgenin Kullanımı
		Kullanılabilirliğin Sürdürülmesi
		Elektronik Belgenin Düzenlenmesi
		Elektronik Belge Kontrolleri
		Elektronik Belgeye Erişim
		Elektronik Belgenin Saklanması
		Elektronik Belgelerde Ayıklama-İmha

Tanımlanan her bir riskin olasılık ve etki boyutunun detaylı analizi ile risk analizi için uygun tekniklerin (Papyon Analizi, İş Etki Analizi) kullanımı ikinci basamak olan ‘Risk Analizi’ başlığında ele alınmaktadır. Çalışmanın ‘Risk Analizi’ bölümünde ele alınan konular Tablo 2.3’te sunulmaktadır:

Tablo 2.3: Risk analizi

Risk Analizi	İş Etki Analizi
	İnsan Güvenilirliği Analizi
	Papyon Analizi

‘Risklerin Değerlendirmesi’ başlığında ise analiz sonucunda elde edilen bilgiler ışığında risklerin önem sırasının belirlenmesi, yüksek risk taşıyan unsurların öncelikli olarak çözümlenmesi ve tekniklerin uygulanması üzerinde durulmaktadır. Çalışmanın ‘Risklerin Değerlendirmesi’ kısmında işlenen konular Tablo 2.4’te verilmektedir:

Tablo 2.4: Risklerin değerlendirilmesi

Risklerin Değerlendirmesi	<i>Riski Değerlendirme Teknikleri</i>	Makul Olarak Uygulanabilir En Düşük Seviye
		Güvenilirlik Merkezli Bakım
		Risk Değerlendirme Matrisleri
		Fayda-Maliyet Analizi

‘Risk Tanımlaması’, ‘Risk Analizi’ ve ‘Risklerin Değerlendirilmesi’ alt başlıklarından oluşan ‘Risk Değerlendirmesi’ aşamasından sonra risk yönetim sürecinin bir sonraki adımı olan ‘Risk Müdahalesi’ devreye girmektedir. Değerlendirilen riskler için uygun müdahale stratejilerinin geliştirilmesi, riskin önlenmesi, azaltılması veya kabul edilmesi gibi farklı seçeneklerin masaya yatırılması, risk müdahale planlarının hazırlanması ve uygulanması bu başlık altında açıklanan konulardır.

Risk yönetim sürecinin periyodik olarak izlenmesi, risklerin güncel durumunun ve müdahale planlarının etkinliğinin değerlendirilmesi, gerekli güncellemelerin yapılması ile ilgili konular ise ‘İzleme ve Gözden Geçirme’ başlığında ele alınmaktadır.

Tüm paydaşların riskleri anlamaları ve bu risklere karşı birlikte çalışarak kontrollü bir şekilde önlem almaları ‘İletişim ve danışma’ bölümünde açıklanmaktadır.

Risk yönetimi sürecinin tüm aşamalarının belgelenmesi ve raporlanması, raporların üst yönetim ve paydaşlarla paylaşılması işlemleri ise ‘Kaydetme ve Raporlama’ başlığında ele alınmaktadır.

2.1. Risk Değerlendirmesi

İş süreçlerine dair önemli bilgiler içeren belgeler, kurumların en değerli varlıklarındandır. Bu varlıkları korumak için etkin bir belge yönetimi sistemi şarttır (Hamidovic, 2010). Bilgi ve belgelerin iyi yönetimi, sağlam bir organizasyonun temel taşıdır. Belgeler, kurum ve kuruluşların geçmiş kararlarını, eylemlerini ve elde ettiği sonuçları kayıt altına alarak iş sürekliliğini desteklemekte ve gelecekteki karar alma süreçlerine ışık tutmaktadır. İyi yapılandırılmış bir belge yönetimi uygulaması, iş süreçlerinin verimliliğini artırarak sürekli iyileştirme çabalarına destek olmaktadır. Bu sayede, iş süreçlerindeki sorunlar tespit edilebilir, hatalar en aza indirilebilir ve genel iş performansı iyileştirilebilir (ISO 16175, 2020, s. vi).

Uluslararası Standartlar Organizasyonu belgelerin yönetimine ilişkin temel ilkeler belirlemiştir. Bu ilkeler şu şekilde sıralanabilir (ISO 15489, 2016, s. 3):

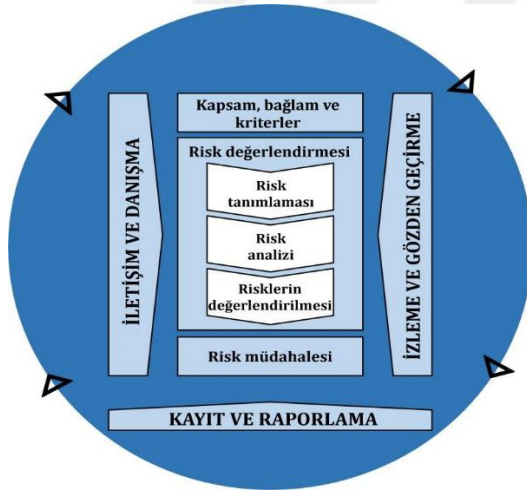
- a) Belgelerin oluşturulması, kayıt altına alınması ve yönetilmesi, iş süreçlerinin ayrılmaz bir parçasıdır ve her aşamada dikkatli bir şekilde yönetilmesi gerekmektedir.
- b) Belgeler, yasal ve iş işlemlerinde kullanılabilmesi için özgünlük, bütünlük, güvenilirlik ve kullanılabilirlik özelliklerine sahip olmalıdır.
- c) Kayıtlar, belgelerin bağlamını, içeriğini, yapısını ve bunların yönetimini açıklayan içerik ve üstverilerden oluşmalıdır.
- d) Bir işletmede belgelerin nasıl oluşturulacağı, saklanacağı ve yönetileceğine ilişkin kararlar verilirken şirketin hedefleri, kanunlar, sektördeki kurallar, müşterilerin beklentileri gibi birçok faktör göz önünde bulundurulmalı ve olası riskler değerlendirilmelidir.
- e) Belge yönetim sistemleri, belge yaşam döngüsünün tüm aşamalarında (oluşturma, saklama, erişim, güncelleme, imha) gerekli kontrollerin uygulanmasını, süreçlerin standartlaştırılmasını ve tanımlanmış belge yönetimi standartlarına uygunluğu sağlamak amacıyla kullanılan yazılımsal ve donanımsal araçlardır. Bu sistemlerin etkinliği, politikalar, sorumluluklar, izleme, değerlendirme ve eğitim faaliyetleriyle desteklenmelidir.

Belgeleri yönetmekle ilgili bu beş prensip, kurumlarda belgelerin korunması ve yönetilmesinin önemine işaret etmektedir. Belge, kurumsal faaliyetlerin kanıtı ve yasal

dayanağı olduğundan kurumlardaki organizasyonu oluşturan hammadde, sermaye ve iş gücü kadar değerlidir. Bu nedenle üretimden arşivleme evresine kadar geçen tüm işlem boyunca sistematik bir şekilde yönetilmesi hayati önem taşır (Odabaş ve Polat, 2008, ss. 3-4).

Kurumlar için hayati önem taşıyan belge yönetimi faaliyetleri, geçmişte fiziki ortamlarda yürütülürken dağınıklık, kaybolma, depolama zorlukları ve güvenlik riskleri gibi sorunlarla karşılaşmaktaydı. Bu faaliyetlerin elektronik ortama taşınmasıyla birlikte ise veri güvenliği ihlalleri, yetkisiz erişim, veri bozulması ve sistem arızaları gibi yeni riskler ortaya çıkmıştır. Bu nedenle kurumların belge yönetim sistemlerini güvence altına almaları, iş sürekliliğini sağlama, yasal uyumluluğu yerine getirme ve rekabet avantajı elde etme için büyük önem taşımaktadır. Aksi takdirde bilgi kayıpları, karar verme süreçlerinde gecikmeler, itibar zedelenmesi ve mali kayıplar gibi ciddi sonuçlar ortaya çıkabilir (Hamidoviç, 2010).

Şekil 2.1: Risk yönetim süreci



Kaynak: ISO 31000, 2018b, s. 9

Şekil 3'te gösterildiği üzere, risk yönetim süreci; risklerin belirlenmesi, analiz edilmesi, değerlendirilmesi, gerektiğinde müdahale edilmesi, kaydedilmesi ve raporlanması adımlarının sistematik olarak uygulanmasını kapsamaktadır. Risk yönetiminin merkezinde risk değerlendirmesi bulunmakta ve bu değerlendirme süreci risklerin tanımlanması, analiz edilmesi ve değerlendirilmesini içeren bir dizi aşamadan oluşmaktadır. Bu sürecin sistematik, sürekli ve iş birliğine dayalı bir şekilde yürütülerek tüm paydaşların bilgi ve görüşlerinin dikkate alınması önemlidir. Riskler değerlendirilirken eldeki tüm bilgilere, geçmişte yaşanan benzer durumlara ve

sektördeki uzman görüşlerine başvurulmalı, gerekirse daha detaylı araştırmalar yaparak eksik bilgiler tamamlanmalıdır (ISO 31000, 2018b).

2.1.1. Risk Tanımlaması

Belge yönetimi sistem ve süreçlerine yönelik yapılacak risk yönetimi planlanmasında diğer disiplinlerde olduğu gibi risk yönetim süreçlerinin adım adım takip edilmesi önem arz etmektedir. Sürecin ilk basamağı riskin tanımlanmasıdır. Riskin teşhis edilmesi anlamına gelen riskin tanımlanması süreci, riskli olduğu düşünülen unsurların tanımlanması ve etkisinin belirlenmesi ile belirsizliklerin azaltılması için kullanılmaktadır (Emhan, 2009). Risk faktörlerinin belirlenmesi, risk yönetimi sürecinin başlangıcında olduğu kadar, süreç boyunca düzenli aralıklarla tekrarlanan bir etkinliktir. Risk tanımlamasının temel amacı, olası riskleri sistematik bir şekilde listeleyerek, daha sonra yapılacak analiz ve değerlendirme çalışmalarına zemin hazırlamaktır (Calp ve Akcayol 2015, s. 7).

Risk yönetim sürecinin temelinde risk tanımlaması yer almaktadır. Geri kalan tüm işlemler, bu aşamada belirlenen riskler üzerine inşa edilmektedir. Bu nedenle titiz ve özenli bir şekilde gerçekleştirilmesi gerekmektedir. Aksi takdirde, tanımlanmayan ve teşhis edilemeyen risklerin analizi, değerlendirilmesi veya azaltılması mümkün olmayacaktır (Bakkal, Tunç ve Kasımoğlu, 2016, s. 96).

Belge üzerindeki riskleri tanımlamanın amacı belgelerin, kuruluşun ihtiyaçlarını destekleme yeteneğini olumlu veya olumsuz etkileyebilecek riskleri bulmak, tanımak ve tanımlamaktır. Bu süreç, kuruluşun hedeflerini etkileyebilecek risklerin, olayların, durumların veya koşulların temelindeki nedenlerin ve kaynakların ortaya çıkarılmasını içermektedir. Belgelerin, kuruluşun iş ihtiyaçlarını destekleme düzeyini değerlendirmek için belge yöneticileri, konunun uzmanları, kullanıcılar ve iş sahipleri gibi farklı paydaşların katılımıyla gerçekleştirilen kapsamlı bir risk tanımlama süreci uygulanır. Bu süreçte, geçmiş deneyimlerden yola çıkarak denetim faaliyetleri, temel neden analizi, beyin fırtınası, derinlemesine görüşmeler ve standartlara dayalı değerlendirmeler gibi çeşitli yöntemler kullanılarak potansiyel riskler belirlenir. Bu faaliyetler, risklerin potansiyel kaynaklarını ve nedenlerini ortaya çıkararak iyi yapılandırılmış risk yönetimi stratejilerinin geliştirilmesine katkı sağlar (ISO 18128, 2024, s. 7).

Risk yönetimi sürecinde, tanımlanan risklerin önceliklendirilmesi, analiz edilmesi ve uygun tedbirlerin belirlenmesi için kontrol listeleri kullanılır. Bu listelerin oluşturulmasında SWOT analizi yaygın olarak kullanılan bir yöntemdir. SWOT (Strengths, Weaknesses, Opportunities, Threats- Güçlü Yönler, Zayıf Yönler, Fırsatlar, Tehditler) analizi, risklerin güçlü ve zayıf yönlerini, fırsat ve tehditlerini belirleyerek, risklerin kabul edilmesi, azaltılması veya transfer edilmesi gibi farklı stratejilerin belirlenmesine yardımcı olur. Kuruluşun iç ve dış bağlamdaki risk faktörlerini belirlemeye yönelik başvuru SWOT analizinin yanı sıra özellikle dış çevreden kaynaklanan siyasi, ekonomik, sosyo-kültürel, teknolojik, çevresel ve yasal faktörlerin yorumlanmasında PESTLE/PESTEL (Political, Economic, Social, Technological, Legal, Environmental - Politik, Ekonomik, Sosyal, Teknolojik, Hukuki, Çevresel) veya STEEPLE/STEEPLED (Social, Technological, Economic, Environmental, Political, Legal, Ethical - Sosyal, Teknolojik, Ekonomik, Çevresel, Politik, Hukuki, Etik) gibi modeller kullanılır. Bu modeller, SWOT analizini tamamlayarak kuruluşların dış çevreye daha iyi adapte olmalarını sağlar (ISO 18128, 2024, s. 9). PESTLE analizi, kuruluşların dış çevreyi analiz etmek için sıklıkla kullandığı bir araçtır. Ancak günümüzün karmaşık ve dinamik iş dünyasında, etik değerler ve demografik değişimler gibi faktörlerin de dikkate alınması gerekmektedir. Bu nedenle PESTLE analizine etik ve demografik faktörlerin eklenmesiyle geliştirilen STEEPLE (Sosyo-kültürel/Demografik, Teknolojik, Ekonomik, Çevresel, Politik, Yasal, Etik) analizi, kuruluşların dış çevreye daha kapsamlı bir bakış açısı kazanmasına ve daha iyi stratejik kararlar almasına yardımcı olur (Edin vd., 2016, s. 103; Koçiyit, 2014).

Çalışmanın bu başlığında (Risk Tanımlaması) yukarıda açıklanan analizlerden faydalanılarak elektronik belge yönetimine yönelik risk tanımlamalarına yer verilmektedir. Bu bölüm, 'Risk Tanımlaması' başlığı altında, elektronik belge yönetim sistemindeki (EBYS) riskler, dış çevresel faktörler, içsel faktörler, EBYS ve süreçleri olmak üzere dört ana başlık altında incelenmektedir. Bu kapsamda oluşturulan ve '2.1.1.5. EBYS ve Süreçlerine İlişkin Muhtemel Risk Tanımlamaları Kontrol Listesi' başlığı altında yer alan kontrol listesinde her bir risk, olası nedenler ve ortaya çıkabilecek sonuçlar dikkate alınarak sınıflandırılmıştır. Bu sayede, risklerin önceliklendirilmesi ve uygun risk yönetim stratejilerinin belirlenmesi kolaylaşmıştır.

2.1.1.1. Dış Etkenlere Bağlı Riskler

Kurumun faaliyet gösterdiği siyasi, ekonomik, sosyal ve teknolojik çevredeki değişimler, doğal afetler, ekonomik krizler, yasal düzenlemeler gibi dış etkenlere bağlı risk faktörlerini beraberinde getirir. Bu faktörler, kurumun strateji, operasyon, itibar ve finansal performansı üzerinde olumsuz etkiler yaratabilir. Bu nedenle bu tür risklerin belirlenmesi ve yönetilmesi, kurumun sürdürülebilirliği için büyük önem taşımaktadır. Dış etkenlerden kaynaklanan durum veya olayları tamamen engellemek mümkün olmasa da etkin bir risk yönetim sistemi kurum genelinde bu tür durumlara karşı daha sağlam ve isabetli kararlar alınabilme ihtimalini önemli ölçüde artırabilir (Usman ve Kaygusuz, 2019, s. 115).

ISO 18128:2024 standardına göre, kurumun faaliyet gösterdiği yasal, düzenleyici, sosyal, kültürel, teknolojik, ekonomik, doğal ve rekabetçi çevredeki değişimler, kurumun iş süreçlerini ve dolayısıyla belge yönetim sistemini doğrudan veya dolaylı olarak etkileyebilecek riskleri beraberinde getirir. Bu riskler, veri güvenliği ihlalleri, uyumsuzluk sorunları ve iş sürekliliği riskleri gibi çeşitli sonuçlara yol açabilir. Olası risk unsurları şu şekilde sıralanmaktadır (ISO 18128, 2024):

- a) Belgelerin oluşturulması, saklanması, erişilmesi ve imha edilmesi gibi kuruluşun belge gereksinimlerini etkileyen yasal ve düzenleyici değişiklikler,
- b) Kuruluşun belgelerini, belge süreçlerini ve sistemlerini etkileyen siber güvenlik, bulut bilişim veya açık veri politikaları gibi hükümet veya idari kuruluşların politikalarında yapılan değişiklikler,
- c) Kuruluşun belgelerini, belge süreçlerini ve sistemlerini etkileyen yeni standartlar veya uygulama kuralları,
- d) Mahremiyet veya unutulma hakkı³ konusunda farkındalığın artması gibi kamuoyunun ve paydaşların beklentilerinin değişmesi,
- e) Makine öğrenmesi yapay zekâ, uç bilişim gibi yeni teknolojilerin toplum genelinde tanıtılması ve benimsenmesi,

³ Unutulma hakkı, dijital ortamda kişi hakkında bulunan içeriklerin, kişinin yapacağı talep üzerine kaldırılması şeklinde tanımlanmış bir haktır. Bu hak, kişinin geçmişte yaşanmış olumsuz olayların veya artık güncelliğini yitirmiş kişisel verilerin internette izini silmesine imkân tanıyarak, dijital hafızada unutulmayı amaçlamaktadır. Dijital çağda bireylerin mahremiyetlerini koruma ve kişisel verileri üzerinde kontrol sahibi olma haklarını güçlendiren önemli bir haktır (Nalbantoğlu, 2018).

- f) Kuruluşun pazar veya müşteri tabanındaki değişiklikler,
- g) Deprem, kasırga, tsunami, sel, yangın, büyük fırtınalar veya uzun süreli kuraklık gibi bölgesel veya yerel çevresel yıkıcı olaylar,
- h) Savaş veya terör eylemlerinin kuruluşun tesislerine veya yakın çevresine büyük yapısal hasar verme veya hizmet sunumunda kesintiye neden olma potansiyeli,
- i) Salgın hastalıklar veya pandemi gibi halk sağlığına ilişkin potansiyel tehditler.

Elektronik belge yönetim sistem ve süreçlerine yönelik dış etkenlere bağlı riskleri genel olarak siyasi-toplumsal bağlamdaki değişiklikler, makroekonomik çevre ve altyapı, fiziksel çevre ve alt yapı, dış güvenlik tehditleri şeklinde sıralamak mümkündür.

2.1.1.1.1. Siyasi-Toplumsal Bağlamdaki Değişiklikler

Dünya genelinde, hukuk sistemleri güvenilir delillere erişime dayanmaktadır ve bu deliller genellikle üç temel biçimde sunulmaktadır. Bunlardan birincisi, ilk elden tanıklar veya uzmanlar tarafından sağlanan sözlü ifadelerdir. İkincisi, suç mahallinde bulunan nesneler gibi fiziksel kanıtlardır. Üçüncüsü ise belgesel kanıtlardır. Bu belgeler, hukuki süreçlerde delil olarak kullanılmak suretiyle, devlet ile vatandaş arasındaki anlaşmazlıkların çözümünde, kurumlar ile çalışanlar arasındaki iddiaların ispat veya reddi süreçlerinde hayati bir rol oynamaktadır. Dolayısıyla, belgelerin nasıl yönetileceğini anlamak için belgelerin üretilip yönetilmesi gereken yasal bağlamın anlaşılması gerekmektedir. Her bir kuruluş, iş yapma şeklini belirleyen yasalara ve politikalara tabi olup bu yasalar ve politikalar, elektronik belgelerin oluşturulması, saklanması ve yönetilmesi süreçlerini etkilemektedir. Ayrıca kuruluşların kendi kültürleri veya çalışma biçimleri, aldıkları kararları ve yaptıkları eylemleri de etkilemektedir. Bu bağlamda belge yönetimi, kuruluşların güvenilir delillere erişimini sağlamanın yanı sıra yasal uyumluluğunu ve iş süreçlerini optimize etmenin önemli bir unsuru haline gelmektedir. Belgelerin güvenliğini, bütünlüğünü ve erişilebilirliğini sağlayarak kuruluşların hukuki yükümlülüklerini yerine getirmelerine ve daha etkin bir şekilde yönetilmelerine yardımcı olmaktadır (International Records Management Trust (IRMT), 2009a, ss. 39-40). Ancak ulusal ve uluslararası düzeydeki siyasi ve toplumsal iklimdeki değişiklikler kurumun belge yönetiminde belirsizlik alanları

oluşturarak riskler meydana getirebilmektedir. Bu risk alanları şu şekilde açıklanabilir (ISO 18128, 2014):

- a) Kurumun belge gerekliliklerini etkileyen yasal ve düzenleyici değişikliklerin olması,
- b) Kurumun belgelerini, belge yönetim süreçlerini ve sistemlerini etkileyen hükümet politikalarının değişmesi,
- c) Kurumun belgelerini, belge yönetim süreçlerini ve sistemlerini etkileyen yeni standartlar veya uygulamaların ortaya çıkması,
- d) Belge yönetim hizmetlerine yönelik işlemleri yapan kişi veya birimlerin taleplerinin değişmesi,
- e) Paydaşların beklentilerinin değişmesi.

Siyasi ve toplumsal değişimler, elektronik belge yönetim sistemlerinde veri güvenliği, veri bütünlüğü ve veri gizliliği gibi temel prensiplerin ihlal edilme riskini artırmaktadır. Bu durum, siber saldırılar, doğal afetler veya siyasi baskılar gibi çeşitli nedenlerle ortaya çıkabilecek veri kayıpları, veri bozulmaları ve yetkisiz erişim gibi sorunlara yol açabilmektedir. Ayrıca değişen yasal düzenlemeler veya politikalar, belge yönetimi süreçlerini etkileyebilmekte ve kurumların mevcut uygulamalarını uyumlu hale getirmelerini gerektirebilmektedir. Siyasi baskılar veya toplumsal talepler, belge içeriğinin manipüle edilmesine veya sansürlenmesine yol açabilmekte, bu da güvenilirlik ve bütünlük açısından risk oluşturabilmektedir. Bu çerçevede, siyasi ve toplumsal değişikliklerin, elektronik belge yönetimi süreçlerine ilişkin güvenlik, erişim ve bütünlük gibi temel alanlarda risklerin artmasına neden olduğu ifade edilebilir. Örneğin, 2000’li yılların başından itibaren elektronik belge yönetimine ilişkin çalışmalar tüm dünyada olduğu gibi ülkemizde de hız kazanmıştır. Bu dönüşüm, basılı ortamda gerçekleşen geleneksel belge yönetimi faaliyetlerini geride bırakırken Elektronik İmza Kanunu, Standart Dosya Planı (SDP) çalışmaları, Elektronik Belge Standardının oluşturulması ve sonrasında EBYS’lerin kurumlarda zorunlu hale getirilmesi gibi önemli gelişmeleri de beraberinde getirmiştir. Bu gelişmeler, basılı ortamda üretilen belgelerin elektronik ortama entegrasyonundan doğan belge bütünlüğüne ilişkin optik karakter tanıma (OCR) hataları, üstveri

kayıpları, format uyumsuzlukları ve veri bozulmaları gibi sorunların ortaya çıkmasına neden olmuştur.

2.1.1.1.2. Makro Ekonomik ve Teknolojik Çevre

Ekonomik büyüme, enflasyon, döviz kuru gibi makroekonomik faktörlerdeki dalgalanmalar, işletmelerin bilgi teknolojisi bütçelerini ve siber güvenlik yatırımlarını doğrudan etkileyerek elektronik belgelerin güvenliği ve yönetimi üzerinde olumsuz sonuçlar doğurabilir. Bu durum, veri yedekleme sistemlerine yapılan yatırımların azalması, güncel güvenlik yazılımlarının satın alınmaması ve personel eğitimlerinin aksamasına neden olarak siber saldırılara karşı daha savunmasız hale gelme riskini artırmaktadır. Makroekonomik ve teknolojik çevreye yönelik risk oluşturabilecek unsurlar şu şekilde açıklanabilir (Yalçınkaya, 2014, s. 18-19):

- *Yönetim önceliklerini ve organizasyonların gelir ve mülkiyet haklarını doğrudan etkileyebilecek değişiklikler, belge yönetiminde belirsizliğe ve dolayısıyla riske yol açabilir. Örneğin, yeni yasal düzenlemeler, ekonomik dalgalanmalar gibi faktörler belgelendirme ve arşivleme süreçlerinde önemli değişikliklere ihtiyaç duyulmasına neden olabilir. Bu durum hem maliyet artışlarına hem de istenmeyen gecikmelere yol açarak risk oluşturabilir.*
- *Organizasyonların amaç ve fonksiyonlarında meydana gelen önemli değişimler, işleyişi olduğu kadar belge yönetim elemanlarını da etkileyebilir. Bu durum, belge yönetim sisteminde beklenmedik süreçlere ve risklere yol açabilir. Örneğin, bir şirketin faaliyet alanını değiştirmesi veya yeni bir departman kurması, belgelendirme ve arşivleme prosedürlerinde güncellemeler yapılmasını gerektirir. Zamanında ve doğru şekilde yapılmayan güncellemeler, belge yönetiminde tutarsızlıklara ve eksikliklere neden olabilir.*
- *Mevzuat düzenleyicilerinin yetersizliği ve dış faktörlerin artan/çeşitlenen belge taleplerine cevap verebilecek bir yapının inşa edilememesi, belge yönetimi stratejilerinde belirsizlikler yaratarak yasal uyumsuzluk riskini artırır. Sektörel düzenlemelerin sıklaşması ve yeni veri koruma yönetmeliklerinin ortaya çıkması gibi durumlar, kurumların belge yönetim sistemlerini sürekli olarak güncellemesini gerektirir.*
- *Hukuki süreçlerde şeffaflık taleplerindeki artış, belge taleplerine de yansımaktadır. Artan dava sayısı, belge yönetimi açısından planlamada*

gecikmelere ve ek iş yüküne neden olabilir. Bu durum, zamanında doğru belge sunabilmeye ilişkin riski artırır ve davaların uzamasına veya olumsuz sonuçlanmasına yol açabilir.

- *Toplum genelinde yeni teknolojilerin yaygınlaşması ve benimsenmesi, ilk bakışta belge yönetimini doğrudan etkileyen bir risk faktörü olarak algılanmayabilir. Ancak bu durum, belge yönetimiyle ilgili belirsizlikleri beraberinde getirir. Örneğin, mobil cihazların ve sosyal medyanın iş çevrelerinde yaygınlaşması, belge yönetimiyle ilgili yeni politikaların ve prosedürlerin geliştirilmesini gerektirebilir. Aksi takdirde, bu yeni teknolojilerin kullanımı, belge güvenliğinde riskler oluşturabilir veya belge yönetim süreçlerinde tutarsızlıklara yol açabilir.*

Kurumlar, teknolojik ilerlemeleri geliştirmeye veya bünyelerine katmaya devam ettikçe yeni ve bazen daha büyük risklerle karşı karşıya kalabilir. Bu nedenle her yeni cihaz, platform, yazılım uygulaması veya iş modeliyle birlikte gelen riskleri tanımlamak ve değerlendirmek kuruluşlar için oldukça önemlidir. DiNapoli (2016, s. 17), bu aşamada yönetimin sorması gereken soruları şu şekilde sıralamaktadır:

- *Yeni teknoloji, kuruluşun misyonunun gerçekleştirilmesine nasıl katkıda bulunuyor?*
- *Yeni teknoloji, hedeflere ulaşılmasını engelleyebilecek riskleri artırıyor mu? Örneğin, veri güvenliğinin azalması, sık veya uzun süreli hizmet kesintileri.*
- *Bu riskleri yönetmek için iç kontrol faaliyetlerinde (örneğin, erişim kontrolleri, veri yedekleme, güncellemeler vb.) hangi değişiklikler gerekmektedir?*

Yeni teknolojik entegrasyon projelerinde, belge yönetim sistemlerine yönelik siber saldırılar, veri kaybı, yetkisiz erişim, yasal düzenlemelere uyumsuzluk ve yeni teknolojilerin getirdiği risklerin belirlenmesi için bu soruların yanıtlanması son derece önemlidir. Belirlenen risklerin önceliklendirilmesi için Hata Türü ve Etkileri Analizi⁴-Failure Mode Effect Analysis (FMEA) gibi yöntemler kullanılarak veri şifreleme, erişim kontrol listeleri ve yedekleme gibi önlemler alınmalıdır. Bu sayede, iş

⁴ FMEA: Bir işletmedeki olası sorunları önceden belirleyerek, hataların oluşmasını engellemeye yönelik yapılan bir çalışmadır. Bu sayede, ürün veya hizmet kalitesi artırılır ve iş süreçleri iyileştirilir (DQS, 2023).

sürekliliği ve yasal uyumluluk sağlanabilir, veri sızıntıları önlenerek kurumların bilgi varlıkları korunabilir.

2.1.1.1.3. Fiziksel Çevre ve Altyapı

Fiziksel çevre, insanın yaşadığı ve etkileşimde bulunduğu, coğrafi (toprak, bitki örtüsü vb.), iklimsel (rüzgâr, güneş, yağış, sıcaklık vb.) ve duyuşsal (ses vb.) özelliklere sahip bir alandır (Yüksel, 2018, s. 109). Bu çevre, doğal afetler veya insan kaynaklı felaketler başta olmak çeşitli risk faktörlerini barındırmaktadır. Böylesi olaylar, fiziksel altyapıya zarar vererek iş sürekliliğini tehdit eder, belgelerin güvenliğini riske atar ve dolayısıyla kurumların temel hizmetlerini aksatabilir. Bu nedenle kurumlar, faaliyet gösterdikleri bölgelerin risk profillerini belirleyerek gerekli önlemleri almalı ve afet yönetimi planları hazırlamalıdır. ISO (18128, 2014), bu kapsamdaki risk alanlarını şu şekilde açıklamaktadır:

- a) *Doğal Afetler: Deprem, kasırga, tsunami, sel, yangın, fırtına, kuraklık gibi doğal olaylar ve iklim değişikliği kaynaklı sıra dışı hava olayları (aşırı sıcaklık dalgaları, şiddetli yağışlar vb.)*
- b) *İnsan Kaynaklı Krizler: Savaş, terör, siyasi istikrarsızlık, büyük çaplı göçler, endüstriyel kazalar, çevresel felaketler (radyoaktif sızıntı, petrol sızıntısı vb.) gibi insan faaliyetlerinden kaynaklanan krizler ve toplumsal olaylar.*
- c) *Altyapı ve Hizmet Kesintileri: Elektrik, su, atık yönetimi, bilgi teknolojisi, ulaşım, iletişim, sağlık hizmetleri gibi önemli altyapı ve hizmetlerin kesintiye uğraması veya yetersiz hale gelmesi.*

Kurumların belge yönetim sistemlerinin hem doğal hem de insan kaynaklı felaketlere karşı korunması, iş sürekliliği için son derece önemlidir. Bu kapsamda yaşanabilecek büyük bir kesinti durumunda kurum faaliyetlerinin devamlılığını sağlamak amacıyla detaylı bir iş sürekliliği planının oluşturulması gerekmektedir. Söz konusu plan, afet durumunda belgelerin nasıl kurtarılacağı, yedeklenmesi ve güvenli bir şekilde saklanması konularında net politikalar ve prosedürler içermelidir (IRMT, 2009a, s. 30).

2.1.1.1.4. Dış Güvenlik Tehditleri

Bir organizasyonun güvenliği, yalnızca fiziksel tesislerin değil aynı zamanda kullandığı sistemler, veriler ve iş süreçlerinin de korunmasını gerektirir. Başlıca dış

güvenlik tehditleri fiziksel ve siber saldırılardır. Bu yöntemlerle kurum ve kuruluşlara ciddi zararlar verilebilir.

Belge yönetim sistemlerine yönelik fiziksel ve siber saldırılar, yetkisiz erişim, veri sızdırma, veri bozma gibi sistem bütünlüğünü tehdit eden her türlü müdahale ciddi güvenlik riskleri oluşturmaktadır. Net ve uygulanabilir güvenlik politikalarının olmaması ve hassas verilerin yeterli güvenlik önlemleri olmaksızın saklanması ciddi riskler doğurmaktadır (Yalçınkaya, 2014, s. 19). Bu durum, kurumların itibar kaybına uğramasına, finansal zarar görmesine ve iş süreçlerinin aksamasına neden olmaktadır.

2.1.1.2. İç Etkenlere Bağlı Riskler

Risk yönetimi faaliyetlerine başlamadan önce kurumun kapsamlı bir şekilde değerlendirilmesi gerekmektedir. Bu değerlendirme, kurum kültürünün, iç paydaşların, organizasyonel yapının, mevcut kaynakların (insan, sistem, süreç, finansal) ve stratejik hedeflerin detaylı bir analizini içerir. Kurumu tam anlamıyla anlamak ve risk yönetimi çalışmalarına uygun bir çerçeve çizmek, başarılı bir risk yönetimi uygulamasının temelini oluşturur. AS/NZS Standardına göre bunun nedenleri şu şekilde sıralanabilir (AS/NZS 4360, 2004):

- *Risk yönetimi, kuruluşun amaç ve hedefleri bağlamında gerçekleşmektedir.*
- *Çoğu kuruluş için en büyük risk, stratejik hedeflerine ulaşamamak ve piyasada rekabet gücünü kaybetmektir.*
- *Kurumsal politika, hedefler ve çıkarlar kurumun risk politikasının tanımlanmasına yardımcı olmaktadır.*
- *Bir projenin başarı kriterleri, sadece kurumun hedefleriyle değil, aynı zamanda potansiyel riskler ve fırsatlar da göz önünde bulundurularak belirlenmelidir.*

Her kuruluş büyüme ve sürdürülebilirlik hedeflerine ulaşmak için risk yönetimi uygulamalarına ihtiyaç duymaktadır. Bu bağlamda, ISO 18128:2024 (ss. 22-23) standardı, kuruluşların karşılaşılabileceği iç etkenlere bağlı riskleri detaylı bir şekilde ele almaktadır. Bu riskler arasında; organizasyondaki değişiklikler (birleşme, devralma, yeniden yapılanma), politikalardaki değişiklikler, personel değişiklikleri, teknolojik gelişmeler ve finansal kaynakların yeterliliği gibi faktörler yer almaktadır. Örneğin, bir şirketin başka bir şirketi satın alması sonucu, iki farklı şirket kültürünün birleştirilmesi gibi bir riskle karşılaşılabılır. Bu tür değişiklikler, çalışanların yeni

prosedürlere uyum sağlamasında zorluklar yaşamasına neden olabilir. Özellikle elektronik belge yönetim sistemleri için, iç faktörler, belge yaşam döngüsünün her aşamasında çok çeşitli riskler oluşturmaktadır. Örneğin, yeni bir belge yönetim sistemine geçiş sırasında veri kaybı riski veya çalışanların yeni sisteme uyum sağlamamasından kaynaklanan verimlilik kayıpları gibi sorunlarla karşılaşmak mümkündür. İnsan kaynakları açısından ise, eğitimsiz personel nedeniyle yanlış belge düzenlemeleri yapılması, hukuki sorunlara yol açabilir. Bu risklerin etkili bir şekilde yönetilememesi, kuruluşların rekabet gücünü zayıflatabilir ve iş sürekliliğini tehdit edebilir. Bu riskleri yönetmek için düzenli yedekleme yapmak, çalışanları yeni teknolojiler konusunda eğitmek, iş süreçlerini iyileştirmek ve risk değerlendirme çalışmalarını düzenli olarak yapmak gibi önlemler alınabilir. Riskleri olasılık ve etki açısından değerlendiren bir risk matrisi oluşturarak hangi risklere öncelik verilmesi gerektiği daha net bir şekilde belirlenebilir.

2.1.1.2.1. Organizasyonel Değişim

Her ülkenin kendine özgü bir kültürü olduğu gibi, her organizasyonun da var olma amacı ve çalışma şekli bakımından kendine has özellikleri vardır. Bir kurumunun belgelerini etkin bir şekilde yönetebilmesi için, söz konusu kurumun kültürünü, yani kurumun içinde bulunduğu sosyo-politik, ekonomik ve örgütsel ortamı anlamak önemlidir. Aşağıda listelenen sorulara verilen yanıtlar, kuruluşun yapısını ve dolayısıyla bilgi ve belgeleri nasıl oluşturduğunu, kullandığını ve paylaştığını ortaya çıkaracaktır (IRMT, 2009a, s. 43).

- *Bu bir şirket, devlet kurumu, kâr amacı gütmeyen kuruluş veya bir dernek mi?*
- *Daha büyük bir kurumun içinde yer alan ve çok özel bir işlevi olan bir departman mı?*
- *Bu kuruluşun veya departmanın görev yetkisi nedir?*
- *Bu kuruluş veya departman hangi hizmetleri sunar?*
- *Bu kuruluş veya departman resmi yasalar ve yönetmeliklere mi yoksa gayri resmi kurallara mı bağlıdır?*
- *Bu kuruluş veya departman resmi bir yapıya göre mi yönetilir yoksa daha serbest bir yapıya göre mi?*

Belge yönetim faaliyetleri organizasyonel yapı göz ardı edilerek uygulandığında başarısızlığa uğrayabilir. Siyasi, finansal, yasal, işletme koşullarında veya diğer koşullarda meydana gelen değişiklikler, kurumun genel veya faaliyet düzeyinde yeniden yapılanmasını gerektirebilir. Birleşmeler, devralmalar, satın almalar, yeniden yapılanma ve küçülme gibi kurum içi değişiklikler, önemli risk alanları oluşturarak belge yönetim sistem ve süreçlerini etkileyebilir (Government Accountability Office, 2001).

Belge sahipliği ve erişim sorunları, belge yönetim sistemlerindeki değişiklikler, bilgi kaybı, politika ve prosedürlerdeki eksiklikler, personel ve eğitim sorunları ile afet durumlarına karşı hazırlıksız olma gibi çeşitli faktörler organizasyonel değişiklikler sırasında önemli sorunlara yol açabilir. Bu süreçte, belge devri, erişim kontrolü, sistem entegrasyonu, veri göçü, lisanslama, kurumsal hafıza, eski belge erişimi, politikalar, prosedürler, personel eğitimi, motivasyon kaybı ve afet planlaması gibi konularda önemli riskler ortaya çıkmaktadır (ISO 18128, 2014).

Belge yönetim sistemlerindeki dönüşümler kurumsal yapıda ve süreçlerde önemli değişiklikleri beraberinde getirmektedir. Bu değişimlerin başarıyla yönetilmesi, çalışanların ihtiyaçlarına uygun, kullanıcı dostu sistemlerin oluşturulmasına bağlıdır (IRMT, 2009b, s. 75).

2.1.1.2.2. Teknolojik Değişim

Bilişim teknolojilerinin kurumlarda yaygınlaşmasıyla birlikte, belge yönetimi faaliyetleri de elektronik ortama taşınmaya başlamıştır. Bu durum, belge saklama ve işleme süreçlerinde önemli bir verimlilik ve maliyet tasarrufu sağlamıştır. Ancak EBYS'nin kurulması ve işletilmesi, bilişim teknolojileriyle ilişkili çeşitli riskleri de beraberinde getirmiştir. Sistemlerin bilişim teknolojileriyle gelen riskler dikkate alınmadan oluşturulması güvenilir veriler üretilmesini zorlaştırmıştır (Yıldız, 2010). Bu durum, bireylerin elektronik bilgiye ihtiyaç duydukları her an ve istedikleri şekilde ulaşma ve bu bilgiyi kişisel kullanım amaçları doğrultusunda işleme yeteneklerini sınırlayarak dijital süreklilik kavramını zedelemektedir. Belge yönetimi, kurumların ihtiyaç duyduğu her türlü bilgi ve belgeye zamanında ulaşmasını, bu bilgileri doğru bir şekilde yorumlamasını ve belgelerin bütünlüğünü koruyarak güvenilirliğini sağlamasını mümkün kılar. Bu sayede dijital süreklilik sağlanır ve iş süreçleri en uygun hale getirilir.

Günümüzde bilgi ve belge yönetimi, teknolojik gelişmeler sayesinde birçok yenilik sunsa da elektronik belgelerin üretiminden arşivlenmesine kadar uzanan süreçte önemli zorluklarla karşı karşıyadır. Aydın ve Saydam (2019)'a göre, bu zorlukların her biri kurumlar için potansiyel riskler taşımaktadır. IRMT (2009a)'de belirtildiği gibi, teknolojik alt yapılar kurumlara birçok fayda sağlamasına rağmen, veri güvenliği, gizlilik, uyumluluk gibi konularda önemli sorunlara yol açabilmektedir. Bu nedenle bilgi ve belge yönetimi süreçlerinde ortaya çıkan bu zorlukların titizlikle analiz edilmesi ve uygun önlemlerin alınması gerekmektedir.

Teknolojinin hızla gelişmesiyle birlikte kurumlar, teknolojik eskime, iş süreçlerinin teknolojiye bağımlılığı, belge kaybı riskleri, güvenlik sorunları, maliyet artışları ve uzman personel ihtiyacı gibi bir dizi yeni sorunla karşı karşıya kalmaktadır (IRMT, 2009a).

Elektronik belgelerin korunması ve saklanması için kullanılan ortamların zamanla değişebileceğinin göz ardı edilmemesi gerekmektedir. Örneğin, bir kuruluş tarafından son on yılda arşivlenen çok sayıda belge, depolama ortamında hasar görmesi veya eski dosya formatlarının daha yeni, günümüzde kullanılan biçimlerle uyumsuz olması nedeniyle artık erişilemez veya okunamaz hale gelebilir. Elektronik belgelerin hukuki geçerliliği için güvenli arşivleme zorunluluğu, hızla değişen teknolojiler nedeniyle ek maliyetlere yol açmaktadır. Eski depolama ortamlarının veya veri formatlarının desteklenmemesi, verilerin geri alınımını (yeniden okunabilirliğini) güçleştirmekte ve yüksek maliyetli dönüşüm işlemlerini gerektirmektedir (Hamidoviç, 2010). ISO 18128'e göre (2014), bir kurumun yeni bir belge yönetim sistemine geçiş yapması, entegrasyon, uyumluluk, belge taşıma, sorumlulukların yeniden tanımlanması, değişiklik yönetimi, politika güncellemeleri, personel eğitimi ve altyapı değerlendirmesi gibi bir dizi karmaşık ve birbirine bağlı süreci içermektedir. Bu süreç kurumlar için büyük fırsatlar sunduğu gibi önemli zorlukları ve riskleri de beraberinde getirmektedir. Bu nedenle teknolojik dönüşüm sürecinde kapsamlı bir planlama ve risk değerlendirmesi yapmak, kurumların başarıya ulaşması için büyük önem taşımaktadır.

2.1.1.2.3. İnsan Kaynakları, Yetkinlikler ve Finansman

Kurum ve kuruluşlarda yeni bir programın geliştirilmesi için yönetimin onayına ve bütçeye gereksinim duyulmaktadır. Bu onay ve bütçeyi alabilmek için üst düzey yönetimin, böyle bir programın neden gerekli olduğunu anlayabilmesi gerekmektedir.

Herhangi bir elektronik belge yönetimi sistemi, programı veya projesinin başarısı, büyük ölçüde üst düzey yönetimin desteğine bağlıdır (IRMT, 2009b, s. 11). Ayrıca sistemin satın alınması, değiştirilmesi, yeni projelere başlanması hususunda karar üst yönetim tarafından verildiğinden dolayı EBYS yazılımı ve buna ait iş süreçlerini hem üst düzey yönetimin hem de personelin sahiplenmesi gerekmektedir. Yöneticileri ikna etmek ve finansmanı sağlamak kendi başına yeterli olmasa da yöneticinin projeye tüm süreç boyunca, özellikle de uygulama sırasında ilgi veya destek göstermesi elzemdir. Kullanıcılar (kurum çalışanları), yöneticinin sistemi kullanmadığını görür veya öğrenirse, otomatik olarak kendilerinin de bunu yapmak zorunda olmadığını hissederler (Leikums, 2012).

Elektronik belge yönetim sistemleri sadece belli bir departmana ya da belirli personelin kullanımına yönelik olmayıp kurumun genelini kapsayan bir uygulamadır (Yalçınkaya, 2016). Üst düzey yönetimin desteğinde veya personel eğiliminde meydana gelen değişiklikler sistemin geneli üzerinde olumsuz bir etki oluşturabilir ve çeşitli riskler meydana getirebilir (ICA, 2008).

ISO standartları çerçevesinde, insan kaynakları konusunda elektronik belge yönetim sistemlerinin karşılaşılabileceği riskler, personel yetkinlikleri, farkındalık kültürü, yönetim desteği, risk yönetimi, performans değerlendirme ve finansal kaynaklar gibi başlıklarda incelenebilir. Personel eğitimi, iş birliği, veri güvenliği, yasal uyum ve sürekli iyileştirme gibi konular, belge yönetimi sistemlerinin başarısı için son derece önemlidir. Yönetimin aktif desteğiyle risklerin sistematik olarak belirlenmesi ve uygun önlemlerin alınması, kurumların bilgi varlıklarını koruması ve iş süreçlerini iyileştirmesine olanak tanır (ISO 18128, 2014).

Elektronik belge yönetimi, kurumların verimliliği ve güvenliği açısından büyük önem taşır. Bu süreçte, personelin bilgi düzeyi, farkındalığı ve yetkinlikleri, sistemin başarısını doğrudan etkiler. Nitelikli personel eksiklikleri, yetersiz eğitimler, sorumlulukların belirsizliği gibi faktörler pek çok önemli risklere yol açabilir. Bu nedenle kurumların belge yönetimi sürecine dahil olan personelin düzenli olarak eğitmesi, farkındalık programları düzenlemesi ve rol ve sorumlulukları net bir şekilde tanımlaması gerekmektedir. Ayrıca çalışanların istifa etmesi durumunda bile bilgi devri süreçlerinin etkin bir şekilde yönetilmesi ve yeni personelin hızlı bir şekilde sisteme entegre edilmesi önem arz etmektedir. Aksi takdirde kurumların kurumsal

hafızası zarar görebilir ve iş sürekliliğine yönelik riskler artabilir. Özellikle yasal düzenlemeler, veri gizliliği ve siber güvenlik konularında çalışanların sürekli olarak bilinçlendirilmesi, kurumların bu alandaki risklerini en alt düzeye indirmelerine yardımcı olacaktır (Lin, 2020).

Belgelerin uygun şekilde yönetilmesini sağlamak için belge uzmanının, ilgili tüm yasal düzenlemeler ve kurum içi politikalar hakkında derinlemesine bilgi sahibi olması gerekmektedir. Yalnızca yasal çerçeveleri bilmek yeterli olmayıp bu düzenlemelerin iş süreçlerine nasıl entegre edilmesi gerektiği konusunda da uzmanlaşması önemlidir. Belge uzmanları, bilgi yaşam döngüsü yönetimi süreçlerini iyileştirerek, kurumun yasal uyumluluğunu sağlayabilir ve riskleri en aza indirebilir (IRMT, 2009a, s. 42).

Eğitim ve İletişim

Yeni bir bilgi sistemi (EBYS) kurulurken sistemin başarılı bir şekilde benimsenmesi ve kullanılması için etkili bir eğitim ve iletişim stratejisi hayati önem taşır. Farklı seviyelerde ve rollerdeki personelin ihtiyaçlarına göre özelleştirilmiş eğitimler, sistemin doğru ve verimli kullanılmasını sağlar. Yöneticilerin eğitime öncülük etmesi, sistemin organizasyon içinde yaygınlaşmasını hızlandırırken bilgi işlem personeli ve belge yöneticileri de kendi alanlarında uzmanlaşarak sistemin teknik altyapısını ve iş süreçlerini desteklerler. Sistem kullanıcılarına yönelik düzenli bilgilendirme ve eğitimler ise, çalışanların değişime daha kolay adapte olmalarını ve yeni sisteme aktif katılım göstermelerini sağlar. Bu sayede hem bireysel performans artırılabilecek hem de kurumun genel belge yönetim süreçleri iyileştirilecektir (IRMT, 2009b, s. 64).

2.1.1.3. Sistem Faktörüne Bağlı Riskler

Çağdaş işletmelerde, yazılım uygulamalarının yaygın kullanımıyla birlikte, kurumsal bilgi yönetimi büyük önem kazanmıştır. Bu bağlamda, iş süreçlerine ilişkin güvenilir belgelerin oluşturulması, saklanması ve imhası, kurumların etkinliğini ve sürdürülebilirliğini sağlamak için önemli bir hale gelmiştir. Belgeler, sadece kurumun yasal ve hesap verebilirlik yükümlülüklerini yerine getirmesine yardımcı olmakla kalmaz, aynı zamanda iş süreçlerinin belgelenmesi, iyileştirilmesi ve sürekli geliştirilmesi için de temel bir girdi oluşturur. Belgelerin eksikliği veya yetersizliği, kurumların iş sürekliliği, rekabet gücü ve itibarı üzerinde olumsuz etkiler yaratabilir. ISO 16175 standardına göre (2020, ss. 4-5), belgeler bir kuruluşun bilgi varlıklarının temelini oluşturur. Bu standart, belgelerin kurumun işleyişini destekleyen, karar verme

süreçlerini iyileştiren ve yasal uyumluluğu sağlayan önemli bir araç olduğunu vurgulamaktadır. İyi bir belge yönetimi sistemi, kurumsal hafızayı korur, bilgi paylaşımını kolaylaştırır ve iş süreçlerinin verimliliğini artırır.

Bilgi toplumu ve e-devlet stratejilerinin bir sonucu olarak Türkiye’de birçok kamu kurumu, temin ettikleri yazılımlar aracılığıyla elektronik belge yönetimine geçiş yapmıştır. Ancak EBYS projelerinin bir kısmı, başta teknik alt yapı olmak üzere yazılım geliştirme yaşam döngüsü boyunca ortaya çıkan çok sayıda risk faktörü nedeniyle beklenen verimliliği gösterememektedir. Elzamly ve diğerlerinin (2016) araştırmasına göre, bu risk faktörlerinin sayısı 50’yi aşmaktadır. Bu durum, EBYS projelerinin başarısız olmasının yanı sıra kurumların dijital dönüşüm süreçlerinde gecikmelere ve maliyet artışlarına neden olabilmektedir (Çiçek, 2020, s. 381). ISO 18128 (2024, s. 25) standardı, belge yönetim sistemlerindeki bu sorunların altında yatan nedenleri risk unsurları çerçevesinde ortaya koymaktadır:

- a. *Sistem tasarımı, konfigürasyonu ve uygulanması,*
- b. *Destek ve bakımın güvenilirliği de dâhil olmak üzere sistem teknolojisindeki değişiklikler,*
- c. *Sistemin ve verilerin nerede tutulacağı: Şirket içi, bulut veya hibrit,*
- d. *Sistemin birlikte çalışabilirliği: Belge sisteminin dâhili veya harici diğer sistemlere bağımlılığı ve bunlarla ilişkileri,*
- e. *Sistemin sürekliliği ve sürdürülebilirliği: Dijital belgelerin zaman içinde katlanarak büyümesini sürdürme ve yönetme yeteneği,*
- f. *Personelin veya işletmenin sistemi nasıl kullandığı,*
- g. *Belgelerin kaybı, belgelerin orijinalliğinin, güvenilirliğinin ve bütünlüğünün zarar görmesi ve belgelere erişim sorunu, yetkisiz işlemler ile ilişkili dış tehditler.*

EBYS, kurumların belgelerini dijital ortamda etkin bir şekilde yönetmelerini sağlayan kapsamlı bir sistemdir. Ancak bu sistemin tasarımı, konfigürasyonu, uygulaması ve kullanımı süreçlerindeki hatalar, teknolojik gelişmeler, veri güvenliği riskleri, personel hataları ve siber saldırılar gibi çeşitli faktörler, sistemin güvenliğini ve performansını olumsuz etkileyebilir.

2.1.1.3.1. EBYS Tasarımı

Başarılı bir elektronik belge yönetimi tasarımı, yalnızca bir yazılım satın almak ve kuruluş genelinde kullanımını sağlamaktan çok daha fazlasını gerektirmektedir. Bir EBYS'nin tedarik edilmesi, kurum tarafından geliştirilmesi veya mevcut sistemin güncellenmesine yönelik yapılacak işlemlerden önce iyi planlanmış bir proje hazırlanması gerekmektedir (IRMT, 2009b).

EBYS, kurumların tüm yönetsel fonksiyonlarını kapsayan ve farklı disiplinlerden uzmanların katılımını gerektiren kapsamlı değişim projeleridir. Sadece teknolojik bir altyapı kurulumu değildir. Projelendirilmeden ve kurumsal gereksinimler belirlenmeden rastgele sağlanan bir yazılım ile elektronik belge yönetim sürecine dahil olmak, kamu kaynaklarının boşa harcanmasına yol açacaktır (Özdemirci vd., 2013, s. 31). Bu nedenle gereksinim duyulan, en uygun, sistemin belirlenmesi önem arz etmektedir. EBYS seçme ve uygulama sürecinin ilk adımı, yazılım ile tam olarak neyin başarılmak istendiğini belirlemektir. Her kurumun kendine özgü işlevleri ve ihtiyaçları olduğu göz önünde bulundurulduğunda, bir sistemi benzerlerinden ayıran birçok özel fonksiyon olabilir. Yine de tüm kurumlar için genel olarak gereksinim duyulan çekirdek özellikler vardır. Bunlar şu şekilde sıralanabilir (IRMT, 2009b; TS 13298, 2015):

- a. *Belgelere sınıflandırma kodları atama,*
- b. *Saklama süreleri belirleme,*
- c. *Elektronik belgelerin alınmasını, saklanmasını, transferini ve imhasını yönetme,*
- d. *Gizli belgeler için güvenlik ve gizlilik sağlama,*
- e. *Depolama kullanımını optimize etme ve belge arama süresini kısaltma,*
- f. *Kâğıt belgeleri tarama ve dijital görüntüleme,*
- g. *Giriş/çıkış işlevi ile kâğıt ve elektronik belgeleri izleme.*

Bu temel özellikler, EBYS'nin kurumun belge yönetimine dair ihtiyaçlarını karşılaması için bir dizi temel fonksiyon oluşturmaktadır.

Bir EBYS'den tam olarak ne beklendiğini belirlemek için, mevcut belge yönetimi ortamının ve kullanıcıların beklentilerinin net bir şekilde anlaşılması gerekir. İlk adım, mevcut belge yönetimi programını gözden geçirerek eksiklikleri ve değişiklik gerektiren alanları tespit etmektir. Bu sayede hangi elektronik belge yönetim

uygulamasının seçileceğine karar vermeyi etkileyebilecek unsurlar belirlenmiş olur. Kullanıcı beklentileri de karar sürecinde önemli bir rol oynayabilir. Örneğin, tapu kadastro müdürlüklerinde çalışan EBYS kullanıcıları, klasik belge formatının yanı sıra parseller, haritalar gibi coğrafi verilere de ihtiyaç duyarlar. Bu nedenle EBYS yazılımının, coğrafi bilgi sistemleriyle entegre çalışabilmesi ve kullanıcıların farklı veri tabanlarında eş zamanlı arama yapabilmesini sağlayan güçlü arama yeteneklerine sahip olması gerekmektedir (IRMT, 2009b, ss. 48-49).

Sistemin tasarımı ve uygulaması aşamalarında belgelerin tanımlanması, saklama süreleri, yönetim süreçleri, sistemin kurumun ihtiyaçlarına uygunluğu, tedarikçi desteği ve teknik belgelere erişim gibi faktörler detaylı bir şekilde analiz edilmelidir. Bu sayede potansiyel riskler önceden öngörülerek sistemin etkin, güvenli ve sürdürülebilir bir şekilde kullanılması sağlanır (ISO 18128, 2014).

EBYS seçiminde dikkat edilmesi gereken en önemli konulardan biri teknik şartnamelerdir. Teknik şartnameler, sistemin kurumun ihtiyaçlarına uygun olarak tasarlanmasını ve uygulanmasını sağlayan temel bir belgedir. Bu belge, sistemin işlevsellik, performans, güvenlik ve uyumluluk gibi özelliklerini detaylı bir şekilde tanımlayarak hem satıcı firma için net bir yol haritası oluşturur hem de projenin başarıyla tamamlanmasını sağlar (Güler, 2018). Ancak teknik şartnamelerin hazırlanmasında belge yönetimi disiplininin kopuk hareket etmek, sistem tasarımında eksikliklere ve sorunlara yol açabilir. Bu nedenle teknik şartnamelerin hazırlanmasında deneyimli belge yöneticilerinin ve ilgili birimlerin katılımı, ilgili standartların dikkate alınması ve bilgi işlem birimi ile iş birliği yapılması büyük önem taşır (Eroğlu, 2019, s. 66).

2.1.1.3.2. EBYS Bakımı

EBYS'lerin sürekliliği ve güvenliği için düzenli bakım büyük önem taşır. Sistemde yapılan değişiklikler, yöneticilerin bilgi düzeyi, tedarikçinin güvenilirliği, bakım prosedürleri, teknik dokümantasyon, yedekleme ve geri yükleme gibi faktörler, bakım sürecinde risk oluşturabilir. Bu riskleri azaltmak için, değişikliklerin önceden değerlendirilmesi, yetkin personelin görevlendirilmesi, güvenilir tedarikçilerle çalışılması, kapsamlı bakım prosedürleri oluşturulması, detaylı dokümantasyonun tutulması ve düzenli yedekleme ile geri yükleme testlerinin yapılması gibi önlemler alınmalıdır (ISO 18128, 2014).

Bilgi Teknolojisi Altyapıları

Bilgi teknolojileri 20. yüzyılın sonlarından itibaren yaygınlaşmaya başlamış ve kullanım alanı hızla genişlemiştir. Günümüzde en basit işlemlerden en karmaşık olanına kadar tüm işlemler bilgi teknolojileri aracılığıyla yürütülmektedir (Bektaş Şeker, 2005, s. 377). Bu teknolojiler verilerin kaydedilmesi, saklanması, işlenerek bilgi üretilmesi, üretilen bilgilerin depolanması, erişimi, dağıtımı gibi süreçlerin etkili ve verimli bir şekilde yürütülmesini sağlamaktadır. Bilgi teknolojilerinde üç temel alt yapı elemanı bulunmaktadır (Kaya Bensghir, 1996). Bunlar dokunabildiğimiz ve görebildiğimiz ana kart, bellek, monitör, işlemci gibi fiziksel ve elektronik yapıyı oluşturan donanım; bilgisayarın anlayabileceği dilde yazılan yapacağı işleme göre komutlardan oluşan programı ifade eden yazılım (Erses vd., 2014, s. 8) ve küresel çapta uygulama, servis ve belgeye erişim sağlayan ağıdır (Karaca, 2006 s. 409).

Bilgi teknolojileri altyapısının etkin yönetimi, işletmelere verimlilik, maliyeti düşürme, güvenlik ve rekabet avantajı gibi birçok fayda sağlar. Bu altyapının başarısı, iyi bir stratejik planlama, risk yönetimi, nitelikli personel ve doğru prosedürlerin bir araya gelmesiyle mümkündür. Elektronik bilgi/belge sistemlerinin ve ağların başarıyla çalışması için sadece güçlü bir donanım ve yazılıma sahip olmak yeterli değildir. Ayrıca bu sistemleri destekleyen teknik altyapı ve bu altyapıyı yöneten ekibin yetkinliği de son derece önemlidir (Bıçakçı, 2022). Bu bağlamda elektronik belge yönetim sistemlerinin etkin çalışması için modern ve uyumlu donanım, yeterli güç kaynağı, kaliteli ağ bağlantısı ve yeterli bant genişliğinden oluşan güçlü bir teknik altyapıya gereksinim duyulmaktadır. Ayrıca teknolojik altyapıyı yönetecek bilgi ve beceriye sahip ve güncel teknolojilere hâkim yetkin bir ekibe ihtiyaç duyulmaktadır. Elektronik belge yönetim sistemi ve sürecinin başarısı, bu iki unsurun yanı sıra sistemdeki olası sorunlara karşı geliştirilmiş strateji ve politikalarla da yakından ilgilidir (IRMT, 2009a, ss. 31-32).

Teknik Destek

Teknik destek, kurumların bilgi sistemlerinin güvenliği ve sürekliliği için vazgeçilmez bir hizmettir. Teknik destek bir sigorta gibi görülmeli ve ihmal edilmemelidir. Nitelikli bir teknik destek ekibi, olası sorunlarda hızlı çözümler üreterek iş süreçlerinin sorunsuz devam etmesine yardımcı olur. Kurumlar, lisanslı ve garantili ekipmanlara

yatırım yapmanın yanı sıra resmi bir teknik destek planı oluşturarak olası risklere karşı önceden hazırlıklı olmalıdırlar (IRMT, 2009a, s. 34).

Yedekleme Sistemleri

Sunucular üzerinde depolama aygıtının arızalanması, virüs bulaşması veya insan hatası gibi çeşitli nedenlerden dolayı sorunlar yaşanabilir. Bu tür sorunlar, verilerin kaybolmasına veya bozulmasına yol açabilir. Verilerin korunması için kurumlar düzenli yedeklemeler yapmalıdır. Yedekler genellikle manyetik bantlar gibi düşük maliyetli depolama ortamlarında saklanır. Ancak manyetik bantlar zamanla bozulabilir ya da yeni teknolojilere uyum sağlayamayabilir. Bu nedenle yedekleme verileri düzenli olarak en yeni medya ortamına kopyalanmalıdır. Kurumlar, yedekleme bantlarını çalışır durumda tutmalı veya yeni ekipman satın aldığı anda yedekleme verilerini yeni teknolojiye taşımalıdır (IRMT, 2009a, ss. 34-35).

2.1.1.3.3. Sürdürülebilirlik ve Süreklilik

Modern belge tanımında sürdürülebilirlik ve süreklilik, içeriğin (faaliyetle ilgili gerçekler), bağlamın (oluşturulduğu koşullar) ve yapının (parçalar arasındaki ilişki) temel unsurlarını kapsamaktadır (Ambira ve Kemoni, 2011, s. 115). Bu sayede belgelerin dijital çağda güvenilir ve kullanışlı bir şekilde yönetilmesi, uzun süreli korunması ve erişime hazır tutulması sağlanır. Belge yönetim sistemlerinin sürdürülebilirliği, kurumun dış ve iç ortamındaki değişikliklerin izlenmesine bağlıdır. Bu sayede belge sistemleri değişen ihtiyaçlara cevap verecek şekilde güncellenebilir.

Belge yönetim sistemleri için süreklilik planlaması, kuruluşun genel iş sürekliliği planı ile uyumlu olmalı ve riskleri göz önünde bulundurmalıdır. Kurulda iş sürekliliği planı yoksa belge uzmanı, öncelikleri belirleyerek belge sistemlerini değerlendirir ve hizmet kesintilerinden sonra geri yükleme prosedürleri oluşturur. Risk alanları arasında doğal afetler, siber saldırılar, insan hataları ve teknik arızalar yer almaktadır. Düzenli yedekleme, yetkisiz erişimi engelleyecek güvenlik önlemleri, personel eğitimi ve planın güncellenmesi gibi unsurlar da süreklilik planlamasında önemli konulardır (ISO 18128, 2014, s. 9).

Sürdürülebilir ve sürekli bir belge yönetim sistemi için kurumun iç ve dış çevresindeki değişimlere uyum sağlama, sistemin kapsamlı bir şekilde tanımlanması ve dokümantasyonu, sistem özelliklerinin bakımı, kararların belgelendirilmesi, sistemin

belgelerin kullanılabilirliğini sürdürmesi, veri aktarımı ve entegrasyon yeteneği, belgelerin uzun süreli saklanması, felaket durumlarında erişim sağlama ve acil durum planlaması gibi birçok faktörün dikkate alınması gerekmektedir. Bu süreçte sistemin düzenli incelenmesi, güncellenmesi ve yedeklenmesi belgelerin bütünlüğü, güvenliği ve erişilebilirliğinin sürdürülebilmesi için önemlidir (Lin, 2020).

2.1.1.3.4. Birlikte Çalışabilirlik

Bilginin kurumlar arasında ve bilgi sistemlerinde kullanılabilir ve transfer edilebilir olma yeteneği olarak tanımlanabilen birlikte çalışabilirliğin en geniş kapsamlı tanımı, etkin bilgi paylaşımıdır (Kalkınma Bakanlığı Bilgi Toplumu Dairesi, 2012, s. 4). Birlikte çalışabilirlik, kurum içi belge yönetim sürecinde rolü olan birimlerin uyumlu ve entegre bir şekilde çalışmasını gerektirmektedir. Dişli'nin (2019) çalışmasında da vurgulandığı gibi, kurumlarda etkin ve şeffaf bir yönetim anlayışının temelini oluşturur. Başarılı bir belge yönetimi için basılı ve elektronik belgeler birbirinden ayrılmaz bir bütün olarak ele alınmalı ve bu birimler arasında bilgi akışı kesintisiz olmalıdır. Kurumlarda etkin ve şeffaf bir yönetim anlayışının temelinde, belgelerin sistematik ve düzenli bir şekilde yönetilmesi yatar. Bu bağlamda, EBYS tek başına yeterli bir çözüm olarak görülmemelidir. Başarılı bir EBYS uygulamasının temelini oluşturan unsur, basılı belge yönetim süreçlerinin sağlam ve etkin bir şekilde işlemesidir. Basılı belge yönetim süreçlerinin kurumun tüm organizasyon yapısına uygun şekilde tasarlanması ve işletilmesi, birimler, kurumlar ve sistemler arası iletişim gücü elektronik belge yönetim sistemlerine geçişi kolaylaştırır ve bu süreci daha sağlıklı hale getirir. Bu bağlamda birlikte çalışabilirlik üç farklı perspektifte değerlendirilmelidir.

1. Belge yönetimi, elektronik ve basılı belgeleri birbirinden ayrılmaz bir bütün olarak ele alan bir disiplindir. Ancak örneğin, üniversitelerde basılı belgelerin yönetimi genellikle Genel Evrak ve Arşiv birimleri tarafından üstlenilirken standart dosya planı (SDP) ve Devlet Teşkilatı Merkezi Kayıt Sistemi (DETSİS) gibi işlemler Strateji Daire Başkanlığı, İdari Mali İşler ve Genel Sekreterlik gibi birimlerin sorumluluğundadır. Elektronik belge yönetimi, e-imza gibi işlemler ise EBYS Koordinatörlükleri veya Bilgi İşlem Daire Başkanlıkları tarafından yürütülmektedir. Bu durum, kurum ve kuruluşlarda belge yönetiminin tek bir merkezden yönetilmediğini ve farklı birimlerin farklı

sorumluluklar üstlendiğini göstermektedir. Başarılı bir belge yönetimi için bu birimlerin entegre bir şekilde çalışması ve bilgi akışının kesintisiz olması son derece önemlidir (Dişli, 2019, s. 39).

2. Kurumlarda iş ve işlemlerin yürütülmesinde farklı özelliklerde bilgi sistemleri kullanılmaktadır. Bu sistemlerde üretilen veri ve bilgilerin EBYS ile entegre çalışması önemlidir (Özdemirci vd., 2013, s. 104). Belge yönetim sistemleri gibi tüm bilgi sistemlerinin etkin kullanımı için sistemler arası birliktelik ve entegrasyon sağlamak önemlidir. Kurumlar, farklı birimler ve kuruluşlarla bilgi paylaşımı ve iş birliği yapabilmek için belgeler üretmekte ve saklamaktadır. Bu nedenle elektronik bir belgenin değerini ve işlevselliğini koruması için EBYS'lerin birlikte çalışabilirlik ve entegrasyon imkanları sunması en önemli hedeflerden birini oluşturmaktadır (Dişli ve Külçü, 2020).
3. EBYS, Kurum içinde kullanılan sistemlerin birlikte çalışabilirliğine ek olarak kurumların birbirleriyle iletişimine de aracılık etmektedir (Özdemirci vd., 2013, s. 104) Resmi yazışmaların EBYS üzerinden yapılması kurumlar arası birlikte çalışabilirliği önemli ölçüde artırmaktadır. Kurumların bu sistemleri kullanmama, reddetme gibi bir durumları yoktur. Çünkü mevzuatın 'Kamu kurum ve kuruluşlarınca resmî yazışmalar, elektronik ortamda e-Yazışma Teknik Rehberi'ne uygun olarak hazırlanan ve güvenli elektronik imza ile imzalanan belgelerle yapılır. Bu belgeler, elektronik ortamda muhatapları ile paylaşılır ve elektronik ortamda saklanır' maddesi aksi durumu ortadan kaldırmaktadır (Resmî Yazışmalarda Uygulanacak..., 2020, s. 2).

Sistemlerin yasal çerçevede kurumlar arası etkileşimi sağlayarak kullanıcıya hizmet verebilmesi için birlikte çalışabilir, uyumlu, güvenli, güvenilir ve denetlenebilir bilgi sistemlerine ihtiyaç vardır. Bu sistemlerin temel amacı, etkin bilgi paylaşımını sağlamak ve kamu hizmetlerini vatandaşların ihtiyaçlarına göre bütünleşik bir şekilde sunmaktır. Bu sayede bilgi teknolojilerine yapılan yatırımların geri dönüşü hızlanırken kullanıcı memnuniyeti de artacaktır. Ayrıca doğru ve güncel bilgilerin kamu kurumları arasında güvenli bir şekilde paylaşılması, kamu hizmetlerinin etkin sunulması ve gelişmiş karar destek süreçlerinin oluşturulması için önemlidir.

Birlikte çalışabilirlik konusunda önemli bir konu da belge sistemlerinin diğer iş sistemleri ile olan entegrasyonudur. Bu durum, veri güvenliği, yetkisiz erişim, veri

bütünlüğü gibi çeşitli güvenlik risklerini beraberinde getirmektedir. ISO 18128 standardına göre belge yönetim sistemlerinin diğer iş sistemleriyle entegrasyonu sırasında yetersiz tanımlama, dış kaynak bağımlılığı, standart uyumsuzluğu, teknolojik değişimlere açıklık ve üstveri yönetimi eksikliği gibi çeşitli sorunlarla karşılaşmaktadır. Bu sorunlar sistemlerin birlikte çalışabilirliğini olumsuz etkileyerek veri güvenliği, erişim kontrolü ve iş sürekliliği gibi konularda riskler yaratmaktadır. Belge yönetim sistemlerinin diğer iş sistemleriyle başarılı bir entegrasyonu için detaylı bir entegrasyon planı oluşturulmalı, farklı sistemler arasında ortak standartlar belirlenmeli, dış kaynaklara bağımlılık en alt seviyeye indirgenerek güvenlik önlemleri alınmalı, teknolojik değişikliklere uyum sağlayabilen esnek bir mimari benimsenmeli ve belgelerin üstverileri düzenli olarak güncellenmelidir (ISO 18128, 2014).

2.1.1.3.5. Güvenlik

Bilgi sistemleri, modern kuruluşların iş süreçlerinin ayrılmaz bir parçasıdır. Bu sistemler, siber saldırılar (kötü amaçlı yazılımlar, kimlik avı, hizmet engelleme saldırıları), doğal afetler ve insan kaynaklı hatalar gibi çeşitli tehditlere maruz kalmaktadır. Bu tehditler, veri gizliliği, bütünlüğü ve kullanılabilirliğini tehdit ederek iş sürekliliğini ve rekabet gücünü olumsuz etkileyebilmektedir (ISO 27000, 2018a, s. 11).

Bilgi sistemlerindeki güvenlik tehditlerinden önemli birini siber saldırılar oluşturmaktadır. Siber saldırılar, dijitalleşmiş ve bilgi toplumuna dönüşen ülkeler için ulusal güvenliği tehdit eden önemli bir risk tehdididir. Geleneksel saldırılardan farklı olarak siber saldırıların yöntemi, hedefleri ve etkileri beklenmedik ve çeşitli olabilir. Siber dünyada meydana gelen ‘savaşlar’ın sonuçları da öngörülemeyen boyutlara ulaşabilir. Bu durumun en çarpıcı örneklerinden biri 2007 yılında Estonya’ya yönelik gerçekleştirilen siber saldırıdır (Dilek vd., 2023 s. 332). Ülke çapındaki siber saldırılar yaşandığında, Estonya, bilgi ve iletişim teknolojilerinin toplumun tüm alanlarında yaygın kullanımı konusunda Avrupa’nın en gelişmiş ülkelerinden biriydi. Ancak doğal olarak bir toplum bilgi ve iletişim teknolojilerine ne kadar bağımlı olursa siber saldırılara karşı da o kadar savunmasız hale gelebilmektedir. Yaşanan siber saldırılar, tekil kurumlarla sınırlı kalmayıp ulusal güvenliği tehdit edebilecek bir boyuta ulaşmıştır. Bu durum, bilgi sistemleri, altyapı şirketleri ve bilgisayar kullanıcıları için

ortak güvenlik standartları ve yasal düzenlemelerin ihtiyacını açıkça göstermektedir. Estonya uluslararası düzeyde siber güvenliğin en önemli savunucularından biri haline gelmiş ve bu tür riskleri yönetebilmek adına birtakım önlemler almıştır. Ancak ülkeler bu tür olayları beklemeden siber altyapılarının güçlü olmasını sağlamalı ve kapsamlı bir risk değerlendirmesini yapmalıdır (Czosseck vd., 2011).

Kurum ve kuruluşların bilgi birikimleri günümüzde büyük oranda elektronik ortamlarda saklanmaktadır. Elektronik ortamların daha yaygın olarak kullanılmasıyla birlikte bu ortamlarda yer alan bilgilere yönelik riskler de artmaktadır. Çünkü elektronik ortamdaki bilgi ve belgelerin korunmasında fiziksel güvenlik önlemleri yetersiz kalmakta ve belgenin üretiminden imhasına kadar olan süreçte sorumluluğu bulunan tüm kullanıcıların güvenliğe katkı sağlaması gerekmektedir (Henkoğlu, 2016 ss. 109-110).

Belgelerin elektronik ortamda yaşam döngüsünü yöneten sistemlerin, belgelerin güvenliğini sağlamak için işletme bilgisini korumaları gereklidir. Güvenli bir ortam sadece belgelerin korunmasıyla sınırlı değildir. Aynı zamanda sistem erişimini yetkilendirmek ve yetkileri hiyerarşik bir düzende düzenlemek de gereklidir. Bu uygulama bir taraftan iş süreçlerini otomatikleştirirken aynı zamanda veri güvenliği ve yetkisiz erişimi önlemek için kullanıcı yetkilerinin detaylı bir şekilde tanımlanması ve sınırlandırılmasını gerektirir. Bu sayede sadece yetkili kullanıcıların belirli işlemleri gerçekleştirebilmesi sağlanır. Örneğin, belgeleri görüntüleme, çıktı alma, kopyalama veya iletim gibi işlemler, sistem tarafından sınırlandırılmalı veya izlenmelidir (Yalçinkaya, 2016, s. 70).

Sistemler iş bilgilerini güvenli bir ortamda tutmalıdır. Güvenlik amacıyla bir iş sürecini otomatikleştiren sistemler genellikle belirli bireylerin elektronik bilgilerle gerçekleştirebileceği eylemleri (örneğin, görüntüleme, yazdırma, düzenleme, kopyalama veya aktarma) sınırlayan önlemler içerir. Sistemler herhangi bir kayda (üstveriler dâhil) yetkisiz değişiklikler yapılmasına izin vermemeli ve izin verilen değişiklikler yapıldığında bunlar tamamen belgelenmelidir (ICA, 2008).

Belge yönetim sistemlerinin güvenliğini değerlendirmek için ISO 27000 standart serisine başvurulabilir. Bu standartlar, risk değerlendirmesi, erişim kontrolü, şifreleme gibi çeşitli güvenlik kontrollerini içermektedir. Belge güvenliği yalnızca fiziksel güvenlik değil, aynı zamanda veri gizliliği, bütünlüğü ve kullanılabilirliği gibi bilgi

güvenliği prensiplerini de kapsamaktadır. Günümüzde, bulut bilişim ve mobil cihazların yaygınlaşmasıyla birlikte belge yönetim sistemlerinin maruz kaldığı tehditler de çeşitlenmiştir. Bu nedenle değerlendirme sürecinde ISO 27005'in Ek B ile D bölümlerinde belirtilen belirsizlik alanlarına (örneğin, bulut hizmetlerinin güvenliği, mobil cihaz yönetimi) özel dikkat gösterilmelidir.

Güvenlik hususunda dikkat edilmesi gereken üç temel nokta şu şekilde açıklanabilir (ISO 18128, 2014):

- Kuruluşun belge, belge yönetim süreci ve sistemlerine ilişkin güvenlik politikası kapsamlı ve güncel olmalıdır.
- Belgeler, belge yönetim süreçleri ve sistemlere ilişkin erişim kuralları ve izinler net bir şekilde tanımlanmalı ve uygulanmalıdır.
- Belgelerin ve belge yönetim sistemlerinin depolanması, erişimi ve kontrolü ile ilgili olarak üçüncü taraflar için de politikalar oluşturulmalı ve kontroller sağlanmalıdır.

EBYS, elektronik belgelerin doğru şekilde kayıt altına alınması ve korunması için özel bir çaba gerektirmektedir. Aksi takdirde bu sistemler istenilen güvenliği sağlayamayabilir. Sahadaki birçok EBYS uygulama yazılımında da benzer riskler taşıma ihtimali yüksektir. EBYS'lerin ortaya çıkardığı ürünler, mevcut uygulama yazılımlarıyla kullanılabilir olsa da bu ürünler ve taşındığı ortamlar, uzun süre arşivlerde tutulmuş ve teknolojik göç ettirme koşulları iyi yönetilmemiş bilgi malzemesi için uygun olmayabilir. Bu nedenle standartlarda belirtilen kriterlere uygun şekilde korunup korunmadıklarıyla ilgili olarak henüz kesin bir sonuca varılamamıştır. Sonuç olarak yarının e-arşivlerini nelerin oluşturacağı hala tartışılmaya devam etmektedir (Çiçek, 2020, s. 379).

Bilgi güvenliği, belge yönetim sistemlerinin temelini oluşturur. Elektronik belgelerin fiziksel güvenliğinden, siber saldırılara karşı korunmaya kadar geniş bir yelpazede önlemler alınmalıdır. Erişim kontrolü, şifreleme ve yedekleme gibi temel güvenlik mekanizmalarının yanı sıra fiziksel altyapı, bilgi teknolojisi sistemleri ve kullanıcı izinlerinin titizlikle yönetilmesi gerekmektedir. Bir taraftan fiziksel erişim kontrolleri, yangın güvenliği sistemleri ve yedek güç kaynakları belgelerin fiziksel olarak zarar görmesini engellerken diğer taraftan güvenlik duvarları, anti virüs yazılımları ve kullanıcı kimlik doğrulama sistemleri siber tehditlere karşı koruma sağlar. Hassas

bilgilerin bulunduğu sistemlerde ise daha katı erişim kontrolleri ve şifreleme yöntemleri uygulanmalıdır. Bu önlemler, kurumun büyüklüğü, sektörü ve yönetmeliklere uyum zorunlulukları gibi faktörlere göre farklılık gösterebilir ancak genel olarak belge yönetim sistemlerinin güvenilirliğini sağlamak için hayati öneme sahiptir (IRMT, 2009d, s. 25).

Belgelere erişim, hassas bilgileri ve varlıkları korumak için kısıtlanabilir. Böylelikle kişisel verilerin (isim, adres, sosyal güvenlik numarası gibi), fikri mülkiyet haklarının (patentler, telif hakları), mülkiyet güvenliğinin (finansal bilgiler, sözleşmeler), devlet güvenliğinin ve yasal gizliliğin (avukat-müvekkil ilişkisi gibi) korunmasına yardımcı olur (Hamidoviç, 2010).

Yasal kabul edilebilirlik tartışmalarında bilgi güvenliği son derece önemlidir. Bu tartışmaların merkezinde genellikle saklanan bilgilerin doğruluğu yatar. ‘Elektronik bilgiler sistem tarafından kaydedildiğinde süreç güvenli miydi?’, ‘Doğru bilgiler elde edildi mi ve tam mıydı?’, ‘Depolama sırasında bilgiler kazara veya kötü niyetli bir şekilde değiştirildi mi?’ sorularına yanıt verirken bilgi güvenliğinin uygulanması ve izlenmesi, özgünlüğü kanıtlamanın anahtarıdır.

ISO 15489-1 (2016) standardına göre güvenilir bir EBYS, kurumsal faaliyetleri desteklemek amacıyla belgeleri sürekli, düzenli ve güvenli bir şekilde saklayıp yetkili kişilerin zamanında erişimine olanak tanımalı, belgelerin bütünlüğünü korumalı ve uzun süreli depolama imkânı sunmalıdır. Sistem aynı zamanda yetkili kişilerin belge üzerindeki işlemlerine olanak tanımalı, belgeleri kullanılabilir formatta sunmalı, veri aktarımı için mekanizmalar içermeli ve belgelerin tasfiye işlemlerine izin vermelidir. Bu unsurların sağlanması, EBYS’nin güvenilirliğini ve dolayısıyla kuruluşların bilgi varlıklarının korunmasını ve yasal gerekliliklere uyulmasını sağlar.

Belge sistemlerinin güvenilirliği, sistemin işletim prosedürlerinin, kullanılan teknolojilerin ve uygulanan güvenlik önlemlerinin detaylı olarak belgelendirilmesi ve işlem loglarının tutulmasıyla sağlanır. Bu sayede sistemin uyumluluğu ve güvenilirliği denetlenebilir.

ISO 15489-1:2016 standardı, elektronik belge yönetim sistemlerinin (EBYS) ‘güvenilir’ olmasının yanı sıra ‘güvenli’ olmasını da şart koşmaktadır. Güvenlik yetkisiz erişim, değiştirme, gizleme veya imha gibi tehditlere karşı belgelerin korunmasını ifade eder. Güvenliği sağlamak için erişim kontrolleri, izleme, kişi

doğrulaması ve yetkisiz imha gibi durumlara ilişkin tedbirlerin alınması gerekir. Bir belgeye uygulanan kontroller ve onlara başvurulduğu ile ilgili bilgiler belgenin işlem üstverilerinde kaydedilmelidir. Ayrıca belgelerle kayıt altına alınan iş ile ilgili riske bağlı olarak belgeyi etkileyen herhangi bir güvenlik olayı süreç üstverisi olarak belgelendirilmelidir. Son olarak örgütsel bilgi güvenliği ve iş sürekliliği tedbirleri, belge sistemlerine yönelik tedbirleri de kapsamalıdır. Bu düzenleme, elektronik belgelerin güvenliğini ve bütünlüğünü korumak için gerekli çerçeveyi sağlar.

EBYS, saklanan belgelerin orijinallliğini ve güvenilirliğini korumak için erişim kontrolü ve güvenlik işlevlerini içermelidir. Bu amaç doğrultusunda kullanıcı rollerine ve belge sınıflandırmalarına dayalı izinler, yetki seviyeleri ve erişim hakları gibi çeşitli yaklaşımlar kullanılır. Örneğin, bir insan kaynakları çalışanı yeni başvuru belgelerini görüntüleyebilirken disiplin dosyalarını göremez. Sistem, yetkisiz erişimi ve değişiklikleri engelleyerek belge yönetimi süreçlerinin bütünlüğünü korur. Bu erişim kontrolleri, belge yönetimi süreçlerinin ve etkinliklerinin bütünlüğünü korur (IRMT, 2009b, s. 53).

2.1.1.4. Elektronik Belge Yönetim Süreçlerindeki Riskler

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 üretilmesinden imhasına kadar, oluşturulmasını, saklanmasını, erişilmesini ve geri alınmasını, bakımını, güvenliğini ve imhasını içeren bilgisayar teknolojisi ve sistemleri aracılığıyla yönetilmesini gerektirmektedir. Sistem fonksiyonları belge yönetimi fonksiyonel 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). Bir kuruluşun işleyişinin temelini oluşturan belgelerin doğru şekilde yönetilmeleri, bilginin korunmasını, erişilebilirliğini ve güvenliğini sağlar. Bu amaçla ISO 18128 standardı, belgelerin yaşam döngüsü boyunca uyulması gereken adımları ve riskleri önleme stratejilerini belirlemektedir. Buna göre belge yönetiminde dikkat edilmesi gerekenler şu şekilde sıralanabilir (ISO 18128, 2024, s. 23):

1. Hangi belgelerin gerekli olduğunu belirlemek için iş faaliyetleri analiz edilmelidir.
2. Tüm ilgili tarafların ihtiyaçlarını karşılayacak şekilde kapsamlı bir belge toplama planı oluşturulmalıdır.
3. Belgeler, içeriğin tanımlanması ve üstveri gereksinimlerini (kimlik, açıklama, kullanım, olay geçmişi, olay planlaması) karşılamalıdır.
4. Belgelerin etkin bir şekilde yönetilebilmesi için içeriklerine ve kullanım amaçlarına uygun, tutarlı ve kapsamlı bir adlandırma ve sınıflandırma sistemi oluşturulmalıdır.
5. Belgelere erişim ve izin kuralları oluşturulmalı, belgelenmeli ve belgelere ihtiyaç duyulduğu sürece muhafaza edilmelidir.

ISO 18128, kuruluşların belgelerini güvenli ve düzenli bir şekilde yönetmelerine, bilgi varlıklarını korumalarına ve iş süreçlerini optimize etmelerine yardımcı olan bir teknik rapordur. Bu raporda, elektronik bir belgenin yaşam süresini modellemek için dört ortamın sağlıklı bir şekilde işletilmesi gerektiği vurgulanmaktadır (Bearman, 2006, s. 25):

Oluşturma Ortamı: Bir eylemin elektronik bir belgenin oluşturulup gönderilmesiyle sonuçlandığı ortamdır.

Aktif Belge Yönetim Ortamı: Elektronik belgenin, sürekli kullanımı destekleyen bir uygulamanın kontrolü altında kaydedildiği veya alındığı ortamdır.

Arşiv Ortamı: Orijinalliğini sağlamak için yeterli üstverilerle tamamlanan bir elektronik kaydın alındığı ve arşivsel olarak yönetildiği ortamdır.

Koruma Ortamı: Belgelerin kullanım ömrünü uzatmak amacıyla arşivciler tarafından müdahalelerin yapıldığı ortamdır.

Her ortam, elektronik belgenin yaşam döngüsünün farklı bir aşamasını temsil eder ve bu ortamlar arasında sorunsuz bir geçiş sağlanmalıdır. Bu sayede elektronik belgelerin bütünlüğü ve erişilebilirliği yıllarca korunabilir. Bu dört ortamda, elektronik belgelerin bütünlüğü ve orijinalliği açısından risk oluşturan unsurlar ayrıntılı bir şekilde ortaya konmalıdır.

Elektronik dosya içeriklerinin özgünlüğünü ve etkinliğini korumak için risk yönetimi kavramı elektronik dosya yönetimi iş akışına entegre edilmelidir. Bu doğrultuda önemli elektronik dosyalardan kaynaklanabilecek riskler belirlenmeli ve bu riskleri azaltacak önceden belirlenmiş ve önleyici tedbirler alınmalıdır (Lin, 2020, ss. 72-73). Uluslararası Arşiv Konseyi (ICA) ilkeleri, bu risk yönetimi yaklaşımının temelini oluşturmaktadır. Bu ilkeler doğrultusunda elektronik belgeler güvenilir bir şekilde muhafaza edilmeli, iş bilgileri üstverilerle bağlanmalı, erişilebilir tutulmalı ve denetlenebilir bir şekilde imha edilebilmelidir (ICA, 2008). Risk yönetimi ve ICA ilkelerinin uygulanmasıyla elektronik belgelerin uzun vadeli erişilebilirliği, bütünlüğü ve güvenilirliği sağlanabilir.

Belgelerin bütünlüğünü ve özgünlüğünü koruyarak uzun süreli erişilebilirliğini sağlamak amacıyla yalnızca elektronik ortamdaki belgelere yönelik gerçekleştirilen faaliyetler yetersiz kalmaktadır. Çünkü birçok kuruluş, günlük faaliyetlerinin bir parçası olarak hem kâğıt hem de elektronik belge oluşturmaya devam etmektedir. Bu hibrit belge kayıt ortamını yönetmek, günümüzde oldukça yaygın bir durumdur. Yakın gelecekte dünyanın herhangi bir yerinde tamamen elektronik bir belge çerçevesinin bulunması pek olası görünmemektedir.

Hibrit bir ortamda, hem fiziksel hem de dijital belgelerle çalışmak, kurumlar için hem bir fırsat hem de bir zorluktur. Bu iki dünyayı bir araya getirirken etkin bir belge yönetimi için bazı temel prensiplere uyulmalıdır (IRMT, 2009c, s. 34):

- Fiziksel ve dijital dosyalama sistemlerinin bütünleşik bir şekilde çalışması, belge yönetimini büyük ölçüde kolaylaştırır. Paylaşılan ağ sürücüler, fiziksel dosyalamanın dijital karşılığı olarak kullanılarak belgelerin tutarlı bir şekilde saklanması ve bulunması sağlanır. Bu sayede hem kâğıt belgelerin güvenliği sağlanır hem de elektronik belgelerin sunduğu esneklik ve erişilebilirlik avantajlarından yararlanır.
- Kâğıt belgelerin dijital ortama aktarılması, depolama alanından tasarruf sağlamak, bilgiye erişimi kolaylaştırmak ve iş süreçlerini iyileştirmek gibi birçok avantaj sunar. Ancak bu süreç, dikkatli bir planlama ve hazırlık gerektirir. Tarama projesine başlamadan önce tarama amaçları net bir şekilde belirlenmelidir. Ayrıca tarama işlemi sırasında elde edilen dijital belgelerin kalitesi, orijinal belgeye en yakın şekilde korunmalıdır.

Hibrit belge yönetimi, kuruluşların kâğıt ve elektronik belgelerin sunduğu avantajlardan yararlanmasına ve bilgi yönetimini optimize etmesine olanak tanır. Bu çerçevede, her iki sistemin de işlevselliğini ve güvenliğini sağlayacak çözümler geliştirmek önemlidir. Ancak elektronik belgeler değiştirilme, manipüle edilme veya yok edilme riski taşır. Bu da orijinal olmayan ve güvenilmez bir belgeye veya daha da kötüsü hiçbir belgeye erişememe riskini doğurur. Bu riski azaltmak için elektronik belgeleri orijinal biçiminde tutmak için gerekli teknolojilere ve uzmanlığa yatırım yapmak önemlidir. Ancak bilgisayarlardaki ve bilgi sistemlerindeki hızlı değişimler, kuruluşların elektronik belgelere orijinal yapılandırmalarında erişebilmek için ‘eski’ bilgisayarları tutma lüksünü tanımayacak kadar hızlı gerçekleşmektedir. Bu nedenle hibrit belge yönetimi sistemleri geliştirirken elektronik belgelerin uzun süreli erişilebilirliği ve bütünlüğü için ayağı yere basan çözümler geliştirmek ve riskleri en aza indirmek için gerekli adımları atmak önemlidir.

2.1.1.4.1. Elektronik Belgenin Oluşturulması

Belge oluşturma, kaydın kendisinin tutulması, belgeyle ilişkili tüm üstverilerin tutulması, kaydın tanımlanması ve bir sınıflandırma şemasına göre sınıflandırılması gibi adımları içerir. Bu süreçte en büyük zorluk, elektronik belge yönetim sisteminin bir elektronik kaydın tüm unsurlarını veya bileşenlerini eksiksiz ve doğru bir şekilde tutabilmesini sağlamaktır (IRMT, 2009b, s. 50).

Belge oluşturma sürecinde uygunluk, entegrasyon, sorumluluk, dış kaynaklı belge yönetimi, üstveri dokümantasyonu ve erişim kontrolü gibi hassas noktalara odaklanmak gerekmektedir. Bu sayede kurumlar daha etkin, güvenli ve verimli bir belge yönetimi sistemi kurabilirler. Belgeler iş süreçlerine tam entegre olur, doğru kişilere zamanında ulaşır ve veri güvenliği ile şeffaflık sağlanır (ISO 18128, 2024, s. 23).

2.1.1.4.2. Elektronik Belgenin Kullanımı

ISO 18128 standardı, belgelerin kurum içinde etkin ve güvenli bir şekilde yönetilmesi için temel ilkeler ortaya koymaktadır. Buna göre belgelerin erişilebilirliği, kullanıcı izinlerinin yönetimi, güvenlik ihlallerine karşı önlemler, erişim kayıtlarının tutulması, personel eğitimi ve uyumluluk gibi konulara dikkat çekilmektedir. Bu ilkelerin uygulanması, belgelerin doğru zamanda doğru kişilere ulaşmasını sağlayarak iş

süreçlerini iyileştirir, veri güvenliğini sağlar ve yasal uyumluluğu destekler (ISO 18128, 2024).

2.1.1.4.3. Kullanılabilirliğin Sürdürülmesi

EBYS'lerin temel ilkesi olan yaşam döngüsü prensibini organizasyonun vizyonu haline getirmek, EBYS'nin uzun vadeli başarısı için önemlidir. Yalçinkaya'nın (2016) da belirttiği gibi bu prensibi vizyona dönüştürmek, sürdürülebilir bir belge yönetimi sistemi oluşturmak için gereklidir. Sürdürülebilirlik politikası, belge yönetimi fonksiyonlarının sadece son kullanıcıya odaklanmamasını, tüm paydaşların ihtiyaçlarını göz önünde bulundurmasını destekler. EBYS uzun vadeli başarısı için dosya planı uygulamasına bağlı kalınmalı, saklama planları detaylı bir şekilde oluşturulmalı ve arşivleme süreçleri titizlikle yürütülmelidir. Belgelerin formatı veya saklandığı ortam ne olursa olsun uzun süreli saklama gerekliliği her zaman göz önünde bulundurulmalıdır.

Elektronik belgelerin uzun süreli korunması, belge yönetimi konusunda önemli bir yer başlık olarak görülmektedir. ISO 18128 standardı, bu süreçte dikkat edilmesi gereken birçok önemli noktaya değinmektedir. Örneğin, *üstverilerin* zaman içindeki anlamını koruyabilmesi için dikkatle tasarlanması ve yönetilmesi gerekir. *Belge güvenliği*, oluşturma, saklama, erişim ve imha gibi tüm yaşam döngüsü boyunca sağlanmalıdır. *Erişilebilirlik* açısından, belgelerin farklı teknolojilere ve formatlara uyumluluğunun sağlanması gerekmektedir. *Şifreleme* ile belgelerin güvenliği sağlanırken *versiyon yönetimi* sayesinde belgelerin geçmiş sürümlerine kolayca erişilebilmelidir. Ayrıca *olay geçmişi belgeleri* sayesinde yapılan tüm değişiklikler takip edilebilmelidir. Sistem, teknolojik gelişmeler doğrultusunda düzenli olarak gözden geçirilmeli *eskime sorunlarına* ilişkin önlemler alınmalıdır (ISO 18128, 2024, ss. 24-25).

2.1.1.4.4. Elektronik Belgenin Düzenlenmesi

EBYS içerisinde belge yaşam döngüsünün yönetimi, kurumların bilgi güvenliği ve verimliliği açısından büyük önem arz etmektedir. ISO 18128 ve IRMT 2 standartları, bu süreçte dikkat edilmesi gereken birçok önemli noktayı vurgu yapmaktadır. Özellikle belgelerin elden çıkarılması süreci, yasal düzenlemelere uygunluk ve veri güvenliği açısından titizlikle yönetilmelidir. Elden çıkarılacak (imha edilecek) belgeler için tasarruf uygulaması oluşturularak imha işlemi detaylı bir şekilde belgelenmelidir.

İmha işlemi yetkili kişiler tarafından onaylanmalı ve tüm aşamalar kayıt altına alınmalıdır. Atılan donanım ve depolama aygıtları için ise adli kurtarma testleri yapılarak veri sızıntısı riskleri en alt düzeye indirgenmelidir. Süresi dolmuş belgelerin zamanında imha edilmemesi, EBYS'nin performansını düşürerek iş süreçlerini olumsuz etkiler. Düzenleme eksikliği ise sistemde bilgi kirliliğine ve verimsizliğe neden olabilir. Bu nedenle belgelerin yaşam döngüsü yönetimi için kapsamlı politika ve prosedürlerin oluşturulması ve uygulanması gerekmektedir (IRMT, 2009b; ISO 18128, 2024).

EBYS'de belgelerin uzun vadeli erişilebilir ve kullanılabilir olması gerekmektedir. Bu nedenle belgelerin orijinal ve gerçek biçimde korunması için sistemde bir denetim mekanizması ve belgelendirme süreci kurulmalıdır. Denetim mekanizması, kaydın ne zaman oluşturulduğunu, hangi yazılım ve işletim sistemiyle üretildiğini, sınıflandırma şemasındaki yerini, kimin erişip kullandığını gibi belgeyle ilgili tüm bilgilerin (üstveriler) tutulmasını sağlar. Bu bilgiler, belgenin zaman içindeki değişimini ve bağlamını anlamayı mümkün kılar. Ayrıca başka bir kuruluşa devredilmiş olsa dahi, belgelerin EBYS'de kaldığı süre boyunca belgelendirilmesi gerekir. Bu sayede belgelerin geçmişi ve izlenebilirliği korunarak uzun vadeli erişim ve kullanılabilirlik sağlanabilir (IRMT, 2009b, s. 53).

2.1.1.4.5. Elektronik Belge Kontrolleri

Üstveri

Belge üstverileri, bir belgenin kim tarafından, ne zaman, neden ve nasıl oluşturulduğu, kullanıldığı ve saklandığı gibi bilgileri içeren yapılandırılmış verilerdir. Belgelerin yapısını ve içeriğini tanımlayan idari, tanımlayıcı ve teknik bilgiler sunan bu veriler, belgenin yaşam döngüsü boyunca değişebilir ve güncellenebilir. Belge üstverileri, etkili bir belge yönetimi için temeldir. Bu veriler sayesinde belgeler kolayca bulunabilir, izlenebilir ve yönetilebilir. ISO 16175 standardına göre belge üstverilerine ilişkin işlevsel gereksinimler, belgeyle ilgili tüm bilgilere kolayca ulaşılabilir ve kullanılabilir hale getirmek için EBYS'nin tüm bileşenlerinde dikkate alınmalıdır (ISO 16175, 2020, s. 14).

Üstveriler ayrıca elektronik belgelerin imha edilmeden veya ulusal arşive aktarılmadan önce nasıl oluşturulduğu, kullanıldığı, yönetildiği ve muhafaza edildiği ile bunların

diğer belgelerle nasıl ilişkili olduğunu açıklayan bağlamsal bilgiler sunar. Bu bağlamsal bilgiler, verilerin kendi başına anlamsız bir dizi sayı veya harften öteye geçerek anlam kazanmasına yardımcı olur. Örneğin, ‘100965 020359 031265 300989 060297’ gibi bir sayısal veri, tek başına bir anlam ifade etmez. Bu sayı, bir nüfus sayısı, bir ürün kodu, bir tarih veya bir deneydeki bir ölçüm sonucu olabilir. Verinin gerçek anlamını ortaya çıkarmak için verinin neyi temsil ettiği, nasıl elde edildiği, hangi birimlerde ölçüldüğü gibi ek bilgilere ihtiyaç duyulur. Bu ek bilgilere üstveri denir. Üstveri, meta verinin özel bir türüdür ve verinin içeriği hakkında daha spesifik bilgiler sağlar. Üstveriler, verinin kalitesini, güvenilirliğini ve yorumlanabilirliğini belirler. Verinin bulunduğu bağlam, üstveriler sayesinde daha iyi anlaşılır ve böylece veriden daha doğru ve anlamlı sonuçlar elde edilir. Bağlam, verinin toplandığı ortam, amaç, kullanılan araçlar ve diğer ilgili faktörleri içerir (IRMT, 2009a, s. 61).

Üstveriler, verileri anlamlı hale getirerek elektronik belge yönetiminin temelini oluşturur ve bu sayede belgelerin uzun vadeli erişilebilirliği ve kullanılabilirliği sağlanır. Belgelerin zaman içinde, farklı alanlarda ve farklı sistemler arasında oluşturulmasına, kaydedilmesine, sınıflandırılmasına, erişimine, korunmasına ve elden çıkarılmasına olanak tanıyan yapılandırılmış veya yarı yapılandırılmış bilgilerdir (ISO 23081-1, 2006).

Belge üstverileri, bir belgenin içeriğini, yapısını, iş bağlamını, diğer belgelerle ilişkilerini, erişim ve sunum bilgilerini ve yaşam döngüsü bilgilerini içeren, belgenin ne olduğu, nasıl kullanıldığı ve nerede saklandığı hakkında detaylı bilgi veren meta veri kümesidir. Belge yönetim sistemlerinde etkili bir bilgi arama, erişim ve yönetim için gereksinim duyulan bu tür üstverilerden yoksun olan belgeler resmî belge vasfından yoksundur (ISO 15489-1, 2016).

Üstveriler belgelerin yasal geçerliliğini sağlamanın yanı sıra belge yönetimi süreçlerine de destek olur. Üstveriler belgelerin yasal geçerliliğini destekler, içeriğin anlaşılmasını kolaylaştırır, güvenilirliği artırır, erişimi kontrol eder, arama ve keşfi hızlandırır, farklı sistemlerdeki uyumluluğu sağlar ve uzun vadede korunmalarını garanti eder. Bu sayede kurumlar, belgelerinin yaşam döngüsü boyunca etkin yönetilmesini, korunmasını ve değerlendirilmesini sağlayabilir. Üstverileri toplamak için iki ana yöntem vardır:

- Bilgisayar sistemleri, belgeler oluşturulduğunda veya değiştirildiğinde üstverileri otomatik olarak yakalayabilir.
- Belgelerin oluşturucuları ve kullanıcıları, form ve şablonları doldurarak üstverileri el ile ekleyebilir.

Belgeler belge yönetim sistemi boyunca aktarılırken üstveriler belge yöneticileri ve arşivciler tarafından da eklenebilir. Son yıllarda, mevcut belgelerden üstverileri otomatik olarak yakalamak için yardımcı programlar geliştirilmektedir. Her iki yöntem de farklı belge türleri için kullanılabilir ve mevcut bilgisayar sistemlerinin niteliğine bağlı olarak birlikte kullanılabilir.

Üstverilerin etkili bir şekilde yönetilmemesi, maliyet artışına, veri kalitesinin düşmesine, kullanıcı hatalarına, tutarsızlıklara ve çalışanların üstveri girişine olan ilgisizliğine yol açabilir. Bu durum, bilgiye erişimi zorlaştırır, karar verme süreçlerini yavaşlatır ve kurumun genel verimliliğini düşürür. Üstverilerin etkili yönetimi için öncelikle iş süreçleri ve bilgi ihtiyaçları analiz edilerek gerekli üstveriler belirlenmeli ve standartlaştırılmış bir yapı oluşturulmalıdır. Otomasyon araçları kullanarak manuel veri girişini azaltmak ve veri kalitesini artırmak önemlidir. Ayrıca kullanıcıların üstveri girişine ilişkin eğitimi, farkındalık yaratılması ve teşvik edilmesi de verimliliği artırır. Üstverilerin doğruluğu ve tutarlılığı için düzenli denetimler yapılmalı ve otomatik doğrulama mekanizmaları kullanılmalıdır. Basit ve anlaşılır üstveri yapıları oluşturarak kullanıcı hatalarını en alt düzeye indirmek ve düşük kodlu platformlar kullanarak veri girişini kolaylaştırmak da önemlidir (IRMT, 2009c, s. 25).

Veri odaklı bir sistemin başarısı, mümkün olduğunca çok sayıda ve çeşitli veri kaynağına erişimini sağlamaktan geçmektedir. Bu bağlamda, kullanıcıların üstveri girişi konusunda isteksiz veya hata yapmaya açık olma olasılığı göz önünde bulundurulmalıdır. Araştırmalar, kullanıcıların ana faaliyetlerinin yürütülmesini engelleyecek kadar sıklıkla işlerine ara vermeyi tercih etmediklerini göstermektedir. Üstelik elle veri girişi, zaman alıcı ve yorucu bir işlem olarak algılanabilir ve bu durum kullanıcıların motivasyonlarını ve üretkenliklerini olumsuz etkileyebilmektedir (ISO 16175-1, 2010, s. 11). Kullanıcıların tüm üstveri öğelerini elle girmesini talep etmek, zaman alıcı, yorucu ve hatalara açık bir süreçtir. Bu nedenle sistemin otomatik veri tamamlama ve ilişkilendirme yeteneğine sahip olması daha verimli ve güvenilir bir yaklaşımı temsil eder (Yalçınkaya, 2016, s. 70). Tüm bunların yanı sıra belge yönetim

süreçlerinin etkinliğini artırmak için üstveri teknik özelliklerinin erişilebilir, yönetilebilir, uyumlu ve esnek bir yapıda olması gerekmektedir. Üstveri teknik özelliklerine kolayca ulaşılabilmesi bir taraftan belgelerin ve süreçlerin daha iyi anlaşılmasını sağlarken diğer taraftan düzenli güncelleme imkânı sayesinde değişen ihtiyaçlara uyum sağlanabilir. Ayrıca farklı sistemler arasında birlikte çalışabilirlik sağlayacak şekilde tasarlanan üstveri şemaları, kurum genelinde bilgi paylaşımını kolaylaştırır ve veri bütünlüğünü korur (ISO 18128, 2024, s. 24).

İş Sınıflandırma Şemaları ve Dosya Planları

İş dünyasında bilgi, giderek daha da önemli hale gelmektedir. Doğru bilgiye hızlı ve kolay bir şekilde erişim, kuruluşların rekabette öne geçmesine ve başarıya ulaşmasına yardımcı olmaktadır. Ancak artan bilgi hacmiyle birlikte bu bilginin organize edilmesi ve yönetilmesi de giderek zorlaşmaktadır. Buna paralel olarak sınıflandırma şemaları da giderek önem kazanmaktadır. Bu şemalar belgeleri kategorilere ayırmak ve etiketlemek için kullanılmaktadır.

İş sınıflandırma şemaları, belgeleri oluşturuldukları bağlamla ilişkilendirmede ve mevcut iş ihtiyaçlarını yansıtacak şekilde güncel tutmada önemli bir rol oynar. Bu şemaları belge sistemlerine entegre etmek, belgelerin düzenli ve erişilebilir olmasını sağlayarak zamandan ve emekten tasarruf sağlar.

ISO 18128 (2024, s. 25) standardı, bilgi ve belgeler için iş sınıflandırma şemalarının geliştirilmesine ve uygulanmasına rehberlik etmektedir. Bu standarda göre iş sınıflandırma şemaları tasarlanırken ve uygularken dikkat edilmesi gereken bazı önemli noktalar şunlardır:

1. Üstveri şeması belgeleri oluşturuldukları birim, proje veya konu gibi bilgileriyle ilişkilendiren bir yapıdır. Bu sayede belgeler hangi bağlamda üretildikleri hakkında kullanıcıya ipuçları vererek aramaları kolaylaştırır ve belgelerin daha hızlı bulunmasını sağlar.
2. Üstveri şeması, iş süreçlerindeki değişiklikler ve yeni bilgi türlerinin ortaya çıkması gibi durumlarda düzenli olarak güncellenmeli ve bakımı yapılmalıdır. Aksi takdirde, şema mevcut iş ihtiyaçlarını yansıtmayarak belgelerin yanlış klasörlere yerleştirilmesine ve kullanıcıların aradığı bilgilere ulaşmakta zorlanmasına neden olabilir.

3. Üstveri şeması, kullanıldığı belge yönetim sisteminde tam olarak işlevsel hale getirilmelidir. Aksi takdirde dosya yönetimi süreçlerinde istenen düzen ve verimlilik sağlanamaz.

Kuruluşların faaliyetlerini ve iş süreçlerini sistematik bir şekilde organize etmelerine yardımcı olan iş sınıflandırma şemaları, tüm iş fonksiyonlarını ve görevlerini belirli kategorilere ayırarak bilgiyi düzenlemeye ve yönetmeye imkân tanır. Bu sayede elektronik belgeler tutarlı ve sistematik bir şekilde sınıflandırılabilir ve dosyalama işlemi kolaylaşır (Northern Territory Government of Australia, 2024). Dosyalama ise belge yönetiminin önemli bir parçasıdır ve yapılan faaliyetler sırasında ortaya çıkan belgelerin kullanıma hazır bir şekilde sistemli ve planlı olarak saklanmasını sağlar (İslam, 2019, s. 108).

Elektronik belge yönetiminde, mevzuat ve standartlara uygun, kurumsal ihtiyaçları karşılamak ve belgenin yapısal ve içerik bütünlüğünü korumak için dosyalama işlemlerinde dosya planları kullanılmaktadır. Belgeler üretildiğinde veya kuruma/birime ulaştığında, organizasyonel ve işlevsel kökenlerinin (bağılıklarının) belirlenmesi ve bu kökene göre dosya/klasör yapıları oluşturulması gerekmektedir (Devlet Arşivleri Başkanlığı, 2023, s. 1). Bunun uygulanması için gerekli dosya plan kodu, resmi bir taksonomi olarak kabul edilen SDP aracılığıyla verilmektedir. Bu sistemin doğru şekilde uygulanması, hem belge içeriğinin doğru konuya ait olduğunun belirlenmesini hem de belgenin neden ve ne kadar süreyle saklanması ve ne zaman ayıklama/imha işlemlerine tabi tutulacağını doğru bir şekilde belirlemeyi sağlamaktadır (Cibaroğlu, 2019, s. 81). Verilen kodların her birine saklama planları atanmaktadır. Dosya tasnif planıyla uyumlu çalışan saklama planları ile belgenin üretildiği anda nerede, ne şekilde, ne kadar süre ile saklanacağını ve sonrasında ne tür işlemlere tabi olacağı belirlenmektedir (Özdemirci, 2007, s. 220). Saklama süreli dosya plan kodunun yanlış girilmesi, uzun süre saklanması gereken bir belgenin imha edilmesi, kısa sürede imha edilmesi gereken bir belgenin sistemde uzun süre kalması ve milli arşivlere aktarılması gereken arşiv belgesi niteliğindeki belgelerin de yok olması gibi ciddi sonuçlara yol açabilir. Bu nedenle dosya plan kodlarının doğru ve titizlikle girilmesi hayati önem taşımaktadır.

Dosyalama işlemi, elektronik belge yönetiminde önemli bir rol oynamakta ve belgeleri konu ve vaka bazlı olmak üzere iki şekilde organize etmektedir. Kurumlar genellikle

konu bazlı dosyalama sistemini tercih etmektedirler. Ancak vaka dosyası oluşturulması gereken durumları da önceden belirlemelidirler. SDP konu bazlı bir sistem sunmaktadır. Vaka dosyaları ise EBYS içerisinde ayrı olarak tanımlanmalıdır. Personel özlük dosyası, dava dosyası, alım dosyası ve proje dosyası gibi belgeler vaka dosyalarına örnek olarak gösterilebilir. Vaka dosyasındaki belge türleri mevzuat ve kurumsal ihtiyaçlara göre belirlenmektedir (Devlet Arşivleri Başkanlığı, 2023, s. 1).

Elektronik belge yönetim sürecinin önemli bir parçası olan dosyalama işlemindeki hatalı uygulamalar, önemli riskleri beraberinde getirmektedir. Çiçek (2016), bu riskleri şu şekilde açıklamaktadır:

Yanlış Dosyalama: Elektronik belgeler, kâğıt belgelerde olduğu gibi bir fonksiyon ve organik bağ kurularak belirli bir bütünlük içerisinde konu ya da vakaya göre dosyalanmalıdır. Ancak birçok elektronik belge yönetimi yazılımında bu işlem doğru şekilde yapılmamaktadır.

Vaka Dosyası Yönetiminin Zorlukları: Vaka dosyaları, birden fazla belgeyi içeren karmaşık belge kümeleridir. Birçok uygulama yazılımında vaka dosyası açma, yönetme ve arşive devretme işlemleri yeterince kolay değildir.

Modüler Dosyalama Eksikliği: Birçok uygulama yazılımında dosyalama, bağımsız bir modül olarak yönetilmemektedir. Bu durum, ilişkili belgeleri bir araya getirmeyi zorlaştırmaktadır.

Sonuç olarak dosyalama işleminin doğru ve sistematik bir şekilde yapılması, elektronik belge yönetiminin başarısı için büyük önem arz etmektedir. Kurumlar, dosyalama politikalarını ve prosedürlerini net bir şekilde tanımlamalı ve personelinin bu konuda bilinçlendirmelidir. Ayrıca güncel dosyalama sistemleri ve araçlarını kullanmak, dosyalama işlemindeki hataları en aza indirmeye ve riskleri yönetmeye yardımcı olacaktır.

2.1.1.4.6. Elektronik Belgeye Erişim

Günümüzde birçok ülkede kamuya ait bilgilere erişim, demokrasinin temel bir unsuru ve vatandaşların temel bir hakkı olarak kabul edilmektedir. Bu durum, devlet ve toplum arasındaki ilişkiyi yeniden tanımlayarak şeffaflık ve hesap verebilirlik kültürünün gelişmesine katkıda bulunur. Ancak bu hak her zaman var olmamıştır. Eskiden devlet belgelerine ve içerdikleri bilgilere erişim, yalnızca kamu görevlileri ve

hükümetin yürütme organı için bir ayrıcalık olarak görülüyordu. Milletvekilleri ve halk, karar ve eylemler hakkında bilgi edinmek için hükümete güveniyordu ve sadece yönetim sürecine dâhil olanlar, oluşturdukları ve kullandıkları belgelere doğrudan erişim imkânına sahipti. 1970’lerde ve 1980’lerde demokrasi ve insan haklarına yönelik artan ilgi, hesap verebilirlik ve şeffaflık çağrılarına yol açtı. Bu durum, dünya çapındaki birçok hükümetin halkın devlet bilgilerine daha geniş erişim imkânı sunan yasalar çıkarmaya başlamasına neden oldu. ‘Bilgiye Erişim’ veya ‘Bilgi Edinme Özgürlüğü’ olarak adlandırılan bu yasalar, halkın belgelere hiç olmadığı kadar fazla erişmesine imkân tanıdı. Artık insanlar, belgelerin arşiv statüsüne ulaşmasını beklemek zorunda değildi. Başka bir ifadeyle halk, bu belgelere, kurumun günlük işleyişi için hala ihtiyaç duyulsa bile erişmeye çalışabiliyordu. Devlet bilgilerine erişim hakkının genişlemesi, belge profesyonelleri için yeni zorluklar da beraberinde getirdi. Bu zorluklardan en önemlilerinden biri, kurumların günlük işlerini kesintisiz olarak yürütebilmelerini sağlarken aynı zamanda kamuya açık erişim imkânı sunmaktır ve bu, hassas bilgilerin korunmasını ve kurumsal iş akışlarının aksamamasını gerektirmektedir. Diğer i se, kamuya açık belgeler kullanıma sunulduğunda kişisel ve gizli bilgilerin uygunsuz bir şekilde ifşa edilmemesini sağlamaktır. Bu durum, veri gizliliği ve etik ilkelerin gözetilmesini, gerekli teknik ve idari önlemlerin alınmasını gerektirmektedir (IRMT, 2009c).

Elektronik belgelerdeki bilgilere kamunun erişimini sağlamak ve bilgilerin gizliliğini korumak, geleneksel kâğıt belgelerden daha zorlayıcı olabilir. Belgelerin değeri zamanla değişir ve siyasi, sosyal veya diğer zorunluluklara bağlı olarak halkın farklı konulara olan ilgisi artıp azalır.

Elektronik belgelerin bulunması ve alınması hızlı bir şekilde gerçekleştirilebilir. Fakat aynı zamanda uygunsuz ifşa, istenmeyen çoğaltma veya kasıtsız imha riski de artar. Bu nedenle elektronik ortamda kamunun erişiminin sağlanması için bazı önemli hususlara dikkat edilmesi gerekmektedir (IRMT, 2009a, ss. 55-56):

- Oluşturma, yönetim ve saklama için kullanılan teknolojilerdeki değişiklikler erişimi nasıl etkileyecek?
- Hangi sürümün kamuya açıklanması uygun olacak? Birden fazla kopya veya sürüm arasında ayırım nasıl yapılacaktır?

- Hangi donanım ve yazılıma ihtiyaç duyulacak? Elektronik bilgilere kuruluş çapında erişimden farklı olarak kamu erişimi için özel sistemler gerekli mi?
- Elektronik belgelerin gerçekliği nasıl korunacak? Geleneksel kâğıt belgeler gibi 'sertifikalı' olacaklar mı?
- Elektronik belgelere erişim için ücret alınacak mı? Basılı kopyalar için ücretler ne olacak?
- Halkın erişim taleplerini elektronik ortamda iletmesine izin verilecek mi? Bu tür taleplerin belgelenmesi ve takip edilmesi için hangi belgeler gerekli olacak?
- Geçmiş erişim talepleri yoluyla açıklanan belgeler de dahil olmak üzere kamuya açık bilgilerin çevrimiçi bir deposu oluşturulacak mı? Bu kaynağın oluşturulması ve sürdürülmesinin maliyeti ne olacak?

Bu sorulara verilecek olan yanıtlar, elektronik belgelere kamu erişiminin sağlanması için sağlam bir çerçeve oluşturulmasına yardımcı olacaktır.

Belgelere erişim zorluğu veya kayıpları gün geçtikçe artan bir sorun haline gelirken üst düzey yöneticiler, önemli bilgilere ihtiyaç duyanların doğru ve zamanında bu bilgilere ulaşmasının ne kadar önemli olduğunu daha iyi anlamaktadır. Kurum ve kuruluşlar, dijital dönüşümle birlikte artan veri hacmi ve karmaşıklığı karşısında, yetersiz bilgi teknolojileri ve yanlış bilgi yönetimi uygulamalarının yol açabileceği karar verme hataları, yasal sorunlar ve iş süreçlerindeki aksamalar gibi risklerin farkında olarak etkili belge yönetimi çözümleri arayışına girmiştir (IRMT, 2009a, s. 30).

Belge sistemleri içerisinde belge kullanımının takibi kuruluşlar için önemli bir güvenlik önlemidir. Bu sayede yalnızca uygun izinlere sahip kullanıcıların yetkili belge görevlerini gerçekleştirmesi sağlanır. Erişimin ve kullanımın kaydedilmesinin kontrol derecesi ise işin niteliğine ve oluşturduğu belgelere bağlıdır (Hamidoviç, 2010).

Belgelere erişim ve izin kuralları, yalnızca yetkili kullanıcıların bilgiye ulaşmasını sağlamak amacıyla titizlikle belirlenmeli ve sistemlerde etkin bir şekilde uygulanmalıdır. Bu kurallar, yasal düzenlemeler, kurum politikaları ve organizasyonel yapıda meydana gelen değişikliklere uygun olarak düzenli olarak gözden geçirilmeli ve güncellenmelidir. Gereksiz kısıtlamaların önlenerek bilgiye erişimin

kolaylaştırılması ve verimliliğin artırılması hedeflenmelidir (ISO 18128, 2024, ss. 24-25).

2.1.1.4.7. Elektronik Belgenin Saklanması

Elektronik bilgiler, sıfırlardan ve birlerden oluşan baytlar halinde saklanır. Her bayt, sekiz bitten veya bir karakterden oluşur. Örneğin, büyük 'H', 01001000 binary kodu ile temsil edilir. Birden fazla bayt birleştirilerek kelimeler, resimler ve diğer içerikler oluşturulur. Elektronik belgeler, bitlerden (dijital temsil) ve bu bitlerden üretilen algılanabilir ürünlerden (metin, ses vb.) oluşur. Bu ürünler, klavye veya başka cihazlar aracılığıyla bilgisayara veri girildiğinde anında oluşur. Elektronik bir belgeyi 'yaratmak' için ne algılanabilir ürün ne de dijital temsil ayrılabilir. Elektronik belgelerin uzun süreli saklanması, sadece 'kaydın' saklanması gibi değil, aynı zamanda gelecekte herhangi bir zamanda bu algılanabilir ürünün yeniden üretilebilmesini sağlamak için dijital temsilin (bitlerin) korunmasını da içerir. Bu nedenle elektronik belgelerin saklanması özel bir önem taşır (IRMT, 2009a, s. 22).

Her elektronik belge, tıpkı kelime işlemcili bir belge gibi bir araya gelen veri parçalarından oluşur. Ancak bazı elektronik belgeler, birçok farklı unsuru içerir. Örneğin, bir rapor, bir web sayfasının görüntüsünün yanı sıra bir fotoğraf, bir PowerPoint slaydı, bir elektronik tablo sayfası, bir veri tabanından bir alıntı ve hatta bir video veya ses kaydının bir klibini içerebilir. Web sayfası veya video klip, o görüntünün görünür hale getirilmesi veya video klibin oynatılmasına izin verilmesi için gereken farklı bilgisayar öğelerini içerir. Karmaşık bir elektronik belgedeki her bir bileşenin farklı saklama, çoğaltma ve kullanım gereksinimleri olabilir. Bu nedenle bir elektronik kaydı saklarken belge içindeki her öğenin korunmasına ve bu öğelere erişime izin verecek mekanizmaların mevcut olduğundan emin olmak büyük öneme sahiptir (IRMT, 2009a, s. 25).

Belge yönetiminde 'arşivleme', kalıcı değere sahip bilgilerin uzun vadeli saklanması amacıyla bu bilgilerin orijinallik, bütünlük, güvenilirlik ve erişilebilirlik ilkelerine uygun olarak yönetilmesi sürecidir (ISO 16175, 2020, s. 14). Arşivleme stratejisi, belgelerin oluşturulma aşamasından itibaren bakımı, işlenmesi ve saklanması için verimli ve etkili yöntemlerin belirlenmesiyle başlar. Değişen iş gereksinimlerine göre saklama düzenlemelerinin sürekli olarak gözden geçirilmesi ve depolama seçeneklerinin genel belge yönetim sistemiyle entegre edilmesi, başarılı bir arşivleme

için önemlidir. Kâğıt belgeler, uygun koşullarda saklanarak uzun yıllar korunabilirken elektronik belgelerin korunması için uzmanlık ve teknolojik altyapı gereklidir. Erken dönemde başlatılmayan koruma çalışmaları, elektronik belgelerin kaybolmasına veya erişilemez hale gelmesine yol açabilir (IRMT, 2009d, s. 21).

Arşivlemede veri kaybı yaşanmaması için, önemli iş belgelerinin yedek kopyaları düzenli olarak alınmalıdır. Bir felaket veya medya arızası gibi beklenmedik bir olay sonrasında tüm önemli iş bilgilerinin kurtarılabilmesini sağlamak için yeterli yedekleme olanakları şarttır (Hamidoviç, 2010). Yedekleme sistemleri, elektronik belgelerin birden fazla kopyasının farklı ortamlarda saklanmasıyla sistem arızalarında oluşabilecek veri kayıplarını önlemek için tasarlanır. Düzenli yedekleme planları, hem rutin hem de acil durumlarda verilere erişimi sağlayacak şekilde oluşturulmalıdır. Ayrıca yedek kopyaların uzun ömürlü olmasının sağlanması için düzenli bakım gerekmektedir. Veri bozulmalarını engellemek için yedeklerin belirli aralıklarla gözden geçirilmesi ve teknolojik gelişmelere paralel olarak donanım ve yazılımların yenilenmesi elzemdir.

Sürekli saklanması gereken belgeler, uzun süreli muhafaza için uygun ortamlarda saklanmalıdır. Belge koruma stratejileri, erişilebilirlik, bütünlük, orijinallik ve maliyet gibi faktörleri göz önünde bulundurarak seçilmelidir. Belgelerin uzun süreli korunması için kopyalama, dönüştürme ve geçiş gibi yöntemler kullanılmaktadır. Kopyalama, aynı formatta birden fazla kopya oluştururken dönüştürme, farklı bir formata geçişle bilginin korunmasını sağlar. Geçiş ise teknolojik gelişmelere paralel olarak farklı platformlara aktarım anlamına gelir. Bilgilerin uzun ömürlü olması için teknolojinin ömründen daha uzun süre saklanabilir olması, düzenli olarak depolama ortamı geçişleri yapılması ve endüstri standardı formatların kullanılması önemlidir. Ayrıca üstverilerin de korunması, geçiş süreçlerinin belgelenmesi ve yeni teknolojilerin takip edilmesi gerekmektedir. Gerekli durumlarda harici bir saklayıcıyla anlaşma yaparak belgelerin güvenliği sağlanabilir (Hamidoviç, 2010).

2.1.1.4.8. Elektronik Belgelerde Ayıklama ve İmha

Belgelerin uzun vadede kalıcı bir değeri olmadığı değerlendirilmişse, kullanım ömürlerinin sonunda imha edilebilirler. Kâğıt belgeler için imha, belge ortamının parçalanması, yakılması veya başka bir şekilde yok edilmesi yoluyla kaydın fiziksel olarak imha edilmesi anlamına gelir. Elektronik belgelerin imhası çok daha karmaşık

olabilir. Bir bilgisayar dizinindeki belgeleri silmek kendi başına yeterli değildir. Elektronik belgeyle ilişkili bileşenlerin ve üstverilerin imha edilmesi de gerekli olabilir. Bu imhanın gerçekleştirilmesini sağlamak için teknik uzmanlığa gereksinim vardır. İmha sürecinin denetim takibinin sürdürülmesi de önemli bir gerekliliktir (IRMT, 2009c, s. 47).

Elektronik belgelerin imhası, fiziksel belgelerle benzer şekilde yetkili bir komisyon tarafından titizlikle yürütülmesi gereken bir süreçtir. IRMT Module 3'e göre (2009) bu komisyon, belge saklama sürelerinin belirlenmesi, değerlendirme ve ayıklama kararlarının alınması, sistem üzerindeki yetkilerin yönetimi gibi önemli görevleri üstlenir. Bu sayede hem yasal gereklilikler yerine getirilir hem de kurumun bilgi güvenliği sağlanır.

Kalıcı değere sahip olduğu belirlenen elektronik belgeler, kurum dışı bir arşiv veya kurum içi özel bir depolama alanına aktarılır. Aktarma sürecinde öncelikle belgelerin formatı (yerel, koruma veya erişim formatı) belirlenir, ardından kopyalanır ve gerekirse yeniden biçimlendirilir. Ayrıca hazırlanan belgelerin detaylı bir envanteri oluşturulur. Bu envanter kullanılan dosya formatları, erişim ve koruma bilgileri gibi teknik detayları içerir. Belgeler ve envanter, arşiv sistemine aktarılır ve işlemin başarılı bir şekilde tamamlandığı doğrulanır. Son olarak kaynak sistemdeki belgeler güvenli bir şekilde silinir (IRMT, 2009c, ss. 48-49).

Dijital belgelerin aktarılması, karmaşık bir teknolojik süreçtir. Bu nedenle belge profesyonellerinin bilgi teknolojisi uzmanlarıyla birlikte çalışması gereklidir. 21. yüzyılda elektronik teknolojiler artan verimlilik, gelişmiş iletişim ve daha fazla hesap verebilirlik/şeffaflık gibi birçok fayda sağlayarak yaşamın bir gerçeği haline gelmiştir. Belge uzmanları, elektronik belge yönetimi programlarının zorluklarından kaçınmak yerine tüm belge yönetimi çerçevesini geliştirmek için teknolojinin sunduğu fırsatlardan yararlanmalıdır. Belge uzmanları, elektronik belge yönetimi programlarının etkili bir şekilde uygulanması ve tüm ortamlarda belgelerin oluşturulması ve yönetilmesi için makul ve açık politikalar ile prosedürler oluşturarak bu fırsatlardan yararlanabilir ve riskleri azaltabilir. Elektronik belgelerle ilgili önemli görülen hususları şu şekilde maddelendirmek mümkündür (IRMT, 2009a, ss. 12-13):

- Tam olarak teknolojiye bağımlıdırlar.

- Teknolojideki hızlı deęişiklikler nedeniyle sürekli gözden geçirilmesi ve güncellenmesi gerekmektedir.
- Teknolojik eskime ve bağımlılık bilginin uzun vadeli yönetimini ve erişimini karmaşılaştırır.
- Tüm sorunları çözecek tek bir strateji yoktur.
- Dijital medya, donanım ve yazılım uyumsuzlukları, veri bozulması ve yanlış kullanım gibi nedenlerle kaybolma riskine karşı hassastır.
- Elektronik belge yönetimine yaklaşım genellikle geçici veya tepkiseldir.

2.1.1.5. EBYS ve Süreçlerine İlişkin Risk Tanımlamaları Kontrol Listesi

Günümüz bilgi toplumunda kurumlar ve bireyler, hassas bilgiler içeren muazzam miktarda belgeyi yönetmektedir. Bu belgelerin güvenliği veri kaybı, kimlik hırsızlığı ve yasal yaptırımlar gibi önemli riskler taşımaktadır. Bu risklerin her biri, kurumsal itibarı zedeleyebilir, mali kayıplara yol açabilir ve hatta yasal sorumluluk doğurabilir. Bu riskleri etkin bir şekilde yönetmek için belge risklerinin kaynaklarını belirlemek ve bunlara karşı uygun önlemleri almak son derece önemlidir. Tablo 2.5’te belgeye ilişkin risk kaynakları ve olası sonuçlar kapsamlı bir şekilde sunulmaktadır (ISO 18128, 2024; Public Record Office Victoria, 2010; Lin, 2020):

Tablo 2.5: Elektronik belge risklerinin kaynaklarına ilişkin örnekleri içeren kontrol listesi

<i>Kategori</i>	<i>Olası Risk Kaynakları</i>	<i>Olası Sonuçlar</i>
<i>Belge Yönetim Sistemi</i>	<i>Belge yönetimi personelinin sistemin tasarımı, geliştirilmesi ve uygulanmasına dahil edilmemesi</i>	Belge yönetim sisteminin) tasarımı, geliştirilmesi ve uygulanması aşamalarında belge yönetimi ekibinin yer almaması, sistemin gereksinimleri karşılayamamasına ve kullanım zorluğuna yol açabilir. Bu durum, kullanıcı memnuniyetsizliği, ek maliyetler ve gecikmeler gibi bir dizi olumsuz sonuca neden olabilir.
	<i>İş süreçlerinde ve sistem uygulamalarında planlama ve kontrol mekanizmalarının yetersizliği</i>	EBYS'nin planlama ve uygulama aşamalarında gerekli özen gösterilmemesi, sistemin iş ihtiyaçlarını karşılamamasına, gecikmelere, maliyet aşırımlarına ve kullanıcı memnuniyetsizliğine yol açabilir. Bu durum, EBYS'nin beklenen faydalarını sağlayamamasına ve kuruluş için bir yatırım kaybına dönüşmesine neden olabilir.
	<i>Sistemin kullanımdan kaldırılmasına ilişkin bir dosya aktarım politikasının olmaması</i>	Belge yönetim sisteminin kullanımdan kaldırılması veya değiştirilmesi gerektiğinde, dosyaların ve verilerin yeni sisteme güvenli ve eksiksiz bir şekilde aktarılmasını sağlayacak bir plana sahip olmamak, veri kaybına, iş kesintilerine ve mali kayıplara yol açabilir. Bu plan, veri yedekleme, dosya dönüştürme ve sistem entegrasyonu gibi adımları içermelidir.
	<i>Alt yapı uyumsuzluğu ve teknolojik gerilik</i>	EBYS'nin kurumun mevcut teknolojik altyapısıyla uyumlu olmaması veya en son teknolojiyi kullanmaması, sistem performansını ve işlevselliğini olumsuz etkileyebilir. Bu durum, entegrasyon sorunlarına, veri kaybına ve siber saldırılara karşı savunmasızlığa yol açabilir.
	<i>Sistem uygulamalarını sürdürmek ve güncel tutmak için uzman personel ve/veya kaynak eksikliği</i>	EBYS'yi yönetmek ve geliştirmek için gerekli becerilere sahip personelin eksikliği, sistemin etkin bir şekilde kullanılmasını ve korunmasını zorlaştırabilir. Bu durum, teknik problemlere, gecikmelere ve ek maliyetlere yol açabilir.

	<i>Belge sistemlerini etkileyen iş ve işletim sistemlerindeki değişiklikler</i>	Kuruluşun iş süreçlerinde veya kullandığı diğer sistemlerde yapılan değişiklikler, EBYS ile uyumluluk sorunlarına yol açabilir. Bu durum, ek maliyetlere, veri tutarsızlığına ve sistem kesintilerine yol açabilir.
	<i>Destek ve bakım eksikliği</i>	EBYS'ye yeterli destek ve bakım sağlanmaması, sistemin arızalanmasına, güncelliğini yitirmesine ve güvenlik açıklarına karşı savunmasız kalmasına neden olabilir. Bu durum, veri kaybına, mali kayıplara ve itibar zedelenmesine yol açabilir.
	<i>Verimlilik, tutarlılık veya diğer önlemler açısından yetersiz sistem performansı</i>	EBYS'nin beklenen performans seviyesini karşılayamaması, iş akışında aksaklıklara, gecikmelere ve ek maliyetlere yol açabilir. Bu durum kullanıcı memnuniyetsizliğine ve kurumun genel verimliliğinin düşmesine neden olabilir.
	<i>Sistemin dış saldırılara (bilgisayar korsanları, kötü amaçlı kod vb.) karşı korunamaması</i>	Belge yönetim sisteminin siber saldırılara karşı yeterince korunmaması, veri hırsızlığı, kimlik hırsızlığı ve sistem arızalarına yol açabilir. Bu durum yasal yaptırımlara, itibar zedelenmesine ve mali kayıplara yol açabilir.
<i>Belgeler</i>	<i>Belirsiz/Yetersiz belge oluşturma süreçleri</i>	Belirsiz veya eksik prosedürler, yetersiz inceleme ve onay ile belgelerin güncel olmaması, kurumlarda önemli sorunlara yol açmaktadır. Belgelerin nasıl oluşturulacağı ve güncelleneceğine dair net yönergelerin bulunmaması, tutarsızlıklar ve hatalara neden olurken yetkili kişiler tarafından gözden geçirilmemesi veya onaylanmaması, yanlış veya eksik bilgilere yol açmaktadır. Bu durum, belgelerin güncel yasalara ve iş uygulamalarına uygun olmamasına ve kurumun genel etkinliğini olumsuz etkilemesine sebep olmaktadır.
	<i>Düzensiz/Yetersiz belge yönetimi süreçleri</i>	Düzensiz arşivleme, yetersiz erişim kontrolü ve yetersiz yedekleme gibi sorunlar, kurumların belge yönetimi süreçlerinde ciddi riskler oluşturmaktadır. Belgelerin

		güvenli ve erişilebilir bir şekilde saklanmaması, kaybolmasına veya hasar görmesine neden olurken yetkisiz erişim, gizli bilgilerin sızmasına yol açabilir. Ayrıca belgelerin düzenli olarak yedeklenmemesinin sonucu olarak yaşanan veri kayıpları, iş süreçlerini olumsuz etkileyebilir ve kurum itibarına zarar verebilir.
	<i>Belgeleri oluştururken yanlış format kullanımı</i>	Belgelerin farklı formatlarda olması ve profesyonel olmayan bir şekilde biçimlendirilmesi, hem erişimi zorlaştırarak bilgiye ulaşımı engellemekte hem de güvenilirliği azaltarak karar verme süreçlerini olumsuz etkilemektedir.
	<i>Belgeleri kayıt altına alınmasında eksik/yanlış üstveri tanımlamaları</i>	Üstverinin eksikliği, güncel olmaması veya yanlışlığı, belgelerin ne anlama geldiğini ve nasıl kullanılacağını anlamayı güçleştirerek bilgi yönetimi süreçlerinde verimsizliğe ve hatalara yol açar.
<i>Belge Yönetim Süreçleri</i>	<i>Belgeleri ve üstverileri tutmaya ve yönetmeye yönelik işlevsel bir sistemin tasarlanmaması</i>	Kullanılan sistem, belgelerin ve ilgili üstverilerin ihtiyaç duyulan şekilde saklanması, düzenlenmesi, geri alınması ve erişimi için yeterli işlevsellik sunmayabilir. Bu durum, belge kaybına, veri bozulmasına, arama/erişim zorluklarına ve yasal uyumluluk risklerine yol açabilir.
	<i>Süreçlere ilişkin dokümantasyonun eksikliği</i>	Belge yönetim süreçlerinin net ve güncel bir şekilde belgelenmemesi, çalışanların görevlerini doğru şekilde yerine getirmesini zorlaştırabilir. Bu durum, tutarsızlıklara, hatalara, gecikmelere ve verimsizliğe yol açabilir.
	<i>Eksik ve/veya tutarsız veriler</i>	Belgelerden veya sistemlerden eksik veya hatalı veri yakalanması, yanlış bilgi ve kararlara yol açabilir. Bu durum, mali kayıplara, itibar zedelenmesine ve yasal yaptırımlara yol açabilir.

	<i>Sistem yöneticilerinin beceri düzeyi</i>	Sistem yöneticilerinin yetersiz bilgi ve beceriye sahip olması, sistemin düzgün çalışmasını ve belgelerin korunmasını tehlikeye atabilir. Bu durum, veri kaybına, sistem arızalarına ve siber saldırılara karşı savunmasızlığa yol açabilir.
	<i>Belge yönetim sisteminin, belge süreçlerinin tüm gereksinimlerini karşılayamaması</i>	Belge yönetim sisteminin işlevselliği, kuruluşun belge yönetim süreçlerinin özel gereksinimlerini karşılayamayabilir. Bu durum, iş akışında aksaklıklara, ek maliyetlere ve verimsizliğe yol açabilir.
	<i>Teknolojinin ve formatların eskimesi</i>	Belge depolama ve yönetim için kullanılan teknolojinin ve formatların eski veya modası geçmiş olması, sistemin güvenliğini, erişilebilirliğini ve işlevselliğini tehlikeye atabilir. Bu durum, veri kaybına, uyumluluk sorunlarına ve güncelleme maliyetlerine yol açabilir.
<i>Belge Kontrolleri</i>	<i>Belgelerin tutulmasında kontrol sisteminin yetersizliği</i>	Belge kontrol sisteminin, tüm belgeleri doğru ve eksiksiz bir şekilde tutamaması, yetkisiz erişim, veri sızıntısı ve yasal uyum risklerine yol açabilir. Bu durum, denetim izlerini takip etmeyi zorlaştırabilir ve hangi belgelerin gözden geçirilmesi ve onaylanması gerektiğini belirlemeyi zorlaştırabilir.
	<i>Uygun olmayan erişim kuralları, izinler ve güvenlik politikaları</i>	Belgelere erişimi düzenleyen kuralların ve izinlerin yeterince katı olmaması veya yanlış tanımlanmış olması, yetkisiz kişilerin hassas bilgilere erişmesine olanak tanıyabilir. Bu durum, veri ihlalleri, kimlik hırsızlığı ve mali kayıplara yol açabilir.
	<i>Kullanıcının yanlışlıkla hassas verileri veya bilgileri tehlikeye atması</i>	Kullanıcıların eğitim eksikliği veya dikkatsizliği nedeniyle hassas bilgileri yanlışlıkla ifşa etmesi veya silmesi, veri sızıntısı ve itibar zedelenmesine yol açabilir. Bu durum, yasal yaptırımlara ve müşteri güveninin kaybedilmesine yol açabilir.
<i>Dosya Konumlandırma ve Alaka Düzeyi</i>	<i>Kurumun tüm elektronik dosyaların depolandığı konumları</i>	Kurumun tüm elektronik dosyaların depolandığı konumları kapsayan merkezi bir arama yeteneğine sahip olmaması, istenen

<i>kapsayan merkezi bir arama yeteneğine sahip olmaması</i>	bilgileri bulmayı zorlaştırabilir ve zaman kaybına yol açabilir. Bu durum, denetim ve uyumluluk sorunlarına da yol açabilir.
<i>Kurum çalışanlarının elektronik belgeleri nerede sakladığına ilişkin yazılı düzenlemelerden yoksun olması</i>	Kurumun, çalışanların elektronik belgeleri nasıl ve nerede saklayacağı hakkında net kurallara sahip olmaması, veri yönetimi ve güvenliği açısından riskler yaratabilir. Bu durum, dosya çoğaltılmasına, veri kaybına ve yetkisiz erişime yol açabilir.
<i>Elektronik belgeleri aramak için etkili araçların olmaması</i>	Yeterli arama işlevselliğine sahip olmayan veya kullanımı zor olan arama araçları, bilgileri bulmayı zorlaştırabilir ve zaman kaybına yol açabilir. Bu durum, verimliliği ve üretkenliği düşürebilir.
<i>Elektronik belgelere yönelik sınıflandırma standartlarının olmaması, sınıflandırmanın yeterli olmaması veya yetersiz şekilde uygulanması</i>	Elektronik belgelerin nasıl sınıflandırılacağına dair net ve tutarlı standartların olmaması veya bu standartların yeterince titiz olmaması, dosyaları bulmayı ve yönetmeyi zorlaştırabilir. Bu durum, veri yönetimi ve güvenliği açısından da riskler yaratabilir.
<i>Elektronik dosya bağlantıları kurmanın önemi konusunda farkındalığın olmaması</i>	Çalışanların elektronik dosyalar arasında bağlantı kurmanın ve sürdürmenin önemini anlamaması, bilgi akışını engelleyebilir ve tekrarlayan görevlere yol açabilir. Bu durum, verimliliği ve üretkenliği düşürebilir.
<i>Personelin farklı arşiv biçimleri arasındaki bağlantıların farkında olmaması (Örneğin: kâğıt ve elektronik dosyalar arasındaki ilişki)</i>	Çalışanların kâğıt ve elektronik dosyalar arasındaki ilişkileri anlayamaması, bilgi erişimini ve iş birliğini zorlaştırabilir. Bu durum, veri tutarsızlığına ve hatalara yol açabilir.
<i>Sistem geliştiricilerinin ilgili elektronik dosya bağlantılarını kurma zorunluluğunun olmaması</i>	Sistem geliştiricilerinin, yeni sistemler ve uygulamalar tasarlarken ilgili elektronik dosya bağlantılarını kurma sorumluluğuna sahip olmaması, bilgi akışında kopukluklar yaratabilir ve veri yönetimini zorlaştırabilir. Bu durum, veri tutarsızlığına ve hatalara yol açabilir.
<i>Hangi elektronik dosya üstverilerinin oluşturulması veya</i>	Elektronik dosyalar için hangi üstverilerin oluşturulması veya alınması gerektiğine dair

	<i>alınması gerektiğine ilişkin düzenlemelerin olmaması</i>	net kuralların olmaması, veri yönetimini ve analizini zorlaştırabilir. Bu durum, veri tutarsızlığına ve hatalara yol açabilir.
<i>Elektronik Dosyaların Ayıklanması</i>	<i>Elektronik dosyalara yönelik kapsamlı bir ayıklama planının bulunmaması.</i>	Hangi elektronik dosyaların ayıklanacağına, ne zaman ve nasıl ayıklanacağına dair net bir planın olmaması, ayıklama işleminin rastgele ve tutarsız olmasına yol açabilir. Bu durum, yasal ve düzenleyici uyumluluk risklerine yol açabilir.
	<i>Elektronik belgelerin imha izni onaylanana kadar yasal geçerliliğini sürdürme olanağının olmaması</i>	İmha için onay bekleyen elektronik belgelerin yasal olarak geçerliliğini kaybetmemesi için özel bir sistemin olmaması, yasal ve mali risklere yol açabilir. Bu durum, davalara veya tazminat taleplerine yol açabilir.
	<i>Elektronik arşivlerde uygun imha işleminin gerçekleştirilememesi ve imhalık malzemenin değerinin zamanında belirlenememesi.</i>	Elektronik arşivlerin değeri zamanında belirlenmezse ve uygun imha işlemleri uygulanmazsa, veri sızıntısı, kimlik hırsızlığı ve yasal uyum riskleri ortaya çıkabilir. Bu durum, itibar zedelenmesine ve mali kayıplara yol açabilir.
	<i>Kurumun bilişim departmanının, bazı nedenlerden dolayı (örneğin: yetersiz sabit disk alanı vb.) dosya yönetimi departmanının onayı olmadan elektronik dosyaları silmesi</i>	Bilgi işlem biriminin dosya yönetimi departmanının onayı olmadan elektronik dosyaları silmesi, veri kaybına, yasal uyum risklerine ve departmanlar arasında koordinasyonsuzluğa yol açabilir. Bu durum, kurum içinde güvensizliğe ve çatışmalara yol açabilir.
<i>Elektronik Dosyaların İmhası</i>	<i>Kuruluşun ekipman hasarı nedeniyle (örneğin bilgisayar sunucusu sabit disk hasarı vb.) elektronik dosyalara zarar vermesi</i>	Bilgisayar sunucusu sabit disk gibi depolama ekipmanlarının hasar görmesi veya arızalanması, elektronik dosyaların kaybolmasına veya zarar görmesine yol açabilir. Bu durum, veri kaybına, yasal uyum risklerine ve mali kayıplara yol açabilir.
	<i>Kurumun elindeki elektronik dosyaların saklama ortamını ve formatını doğrulayamaması ve dosyaların kullanılamaz hale gelmesi</i>	Elektronik dosyaların saklandığı ortamın ve formatın zamanla bozulması veya eski teknolojiler kullanılması, dosyalara erişimi zorlaştırabilir veya imkânsız hale getirebilir. Bu durum, veri kaybına, yasal uyum risklerine ve mali kayıplara yol açabilir.

	<i>Kullanılan elektronik dosya formatlarının güncelliğini yitirmeye eğilimli olması</i>	Teknolojinin hızla değişmesi nedeniyle kullanılan elektronik dosya formatları zamanla güncelliğini yitirebilir ve yeni yazılımlarla açılmaz hale gelebilir. Bu durum, veri erişimi zorluklarına, veri kaybına ve mali kayıplara yol açabilir.
	<i>Elektronik dosyaların saklanması ve arşivlenmesi için ayrılmış bir saklama deposunun olmaması</i>	Elektronik dosyaların güvenli ve düzenli bir şekilde saklanması için özel bir alanın olmaması, veri kaybına, veri hırsızlığına ve yasal uyum risklerine yol açabilir. Bu durum, kurumun itibarını zedeleyebilir ve mali kayıplara yol açabilir.
<i>Yetkisiz Kullanım</i>	<i>Kimlik doğrulama teknolojisinin benimsenmemesi</i>	Güçlü parolalar, çok faktörlü kimlik doğrulama ve biyometrik doğrulama gibi sağlam kullanıcı kimliği doğrulama yöntemlerinin kullanılmaması, yetkisiz kişilerin sisteme erişmesini kolaylaştırabilir. Bu durum, veri hırsızlığı, kimlik hırsızlığı ve yasal uyum risklerine yol açabilir.
	<i>Çeşitli kullanıcı türlerinin erişim haklarının tanımlanmaması veya bunların uygunsuz şekilde tanımlanması</i>	Her kullanıcı türü için ayrı erişim hakları ve yetki seviyeleri tanımlanmazsa veya bu haklar uygun şekilde yönetilmezse, yetkisiz kişilerin hassas bilgilere erişmesi kolaylaşabilir. Bu durum, veri kaybına, yasal uyum risklerine ve itibar zedelenmesine yol açabilir.
	<i>Bilgi danışmanlığına ilişkin yazılı düzenlemelerden yoksunluk</i>	Kurumun, dış bilgi danışmanlık hizmeti veren firmalarla yaptığı anlaşmalar için yazılı ve net düzenlemeleri olmaması, veri güvenliği ihlallerine yol açabilir. Bu durum, yasal sorumluluk ve itibar riskleri yaratabilir.
	<i>Elektronik dosya erişim belgelerinin (yetkisiz erişim girişimleri belgeleri gibi) denetlenmemesi veya analiz edilememesi</i>	Elektronik dosyalara erişim kayıtlarının ve yetkisiz erişim girişimlerinin yeterince denetlenmemesi veya analiz edilmemesi, siber saldırıları ve veri sızıntılarını tespit etmeyi zorlaştırabilir. Bu durum, zamanında önlem alınmamasına ve daha büyük kayıplara yol açabilir.
	<i>Dış kaynak kullanım sözleşmesinde bilgi sızıntısını</i>	Dış kaynak hizmeti veren firmalarla yapılan sözleşmelerde, bilgi güvenliği ve veri

	<i>önlemek için bilgi güvenliği kontrol maddelerinin öngörülmemesi</i>	koruma ile ilgili maddeler yer almaması, veri sızıntılarına ve yasal risklere yol açabilir. Bu durum, kurumun itibarını zedeleyebilir ve mali kayıplara yol açabilir.
	<i>Sabotajlara ilişkin tedbirlerin olmaması</i>	Kurumun, çalışanlar veya eski çalışanlar tarafından yapılabilecek kasıtlı veri tahribatı veya sistem sabotajlarına karşı gerekli önlemleri almaması, önemli veri kayıplarına ve iş kesintilerine yol açabilir. Bu durum, mali kayıplara, itibar zedelenmesine ve yasal yaptırımlara yol açabilir.
<i>Stratejik Yönetim</i>	<i>Elektronik arşivler içerisinde yer alan materyaller için resmî belge statüsüne açıklık getirilmemesi</i>	Elektronik belgelerin ve arşivlerin resmi yasal belgeler olarak kabul edilip edilmediğine dair net bir yasal çerçeve veya kurumsal politika olmaması, yasal uyumsuzluklara ve itibar zedelenmesine yol açabilir. Bu durum, kurumun yasal yükümlülüklerini yerine getirmesini zorlaştırabilir ve ticari faaliyetlerini olumsuz etkileyebilir.
	<i>Elektronik belge yönetimine ilişkin herhangi bir operasyonel kılavuzun oluşturulmaması</i>	Elektronik belge yönetimiyle ilgili net ve güncel bir operasyonel kılavuzun olmaması, iş süreçlerinde tutarsızlıklara, hatalara ve gecikmelere yol açabilir. Bu durum, verimliliği düşürebilir, maliyetleri artırabilir ve kurumsal riskleri artırabilir.
	<i>Mevcut elektronik belge yönetimi stratejisinin güncellenmemesi</i>	Var olan elektronik belge yönetimi stratejisinin güncellenmemesi veya değişen iş ihtiyaçlarını karşılamaması, kurumun stratejik hedeflerine ulaşmasını zorlaştırabilir. Bu durum, rekabet avantajını kaybetmeye ve yeni pazar fırsatlarını kaçırmaya yol açabilir.
	<i>Kuruluşun sözleşmesi veya anlaşması, dış kaynak kullanan satıcıların veya üçüncü taraf grupların elektronik belge yönetimi hizmetleri (örneğin, bulut sürücülerinin kullanımı) sağlarken uyması gereken</i>	Dış kaynaklı elektronik belge yönetimi hizmeti veren firmalarla yapılan sözleşmelerde, veri güvenliği ve gizliliği ile ilgili net ve katı şartlar belirlenmemesi, veri sızıntılarına ve yasal risklere yol açabilir. Bu durum, kurumun itibarını zedeleyebilir ve mali kayıplara yol açabilir.

<i>standartları ve prosedürleri açıkça belirtmemesi</i>	
<i>Kuruluşun ortak çalışma alanlarında ve sosyal medyada saklanan elektronik dosyalara ilişkin resmi politikalarının ve yönetim prosedürlerinin bulunmaması</i>	Ortak çalışma alanlarında ve sosyal medyada paylaşılan elektronik dosyalarla ilgili net kurallar ve prosedürlerin olmaması, veri kaybına, veri sızıntılarına ve yasal uyum risklerine yol açabilir. Bu durum, kurumun itibarını zedeleyebilir ve yasal yaptırımlara yol açabilir.
<i>Kuruluşun elektronik belgelerin yönetimine yeterli kaynak ayırmaması</i>	Elektronik belge yönetimi için gerekli insan gücü, bütçe ve altyapı kaynaklarının yeterince tahsis edilmemesi, sistemin işleyişini ve verimliliğini olumsuz etkileyebilir. Bu durum, veri kaybına, gecikmelere ve maliyet artışlarına yol açabilir.
<i>Kuruluşun, elindeki elektronik dosyaların orijinallliğini, tamlığını ve erişilebilirliğini sürdürüp sürdürmediğini doğrulamak için ilgili plan veya yöntemlerden yoksun olması</i>	Elektronik dosyaların orijinallliği, bütünlüğü ve erişilebilirliği üzerinde yeterli kontrol mekanizmalarının olmaması, veri güvenliği ihlallerine ve yasal uyumsuzluklara yol açabilir. Bu durum, kurumun yasal yükümlülüklerini yerine getirmesini zorlaştırabilir ve itibar zedelenmesine yol açabilir.
<i>Kuruluşun elektronik dosya yedekleme önlemlerinin bulunmaması (Örneğin: tesis dışı yedekleme)</i>	Elektronik dosyaların tam ve güncel yedeklerinin alınmaması veya yedekleme sisteminin yeterince güvenli olmaması, veri kaybına ve sistem kesintilerine yol açabilir. Bu durum, kurumun faaliyetlerini ciddi şekilde etkileyebilir ve mali kayıplara yol açabilir.
<i>Sistemin temin edildiği tedarikçi firmanın elektronik dosyaların yedeğinin tamamen geri yüklenip kullanılabileceğini garanti edememesi</i>	EBYS'nin tedarik edildiği firmanın, sistemin arızalanması veya veri kaybı durumunda yedeklemelerden tam bir geri yükleme yapabileceğini garanti edememesi, önemli bilgilere erişimin kesilmesine ve iş kesintilerine yol açabilir. Bu durum, mali kayıplara, itibar zedelenmesine ve yasal yaptırımlara yol açabilir.
<i>Kuruluşun genel elektronik belge yönetimi performansını ölçmek</i>	EBYS'nin etkinliğini ölçmek için herhangi bir gösterge veya planın olmaması, sistemin

	<i>için herhangi bir planının veya yönteminin bulunmaması</i>	zayıflıklarının ve iyileştirme alanlarının belirlenmesini zorlaştırabilir. Bu durum, sistemin zamanla yetersiz kalmasına ve kurumun ihtiyaçlarını karşılayamamasına yol açabilir.
<i>Çevresel Hasar</i>	<i>Yangın, sel, deprem gibi doğal afetler (kayıtlar geri dönüşü olmayacak şekilde zarar görebilir veya tamamen yok olabilir)</i>	Yangın, sel veya deprem gibi doğal afetler, EBYS'nin bulunduğu altyapıya zarar verebilir veya tamamen yok edebilir. Bu durum, önemli bilgilere erişimin kesilmesine, veri kaybına ve iş kesintilerine yol açabilir. Ayrıca mali kayıplar, itibar zedelenmesi ve yasal yaptırımlar da öngörülebilir riskler arasındadır.
	<i>Haşere istilası (elektrik kablolarını çiğneyerek yangın riskini artırabilir)</i>	EBYS'nin bulunduğu alandaki haşere istilası, örneğin elektrik kablolarına zarar verebilir ve yangın riskini artırabilir. Bu durum hem veri kaybına hem de mali kayıplara yol açabilir. Haşereler ayrıca elektronik cihazlara ve veri taşıyıcılarına da zarar verebilir.
	<i>Depolama alanındaki kirlilik</i>	Depolama alanındaki kirlilik, özellikle video veya film gibi hassas medyalar için nem veya asit oranında artışa yol açabilir. Bu durum, kayıtların daha hızlı bozulmasına ve veri kaybına yol açabilir. Kirlilik ayrıca elektronik cihazlara da zarar verebilir ve sistemin arızalanmasına neden olabilir.
	<i>Isınma</i>	EBYS sunucularının bulunduğu ortamın aşırı sıcak olması, donanımın aşırı ısınmasına ve arızalanmasına yol açabilir. Bu durum, sistemin arızalanmasına ve veri kaybına neden olabilir.
<i>Donanım Arızası</i>	<i>Bir bilgisayar-sunucu sabit diskinin çökmesi</i>	Sabit diskin çökmesi, tüm verilerin kaybolmasına ve sistemin tamamen işlevsiz hale gelmesine yol açabilir. Bu durum, kurum için ciddi mali kayıplara, yasal yaptırımlara ve itibar zedelenmesine neden olabilir.
	<i>Kurumun bilgisayar sistemlerini yedeklememesi</i>	Düzenli yedekleme yapılmaması, veri kaybı durumunda kurtarma imkânını ortadan kaldırır. Bu durum, donanım arızası dışında,

		siber saldırılar, insan hataları veya doğal afetler gibi durumlarda da veri kaybına yol açabilir. Yedekleme eksikliği, kurumun işleyişini önemli ölçüde etkileyebilir ve hatta faaliyetlerini durdurmasına neden olabilir.
	<i>Kullanılan sistemin geriye dönük olarak uyumlu olmaması</i>	Sistemin eski sürümlerle uyumsuz olması sistem arızalarına veya veri kaybına yol açabilir. Bu durum, sistemin güncellemelerini engelleyebilir ve yeni teknolojilerle entegrasyonu zorlaştırabilir.
	<i>Güç Kaybı</i>	Ani elektrik kesintileri veya voltaj dalgalanmaları, EBYS'nin donanımına zarar verebilir ve veri kaybına yol açabilir. Bu durum, sistemin arızalanmasına ve iş kesintilerine neden olabilir.
	<i>Yazılım-Donanım Uyumsuzluğu</i>	EBYS'nin işletim sistemi veya yazılımları ile donanımın uyumsuz olması, sistem arızalarına ve veri kaybına yol açabilir. Bu durum, sistemin performansını düşürebilir ve kullanım konforunu olumsuz etkileyebilir.

Kaynak: ISO 18128, 2024; Public Record Office Victoria, 2010; Lin, 2020

2.1.2. Risk Analizi

Risk unsurları belirlendikten sonra, risk analizi aşaması devreye girer. Bu aşamada amaç, risklerin kapsamlı bir şekilde anlaşılması ve gerekli durumlarda iyileştirilmesi için stratejiler geliştirilmesidir. AS/NZS 4360 (2004) standardına göre risk analizi, risk kaynaklarının, bunların olası olumlu ve olumsuz sonuçlarının ve bu sonuçların ortaya çıkma olasılığının değerlendirilmesini içerir. Bu sayede risklerin niteliği ve seviyesi belirlenerek, risk değerlendirmesi ve risk tedavisi için sağlam bir zemin hazırlanır. ISO 27005 (2022, s. 5) standardında da vurgulandığı gibi, risk analizi kısaca risk tahmini olarak özetlenebilir.

ISO 31000 (2018b) standardına göre risk analizi, riskin tüm yönlerini anlamaya odaklanır. Bu kapsamlı süreçte, belirsizliklerin, risk kaynaklarının, olası sonuçların ve gerçekleşme olasılıklarının yanı sıra mevcut kontrollerin etkinliği de detaylı bir şekilde

değerlendirilir. Farklı senaryolar incelenerek risklerin tam olarak anlaşılması hedeflenir.

Risk analizi, kapsamlı bir değerlendirme için çeşitli faktörleri göz önünde bulundurmalıdır. ISO 18128:2024 standardına göre dikkate alınması gereken unsurlar şunlardır:

- Olayların ve sonuçların olasılığı: Her bir olayın gerçekleşme şansının ve potansiyel sonuçların ne kadar olası olduğunun belirlenmesi.
- Sonuçların niteliği ve büyüklüğü: Olumsuz sonuçların potansiyel etkilerinin ve ciddiyetinin değerlendirilmesi.
- Karmaşıklık ve bağlantısallık: Farklı risklerin birbiriyle nasıl etkileşime girdiğinin ve genel risk profilini nasıl etkileyebileceğinin analiz edilmesi.
- Zamana bağlı faktörler ve oynaklık: Risklerin zaman içinde nasıl değişebileceğinin ve bu değişimlerin nasıl ele alınacağına değerlendirilmesi.
- Duyarlılık ve güven seviyeleri: Farklı varsayımlara ve koşullara karşı riskin ne kadar hassas olduğunun ve analiz sonuçlarının ne kadar güvenilir olduğunun belirlenmesi.

Analiz teknikleri, kullanılan faktörlere ve analiz sonuçlarının kullanım amacına bağlı olarak niteliksel, niceliksel veya her ikisinin bir kombinasyonu olabilir.

2.1.2.1. İş Etki Analizi (Business Impact Analysis)

İş Etki Analizi (İEA), bir olay veya kesintinin kuruluşun belge ve belge yönetimi fonksiyonlarını nasıl etkileyebileceğini değerlendirmeye yönelik bir tekniktir. Bu analiz, kesintinin potansiyel sonuçlarını belirlemek, önemli belgeleri ve süreçleri tanımlamak ve bu riskleri yönetmek için gerekli yetenekleri belirlemek ve ölçmek için kullanılır. Analiz kapsamında, olası olaylar ve bunların gerçekleşme olasılıkları, her bir olayın belge ve belge yönetimi üzerindeki potansiyel etkileri, bu etkilerin şiddeti ve süresi, önemli belgelerin ve süreçlerin tanımlanması ve bu riskleri yönetmek için gerekli kaynakların ve yeteneklerin belirlenmesi yer alır (ISO 18128, 2024, s. 11).

Özetle, iş etki analizi, kuruluşların belge ve belge yönetimi sistemlerinin direncini ve sürdürülebilirliğini geliştirmelerine yardımcı olan önemli bir risk değerlendirme aracıdır.

2.1.2.2. İnsan Güvenilirliği Analizi (Human Reliability Analysis)

İnsan hatası, sistemin tasarımından üretimine, kurulumundan işletimine, bakımından sürdürülebilirliğine kadar her aşamada meydana gelebilir. Bu hatalar sistemlerin karmaşıklığı arttıkça daha sık oluşabilir ve ciddi sonuçlar doğurabilir. İnsan güvenilirliği ise, bir çalışanın görevi doğru bir şekilde, zamanında ve sistemin işleyişini bozabilecek herhangi bir hata yapmadan yerine getirme yeteneği olarak tanımlanmaktadır. İnsan güvenilirliğinin belirlenmesi, insan hatalarından kaynaklanan kazaların önlenmesinde önemli rol oynamaktadır. İnsan güvenilirliğini belirlemek için İnsan Güvenilirliği Analizi (İGA) yapılır. Bu analiz insan hatalarının nedenlerini sonuçlarıyla birlikte belirleyerek bir kişinin sistem güvenilirliğine ve güvenliğine etkisini değerlendiren bir yöntemdir. Özellikle doğru performansın büyük önem taşıdığı görevlerde taktik düzeyde uygulanmalıdır (Yalçın, Altun Çiftçioglu ve Güzel, 2024).

İGA, kurumlarda belge yönetimi sürecinde sistem kullanıcılarının yaptıkları hataların sonuçlarını tespit etmek, kullanıcıların sistem güvenilirliğine etkisini değerlendirmek ve buna ilişkin önlemler geliştirmek için de başvurulmuş bir yöntemdir. Bu yöntem sayesinde belge yönetiminin tasarım, uygulama ve değişiklik aşamalarında hataları en aza indirecek şekilde tasarlanması ve korunması sağlanır. İGA'nın belge yönetiminde iki farklı kullanım alanı mevcuttur:

Tasarım aşaması: Belge yönetim sistemlerinin çalışanların hata olasılığını en aza indirecek şekilde tasarlanmasını sağlamak.

Uygulama aşaması: Hataları azaltacak şekilde prosedürleri iyileştirmek.

İGA uygulamasında, öncelikle belge süreçleri ve sistemlerdeki tüm faaliyetler detaylı bir şekilde analiz edilerek hiyerarşik bir görev analizi gerçekleştirilir. Bu analiz sonucunda, her bir faaliyet için potansiyel hata mekanizmaları, anahtar kelime istemleri kullanılarak belirlenir. Belirlenen her hata mekanizmasının, süreç üzerindeki olası etkileri ve gerçekleşme olasılığı detaylı bir şekilde değerlendirilir. Son olarak, bu değerlendirmeler doğrultusunda hataları önlemek veya etkilerini azaltmak için uygun kontrol stratejileri geliştirilir. Bu adımlar, İGA'nın sistematik ve kapsamlı bir şekilde uygulanmasını sağlayarak belge yönetimindeki hata risklerinin kontrollü bir şekilde belirlenmesine ve azaltılmasına yardımcı olur (ISO 18128, 2024, s. 12).

2.1.2.3. Papyon Analizi

Papyon diyagramları, bir olayın nedenlerinden sonuçlarına uzanan yolları ve bu yolları etkileyen kontrolleri görselleştiren güçlü bir risk analizi aracıdır. Karmaşık riskleri basit ve anlaşılır bir şekilde sunarak farklı senaryoların değerlendirilmesini kolaylaştırır. Arıza ve olay ağaçlarından türetilen papyon diyagramları, genellikle bir atölye ortamında doğrudan bir ekip tarafından da çizilebilir. Bu teknik, bir olayın birden fazla olası nedeni ve sonucu olabileceği durumlarda risk bilgilerini etkili bir şekilde iletmek için idealdir. Her yolun etkili kontrollere sahip olduğunu ve bu kontrollerin başarısız olmasına neden olabilecek faktörlerin (yönetim sistemi arızaları dâhil) analiz edildiğini de kontrol eder (ISO 18128, 2024, s. 12). Papyon diyagramları, riskleri görselleştirmenin ve analiz etmenin basit ve etkili bir yoludur ve elektronik belge yönetimi gibi karmaşık sistemlerde risk yönetiminde önemli bir rol oynar.

Risklerin analizi ve değerlendirilmesinde basit ve etkili bir yöntem olarak kabul gören risk matrisleri, elektronik belge yönetiminde de önemli bir araçtır. Bu matrisler, kurumun yapısına ve işlevine göre belirlenen sonuç derecelendirme ölçeği ve her bir riskin etkisinin analizi ile riskin gerçekleşme olasılığını gösteren bir olasılık tablosundan oluşur (Cox, 2008: 498; Public Record Office Victoria, 2010). Risk matrisi ile elektronik belge yönetimindeki riskler sistematik olarak değerlendirilir ve karşılaştırılır. Bu sayede riskler önceliklendirilir ve risk yönetimi planları geliştirilir. Mevcut sistem ve program doğrultusunda tespit edilen riskler analiz edildikten sonra her birinin etkisi (sonucu) değerlendirilir ve sonuçlar risk kaydına alınabilir. Bu sayede;

- Riskler sistematik bir şekilde değerlendirilebilir ve karşılaştırılabilir,
- Öncelikli riskler belirlenebilir,
- Risk yönetim planları geliştirilebilir,
- Kurumun risklere karşı hazırlıklı olması sağlanır.

Elektronik belge yönetimi sistemlerinin güvenliği ve sağlamlığı, kurumların itibarı ve işleyişi için hayati önem taşır. Bu nedenle elektronik belge yönetimindeki riskleri belirlemek ve analiz etmek oldukça önemlidir. Risklerin etki düzeylerini değerlendirmek, risk yönetimi sürecinin önemli bir aşamasıdır. Bu aşamada, her bir riskin potansiyel olarak neden olabileceği zararı veya hasarı ölçmek gerekir. Risklerin etki düzeylerini değerlendirmek için çeşitli yöntemler kullanılabilir. Elektronik belge

yönetiminde yaygın olarak kullanılan yöntemlerden biri Risklerin Etki Düzeylerinin Değerlendirilmesi Ölçeği'dir. Risk derecelendirmelerini 'çok ciddi'-'önemsiz' aralığında 5 grup altında toplayan bu ölçek Tablo 2.6'da yer almaktadır.

Tablo 2.6: Risklerin etki düzeylerinin değerlendirilmesi ölçeği

Ölçek	Derecelendirme	Riskin gerçekleşmesi durumunda sonuç
5	Çok ciddi	İşletmenin temel hedefleri için hayati etkisi vardır ve çok büyük mali sonuç yaratabilir.
4	Ciddi	Kurum için büyük siyasi utanç meydana getirir.
3	Orta	Mevzuat veya iş gereksinimleriyle uyumu bozar.
2	Hafif	Önemli veriler kaybolur.
1	Önemsiz	Verimsiz iş süreçlerine neden olur. Alınan kararlar ve gerçekleştirilen aksiyonlar eksik veya güncel olmayan bilgilere göre yapılır.

Kaynak: Valipour vd., 2014, s. 25

Risklerin etki düzeylerini değerlendirmek, risk yönetimi sürecinin önemli bir aşamasıdır. Bu ölçek, elektronik belge yönetimindeki riskleri sistematik bir şekilde değerlendirmek ve bu risklere karşı uygun önlemleri almak için faydalı bir araçtır.

Risk yönetimi sürecinin önemli bir diğer aşaması da risklerin gerçekleşme ihtimallerinin değerlendirilmesidir. Bu aşamada, her bir riskin ne kadar olasılıkla gerçekleşebileceğini belirlemek gerekir. Risklerin gerçekleşme ihtimallerini değerlendirmek için çeşitli yöntemler kullanılabilir. Elektronik belge yönetiminde risklerin gerçekleşme ihtimallerini değerlendirmek için kullanılan olasılık seviyeleri ve açıklamaları Tablo 2.7'de yer almaktadır.

Tablo 2.7: Risklerin gerçekleşme ihtimallerinin değerlendirilmesi

Seviye	Olasılık	Açıklaması
A (5)	Neredeyse kesin-kesinlikle- çok yüksek	Risk senaryosunun gerçekleşme ihtimali çok yüksek (Olayın gerçekleşmesi bekleniyor)
B (4)	Muhtemelen- büyük ihtimalle- yüksek	Risk senaryosunun gerçekleşme ihtimali yüksek. (Olay muhtemelen gerçekleşecektir)
C (3)	Olası- orta ihtimalle- orta	Risk senaryosunun gerçekleşme olasılığı orta seviyededir. (Olay herhangi bir zamanda meydana gelebilir)
D (2)	Olasılık dışı- az ihtimalle- küçük	Risk senaryosunun gerçekleşme olasılığı düşüktür. (Pek olası değil ama olayın herhangi bir zamanda meydana gelmesi mümkündür)

E (1) Olasılıksız

Risk senaryosunun gerçekleşme ihtimali çok düşük. (Olayın meydana gelmesi pek olası değil)

Kaynak: ISO 27005, 2022, s. 42; Karahan ve Aydoğmuş, 2023, s. 57

Elektronik belge yönetiminde risklerin gerçekleşme ihtimallerini değerlendirmek için Tablo 2.7’de yer alan olasılık seviyeleri ve açıklamalar kullanılabilir. Bu ölçek, risklerin ne kadar olasılıkla gerçekleşebileceğini belirlemek için bir çerçeve sağlar. Risklerin gerçekleşme ihtimallerini ve etki düzeylerini birlikte değerlendirerek her bir riskin önem derecesini ve öncelik sırasını belirlemek mümkündür. Bu bilgiler, risk yönetimi planları geliştirmek ve risklere karşı uygun önlemleri almak için kullanılabilir.

Risk analizi, elektronik belge yönetim sistemlerinde ve süreçlerindeki riskleri belirlemek ve değerlendirmek için kullanılan önemli bir yöntemdir. Bu analiz sayesinde her bir riskin potansiyel sonuçları ve gerçekleşme ihtimalleri belirlenerek risklere karşı en uygun önlemler alınabilir. Risk analizi sonucu, her bir risk için bir risk sonuç derecesi ve olasılık derecelendirmesi yapılır. Bu derecelendirmeler, riskin önemini ve acil müdahale ihtiyacını belirlemek için kullanılır. Risk sonuç derecelendirmesi, riskin gerçekleşmesi durumunda oluşabilecek hasarın veya kaybın boyutunu ifade eden bir analiz tekniğidir. Aşağıda risk analiziyle ilgili bir örnek yer almaktadır.

Tablo 2.8: Risk analizi tablosu örneği

<i>Risk Kategorisi</i>	<i>Risk</i>	<i>Sonuçlar</i>	<i>Risk Sonuç Derecelendirmesi</i>	<i>Risk Olasılığı Derecelendirmesi</i>
Yetkisiz erişim	Yetersiz belge erişim kontrolleri, gizli belgelerin sızdırılmasına ve bu durumun siyasi bir skandala yol açmasına neden olabilir.	Gizli belgelerin sızması, kurumsal ve siyasi itibar kaybına, işten çıkarmalara ve yasal soruşturmalara yol açabilir.	4 – Çok Yüksek / Büyük	C – Mümkün
Uygunsuz güvenlik uygulamaları	Uygunsuz güvenlik önlemleri, gizli dosyaların sızmasına ve sözleşmenin ihlali davası açılmasına yol açabilir.	Ticari sır niteliğindeki bilgilerin sızması, acenteye tazminat davası ve iş kaybı ile sonuçlanabilir.	4- Çok Yüksek / Büyük	C – Mümkün

Veri sızdırılması	Müşteri bilgilerinin yetersiz güvenlik nedeniyle korunmaması, Bilgi Gizliliği mevzuatına uymama riskini doğurur.	Bilgi Gizliliği mevzuatı nedeniyle kurum yasal yaptırımlara maruz kalabilir.	3 – Orta / Ilıman	B – Muhtemel
İnsan hataları	Yetkisiz belge imhası, kurumun Uyum ihlali nedeniyle Suçlar (Belge İmhası) Yasası'na aykırı düşerek para cezası ödemesine yol açabilir.	Belgelerin yasal gereklilikler doğrultusunda saklanmaması, kurumsal itibar kaybına, yasal yaptırımlara ve maddi tazminat yükümlülüğüne yol açabilir.	3 – Orta / Ilıman	C – Mümkün

Kaynak: Public Record Office Victoria, 2010

Bu risk analizi tablosu örneği, elektronik belge yönetim sistemlerindeki yaygın riskleri ve bu risklerin potansiyel sonuçlarını, risk sonuç derecelendirmelerini ve olasılık derecelendirmelerini göstermektedir. Tablo 2.8’de yer alan örnek yetkisiz erişim, veri sızdırılması, insan hatası ve uygunsuz güvenlik uygulamaları gibi çeşitli risk türlerini kapsamaktadır. Risk analizi, elektronik belge yönetim sistemlerindeki riskleri belirlemek ve değerlendirmek için önemli bir araçtır. Bu analiz sayesinde, her bir riskin potansiyel etkisi ve gerçekleşme olasılığı sistematik bir şekilde değerlendirilebilir. Risklerin sonuçlarına ve olasılıklarına göre öncelik sıralaması yapılarak risklere karşı en uygun önlemler alınabilir. Bu tabloda yer alan risklerin her biri elektronik belge yönetim sistemlerinin güvenliğini ve bütünlüğünü önemli ölçüde etkileyebilir. Bu nedenle bu risklere karşı uygun önlemler almak ve risk yönetim planları geliştirmek önemlidir. Risk yönetim planları, risklerin azaltılması veya ortadan kaldırılması için gerekli adımları ve bu adımların sorumlularını tanımlamalıdır. Ayrıca planlarda risklerin izlenmesi ve değerlendirilmesi için mekanizmalar da yer almalıdır.

Elektronik belge yönetim sistemlerinde risk analizi ve risk yönetimi, sistemlerin güvenliğini ve bütünlüğünü korumak, yasal uyumluluğu sağlamak ve işletmenin itibarını korumak için oldukça önem taşımaktadır.

2.1.3. Risk Değerlendirme ve Teknikleri

Risklerin değerlendirilmesi, potansiyel tehlikelerden kaynaklanabilecek risklerin büyüklüğünü tahmin etme ve mevcut kontrol mekanizmalarının bu riskleri bertaraf etmede ne kadar yeterli olduğunu değerlendirme sürecidir. Bu sayede risklerin kabul edilebilir olup olmadığına karar verilebilir ve kabul edilemez riskler için gerekli önlemler belirlenebilir. Ceylan ve Başhelvacı'ya (2011, ss. 26-27) göre risk değerlendirmesinin iki temel amacı vardır:

- Risklerin Kabul Edilebilirliği: Mevcut risklerin kabul edilebilir bir seviyede olup olmadığını belirlemek.
- Risk Azaltma Tedbirleri: Kabul edilemez riskler için gerekli önlemleri ve tedbirleri tanımlamak.

Risklerin değerlendirilmesi, çalışma ortamlarında iş kazaları ve meslek hastalıklarını önlemek için oldukça önemli bir araçtır. Ayrıca kurumsal itibar kaybı, maddi tazminat yükümlülükleri ve yasal yaptırımlar gibi olumsuz sonuçları da önleyebilmektedir.

Risklerin değerlendirilmesi, risklerin kabul edilebilirlik seviyesini belirlemek için risk analizinin sonuçlarını risk kriterleriyle karşılaştırma işlemidir (ISO 27005, 2022).

ISO 31000 (2018b) standardına göre yapılan risk değerlendirmesi sonucunda beş temel karar alınabilir: Risk kabul edilebilir seviyede ise herhangi bir ek işlem yapmaya gerek duyulmaz. Aksi takdirde, riski azaltmak için farklı kontrol mekanizmaları değerlendirilir veya risk tam olarak anlaşılmıyorsa daha detaylı analizler yapılır. Mevcut kontroller riski yeterli seviyede yönetiyorsa bu kontroller sürdürülür. Ancak risk, kuruluşun genel hedeflerini tehdit eder nitelikteyse bu hedefler yeniden değerlendirilir.

Risk değerlendirmesinin sonucu yazılı olarak kaydedilmeli, ilgili kişilere iletilmeli ve kuruluşun uygun seviyelerinde doğrulanmalıdır. Bu sayede riskler güncel tutulur ve gerekli önlemler zamanında alınabilir.

2.1.3.1. Makul Olarak Uygulanabilir En Düşük Seviye (As Low As Reasonably Practicable) (ALARP)

ALARP ilkesi, riskleri kabul edilebilirlik seviyelerine göre üç ana kategoriye ayırmaktadır. Kabul edilemez bölgedeki riskler, acil önlemlerle ortadan kaldırılmalı veya tolere edilebilir seviyeye indirilmelidir. Tolere edilebilir bölgedeki riskler, kazançlar karşılığında kabul edilebilir olsa da zamanla azaltılmaya çalışılmalıdır.

Kabul edilebilir bölgedeki riskler ise günlük yaşamın bir parçası olarak kabul edilebilecek kadar düşüktür ve makul önlemlerle daha da azaltılabilir. Örneğin, yangın söndürme sistemlerinin yetersizliği kabul edilemez, tehlikeli madde taşımacılığı tolere edilebilir, ofis ortamında kayma riski ise kabul edilebilir bir risk olarak değerlendirilebilir (Baybutt, 2013).

ALARP ilkesi, risklerin kabul edilebilir seviyelerini belirlemede ve uygun risk yönetimi stratejileri geliştirmede önemli bir araçtır. Bu ilke sayesinde, kuruluşlar ve bireyler kaynaklarını en etkili şekilde kullanarak riskleri en aza indirebilir ve güvenli bir ortam oluşturabilirler. Aşağıdaki örnekte (Tablo 2.9), ALARP modeli kullanılarak belge yönetimiyle ilgili risklerin sınıflandırılmasına yönelik bir örnek gösterilmektedir.

Tablo 2.9: ALARP modeli örneği

<i>Küçük</i>	<i>Orta</i>	<i>Büyük</i>	<i>Şiddetli</i>
Belgelere erişim kısıtlanmasının ihlali (a)	Belgelere yetkisiz erişim (b)	Belgelere izinsiz erişim (b)	Yaygın, kayıp, yetkisiz erişim ve belgelere zarar verilmesi (c)
Bir iş ortamındaki az miktardaki belgenin hasar görmesi (a) <i>-Küçük bir iş ortamındaki belgelerde meydana gelen az miktarda hasar</i>	Bir operasyon alanında önemli miktarda belgede hasar meydana gelmesi (b) <i>-Tek bir iş ortamındaki belgelerde meydana gelen önemli miktarda hasar</i>	Çeşitli alanlara yayılan operasyonel belgelerdeki hasar(b) <i>-Belgelerdeki hasarın birkaç alanı etkilemesi</i>	Operasyon alanlarının çoğunda hayati önem taşıyan belgelerin hasar görmesi <i>-İş ortamındaki çoğu önemli belgenin hasar görmesi</i>
Sınırlı belge/veri kaybı (b)	Veri kaybı/belgelerin güvenilirliğinde hasar (b)	Veri kaybı/belgelerin güvenilirliğinde hasar (b)	Veri kaybı/güvenilirlik kaybı/kamu güveninin kaybı (c)
Kurtarılabılır belge kaybı (b)	Operasyonlar kesintiye uğramaz; belgeler çabayla kurtarılabılır (b)	Kaybın kabul edilmesi; birden fazla faaliyet alanında kesinti; belgelerin kurtarılmasının maliyetli olması veya mümkün olmaması (c)	Operasyonların durması; kurtarma çabalarının maliyetli ve zaman alıcı olması; belgelerin kurtarılamaz durumda olması (c)
(a) Geniş ölçüde kabul edilebilir, ALARP azaltılabilir.			

(b) Tolere edilebilir ve ALARP azaltılmalıdır.

(c) Kabul edilemez.

Kaynak: ISO 18128, 2024, s. 14

2.1.3.2. Güvenilirlik Merkezli Bakım (Reliability Centred Maintenance)

Güvenilirlik Merkezli Bakım (GMB), bir varlığın (makine, ekipman vb.) ömrü boyunca en yüksek performans ve güvenilirliği sağlamak amacıyla tasarlanmış, risk temelli bir bakım stratejisidir. Bu strateji, geleneksel reaktif bakım yöntemlerinin aksine arızaların meydana gelmesinden önce olası sorunları tespit ederek ve önleyici tedbirler olarak beklenmedik duruş sürelerini en alt seviyeye indirir. GMB, varlıkların kritikliği, arıza etkileri ve olası arıza modları gibi faktörleri detaylı bir şekilde analiz ederek veri toplama, analiz ve önleyici bakım uygulamalarıyla desteklenir. Bu sayede planlanmamış duruşlar azaltılır, bakım maliyetleri düşürülür, varlık ömrü uzatılır, güvenlik artırılır, enerji verimliliği sağlanır ve üretim kalitesi yükseltilir. Titreşim analizi, yağ analizi, termal görüntüleme ve akıllı sensörler gibi teknolojiler, GMB uygulamalarında sıklıkla kullanılır. GMB'nin başarılı olması için güçlü bir veri tabanı, eğitimli personel ve yönetimin desteği gibi faktörler önemlidir (ISO 18128, 2024, ss. 14-15).

GMB yöntemi bir dizi adımdan oluşmaktadır. Yöntem, bu adımların tekrarlanabilir ve sürekli iyileştirilebilir bir döngü halinde uygulanmasını gerektirir. Sistematik olarak izlenmesi gereken bu süreç genellikle aşağıdaki adımları içermektedir:

- GMB uygulanacak sistemin tanımlanması ve sınırlarının belirlenmesi.
- Potansiyel arıza modlarının belirlenmesi ve her birinin olasılığı, etkisi ve kritikliği değerlendirilmesi.
- Her arıza modu için en uygun bakım stratejisinin belirlenmesi.
- Bakım faaliyetlerinin planlanması ve programlanması.
- Bakım planının uygulanması ve izlenmesi.
- Bakım faaliyetlerinin etkinliğinin değerlendirilmesi ve gerekli iyileştirmelerin yapılması.

GMB'nin EBYS üzerinde başarılı bir şekilde uygulanması için belge yönetim ilkeleri ve temellerinin, ilgili araçların ve yapının, iş ortamının ve alt sistemlerin iyi anlaşılması, olası arızaların ve bu arızaların sonuçlarının tutarlı bir şekilde analiz

edilmesi gerekmektedir. Bu analiz, bakım işlerinin tamamlanması, iş ortamındaki değişiklikler veya diğer eylemler gibi çalışmanın nihai sonucunu belirlemektedir.

Tablo 2.10: GMB tekniği uygulanarak bakım görevleri listesine örnek

Belgelerin ve belge sistemlerinin bütünlüğünü, kullanılabilirliğini etkileyen işlevsel arızalar				
<i>Belgeler/Belge süreçleri, sistemleri veya kontrolleri</i>	<i>Hata modu</i>	<i>Nedenler</i>	<i>Görev türü</i>	<i>Azaltma görevi tanımı ve aralığı</i>
Belgeler: Kritik önem taşıyan belgeler	Kayıp	Kasıtlı saldırı, sistem arızası veya doğal afet sonucu sisteme verilen zararlar	Proaktif Proaktif	- Günlük bir yedekleme rejimi ayarlanmalı. - Yedekleme geri yükleme süreci ve koordinasyonu yılda bir kez prova edilmeli. Tespit edilen tüm sorunlar ele alınmalı. - Hayati önem taşıyan belgeler kontrollü bir ortamda saklanmalı. - Fiziksel belgeler üzerinde kopyalama/dijitalleştirme veya çoğaltma çalışmalarının yapılması.
Belge süreci: Düzenleme	Kayıp	İzinsiz imha	Önleyici Proaktif	- Belgeleri yok etme iznine sahip kişi sayısının sınırlanması. - Belgelerin imhası konusunda eğitim ve farkındalık
Belge kontrolleri: Belgelere erişim	Yetkisiz erişim	Personel ihlali	Proaktif Reaktif	- Belgelere erişim veya erişim üyelik gruplarının yıllık olarak gözden geçirilmesi - Belge sınıflandırma şemasına uygulanan varsayılan erişim hükmünün yıllık bazda gözden geçirilmesi - Sürekli olarak kullanıcı farkındalığı eğitiminin sağlanması - Erişim kontrollerinin üç ayda bir gözden geçirilmesi - Olası ihlallerin belirlenmesi için kullanıcı erişim günlüklerinin üç ayda bir denetlenmesi. - Olayın incelenmesi ve temel nedenin anlaşılması, belgelerin kontrol önlemlerinin iyileştirilmesi
Belge sistemi	Güvenliği tehlikede olan (Sınırlı, Tehlikede)	Siber saldırı	Önleyici Proaktif	- Yılda bir kez siber güvenlik testlerinin yapılması - Ayda bir kez sistem güvenliğinin kontrol edilmesi - Ağ güvenliğinin iyileştirilmesi

Belge sistemi	Sistem kesintisi	• Zayıf sistem performansı, dengesiz platform • Elektrik kesintisi	Önleyici Proaktif	• Yılda iki kez sistemin sağlık kontrolünün yapılması • Yedek gücün ayarlanması

Kaynak: ISO 18128, 2024

GMB tekniği kullanılarak oluşturulmuş örnek bir bakım görevleri listesi olan Tablo 2.10'da, belgelerin ve belge sistemlerinin bütünlüğünü ve kullanılabilirliğini etkileyen işlevsel arızalar için potansiyel hata modları, nedenleri, görev türleri ve azaltma görevlerine ilişkin açıklamalar yer almaktadır. Bu örnek, GMB'nin nasıl kullanılabileceğine dair bir başlangıç noktasıdır. Her kuruluşun özel ihtiyaçlarını ve risklerini göz önünde bulundurarak kendi programını geliştirmesi önemli görülmektedir.

2.1.3.3. Risk Değerlendirme Matrisleri

ABD askeri standardı MIL-STD_882-D olarak da bilinen risk değerlendirme karar matrisi, sistem güvenlik program gereksinimlerini karşılamak amacıyla geliştirilmiş bir araçtır. Bu matris, iki veya daha fazla değişken arasındaki ilişkiyi analiz etmek için kullanılmaktadır. Bu matrislerden L Tipi Matris (LTM) yönteminde tehlikelerin oluşma olasılığı ile meydana gelme olasılığı arasındaki ilişki analiz edilmektedir (Department of Defence, 2000). Genel olarak 5x5 Matris yöntemi olarak bilinen ve L tipi matris olarak da adlandırılan metot, kolay anlaşılıp kolay uygulanabilir olmasından dolayı ülkemizde en çok tercih edilen risk değerlendirme yöntemidir (Kabakulak, 2019, ss. 100-101).

Bu yöntemde değerlendirme yapmak için risk model formülü kullanılmaktadır. Formül, riskin meydana gelme olasılığı ile meydana gelmesi sonucundaki etkinin çarpımıdır (Saffady, 2005; Bannerman, 2008, Cox, 2008, Ceylan ve Başhelvacı, 2011; Kuzucuoğlu, 2014; Hazine ve Maliye Bakanlığı, 2024).

'Risk = Tehlikeli Bir Olayın Meydana Gelme İhtimali (Olasılık) * Tehditin Etkisi/Şiddeti'

Tablo 2.11: Risk değerlendirme tablosu

RİSK DÜZEYİ = Olasılık x Şiddet					
ŞİDDET					
OLASILIK	Çok ciddi (5)	Ciddi (4)	Orta (3)	Hafif (2)	Önemsiz (1)
Çok yüksek (5)	Yüksek (25)	Yüksek (20)	Yüksek (15)	Orta (10)	Düşük (5)
Yüksek (4)	Yüksek (20)	Yüksek (16)	Orta (12)	Orta (8)	Düşük (4)
Orta (3)	Yüksek (15)	Orta (12)	Orta (9)	Düşük (6)	Düşük (3)
Küçük (2)	Orta (10)	Orta (8)	Düşük (6)	Düşük (4)	Düşük (2)
Çok Küçük (1)	Düşük (5)	Düşük (4)	Düşük (3)	Düşük (2)	Düşük (1)

Kaynak: Ceylan ve Başhelvacı, 2011, s. 29

Çarpım sonucunda risk düzeyleri belirlenmekte ve buna göre bir risk ısı haritası yapılmaktadır. Bu aralıklardan 15 – 25 = Yüksek Risk (Kırmızı), 8 – 12 = Orta Risk (Sarı), 1 – 6 = Düşük Risk (Yeşil) olarak belirlenmektedir. Risk düzeyinin belirlenmesinin ardından sonucunun kabul edilebilirlik değerleri tespit edilmektedir. Söz konusu bu aşama Tablo 2.12’de açıklanmaktadır (Çelikleş ve Ünlü, 2018):

Tablo 2.12: Sonucun kabul edilebilirlik değerleri

Sonuç	Yapılacak Çalışmalar
Tolere Edilemez/ Katlanılamaz Risk (20-25)	Risk kabul edilebilir seviyeye çekilene kadar çalışmaya başlanmaz, çalışma yapılıyorsa durdurulur. Yapılan çalışmalara rağmen risk düşürülemediyse, faaliyet engellenmelidir.
Kabul Edilemez/Önemli Riskler (15, 16)	Belirlenen risk azaltılınca kadar iş başlatılmamalı eğer devam eden bir faaliyet varsa derhal durdurulmalıdır. Risk işin devam etmesi ile ilgiliyse acil önlem alınmalı ve bu önlemler sonucunda faaliyetin devamına karar verilmelidir.
Dikkate Değer/Orta Düzey Risk (8, 9, 10, 12)	Riski azaltıcı faaliyetler başlatılır. Oluşacak maliyetler, dikkatle ölçülür ve sınıflandırılır. Risk azaltma önlemleri için belirli zamanlar ve periyotlar belirlenir.

Kabul Edilebilir/ Katlanılabilir Risk (2, 3, 4, 5, 6)	Mevcut kontrollere devam edilir. Mevcut kontrollerin, uygulanıp uygulanmadığı denetlenmelidir. İlave faaliyete ihtiyaç yoktur.
Önemsiz Risk (1)	Belirlenen riskleri ortadan kaldırmak için kontrol tedbirleri planlamaya ve gerçekleştirilecek faaliyetlerin belgelerini saklamaya gerek yoktur.

Kaynak: Çelikaş ve Ünlü, 2018

Bu teknik, puanlama yöntemi kullanarak riskleri ölçmek için bir çerçeve sunar. Farklı riskleri karşılaştırmak, en önemli riski belirlemek ve zaman içinde riskin nasıl değiştiğini izlemek için kullanılabilir. Olabilirlik endeksi ve etki endeksi birleştirilerek risklerin ciddiyeti ve önemi net bir şekilde belirlenebilir. Bu sayede riskler kontrollü bir şekilde yönetilebilir ve gerekli önlemler zamanında alınabilir.

Olasılık ve etki ölçeklendirilirken 5x5 yapılabileceği gibi 4x4 veya 3x3 olarak da belirlenebilmektedir. ISO 18128:2024 risk endeksini 4x4 olarak tablo halinde örneklendirmektedir. Buna göre olasılık seviyeleri; ‘1: Nadir’, ‘2: Düşük’, ‘3:Orta’, ‘4:Yüksek’ olarak belirlenmiştir. Etki seviyeleri ise; ‘1: Az’, ‘2: Orta’, ‘3:Yüksek’, ‘4: Şiddetli’ olarak tayin edilmiştir. Risk puan hesaplaması bu iki seviyenin çarpılması ile hesaplanmakta ve ortaya risk endeksi çıkmaktadır. Risk endeksinde: ‘1-2 = Düşük’; ‘3-4 = Orta’; ‘5-10 = Yüksek’; ve ‘12-16 = Aşırı’ olarak değerlendirilmektedir.

Tablo 2.13, bileşik puanlama yöntemini kullanarak riskleri değerlendirmek için bir örnek sunmaktadır. Bu tabloda, her bir risk olayı için olasılık ve etki seviyeleri belirlenmiş ve bu seviyelerin çarpılmasıyla risk puanı hesaplanmıştır. Risk puanı, risk endeksi kategorisine göre değerlendirilmiştir.

Tablo 2.13: Bileşik puanlama kullanan risk endeksi sistemi örneği

Risk OLAYI	Olasılık				Etki				Risk puanı	Risk Endeksi
	Nadir 1	Düşük 2	Orta 3	Yüksek 4	Önemsiz 1	Orta 2	Önemli 3	Şiddetli 4		
Belgeler yanlış sınıflandırılmış, yanlış erişim durumu				Yüksek - Aylık veya daha fazla	Mevcut prosedürler kapsamına kurtarılabilmektedir				4	Orta
Gizliliğin korunması			Orta -			Erişim kısıtlamaları			6	Yüksek

kanununda yapılan değişiklikler			Yıld a bir kez			nı etkiler; diğer işlemlerdeki akışı bozar				
Belge sisteminin indeksleme işlevi başarısız		Düşük - 3 yılda bir			Mevcut prosedürler kapsamında a kurtarılabilir				2	Düşük
Yanlışlıkla imha edilmek üzere belirlenen belgeler			Orta - Yıld a bir kez		Mevcut prosedürler kapsamında a telafi edilebilir				3	Orta
Personel belgelerine izinsiz erişim		Düşük - 3 yılda bir				Kurtarılamaz			4	Orta
Güç kaynaklarında 8 saat süreyle kesinti		Düşük - 3 yılda bir					Tüm belge sistemleri ni etkiler; bir günlük işlemler kaybedilir		6	Yüksek
Kişisel verileri etkileyen belge sistemine siber saldırı				Yüksek - Aylık veya daha fazla				Halkın güveninin ve belge bütünlüğünün kaybı	16	Aşırı
Yangın nedeniyle belge arşivinin yok olması	Nadir - Her 10 yılda bir							Önemli belgelerin kaybı; operasyonda kesinti; halkın güveninin kaybı	4	Orta
Kritik iş operasyonların ı etkileyen koordinasyons uz sistem bakımı			Orta - Yıld a bir kez					Kamu güveninin ve sistem üzerinde belge bütünlüğünün kaybı	12	Aşırı

Kaynak: ISO 18128, 2024, ss. 17-18

Riskleri değerlendirmek için bileşik puanlama yöntemini kullanarak bir örnek sunulan Tablo 2.13'te değerlendirilen riskler, olasılık ve etki seviyelerine göre sınıflandırılmış ve her bir risk için risk puanı ve risk endeksi belirlenmiştir. Riskler değerlendirilirken her bir riskin kuruluş için özel önemi ve potansiyel etkisi göz önünde bulundurulmalı, mevcut kontrol tedbirleri ve risk azaltma stratejileri dikkate alınmalı, farklı risklerin karşılaştırılması ve en önemli risklerin belirlenmesi için objektif bir çerçeve kullanılmalı ve risk yönetim planı düzenli olarak gözden geçirilerek güncellenmelidir.

2.1.3.4. Fayda-Maliyet Analizi

Fayda-maliyet analizi, farklı projelerin ekonomik açıdan karşılaştırılmasını sağlayan güçlü bir risk değerlendirme aracıdır. Bu teknikte, projenin ömrü boyunca yapılacak tüm harcamalar ve elde edilecek tüm faydalar, bugünkü değerlerine indirgenerek maliyet-fayda analizi hesaplanır. Bu sayede gelecekteki farklı zamanlarda gerçekleşecek parasal akışlar, bugünkü değerleri ile karşılaştırılabilir hale gelir. Karar verme sürecinde önemli bir rol oynamaktadır (Şataf, 2014, s. 108). Elektronik belge yönetimine dayalı olası riskleri değerlendirmek için de kullanılabilen fayda maliyet analizine ilişkin örnek Tablo 2.14'te verilmektedir.

Tablo 2.14: Maliyet/fayda seçenekleri analizi örneği

	<i>Seçenek 1</i>	<i>Seçenek 2</i>	<i>Seçenek 3</i>
<i>Tanım</i>	Eski bordro sistemini 20 yıl daha çalışır durumda tutun, sonra halledin.	Belgeleri yeni maaş bordrosu sistemine taşıyın.	İstihdam geçmişi raporlarının özetlerini oluşturmak ve kurum kayıt sisteminde arşivlemek için bir veri tabanı uzmanı, işe alınmalıdır.
<i>Yararlar</i>	Belgeleri, önümüzdeki 2-3 yıl boyunca en güvenilir şekilde orijinal ortamında tutun.	Belge kayıplarını ve gizlilik ihlallerini azaltın.	İstihdam geçmişi özet belgelerinin tam ve doğru olarak tutulması ve belgelerin bir belge kayıt sisteminde tutularak zaman içerisinde kullanıma sunulması.
<i>Risk değerlendirmesi</i>	Artık aktif olarak desteklenmediğinden salt okunur sistemin bozulması nedeniyle belgelerin ve verilerin tamamen kaybolması riski. Ya en katı bakım rejimi uygulanır (daha maliyetli) ya da düşük bakım uygulanarak siber saldırıya	İki sistem arasındaki üstveri şeması geçişi doğrudan bir eşleşme değildir. Yeni sisteme geçilebilmesi için eski belgelerin düzeltilmesi gerekmektedir.	Raporların orijinalliğini ve güvenilirliğini koruyacak şekilde oluşturulmasını sağlamak için, tam yetenekli ve eski bordro sistemi hakkında derinlemesine bilgi sahibi olan bir veri tabanı uzmanı gerekir.

	maruz kalma riski artar. Bu durum veri ve gizlilik ihlallerine neden olur.	Bu, eski bağlamsal veri şeması artık mevcut olmadığından istihdam özeti belgelerinin orijinallliğini tehlikeye atabilir veya bunlara zarar verebilir.	Bu aktivite mevcut koşullar altında gerçekleştirilirse risk önemli ölçüde azalır.
	Bu risk, sistemin yönetilmeden bırakıldığı yıllara bağlı olarak artar.		Veri tabanı uzmanı kaynağı, yeni bordro sisteminin benimsenmesinden önce veya hemen sonra hâlâ kullanılabilir durumdadır.
Maliyet	Eski sistemi sürdürmenin maliyeti her yıl artmaktadır.	Belgeler ve veri geçişi için proje maliyeti tek seferliktir.	Bir veri tabanı uzmanının istihdam geçmişi raporunun bir özetini oluşturmalarının maliyeti tek seferliktir ve diğerlerine nazaran daha uygundur.
	Sistem ne kadar uzun süre yönetilmezse, toplam maliyet zamanla artar.		

Kaynak: ISO 18128, 2024, s. 20

Tablo 2.14'teki maliyet-fayda analizi, incelenen üç seçenek arasında, eski bordro sistemindeki istihdam belgelerinin özetini korumak için üçüncü seçeneğin en uygun maliyet-fayda dengesini sunduğunu ortaya koymaktadır. Bu analizde belge bütünlüğü riski ve erişim kaybı gibi önemli faktörlere odaklanılarak farklı seçeneklerin maliyetleri ve faydaları karşılaştırılmaktadır. Ancak her kuruluşun özel ihtiyaçları, mevcut altyapısı ve mevzuat gereksinimleri gibi faktörler, maliyet-fayda analizinin sonuçlarını önemli ölçüde etkileyecektir (ISO 18128, 2024). Bu nedenle her kuruluş kendi özel durumuna uygun bir maliyet-fayda analizi yapmalıdır.

Risk değerlendirmesi, elektronik belge yönetimi sistemlerinin ve süreçlerinin iyileştirilmesi için büyük öneme sahiptir. Elektronik belgelerin tüm yaşam döngüsü boyunca, oluşturulmasından imhasına, uzun süreli saklanmasıyla erişilebilirliğine ve sistem tasarımıyla güvenliğine kadar birçok risk faktörü göz önünde bulundurularak analiz edilmelidir (ISO 16175-1, 2020). Bu kapsamlı analiz, sistemlerin ve süreçlerin iyileştirilmesi için önemli fırsatlar sunmaktadır.

2.2. Risk Müdahalesi (Risklerin Tedavi Edilmesi/Risk İyileştirilmesi)

Risklerin tanımlanması ve değerlendirilmesinin ardından, bu riskleri yönetmek için çeşitli seçenekler değerlendirilir ve en uygun tedavi yöntemi belirlenir. Bu süreçte amaç riskleri tamamen ortadan kaldırmak yerine, kabul edilebilir bir seviyeye indirmek veya risklerin oluşturabileceği potansiyel zararları azaltmaktır (McDowall, 2005).

Risk yönetimi, risklerle başa çıkmak için çeşitli stratejiler sunar. Bunlardan biri olan *risk azaltma*, risklerin oluşma olasılığını veya etkilerini azaltmak için önceden belirlenmiş kontrol faaliyetlerinin uygulanmasıdır (Derici vd., 2007). *Risk transferi* ise risklerin üçüncü bir tarafa devredilmesiyle (ör. sigorta yaptırmak) gerçekleşir (Paksu ve Bozdemir, 2021). *Riskle mücadele* ise, risklerin olumsuz etkilerini azaltmak için önceden ve sonrasında yapılacak faaliyetleri kapsar (Bozkurt, 2010). Son olarak *riskten kaçınma*, riskli faaliyetlerden tamamen vazgeçmeyi ifade eder ve genellikle diğer seçeneklerin mümkün olmadığı durumlarda kullanılır (TÜSİAD, 2008; Vaughan ve Vaughan, 2008). Risk yönetimi sürecinde, hangi stratejinin kullanılacağı risklerin türüne, büyüklüğüne ve kuruluşun risk toleransına göre belirlenir.

En uygun risk iyileştirme seçeneklerinin seçilmesi, amaçların gerçekleştirilmesi ile elde edilebilecek potansiyel faydaların, seçilen uygulamanın maliyeti, gerektirdiği çaba ve dezavantajları ile dengelenmesini içerir (ISO 31000, 2018b). Örneğin, elektronik belgelere yetkisiz erişim riski, kurumlar için önemli bir tehdit oluşturmaktadır. Bu riski yönetmek için genellikle dört ana yaklaşım benimsenir: Kabul etme, azaltma, devretme ve kaçınma. *Riski kabul etmek*, riskin sonuçlarının önemsiz olduğu kararının verilmesi anlamına gelir. *Riski azaltmak* ise, teknik ve organizasyonel önlemlerle riski kabul edilebilir bir seviyeye indirmeyi amaçlar. *Risk devretme*, riskin bir kısmının veya tamamının üçüncü bir tarafa aktarılmasıyla gerçekleşir. Son olarak *riskten kaçınmak*, riskin tamamen ortadan kaldırılması için faaliyetten vazgeçilmesi anlamına gelir. Her bir yaklaşımın kendine özgü avantajları ve dezavantajları bulunmaktadır. Örneğin, riski kabul etmek en basit ve en az maliyetli seçenek olsa da verilere yetkisiz erişimin sonuçları kabul edilemez olabilir. Benzer şekilde, riski azaltmak maliyetli ve karmaşık olabilirken riski devretmek kontrol kaybına yol açabilir. Dolayısıyla, hangi yaklaşımın seçileceği, riskin doğası, kurumun risk toleransı ve mevcut kaynaklar gibi faktörlere bağlı olarak değişir (DiNapoli, 2016).

Sonuç olarak risk müdahalesi, organizasyonların olası zararları en aza indirmek için sistematik bir yaklaşım benimsemesini gerektirir. Bu süreçte risklerin türü, büyüklüğü ve olasılığı dikkatlice değerlendirilerek uygun stratejiler belirlenir (Türedi ve Koban,

2016). Özellikle elektronik belgelere yetkisiz erişim riski gibi konularda, risk iştahı⁵, mevcut kaynaklar ve risklerin doğası göz önünde bulundurularak riski kabul etme, azaltma, devretme veya tamamen önleme gibi farklı stratejiler değerlendirilir.

2.3. İzleme ve Gözden Geçirme

Değişen risk ortamına ayak uydurmak için risk yönetimi programlarının da sürekli güncellenmesi ve gözden geçirilmesi gerekir. Yeni risklerin ortaya çıkması ve eski risklerin ortadan kalkması, geçmişte uygun olan çözümlerin günümüzde de yeterli olmayabileceği anlamına gelir. Bu nedenle risk yönetimi programının düzenli olarak gözden geçirilmesi ve izlenmesi, olası felaketlerin önlenmesine yardımcı olur. Gözden geçirme süreci, geçmiş risk değerlendirmelerinin ve uygulama seviyelerinin güncelliğini ve geçerliğini sorgulamayı içerir. Bu sayede risk yönetimi sürecinin her adımı, değişen koşullara ve yeni tehditlere karşı kontrollü biçimde ele alınacaktır. Düzenli risk yönetimi gözden geçirmeleri ve izleme faaliyetleri, kuruluşların değişen risk ortamına ayak uydurmasına ve olası tehditlere karşı kontrollü bir şekilde korunmasına yardımcı olur (Vaughan ve Vaughan, 2008, ss. 30-31).

Risk yönetimi programlarının gözden geçirilmesi ve izlenmesi, risk yönetim politikalarına ve ilkelerine uygun süreçlerin iyileştirilmesini ve sürdürülebilirliğini sağlamayı amaçlar. Bu sayede risk yönetimi faaliyetlerinin etkinliği ve verimliliği denetlenirken risk yönetim politikalarıyla uyumlu olmayan veya fayda sağlamayan eylemlerin ve tedbirlerin belirlenmesi sağlanır (Usta, 2018, s. 109).

Etkin bir risk yönetimi programı, risklerin doğru şekilde tanımlanması ve ele alınması için gereklidir. Bunu başarmak için uygun kontrol ve yanıt mekanizmalarının uygulanması ve bunların etkinliğinin izlenmesi ve gözden geçirilmesi için bir yapıya ihtiyaç duyulur. Bu yapı, politika ve standartların düzenli olarak gözden geçirilmesini ve performanslarının değerlendirilmesini içermelidir. Bu sayede ilerleme fırsatları belirlenebilir ve gerekli iyileştirmeler yapılabilir. Kuruluşların dinamik olduğu ve değişen ortamlarda faaliyet gösterdiği unutulmamalıdır. Bu nedenle kontrollü bir risk yönetimi yaklaşımı benimsemek ve riskleri kontrollü biçimde yönetmek son derece

⁵ Bir kuruluşun stratejik hedeflerine ulaşmak amacıyla kabul edebileceği risk düzeyini ifade etmektedir. Kurumsal risk yönetiminin temel unsurlarından biri olan bu kavram, risk ile getiri arasındaki dengeyi yansıtmaktadır. Üst yönetim tarafından belirlenmekte ve kuruluşun genel stratejisiyle uyumlu olması beklenmektedir (Hazine ve Maliye Bakanlığı, 2024, s.30).

önemlidir. İzleme ve gözden geçirme süreçleri, bu yaklaşımın temelini oluşturmaktadır. Bu süreçler kapsamında kuruluştaki değişiklikler ve faaliyet gösterilen ortam belirlenmeli ve buna göre gerekli düzenlemeler yapılmalıdır. İzleme ve gözden geçirme faaliyetleri, kullanılan kontrollerin kuruluşun faaliyetlerine uygunluğunu, prosedürlerin anlaşılmış olduğunu ve takip edildiğini teyit etmelidir. Bu süreçler uygulanan ölçülerin istenilen sonuçları sağlayıp sağlamadığını, kullanılan prosedürlerin ve toplanan bilgilerin uygunluğunu, geliştirilen bilginin daha iyi kararlar alınmasına yardımcı olup olmadığını, gelecekteki değerlendirmeler ve risk yönetimi çalışmaları için hangi derslerin çıkarılabileceğini belirlemede de önemli rol oynamaktadır (Federation of European Risk Management Associations, 2003, s. 14).

Değişen koşulların risk önceliklerini veya risk azaltma stratejilerini etkilememesi için belge yönetimiyle ilgili risklerin düzenli olarak izlenmesi ve gözden geçirilmesi hayati önem taşımaktadır. Tanımlanan riskler ele alındıkça ve kontroller iyileştirildikçe veya geliştirilip uygulandıkça belge yönetimi risklerinin bağlamı da değişecektir. İzleme ve gözden geçirme sürecinin başarılı olması için birtakım yöntemler belirlenmekte ve buna yönelik faaliyet alanları oluşturulmaktadır. Public Record Office Victoria (2010), belge yönetimi risklerini etkin bir şekilde yönetmek için kapsamlı bir yaklaşım sunmaktadır. Bu yaklaşım, sürekli izleme, değerlendirmeler, dış denetimler ve öz değerlendirmeler gibi çeşitli yöntemleri içerir. *Sürekli izleme*, mevcut ve potansiyel risklerin düzenli olarak takip edilmesini sağlarken *değerlendirmeler* ve *denetimler* ise risklerin belirlenmesi ve değerlendirilmesi için kullanılır. *Dış denetimler*, kurum dışındaki uzmanların bakış açısıyla riskleri değerlendirmeye yardımcı olur. Bu yöntemler sayesinde, kurumlar belge yönetimi uygulamalarının etkinliğini sürekli olarak iyileştirebilirler. Belge yönetimi risklerini etkin bir şekilde yönetmek için tetikleyici olayların takibi, paydaşların aktif katılımı, düzenli iç ve dış denetimler, risk yönetimi çerçevesinin periyodik gözden geçirilmesi, öz değerlendirmelerin yapılması ve detaylı raporlama gibi çeşitli faaliyetler gerçekleştirilir. Bu faaliyetler sayesinde, potansiyel riskler önceden tespit edilir, değerlendirilir ve uygun önlemler alınarak belge yönetimi süreçlerindeki riskler asgari düzeye indirilir. Böylece kurumlar, yasal uyumluluğu sağlarken veri güvenliğini koruyarak ve iş sürekliliğini destekleyerek rekabet avantajı elde ederler.

Risk yönetimi kontrollü bir şekilde idare edilmesi gereken bir süreç olsa da her zaman beklenmedik olaylar yaşanabilir. Bu gibi durumlarda kuruluşların hızlı ve etkili bir şekilde yanıt vermesi ve riskin etkisini en aza indirmesi önemlidir. Tanımlanan bir riskin gerçekleşen bir olaya dönüşmesi durumunda olay, risk sahibi (yani iş birimi yöneticisi) tarafından incelenmeli ve ‘Riskin gerçekleşmesine neyin yol açtığı’, ‘Olayın tekrarlanmasını önlemek için beklenebilecek uyarı işaretlerinin olup olmadığı’, ‘Daha önce riske uygulanan derecelendirmelerin değerlendirilmesi’ konularına odaklanılmalıdır.

Risk yönetimi programlarının etkinliğini ve verimliliğini artırmak için inceleme sonuçlarının sistematik bir şekilde analiz edilmesi ve bu sonuçlara dayalı iyileştirmelerin yapılması gerekmektedir. Bu analizler risklerin güncelliğini, risk yönetim planlarının yeterliliğini ve kontrol mekanizmalarının etkinliğini değerlendirerek risk yönetimi süreçlerinin sürekli iyileştirilmesine katkı sağlar. İnceleme sonuçları, risk yönetimi çerçevesi kapsamında şu şekilde değerlendirilebilir:

- *Risk kategorilerinin revizyonu:* Sonuçlar, mevcut risk kategorilerinin güncelliğini ve kapsamını değerlendirmek için kullanılabilir. Gerekirse yeni risk kategorileri eklenebilir veya mevcut kategoriler yeniden tanımlanabilir.
- *Risk derecelendirmelerinin güncellenmesi:* Bulgular, risklerin olasılık ve etki değerlendirmelerinin doğruluğunu teyit etmek için kullanılabilir. Gerekirse risk derecelendirmeleri güncellenebilir.
- *Tedavi seçeneklerinin ayarlanması:* Sonuçlar mevcut risk tedbirlerinin etkinliğini değerlendirmek ve gerekirse yeni veya güncellenmiş tedbirler geliştirmek için kullanılabilir.
- *Sistemlerin ve raporlama mekanizmalarının geliştirilmesi:* Bulgular, risk yönetimi sistemlerinin ve raporlama mekanizmalarının eksikliklerini belirlemek ve gerekli iyileştirmeleri yapmak için kullanılabilir.
- *Yeni veya güncellenmiş prosedürler ve süreçler:* Sonuçlar, risk yönetimi ile ilgili prosedürlerin ve süreçlerin güncelliğini ve etkinliğini değerlendirmek ve gerekirse yeni veya güncellenmiş prosedürler geliştirmek için kullanılabilir.

2.4. İletişim ve Danışma

Risk yönetimi sürecinin başarısı için etkili bir iletişim ve danışma stratejisinin geliştirilmesi önemli görülmektedir. Bu strateji çerçevesinde, risk farkındalığını ve anlayışı artırmaya odaklanan iletişim, paydaşlara risklerin doğası, potansiyel etkileri ve olası sonuçları hakkında bilgi sunarak şeffaflığı ve katılımı teşvik etmektedir. Danışma ise farklı uzmanlık alanlarından gelen paydaşların görüşlerini toplayarak risk kriterlerinin belirlenmesi ve değerlendirilmesinde çeşitli bakış açılarının dikkate alınmasını sağlar. Bu sayede daha kapsamlı ve sağlam bir risk analizi gerçekleştirilebilir ve risklerin kontrollü bir biçimde yönetilmesine imkân tanınır (ISO 31000, 2018b).

Risk yönetimi sürecinde etkin bir iletişim ve danışma stratejisi benimsemek, kuruma birçok açıdan fayda sağlar. Bu sayede risk gözetimi ve karar verme kolaylaşır, paydaşlar arasında sahiplenme ve müdahil olma duygusu oluşur, şeffaflık ve katılım artar. Yeterli bilgi akışı sayesinde riskler sağlıklı bir şekilde yönetilebilir ve bilinçli kararlar alınabilir. Risk yönetimi sürecine aktif olarak katılan paydaşlar, risklerin kontrol altına alınmasına daha fazla katkıda bulunur. Açık ve şeffaf bir iletişim ise tüm paydaşların risk yönetimi sürecine güvenmesini ve katkıda bulunmasını sağlayarak genel bir risk yönetimi başarısı elde edilmesine yardımcı olur (TÜSİAD, 2008, s. 64).

Başarılı bir iletişim ve danışma stratejisi için uygulanması gerekenleri literatürden elde edilen bilgiler ışığında şu şekilde açıklamak mümkündür (Hazine ve Maliye Bakanlığı, 2024, s. 82; ISO 31000, 2018b, s. 9; TÜSİAD, 2008, s. 64):

Rol ve sorumluluklar: Risk yönetimi sürecindeki her paydaşın rolü ve sorumluluğu açıkça tanımlanmalı ve görev tanımlarına işlenmelidir.

İletişim planı: Kurum içi ve kurum dışı paydaşlarla iletişimi düzenleyen bir plan oluşturulmalı ve bu plan riskler ve risk yönetimi süreciyle ilgili tüm dikkate değer konuları kapsamalıdır.

Karşılıklı diyalog ve takım çalışması: Tek yönlü bilgilendirmeden ziyade karar alıcılar ve menfaat sahipleri arasında karşılıklı bir diyalog ortamı teşvik edilmelidir. Farklı bakış açılarının risk analizine dâhil edilmesi ve değerlendirilmesi önemlidir.

Geri bildirim ve iyileştirme: İletişim ve danışma faaliyetlerinin kayıt altına alınması ve karar alma sürecine entegre edilmesi, paydaşların geri bildirimlerinin toplanmasına ve risk yönetimi sürecinde gerekli iyileştirmelerin yapılmasına olanak sağlar.

Etkili bir iletişim ve danışma stratejisi, risk yönetimi sürecinin temelini oluşturur ve paydaşların katılımını, şeffaflığı ve bilinçli karar vermeyi teşvik ederek kuruluşun riskler üzerinde kontrol sağlamasına, yönetmesine ve hedeflerine ulaşmasına yardımcı olur.

2.5. Kaydetme ve Raporlama

Kuruluşlar, ISO 31000 standardına uygun olarak risk yönetimi süreçlerini ve sonuçlarını belgelemeli ve raporlamalıdır. Bu sayede tüm paydaşlar bilgilendirilerek karar verme süreçleri desteklenir, sistem sürekli iyileştirilir ve risklerden sorumlu olanlarla etkileşim artırılır. Böylece risk yönetimi sisteminin etkinliği artırılarak kurumsal hedeflere ulaşmada önemli bir rol oynar (ISO 31000, 2018b, ss. 14-15).

Risklerin sistematik olarak takip edilmesi, risk kültürünü yaygınlaştırmak, risk sahiplerini güçlendirmek ve veriye dayalı kararlar almak için etkili bir risk kaydetme ve raporlama yapısının kurulması gerekmektedir (Hazine ve Maliye Bakanlığı, 2024, s.75). Her türlü belge ve kayıt, doğru zamanda anlaşılır bir şekilde hazırlanmalıdır. Belgeler, doğrulama için gerekli teknik derinliği ve değerlendirmenin ileride kullanılabilmesi için yeterli ayrıntıyı sunmalıdır. Bilgiler hem süreçlerin izlenmesini hem de sonuçların değerlendirilmesini ve doğrulanmasını sağlayacak kadar kapsamlı olmalıdır. Varsayımlar, veri veya yöntemdeki sınırlamalar ve önerilerin gerekçeleri açıkça belirtilmelidir. Riskler açık bir şekilde ifade edilmeli, net ve doğru olmalıdır. Sonuçların doğruluğu ve güvenilirliği, sunum yapanların kendi yetkinlikleri ve ekiplerinin uzmanlığına olan güvenleriyle doğrudan ilişkilidir. Belirsizlikler, istatistiksel anlamlılık veya güven aralıkları gibi uygun yöntemlerle ifade edilmelidir (United Nations Development Programme, 2023, ss. 78-79).

Bu süreçte raporlamadan elde edilen veriler, sadece bir sonraki risk belirleme sürecinin girdilerini oluşturmakla kalmayacak aynı zamanda risk yönetimi döngüsünü de besleyecek bir geri bildirim mekanizması görevi görecektir. Her raporlama döngüsü, geçmişte alınan önlemlerin riskleri ne kadar azalttığını, yeni risklerin ortaya çıkıp çıkmadığını ve mevcut risklerin nasıl değiştiğini anlamamızı sağlayarak risk profilinin

sürekli güncellenmesine ve iyileştirilmesine katkıda bulunacaktır. Bu sayede risk yönetimi kontrollü ve dinamik bir hale gelerek, kuruluşun hedeflerine ulaşmasını engelleyebilecek tehditlere karşı her zaman hazırlıklı olmasını sağlayacaktır (İnce, 2019, ss. 290-291).

Riskleri azaltmak hatta yok etmek için süreçler adım adım takip edilmelidir. Her bir aşamada olduğu gibi bu süreçte de üst yöneticinin desteği oldukça önemlidir. Üst yöneticinin kurumsal risk yönetimine bakış açısı ve desteği, yöneticilerin ve çalışanların bu konuya verdiği önemi doğrudan etkiler. Bu nedenle üst düzey yönetimin aktif katılımı ve desteği, risk yönetimi sürecinin başarısını etkiler. Üst yönetici, risk yönetimi sürecinin liderliğini üstlenmeli ve tüm paydaşların bu konudaki sorumluluklarını açıkça tanımlamalıdır. Ayrıca risk yönetimi faaliyetlerinin yürütülmesi için gerekli kaynakları tahsis etmeli ve şeffaf bir iletişim ve raporlama yapısı oluşturmalıdır. Bu yapı kurumda bir risk kültürü oluşturmaya yardımcı olur. Bu sayede tüm çalışanlar risklerin farkında olur ve bu riskleri azaltmak için gerekli adımları atar (United Nations Development Programme, 2023, s. 76).

3. BULGULAR

Çalışmanın bu bölümünde, araştırmanın amaçları doğrultusunda yürütülen iki farklı veri toplama sürecinden elde edilen verilerin analizine yer verilmiştir. Bu doğrultuda ilk aşamada EBYS’de risk yönetimini açıklayan gelişmiş bir eğitim materyalinin ortaya çıkarılabilmesi ve ülkemizde risk yönetimine ilişkin genel durumun anlaşılabilmesi için kurumlar, uzmanlar/akademisyenler ve EBYS yazılımı geliştiren firma temsilcileriyle gerçekleştirilen görüşmelerden derlenen veriler analiz edilmiştir. İkinci aşamada ise hazırlanan eğitim materyalinin etkililiğini ölçmek amacıyla, ÇAKÜ’de görev yapan yazışma personeline (sekreterlere) verilen eğitimin etkisini saptayabilmek amacıyla yapılan ön-son test sonuçlarına ilişkin veriler değerlendirilmiştir.

Analizlere geçmeden önce eğitim materyalinin geliştirilmesi ve ülkemizde risk yönetimi uygulamalarının saptanması amacıyla gerçekleştirilen görüşmelerden elde edilen verilerin analiz süreci açıklanmıştır.

3.1. Risk Yönetimi Süreçlerinde Karşılaşılan Temel Sorunlara İlişkin Elde Edilen Verilerin Analize Hazırlanması

EBYS’de risk yönetimi eğitim materyalinin geliştirilmesi ve ülkemizdeki genel durumun anlaşılabilmesi için kurumlar, uzmanlar/akademisyenler ve EBYS yazılımı geliştiren tedarikçi firma temsilcileriyle yapılan görüşmelerden elde edilen verilerin analize hazırlık süreci bu başlık altında detaylı olarak açıklanmıştır.

Araştırma kapsamında yapılan görüşmeler yüz yüze ve çevrim içi ortamda (Zoom ve Microsoft Teams) gerçekleştirilmiştir. Çevrimiçi görüşmelerde tutulan kayıtlar, Microsoft Word yazılımı aracılığıyla otomatik olarak metne çevrilmiştir. Yüz yüze gerçekleştirilen görüşmelerde ise katılımcıların izni alınarak yapılan kayıtlar 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.

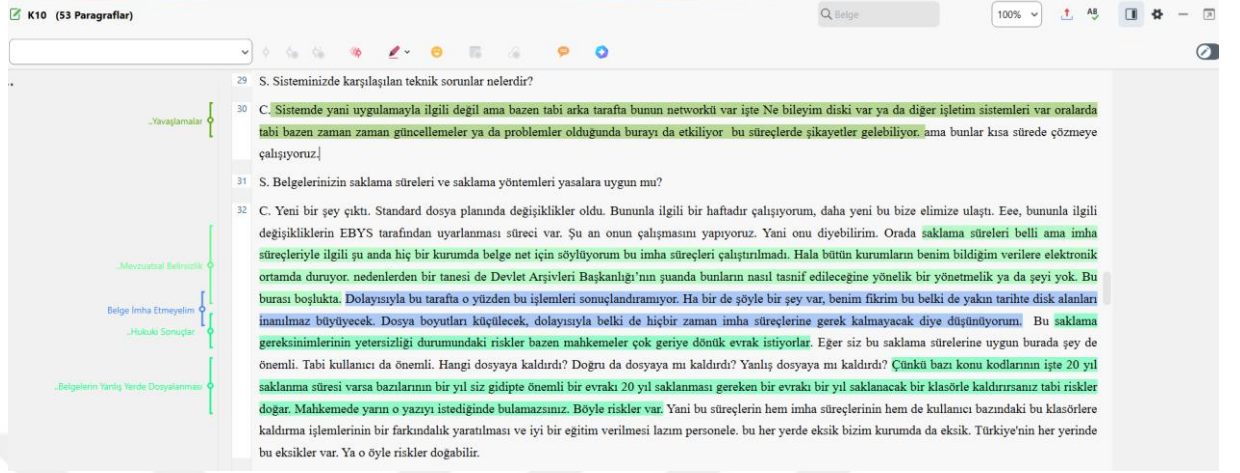
Bu kayıtlardan elde edilen belgeler, görüşme yapılan grupların özelliklerine göre (kamu kurumları, uzmanlar/akademisyenler, firma temsilcileri) kategorilere ayrılmış

ve MaxQDA 2024 yazılımına “belge grubu” formatında aktarılmıştır. Kodlamaya geçmeden önce belgeler tekrar gözden geçirilmiş, içerik bütünlüğünün ve doğruluğunun teyit edilmesi amacıyla ses kayıtlarıyla karşılaştırılmıştır. Böylece metin analizi için hazır duruma getirilen görüşmelerden toplam 253 sayfadan oluşan kapsamlı bir nitel veri kümesi elde 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, Huberman ve Saldaña, 2014, s. 79). Kodlama aynı zamanda verilerin analize uygun hale getirilmesinde de önemli bir rol oynar. Kodlama süreci araştırmacının elde ettiği metinleri dikkatle incelemesiyle başlar. Bu süreçte metinlerin içerikleri anlamlı ve kavramsal parçalara ayrılır. Bu parçalar tek bir kelime, bir cümle, bir paragraf ya da daha geniş veri bloklarından oluşabilir. Her bir anlam birimi, kendi içerisinde tutarlı olduğu ölçüde bir ‘kod’ olarak tanımlanmakta ve araştırmacı tarafından uygun ifadelerle etiketlenmektedir. Kodlama, basit bir teknik işlemde daha çok analitik düşünme, kavramsallaştırma ve yorumlama becerilerini gerektiren bilişsel bir etkinliktir. Verilerin sistematik analizi ve doğru yorumlanması ancak kodlar arasında tutarlılık sağlandığında mümkün olmaktadır. Bu bağlamda kodlama, verilerin sınıflandırılması, tematik desenlerin belirlenmesi ve ilişkili kavramların açığa çıkarılması için önemli bir analitik çerçeve sağlamaktadır (Yıldırım ve Şimşek, 2018, s. 228).

Bu çalışma kapsamında elde edilen 253 sayfalık veri kümesi araştırmanın amaçları doğrultusunda analiz edilebilir ve karşılaştırılabilir bir yapıya kavuşturulmak üzere MaxQDA 2024 yazılımı aracılığıyla kodlanmıştır. Kodlama sürecine geçilmeden önce, görüşme metinleri dikkatle incelenmiş, içeriklerin doğruluğu ses kayıtlarıyla yeniden karşılaştırılarak teyit edilmiştir. Ardından veri analizinin ilk aşaması olan kodlama süreci başlatılmıştır. Bu süreçte 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 (bkz. Şekil 3.1).

Şekil 3.1: MaxQDA kodlama

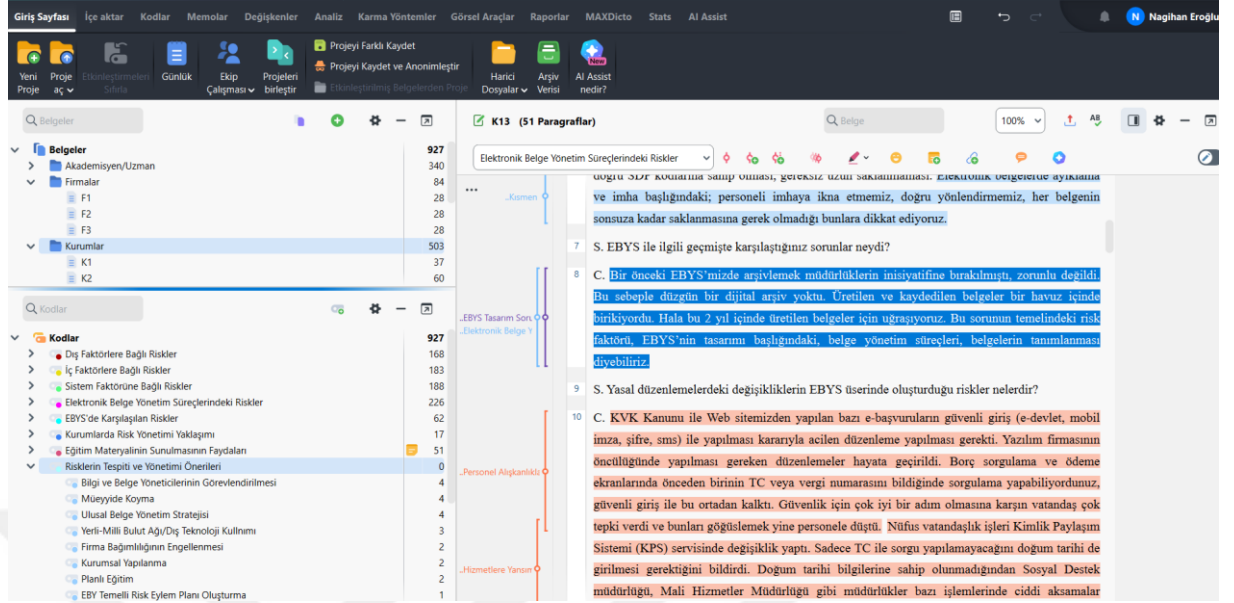


Metin üzerinde gerçekleştirilen kodlama sürecine ilişkin bir örnek Şekil 3.1’de sunulmuştur. Bu aşamada katılımcılara yöneltilen görüşme sorularına verilen yanıtlar analiz edilmiştir. Burada her bir yanıt, içerdiği anlamlara göre tanımlayıcı kodlarla etiketlenmiştir. Kodlama süreci yürütülürken metinler tekrar tekrar okunmuş ve bu okumalar sırasında saptanan yazım/anlam hataları düzeltilmiştir. Ayrıca gerektiğinde yeni kodlar oluşturulmuş ya da mevcut kodlarda düzenlemelere gidilmiştir. Bu sayede kodların içerikle uyumlu ve kavramsal olarak tutarlı olması sağlanmıştır.

Kodlama sürecinin ardından nitel veri analizinin ikinci aşaması olan tema oluşturmaya 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.

MaxQDA yazılımı aracılığıyla oluşturulan kod sistemine ait temalar ve bu temaların altında gruplandırılmış kodlar Şekil 3.2’de sunulmaktadır. 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.

Şekil 3.2: MaxQDA kod sistemi



Tüm kodlama işlemlerinin tamamlanmasının ardından MaxQDA yazılımının ‘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 aşaması ise ‘anonimleştirme’ olmuştur. Bu aşamada 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.

Yapılan analizler sonucunda risk unsurları (1 dış faktörlere bağlı riskler, 2 iç faktörlere bağlı riskler, 3 sisteme özgü yapısal riskler, 4 belge yönetim süreçlerine ilişkin riskler) dört ana başlık altında toplanmıştır. Bunların yanı sıra katılımcıların geçmiş deneyimlerinden ve bilgi birikimlerinden yola çıkarak yaşanmış risk örnekleri ve

mevcut risk yönetimi uygulamaları konularında da bulgulara ulaşılmıştır. Bunlar ilgili temalar altında tablolar halinde sunularak katılımcı ifadelerinden alınan alıntılarla somutlaştırılmıştır. Böylece bir taraftan ülkemizdeki uygulamalarda ortaya çıkan risk unsurları gerçek deneyimlere dayandırılmış diğer taraftan da eğitim materyalinin geliştirilmesine katkı sağlanmıştır.

3.2. Risk Yönetimi Süreçlerinde Karşılaşılan Temel Sorunlara İlişkin Bulgular

EBYS’de risk yönetimi kapsamında kurum ve kuruluşlarda karşılaşılan ya da karşılaşılabilecek risk unsurlarını belirlemeye yönelik yürütülen nitel araştırmanın bulguları bu başlık altında sunulmuştur. Araştırma kapsamında 13 farklı kurumdan EBYS temsilcileri, sekiz akademisyen/uzman ve üç EBYS firma yetkilisi ile görüşmeler gerçekleştirilmiştir. Elde edilen nitel veriler MaxQDA yazılımı kullanılarak analiz edilmiş, tematik analiz yöntemiyle kodlanmış ve belirli ana temalar altında sınıflandırılmıştır.

3.2.1. EBYS Kapsamında Risk Unsurlarının Tematik Dağılımı

EBYS’deki risk unsurlarının tematik analizi sonucunda elde edilen bulgular bu başlık altında yer almaktadır. Bu kısımda görüşmelerden elde edilen veriler doğrultusunda riskler dış faktörlere, iç faktörlere, sistem faktörüne ve belge yönetim süreçlerine bağlı olmak üzere dört ana tema altında gruplandırılmıştır. Her bir tema katılımcı ifadeleriyle desteklenerek açıklanmıştır. Dolayısıyla sistematik olarak değerlendirilen bu temalar, EBYS süreçlerindeki risklerin kapsamlı bir şekilde anlaşılmasını sağlamıştır.

3.2.1.1. Dış Faktörlere Bağlı Riskler

Doğal afetler, siber saldırılar, ekonomik krizler gibi beklenmedik olayların oluşturduğu riskler dış faktörlere bağlı riskler kategorisindedir. Ayrıca hükümet politikaları, yasal düzenlemeler ve yeni teknolojinin beraberinde getirdiği riskler de bu temada yer almaktadır. Kısacası sistem dışında gelişmesine rağmen EBYS’yi etkileyen faktörler bu kategoride değerlendirilmektedir.

3.2.1.1.1. Beklenmedik Olayların Oluşturduğu Riskler

Beklenmedik olaylar, umulmadık zamanda gerçekleşerek geniş etki alanı oluşturmaktadır. Ayrıca büyük bir belirsizlik yaratarak pek çok riski meydana getirebilmektedir.

Kurum ve kuruluşlarda yapılan işlerin yönetilmesi ve faaliyetlerin devamlılığının sağlanmasında EBYS'ler son derece önemlidir. Ancak beklenmedik olaylar bu sistemlerin, dolayısıyla da iş süreçlerinin sürdürülebilirliğine zarar verebilir. Tablo 3.1'de beklenmedik olaylar sonucu ortaya çıkabilecek riskleri tetikleyen etmenlere ilişkin katılımcı görüşlerine yer verilmektedir:

Tablo 3.1: Beklenmedik olaylara bağlı risk tetikleyicileri

<i>Risk (N=30)</i>	<i>Katılımcılar</i>
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

Tablo 3.1 incelendiğinde, beklenmedik olayların meydana getireceği risk etmenleri hususunda katılımcıların 14'ünün önlem eksikliği, 9'unun ekonomik krizler ve 7'sinin bilgi eksikliğini belirttiği görülmektedir. En yaygın risk kategorisinin önlem eksikliği olduğu anlaşılmaktadır.

Katılımcılardan AU7, önlem eksikliğine yönelik görüşlerini kapsamlı biçimde açıklamıştır. Katılımcı, özellikle doğal afetlerle ilgili risk planlamasında temel prensibin “birden fazla kopya riskleri engeller” yaklaşımı olduğunu ve buna göre verinin tek bir lokasyonda değil, farklı coğrafi bölgelerde ve çeşitli afet risklerine göre korunaklı alanlarda tutulması gerektiğini vurgulamıştır. AU7'ye göre, örneğin sel riski yüksek olan Bartın'da verilerin yedeği sel ve deprem riski düşük başka bir bölgeye taşınmalı, deprem riski yüksek yerlerde ise deprem riski düşük alanlarda fiziksel yedekleme tercih edilmelidir. 6 Şubat 2023 tarihinde Maraş'ta meydana gelen deprem sonrası birçok kurumun Ankara'da güvenli alanlarda sunucu ve disklerini barındırdığını belirten AU7, bu önlemlerin felaket gelmeden önce alınmasının gerekli olduğunu ve doğal afet türüne göre risklerin kabul edilip edilmeyeceğinin belirlenerek yedekleme stratejilerinin oluşturulması gerektiğini ifade etmiştir.

Katılımcılardan AU4 ise önlem eksikliğini siber saldırılar ve doğal afetler açısından ele almış ve bu durumu “*Siber saldırı riski hep vardı ve olacaktır da. Bunun ancak ulusal düzeyde alınacak güvenlik önlemleriyle çözebiliriz. Kurumlar ise alınan önlemlere ve stratejilere uygun hareket etmelidir. Doğal afetler dediğimiz durum ise Türkiye'nin acı gerçeği. Biliyorsunuz ülkemiz deprem riski yüksek bir ülke. Böyle*

ülkelerin veri güvenliğini, yedekleme ünitelerini ve güvenliğini sağlaması gerekir. Uygulamalı senaryolar geliştirilmeli, felaket kurtarma planları yapılmalı, eğitimler verilmelidir. Hatta olağanüstü hâl eğitimleri bir defa değil düzenli olarak verilmeli ki personel de bu duruma hazır hale gelsin.” şeklinde açıklamıştır.

Tabloda öne çıkan diğer risk unsurunu ekonomik krizler oluşturmaktadır. Katılımcılar bu durumun doğrudan sistemin sürdürülebilirliğini riske atacağını vurgulamıştır. AU7 riski şöyle özetlemektedir:

“Ekonomik krizler, sahip olduğumuz teknolojik koşulların devam ettirilmemesi gibi bir riske sebep oluyor. Bu duruma kurum ne kadar çözüm getirebilir ciddi bir mesele. Öncelikle bazı firmalar bakım sözleşmesi yapmayabilir ya da bakım sözleşmesinin içeriğini düşürebilir. Aldığı anlık yedeklemelerde sayıyı azaltabilir veya teknolojiyi yenileyemez böyle risklere de sebep olabilir.”

Bilgi eksikliği riskine yönelik katılımcılar, özellikle siber saldırılara karşı yetersiz bilgi ve farkındalık düzeyine dikkat çekmiştir. Bununla birlikte EBYS kullanıcılarının siber saldırılara karşı savunmasız olabileceğine ve özellikle oltalama (phishing) gibi tehditlere karşı personelin farkındalık düzeyinin artırılması gerektiğini vurgulamıştır. Şifre paylaşımı ve cihaz güvenliği gibi temel zafiyetlerin farkındalık eğitimleriyle azaltılabileceğine değinen katılımcılar teknik tedbirlerin bilgi işlem birimleri tarafından yürütülmesi gerektiğini ifade etmiştir.

Beklenmedik olayların ortaya çıkması, EBY sistem ve süreçlerinde riskler meydana getirmektedir. Bu risklere ilişkin katılımcı görüşleri Tablo 3.2’de sunulmaktadır:

Tablo 3.2: Beklenmedik olaylar sonucu ortaya çıkabilecek riskler

<i>Risk (N=39)</i>	<i>Katılımcılar</i>
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
Erişilebilirlik (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
Maliyetin Artması (N=2)	AU1, F1

Personelin Farkındalık Eksikliği (N=2)	AU1, AU3
Hak Kaybı/Mağduriyet (N=1)	K7

Tablo 3.2'ye göre beklenmedik olayların sonucunda meydana gelebilecek 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 erişilebilirlik (N=3) ve verilerin bozulması (N=3) faktörlerinin de EBY sistem ve süreçlerini tehdit eden önemli unsurlar olduğu gözlemlenmektedir.

Beklenmedik olayların oluşturduğu riskler arasında en çok vurgulanan unsur olan veri kaybı riskini katılımcılardan F1; *“Doğal afetler için bütün kurumların yedekli çalışması gerekir. Herhangi bir afet durumunda ODM (Olağanüstü Durum Merkezi) kurulumunun daha önce yapılmış ve hazırlanmış olması önemlidir. ODM ile mevcut sistemin bir nevi replikası oluşturularak ağ ya da disk sorunlarında işleyiş kaldığı yerden devam edecektir. Burada sistem yedeğinin eş zamanlı olarak tutulması önemlidir. Bunlar yapılmazsa veri kaybı, hizmet kesintisi, maliyet kaybı gibi birçok riskler karşılaşılabılır.”* şeklinde açıklamıştır. Bir diğer katılımcı olan F3, felaket kurtarma merkezlerinin (FKM) yokluğunda tüm verilerin kaybolma riskinin yüksek olduğunu belirtirken K4, veri depolama cihazlarının standartlara uygun yedekleme mekanizmalarına sahip olmamasına dikkat çekmiştir. Ayrıca yedekleme mekanizması, felaket kurtarma merkezleri gibi yapılanmaların eksikliğinin ciddi veri kayıplarına neden olabileceğinin altını çizmiştir. AU5, felaket kurtarma merkezlerinin ve yedekleme sistemlerinin eksikliğinin, doğal afetler gibi beklenmedik durumlarda veri kaybına yol açabileceğini ve tüm verilerin yok olabileceğine değinmiştir. Bu ifadeler, veri kaybı riskinin önlenmesi için yedekleme sistemlerinin ve felaket kurtarma merkezlerinin ne denli önemli olduğunu göstermektedir.

Tabloda dikkat çeken risklerden biri olan veri güvenliğini AU5 şu şekilde açıklamaktadır: *“Kırılmayacak sistem yoktur. Dolayısıyla bir yerde siber saldırı gerçekleşiyorsa, bu sadece veri ele geçirme değil, aynı zamanda veriyi bozma amacıyla da yapılabilir. Bu nedenle standartların eksiksiz ve tam anlamıyla uygulanması zorunludur. Burada kastettiğim, sadece kâğıt üzerinde ‘bunları yaptık’ demek değil; uygulamada gerçek anlamda tam güvenliğin sağlanmasıdır. Örneğin, geçtiğimiz aylarda e-devlet, Hepsiburada veya Yemeksepeti gibi platformlarda*

kullanıcı verilerinin çalındığı haberlerini okuduk. Bir kez veri sızdığında ne kadar önlem alınırsa alınsın, veri zaten kaybolmuş olur ve bu durum çok büyük bir risk teşkil eder.”

Güvenlik riski konusunda katılımcılardan AU7, dış saldırılara karşı belge sayısallaştırma ve tarama süreçlerinde dış ağ erişiminin sınırlandırılmasının önemli bir tedbir olduğunu, ancak bunun kurumun risk iştahına bağlı olduğunu belirtmiştir. Kurumların öncelikle kendi risk toleranslarını belirleyip buna uygun sistem tasarımı yapmaları gerektiğine dikkat çekmiş ve siber güvenlik önlemlerinin de buna göre değerlendirilmesinin önemli olduğunu ifade etmiştir. Türkiye’de yeni kurulan Siber Güvenlik Başkanlığının görevlerinin önemine ve Avrupa Birliği’nin siber güvenlik direktiflerinin yakından takip edilmesinin gerekliliğine vurgu yapan AU7, uluslararası düzenlemelere uyum sağlama taahhüdü kapsamında kurumların hazırlıklı olması gerektiğini savunmuştur. Önlemler konusunda sorumluluğun yalnızca Devlet Arşivleri Başkanlığına bırakılmaması, kurumların da talepkâr olmasının önemine dikkat çekmiştir.

3.2.1.1.2. Yasal Düzenlemeler ve Politik Riskler

EBYS’ler, yasal mevzuat ve hükümet politikaları çerçevesinde şekillenen kurumsal yapılarıdır. Bu nedenle yürürlükteki yasal düzenlemelerdeki değişiklikler veya hükümet politikalarındaki yön değişimleri, sistemin işleyişini doğrudan etkileyebilecek riskler doğurabilmektedir. Hükümet politikaları ve yasal düzenlemelerdeki değişikliklerin, eksikliklerin ve sorunların ortaya çıkarabileceği risklere ilişkin katılımcı görüşleri Tablo 3.3’te gösterilmektedir:

Tablo 3.3: Hükümet politikaları ve yasal düzenlemelerin oluşturabileceği riskler

<i>Risk (N=43)</i>	<i>Katılımcılar</i>
Personel Alışkanlıkları/Uyum Sorunu (N=9)	AU5, AU6, F1, K1, K5, K8, K10, K12, K13
Sistemin Uyum Sorunu (N=6)	AU1, AU4, F3, K1, K6, K10
Mevzuat Eksikliği/Belirsizliği (N=5)	AU1, AU8, K7, K9, K10
Hizmetlere Yansımaları (N=3)	AU1, AU7, K13
İş Yüğü (N=3)	K1, K2, K10
Belge Sürekliliğinin Sağlanamaması (N=2)	AU7, AU8
Kurumsal Hazırlık Eksikliği (N=2)	AU7, AU8
Belge Güvenliği (N=1)	AU2

Belgenin Delil Değerini Kaybetmesi (N=1)	K3
Bilgilendirme Eksikliği (N=1)	K10
Erişim (N=1)	K4
Maliyet (N=1)	AU4
Personel/Sistem Değişikliği (N=1)	K11
Planlama Eksikliği (N=1)	AU1
Sistemin Yeniden Yapılanması (N=1)	F3
Standartlaşmama (N=1)	F3
Teknoloji Üretimi (N=1)	AU3
Uygulama ve Denetleme Eksikliği (N=1)	AU3
Uzman Personel Eksikliği (N=1)	AU8
Yazılımcıların Bilgi Eksikliği (N=1)	AU4

Tablo 3.3'te yer alan veriler incelendiğinde, 9 katılımcının personel alışkanlıkları/uyum sorununa dikkat çektiği görülmektedir. 6 katılımcının sistemde uyum sorunları yaşanabileceğine dikkat çektiği anlaşılmaktadır. Ayrıca 5 katılımcının mevzuat düzenlemelerinde eksikliğe/belirsizliğe değindiği izlenmektedir.

Katılımcılar tarafından sıklıkla dile getirilen personel alışkanlıkları/uyum sorunu riskini katılımcı AU5 şu şekilde ifade etmiştir “*Kullanıcının EBYS’yi etkileyen yeni düzenlemelere uyum sağlaması biraz zaman alabilir. Tüm kurumlar aynı şeyden şikâyetçi. Kullanıcılar bir türlü benimsemiyor. Yakın zamanda SDP kodlarında revize oldu; örneğin 713 kapandı. Bizim tarafta çok kullanılan kod, adam taslak dosya oluşturmuş hep onun üzerinden gitmek istiyor. Neden değişti ne gerek vardı diye sürekli telefonla bizi arıyorlar. Farz edelim ki 713 kodunu bulamadı bambaşka bir kod verebilecek bu da dosyalama, arşivlemeyle ilgili farklı sonuçlar doğuracak.*” Sistemde de uyum sorunlarıyla karşılaşılabilmesine değinen F3, “*Mesela verilerin güncel tutulduğu formatlarıyla belki uyumsuzluklara sebep olabilir*” şeklinde yanıt vermiştir. Benzer şekilde sürecin yönetilememesinin yarattığı uyum sorununa dikkat çeken K1, “*Bundan yirmi (20) yıl sonra Devlet Arşivleri Başkanlığı biz belgeleri elektronik olarak almaya başladı dediklerinde on (10) yıl önceki standartların yeni yapıya uymadığı ortaya çıktığında ne yaşayacağımızı bilmiyoruz. Bütün kurumları bu kadar serbest bıraktıktan sonra herkes kafasına göre diyeceğim artık bir sistem kullandıktan sonra bunları geri almaya kalkışmak inanılmaz zor olacak. Belki de başaramayacaklar bilmiyorum*” diyerek konuyla ilgili önemli bir etmene değinmiştir.

Tablo 3.3 incelendiğinde katılımcılar tarafından üzerinde durulan önemli bir konunun da mevzuat eksikliği olduğu görülmektedir. Katılımcılardan AU1, mevzuattaki eksikliklerin ve belirsizliklerin ortaya çıkarabileceği risklere ilişkin durumu şu şekilde açıklamıştır:

“Devlet Arşivleri Başkanlığı elektronik belge yönetim standartlarıyla ilgili genelge yayınlanalı on yedi (17) yıl olmuş. Bu belgelerin bir e-arşivde saklanması gerektiği bir gerçek. Yani, elektronik olarak ürettiğin belgeyi e-arşivde saklarsın. 2008’den bu yana bir şekilde bunun çalışmasının yürütülmesi gerekiyordu. Şimdi mesela araştırmalarımı yapıyorum, bakıyorum; 2013’te, 2014’te insanlar yurt dışında e-arşiv ile alakalı bizim şu anda tartıştığımız şeyleri tartışıyorlarmış. Yani forumlara, vesairelere bakıyorum, bildirilere bakıyorum; 2013’ler, on iki (12) yıl. Devlet Arşivlerinde çalışma var mı? Var, ama BAYS çalışıyorlar. 2019’dan beri; ama onun da yani strateji belgelerinden ileri gidemedi. Strateji belgelerinde işte “çalışma başlatılmıştır”, “teknik şartname hazırlanmıştır”, “ihaleye çıkılmıştır” gibi... Böyle altı (6) yıl oldu başlayalı. Ben eminim ki, başlasak da mesela bu yarın yayınlandı; kurumlar BAYS’a göre işlem yapacak deseler de birçok sıkıntı çıkacaktır aktarım konusunda. Çoğu kurumda dosya yönetimi de yok. Bir kurumda sordum: “Dosya erişimi nerede? Klasörler nerede?” “Klasör yok” dediler. Nereye gidiyor bunlar o zaman? Neden konu kodu veriyorum? Belge üretiliyor, tamam, hepsi bir havuzda toplanıyor. Yarın Devlet Arşivleri bir şey yayınlasa, kim yapacak bu kadar işi? Çok zor. Bir yandan da şöyle: Devlet Arşivleri bizim belgelerimizi alacak, ama bir kısmını alacaklar; hepsini almayacaklar. Mesela gizli, gizlilik dereceleriyle alakalı hâlâ işte o düşürülmesi, bu yeni son çıkan yönetmelikle birlikte gizlilik derecelerinin düşürülmesi ile alakalı uygulamalar var. Onunla alakalı ne yapılacak? Net değil. Devlet Arşivleri’ne devredilecek mi? Süresi gelecek, ama belki gizlilik kalkmayacak. Tamamı mı devredilecek? Bir diğer husus: Biz tüm ülkenin, tüm kamu kurumlarının belgesinden bahsediyoruz. Nasıl bir teknolojik altyapı gerekir? Nasıl bir depolama alanı gerekir? Ben Devlet Arşivlerini yani çok mümkün görmüyorum.”

Diğer bir katılımcı (K10) ise mevzuat eksikliğiyle ilgili şu ifadeleri kullanmıştır: *“Hem teknik hem de yasal düzenlemenin birbirine paralel şekilde yürütülmesi lazım. Bazen yasal bir düzenlemenin teknik karşılığı olmuyor. Öyle olunca tabi sıkıntılar baş*

gösteriyor. Belgenin tarafında nasıl bir şey var dersiniz mesela tüzel ve gerçek kişiler için özellikle gönderdikleri evraklarla ilgili bir standart yok. Mesela kamu kurumları arasında bir standart var EYP var ve bu standardın dışında evrak gönderimi engelleniyor ya da iade ediliyor karşı tarafa ama vatandaş ya da tüzel kişilik hangi formatta gönderirse göndersin kurumdan o belgeyi kabul etmesi bekleniyor. Bunun arka taraftaki yasal dayanağının olması lazım mesela orada bir eksiklik var.”

Kurum ve kuruluşların EBYS’ye yönelik yeterli hazırlık yapmadıklarını, bundan dolayı olası değişikliklere uyum sağlama konusunda ciddi sorunlar yaşayabileceğini belirten katılımcılardan AU7 durumu şu şekilde açıklamıştır:

“TS 13298 2015’in güncellenmesinden sonra arşiv yönetim sistemi de devreye girdi ve bu durum bazı riskleri beraberinde getirdi. Bazı kurumlar, belgeyi arşivleyecekmiş gibi düşünmedikleri için değerlendirme yapmadılar; saklama süresi dahi tayin etmediler ve bir saklama planı oluşturmadılar. Oysa yeni standart, arşiv yönetim sistemine geçilmesini ve belgelerin bu sisteme aktarılmasını zorunlu kılıyor. Arşivin geliştirdiği bütünleşik arşiv yönetim sistemi kapsamında, kamu kurumlarına ait e-imzalı belgelerin arşive devredilmesi planlanıyor. Elektronik belgeler, kurumlardan dosya olarak alınacak ve arşive aktarılacak gibi görünüyor. Bu yeni standart kapsamında, TS’ye ek bir güncelleme yapıldı ve güncellemede dosya olarak arşive devrin zorunlu olduğu belirtildi. Ancak kurumlar, dosya formatında belge oluşturmadıkları için bu durum bir risk unsuru haline geliyor; uyum sağlayamama problemi ortaya çıkıyor. Ayrıca sadece dosya olarak değil, sistem içinde X uygulamasının yapılması gerektiği belirtiliyor; eğer kurum bu uygulamayı gerçekleştirmediyse, bu da ayrı bir risk unsuru oluşturuyor.”

3.2.1.1.3. Yeni Teknolojilerin Riskleri

Yeni teknolojilerin (yapay zekâ, nesnelerin interneti vb.) kurumsal sistemlere entegrasyonu, iş süreçlerinin hızlanması ve verimliliğin artması açısından önemli fırsatlar sunmaktadır. Ancak bu entegrasyon süreci birçok riski de beraberinde getirmektedir. Söz konusu teknolojilere entegrasyonla birlikte EBYS’de karşılaşılabilecek risklere yönelik katılımcı görüşlerine ilişkin veriler Tablo 3.4’te sunulmaktadır:

Tablo 3.4: Yeni teknolojilerin riskleri

<i>Risk (N=68)</i>	<i>Katılımcılar</i>
Güvenlik/Gizlilik (N=17)	AU1-AU8, F1, F3, K1, K4, K5, K7, K9, K11, K12
Teknolojik Alt Yapı 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
Manipülatif Etkiler (N=2)	AU3, AU7
Mesleki Tehdit (N=2)	AU3, AU4
Projenin Başarısız Olması (N=2)	AU8, K2
Belirsizlikler (N=1)	AU3
Bütçe (N=1)	K3
Erişim (N=1)	AU1
İnsani Değerler (N=1)	AU4
Kişisel Veri (N=1)	AU1
Sürekli İyileştirme (N=1)	K2

Tablo 3.4 incelendiğinde, katılımcılar tarafından yeni teknolojilerin entegrasyonu konusunda en çok vurgulanan risk unsurunun güvenlik ve gizlilik (N=17) olduğu görülmektedir. Bunu, teknolojik altyapı yetersizlikleri (N=10) ve yapay zekâ için hazırlanan veri setinin beraberinde getireceği riskler (N=10) izlemiştir. 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.

Katılımcılar tarafından en çok vurgulanan unsur olan güvenlik ve gizlilik risklerini AU7, “*Kendi derin öğrenme modellerimizi oluşturabiliriz ancak bu süreçte kullandığımız algoritmaların belgemizi ifşa etme riski genellikle düşük olsa da karşı tarafa yüklenen eğitim setlerinin gizliliği belirsizdir*” şeklinde açıklamıştır. AU7, sağlık alanında bir örnek vererek bir ilaç şirketinin hastanenin MR (manyetik rezonans görüntüleme) sonuçlarını değiştirebilen zararlı yazılımlar geliştirdiğini ve böylece kendi ilacını teşvik ettiğini ifade etmiştir. Bu durumun ileride yapay zekâ destekli savaşlar gibi daha büyük risklere yol açabileceğini vurgulamış ve gizli kalması

gereken belge setlerine yapay zekânın erişme ihtimalinin önemli bir tehdit olduğunu vurgulamıştır. Ayrıca yapay zekâ algoritmalarının da yazılım kaynak kodları gibi bağımsız ve akredite mekanizmalar tarafından denetlenmesi gerektiğini, bunun kamuoyunda güvence sağlayacağını savunmuştur. Bu tür önlemler alınmadığı takdirde mahremiyetin ihlali ve toplumsal kaosa yol açabilecek beklenmedik sonuçların ortaya çıkabileceğini ifade etmiştir. AU7 ayrıca veri düzenlemesinin önemini şu şekilde vurgulamıştır: *“InterPARES projesinin güvenilir yapay zekâ (Inter pares Trust AI) alanında yaklaşık dört yıldır çalışmalar yürütülüyor fakat beklenen ilerleme sağlanamadı. Bunun temel sebebi, yapay zekâyı besleyecek belgeler yeterince nitelikli değil. Yani dosya kodları eksik ve üstveri ilişkileri kurulamamış. Yapay zekâdan başarılı sonuçlar almak için önce veri kalitesinin artırılması, nitelikli veri düzenlemesinin yapılması gerekir. Ancak bu temel sağlandıktan sonra derin öğrenme, nesnelerin interneti gibi ileri teknolojilerin etkin şekilde kullanılabilir. Yeni teknolojilerin aceleyle benimsenmesi istenen sonuçları vermeyecektir. Çünkü öncelikle eldeki verinin yeterli kalitede olması gerekir.”*

Katılımcılar, veri setinin hazırlanma risklerinin üzerinde önemle durmuştur. Örneğin F3, veri seti hazırlanmasının önemini vurgulayarak bu konuyu *“Yapay zekâlar bildiğiniz gibi öğrenmeyle eğitilerek çalışır. Yanlış öğrenme veya hatalı algoritmalarla eğitildiklerinde özellikle kurumların karar destek sistemi olarak kullandığı durumlarda, karar verme süreçlerinde hatalara yol açabilirler.”* şeklinde açıklamıştır. Bir diğer katılımcı olan K4 de F3 ile benzer görüştedir: *“Yapay zekâdaki öğrenme süreçlerini, özellikle derin öğrenme kısmında, kullanıcıların yaptığı hataları doğruymuş gibi algılama var. Burada yapay zekâ modellerini yazarken ya da eğitirken tamamen doğru yönlendirmek ve aslında yapay zekâyı verileri sağlarken de modeli çıkartmak için hatalı yapılan işlemlerin neler olduğunu işaretleyip bunların hatalı olduğunu belirtmek gerekiyor. Yoksa yapay zekânız hatayı doğruymuş gibi kabul edecek”.*

Katılımcılar yeni teknolojilerin ortaya çıkmasında personelden kaynaklı hataların önemli riskler meydana getirebileceğini belirtmiştir. Katılımcılardan K13 bu durumu *“İnsan kontrolünün belli bir süre bu süreçleri incelemesi, düzeltmeler yapması, daha da geliştirmesi gerektiğini düşünüyorum. Yapay zekâyı kurumun ihtiyaçlarına yönelik akıllandırmak da yine yetkin personellerin işidir. Yapay zekâ çalışmalarının doğru*

bilgileri aktaracak kişilerce yapılmasını savunuyorum.” şeklinde ifade etmiştir. K11 de benzer şekilde bu durumu şu sözlerle desteklemiştir:

“Resmi yazı dediğiniz şey standart olabilir evet, ama kamuda standart olmayan durumlar da mevcut. Sizden bir karar veya talimat beklenir. Yapay zekâlar bu talimatı veya kararı veremez, çünkü birçok kurum aynı nitelikteki yazıya bazen ‘evet’ derken bazen ‘hayır’ diyebilir. O yüzden kullanıcı işini bilecek, zekâsını doğru kullanacak. Yani yapay zekâyı da eğitecek olan yine insan olacak. Biz de kurum olarak yapay zekânın değil ortalama bir zekânın peşindeyiz.”

Katılımcılar dış kaynak kullanımının potansiyel risklerine çeşitli perspektiflerden yaklaşmıştır. AU7, kullanılan yapay zekâ ve derin öğrenme algoritmalarının kodlarına hâkim olmanın gerekliliğini vurgulayarak *“Kullandığımız yapay zekâ algoritmasının ya da derin öğrenme algoritmasının kodlarına hâkim olmamız gerekiyor. İşte bu, açıklanabilir yapay zekâ dediğimiz bir mesele var, XAI diye geçer. Açıklanabilir yapay zekâ, işte üretken yapay zekâ var. Bunların kodlarının bizim elimizde olması lazım”* ifadelerini kullanmıştır. Benzer şekilde, AU4 ise dış kaynaklı teknolojilerin sağladığı avantajlara rağmen kontrol, yönetim ve çözüm eksikliğinin uzun vadede risk oluşturabileceğine dikkat çekerek: *“Çoğunlukla dış kaynaklı bu tür teknolojileri kullanmak birçok avantaj sağlasa da kontrol, yönetim ve çözümlerin elinizde olmadığı bu teknolojiler, uzun dönemde aleyhimize kullanılma riski barındırır.”* açıklamasını yapmıştır.

Bulut teknolojileri konusunda ise AU6, güvenlik endişelerini öne sürerek şunları ifade etmiştir: *“Bulut teknolojisini kullanalım. Sunucular için ayrı bir yer, ayrı bir maliyet.. olmasın deniliyor ama nasıl güvenliğini sağlayacaksınız? Microsoft’un bulutunu kullanıyorsunuz diyelim Amerika kökenli. Tüm belgeleri onlara vermek demek bu. Yerli, milli bir bulut ağımızın olması gerekir.”* Bu görüşler, dış kaynak kullanımında teknolojik bağımsızlık, veri güvenliği ve ulusal altyapının ne denli önemli olduğuna dikkat çekmektedir.

Mevzuat eksikliği riskini K4, *“Yapay zekâ çok yeni, çok yeni olduğu için kullanılacağı alanlar net değil. Mesela Chat GPT olsun diğer yapay zekâ ürünleri olsun Google’ın geliştirdikleri olsun hani buralarda yapay zekâyı EBSY’ye entegre edebiliriz ama bunların bir sınırlaması olması gerekiyor ve bunların kanunları mevzuatlarla düzenlenmesi gerekiyor ki ondan sonra böyle bir sisteme entegre edelim”* şeklinde

açıklamaktadır. AU4 bu risk faktörünü kişisel veriler bağlamında ele almış ve şu ifadeleri kullanmıştır: “Teknolojinin hızı ve dönüşümü, yakın gelecekte gizlilik ve güvenlik konusunu daha çok konuşulur hâle getirecek. Özellikle Kişisel Verilerin Korunması Kanunu (KVKK) ve buna ilişkin uygulamaların EBYS’deki karşılığı yeteri kadar ele alınmadı. Sistemin fonksiyonlarını etkileyip etkilemediği konusu tartışılmalı. Örneğin, bir resmi yazıda T.C kimlik numarası varsa, bu belge KVKK kapsamında mıdır, yoksa belge yönetimi ve arşiv disiplini kurallarına mı tabidir? Bu etkilerin olası sonuçları karmaşa ve belirsizlik doğurabilir. Bu durumda kişisel inisiyatifler devreye girebilir, bu da standart uygulama adımlarını ortadan kaldırır. Aynı zamanda hukukun hareket alanı karmaşıklaşır, yani kuralsızlık doğar.”

Katılımcılar ayrıca yeni teknolojilerin mesleki tehdit riski oluşturduğuna da dikkat çekmiştir. Bu teknolojilerin bilgi ve belge yönetimi alanında çalışan personelin görevlerini devralma potansiyeline sahip olduğuna işaret eden katılımcılar, bunun önemli bir endişe kaynağı olduğunu belirtmiştir.

Yapay zekâ, makine öğrenmesi ve nesnelerin interneti gibi yeni teknolojilerin EBYS’leri tehdit etmesinin yanı sıra kullanılan teknolojinin kendisindeki değişim ve dönüşüm de sistemsal risklere neden olmaktadır. Teknolojik altyapının sürekli değişmesi/gelişmesine paralel olarak sistemlerin güvenliği, erişilebilirliği ve belgelerin bütünlüğü üzerinde doğrudan etkiler meydana getirmektedir. Teknolojik değişimlerin sistem güvenliği veya uyumluluk üzerinde oluşturabileceği risklere yönelik akademisyen/uzmanların görüşlerine dayalı veriler tablo 3.5’te sunulmaktadır:

Tablo 3.5: Teknolojik değişim riskleri

<i>Riskler (N=10)</i>	<i>Katılımcılar</i>
Güvenlik (N=5)	AU1, AU3-AU5, AU8
Belgenin Delil Değerinin Bozulması (N=2)	AU1, AU7
Erişim (N=2)	AU3, AU5
Bütünlüğün Bozulması (N=1)	AU1

Tablo 3.5’te görüldüğü üzere teknolojik değişimin meydana getirebileceği riskler konusunda 5 katılımcı güvenlik, 2 katılımcı belgenin delil değerinin bozulması, 2 katılımcı erişim ve 1 katılımcı da belge bütünlüğünün bozulması üzerinde durmuştur.

Katılımcıların teknolojik değişimlerin 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. Benzer şekilde, AU3 teknolojik değişikliklerin hızının sistemlerin güvenlik sürekliliğini olumsuz etkilediğini belirterek *“Yeniye uyum da bir güvenlik meselesidir”* ifadesini kullanmıştır. AU5 ise hem donanım hem yazılım alanında ortaya çıkan risklere işaret ederek, teknolojik değişikliklerin sistemlerin siber saldırılara karşı dayanıklılığını etkileyebileceğini belirtmiş ve bu bağlamda EBYS yazılımlarının arka plandaki konfigürasyonlarının eksiksiz yapılmasının önemini vurgulamıştır: *“Donanım ya da yazılımlar değiştirildiğinde, konfigürasyonlar tam olarak yapılmazsa siber saldırı ya da veri kaybı riski ortaya çıkmaktadır ki bu çok önemli bir risktir.”*

Belgenin delil değerine ilişkin riskler de katılımcılar tarafından önemli bir unsur olarak ifade edilmiştir. AU7, teknolojik ortamın değişiminin belge yönetimi üzerindeki etkisini örneklerle açıklamıştır: *“Disketler, CD’ler derken şimdi SSD’lere, NVMe teknolojisine geçildi. Bu değişikliklerin aktarımı, yeni sistemin özelliklerine uygun olmalı ve zamanında yapılmalıdır. Aksi takdirde, sistem eskidikçe uyumluluk sorunları ortaya çıkar. Örneğin, bugün PDF belgeler kullanılıyor, ancak ileride yeni formatlar çıkabilir ve o zamana kadar gerekli dönüşümler yapılmazsa, belgenin varlığı ve delil değeri tehlikeye girer.”* Dolayısıyla teknolojik değişim sürecinde kurumların risk iştahının düşük olması ve süreçte hiçbir açığı kabul etmemesi gerektiğini ifade etmek gerekir.

Erişim risklerine dair değerlendirmelerde ise AU5, yaşanmış bir olaya atıfta bulunarak sistem odası taşınması sırasında EBYS’de imzalı belgelerin kaybolmasının ciddi bir risk olduğunu belirtmiş, bu tür durumlarda yedekleme ve geri yüklemenin önemine dikkat çekmiştir. AU3 ise eski ve yeni sistemlerin uyumunun sağlanamaması halinde yakın geçmişe erişimin imkânsızlaşacağını ve eski donanım ihtiyacının ortaya çıkmasının ciddi sorunlara yol açabileceğini söylemiştir: *“Eskiye erişebilmek için eski donanıma ihtiyaç duyulması ciddi bir problemdir. Bu nedenle eski sistemlerin hızla yeni sistem ve donanıma transfer edilmesi gerekir.”* Katılımcılar teknolojik değişim

riskiyle ilgili genel olarak teknolojik değişikliklerin sistem erişilebilirliği açısından dinamik ve sürekli güncellenen bir süreç gerektirdiği üzerinde durmuştur.

3.2.1.2. İç Faktörlere Bağlı Riskler

EBYS'lerin etkinliği sadece teknik altyapıyla değil aynı zamanda kurum içi yapı ve dinamiklerle de doğrudan ilgilidir. Kurum kültürü, organizasyonel yapı, personel yeterliliği, yönetim anlayışı ve iç politika eksiklikleri gibi unsurlar sistemin başarısını etkileyen temel iç faktörler arasında yer almaktadır. Bu bölümde elektronik belgenin kurum kültüründeki yeri, firmaya iletilen talepler, organizasyonel değişiklikler, personel ve eğitim, politika ve prosedür eksikliği, yönetim desteği gibi başlıklarda iç faktörlere dayalı risk unsurları katılımcıların görüşleri doğrultusunda ele alınmaktadır.

3.2.1.2.1. Elektronik Belgenin Kurum Kültüründeki Yeri

Elektronik belgelere kurum kültüründe verilen önem ile kâğıt odaklı bir kültürden dijital bir kültüre geçişte yaşanan risklere ilişkin kurum temsilcisi katılımcılardan elde edilen veriler Tablo 3.6'da sunulmaktadır:

Tablo 3.6: Elektronik belgenin kurum kültüründeki yeri

<i>Riskler (N=25)</i>	<i>Katılımcılar</i>
E-Belgenin Çıktısının Alınması (N=7)	K1-K3, K8, K10-K12
Yeniliklere/Değişikliklere Direnç (N=5)	K5-K7-, K9, K10
EBYS'ye Ait Birimin Olmaması (N=3)	K4, K10, K11
Jenerasyon Farkı (N=3)	K1, K5, K13
EBYS Ekibinin Sorun Çözme Yetisi (N=2)	K2, K3
Yöneticinin Tutumu (N=2)	K3, K4
Adaptasyon (N=1)	K13
Islak İmzalı Belge Üretiminin Devam Etmesi (N=1)	K11
Teknik Bilgi Yetersizliği (N=1)	K1

Tablo 3.6'da, katılımcıların en çok vurguladığı riskin e-belgenin çıktısının alınması (N=7) olduğu görülmektedir. Bunu, yeniliklere/değişikliklere direnç (N=5), EBYS'ye ait birimin olmaması (N=3), jenerasyon farkı (N=3) risklerinin izlediği anlaşılmaktadır. EBYS ekibinin sorun çözme yetisi (N=2) ve yöneticinin tutumu (N=2) risklerinin de elektronik belgenin kurum kültüründe oluşturabileceği riskler arasında belirtildiği gözlemlenmektedir.

Katılımcılar çoğunlukla elektronik ortamda belgelerin üretildiğini fakat bunların çıktısının alınıp dosyalandığını ifade etmiştir. K3, kurumundaki bazı birimlerde tüm belgelerin çıktısının alındığını, bunun sistemin çökme ihtimaline karşı bir önlem olarak görüldüğünü ve bu durumun sisteme duyulan güvensizlikten kaynaklandığını belirtmiştir. Benzer şekilde, katılımcı K1 de bireysel tutumdan, yöneticilerin yaklaşımından ya da kurumsal kültürden kaynaklı dijital ortamda hazırlanan belgelerin çıktısını alma alışkanlığının sürdüğünü ifade etmiştir.

Eski alışkanlıkların sürdürülmesi ve yeniliklere karşı direnç, elektronik belge yönetim sistemlerinin kurumsal düzeyde benimsenmesini zorlaştıran temel etkenlerdendir. Katılımcı K9, bu durumu şu sözlerle ifade etmiştir: *“Elektronik belgeden ziyade belgeye yönelik, belge yönetiminin önemine yönelik bir şey yok. Yani kimle konuşursanız EBYS çok önemli belgeler çok önemli şudur budur hep aynı hikâyeleri söylüyor. Ama önemli olan bir şeye de hiçbir şekilde önem vermiyorlar. Kurum çalışanlarının olsun yöneticilerin olsun derdi yazı yazabiliyor muyum yazdım, aradığım zaman bulabiliyor muyum buldum. Onlar için bu kadar. Yöneticiler de olsun çalışanlar da olsun kâğıt üzerinde okuyup onun üzerinden not alıp altını çizme, sağını solunu karalama kültürünü hala devam ettirmek isteyen insanlar var. Bilgisayara bakmak gözümüzü yoruyor niye önümüze gelse de biz kâğıttan yapsak diyen bu işi savunan insanların varlığı devam ediyor.”* Bu ifadeler, elektronik belge yönetiminin teknik uygulanabilirliğinden ziyade kullanıcı alışkanlıkları ve kültürel dirençle şekillendiğini göstermektedir.

EBYS için oluşturulmuş bir birimin olmaması, kurum işleyişini etkileyen önemli bir risk unsuru olarak görülmüştür. Katılımcılardan K10 bu riski şu şekilde belirtmiştir:

“Bu EBYS konusu bir çocuğu yetiştirme gibi düşünün. Siz çocuğun altını değiştirmezseniz işte acıktığında yemeğini vermezseniz o çocuk ölür. Bu yaşayan bir sistem. Eğer başında uzman birileri yoksa sadece bir kişi vermişlerse o da izine ayrıldıysa kimse de ona bakmıyorsa o çocuk ya açlıktan ölecek ya altı değiştirilmeyecek hasta olacak. Ciddi anlamda buna bakan bir birim olması önemli, bir başkanlık, bir müdürlük varsa bu süreç daha sağlıklı yürüyor.”

3.2.1.2.2. Organizasyonel Değişiklikler

Organizasyonel değişiklikler, dış etkenlerden (makroekonomik koşullar, teknolojik gelişmeler, merkezi yönetim kararları) kaynaklansa da kurumların iç işleyişine ve belge yönetim süreçlerine doğrudan etkisi vardır. Örneğin, kurumun/birimin kapanması, birimlerin birleşmesi gibi yapısal dönüşümler EBYS açısından çeşitli riskler taşımaktadır. Bu değişimleri tetikleyen unsur merkezi kararlar olsa da sonuçlar kurumların içsel bütünlüğünü etkilemektedir (Albayrak, 2020, s. 1519). Organizasyonel değişiklikler (birimlerin birleşmesi, ayrılması, yeni bir birimin kurulması ya da kurumun yeniden yapılanması vb.) EBYS’de çeşitli risklerin ortaya çıkmasına neden olmaktadır. Bu nedenle organizasyonel değişimlerin risk yönetimi bağlamında sistematik olarak değerlendirilmesi ve risklerin tanımlanması, değerlendirilmesi, yönetilmesine yönelik yapıların oluşturulması gerekmektedir (Ermisket, 2011, s. 59).

Bu çalışmada söz konusu değişimlerle birlikte ortaya çıkan riskler, iç faktörler kategorisinde değerlendirilmiştir. Çünkü bu riskler her ne kadar dışarıdan bir etki tarafından tetiklense de sonuçları içyapıyı etkilemektedir. Böylece risklerin daha bütüncül bir yaklaşımla ele alınması amaçlanmıştır. Organizasyonel değişikliğin meydana getirebileceği risklere yönelik katılımcı görüşlerine dayalı veriler Tablo 3.7’de sunulmaktadır.

Tablo 3.7: Organizasyonel değişiklik riskleri

<i>Riskler (N=36)</i>	<i>Katılımcılar</i>
Erişim (N=5)	AU8, K1, K9, K10, K12
İş Yüğü (N=5)	AU6, AU8, K1, K2, K9
Veri Kaybı (N=4)	AU1, AU6, F3, K1
Yönetmel Karmaşıklık (N=4)	AU1, K5, K6, K13
Firma Değişikliği (N=3)	AU4, AU6, AU8
İş Sürecinin Aksaması (N=3)	F1, F3, K1
Belge Bütünlüğünün Bozulması (N=2)	AU7, K8
DETSİS Kodlarının Güncellenmemesi (N=2)	AU5, K11
Adaptasyon (N=1)	K12
EBYS’nin Hantallık ve Uyum Sorunları (N=1)	K9
Ortak Sistemlerin Kullanılmaması (N=1)	AU3

Prestij Kaybı (N=1)	AU1
Uzun Vadeli Sorunlar (N=1)	K7
Veri Güvenliği (N=1)	F2
Veri Uyuşmazlığı (N=1)	K4
Yasal Yükümlülüğün Sağlanamaması (N=1)	AU1

Tablo 3.7’de yer alan organizasyonel değişikliklerin oluşturabileceği riskler incelendiğinde, 5 katılımcının kurumlarda belgeye erişim riski üzerinde durduğu görülmektedir. Ayrıca değişikliklerin personele iş yükü artışı olarak yansıtacağını 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.

Erişim riski ile ilgili katılımcılardan K9, klasörlerin düzgün taşınmaması durumunda gittiği yerdeki çalışanların o verilere ulaşamayacağını belirtmiştir. K12 ise birim değişikliklerinde kullanıcıların hesaplarının kapatıldığını ve yeni birime hesap açıldığını ancak bazı personelin eski belgelere ulaşmak istemesi yüzünden çok sıkıntı yaşadıklarını dile getirmiştir.

Katılımcılar tarafından organizasyonel değişiklikler sonucunda iş yükünün arttığı ifade edilmiştir. Katılımcılardan AU6 bu durumu “*Aslında belge oluşturup dağıtımını yaparken arka planda bir sürü algoritma çalışıyor. Her bir işlem içim 0 ve 1’lerden oluşan kodlar devreye giriyor. Bir kurum veya birim ayrıldığında kurduğun o döngüyü de koparmış oluyorsun. Yeniden bir yapılanma demek oluyor bu.*” şeklinde ifade etmiştir. K9 “*Yakın zamanda bizim organizasyonda değişiklik oldu arkadaşlar çok perişanlar*” diyerek durumu özetlemiştir. AU8 ise konuyu “*Bu değişiklikler bizlerin arşivcilerin ve EBYS yöneticilerin aslında hiç denk gelmek istemediğimiz korkulu rüyalarımızdan bir tanesi. Hem fiziki anlamda hem elektronik anlamında düşünecek olursak bu süreçler biraz zorlayıcı süreçler olabiliyor. Ekstra bir çalışma gerektiriyor.*” şeklinde açıklamıştır.

Organizasyonel değişiklikler sürecinde özellikle birim birleşmeleri, ayrılmaları ya da kurum değişiklikleri sırasında veri ve belge kaybı riski, katılımcılar tarafından ciddi bir sorun alanı olarak dile getirilmiştir. AU1 veri kaybı riskini şu şekilde açıklamıştır:

“Bence ilk başta yaşanacak risk veri kaybı ya da buna belge kaybı da diyebiliriz. Şimdi birleşme ya da ayrılmalarda, devralmalarda bir kere veri kimin verisi? Yani belge kimin belgesi? Birleştik sıkıntı yok çünkü birleşiyoruz. Tek bir havuzun içerisine giriyor. Ancak yeniden yapılanma iki ayrı bir daire başkanlığına bölünme durumlarında belge kimin belgesine dönebilir durum. Yanlış yerde konumlandırılabilir. Muhakkak yanlış bir uygulamaya sebep olacaktır böyle bir durum ki ülkemizde bu özellikle bakanlık seviyesinde çok fazla yaşanan bir şey. Çünkü yani her şey gibi bürokrasi de değişiyor sürekli olarak”

Katılımcılardan F3 veri kaybı riskiyle ilgili şunları aktarmıştır: *“Veri kaybı karşılıklı bir konu şöyle, kurumun size doğru veriyi tanımlaması lazım. Yani şu veri mesela Aile Bakanlığına gidecek bu veri Çalışma Bakanlığına gidecek demesi lazım. Biz veriyi taşıırken migrasyon yaparken veri kaybı olmuyor pek. Ama bu konuda çok profesyonel olduğumuz için olmuyor. Dediğim gibi yüzden fazla kurumun migrasyonunu yaptık bugüne kadar. Ama yine yetkin bir yer olmadığında çok büyük bir risk. Veri kaybı çok büyük bir risk. Karşılıklı mutabık kalmak gerekiyor kurumla. Kurumun da onu çok güzel ayırıştırması gerekiyor. Sizin de onu çok iyi ayırıştırmanız gerekiyor. Bu çok ciddi yürütülmesi gereken ve çok ciddi riskler barındıran bir süreç.”*

Kurum temsilcilerinden K1, organizasyonel değişiklikler sırasında veri kayıplarının sıkça yaşandığını, bazı kurumların bu kayıpların henüz farkında olmadığını belirtmiştir. Bu durumun ilerleyen süreçte belgeye ihtiyaç duyulduğunda, belgenin bulunmadığında fark edileceğini ve verilerin kaybolduğunun o zaman anlaşılacağını ifade etmiştir.

3.2.1.2.3. Personel ve Eğitim Riskleri

EBYS yalnızca belirli bir birimin faaliyetlerini yerine getirmek için değil kurum genelinde tüm birimlerce kullanılan bir sistemdir. Bu kapsamda personelin sistemle ilgili bilgi düzeyi, verilen eğitimlerin niteliği ve kurum içindeki personel hareketliliği gibi faktörler sistemde önemli risk alanlarını oluşturmaktadır. Katılımcı görüşlerine dayanarak bu başlık altında; eğitim etkililiği, eğitim eksikliği ve personel devir hızına bağlı riskler analiz edilmektedir.

Eğitimin Başarısını Etkileyen Riskler

Kurumlarda EBYS'ye yönelik pek çok eğitim verilmektedir. Fakat çoğu zaman bu eğitimlerin başarıya ulaşmadığı, hataların devam ettiği görülmektedir. Eğitimin başarısını etkileyen risklere yönelik katılımcı görüşlerine dayalı veriler Tablo 3.8'de sunulmaktadır:

Tablo 3.8: Eğitimin başarısını etkileyen risk unsurları

<i>Riskler (N=29)</i>	<i>Katılımcılar</i>
Denetim/ Yaptırım Eksikliği (N=7)	AU2, K1, K2, K4, K5, K9, K12
İş Yapmaya İsteksizlik/İlgisizlik (N=4)	K1, K5, K10, K12
EBYS Ekibinin Büyüklüğü ve Yetkinliği (N=3)	AU2, K3, K10
Yönetimin Desteği (N=3)	K2, K3, K11
Eğiticilerin Yetkin Olmaması (N=2)	K4, K10
Eğitim İçeriği (N=2)	AU8, F2
Personel Kapasitesi (N=2)	F2, K13
Personelin EBYS'ye Bakışı (N=2)	K5, K9
Eğitime İsteksizlik (N=2)	AU6, K1
Eski Alışkanlıklar (N=1)	K1
Personelin Yaşı (N=1)	K2

Tablo 3.8'e göre en çok vurgulanan riskin denetim/yaptırım eksikliği (N=7) olduğu görülmektedir. Bunu iş yapmaya isteksizlik/ilgisizlik (N=4) takip etmektedir. Ayrıca EBYS ekibinin büyüklüğü ve yetkinliği (N=3) ile yönetim desteğinin (N=3), katılımcılar tarafından üzerinde durulan kayda değer unsurlar olduğu anlaşılmaktadır.

En sık ifade edilen risk unsuru olan denetim/yaptırım eksikliği riskini K9 “*Eğitim mutlaka şart. Eğitim veriyoruz ama eğitimden ziyade denetim gerekiyor. Birim amirlerine çok iş düşüyor. Bir yazıyı hazırlayıp imzaya gönderiyorsunuz, noktasına virgülüne bakıyor ama dosya plan kodunun doğru olup olmadığına bakmıyor. O belgeler sadece içerik olarak okunmamalı. Bütün boyutlarıyla, işte dosya kodlarından tutun da antetine kadar bütün olarak kontrol etmeleri lazım. Maalesef yöneticilerin ne burada ne de diğer kurumlarda bu noktada en ufak bir inisiyatif almadıkları gibi almaya niyetleri de yok. Şunu diyorlar: “Biz dosya kodlarını mı öğreneceğiz ya?” Öğrenme, senin biriminde kullandığın zaten on (10)tane dosya kodu var. 1500 kod*

olabilir ama senin birimini ilgilendiren beş (5) tane kod var. O beş tane kodu da öğreniver ve o iki (2) tane yazıyı ben hâlâ iddia ediyorum iki (2) tane yazıyı sırf dosya planı kodu yanlış verilmiş diye gönder, o çalışan bir daha o hatayı yapmaz kesinlikle. Yani farkındalık olması lazım ve sürekli denetim olması lazım. Yani belli bir seviyeye gelene kadar denetimlerin olması lazım” şeklinde belirtmiştir. AU2 ise, “Burada en zayıf halka insan, EBYS’yi hatta diğer bilgi sistemlerini kullanan insanlar. Dolayısıyla insanlardaki farkındalığın artması gerekmektedir. İnsana dayalı güvenlik zafiyetlerini azaltmak için çok sık eğitim verilmeli. Yani bu işlemi yapan insanlara eğitim verilmeli. Ayrıca birimler denetlenmeli. Yani yerinde nasıl işlem yapıyorlar, ne tür sorunları var, yaptıkları hatalar varsa bunları süre verilerek düzeltmeleri istenmeli. Denetim olmazsa insanlar yanlış yapmaya devam eder.” şeklinde ifade etmiştir.

Katılımcı K1, iş yapmaya yönelik isteksizlik ve ilgisizlik riskinin temelinde bilgi eksikliğinden ziyade kamu görevine ilişkin sorumluluk bilincinin yeterince gelişmemesinin yattığını vurgulamıştır. Katılımcıya göre kurumsal olarak gerekli tüm eğitimler verilmesine rağmen bazı personel görevleri öğrenmekten bilinçli olarak kaçınmaktadır. İş nasıl yapacağını öğrenmesi durumunda sorumluluğun kendisine kalacağı endişesini taşımaktadır. Bu durum kamu hizmetine yönelik görev anlayışındaki zayıflıkla ilişkilidir ve öğrenmeye karşı isteksizliğe neden olmaktadır.

Eğitim Eksikliğinin Riskleri

EBYS’nin etkin kullanılabilmesi, kullanıcıların sistemle ilgili bilgi düzeyiyle ilişkilidir. Bu bağlamda eğitim eksikliği, sistemin yanlış ya da eksik kullanılmasına dolayısıyla belge yönetimi süreçlerinde çeşitli aksaklıklara neden olabilmektedir. Eğitim eksikliğinin oluşturabileceği risklere ilişkin katılımcı görüşlerine dayalı veriler Tablo 3.9’da sunulmaktadır.

Tablo 3.9: Eğitim eksikliğinin riskleri

<i>Riskler (N=16)</i>	<i>Katılımcılar</i>
İşlemlerin Yanlış Yapılması (N=7)	AU8, F1, K2-K4, K8, K13
Dosyalamanın Yapılmaması/Yanlış Yapılması (N=3)	K2, K5, K12
İş Sürecinin Aksaması (N=3)	F2, F3, K13
Dijital Çöplük (N=1)	K9
Güncellemelerin Takip Edilememesi (N=1)	AU7

Güvenlik (N=1)	K5

Tablo 3.9’da eğitim eksikliğinin doğurabileceği risklerin başında işlemlerin yanlış yapılmasının (N=7) geldiği görülmektedir. Bunu dosyalama hataları (N=3) ve iş süreçlerinin aksaması (N=3) riskleri izlemektedir.

Eğitim eksikliğinin bir sonucu olarak ortaya çıkabilecek riskler arasında en çok vurgulanan risk işlemlerin yanlış yapılmasıdır. Katılımcı F1, bu durumu şu sözlerle ifade etmiştir: *“Gerekli eğitimlerin alınmaması ya da eğitim sonrası ölçümleme yapılmaması sorun teşkil eder. Eğitim yetersizliği ve liyakatsizlik gibi sorunlar kurumu genel olarak sıkıntıya sokabilecek durumlar doğurur. Hatta yasal müeyyidelerle karşı karşıya kalınabilir. Örneğin onay verilmemesi gereken bir evrakta onay verilmesi nedeniyle ihale ve satın alım evraklarında yapılan denetimlerde yaptırım uygulanması söz konusu oluyor.”* Benzer şekilde AU8, kullanıcıların sisteme entegre edilememesi durumunda süreçlerin standartlaşamayacağını ve bu durumun yanlış işlemlere yol açacağını belirterek *“Kullanıcıyı sisteme entegre edemezsek sistemin yönetilmesi mümkün değil. Çünkü farklı farklı süreçler oluşacak, farklı alışkanlıklar devam ettirilmek istenecek... yanlış işlemler yapılmasına neden olacak”* sözleriyle sürece dikkat çekmiştir. Bu ifadeler, eğitim eksikliğinin sadece bireysel değil, kurumsal düzeyde iş süreçlerini ve yasal uyumu olumsuz etkileyen önemli bir risk alanı olduğunu göstermiştir.

Personel Devir Hızı

Personel devir hızı, elektronik belge yönetim sistemlerinin işleyişinde çeşitli risklerin ortaya çıkmasına neden olmaktadır. Katılımcı görüşlerine dayalı olarak belirlenen riskler aşağıdaki Tablo 3.10’da sunulmaktadır:

Tablo 3.10: Personel devir hızının oluşturduğu riskler

Riskler (N=18)	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
Yanlış Uygulamalar (N=2)	AU5, K7

Hizmet Kalitesinin Düşmesi (N=1)	AU7
Prosedür Eksikliği (N=1)	K5
Veri Güvenliği (N=1)	K9

Tablo 3.10'a 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), uzmanlaşmanın sağlanamaması (N=2) ve yanlış uygulamaların (N=2) artması katılımcılar tarafından dile getirilen önemli diğer riskler arasındadır.

İş sürecinin aksamasının sıklıkla vekâletlerde yaşandığını dile getiren katılımcı (K11) *“Vekâlet bıraktığın zaman mesela bir başkan, başkan yardımcısına vekalet bırakıyor. Orada bir yazı hazırlanmış, başkanın imzalaması gerekir ama ertesi güne kalmış ve başkan da yok. Vekâlet bırakıp gittiği zaman o belgenin üstünde yine aynı kişinin adı çıkıyor. Onu geri çekmesi gerekiyor. Personelin tekrar bir imza akışı yapıp yeniden imzaya çıkarması gerekiyor ve orada sıkıntılarımız oluyor”* şeklinde açıklamıştır. Bu durumları sıkça yaşayıp çözüm bulduğunu ifade eden K13 *“Vekâlet durumlarında yetki devirlerinin EBYS'ye hızlı bir şekilde tanımlanması iş aksamalarının önüne geçer. Sisteme konu ve akışlar tanımlanır ve vekâlet durumları otomatik hale getirilebilir. Sistemimizde kişiye iş ya da imzalaması gereken bir yazı geldiğinde telefonuna mesaj geliyor. İşlerde aksama yaşanmaması ya da yazıların tekrar yazılmasının önüne geçmek için bence uygun bir sistem.”* şeklindeki açıklamalarıyla sorunun çözülebileceğine dikkat çekmiştir.

Katılımcı AU1, personel devir hızına bağlı olarak yetkisiz erişim riskinin ortaya çıktığını belirtmiştir. Katılımcıya göre erişim yönetimi konusundaki bilgi eksiklikleri, belge güvenliği açısından çeşitli sorunlara yol açmaktadır. Sistemin doğru kullanılmaması sonucunda kullanıcılar, erişim yetkisine sahip olmadıkları belgelere ulaşabilmekte ya da erişimleri gereken belgelere erişememektedir. Katılımcı bu durumun, yalnızca günlük iş akışını aksatmakla kalmayıp daha ciddi sonuçlara neden olabileceğini hata ve güvenlik açıklarını beraberinde getireceğini ifade etmiştir. K11 de benzer şekilde bu durumu *“EBYS'deki yetki yönetimi çok önemli. En riskli alanlardan bir tanesi onun doğru yönetilmemesi. EBYS'nin yönetimi aslında bir sistem yönetimi değil operasyonel bir yönetim, organizasyonun yönetimi. Yoksa yani buraya hangi sistemi kurarsanız kurun teknik olarak yeterliliği varsa çalışacaktır. Ama*

burada sistem yönetmek, belge yönetmek aslında insanı yönetmek. Bu yetki yönetimini personel değişikliklerinde sağlıklı yapamazsanız çok büyük erişim problemleri yaşarsınız.” sözleriyle açıklamıştır.

3.2.1.2.4. Politika ve Prosedür Eksikliği

Elektronik belge yönetiminin kurumsal düzeyde kurallara uygun bir şekilde işletilip takip edilebilmesi için politika ve prosedürlerin belirlenmesi gerekmektedir. Politika ve prosedür eksiklikleri, belge yönetimi süreçlerinde çeşitli yönetsel ve teknik risklerin ortaya çıkmasına neden olabilmektedir. Politika ve prosedür eksikliğine ilişkin katılımcı görüşlerine dayalı riskler Tablo 3.11’de sunulmaktadır:

Tablo 3.11: Politika ve prosedür eksikliği riskleri

<i>Riskler (N=24)</i>	<i>Katılımcılar</i>
Yetki ve Sorumluluk Belirsizliği (N=4)	AU5, K1, K2, K5
Yanlış Uygulamalar (N=4)	AU1, AU2, AU6, K5
Belge Erişimi (N=2)	AU3, AU6
Elektronik ve Fiziksel Arşivleme Entegrasyonu (N=2)	K2, K13
İş Etkinliği (N=2)	K3, K10
Personel Hataları (N=2)	K7, K8
Sürdürülebilir Hizmet (N=2)	AU4, AU6
Bilgi Eksikliği (N=1)	AU7
Donanım ve Sistem Değişiklikleri (N=1)	AU3
Firma Bağımlılığı (N=1)	AU8
Kurumlar Arası Belge Entegrasyonu (N=1)	K12
Kurumsallaşamama (N=1)	AU1
Teknolojik İlerleme (N=1)	AU3

Tablo 3.11’de en sık dile getirilen risk unsurunun yetki ve sorumluluk belirsizliği (N=4) ile yanlış uygulamaların (N=4) ortaya çıkması olduğu görülmektedir. Belge erişimi (N=2), elektronik ve fiziksel arşivleme entegrasyonu (N=2), iş etkinliği (N=2), personel hataları (N=2), sürdürülebilir hizmetin sağlanamaması (N=2) risklerinin de politika ve prosedür eksikliğinden kaynaklanabilecek riskler arasında olduğu gözlemlenmektedir.

Öne çıkan yetki ve sorumluluk belirsizliği riskini katılımcı K1 şu şekilde açıklamıştır:

“EBYS bir uygulamadır ve bir otomasyon uygulamasıdır. Otomasyon uygulamaları da en başında doğru bir kurguyla yürütülmesi gereken uygulamalardır. Eğer sizin bir yönergeniz yoksa bu kurgu en başında değil ilerledikçe ortaya çıkar. Bu da işte tabii birtakım adaletsizlikler doğurabilir. Yanlışın yanlışla kapatılması gibi süreçler doğurabilir. O yüzden bu anlamda riskler taşır. Yani adı konulmamış süreçler farklı karar mekanizmalarımızın sürece dâhil olmasına sebep olur. Kimin karar vereceğinin belli olmadığı durumlarda sorumluluktan kaçma bir risktir, yetkisizlerin sorumluluk alması bir risktir, kurgunun bozuk yapılması geri dönülemeyen süreçlerde yani yazı gitmiş, mesela ama geri dönüp biz bir yönergeden destek almamışsak referans almamışsak böyle geri dönülmez sonuçlara yol açabilir. Böyle riskleri olur yani mutlaka bu EBYS işinin bir yönerge ya da bir prosedür altında yürütmesi lazım”

3.2.1.2.5. Yönetim Desteği

EBYS'nin, kurum genelinde etkin ve sürdürülebilir bir şekilde uygulanabilmesi, üst yönetimin sürece olan yaklaşımı ve desteğiyle doğrudan ilişkilidir. Yönetim desteği yalnızca karar alma süreçlerini değil, aynı zamanda kurum genelindeki işleyişi, personel tutumunu ve sistemin stratejik düzeyde benimsenmesini de etkilemektedir. Bu bağlamda, katılımcı görüşlerine dayalı olarak yönetim desteğinin yetersizliğine bağlı ortaya çıkabilecek riskler Tablo 3.12’de sunulmaktadır:

Tablo 3.12: Yönetim desteğine bağlı riskler

Riskler (N=24)	Katılımcılar
Sistemin Geliştirilmesi/Sürdürülebilirliği (N=4)	K3, K5, K11, K12
Desteğin Diğer Birimlere/Personele Yansıması (N=4)	K3, K10, K11, K13
Kurum Hizmetlerine Etkisi (N=2)	K2, K10
Politika Geliştirme (N=2)	K5, K8
Sistemin Yanlış İşletilmesi (N=2)	K4, K10
Yazışmaların Yanlış Yapılması (N=2)	K3, K5
Belge Bütünlüğü (N=1)	K7
Dijital Çöplük (N=1)	K9
Erişim (N=1)	K7
Geçerlilik (N=1)	K7
Güvenilirlik (N=1)	K7
Güvenlik (N=1)	K12

Hedeflere Ulaşma (N=1)	K2
Kurum İmajı (N=1)	K2

Tablo 3.12'deki veriler incelendiğinde, yönetim desteğine ilişkin en sık dile getirilen risklerin, sistemin geliştirilmesi ve sürdürülebilirliği (N=4) ile desteğin diğer birimlere/personele yansımaları (N=4) şeklinde ortaya çıktığı görülmektedir. Bu riskleri, desteğin kurum hizmetlerine etkisi (N=2), politika geliştirme eksikliği (N=2), sistemin yanlış işletilmesi (N=2) ve yazışmalarda yapılan hataların oluşturacağı risklerin (N=2) izlediği gözlemlenmektedir.

Katılımcı görüşleri, EBYS'nin sürdürülebilirliğinin büyük ölçüde üst yönetim desteğine bağlı olduğunu ortaya koymaktadır. En sık belirtilen risklerden biri olan sistemin geliştirilmesi/sürdürülebilirliği konusunda katılımcı K5, yönetim desteğinin yetersiz kalması durumunda sistemin sürdürülebilirliğinin ciddi biçimde tehdit altında olacağını belirtmiştir. Özellikle arşivleme alanında yaşanacak kapasite sorunlarına dikkat çeken katılımcı, mevcut kaynaklarla sistemin yalnızca belirli bir süre daha sürdürülebileceğini, uzun vadede fiziksel ve dijital kapasite sınırlarının süreci tıkayacağını ifade etmiştir. Katılımcılardan K11 ise üst yönetimin vizyoner yaklaşımının sistemin gelişimi açısından belirleyici olduğunu vurgulamıştır. Yönetimin projelere olumlu yaklaşması ve gerekli desteği sunması sayesinde ilerlemenin mümkün hale gelebileceğini vurgulamıştır.

Katılımcı K13, yönetim desteğinin sadece teknik değil, kurumsal etki yarattığını vurgulayarak desteğin diğer birimlere/personele yansımaları hususunu, *“Yönetim destekli bir EBYS projesi personelde işini daha iyi yapma ve EBYS birimi ile iş birliği içinde bir çalışmayı beraberinde getiriyor. Yeni programlara karşı personelde genelde bir direniş oluyor. Alıştıkları ve bildikleri konular içinde kendilerini güvende hissediyorlar. Programı önce yöneticiler sahiplenmeli ki personelini teşvik edebilsinler. Yoksa zaten personel sistemi, yeni gelecek uygulamaları vb. kullanmak istemiyor.”* şeklinde açıklamıştır. Benzer şekilde K3, yönetim desteğinin yalnızca teknik süreçleri değil, personel algısını ve kurumsal iletişim düzeyini de etkilediğini belirtmiştir. Katılımcıya göre basit bir eğitim bile üst yönetimin imzasıyla duyurulduğunda çalışanlar nezdinde daha fazla ciddiyet kazanmaktadır. Yöneticilerin desteği hem mali kaynakların sağlanmasında hem de diğer personel ve birimlerin projeye yaklaşımında belirleyici bir rol oynamaktadır. Katılımcı, aksi taktirde

EBYS'nin birimlerce önemsenmeyen sadece yazı yazılan bir sistem olarak görüleceğine vurgu yapmıştır. Bu doğrultuda, EBYS projelerinin kurumsal başarıya ulaşmasında üst yönetim desteğinin stratejik bir gereklilik olduğu ifade edilmelidir.

3.2.1.3. 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 bulgulara, sistem tasarım ve yapılandırma, sürdürülebilirlik ve süreklilik, bakım ve güvenlik uygulamaları, tedarikçi bağımlılığı, hukuki riskler, teknik riskler gibi risklerin olduğu görülmektedir. Bu bölümde, katılımcı görüşlerinden elde edilen veriler doğrultusunda sistem faktörüne bağlı riskler ele alınmaktadır.

3.2.1.3.1. Sistem Tasarım ve Yapılandırma

EBYS'nin tasarım ve yapılandırma sürecinde akademisyenler/uzmanlar ve firma temsilcileriyle gerçekleştirilen görüşmelerden elde edilen risklere ilişkin veriler Tablo 3.13'te sunulmaktadır:

Tablo 3.13: Sistem tasarım ve yapılandırma riskleri

<i>Riskler (N=26)</i>	<i>Katılımcılar</i>
Kurumsal Analiz Eksikliği(N=7)	AU1, AU4, AU5, AU7, AU8, F1, F2, K2,
Firmaya Gelen Kurum Talepleri (N=3)	F1, F2, F3
Firma Bağımlılığı (N=3)	AU2, AU4, AU5
EBYS Ekibinin Yetkinliği (N=3)	AU1, AU2, AU4
Yazılım Mimarisi Geliştirme Süreci (N=2)	F1, F2
Dijital Dönüşüm (N=2)	AU1, AU3
Sistemler Arası Entegrasyon (N=2)	F1, F2
Fonksiyon Değişikliği (N=1)	AU7
Ara Yüz (N=1)	AU5
Rekabet Ortamının Sağlanamaması (N=1)	AU1
Uygulama Birliğinin Sağlanamaması (N=1)	AU1

Tablo 3.13'de en sık belirtilen riskin, kurumsal analiz süreçlerindeki yetersizlik (N=7) olduğu görülmektedir. Bunu kurumların firmalara yönelttiği talepler (N=3), firma

bağımlılığı (N=3) ile EBYS ekibinin teknik ve yönetsel yeterliliği (N=3) risklerinin takip ettiği anlaşılmaktadır. Yazılım mimarisi geliştirme süreci (N=2), sistem entegrasyonu (N=2) ve dijital dönüşüm (N=2) gibi hususların da sistem tasarım ve yapılandırma riskleri arasında olduğu gözlemlenmektedir.

En sık dile getirilen risk olan kurumsal analiz eksikliğini AU4: *“Sistemi yapılandırmada modellemenin çok iyi yapılması gerekir. Modüllerin yerinde ve gerektiği şekilde tasarlanması çok önemlidir. Hazır paket EBYS uygulama yazılımlarının temininde sistem uygulanacağı kuruma göre yeniden tasarlanıp yapılandırılmalı. Kurum kültürü, organizasyonel yapı, yetkiler, fonksiyon ve iş süreçleri o örgütün kurum kültürü, iş yapma stratejisi ve iş modeline göre tekrar gözden geçirilmeli. Bu süreç satın alma sözleşmesinde çok akıllıca tasarlanıp yazılmalı. Aksi halde satın alınan ama uygulanamayan bir programla yüz yüze kalma riski hep olacaktır”* şeklinde açıklamıştır. Konuyla ilgili açıklama yapan F1:

“Tasarımın kurulum aşamasında detaylı yapılmamasından dolayı güncel kullanımlarda değişiklik talepleri geldiğinde bunların karşılanması kimi durumlarda mümkün olamıyor. Buradaki neden ise olacak etki tüm sistemi etkileme ihtimalidir. Belge tanımlamalarının kurum kültürü oturtularak net çizgilerle belirlenmemesi de kullanım aşamalarında sorunlar oluşturuyor.” İfadelerini kullanmıştır.

Firma etkisi, sistem tasarımı ve yapılandırma sürecinde öne çıkan önemli risk alanlarından biri olarak değerlendirilmektedir. Katılımcılardan AU4, hizmet alan kurumlarda EBYS konusunda yetkin personel eksikliğinin, sistemin kurulum ve işletim süreçlerini büyük ölçüde tedarikçi firmanın inisiyatifine bıraktığını belirtmiştir. Bu durumun, firmanın sistemi teknik gereklilikler ve standartlardan ziyade kendi önceliklerine göre şekillendirmesine yol açtığını vurgulamıştır. Bunun sonucunda ise kurumun ihtiyaçlarını karşılamayan planların sisteme entegre edildiğini ve çok yönlü risklerin ortaya çıktığını söylemiştir. Diğer yandan AU2 bu riski daha doğrudan bir ifadeyle şu sözlerle açıklamıştır: *“Birçok yazılım firması vardı, kimi yürütemedi iflas etti, kimi çok az kurumla iş yapıyor, kimisi de el değiştirdi. Bunlar kurumlar için çok büyük risk. Kurumun kullandığı firmanın değişmesi, belgelerin sürdürülebilirliği, kullanıcı erişim yetkilerinin yeniden tasarlanması gibi birçok riski beraberinde getirir.”*

3.2.1.3.2. Sürdürülebilirlik ve Süreklilik

EBYS'lerin sürdürülebilirliğini tehdit edebilecek, belgelerin uzun vadede kullanılabilirliğini etkileyebilecek riskler akademisyenler/uzmanlar ve kurumlardan alınan cevaplar doğrultusunda Tablo 3.14'te verilmektedir:

Tablo 3.14: Sürdürülebilirlik ve sürekliliğe ait riskler

<i>Riskler (N=33)</i>	<i>Katılımcılar</i>
Teknoloji (N=7)	AU3, AU5, AU7, K2, K9, K11, K13
Kurumsal Sorumluluk (N=6)	AU7, K4, K5, K7, K8, K10
E-imza Durumu (N=3)	K2, K4, K13
Firma Bağımlılığı (N=2)	AU4, AU8
Yetkin Personel (N=2)	AU7, AU8
Maliyet (N=2)	K9, K10
Yetkili Kurumların Sorumluluğu (N=2)	K2, K11
Belge Saklama Formatındaki Belirsizlik (N=2)	K2, K4
Bilgi/Bilinç Eksikliği (N=1)	AU3
Veri Güvenliği (N=1)	AU4
Nitelikli Üstveri (N=1)	AU7
Eğitim (N=1)	AU7
Firmalar Arası Rekabet (N=1)	AU8
Firmanın Yetkinliği (N=1)	K3
Bütünlüğün Bozulması (N=1)	K2

Tablo 3.14 incelendiğinde, katılımcılar tarafından EBYS'nin sürdürülebilirliğini ve sürekliliğini tehdit konusunda en çok dile getirilen risk alanının teknoloji (N=7)' olduğu, bunu kurumsal/yönetimsel sorumlulukların (N=6) takip ettiği görülmektedir. E-imza uygulamalarındaki riskler (N=3), tedarikçi firmalara olan bağımlılık (N=2), yetkin personel eksikliği (N=2), maliyet (N=2), yetkili kurumların rehberlik ve denetim sorumluluğu (N=2) ve belge saklama formatındaki belirsizlik (N=2) hususları da dikkat çeken riskler arasındadır.

Katılımcı görüşleri, teknolojiye bağlı sürdürülebilirlik risklerinin özellikle teknolojik eskime, dijital ortamın kırılganlığı ve uzun vadeli erişilebilirlik gibi başlıklarda yoğunlaştığını ortaya koymuştur. AU5, bu durumu şu sözlerle açıkça ifade etmiştir: *“En önemli risk faktörü burada EBYS'lerin dijital ortamda olması aslında. Çünkü*

dijital ortam biraz daha kırılğan fiziksel ortama göre. Belli yıl sonra EBYS’de PDF’leri görüntüleyebileceğiniz konusunda şüpheler var. Mesela teknoloji eskimesi diye bir tabir vardır. Burada özellikle belgelerin hem PDF görüntüsü hem üstverilerinin hiçbir şekilde bozulmadan saklanmasına dair bir güvenilirlik garantisi şu an yok. Çünkü sürekli yazılımlar değişiyor, güncelleniyor. 20, 30 yıl sonra word ya da pdf diye bir şey kalmayabilir. Bu durumda da özellikle tarihi araştırmacılar ve hukuki anlamda geriye dönük araştırmalar için EBYS’lerin bu ilk oluşturulduğu andaki gibi uzun süreli korunmasını sağlanması lazım.” Bu görüş, dijital belgelerin uzun vadeli erişilebilirliğine yönelik teknolojik güvencelerin yetersizliğini açıkça ortaya koymaktadır. Katılımcılardan AU7, sürdürülebilirliğin sağlanamamasını iyi teknolojik koşulların tesis edilememesi ile ilişkilendirerek bu durumu doğrudan bir risk olarak değerlendirmiştir. Benzer şekilde K11, belge formatlarının zaman içinde geçerliliğini yitirme olasılığına dikkat çekmiş, K9 ise depolama teknolojilerindeki hızlı değişimin kurumları sürekli donanım yenilemeye zorladığını ve bunun da teknik ve mali boyutlarıyla sürdürülebilirliği tehdit ettiğini ifade etmiştir.

3.2.1.3.3. Tedarikçi İlişkilerindeki Riskler

Günümüzde çoğu kurum ve kuruluş kendi EBYS yazılımını geliştirip kullanmak yerine tedarikçi bir firmadan temin yoluna gitmektedir. Bu sistemlerin kurulum, entegrasyon, işletim, bakım gibi süreçlerde dış tedarikçilerle yürütülen iş birliği, çeşitli risk unsurlarını beraberinde getirmektedir. EBYS tedarikçileriyle yaşanabilecek risklere ilişkin bulgular kurum temsilcilerinden alınan cevaplar doğrultusunda Tablo 3.15’te sunulmaktadır:

Tablo 3.15: EBYS tedarikçi ilişkilerindeki riskler

<i>Riskler (N=19)</i>	<i>Katılımcılar</i>
Zamansal Sorunlar (N=4)	K2-K4, K6
Versiyon Geçişleri (N=3)	K7, K10, K12
Yönetici Talepleri (N=2)	K5, K10
Belge Güvenliği (N=2)	K3, K8
Firma Bağımlılığı (N=2)	K2, K3
Kurumun Uzman Personel Durumu (N=2)	K1, K2
Firmanın Yetkinliği (N=1)	K3

Firmanın Sürdürülebilirliği (N=1)	K10
Süreç Yönetiminin İşletilmemesi (N=1)	K2
Maliyet (N=1)	K2

Tablo 3.15’te, zamansal sorunlar (N=4), versiyon geçişleri (N=3) yönetici talepleri (N=2), belge güvenliği(N=2), firma bağımlılığı (N=2) ve kurum içinde yeterli düzeyde uzman personel bulunmaması (N=2) unsurlarının EBYS tedarikçileriyle olan ilişkilerin ortaya çıkardığı riskler arasında yer aldığı görülmektedir.

Katılımcı görüşleri, tedarikçi firmalarla yürütülen süreçlerde karşılaşılan zamansal problemlerin, özellikle firmaya iletilen taleplere geri dönüşün hızlı olamamasından kaynaklandığı yönündedir. K12 bu durumu “*Zamansal sorunlar yaşıyabiliyoruz. Onlar çok fazla aktif çalışıyorlar. Başka kurumlarla da şirketlerle de çalışıyorlar. Bazen anında erişim sağlayamayabiliyoruz.*” şeklinde açıklamıştır. Bu ifade, tedarikçi firmaların aynı anda birçok kurumla çalışıyor olmasının, kurumların acil müdahale ya da destek ihtiyaçlarında gecikmelere neden olabildiğini ve bunun da EBYS süreçlerinin kesintiye uğramasına yol açabilecek bir risk unsuru oluşturduğunu göstermiştir.

Katılımcılar versiyon geçiş süreçlerinde ise gecikmeler, teknik uyumsuzluklar, çalışan bir fonksiyonun çalışmaması gibi durumlarla karşılaştıklarını ve bu durumların sistem sürekliliğini olumsuz etkilediğini belirtmiştir. Bu durum versiyon geçişlerinin iyi planlanmadığı ve kurumsal ihtiyaçlarla yeterince uyumlu yürütülmediği durumlarda önemli riskler oluşturduğuna işaret etmektedir.

3.2.1.3.4. Teknik Riskler

Belgelerin elektronik ortamda yönetilmesini sağlayan EBYS, teknolojik bir yapıya sahip olmasından dolayı içerisinde çeşitli teknik riskler barındırmaktadır. Yapılan görüşmelerde kurum temsilcilerine, kullandıkları sistemlerde yaşadıkları teknik riskler sorulmuş ve elde edilen veriler Tablo 3.16’da sunulmaktadır:

Tablo 3.16: Yaşanan teknik riskler

<i>Riskler (N=13)</i>	<i>Katılımcılar</i>
Yavaşlamalar (N=7)	K2-K5, K9, K10, K13
Güncelleme Sonrası Hata (N=2)	K6, K12
E İmza Kaynaklı Sorunlar (N=2)	K4, K12

Belgelerin Askıda Kalması (N=1)	K3
Erişim Sorunu (N=1)	K8

Tablo 3.16 incelendiğinde en sık dile getirilen risk unsurunun yavaşlamalar (N=7) olduğu görülmektedir. Güncelleme sonrası hata (N=2) ve e-imza kaynaklı sorunların (N=2) da teknik riskler arasında bulunduğu anlaşılmaktadır.

Firma temsilcisi katılımcılar ise konuya başka açıdan yaklaşmıştır. Firmalara EBYS tasarım, geliştirme gibi süreçlerde karşılaşılan risklerin neler olabileceği sorulmuştur. Firmalar teknik sorunların genellikle kısa sürede çözüme kavuşturulabildiğini ancak asıl tehdit oluşturan ve gelecekte yaşanması muhtemel risklerin bulunduğunu ifade etmiştir. Bu risklerin, elektronik arşivleme belirsizliği, bütünleşik yapılaşmanın sağlanamaması, insan faktörü ve veri güvenliğinin sağlanamaması gibi unsurlar olduğunu belirtmiştir.

3.2.1.3.5. Mevzuat/Standartlarla Uyum ve Hukuki Riskler

Akademisyenler ve uzmanlardan, uluslararası belge yönetimi standartlarının Türkiye’de benimsenmesi ve Türkiye’deki kurumların mevzuat ile standartlara uyum sağlaması konusunda karşılaşılabilecek riskler hakkında görüşleri alınmış ve bu görüşlere ilişkin veriler Tablo 3.17’de sunulmaktadır:

Tablo 3.17: Hukuki riskler

<i>Riskler (N=23)</i>	<i>Katılımcılar</i>
Uluslararası Belge Yönetim Standartlarının Uyarlanması (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
Veri Gizliliği (N=1)	AU7
Yanlış Uygulamalar (N=1)	AU1
Elektronik Arşiv Belirsizliği (N=1)	AU1
Uzun Süreli Koruma (N=1)	AU1

Tablo 3.17’de, en sık dile getirilen riskin uluslararası belge yönetim standartlarının uyarlanmasıyla (N=7) ilgili olduğu görülmektedir. Bu konuya değinen katılımcılar, Türkiye’deki kurumların bu standartlara uyum sağlayamadığını, böyle bir çabalarının

da genellikle olmadığını belirtmiştir. Tablo 3.17’de 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 standartlarının uyarlanması konusunda katılımcılardan AU8, bu standartların ülkemizde uluslararası düzeyde beklenen değeri taşımadığını düşünmektedir. 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. Ayrıca ülkemizde mevzuatın bu konuda yeterli olmadığına ve birçok noktada açıklıkların bulunduğuna dikkat çekmiştir. Elektronik imza kanununda elektronik imzanın ıslak imzayla aynı hukuki değere sahip olduğuna dair açık maddeler bulunmasına rağmen bazı süreçlerin bu kapsamda değerlendirilemediği ve denetimsel süreçlerde eksikliklerin devam ettiğini düşünmektedir. Bu durumun uluslararası standartların etkin bir şekilde uyarlanmasının önünde önemli bir engel teşkil ettiğini ve bu görüşler doğrultusunda mevzuatın geliştirilmesi gerektiği vurgulanmıştır.

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 yönetiminin süreç yönetimiyle ve mevzuatla ilişkilendirdiğini, farklı mevzuatlara tabi süreçlerin ortaya çıkardığı belgelerin niteliğinin değiştiğini vurgulamaktadır. Ancak pratikte kurumların farklı belge grupları için aynı tür üstverileri kullandığını, oysa kanunun farklı üstveriler talep ettiğini dile getirmiştir. Katılımcı, kanun tipolojisine göre hareket ederek hangi mevzuatın hangi tür bilgiyi istediğinin tespit edilmesi gerektiğini ve üstverilerin 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 resmi olarak tanınmadığını belirtmiştir.

Katılımcı, bu durumun özellikle Devlet Arşivleri'ne intikal eden belgelerde delil niteliği açısından sorunlar yaratacağını, hukukun önerdiği formatları kullanmadıkları için format bazlı problemlerin ortaya çıkacağını vurgulamıştır. Bu bağlamda belge formatları ile mevzuat uyumunun delil değeri açısından önemli risk unsurları arasında olduğunun altını çizmiştir.

Katılımcılardan AU1 ise belgenin delil değeri riskini şu şekilde açıklamaktadır: *“Mevcut durumda EYP 2.1 sürümünün yürürlükte ve bu sürüme göre paket oluşturuluyor. Paketler karşı tarafa iletiliyor, karşı taraf aynı API'yi kullanarak sistemi açıp okuyabiliyor ve böylece belgelerin bütünlüğü ile delil değeri korunmaya çalışılıyor. EYP birçok fırsat sunuyor. Ancak arşiv boyutunda yeterli olmadığını düşünüyorum. Dijital Dönüşüm Ofisindeki yetkililerin de aynı görüşte olduğunu ve arşiv imzası için daha uzun süreli koruma sağlayabilecek yeni bir paket hazırlığı içinde olduklarını biliyorum. Bence Türkiye’de elektronik arşiv kurulum çalışmaları henüz emekleme aşamasında ve kurumlar bunu yeni yeni entegre etmeye başladı. Kurumsal arşivler, şu anda daha çok depo işlevi görüyor, belgelerin nasıl yönetileceği, korunacağı ve uzun vadede erişilebilir kılınacağı konuları henüz kurumlar tarafından yeterince sorgulanmıyor. Ancak akademik çevrelerde bu sorular gündemde. Belgelerin delil değerinin bozulması ve kurumların belgeleri uzun süreli koruyamaması gibi birçok risk var. Bu durum belgelerin işlevini yitirmesine yol açabilir ve dolayısıyla kurumların ellerindeki belgeler işlevsiz hale gelebilir. Delil değerini ve belge niteliğini koruyamamak, arşiv belgesinin sahip olması gereken belli üstveriler ve paket bileşenleri nedeniyle hukuki açıdan riskler doğurur.”*

Katılımcı AU7, e-imza güvenliğiyle ilgili risklerin özellikle SHA (Secure Hashing Algorithm) algoritmalarının güncellenmesi gerektiğini belirtmiştir. Katılımcı, Kamu Sertifikasyon Merkezi'nin (Kamu SM) bu süreci takip edip uyguladığını, ancak Kamu SM'nin işlevini geçici olarak yerine getirememesi halinde elektronik imza sisteminin çökebileceğini ve ciddi sorunlar ortaya çıkabileceğini vurgulamıştır. Ayrıca elektronik imza sağlayıcılarının sahte kimliklerle ya da kişinin haberi olmadan elektronik imza oluşturduğu ve bunun sahtecilik riski yarattığını belirtmiştir. Katılımcı, 15 Temmuz darbe girişimi sırasında, bir belediyede benzer olayların yaşandığına dikkat çekmiş ve kamuda bu tür risklere karşı ciddi bir teyakkuz bulunduğunu ifade etmiştir. İmza güvenliği alanındaki bu risklerin önemli bir tehdit oluşturduğunu da eklemiştir.

AU3 uzman personel eksikliği konusunda, hukukun teknolojinin hızına şu an yetişme imkânı bulunmadığını ifade etmiştir. Hukuki düzenlemelerin esnek olması gerektiğini ve bu çerçeveyi belirleyerek hukukçulara yol gösterecek unsurun belge yöneticileri olduğunu belirtmiştir. Ayrıca alanda uzman personel eksikliğin mevcut olduğunu da vurgulamıştır. Katılımcılardan AU7 veri gizliliğinin hukuki boyutunu şöyle açıklamıştır:

“Veri gizliliği kısmında şöyle düşünelim, Merkez Bankası’nda çalışıyorsunuz ve banka bir değerlendirme yapıyor. Merkez Bankası’nın iç değerlendirmeleri tutarlıdır, yani kendi içinde az çok bir şeyi belli eder. Dedi ki bunun da gizli kalması gerektiğini düşünelim. Yani sadece işte beş kişinin okuması gerek. Dolar dedi, elli lira olacak diye düşünüyoruz ya da işte yatırım düzenleyecekler, diyorlar ki şu hisse çok artacak, biz bu hisseyi alalım. Siz de bu bilgiye, kamu görevinden dolayı vakıf olmamanız gereken bir bilgiye sahip oldunuz. Kendinizi de tutamadınız diyelim ve gittiniz o hisseyi satın aldınız, buradan çıkar da elde etmiş oluyorsunuz. Ve bu veri gizliliğini sağlamazsak, işin böyle de bir sıkıntılı tarafı var. Benzer durum Sağlık Bakanlığı’nda yaşandı. Nasıl yaşandı? Sağlık Bakanlığı e-Nabız’ı Türk bir firmaya yazdırıyor, Türk firmanın elinden daha sonra alıyorlar, bu e-Nabız’ı ya Katarlı ya Dubaili bir firmaya satıyorlar. Daha sonra Türk firma tabii itiraz ediyor; “Sen misin itiraz eden?” deyip Türk firmaya dava açıyorlar, e-Nabız’daki bilgileri işte edinip oradan haksız kazanç elde ettiler diye. Bu veri gizliliğinden tabii bağımsız bir durum, biraz politik de bir durum, yani gruplar arası diyelim politik bir mesele ama sonuçta bunun veri gizliliği ayağı da var. Çünkü e-Nabızlılar da kendi geliştirdikleri program olduğu için silmemişler. Sağlık Bakanlığı diyor ki, “Sen kendin geliştirmiş olabilirsin ama bunu da silmen lazım,” diyor. Belki bunun bir veri gizliliğine ya da veri değerlendirmesine tabi tutabiliriz. Burada böyle bir sıkıntımız var; buna da tabii dikkat etmek lazım, böyle bir risk var. Yani bugün riski nasıl adlandırabiliriz? Kişinin sahip olmaması gereken bilgiye erişme riski olarak ifade edebiliriz. Gizlilikte bu açıdan önemli.”

3.2.1.3.6. Bakım ve Güvenlik Riskleri

EBYS’lerin güncelliğini ve performansını etkileyen bakım ile sistemdeki bilgi ve belgelere yetkisiz erişime yol açabilecek güvenlik riskleri katılımcılardan elde edilen veriler doğrultusunda Tablo 3.18’de sunulmaktadır:

Tablo 3.18: Bakım ve güvenlik riskleri

<i>Riskler (N=39)</i>	<i>Katılımcılar</i>
Veri Güvenliği (N=10)	F1, F2, K2-K5, K7-K9, K12
Yedekleme ve Geri Yükleme Riskleri (N=8)	
<i>Veri Kaybı (N=3)</i>	AU5, K2, K12
<i>Hizmet Kesintisi (N=3)</i>	K2, K3, K12
<i>Fiziksel Cihazların Deforme Olması (N=2)</i>	K3, K9
Alt Yapı (N=4)	AU1, AU4, AU5, AU7
Güven Kaybı (N=2)	K7, K13
Teknik Şartname (N=2)	F1, AU8
İnsan Faktörü (N=2)	F1, AU3
Belge Bütünlüğü (N=1)	K2
E-imzanın Paylaşılması (N=1)	K6
Hizmet Aksaması (N=1)	K7
Veri Kaybı (N=1)	F2
İmzalama Süreci (N=1)	F2
Firma Bağımlılığı (N=1)	AU8
Maliyet (N=1)	AU8
Firma Değişikliği (N=1)	AU7
Bakım Süreçlerinin Dokümantasyonu (N=1)	AU7
Firmanın Güvenilirliği (N=1)	AU5
Versiyon Geçişleri (N=1)	AU1

Tablo 3.18’ye göre, bakım ve güvenlik risklerinin başında veri güvenliği (N=10)’nin geldiği görülmektedir. Bunu yedekleme ve geri yükleme ile ilgili risklerin (N=8) takip ettiği ve bu risk kategorisinin altında veri kaybı (N=3), hizmet kesintisi (N=3) ve fiziksel cihazların deforme olması (N=2) unsurlarının yer aldığı izlenmektedir. Ayrıca altyapı (N=4) ile ilgili sorunlar da bakım ve güvenlik riskleri arasındadır.

Katılımcılardan F1 veri güvenliği riskini “*Kullanıcı erişim ve izinlerindeki eksiklikler sistemi bütüncül olarak tehdit eder. Bu noktada yetkilendirme yapan personelin dikkatli ve liyakatli olması gerekir. Log kayıtlarının da detaylı olması önemlidir. Olumsuz durumlar veri güvenliği için tehlike oluşturur. Kurum içi hiyerarşide de kargaşa meydana getirebilir.*” şeklinde ifade ederken K9 “*EBYS’ler de diğer*

uygulamalar da yetki bazlı çalışıyor. Yetkiniz yoksa herhangi bir belgeye herhangi bir klasöre erişme şansınız yok. Ama zaman zaman karşılaşıyoruz. Biz kullandığımız yazılımda karşılaştık mesela geçen bir arkadaş geldi bir sorgulama yapmış dünyanın belgesi görmüş, bu ne böyle dedim. Sistemsal birtakım takılmalar olabiliyor ama onun çözümü de yok. O anda neden kaynaklanıyor bilemiyoruz. Yani veri sızıntısı veya güvenlikle alakalı sıkıntı olabiliyor. Yani yetkisi olmayan insanlar belgeleri görebiliyor bazen” şeklinde açıklamıştır.

3.2.1.3.7. Saklama Gereksinimlerinin Yetersizliği

EBYS’deki belgelerin uzun süre belge özelliklerinin korunarak muhafaza edilmesi yasal ve idari açıdan gerekli bir durumdur. Saklama gereksinimlerinin yetersiz olması birçok riski beraberinde getirir. Sistemdeki saklama gereksinimlerinin yetersizliğinin meydana getirebileceği riskler, kurum temsilcileriyle yapılan görüşmelerden elde edilen veriler doğrultusunda Tablo 3.19’da sunulmaktadır.

Tablo 3.19: Sistem saklama gereksinimleri yetersizliğinin oluşturduğu riskler

Riskler (N=30)	Katılımcılar
Belgeyi Gereksiz Saklama (N=5)	K2, K5, K7, K8, K13
Mevzuatsal Belirsizlik (N=4)	K3, K5, K6, K10
Yanlış İmha (N=4)	K2, K7, K12, K13
Belgelerin Yanlış Yerde Dosyalanması (N=3)	K2, K10, K13
Ayıklama-İmha İşlemlerinde Zorluk (N=3)	K1, K2, K11
Maliyet (N=2)	K4, K8
Belge Transfer Sorunu (N=2)	K7, K8
Hukuki Sonuçlar (N=2)	K2, K10
Arşiv Şişmesi (N=1)	K13
Arşivlemenin Yapılamaması (N=1)	K12
Sürdürülebilirlik (N=1)	K3
Erişim (N=1)	K3
Belge Bütünlüğünün Bozulması (N=1)	K3

Tablo 3.19’deki veriler incelendiğinde, belgeyi gereksiz saklama (N=5), mevzuatsal belirsizlik (N=4), yanlış imha (N=4), belgelerin yanlış yerde dosyalanması (N=3),

ayıklama-imha işlemlerinde zorluk yaşanması (N=3) gibi durumların belirtildiği görülmektedir.

Katılımcılara göre, sistemde yalnızca kısa süreli saklanması gereken belgelerin, gereksiz yere uzun süre tutulması önemli bir risk oluşturmaktadır. Bu durum, sistemdeki disk kapasitesinin hızla dolmasına yol açmakta ve sürekli olarak disk büyütme ihtiyacı doğurmaktadır. Bu tarz riskler, sistemde gereksiz belgelerin uzun süre saklanmasıyla ortaya çıkmakta ve verimli bir saklama süreci sağlanamadığında, disk kapasitesinin aşılması gibi sorunlarla karşılaşılabilir.

Mevzuattaki belirsizlik riskini katılımcı K3 *“EBYS’lerde belge saklamadan ziyade arşivin, arşiv nete aktarılması söz konusu fakat onda da biz Devlet Arşivleri’ni bekliyoruz. Biraz da onlar standart belirleyecekler, biz de ona istinaden yol alacağız. Mesela TIFF mi olacak PDF mi olacak? TIFF çok yer kaplıyor arşiv nette yaşadık. Hangi formatta saklayacaksın ne kadar saklayabileceksin çünkü saklama kapasiteleri de arttıkça maliyeti de artacak”* şeklinde ifade ederken katılımcı K10 *“saklama süreleri belli ama imha süreçleriyle ilgili şu anda hiçbir kurumda bu imha süreçleri çalıştırılmadı. Hala bütün kurumların benim bildiğim verileri elektronik ortamda duruyor. Nedenlerden bir tanesi de Devlet Arşivleri Başkanlığı’nın şu anda bunların nasıl tasnif edileceğine yönelik bir yönetmelik ya da şeyi yok. Burası boşlukta.”* şeklinde ifade etmiştir.

3.2.1.4. Belge Yönetim Sürecine Bağlı Riskler

Belge yönetimi, kurumların günlük iş süreçlerinde oluşturdukları, faaliyetlerin deliliği niteliğindeki belgelerin format, içerik, ilişkisel özelliklerin korunarak bu belgelerin üretiminden nihai tasfiyesine kadar olan süreçte yönetilmesini içermektedir (Türkiye Bilişim Derneği, 2009). Katılımcılardan elde edilen bulgular doğrultusunda, belge yönetim sürecinde karşılaşılan riskler bu bölümde verilmektedir.

3.2.1.4.1. Belge Üretim Sürecindeki Riskler

Belge üretim süreci, doğru ve tutarlı verilerin kaydedilmesi açısından önemli bir aşamadır. Bu sürecin etkin bir şekilde yönetilmesi, sonraki belge saklama, erişim, güvenlik ve yönetim süreçlerinin sağlıklı bir şekilde işlemlerini sağlamaktadır. Katılımcılardan elde edilen bulgular, bu süreçte belirli risk unsurlarının ortaya çıkabileceğini göstermektedir. Özellikle, üstveri ve üstveri alanlarından biri olan SDP hataları, önemli risk faktörleri arasında yer almaktadır. Üstveri hatalarının

oluşturabileceği risklere ilişkin katılımcı görüşlerinden elde edilen veriler Tablo 3.20’de yer almaktadır:

Tablo 3.20: Üstveri riskleri

<i>Riskler (N=14)</i>	<i>Katılımcılar</i>
Erişim (N=4)	F3, AU1, AU3, AU8
Süreç Yönetimini Sağlayamama (N=2)	AU7, F3
İş Sürecinin Aksamaması (N=2)	AU1, F1
Belge Özelliğinin Sağlanamaması (N=1)	AU8
Personel (N=1)	AU7
Mevzuata Uymama (N=1)	AU7
Üstveri Şemasının Olmaması (N=1)	AU7
Belge Türüne Göre Üstveri Eksikliği (N=1)	AU7
Bütünlük (N=1)	AU4

Tablo 3.20’e göre, en sık dile getirilen üstveri riskinin belge erişimi (N=4) olduğu görülmektedir. Süreç yönetimini sağlama konusunda yaşanan zorluklar (N=2) ve iş sürecindeki aksaklıklar (N=2)’ın bunu takip ettiği izlenmektedir. Diğer yandan, belge özelliğinin sağlanamaması (N=1), personel (N=1) ve mevzuata uyumsuzluk (N=1), üstveri şemasının olmaması (N=1), belge türüne göre üstveri eksikliği (N=1), belge bütünlüğünün sağlanamaması (N=1) gibi unsurların da üstveri yönetiminde karşılaşılan diğer riskler arasında olduğu anlaşılmaktadır.

Belge üretim sürecinde kullanılan ve üstveri alanlarından biri olan SDP, sadece konu kodu olarak kullanılmamaktadır. Belge saklama süreleri ile doğrudan ilişkisi bulunan bu kodlar, dosyalama ve tasfiye işlem tanımlarını belirleme gibi önemli özelliklere sahiptir. Bu bağlamda katılımcılara standart dosya planına uyulmamasının oluşturabileceği riskler sorulmuş ve elde edilen veriler Tablo 3.21’de sunulmuştur:

Tablo 3.21: SDP hata riskleri

<i>Riskler (N=53)</i>	<i>Katılımcılar</i>
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=9)	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
Kontrollü Sözlük (N=2)	AU7, AU8
Bütünlük (N=2)	AU4, K7

Tablo 3.21’e 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=9), hukuki riskler (N=8) gibi kurumların hesap verilebilirliğini etkileyecek durumların ortaya çıkabileceği görülmektedir.

SDP hatalarına neden olan unsurlara ilişkin katılımcı görüşleri Tablo 3.22’de verilmektedir:

Tablo 3.22: SDP hata nedenleri

<i>Riskler (N=23)</i>	<i>Katılımcılar</i>
Personel (N=7)	AU1, AU4, AU5, K1, K7, K10, K13
Denetim/Kontrol Eksikliği (N=7)	AU4, AU5, K1, K5, K11-K13
Kurumun Çözüm Eksikliği (N=4)	AU3, AU7, K11, K13
Kontrollü Sözlük (N=3)	AU5, AU7, AU8
Dosya Planı Uygulanmaması (N=1)	AU7
Planın Güncelliği (N=1)	AU4

Tablo 3.22’ye göre dosya planı hatalarının çoğunlukla personel (N=7) ve denetim/kontrol eksikliği (N=7)’nden kaynaklandığı görülmektedir. Bu durum personelin bilgisiz veya ilgisiz olduğunu ve bu süreçlerin bir kontrol mekanizmasından geçmediğini göstermektedir. Ayrıca kurumun çözüm eksikliği (N=4) ve kontrollü sözlüğün olmaması (N=3) SDP hatlarına neden olan durumlar arasındadır.

Katılımcılardan AU7 üstveri ve standart dosya planı ile ilgili şu açıklamayı yapmıştır: “Belge yönetiminde üstveri ve standart dosya planı eksiklikleri önemli riskler doğurur. Ülkemizde özellikle, belge türüne özgü üstveriler yok. Bu aslında mevzuatın gerektirdiği bilgilerin eksik olmasına neden oluyor. Bir de bu eksiklikler yüzünden belge oluşturma sürecinde hata yapılıyor. Bu durum belgelerin doğru şekilde üstverilerle üretilmemesine yol açıyor. Diğer bir unsur yani bu risklere neden olan durum, kontrollü sözlüklerin olmaması ile ilgilidir. Örneğin, personel dosyaları gibi belirli dosya kodlarının doğru şekilde atanamaması, verilerin yanlış kaydedilmesine

sebepler oluyor. Ayrıca dosya planı uygulamalarındaki eksiklikler de ciddi sorunlar yaratıyor. Birçok kurumda dosya planı yok ya da doğru kullanılmıyor ve bu eksiklik nedeniyle belgelerin hangi dosyayla ilişkilendirileceği ve ne kadar süreyle saklanacağı belirsiz. Bu da belgelerin doğru şekilde arşivlenmemesine, saklama sürelerinin belirlenememesine ve dosya grubunun yönetilememesine neden oluyor. Ayrıca dosya planı uygulamaları eksik olduğunda, farklı formatlara geçişte de belgenin içeriğiyle uyumsuzluk yaşanır ve bu, belgenin delil değeri üzerinde olumsuz etkiler yaratır. Bu tür riskler, belgelerin yönetimi ve güvenliği açısından önemli tehditler oluşturur. Yani bir dosya planı birçok riske neden olur.”

Katılımcılara göre, üstveri ve SDP yönetimi ile erişim arasında önemli bir ilişki bulunmaktadır. AU3, bu sürecin en büyük riskinin gelecekte hukuki eksikliklere yol açması olabileceğini belirtmiş ve üstveri yönetimi ile dosya planı uygulamalarındaki eksikliklerin, belgelerin erişilmesini zorlaştırabileceğini vurgulamıştır. K13 ise, EBYS üzerinde kayıt altına alınan her belgenin doğru bir doküman tipiyle ilişkilendirilmesi gerektiğini ifade etmiş, aksi takdirde belgelerin dijital arşivde erişilemez hale geleceğinin altını çizmiştir.

Tasfiye sürecindeki riskleri K6 “Dosya planı tanımlama belge üretirken önemli değilmiş gibi gözükse de belgenin erişimini, saklanmasını ve imhasını etkileyen bir şey. Bu yüzden çok önemli. Yanlış, eksik olması belgenin yok olmasına kadar gidebilir.” şeklinde ifade ederken K9 “Şu ana kadar bildiğim kadarıyla hiçbir kurumda elektronik belgeler üzerinde bir ayıklama imha yapılmadı. Elektronik imza kanunu 2005’te çıktı, 2025 oldu 20 sene geçti. Saklama planına baktığımız zaman 5 sene 10 sene gibi kavramlar var. Bu 5 sene 10 sene olanların imha edilmesi lazım. Hiçbir kurumda ben duymadım bununla ilgili bir çalışma da yok. Çünkü kimse güvenemiyor. Fiziksel belgeye masanın üstünde yayıyorsunuz, bu önemliymiş ya buraya koymuş ama bunu ayırayım diyorsunuz. Yani sistem ne yapacak 060, 5 sene sonra imha bütün 060’lar getirecek ama o kod gerçekten 060 mı değil. Onun için kimse cesaret etmiyor. Biraz da cesaret de etmesinler” şeklinde açıklamıştır.

Yanlış imha konusu ile ilgili olarak AU5, bu durumun çok büyük sıkıntılara yol açabileceğini ve yanlış dosya planına göre yapılan imhaların, önemli belgelerin yanlışlıkla imha edilmesine neden olabileceğini ifade etmiştir. Katılımcı F2 ise bu görüşü destekleyerek, standart dosya planındaki hataların, örneğin bir belgenin 100 yıl

süreyle saklanması gereken bir evrakın, yanlış bir dosya kodu ile yalnızca 15 yıl sonra Devlet Arşivleri Başkanlığı'na gönderilmesine ya da imha edilmesine sebep olabileceğini belirtmiştir. Bu durumun hukuki sonucunu katılımcı K9 şu ifadelerle açıklamıştır:

“Çok önemli belgelerin atılmasına neden olur. Bu durumda belgelerinizi kaybedersiniz. Belgeleriniz yoksa hakkınızı, hukukunuzu da ispat edemezsiniz. Şöyle bir örnek vereyim. 1951 yılında göçmen ve mültecilere yardım amacıyla Türkiye Birliği diye bir dernek kurulmuş, 1955’e kadar falan dernek faaliyetini sürdürmüştü. Dernek faaliyetini sürdürürken de kurulurken de ana tüzüğünde, 1953 yılındaki yönetim kurulunda diyor ki “dernek bir gün feshedilirse, bu derneğin malı mülkü Kızılay’a devredilir.” Biz devir yazısını, devir kararlarını saklamışız, sahip çıkmışız. Böylelikle hakkınızı koruyorsunuz. İşte yazı yazıyor, şimdi diyeceğiz ki şu tarihte kurulmuş, şu tarihte yönetim kurulu kararıyla bize devredilmiş ama neler devredilmiş? Belgelerin kararı var ama neler devredilmiş bilmiyorsak, önemli olan belgelerin ayrımını yapıp saklayamazsınız, yok olursunuz, yani kurumunuzun hafızası yok olur. Ha, Devlet Arşivleri’nin belirlediği dosya planına göre önemli belgeler, önemli seriler belirlenmiş durumda ama sizin onu belirlemiş olmanız bir mana ifade etmiyor. Onu kullanmanız, işler halde tutmanız mana ifade eder. Yani burada bir sepet var ve o sepete değil de yanındaki sepete koyarsanız, yani şimdi temizlik elemanı ne yapıyor? İşte mavi, yeşil şeyler... Yeşiller tıbbi atık oluyor, onları götürüyor başka bir yere koyuyor. Öbürlerini götürüyor, başka bir yere koyuyor. Yani onun için, kuralların koyulması önemli ama önemli olan o kuralları işletmek. Burada da standart dosya planını, saklama planını düzgün işletmezseniz ya hepten yok edersiniz ya da dijital bir çöplüğü devasa hale getirirsiniz ki şu anda dijital bir çöplük devasa büyüyor.”

Personelin dosya planı kodlarını kullanmasıyla ilgili katılımcıların görüşleri, bu sürecin potansiyel risklerini ortaya koymaktadır. K6, standart dosya planı kodlarının kullanıcılar tarafından doğru bir şekilde kullanılmamasının en büyük risk olduğunu ifade etmiştir. Özellikle, belge ayıklama ve imha süreçlerinde yanlış dosya planı kodu kullanılması durumunda belgelerin yanlışlıkla imha edilme olasılığının yüksek olduğunu vurgulamıştır. Bu bağlamda, ilk onay akışında birim amirlerinin denetim yapması önemli bir önlem olarak önerilmektedir. Amirlerin, evrakların doğru dosya planına ve doğru klasöre yönlendirilip yönlendirilmediğini kontrol etmeleri gerektiği

bu sürecin etkinliğini artıracak bir yaklaşım olarak öne çıkmaktadır. AU4 ise dosya planlarının güncel olmamasını ve örgütün sahada yürüttüğü işlerle ilgili gerçek fonksiyonların planda yer almamasını eleştirmektedir. Bunun yanı sıra, dosya planında mevcut olan kodların doğru kullanılmaması, örneğin “99-Diğer” kodu ile belgelerin geçici olarak işaretlenmesi ve ana konu kodlarının kullanılması önemli bir sorun olarak ortaya çıkmaktadır. Bu durum, kodların doğru kullanılmaması ve güncellenmemesi nedeniyle belgelerin doğru şekilde sınıflandırılmaması riskini artırmaktadır.

Kurum temsilcilerinden K11’e göre, Devlet Arşivleri tarafından standart dosya planı ile ilgili genel kurallar belirlenmiş olsa da her kurumun kendi belge türlerine hâkim olarak özgün çözümler geliştirmesi gerekmektedir. Katılımcı, her kurumun kendine özgü riskleri bulunduğunu ve bu nedenle tek tip bir yaklaşımın yetersiz kalabileceğini belirtmiştir. Örneğin, Çankırı Üniversitesi ile Hacettepe Üniversitesi’nin risk yapılarının farklılaşabileceğini, her iki kurumda da belge türünün üniversite belgesi olmasına rağmen bu farkların görülebileceğini vurgulamıştır. Bu doğrultuda EBYS’lerde kurumun belge türleri, kullanıcı ve yönetim profili gibi özelliklerinin dikkate alınması gerektiği yönünde bir bakış açısının benimsenmesi gerektiğini dile getirmiştir. Katılımcı Ayrıca kurumlarında SDP ile yaşanan sorunları çözebilmek amacıyla birimlere özel dosya planları oluşturduklarını, her birim için kullanılabilecek yaklaşık on farklı SDP belirlediklerini ve bunlara ek olarak ortak belgeler için de ayrı kodlamalar geliştirdiklerini aktarmıştır. EBYS içinde kullanıcıların yanlış dosya planı seçimini önlemek amacıyla sistemin, “Bu SDP kodu biriminizde kullanılmamaktadır, lütfen listeden seçim yapınız” şeklinde bir uyarı vermesi gerektiğini, bu tür çözümlerin mevcut sorunların önüne geçilmesine katkı sağlayacağını ifade etmiştir. Aksi takdirde, dosya planındaki hataların önlenemeyeceği ve bu durumun belgenin tüm sürecini olumsuz yönde etkileyebileceği üzerinde durmuştur.

3.2.1.4.2. Belge Gönderme/Dağıtım Sorunları

Katılımcılar belge gönderme sorunları konusunda, iş akış belirsizliği, mevzuata uygun olmayan durumların yaşandığı ve DETSİS kaynaklı risklerin olduğunu belirtmektedir.

İş akış sürecindeki belirsizlik riskini katılımcı K5, kurumlarında aktif bir elektronik yazışma yönetmeliği bulunmaması nedeniyle yazışma süreçlerinin standardize edilemediği ve bu belirsizliğin ciddi sorunlara yol açtığı şeklinde açıklamıştır. Özellikle kimlerin vekâletle kime yetki verebileceği, kimlerin vekâletleri

onaylayabileceği ve izinlerin kimler tarafından onaylanabileceği gibi temel iş akışlarının netleşmemesinin yazışmaların düzensiz ve standart dışı olmasına neden olduğunu söylemiştir. Katılımcı, bu belirsizliklerin belge gönderme ve dağıtım sürecinde zorluklar yaşanmasına yol açtığını ve evrakların doğru yerlerde işleme alınmaması gibi önemli riskler doğurduğunu belirtmiştir. Ayrıca arşiv modülünün devreye girmesiyle birlikte evrakların standart hale getirilememesinin arşivleme süreçlerinde de sorun yaratabildiğine değinmiştir.

Belge gönderme risklerinden biri olan mevzuata uygun olmayan durumları K10 örneklerle açıklamıştır:

“Mesela, Resmi Yazışma Usul ve Esasları Hakkındaki Yönetmelik şöyle diyor, kamu kurum ve kuruluşları teknik rehberlere uymak zorundalar. Şimdi Noterler Birliği diye bir birlik var. Bu da kamu kuruluşu ama kendini bazen kamu kuruluşu niteliğinde olmadığını düşünüyor. Bana gönderdiği evraklar ne EYP paketine uyuyor ne gizlilik kleransı ile gönderiyor, yönetmeliğe de uymuyor. Hadi kamu kuruluşu değilsin, bu gönderdiği evrakı ben burada işleme alamıyorum, açamıyorum. Arkadaşlar bin tane takla attırmak zorundalar çünkü standartlara uygun değil. Risklerden biri bu. Orada hak kaybı oluşabilir. Çünkü gönderdiği evrak acil, yani bir vekâleti iptal etmeyle ilgili yazılar. Ben işleme almadığım zaman o vekâletle gelip ilgili kişinin taşınmazını satabilir ve o kişi bir risk altında kalır. Sonrasında, yine Resmi Yazışma Usul ve Esasları Hakkındaki Yönetmelik’te kısaca şöyle diyor: Resmi kurumlar zorunlu haller dışında elektronik ortamda yazışırlar. Geçen bir olay oldu. Bizde şöyle belediyenin taşınmazlarıyla ilgili hafta içi veya iki haftada bir, bir kişi görevlendirilip belediyeden gelir ve o taşınmazlarla ilgili imza yetkisine sahiptir, imza atar. Müdürlüğün bir tanesine elden, işte “şu belediyenin taşınmazlarıyla ilgili işlem yapmaya filanca kişi yetkilidir” şeklinde bir evrak getiriyorlar. İlgili müdürlük evrakın doğrulama koduna bakıyor ki doğrulama sayfası da çalışmıyor ayrıca belediyenin. Ondan sonra o kişiyle beraber belediyenin taşınmazını birine satıyorlar. Evrak sahte. Şimdi karşı kurum KEP üzerinden evrak göndermek zorunda, yani çünkü bir savaş hali yok, bir şey yok. Doğrulamasının çalışması lazım. İlgili arkadaş da kontrol etmeden işleme alıyor. Mesela bu risk. Sonra yine buna benzer bir olay, Kadastro Müdürlüğüne bir dilekçe ile vatandaşın biri başvuruyor. Hak sahipliği ile ilgili, kadastro müdürlüğü de ‘hak sahibi değilsin’ diye bir yazı veriyor. Vatandaş gidiyor, bu yazının bir kopyasını

oluşturuyor, 'hak sahibidir' diyor, altına tekrardan onunla gidip altta belge kodu falan da var, yine gidiyor belediyeye veya bakanlığa mı artık bilmiyorum. Hak sahipliğiyle ilgili işlem yaptırıyor. Sahte evrak üzerinden. Yani bunların hepsi risk. Burada Resmi Yazışma Usul ve Esasları Yönetmeliğinde ne yazıyorsa, kontrol etmen gereken ne ise, bunların hepsini kontrol etmek zorundasın. Yani bunu tek tek eğitimle de olmuyor. Bu yönetmelikler bütün devlette çalışan memurları kapsıyor. Mesela şöyle de oluyor, keyfilik de var. Bazı belediyeler fiziksel evrak gönderiyor, sonra da baskı yapıyor bunu işleme alın diye. Yani orada bir yönetmelik var, yönetmelik herkes için ve ona uymak zorundasın, bu kadar. Yani dik durduğunda da bu sefer sorun yaşıyorsun, öbür taraftaki bürokrat gibi, süreler de var. Yani bunu topyekûn şekilde işlemek lazım. İşte yönetici burada da önemli, kararı çok önemli. Ben olsam hiçbir işlem yapmam, geri gönderirim. Mesela noterlerden gelen o yazıların hiçbirini işleme almam, geri gönderirim, buna uyun diye. Zaten birkaç defa gönderse düzelecek ama kabul ettikçe düzelmiyor. Yaşadığımız sıkıntılar, yani ciddi boyutta yaşadığımız sıkıntılar bunlar.”

Katılımcı, tebligat gönderimi konusunda da toplumda yeterli bilincin oluşmadığını ifade etmiştir. Tebligatın ne işe yaradığının, nasıl düşeceğinin ve nasıl kontrol edilmesi gerektiğinin çoğu kişi tarafından bilinmediğini vurgulamıştır. Yeni bir yasal mevzuatla ilgili olarak 1975 ve sonrasındaki işlemler için ulusal elektronik tebligat sisteminin zorunlu hale geleceği, ancak bu konuda toplumda ve kamu görevlilerinde yeterli bilinçlenmenin olmadığını aktarmıştır. Katılımcı, vatandaşlara ve memurlara bu yeni sistemin gerekliliği hakkında ön bilgilendirme yapılmadan zorunluluk getirilmesinin büyük bir sorun oluşturduğunu, bunun sonucunda da sistemin etkin bir şekilde uygulanamadığını dile getirmiştir. Bir emekli personelin eski yetkili olduğu için sürekli tebligatlar aldığı gibi örneklerle, bu eksikliklerin işlem yapılmayan tebligatlara yol açtığını ve hak kayıplarına neden olduğunu anlatmıştır. Katılımcı, bu tür düzenlemelerin etkilediği kişilere önceden duyuru yapılmadan, sadece teknik ve idari düzenlemelerle hayata geçirilmesinin, uygulamada büyük aksaklıklara yol açtığını ve sonrasında hak kayıplarının yaşandığını belirtmiştir.

Katılımcı K11 ise DETSİS kaynaklı sorunlara dikkat çekmiştir:

“DETSİS ile ilgili hâlâ bir kısmı çözülmüş değil. Mesela bazı kamu kurumları orada mevzuata bağlı olarak yanlış adlandırılıyor. Biz de şeyi yaşıyoruz: Ombudsmanlık, Kamu Denetçiliği bizim bağlı kuruluşumuz, ama Kamu Denetçiliği Kurumu diye

DETSİS'te bir kod yok; Kamu Başdenetçiliği diye bir kod var. Şimdi kullanıcı bunu bilmez, kullanıcı ne yapıyor, meclisi seçiyor, nasılsa Kamu Denetçiliği bize bağlı diye. Ve şu anda bizim genel evrak bölümüne en çok, en hatalı gelen dışarıdan gelen belgeler, yani DETSİS'ten kaynaklı sorunlar. DETSİS yapılanması, daha doğrusu buradaki yapılanma sadece EBYS'ye bağlı yapılanma değil. Cumhurbaşkanlığı sistemine girdikten sonra kamu yapılanması çok değişti. Kamuda yeni yeni örgütlenme modelleri çıktı, koordinatörlük gibi, ofis başkanlığı gibi. Hatta Cumhurbaşkanlığı Genel Sekreterliğe geri döndü, genel sekreterlik yapısına. Yani bu, Türk kamu yönetiminin Cumhurbaşkanlığı sistemiyle farklılaşmasından kaynaklanıyor. EBYS'yi niye etkiliyor? EBYS'de yazı yazıyoruz, yani biz o kurumlara yazı yazıyoruz. Şimdi kurumun adı doğru yapılandırılmazsa, yazının hitap bölümünde sorunlar başlamış oluyor. Biz de o sorunları çok yaşıyoruz, sık sık resmi yazışma eğitimi veriyoruz bunu gidermek için”

AU1 ise gelen bir belgenin dağıtımı sırasında yaşananları “EBYS geldi belge sayısı arttı, gereksiz belge üretiyoruz diyen hocalarla karşılaştım. İşte bu daha önce böyle bir şey yoktu bu kadar belge görmüyorduk. Niye bu kadar belge görüyoruz. Haklılar o konuda da çünkü doğru yönetilmiyor sistem. Yani örnek veriyorum, fakülteye bir Hititoloji Bölümü sempozyumuyla alakalı bir yazı geliyor ve hepimize tebliğ ediliyor. Yani bu beni ilgilendiren bir yazı değil ama neden burada? Aslında EBYS'nin suçu yok. Doğru yönetilmemesinin suçu var. Sekreterleri ya da işte hani üst birim amirlerine ne kadar söylersek söyleyelim. Onlar uygulamadığı noktada aslında kendi kendimize bir olumsuz dinamik” şeklinde aktarmıştır.

3.2.1.4.3. Saklama ve Erişilebilirlik

Akademisyenler/uzmanlar ve firmalara elektronik belgelerin saklanması ve erişilebilirliği sırasında karşılaşılabilecek riskler sorulmuş ve alınan cevaplara ilişkin veriler bu risklere neden olan etmenler ile meydana gelen riskler olarak iki ayrı tabloda Tablo 3.23, Tablo 3.24'te verilmiştir:

Tablo 3.23: Saklama ve erişilebilirlik risklerine neden olan etmenler

<i>Riskler (N=17)</i>	<i>Katılımcılar</i>
Üstveri (N=7)	AU1, AU4, AU6-AU8, F1, F2
Teknik Yetersizlik (N=5)	AU1, AU5, AU7, AU8, F3

Yetkilendirme (N=3)	AU5, AU7, F2
Mevzuat Boşluğu (N=1)	AU1
Arşivleme Planlaması (N=1)	AU7

Tablo 3.23'e göre saklama ve erişilebilirlik risklerine üstveri (N=7) alanlarının eksik veya yanlış oluşturulması, sistemin teknik yetersizliği (N=5)'nin neden olduğu anlaşılmaktadır. Ayrıca yetkilendirme (N=3) işlemlerinin hatalı yapılması katılımcılara göre erişilebilirlik risklerine neden olmaktadır.

Tablo 3.24: Saklama ve erişilebilirlik riskleri

<i>Riskler (N=23)</i>	<i>Katılımcılar</i>
Maliyet (N=5)	AU1, AU4, AU6, AU7, F3
Güvenlik (N=4)	AU3, AU5, AU7, F3
Teknoloji Eskimesi (N=2)	AU1, AU7, F2
Belge Formatı Uyumsuzluğu (N=1)	AU7
Yavaşlama (N=1)	F3
Belge Yönetim Yapısının Bozulması (N=1)	F1
Bütünlük (N=1)	AU1
İş Sürecinin Aksaması (N=1)	F3
Belge Delil Değeri (N=1)	AU1

Tablo 3.24 incelendiğinde, saklama ve erişilebilirlik konusunda maliyet (N=5), güvenlik (N=4), teknoloji eskimesi (N=2) gibi risklerin meydana gelebileceği görülmektedir.

Katılımcılardan AU1 belgelere erişimde üstverinin önemini şu şekilde açıklamıştır:

“Uzun vadede erişilebilirliğin sağlanmasında erişim uçları çok önemli. EBYS’lerde belge temelli arama yapılıyor ama arşivlerde bilgi temelli bir arama var. Yani arşivde belgeyi aramıyoruz ama bilgiyi arıyoruz. O bilgiye ihtiyaç duyuyoruz. Dolayısıyla erişim uçlarının üstverilerin ona göre belirlenmesi gerekiyor. Erişilebilirliği ancak o şekilde sağlayabiliriz. Doğru üstverilerin atanması, üstveriyi yönetiminin doğru yapılması, mevcut üstveriler belki de arşiv için yeterli olmayacak, yeni üstverilerin eklenmesi gibi üstveri yönetimi çok önemli.

Katılımcılar, erişimi etkileyen teknik risklerle ilgili çeşitli endişelerini dile getirmiştir. AU1, belgelerin uzun süreli korunmasının önemli bir teknik risk olduğunu ve belge bozulduğunda, erişilebilir olsa bile delil değerinin kaybolacağını vurgulamıştır. Bu durumda, bozulmuş bir belgenin herhangi bir mahkemeye sunulamayacağına dikkat çekilmektedir. AU3, belgelerin yeni donanım ve sistemlere transferindeki eksikliklerin, erişim üzerinde ciddi olumsuz etkiler yaratabileceğini belirtmiştir. Bunun yanı sıra F3, elektrik ve internet kesintileri gibi teknik aksaklıkların, belge erişimini ve yönetimini doğrudan etkileyebileceğini ifade etmiştir. Bu tür teknik riskler, belge yönetim süreçlerinde kesintilere ve veri kaybına yol açarak erişim sürecini olumsuz yönde etkileyebilmektedir.

Katılımcı AU4 maliyet konusuna şu ifadeyle vurgu yapmıştır: *“Saklamada sıkıntı yok gibi de erişimde problemler yaşıyor. İmha hemen hemen hiç yapılmıyor. Özellikle dijital malzeme için imha düşünülüyor. Oysa arşivlenen her belgenin bir saklama, arşivleme ve tekrar erişim maliyeti var. Bu şimdilik pek göz önünde bulundurulmuyor. Bugün 0,25 cent üretim maliyeti olan bir e-belgenin 100 yıl sonraki erişim ve kullanım maliyeti bugünkü teknolojik değişim ve dönüşüm göz önünde bulundurulduğunda ortalama 94 dolar olarak hesaplanabilir.”*

3.2.1.4.4. Saklama Süreli Belgelerin Yönetimi ve İmha İşlemleri

Yaşam döngüsü içerisindeki belgelerin belirli bir ömrü vardır ve bu süre sonunda belgeler tasfiye edilmektedir. Tasfiye yer yer imha ile eş anlamlı kullanılsa da imha etmek değil belgenin akıbetine karar vermektir. Yani saklama süresi dolan belgelerin hangi işleme tabi olacağını (Devlet Arşivleri'ne gönderilir, kurumunda saklanır, ayıklama imha komisyonunca değerlendirilir, Devlet Arşivlerine gönderilmez) belirlemektedir (Çiçek, 2023, s. 272).

Saklama süreli belgelerin yönetimine ilişkin süreçlerin eksiklikleri ve tasfiye işlemlerinin belirsizliği, kurumlar için ciddi riskler yaratmaktadır. Katılımcılardan 6'sı (AU6, F2, K2, K3, K10, K11) bu durumun nedeni olarak yetkili kurumların sorumsuz davranmasına işaret etmektedir. Katılımcı görüşleri doğrultusunda belirlenen tasfiye işlem belirsizliğinin oluşturabileceği risklere ilişkin veriler Tablo 3.25'te gösterilmektedir:

Tablo 3.25: Tasfiye işlem belirsizliği riskleri

<i>Riskler (N=37)</i>	<i>Katılımcılar</i>
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
Erişim (N=2)	AU1, F3
Yönetilemez Yapı (N=2)	AU1, AU8
Maliyet (N=2)	AU4, K2
Veri Gizliliği (N=1)	F1
Yetkin Personel (N=1)	AU5
Kurum İmajı (N=1)	AU1
Kurumsal Benliğin Kaybolması (N=1)	AU1
Arşivlemenin Yapılamaması (N=1)	K5
Yavaşlama (N=1)	K4
Bütünlüğün Bozulması (N=1)	K3

Tablo 3.25 incelendiğinde, 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 belirtilen riskler olduğu anlaşılmaktadır. Karbon ayak izi (N=2), erişim (N=2), yönetilemez yapının (N=2) meydana gelmesi, maliyet (N=2) gibi unsurların da tasfiye işlem belirsizliklerinin oluşturabileceği riskler arasında olduğu anlaşılmaktadır.

Katılımcılardan AU7, tasfiye süreçlerinin belirlenmemesinin oluşturabileceği temel riskleri şu şekilde özetlemiştir:

“Ben henüz imha yapan bir kurum görmedim. Elektronik imhadan bahsediyorum. Bir şeyi imha edebilmeniz için neyi saklayacağınızı bilmeniz gerekir. Neyi saklayacağınızı bilmiyorsanız da neyi saklamamanız gerektiğini bilmeniz gerekir. Biz deriz ki arşivciliğin aslında %90’ı bazen de neyi saklamayacağını bilmektir. Doğal olarak kurumlar böyle bir şey yapmadığı için yani kurumlar şu anda veri alanımız çok geniş, bu bizim için sıkıntı değil, biz belgeleri üretelim, şu an imha etmesek de olur

madundalar. Hâlbuki imhanın başka bir teorisi var imha teorisi dediğimiz. Belgeleri saklamanın ve saklamamanın da başka bir teorisi var. Burada nasıl bir eksik, nasıl bir sonuç olabilir? İmha yaptığımızı düşünelim, eğer imha yapıyoruz. Saklama süremizi tayin etmedik. Saklama süremizi doğru tayin etmedik ama işte aradan on (10) yıl geçtiği için bunu imha ettiğimizi düşünüyorum. O zaman delil değeri taşıyan bir belgeyi imha etmiş olabilmek ihtimalimiz var ve doğal olarak davalarda sıkıntı yaşayabilme ihtimalimiz oluyor. Mesela fiziki belgeler için söylerler. Devlet kamulaştırmış mesela bazı demir yolu arazilerini fakat kamulaştırdığına dair belgeleri tutmadığı için tekrardan kamulaştırma parası vermiş. Devlet Demiryollarının arşivinde bu belgeler tutulmadığı için orada durumu bilen kişiler de tayin olmuş vesaire oranın kamulaştırıldığını haberdar değiller. Tekrar tekrar kamulaştırma ücreti veriliyor. Bunun elektronik ortamdaki meselesini düşünelim. Eğer siz bu belgeyi onun gibi düşünüp imha ederseniz, 30-40 yıl sonra bu belge size lazım olduğunda bunu sunamayacak ve bir hak yetki ve sorumluluğu da ispatlayamayacaksınız. Böyle bir sıkıntımız var. Böyle bir sorununuz var. Belge yönetimi, saklama süreleri ve imha işlemleriyle ilgili. Burada esas olan yine dediğim gibi saklama süreli dosya planını oluşturmak.”

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” AU1 bu durumun belgenin yok olmasına, kurumsal bilginin ve belleğin kaybına neden olduğunu vurgulamıştır.

Yetkili kurumların sorumsuz davrandığına dikkat çeken K10 durumu “Standart dosya planımız güncel, yani şimdi yeni çıkanlara göre de güncelleyeceğiz. Saklama planlarımız da güncel ama şimdi bana şey söylemesi lazım Devlet Arşivlerinin yani ben oraya eğer bir evrak göndereceksem bunun teknik anlamda üstverileri neler olacak işte ne şekilde göndereceğim? Web servislerini göndereceğim yoksa eski usul bir diske çekip öyle mi göndereceğim? Bunların detaylandırılıp bana bir yönetmelik ya da şey bir yasa şeklinde gelmesi lazım. Bu yok ama her geldiklerinde bir şikâyet

olsun bu da bunlardan bahsediyorlar yani ama kendilerinin bize bildirdikleri bir şey yok.” şeklinde açıklamıştır.

Katılımcılardan K3 ve K2, elektronik belgelerin tasfiyesi ve uzun vadeli arşivlenmesi sürecine ilişkin belirsizliklerin sürdüğünü ifade etmiştir. K3, elektronik belgelerin tasfiyesinin e-arşiv sistemi üzerinden mi yoksa EBYS uygulamaları aracılığıyla mı yürütülmesi gerektiğine dair kurum içinde farklı görüşler bulunduğunu ve bu konuda net bir standardın henüz oluşmadığını belirtmiştir. Bu nedenle Devlet Arşivleri Başkanlığı’ndan gelecek yönlendirme ve standartların beklendiğini söylemiştir. Benzer şekilde K2 de dijital ortamda saklanması gereken belgelerle devri gerçekleştirilmesi gereken belgelerin ayrımının yapılması gerektiğine dikkat çekmiştir. Ayrıca Devlet Arşivleri’nin henüz bu süreci karşılayabilecek altyapıya sahip olmamasına rağmen kurumların elektronik belgeleri teknik olarak istenilen formatta ve yapıda iletebilecek durumda olduklarını ifade etmiştir. Her iki katılımcı da dijital arşivleme süreçlerinde kurumsal hazırlığın bulunduğunu ancak merkezi standart ve yönlendirmenin eksikliği nedeniyle sürecin belirsizlik taşıdığını belirtmiştir. Ayrıca Devlet Arşivleri Başkanlığı tarafından yapılamayacaksa Cumhurbaşkanlığı’nın olaya dâhil olması ya da başka bir yetkili merciinin durumu çözmesi gerektiğine işaret etmiştir.

Akademisyen/uzman temsilcilerinden AU6 benzer şekilde durumu şu ifadelerle açıklamıştır: *“Fiziki belge yönetimini düşünün belgeler üretildi idari, mali, hukuki süreçlere göre saklama süreleri tayin edildi ve arşiv belgesi saklama süresi sonunda Devlet Arşivleri’ne gönderilir denildi. Fiziki olarak bunu yapıyor kurumlar ama elektronik olarak yapıldı mı? Kurumların Devlet Arşivleri’ne göndereceği belgeler var peki Devlet Arşivleri bunu alabilecek teknolojik altyapıya sahip mi? Hepsi soru işareti. Tuz Gölü’nün orda, Gölbaşı’nda büyük bir tesis kurulacağından falan bahsediliyor ama şu an uygulamada yok”*

Firma temsilcilerinden F2, EBYS üzerinde ayıklama ve imha işlemlerinde ortaya çıkabilecek risklerle ilgili şu sözleri aktarmıştır: *“Saklama süreleri belirli olsa bile biz kullanıcının inisiyatifine bırakmıyoruz ya da sistemin kendi otomatik olsun diye bırakmıyoruz. İmha edilecek bir işlemse bunun bir için bir komisyon ve arka tarafta imha prosedürlerini çalıştırmak gerekiyor. Bunu yapmıyoruz. Aslında girilen dosya koduna göre imha seçildiyse arka tarafta sistem kullanıcıya sormadan bunu imha*

etmesi gerekir ama biz onu uygulattırmadık. Çünkü yanlış girme olasılığı olabiliyor. Hatalı dosya kodu girme olasılığı olabiliyor. Burada kullanıcıya bu işlemi yaptırmıyoruz. Saklama süresi dolan bir belge de olsa Devlet Arşivleri tarafından nasıl davranılacağı belli olmadığı için biz onu yine bekletiyoruz. Kurum ya da kullanıcı sorduğu zaman yapacağı bir işlem varsa ona yönlendiriyoruz, onun üzerinden işlem yaptırıyoruz. Yazılımımızı kullanan kurumların hiçbirinde şu anda bir imha işlemi gerçekleştirilmedi. Elektronik ortamda imha işlemleri prosedürleri henüz belli olmadığı için bekletiliyor. Çünkü geri dönüşü olmuyor. Burada bizim sistemimizde imha edildiğinde sadece meta bilgileri yer alıyor. PDF bilgileri ortadan kalktığı için yanlış ya da hatalı bir işlemde geri dönüşü olmayacaktır. O yüzden biz bunu yaptırmıyoruz kurumlara.”

3.2.1.4.5. Kâğıt ve Elektronik Belge Süreçlerinde Entegrasyon

Ülkemizde belge yönetim işlemleri elektronik ortamda yürütülse dahi kurumların bazı birimlerinde fiziki evrak üretimi devam etmektedir. Ayrıca kurumların fiziki arşivleri aktif bir şekilde kullanılmaktadır. Kâğıt ve elektronik belge arşivleme süreçlerinin ayrı tutulmasının riskleri kurum temsilcilerinden elde edilen veriler doğrultusunda Tablo 3.26’ da gösterilmektedir:

Tablo 3.26: Kâğıt ve elektronik belge süreçlerinde entegrasyon riskleri

Riskler (N=19)	Katılımcılar
Bütünlüğün Bozulması (N=8)	K1, K4, K5, K7, K9, K11-K13
İş Sürecinin Aksaması (N=6)	K2, K6-K9, K13
Eksik Bilgi (N=3)	K2, K10, K13
Belge Erişim (N=2)	K2, K7

Tablo 3.26 incelendiğinde, kâğıt ve elektronik belge süreçlerinin ayrı tutulmasının riskleri arasında en sık vurgulanan unsurun bütünlüğün bozulması (N=8)’olduğu görülmektedir. Katılımcılar ayrıca bunun iş sürecinde aksamalara (N=6) neden olabileceğinin üzerinde durmaktadır.

Katılımcılar, belge ve dosya bütünlüğünün sağlanamamasının EBYS kapsamında önemli bir risk oluşturduğunu ifade etmiştir. K5, fiziksel ortamda oluşturulan bir belgenin elektronik ortamda üretilen devam belgeleriyle ilişkilendirilmemesi durumunda arşivsel bağlamın kaybolduğuna dikkat çekmiştir. Katılımcıya göre,

sistemin ilk kullanım dönemlerinde fiziksel belgelerin taranarak elektronik ortama aktarılması ve elektronik belgelerde bu ilişkilere atıfta bulunulması gerekmektedir söz konusu bağlantı çoğu zaman kurulmamış ve belgeler arasında olması gereken süreklilik sağlanamamıştır. K9 da benzer şekilde, belge ve dosya bütünlüğünün sağlanmaması durumunda eksik ya da kopuk bilgilere ulaşılabileceğini belirtmiştir. Katılımcı, belge yönetim sürecine sahiplenici bir yaklaşımla bakılmadığı takdirde kullanıcıların yalnızca EBYS üzerinden yapılan sorgularla yetindiğini ve daha geniş bir belge setine ulaşma çabasında olmadığını ifade etmiştir. Bu durumun veri bütünlüğü açısından ciddi riskler barındırdığını vurgulamıştır. Her iki katılımcı da, bütüncül belge ilişkilendirmesinin ve belgeler arası bağın hem arşivsel değer hem de kurumsal bilgi güvenliği açısından son derece önem taşıdığını dile getirmiştir. Katılımcı K13 konuyla ilgili yaşadıklarını şu şekilde anlatmıştır: *“Kurumdaki ihale dosyalarında fiziksel ve dijital dosyalarda fark bulunuyordu. Fiziksel dosyadaki belgeler tamken dijital dosyanın içi neredeyse boştu. Bunu fark ettikten sonra müdürlüklerde ihale yapan personelleri davet ettiğimiz bir toplantı yaptık. Toplantıda bu durumun sebebini öğrenmeye çalıştık. Esas mesele, ihale dosyalarında bulunan çeşitli sayıda belgenin dijitalleştirilmesi için ekstra zaman harcamaktı ki bu konuda haklılar. Ancak ihale dosyalarının önemli olduğunu ve onları dijital ortamda daha güvenle saklayabileceğimizi, ilk akla gelen dosyanın artık dijital dosyalar olması gerektiğiniz konuştuk ve fikir birliğine varabildik. Fiziksel ve elektronik belgelerin ayrı yürütülmeye çalışıldığı bir düzende dosya bütünlüğünden bahsedemeyiz.”*

3.2.1.4.6. Dijitalleştirme Sürecindeki Riskler

Fiziki belgelerin elektronik ortama aktarılmasını sağlayan dijitalleştirme kurumlara özellikle erişim konusunda büyük kolaylık sağlamaktadır. Belgelere hızlı erişimi sağlarken aynı belgeye aynı anda birden fazla kullanıcının da erişimine imkân tanımaktadır. İş birliğini kolaylaştırarak zamandan tasarruf sağlamak ve verimlilik artmaktadır. Fakat dijitalleştirme sürecinde çeşitli risklerle karşılaşmaktadır. Kurum temsilcilerinden elde edilen veriler doğrultusunda dijitalleştirme sürecinde yaşanabilecek risklerin yer aldığı bulgular Tablo 3.27’de sunulmaktadır:

Tablo 3.27: Dijitalleştirme sürecindeki riskler

<i>Riskler (N=26)</i>	<i>Katılımcılar</i>
Kurumsal Analiz Eksikliği (N=5)	K1, K5, K6, K10, K13
Üstveri Hataları/Erişim (N=4)	K2-K4, K13
Görüntüleme/Okuma Sorunları (N=3)	K7, K9, K13
Belgenin Yıpranması/Zarar Görmesi (N=3)	K3, K9, K13
Maliyet (N=2)	K9, K10
Belge Güvenliği (N=2)	K3, K12
Bütünlüğün Bozulması (N=2)	K3, K7
Belge Kaybı (N=2)	K3, K4
Firmanın Yetkinliği (N=1)	K10
Dijitalleştirilen Belgenin Fizikisinin İmhası (N=1)	K7
Firmanın Sürdürülebilirliği (N=1)	K3

Tablo 3.27’e göre, dijitalleştirme sürecinde en sık dile getirilen riskin kurumsal analiz eksikliğidir (N=5). Bunu üstveri hataları/erişim sorunlarının (N=4) izlediği görülmektedir. Görüntüleme/okuma sorunları (N=3), belgenin yıpranması/zarar görmesi (N=3), maliyet (N=2), belge güvenliği (N=2), bütünlüğün bozulması (N=2), belge kaybı (N=2) gibi durumların da belirtilen riskler arasında olduğu izlenmektedir.

Bu süreçte yaşanılabilecek riskleri katılımcılardan K10 şu şekilde açıklamıştır:

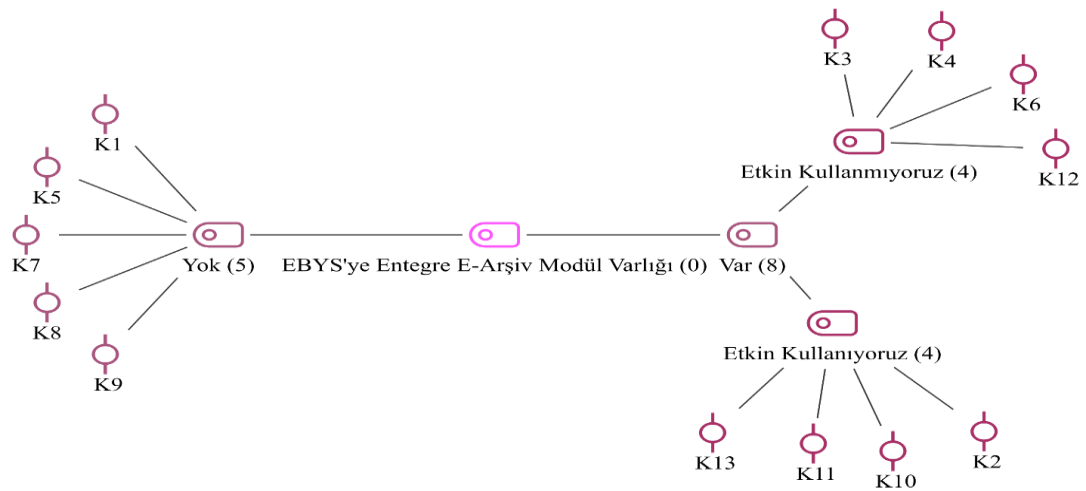
“Şimdi bir kere ilgili birim fiziksel arşivini çok iyi bilmek zorunda. Orada hangi verilerin, hangi malzemelerin sayısallaştırılacağını ve hangi üstverilerle bunların tutulacağını iyi şekilde analiz etmesi lazım. Dolayısıyla analiz sürecinde çok iyi karar vermek lazım. Bu işlerde çok iyi bir şekilde malzeme tiplerinin ayrılması lazım. Bu risk var. Bir de şu var gördüğüm kadarıyla bunu söyleyeyim. Birkaç firmayla çalışıyoruz. Türkiye’deki firmalar sayısallaştırma konusunda zayıflar, yönlendirmiyorlar da ilgili şeyleri. Yani sadece işte biz bu evrakları tarayalım, ondan sonra bize verilen şekilde bunların akıllandırmasını yapalım, bir yerde muhafaza edelim şeklinde çalışıyorlar. Ama firmaların daha yetkin olmaları lazım. Daha yönlendirici olmaları lazım. Bir de yaptıkları işin arkasında durmaları lazım. Bizde maalesef bunlar merdiven altı firmalar gibi firmalar üzerinden gidiyor. Dolayısıyla bir sürü risk çıkıyor. Eğer doğru yönetilmiyorsa kurum da bilmiyorsa bu işi ve doğru yönetmiyorsa ortaya çıkan şey asla kullanılabilir olmuyor. Sadece firmaya bağımlı kalıyorsunuz. Firma ne ürün verirse belki de kullanamayacaksınız yani. Çünkü sen ne istediğini bilmiyorsan kullanım

konusunda da sorunlar yaşıyorsun. Bir kere bunu nasıl kullanacağın da önemli. Yani ona iyi karar vermek lazım. Ona göre de dizayn etmek lazım analiz sürecini. Eğer biz sadece firmaya bağımlı kalıyorsak onun verdikleri hizmetlerde sınırlı kalıyorsak kendimizi geliştirmiyorsak burada da aynı riskli karşılaşılabiriz. Tabi onun da maliyetleri var arka tarafta. Şimdi sen eğer her şeyi kendim yapıyorum dersen gidip de belge net gibi bir ürünü yapamaz mısın? Yapabilirsin, sıkıntı değil ama bunun sana bir maliyeti var. Yıl olarak maliyeti var. Emek olarak maliyeti var. Fiyat olarak maliyeti var. Dolayısıyla hazır bir ürün almak, kurumlar açısından daha basit. Ama bunun risklerine karşılık da hazırlık yapması lazım.”

3.2.1.4.7. E-Arşiv Modülünün Olmama Riskleri

Elektronik arşivleme hem dijitalleştirilmiş hem de dijital ortamda üretilmiş belgelerin belirli kurallar çerçevesinde güvenli ve düzenli bir şekilde saklanması ve yönetilmesini kapsayan bir süreçtir. Geçmiş ile gelecek arasında köprüünün kurulduğu bu süreç, kurumsal hafızanın önemli bir parçasını oluşturmaktadır. Kurumsal bilgi ve belge yönetiminin sürekliliği, güvenliği ve erişilebilirliği açısından e-arşivlemenin yapılması gerekmektedir. Bu bağlamda kurum temsilcilerine kurumlarında EBYS'ye entegre e-arşiv modülünün varlığı sorulmuş ve elde edilen yanıtlar Şekil 3.3'te gösterilmiştir:

Şekil 3.3: E-arşiv modülü



Yapılan görüşmeler neticesinde, incelenen 13 kurumdan 5'inde e-arşiv modülünün hiç bulunmadığı, modüle sahip olan 8 kurumdan 4'ünde ise bu modülün aktif olarak kullanılmadığı tespit edilmiştir. Bu durum, kurumların belge yaşam döngüsünü tam anlamıyla yönetemediğini ve bu eksikliğin çeşitli risk unsurlarını doğurduğunu ortaya koymaktadır.

Arşiv modülün olmadığını ifade eden katılımcı K1, konuyu şu şekilde özetlemiştir: *“Arşiv modülü yok. Prosedür belli olmadığı ve zorunlu olmadığı için satın alıp oraya bütçe vermek istemedik. Her şey belli olsun ondan sonra alacağız.”*

Arşiv modülü olup da etkin kullanmayan katılımcılardan K4 ise kurumundaki e-arşiv modülüyle ilgili uygulamaları şu şekilde açıklamıştır: *“Var ama kullanmıyoruz. Çünkü arşiv prosedürlerinin net olarak belirli olmaması, arşiv prosedürlerini net olarak bilemediğimiz için o yüzden kullanmayı tercih etmedik. Şu anda belgeler bir havuzda toplanıyor. Bu aslında büyük bir problem, süreç belli olduğunda dosyalamalar, klasör yapıları tek tek incelenecek ve arşive aktarılacaklar belirlenecek iş yükü hepsi.”*

Arşiv modülünü aktif olarak kullanmayan kurum temsilcilerinden K6 benzer şekilde açıklama yapmış ve durumu şu şekilde izah etmiştir: *“Uygulamaya konulmadı, içerisinde herhangi bir şey yok. Kurumdan da talep olmayınca kullanmayacağız denildi. Biz de sonra kullanılacak denildi. Talep olmayınca biz kendi kafamıza göre bir şey yapamıyoruz yazı olur, Devlet Arşivleri bir şey çıkarır o zaman geçeriz”*

E-arşiv modülünü kullanan kurum temsilcilerinden K10, modülün kullanımını şu şekilde örneklendirmiştir: *“Personel Daire Başkanlığının özlük verileri mesela arşiv modülü üzerinde var. Şu anda onlar aktif bir şekilde kullanıyor. Belli atama yazıları vesaireler yine arşiv net üzerindeki diske kaydediliyor. Daha sonra çağrıldığında bulunabilmesi için.”*

E-arşiv modülüne geçiş sürecine değinen K11, bu süreçteki deneyimi şu şekilde ifade etmiştir:

“Var. Elektronik arşivleme de şöyle yaptık: Bir arşiv yönetim sistemi, onu da kendi yazılımımız. Üç sene önce bir çalışma başlattık, bütün kurumda analiz yaptık ve arşiv yönetim sistemi ihtiyacını tespit ettik. Her süreçte analiz yapılması lazım. Sisteme geçişte, e-arşive geçişte kurumsal analiz yapılmadan bir işe başlanması birçok riski beraberinde getirir. Biz üst yönetimi ikna ettik,

neyse sonra o içeriden bir programla yapılmasına karar verildi. Şimdi o sisteme veri aktarılıyor ve o taranmış şeyler o sisteme aktarılıyor, araştırmacılara da galiba o platformda paylaşılacak, öyle bir niyet var. İlk etapta Osmanlıca belgelerimiz vardı, onlar aktarıldı ve içeriden araştırmacılara açıldı. Biz bu çalışmaları bir taraftan birimlerle yapıyoruz. Bu çalışmaları bitirdikten sonra EBYS'deki belgelerimizin nihai adresi orası olacak. Ama hangi belgeler süresiz saklanacak? Yani onu öyle bir ilke kararı aldık. Süresiz saklayacağımız, yani nitelik kodu B, arşiv kodu A olan belgelerimiz arşiv yönetim sistemine aktarılacak. Yani bizim yol haritamız aslında belli. Devlet Arşivleri'nden niye şey bekliyoruz? Bir programımız var, o programımızın buna yetkinliği de var, ama Devlet Arşivleri kamuyla uyum içinde çalışmak için. Çünkü o bütünleşik sistemde bütün kamu dediler, onu o anlamda bekliyoruz. Yoksa yol haritamız belli.”

E-arşiv olmamasından kaynaklanabilecek riskler kurum temsilcilerden alınan görüşler doğrultusunda Tablo 3.28’de sunulmaktadır:

Tablo 3.28: E-arşiv modülünün olmama riskleri

Riskler (N=17)	Bölümler
İşlerin Aksaması (N=5)	K2, K7, K9, K10, K13
Belge Yönetim Sürecinin Tamamlanamaması (N=4)	K3, K4, K5, K7
Erişim (N=4)	K1, K2, K7, K12
Sistem Hızının Yavaşlaması (N=2)	K1, K9
Farklı Belge Türlerinin Arşivlenememesi (N=1)	K10
İş Yüğü (N=1)	K4

Tablo 3.28 incelendiğinde, e-arşiv modülünün olmamasına bağlı olarak katılımcılar tarafından en sık dile getirilen riskin işlerin aksaması (N=5) olduğu görülmektedir. Bunu belge yönetim sürecinin tamamlanamaması (N=4) ve erişim (N=4) sorunlarının takip ettiği görülmektedir.

Katılımcılar, EBYS kapsamında e-arşiv modülünün bulunmamasının, belge yönetim süreçlerinde ciddi riskler doğurduğunu ifade etmiştir. K13, kurumsal arşivleme süreçlerinin belirli bir standarda oturtulmaması durumunda, sorumluluğun her müdürlüğün kendi inisiyatifine bırakıldığını belirtmiştir. Bu durumun belge yönetiminde parçalı ve düzensiz uygulamalara yol açtığını ve sistemin sağlıklı

işlemesini engellediğini ifade eden katılımcı, kurumsal bütünlüğün de bozulduğunu vurgulamıştır. Benzer şekilde K3, arşivleme yazılımlarının eksikliğinde belgelerin etkin biçimde yönetilmesinin imkânsız hâle geldiğini, bu durumda sistemin yalnızca belge üretimi ve dağıtımını için kullanıldığını fakat ayıklama, imha ve arşivleme gibi temel işlevlerin gerçekleştirilemediğini aktarmıştır. Her iki katılımcı da e-arşiv modülünün kurumsal bellek oluşturulması ve bilgiye erişimin sürdürülebilirliği için önemli bir bileşen olduğunun altını çizmiştir. Konuyla ilgili K2 şu örneği vermiştir: *“Entegre olmasaydı oluşabilecek potansiyel risklere şu şekilde örnek verebilirim, belgeye erişim çok önemli bir konu o ayrı bir mevzu ama biz çok fazla yapının belgesini, dosyasını tutuyoruz ve bu dosyalara erişim için ilk başta başvurduğumuz yer dijital arşivimiz. Yani ada parsel bir sorgulama yaptığımızda o dosyanın fiziki koduna ulaşıp raftaki yerini belirliyoruz. Bu bize çok büyük bir kolaylık sağlıyor. Olmasa erişimde çok zaman kaybederdik. Belki de erişemezdik.”*

3.2.2. EBYS’de Karşılaşılan Riskler

Katılımcılardan elde edilen bulgular doğrultusunda, EBYS ile ilgili geçmişte yaşanan veya karşılaşılmaması muhtemel riskler belirlenmiştir. Bu riskler, EBYS uygulamaları sırasında farklı düzeylerde ve çeşitli alanlarda karşılaşılan sorunları kapsamaktadır. Konuyla ilgili katılımcı görüşlerine ilişkin veriler Tablo 3.29’da gösterilmektedir:

Tablo 3.29: EBYS’de karşılaşılan riskler

<i>Riskler (N=57)</i>	<i>Katılımcılar</i>
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
Firma Bağımlılığı (N=2)	AU4, AU6
Maliyet (N=2)	AU4, AU8
Kurumsal Entegrasyon Eksikliği (N=1)	K1

Belge Gönderme/Dağıtım Sorunları (N=1)	AU1
Belge-İş İlişkisinin Kurulmaması (N=1)	AU7
Firmanın El Değiştirmesi (N=1)	AU4
Kurumsal Politika/Prosedür Eksikliği (N=1)	AU6
Sistem Başarısının Takip Edilememesi (N=1)	AU4
Teknoloji (N=1)	AU3
Veri Tabanı Kaynaklı Riskler (N=1)	K4
Yasal Değişiklik (N=1)	K12
Yedekleme/Depolama Alanlarının Yetersizliği (N=1)	AU5

Tablo 3.29'a göre en sık vurgulanan unsurların personel ve kullanıcı kaynaklı riskler (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. Katılımcılar bu durumun belge güvenliği ve yanlış yönlendirme gibi sorunlara yol açabileceğini dile getirmiştir. K8, teknik altyapıdan ziyade en büyük sorunun insandan kaynaklandığını belirtmiştir. Çalışanların ilgili mevzuat ve yönetmeliklere yeterince hâkim olmaması ve genel olarak okuma alışkanlığının zayıf olmasının süreci olumsuz etkilediğini ifade etmiştir. F1, eğitim yetersizliği ve liyakat

sorunlarının yalnızca iş sürecini etkilemediğini aynı zamanda yasal yaptırımlara yol açabilecek nitelikte olduğunu vurgulamıştır. K9 ise belge yönetiminin kurumsal bir yapı içinde yürütülmemesini eleştirmiştir. Çalışanların belge üretim ve yönetiminde kişisel yaklaşımlar sergilemesinin süreci riskli hâle getirdiğini ve bu konuda yukarıdan aşağıya bir farkındalık eksikliği bulunduğunu ifade etmiştir. Son olarak AU6 kurumsal yapının da önemli bir unsur olduğunu, EBYS’ye yönelik bir başkanlığın kurulması gerektiğini ifade etmiştir. Katılımcı, belge yönetimi birimlerinin profesyonel kadrolarla yapılandırılması durumunda insan kaynaklı risklerin önemli ölçüde azaltılabileceğini savunmuştur.

3.2.3. Risklerin Tespiti ve Yönetimine Yönelik Öneriler

EBYS uygulamalarında karşılaşılan risklerin etkili bir şekilde yönetilmesi ve risklerin azaltılabilmesi için uzmanların ve akademisyenlerin görüşleri alınmıştır. Bu önerilere ilişkin veriler Tablo 3.30’da gösterilmektedir:

Tablo 3.30: Risklerin tespiti ve yönetimine yönelik öneriler

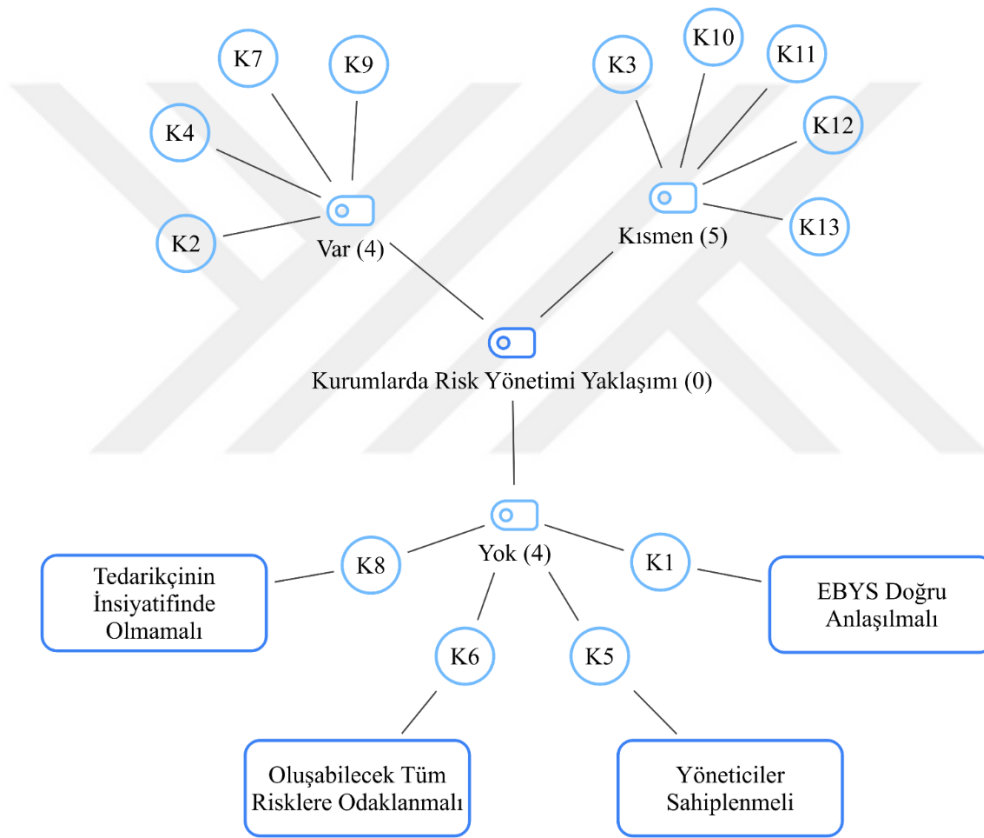
<i>Öneriler (N=31)</i>	<i>Katılımcılar</i>
Bilgi ve Belge Yöneticilerinin Görevlendirilmesi (N=5)	AU2, AU3, AU6, AU7, AU8
EBY Temelli Risk Eylem Planı Oluşturma (N=4)	AU1, AU5-AU7
Müeyyide Koyma (N=4)	AU1, AU2, AU5, AU7
Ulusal Belge Yönetim Stratejisi (N=4)	AU2-AU4, AU7
Yerli-Milli Bulut Ağı/Dış Teknoloji 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
E-İmza Güvenliği Sağlama (N=1)	AU6
Firma Desteği (N=1)	AU8
Kurumsal Veri Sözlüğü (N=1)	AU6
Standartların Uygulanmasının Sağlanması (N=1)	AU5
Yazılım-Donanım Güncelliği (N=1)	AU5

Tablo 3.30’a göre en çok vurgulanan çözüm önerisinin bilgi ve belge yöneticilerinin görevlendirilmesi (N=5) olduğu anlaşılmıştır. 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.

Şekil 3.4: Risk yönetimi yaklaşımı



Şekil 3.4 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 işlemlerini sağlamadığını, yöneticilerin de bu süreci sahiplenmesi gerektiğini ve böyle bir yaklaşımın en üst düzeyden başlaması gerektiğini vurgulamıştır.

Katılımcı K6, yaşanmış veya yaşanabilecek tüm risklerin göz önüne alınarak buna yönelik bir yaklaşım geliştirilmesi gerektiğini vurgulamıştır. K8 ise EBYS'lerin yalnızca tedarikçi inisiyatifine bırakılan bir yapıdan çıkması gerektiğini ve risk yönetim yaklaşımının kurum tarafından geliştirilip firmayı yönlendirmesi gerektiğini ifade etmiştir.

Katılımcılara hazırlanan eğitim materyalinin sunulmasının faydalı olup olmayacağı sorulmuştur. Katılımcıların tamamı (N=24) eğitim materyalinin geliştirilmesinin EBYS sürecinde faydalı olacağını belirtmiştir. Katılımcılardan elde edilen bulgulara göre eğitim materyalinin sunulmasının faydaları Tablo 3.31'de verilmektedir:

Tablo 3.31: Eğitim materyalinin sunulmasının faydaları

<i>Faydalar (N=26)</i>	<i>Katılımcılar</i>
Alandaki Çalışma Azlığının Giderilmesi (N=7)	AU1, F1-F3, K1, K3, K8, K12
Bilgi Eksikliğinin Giderilmesi/Bilincin Artırılması (N=7)	AU3, AU5, AU6, F3, K2, K10, K11
Sistemin Doğru Kullanılması/Sürecin Doğru İşlemesi (N=6)	AU4, AU8, K2, K5, K7, K9
Farkındalık (N=3)	AU2, AU7, K13
Önlem Alınması (N=3)	AU6, K4, K6

Tablo 3.31'e göre eğitim materyali sunulmasında en sık belirtilen faydaların alandaki çalışma azlığının giderilmesi (N=7) ve bilgi eksikliğinin giderilmesi/bilincin artırılması (N=7) olduğu görülmektedir. Ayrıca sistemin doğru kullanılması ve sürecin doğru işlemesi (N=6), ile farkındalık (N=3) ve önlem alınması (N=3) hususları eğitim materyalinin sunulmasının gerekçeleri arasında sayılmaktadır.

3.3. Eğitim Materyalinin Geliştirilmesi

Eğitim materyalinin geliştirilme sürecinde literatürdeki kaynaklar (rehberler, standartlar, akademik çalışmalar vb.) ile görüşmelerden elde edilen veriler birlikte değerlendirilmiştir. Bu doğrultuda materyalin iyileştirilmesi amacıyla kurumlardaki EBYS sorumluları, akademisyenler/uzmanlar ve EBYS tedarikçisi firma temsilcilerinden görüşler alınmıştır. Görüşmelere gitmeden önce katılımcılarla eğitim materyali taslağı ve yarı yapılandırılmış görüşme formu paylaşılmıştır.

Görüşmeler sırasında görüşme formunda yer alan *“Taslak eğitim materyali hakkında eksik veya eklenmesi gereken alanlar olduğunu düşünüyor musunuz? Açıklayınız.”* sorusu üzerine tartışmalar gerçekleştirilmiştir. Bunun yanı sıra görüşme süresince bu sorudan bağımsız olarak katılımcıların önem atfettiği ve eğitim materyalini iyileştireceği düşünülen diğer hususlar da değerlendirilmiş ve elde edilen tüm görüşler birlikte değerlendirilerek eğitim materyaline yansıtılmış ve materyal iyileştirilmiştir.

Eğitim materyalinin iyileştirilmesine yönelik olarak yürütülen bu süreçte aşağıda sıralanan unsurlar dikkate alınmış ve içerik bu doğrultuda yapılandırılmıştır:

1. *EBYS ve riske ilişkin temel kavramlara yer verilmeli, EBYS ile risk arasındaki ilişki giriş bölümünde açıklanmalıdır.*

Bu doğrultuda eğitim materyaline belge, belge yönetimi, belge yönetim süreç ve kontrolü, elektronik belge, elektronik belge yönetimi, elektronik belge yönetim sistemi, risk, risk yönetimi, risk yönetim süreci, risk iştahı kavramları eklenmiştir. Sonrasında EBYS ve risk arasındaki ilişki açıklanmıştır.

2. *Belge yönetimiyle ilgili standartlara atıf yapılmalıdır.*

Uluslararası Belge Yönetimi Standardı ISO 15489, TS 13298 Elektronik Belge ve Arşiv Yönetimi Standardına ve alandaki çalışmalara atıf yapılarak EBYS ve risk bağlantısı açıklanmıştır.

3. *Somut olaylara dayalı örnekler verilmeli ve katılımcı görüşleri de yer almalıdır.*

Öneri doğrultusunda, kurumlarda EBYS’de risk olarak karşılabilecek senaryolar, ülkemizden örnekler ve katılımcı görüşlerinden doğrudan alıntılar yapılarak eğitim materyaline eklemeler yapılmıştır.

4. Sunumlarda görsel kullanımına önem gösterilmelidir.

Bu doğrultuda EBYS ve süreçlerine ilişkin belirlenen temalar ile alt temalara yönelik renkli akış şemaları oluşturulmuştur. Ayrıca sunum içeriğine göre görseller kullanılarak metin yoğunluğu azaltılmıştır.

5. Geniş kapsamlı bir eğitim materyali ortaya çıkarılmalıdır. Materyalde mevcut ve potansiyel risk unsurları ayrıntılı şekilde açıklanmalıdır.

Eğitim materyali, kurumlarda yazışma yapan personeli, bilgi işlem personeli ve yönetimi kapsayacak, ihtiyaç halinde özelleştirme yapılacak nitelikte hazırlanmıştır. Literatürden ve yapılan görüşmelerden elde edilen veriler ışığında risk unsurları değerlendirilmiş ve eğitim materyaline ayrıntılı olarak eklenmiştir.

6. Tüm risk unsurları anlaşılır bir dille açıklanmalıdır.

Eğitim materyalinde geçen teknik ifadeler sade bir Türkçe ile açıklanmış, karmaşık unsurları anlaşılır hale getirebilmek için tablolar, grafikler, şemalar kullanılmıştır.

7. Yapay zekâ, makine öğrenmesi, nesnelerin interneti gibi yeni teknolojilerin ve mobil cihaz kullanımı, sosyal medya gibi uygulamaların beraberinde getirdiği risklere değinilmelidir.

Bu doğrultuda yeni teknolojilerin avantajlarının yanı sıra getirdiği riskler üzerine odaklanılmış ve katılımcı görüşlerinden örnekler verilmiştir.

8. Teknoloji eskimesiyle ilgili riskler açıklanmalıdır.

Teknolojinin değişmesi ve eskimesinin özellikle belgenin uzun vadeli geçerliliği ile delil değerini tehdit ettiği vurgulanmış, belgenin zamanında ve uygun formatta aktarılamamasının oluşturabileceği riskler anlatılmış ve çözüm önerileri sunulmuştur.

9. Eğitim materyalinin başlık hiyerarşisi, öneriler doğrultusunda yeniden yapılandırılmalıdır.

Bu doğrultuda, “Elektronik Belge Yönetim Sistemlerinde ve Süreçlerinde Risk Unsurları” tablosu yeniden düzenlenmiş ve başlıklara numaralar verilerek akış sağlanmıştır.

10. EBYS’de risk yönetimine yönetim desteğinin önemi vurgulanmalıdır.

Kurumlardaki yönetim kademesinin EBYS’ye yönelik desteğinin sistemin kurumsal önceliklere entegre edilmesi ve tüm birimlerce benimsenmesi açısından belirleyici olduğu vurgulanmıştır. Ayrıca yönetim desteğinin yetersiz olması durumunda karşılaşılabilecek riskler katılımcılardan elde edilen veriler doğrultusunda tablo halinde verilmiştir.

11. İnsan kaynaklı risklerin, risk yönetimindeki önemli rolüne mutlaka değinilmelidir.

EBYS’nin belirli bir birimde değil, kurumun tüm birimlerinde ve farklı düzeylerde görev yapan personel tarafından kullanıldığı, sistemin başarılı işleminde personelin kilit nokta olduğu vurgulanmıştır. Bunun yanı sıra personel devrinin hızlı olmasının beraberinde getirdiği riskler ele alınmıştır.

12. EBYS’de risk yönetimine ilişkin eğitimlerin düzenli olarak gerçekleştirilmesi ve bu süreçlerin denetimlerle desteklenmesinin önemi belirtilmelidir.

Bu doğrultuda eğitim materyaline, EBYS’nin etkin kullanımının personelin bilgi ve yetkinliğine bağlı olduğu, bu kapsamda personelin nitelikli eğitimlere ihtiyaç duyduğu ve eğitimin tek başına yeterli olmayıp denetim ve yaptırım mekanizmaları ile desteklenmesi gerektiğine ilişkin eklemeler yapılmıştır. Ayrıca konuyla ilgili katılımcı görüşüne yer verilmiştir.

13. Kurumlarda EBYS’de risk yönetimine ilişkin politika ve prosedürlerin geliştirilmesi ile ulusal düzeyde mevzuat hazırlanmasının gerekliliği vurgulanmalıdır.

Elektronik belge yönetim süreçlerinin kurum genelinde yürütülebilmesi için politika, prosedür ve yönergelerin varlığına gerek olduğu belirtilmiş, bu tür düzenlemelerin bulunmaması veya güncel olmamasının beraberinde getirdiği riskler tablo halinde sunulmuştur.

14. EBY sistem ve sürecinin yönetilmesinde bilgi işlem teknik personelinin yanı sıra bilgi profesyonellerinin de etkin rol alması gerektiğine dikkat çekilmelidir.

Bu doğrultuda EBYS'nin yönetimi için teknik personelin yanı sıra lisanslı belge yöneticisinin olması gerekliliği vurgulanmış ve bu uzman personel eksikliğinin oluşturacağı riskler vurgulanmıştır.

15. EBYS'de yalnızca tedarikçi firmaya bağımlı kalınmaması gerektiği ve kurumların sistem geliştirme sürecine doğrudan katkı sağlaması gerektiği ifade edilmelidir.

Bu doğrultuda tedarikçi firma seçiminde ve teknik şartnamede dikkat edilmesi gereken hususlara değinilmiş, tedarikçi/aracı firma anlaşmalarından doğabilecek riskler ele alınmış, katılımcı görüşlerine yer verilmiş ve kurumların bu sürece aktif olarak katılması gerektiği vurgulanmıştır.

16. Güncelleme, yedekleme, güvenlik ihlalleri gibi EBYS'yi doğrudan etkileyen tüm riskler için veri kaybını önleyici önlemlerin alınması gerektiğine ve bu doğrultuda güvenlik politikalarının oluşturulmasının önemine değinilmelidir.

Yedekleme, bakım, depolama, erişim, yetkilendirme gibi süreçlerde yapılan hataların meydana getirebileceği riskler ele alınmış, güvenlik politikaları, bilgi güvenliği standartları açıklanmış ve güvenlik ihlallerinin oluşturabileceği riskler tablo halinde sunulmuştur.

17. Birlikte çalışabilirlik ilke, standart ve mevzuatlarına uyulması gerektiğine değinilmelidir.

Katılımcılar ülkemizde bazı kurumların Birlikte Çalışabilirlik Esasları Rehberine uymadığını, örneğin farklı formatlarda belgeler üretildiğini dile getirmiş ve bu durumun eğitim materyaline eklenmesi gerektiğini ifade etmiştir. Bu doğrultuda

lkemizde EBYS'lerin birlikte alıřabilirlik erevesinde ilgili mevzuata ve rehberlerde, standartlarda belirtilen ilkelere uyulması gerektiđine iliřkin aıklamalar yapılmıřtır. Uyulmaması durumunda ortaya ıkabilecek riskler aktarılmıřtır.

18. Belge retimi ařamasında Standart Dosya Planı'na (SDP) uyulmamasının meydana getirebileceđi riskler aıklanmalıdır. SDP zerinde zellikle durulmalıdır.

Katılımcılar SDP'nin ve neminin kurumlarda yeterince bilinmediđini, yanlıř uygulamaların belge yařam dngsnde ciddi riskler oluřturduđunu ve bu alanın sunumda mutlaka anlatılması gerektiđini vurgulamıřtır. Bu dođrultuda stveri alanlarından biri olan SDP'ye ynelik risk unsurları aıklanmıř, katılımcı grřlerinden de yararlanılarak eđitim materyaline eklenmiřtir.

19. Kayıtlı Elektronik Posta (KEP), Elektronik Yazıřma Paketi (EYP) ve Devlet Teřkilatı Merkezi Kayıt Sistemi (DETSİS) kaynaklı riskler ele alınmalıdır.

Katılımcılar zaman zaman KEP, EYP ve DETSİS kaynaklı sorunlar yařandığını ve bunların eđitim materyaline eklenmesinin faydalı olacađını belirtmiřtir. Bu dođrultuda, bahsi geen terimlerin aıklamaları ve bu alana ynelik risklerin neler olabileceđi katılımcı grřlerine de yer verilerek materyale eklenmiřtir.

20. Eriřimle ilgili riskler ile belgelere zamanında eriřilememesinin yol aabileceđi olumsuzluklara mutlaka yer verilmelidir.

Bu dođrultuda, elektronik belgelerin sadece oluřturulması ve saklanması değil aynı zamanda yetkili kiřiler tarafından dođru zamanda, gvenli řekilde eriřilebilmesinin etkili belge ynetimin temel unsurlarından biri olduđu belirtilmiřtir. Bu nedenle eđitim materyalinde eriřimi etkileyecek unsurlara yer verilmiř ve bu alandaki riskler katılımcı grřleri dođrultusunda aıklanmıřtır.

21. Elektronik belgelerin arřivlenmesi konusuna mutlaka deđinilmeli ve lkemizde bu alanda gzlemlenen eksiklikler vurgulanmalıdır.

Katılımcılar elektronik arřivlemeyle ilgili belirsizliklerin olduđunu, birok kurumun EBYS ile entegre arřiv modln etkin bir řekilde kullanmadığını ve bunun getireceđi

ciddi risklerin olduğunu belirtmiştir. Bu doğrultuda kâğıt ve elektronik ortamdaki belgelerin arşivlenmesi hususu da materyale eklenerek elektronik arşivleme eksikliğinin getireceği riskler katılımcı görüşlerinden de faydalanılarak açıklanmıştır.

22. Ayıklama ve imha süreci detaylı olarak ele alınmalı ve bu süreçte karşılaşılabilecek riskler açıklanmalıdır.

Bu doğrultuda ayıklama ve imhayı etkileyebilecek personel yetersizliği/bilgi eksikliği, altyapı ve teknik kapasite, saklama süresi ve SDP'ye uyumsuzluk, kurumsal politika eksikliği, izlenebilirlik eksikliği ile hukuki riskler materyale eklenmiştir. Ayrıca tasfiye sürecinde meydana gelebilecek riskler katılımcı görüşleri dikkate alınarak tablo halinde sunulmuş ve katılımcıların bu konudaki görüş ve değerlendirmeleri materyale eklenmiştir.

23. Dijitalleştirme çalışmalarında ortaya çıkabilecek riskler eğitim materyali içerisinde yer almalıdır.

Bu doğrultuda, standart dışı tarama işlemleri, eksik veya hatalı dijitalleştirme, asıl belge ile dijital kopya arasında tutarsızlık, üstveri eksiklikleri, süreç yönetimi eksikliği, güncel olmayan format ve kısa süreli imha edilecek belgelerin dijital ortama aktarılmasından doğabilecek riskler ile bu durumun sonuçları materyale eklenmiştir.

3.4. Eğitim Materyalinin Etkinliğine İlişkin Bulgular

Bu başlık altında, eğitim materyalinin ne kadar etkili olduğunu belirlemek için yapılan testlere ait istatistiksel sonuçlara yer verilmektedir. EBYS'de risk yönetimi eğitiminin etkililiğini ölçmek için katılımcılara eğitim öncesi ve sonrası eğitim materyali kapsamındaki konularla ilgili oluşturulan 15 soruluk çoktan seçmeli, 5 soruluk da boşluk tamamlama formatında toplam 20 sorudan oluşan bir test uygulanmıştır. Eğitim öncesi ve sonrası yöneltilen sorular aynıdır. Eğitim öncesi gerçekleştirilen testin hemen ardından katılımcılara seminer verilmiş ve bu eğitim yaklaşık 2 saat sürmüştür. Eğitimin hemen sonrasında aynı test tekrarlanmıştır. Katılımcıların demografik özellikleri ve teste verdikleri cevaplar SPSS 20.0 programı aracılığıyla analiz edilmiştir.

Eğitime katılan katılımcıların özellikleri Tablo 3.32'de sunulmaktadır.

Tablo 3.32: Katılımcıların Özellikleri

<i>Değişkenler</i>	<i>N</i>	<i>%</i>
<i>Cinsiyet</i>		
Kadın	12	48%
Erkek	13	52%
<i>Yaş</i>		
18-22	0	%0
23-27	2	%8
28-32	1	%4
33-37	5	%20
38-42	6	%24
43+	11	%44
<i>Mezuniyet Derecesi</i>		
Lise	4	%16
Ön lisans	7	%28
Lisans	9	%36
Yüksek Lisans	4	%16
Doktora	1	%4
<i>Birim Türü</i>		
Akademik	7	%28
İdari	18	%72
<i>Risk Yönetimi Kavramına Aşinalık</i>		
Hiç aşına değilim	4	%16
Az düzeyde aşınayım	11	%44
Orta düzeyde aşınayım	6	%24
İyi derecede aşınayım	4	%16
Çok iyi derecede aşınayım	0	%0
<i>Memuriyet Süresi</i>		
1-3 yıl	3	%12
4-6 yıl	0	%0
7-10 yıl	1	%4
11-15 yıl	7	%28
16-20 yıl	4	%16
20+ yıl	10	%40
<i>Yazışma personeli olarak hizmet süresi</i>		
1-3 yıl	7	%28
4-6 yıl	4	%16
7-10 yıl	3	%12
11-15 yıl	8	%32
16-20 yıl	1	%4
20+ yıl	2	%8
<i>Kurumsal yazışmalarda riskli durumlarla karşılaşma durumu</i>		
Evet	7	%28
Hayır	18	%72

<i>Geçmişte benzer eğitim alınma durumu</i>	
Evet	3 %12
Hayır	22 %88

Tablo 3.32’ye göre katılımcıların %52’si (N=13) erkek, %48’i (N=12) ise kadınlardan oluşmaktadır. Yaş dağılımında 43 yaş ve üzeri katılımcılar %44’lük oranla (N=11) çoğunluğu teşkil etmektedir. Eğitim durumlarına bakıldığında ön lisans ve lisans mezunları %64 (N=16) grup içerisinde yüksek bir orana sahiptir. Katılımcıların mesleki tecrübelerinin de oldukça yüksek olduğu görülmektedir. Buna göre katılımcıların %84’ünün (N=21) 11 yıl ve üzeri memuriyet süresine sahip olması yazışma personeli arasında deneyimli çalışanların çoğunlukta olduğunu göstermektedir. Ancak katılımcıların %28’inin bu pozisyonda yeni olması da dikkat çekicidir.

Katılımcıların %60’ının (N=15) hiç ya da az düzeyde aşına olduğunu belirtmesi ve ‘çok iyi’ düzeyde aşına olan kimsenin bulunmaması, risk yönetimi kavramına aşinalık düzeyinin düşük olduğunu göstermektedir. Katılımcıların çoğunluğu %28 (N=7) riskli durumlarla karşılaşmadığını belirtse de testler arasındaki puan farkını katılımcıların kendi iş süreçlerindeki potansiyel hata kaynaklı risklerin yeterince bilincinde olmadıklarına ilişkin bir gösterge olarak değerlendirmek mümkündür. Daha önce benzer bir eğitim alan katılımcı oranının oldukça düşük olması (%12) konuyla ilgili personelin temel bilgilere ihtiyaç duyduğu şeklinde yorumlanabilir.

3.4.1. Normal Dağılım Analizi

Çalışmada kullanılan istatistiksel yöntemlerin geçerliliğini sağlamak amacıyla, öncelikle verilerin normal dağılıma uygunluğunun test edilmesi gerekmektedir. Katılımcı sayısının 30’un altında olması (N=25), parametrik testlerin uygulanabilmesi için normallik varsayımının kontrolünü zorunlu kılmaktadır (Field, 2018, s. 181; Shapiro ve Wilk, 1965, s. 610). Bu nedenle eğitim öncesi ve sonrası performans farklarının normal dağılım gösterip göstermediği analiz edilmiştir.

Öncelikle 20 soruluk testin sonuçları katılımcı bazında doğru (1) ve yanlış (0) olarak etiketlenerek katılımcıların ortalama performansları yüzde olarak eğitim öncesi ve sonrası için hesaplanmıştır. Bu doğrultuda ilk olarak eğitim öncesi ve sonrası uygulanan testte katılımcıların % performansları arasındaki fark alınarak ‘performans farkı’ değişkeni oluşturulmuştur. Örneğin eğitim öncesi testte %36 doğruluk

performansına sahip bir katılımcı eğitim sonrası testte %80 skora sahipse ‘performans farkı’ değişkeninde %44 değerini almıştır.

‘Performans farkı’ değişkeninin normal dağılım gösterip göstermediğini ölçmek için ilk olarak çarpıklık ve basıklık değerlerine bakılmaktadır. İkinci olarak Kolmogorov-Smirnov ve Shapiro-Wilk testleri uygulanmaktadır. Son olarak Q-Q grafiği (normal olasılık grafiği) incelenmektedir. Çarpıklık ve basıklık değerleri Tablo 3.3’te verilmektedir. Çarpıklık değeri (0,090) kritik seviye olan 0,05’ten büyük olduğu için anlamlı bir çarpıklık bulunmamaktadır. Basıklık değeri (-0,766) ise aynı şekilde kritik değerden büyük olduğu için anlamlı bir basıklık sapması bulunmamaktadır. Diğer bir ifadeyle yapılan testte ‘performans farkı’ değişkeni için çarpıklık ve basıklık değerleri normal dağılıma uygun şekilde gerçekleşmiştir.

Tablo 3.33: Çarpıklık ve basıklık analizi

	Çarpıklık		Basıklık	
	İstatistik	Standart Hata	İstatistik	Standart Hata
<i>Performans farkı</i>	0,090	0,464	-0,766	0,902

‘Performans farkı’ değişkeninin normal dağılım gösterip göstermediğini ölçmek için uygulanan Kolmogorov-Smirnov ve Shapiro-Wilk testleri Tablo 3.34’te gösterildiği üzere uygulanmıştır. Her iki testin p değerine bakıldığında kritik değer olan 0,05’ten büyük olduğu görülmektedir. Her iki testin sıfır hipotezi (H_0)⁶, verinin normal dağılıma uygun olduğu şeklindedir. P değerlerinin 0,05’ten büyük olması sıfır hipotezinin reddedilemeyeceğini ve verinin normal dağılıma uygun olduğunu göstermektedir.

Tablo 3.34: Normallik testi

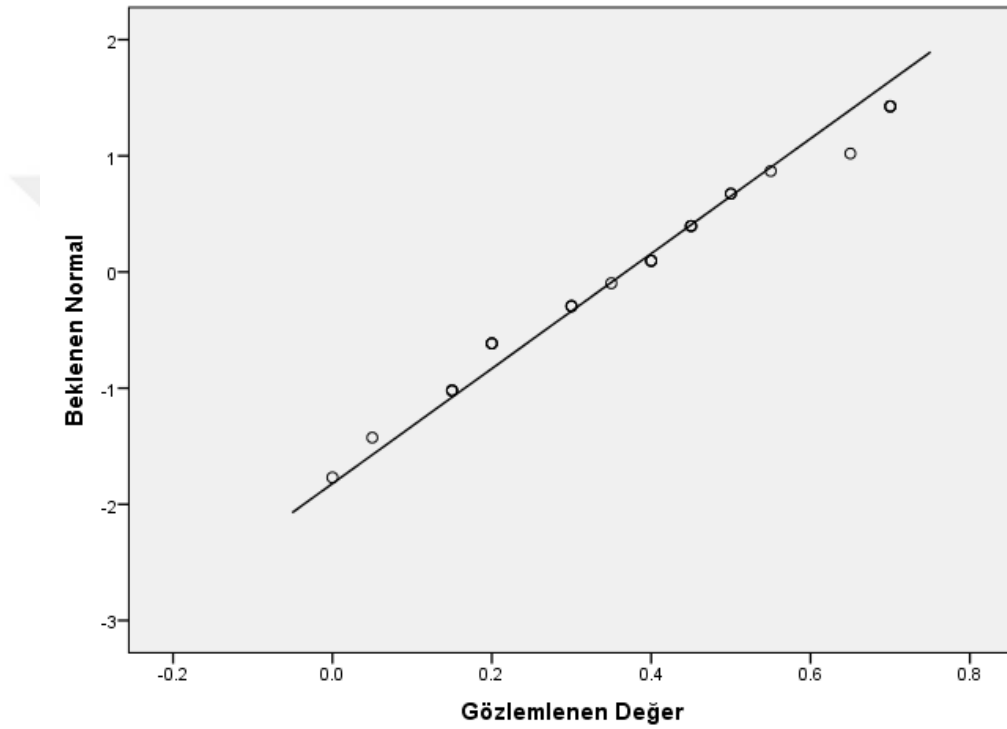
	Kolmogorov-Smirnov			Shapiro-Wilk		
	İstatistik	Serbestlik derecesi	p	İstatistik	Serbestlik derecesi	p
<i>Performans farkı</i>	0,117	25	0,200	0,960	25	0,406

Verinin normal dağılıma uygunluğu ile ilgili en çok kullanılan yöntemlerden biri de Q-Q grafiğidir. Her bir gözlem değerinin (X eksen), normal dağılımdan beklenen teorik değerlerle (Y eksen) karşılaştırıldığı noktalardan oluşan bu grafik (Wilk ve Gnanadesikan, 1968, ss. 5-6), Şekil 3.5’te performans farkı değişkeni için verilmiştir.

⁶ Sıfır hipotezi (H_0), istatistiksel testlerde görülen etkinin, farkın veya ilişkinin şansa bağlı sebeplerden ortaya çıktığı anlamına gelmektedir. Bu hipotez reddedilmek amacıyla kurulur (Kartal, 2022, s. 3).

Q-Q grafiğinde noktaların doğrusal örüntüden sapması, verinin normal olmadığına işaret etmektedir. Şekil 3.5'te görüldüğü üzere performans farkı değerlerinin genellikle referans çizgisi üzerinde yoğunlaştığı ve herhangi bir doğrusal olmayan örüntüye sahip olmadığı gözlemlenmiştir. Bu durum verinin normal dağılıma uygun olduğunu teyit etmekte ve parametrik testlerin uygulanabilirliğine işaret etmektedir.

Şekil 3.5: Q-Q Grafiği



3.4.2. Eğitimin Etkinliği

Performans farkı verisinin normal dağılıma uygunluğu, katılımcı sayısının 30'dan az olmasına rağmen parametrik testlerin uygulanabilirliğini ortaya koymaktadır. Katılımcıların aldıkları eğitimin etkililiğini ölçmek için aynı katılımcıların iki farklı koşul altındaki ölçümlerinin karşılaştırılması amacıyla kullanılan bağımlı örneklemeler t-testi kullanılmaktadır. Bu testte katılımcıların eğitim öncesi ve sonrası performansları karşılaştırılarak önemli bir fark olup olmadığı ölçülmektedir. Bu sebeple eğitim öncesi (ilk skor) ve sonrası (son skor) performans skorlarını içeren iki değişken analize dâhil edilmiştir.

Tablo 3.35’te bağımlı örneklem t-testi sonuçları yer almaktadır. Sonuçlara göre katılımcıların performanslarının eğitim sayesinde ortalama %36,8 oranında arttığı gözlemlenmiştir. Bağımlı örneklem t-testi sonuçlarında p değerine bakıldığında kritik değer olan 0,05’ten küçük olduğu görülmektedir. Bağımlı örneklem t-testinin sıfır hipotezi (H_0), iki örneklem arasında anlamlı bir fark olmadığı şeklindedir. P değerlerinin 0,05’ten küçük olması sıfır hipotezinin reddedileceğini ve eğitim öncesi ve sonrası performans skorları arasında istatistiksel olarak anlamlı bir artış olduğunu göstermektedir.

Tablo 3.35: Bağımlı örneklem t-testi sonuçları

	Eşleştirilmiş Farklar							
	Farkın %95 Güven							
	$\bar{x}$	σ	Std. Hata Ortalaması	Aralığı		t	Serbestlik derecesi	p
				Alt	Üst			
son skor – ilk skor	0,368	0,202	0,040	0,285	0,451	9,108	24	0,000*

* $p < 0,05$

3.4.3. Eğitim Materyalinin Konularına Göre Performans Değerlendirmesi

Katılımcıların tabi tutulduğu testte yer alan sorular yedi ana konudan oluşmaktadır. Testte yer alan sorular, eğitim sürecinde üzerinde durulan konu başlıklarının kapsam ve önem düzeyine göre hazırlanmıştır. Bu nedenle bazı ana konulara ilişkin olarak 5 soruya yer verilirken diğer bazı konular yalnızca 2 soruyla temsil edilebilmektedir. Örneğin standart dosya planı ve dosyalama süreci riskleri konusu dört soru ile temsil edilirken E-imza ve oturum güvenliği riskleri konusu ile ilgili iki soruya yer verilmiştir. Yazışma personeline yönelik hazırlanan eğitim materyali içerisindeki ana konular şu şekildedir:

- Standart Dosya Planı ve Dosyalama Risk Süreci
- EBYS Süreç Yönetimi ve Eğitim Eksikliği
- E-İmza ve Oturum Güvenliği
- Belge Dağıtım ve Yönlendirme
- Üstveri ve Belge Tanımlama
- Saklama Süreçleri ve İmha Riskleri

- Risk Kavramları

Bu yedi konu bazında eğitimin performans skorunda önemli bir artış sağlayıp sağlamadığı yine bağımlı örneklem t-testi ile ölçülmüştür. Tablo 3.36’da konu bazında bağımlı örneklem t-testi sonuçları yer almaktadır. Sonuçlara göre konu bazında performans skorunda %34 ile %44 arasında bir artış sağlandığı görülmüştür. En düşük performans artışının E-imza ve oturum güvenliği konusunda olduğu görülürken en yüksek artışın ise EBYS süreç yönetimi ve eğitim eksikliği konusunda olduğu gözlemlenmiştir. Tabloda p değerlerine bakıldığında bütün konularda istatistiksel olarak anlamlı bir performans artışı olduğu saptanmıştır.

Tablo 3.36: Konu bazında bağımlı örneklem t-testi sonuçları

	Eşleştirilmiş Farklar					t	Serbestlik derecesi	p
	$\bar{x}$	σ	Std. Hata Ortalaması	Farkın %95 Güven Aralığı				
				Alt	Üst			
SDP Konusu Son Test – SDP Konusu İlk Test	0,380	0,369	0,074	0,228	0,532	5,151	24	0,000
EBYS Süreci Konusu Son Test – EBYS Süreci Konusu İlk Test	0,440	0,583	0,117	0,199	0,681	3,773	24	0,001
E-imza Konusu Son Test – E-imza Konusu İlk Test	0,340	0,473	0,095	0,145	0,535	3,597	24	0,001
Dağıtım Konusu Son Test - Dağıtım Konusu İlk Test	0,380	0,354	0,071	0,234	0,526	5,361	24	0,000
Üstveri Konusu Son Test - Üstveri Konusu İlk Test	0,344	0,280	0,056	0,228	0,460	6,143	24	0,000
Saklama Konusu Son Test - Saklama Konusu İlk Test	0,360	0,396	0,079	0,197	0,523	4,548	24	0,000
Risk Kavramları Konusu Son Test - Risk Kavramları Konusu İlk Test	0,380	0,463	0,093	0,189	0,571	4,106	24	0,000

3.4.4. Katılımcı Özelliklerine Göre Performans Değerlendirmesi

Katılımcılardan test öncesi alınan demografik özellikler bazında performans artışında bir fark olup olmadığını ölçmek için bağımsız gruplar t-testi ve tek yönlü varyans analizi (ANOVA) kullanılmıştır. Katılımcı özelliği iki grup içerdiğinde bağımsız gruplar t-testi; ikiden fazla grup içerdiğinde ise tek yönlü ANOVA yöntemine başvurulmuştur. Tablo 3.37’de iki grup içeren cinsiyet, birim türü, riskli durumla karşılaşma ve benzer eğitim alma özellikleri için bağımsız gruplar t-testi analizi sonuçları yer almaktadır. Bağımsız gruplar t-testi analizini yapabilmek için öncelikle bu bağımsız grupların varyanslarının eşit olup olmadığı Levene testi ile ölçülmektedir. Varyansların eşit çıkması durumunda ($p>0,05$) bağımsız gruplarda ortalamaların eşitliği için t-testi sonuçlarına ‘varyanslar eşit’ satırından bakılmaktadır. Varyansların

eşit çıkmaması durumunda ise ortalamaların eşitliği için t-testi sonuçları ‘varyanslar eşit değil’ satırından izlenmelidir.

Tablo 3.37’ye bakıldığında ‘cinsiyet’, ‘birim türü’ ve ‘benzer eğitim alma’ özelliklerinde Levene testi p değerinin 0,05’ten büyük olduğu ve böylece varyansların eşit olduğu gözlemlenmektedir. Bu özelliklerde ‘Varyanslar eşit’ satırına bakıldığında p değerinin 0,05’ten büyük olduğu ve performans artışında bu özelliklerin grupları arasında önemli bir farklılık olmadığı sonucuna ulaşılmıştır. Diğer özellik olan ‘riskli durumla karşılaşma’ için Levene testi p değeri 0,05’ten küçük olduğu için ‘varyanslar eşit değil’ satırına bakılmış ve p değerinin 0,05’ten büyük olduğu gözlemlenerek yine gruplar arasında önemli bir farklılık olmadığı saptanmıştır.

Tablo 3.37: Bağımsız gruplar t-testi analizi sonuçları

		<i>Varyansların Eşitliği için Levene Testi</i>		<i>Ortalamaların Eşitliği için t-testi</i>					
		F	p	t	Serbestlik derecesi	p	Ort. Farkı	Std. Hata Farkı	Farkın %95 Güven Aralığı
									Alt Üst
<i>Cinsiyet</i>	Varyanslar eşit	0,139	0,713	0,921	23	0,367	0,075	0,081	-0,093 0,243
	Varyanslar eşit değil			0,921	22,908	0,366	0,075	0,081	-0,093 0,242
<i>Birim türü</i>	Varyanslar eşit	0,090	0,767	0,377	23	0,710	0,035	0,092	-0,155 0,224
	Varyanslar eşit değil			0,356	9,892	0,729	0,035	0,097	-0,182 0,251
<i>Riskli durumla karşılaşma</i>	Varyanslar eşit	5,877	0,024	0,486	23	0,632	0,044	0,091	-0,145 0,234
	Varyanslar eşit değil			0,382	7,568	0,713	0,044	0,116	-0,227 0,315
<i>Benzer eğitim alma durumu</i>	Varyanslar eşit	2,321	0,141	-1,411	23	0,171	-0,172	0,122	-0,424 0,080
	Varyanslar eşit değil			-2,764	7,246	0,027	-0,172	0,062	-0,318 -0,026

Katılımcı özelliklerinden ‘yaş’, ‘mezuniyet derecesi’, ‘risk yönetimi kavramına aşinalık’, ‘memuriyet süresi’ ve ‘yazışma personeli olarak hizmet süresi’ ikiden fazla grup içerdiği için tek yönlü ANOVA testine tabi tutulmuş ve sonuçlar Tablo 3.38’de verilmiştir. ‘Yaş’, ‘mezuniyet derecesi’, ‘risk yönetimi kavramına aşinalık’ ve ‘memuriyet süresi’ özelliklerinde tek yönlü ANOVA testi sonuçlarına göre gruplar arasında herhangi bir performans artışı farkına rastlanmamıştır ($p > 0,05$).

Tablo 3.38: Tek yönlü ANOVA analizi sonuçları

Özellik	Tür	Kareler toplamı	Serbestlik derecesi	Ortalama kareler	F	p
Yaş	Gruplar arası	0,061	4	0,015	0,330	0,855
	Grup içi	0,919	20	0,046		
	Toplam	0,979	24			
Mezuniyet derecesi	Gruplar arası	0,139	4	0,035	0,829	0,523
	Grup içi	0,840	20	0,042		
	Toplam	0,979	24			
Risk yönetimi kavramına aşinalık	Gruplar arası	0,098	3	0,033	0,780	0,518
	Grup içi	0,881	21	0,042		
	Toplam	0,979	24			
Memuriyet süresi	Gruplar arası	0,188	4	0,047	1,190	0,346
	Grup içi	0,791	20	0,040		
	Toplam	0,979	24			
Yazışma personeli olarak hizmet süresi	Gruplar arası	0,424	5	0,085	2,899	0,041*
	Grup içi	0,556	19	0,029		
	Toplam	0,979	24			

* $p < 0,05$

Tablo 3.38’e dikkatli bakıldığında, ‘yazışma personeli olarak hizmet süresi’ grupları arasında performans artışı açısından istatistiksel olarak anlamlı farklılık olduğu tespit edilmiştir ($p < 0,05$). Bu sonuç, en az bir hizmet süresi grubunun performans iyileştirme düzeyinin diğerlerinden anlamlı olarak farklı olduğunu göstermektedir. Hangi gruplar arasında anlamlı bir fark olduğunu saptamak için Tukey HSD veya Bonferroni post-hoc testlerine başvurulması gerekmektedir. Ancak bu testleri uygulayabilmek için her gruptan en az iki katılımcıya ihtiyaç duyulmaktadır. Yazışma personelinin hizmet süresi grupları arasından bir grubun katılımcı sayısı ikiden az (bir) olduğu için bu testler uygulanamamış ve hangi grubun diğer grup veya gruplardan anlamlı olarak daha fazla performans artışına sahip olduğu tespit edilememiştir.

3.5. 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. EBYS ve süreçlerine ilişkin risklerin tespiti ve yönetilmesi üzerinde durulan bu araştırma iki temel aşamadan oluşmaktadır:

1. EBYS’de risk yönetimi eğitim ihtiyacının belirlenmesi ve buna yönelik eğitim materyalinin geliştirilmesi amacıyla yapılan görüşmeler,

2. Geliştirilen eğitim materyalinin etkililik değerlendirmesi için, EBYS’de Risk Yönetimi eğitiminin verilmesi ve katılımcılara uygulanan testler.

Çalışmanın bu bölümünde hem eğitim ihtiyacının belirlenerek gelişmiş bir eğitim materyalinin oluşturulması amacıyla yapılan görüşmelerden hem de geliştirilen eğitim materyalinin etkililiğini değerlendirmek üzere uygulanan testlerden elde edilen bulgular literatüre dayalı olarak tartışılmaktadır.

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 3.4’e (Risk Yönetimi Yaklaşımı) göre, incelenen 13 kurumdaki 4’ü (%30,8) risk yönetimi konusunda planlı-programlı bir şekilde hareket ederken 5 kurum (%38,5) kısmi ve düzensiz bir yaklaşım sergilemektedir. Diğer 4 kurumda (%30,8) 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-programa sahip olmadığı ifade edilebilir. Risk yönetimi konusunda hiçbir çalışma yürütmeyen kurumların oranının %30,8 düzeyinde olması ise bu alanda ciddi bir iyileştirme yapılması gerektiğine işaret etmektedir.

Gelişmiş bir EBYS’de risk yönetimi eğitim materyalinin, uygulamadaki sorunların çözümüne katkı sağlayıp sağlayamayacağının anlaşılması, bu araştırmanın yürütülmesindeki temel bir gerekçelerden biridir. Türkiye’de kurum ve kuruluşlarda EBYS’nin uygulanmasında çeşitli zorluklarla karşılaşmaktadır. Personelin çalışma alışkanlıklarından vazgeçmekte isteksiz davranması ve dijital dönüşüme direnç

göstermesi bu zorlukların başında gelmektedir. Bu durumun temel gerekçeleri arasında, personelin sistemle ilgili yeterli bilgi ve farkındalığa sahip olmaması ve eğitim eksikliği gösterilebilir (Tahtaloğlu, 2018, ss. 142, 143). Benzer şekilde Johare (2007, s. 549) arşivci, belge yöneticisi, bilgi işlem personeli gibi çalışanların elektronik belgelerle ilgili rol ve sorumluluklarını yerine getirememesini bilgi ve beceri eksikliğine bağlamakta ve bunun ciddi sonuçlar doğurabileceğine dikkat çekmektedir. Bu nedenle kurumlar öncelikle eğitim gereksinimlerini tespit etmeli ve bu yönde eğitimler geliştirmelidir (Tahtaloğlu, 2018, ss. 143). Bu doğrultuda EBYS kullanıcılarına çalışmanın 'Bulgular' bölümündeki 'Risklerin Tespiti ve Yönetimine Yönelik Öneriler' alt başlığında bulunan Tablo 3.31'de (Eğitim materyalinin sunulmasının faydaları) sunulan araştırma verileri, EBYS paydaşlarının tamamının gelişmiş bir eğitim materyalinin kurumların risk yönetim planlarına önemli katkılar sağlayacağı konusunda hemfikir olduğunu göstermektedir. Özellikle alandaki çalışma eksikliğinin giderilmesi (%26,9), bilgi/farkındalık artışı sağlaması (%26,9) ve eğitim materyalinin sistemin doğru kullanımı ve süreç işleyişine katkı sağlaması en çok vurgulanan faydalar olarak öne çıkmaktadır. Bu nedenle söz konusu eğitim materyalinin geliştirilmesinin EBYS risk yönetimi uygulamalarını iyileştirmede etkili bir araç olabileceğini söylemek mümkündür.

EBYS projelerinin başarısı için (benimsenmesi ve uygulanması) insan faktörü son derece önemli bir unsurdur. Özellikle kişisel tutumlar, algı, farkındalık, güvenlik tehditlerinden duyulan korku ve nitelikli personel eksikliği gibi insana bağlı etmenler EBYS'lerin güçlü bir şekilde uygulanabilmesinin önüne geçmektedir. EBYS uygulamalarının niteliğinin artırılabilmesi için başta arşivciler ve belge yöneticileri olmak üzere EBYS ilgililerinin kapasitesinin eğitim yoluyla artırılması gerekmektedir (Clemence, Luambano ve Mwantimwa, 2025, s. 349). Bu doğrultuda çalışmada öncelikle, literatürden derlenen bilgiler ışığında taslak bir eğitim materyali oluşturulmuştur. Ancak bu bilgiler gelişmiş bir eğitim materyalinin ortaya çıkarılabilmesi için yeterli olmamıştır. Bu nedenle eğitim materyalini iyileştirmeye yönelik olarak, çeşitli kurum ve kuruluşlarda EBYS sorumlusu olarak görev yapan personel, alan uzmanları ve akademisyenler ile EBYS tedarikçisi firmaların yetkilileriyle görüşmeler gerçekleştirilmiştir. Bu görüşmelerden eğitim materyalinin iyileştirilmesine yönelik veriler elde edilmiştir. Bu veriler değerlendirilerek eğitim

materyalinde ağırlıklı olarak hangi konulara yer verilmesi anlaşılmıştır. Ayrıca bu veriler, eğitim materyalinin iyileştirilmesi amacıyla bazı hususlara dikkat çekmiştir. Bu bağlamda katılımcılar özetle, EBYS'nin temel kavramları ile risk unsurları arasındaki ilişkinin giriş bölümünde açıklanmasını, belge yönetimi standartlarına atıf yapılmasını, ulusal düzeyde mevzuat geliştirilmesinin önemine değinilmesi gerektiğini ifade etmiştir. Bununla birlikte materyalin somut olay örnekleriyle, katılımcı görüşleriyle ve görsellere zenginleşmesi gerektiğini ifade eden katılımcılar, mevcut ve potansiyel risklerin anlaşılır bir dille ele alınmasının önemine dikkat çekmiştir. Ayrıca materyalde Standart Dosya Planı (SDP), Kayıtlı Elektronik Posta (KEP), Elektronik Yazışma Paketi (EYP) ve Devlet Teşkilatı Merkezi Kayıt Sistemi (DETSİS) kaynaklı hataların erişim ve arşivleme ile ilgili yaratacağı sorunların ayrıntılı biçimde incelenmesi gerektiği aktarılmıştır. Bunun yanı sıra tasfiye ve dijitalleştirme süreçlerinde ortaya çıkabilecek riskler ile bunları meydana getiren etmenlerin açıklanması gerektiğini vurgulayan katılımcılar, EBYS'de yönetimin desteği, düzenli eğitimler ve bilgi profesyonellerinin etkin rolünün önemine değinmiştir. Son olarak kurumların tedarikçi firmaya bağımlı kalmadan sistem geliştirebilmesinin ya da sistem geliştirme süreçlerinde belge yöneticilerinin etkin rol oynayabilmesinin altını çizen katılımcılar bahsi geçen tüm bu konulara değinilmesinin ve risklerin azaltılmasına katkı sağlayan kapsamlı bir eğitim materyalinin ortaya çıkarılmasının önemli olduğunu belirtmiştir. Bu nedenle çalışmada, eğitim materyalinin geliştirilmesi sürecinde, katılımcılardan elde edilen tüm veriler özenle değerlendirilmiş ve eğitim materyaline yansıtılmıştır. Bu doğrultuda eğitim materyalinde sunulan konuların, katılımcıların bilgi ve farkındalık düzeylerinde artış sağlayıp sağlamadığı bağımlı örneklem t-testiyle ölçülmüş (bkz. Tablo 3.36) ve konu bazında performans skorlarında %34 ile %44 arasında bir artış sağlandığı görülmüştür. Önemli bir artışa işaret eden bu oranlarda, eğitim materyalinin hazırlanmasında katılımcı görüşlerine yer verilmesinin etkili olduğu değerlendirilmektedir.

Akdoğan ve Özdemirci (2017, ss. 251-252) bir kurumdaki tüm çalışanların EBYS uygulamalarının muhatabı olduğunu ve kapsama alanı bu denli yaygın olan elektronik belge yönetimi uygulamalarının başarılı bir şekilde sürdürülebilmesi için her düzeyden kullanıcının eğitilmesi gerektiğine vurgu yapmaktadır. Tahtalıoğlu ise (2018, ss. 142,

143) kurumların EBYS'ler için çeşitli eğitim rehberleri yayımladığına ancak bu materyallerin kullanıcılar üzerindeki etkililiğinin bilinmediğine dikkat çekmektedir. Bu çalışmanın eğitim materyalinin etkililik düzeyinin değerlendirilmesi temel odak noktalarından biridir. Bu doğrultuda, geliştirilen eğitim materyali aracılığıyla düzenlenen seminer programının etkililiği analiz edilmiştir. Bulgular bölümünde 'Eğitimin Etkinliği' alt başlığında sunulan analiz sonuçları, EBYS risk yönetimi eğitim programının ÇAKÜ personeli üzerinde kayda değer bir etki yarattığını ortaya koymuştur. Bağımlı örneklem t-testi sonuçları, katılımcıların performansında ortalama %36,8'lik bir artış olduğunu göstermektedir. Bu bulgular, söz konusu eğitim programının EBYS kullanıcılarının bilgi düzeyinde önemli bir iyileşme sağladığı anlamına gelmektedir.

EBYS kullanıcılarının risk yönetimine ilişkin bilgi ve farkındalık seviyelerinde gözlemlenen bu artış tek başına eğitim materyalinin etkililiğiyle açıklanamamalıdır. Ayrıca eğitimi veren kişinin yetkinliği, konuya hâkimiyeti ve süreci yönetebilme becerisi de önemlidir. Taşkaya (2012, s. 283), eğitimin niteliğini etkileyen unsurların başında eğitimcinin geldiğini ifade etmektedir. Benzer şekilde eğitimcinin eğitim sürecine katkısının son derece önemli olduğuna değinen Sayan (2015, ss. 590-591), eğitimcinin sahip olması gereken nitelikleri; konuya hâkim olma, hedef kitleyi tanıma, eğitim etkinliklerini planlama, öğreteceği konunun özelliğine göre öğretim yöntem ve tekniklerini kullanabilme, öğrenenlerle sağlıklı iletişim kurabilme, öğrenme ortamını öğrencilerin ve ders konusunun özelliklerine uygun hale getirebilme ve derse aktif katılımı sağlayabilme şeklinde sıralamaktadır. Bu çalışmada, eğitim programının başarıya ulaşabilmesi için planlama aşaması titizlikle yürütülmüştür. Ayrıca hazırlanan eğitim materyalindeki konulara yoğun bir şekilde çalışılmış ve konuya hâkimiyet sağlanmıştır. Eğitim öncesinde, eğitim verilecek salon hazırlanmış, katılımcıların odaklanabilmesini sağlayacak (ışık, iklimlendirme, görüntü netliği, ses/gürültü vb.) önlemler alınmıştır. Eğitim sırasında, materyalde yer alan konular, senaryolar ve örnekler katılımcıların ilgisini çekecek şekilde aktarılmıştır. Bunun için eğitim öncesinde provalar yapılmıştır. Eğitim yaklaşık 2 saat sürmüştür. Bu süreçte katılımcıların odaklarını kaybetmemesini ve konuya olan ilgisinin artmasını sağlamak amacıyla zaman zaman katılımcılara söz hakkı verilmiş, deneyimlerine ve konuyla ilgili yorumlarına başvurulmuştur. Bunların yanı sıra katılımcılara uygulanan testler,

eğitim başlamadan sona erdirilmiş ve soru formları toplanmıştır. Eğitim sonrası uygulanan test formu ise sunumun ardından dağıtılmıştır. Böylece eğitim esnasında katılımcıların dikkatinin dağılmaması sağlanmıştır. Bu aşamaların itinayla uygulanmasının katılımcıların konuyla ilgili bilgi ve farkındalık düzeylerinin artmasında ve eğitimin başarıya ulaşmasında önemli bir payı olduğu değerlendirilmiştir.

Eğitim materyalinin iyileştirilmesi ve eğitimin etkili olup olmadığının anlaşılması için öne çıkan bulgular araştırma soruları bağlamında tartışılmıştır. Bunun yanı sıra çalışmada EBYS’de risk yönetimi konusunda ülkemizdeki mevcut durumun anlaşılması amacıyla görüşmelerden elde edilen verilere de yer verilmiştir. Bu veriler değerlendirildiğinde birçok önemli bulgunun olduğu anlaşılmış ve bu sebeple tartışma konusu olmuştur.

Bilgi ve belge güvenliği için politikalar, talimatlar, prosedürler ve formlar oluşturmali, 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 3.1). Önlem eksikliği sonucunda beklenmedik olayların, en çok risk yaratacağı alanlar ise veri kaybı ve veri güvenliğidir (bkz. Tablo 3.2). Bu durum kurumların önlem alma konusunda yetersiz olduğunu, EBYS’ye yönelik olağanüstü hâl senaryolarını geliştirmediğini göstermektedir. Bunun neticesinde sistemdeki 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 3.4) teknolojik risklerin katılımcılar tarafından üzerinde önemle durulan bir konu olduğunu göstermektedir. Yeni teknolojilerin getireceği riskler arasında güvenlik/gizlik, teknolojik alt yapının 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, veri

ihlali gibi potansiyel birçok riski akıllara getirmektedir. Mooradian, Franks ve Srivastav (2025, s. 157), kurum ve kuruluşların iş yapma biçimlerini iyileştirmek amacıyla yapay zekâyı giderek daha fazla benimsediğine dikkat çekmektedir. Ancak yapay zekânın sağladığı pek çok fayda olsa da başta veri gizliliği olmak üzere birçok riski 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.

EBYS’lerde doğru yapılmadığı takdirde beraberinde birçok risk unsuru getiren önemli bir husus da SDP’dir. SDP kodlarının doğru seçilmesi belge yaşam döngüsünün verimli yönetilebilmesi ve belgelere erişimde sorun yaşanmaması için önemlidir. Fakat kişisel, kurumsal veya yönetsel koşulların oluşturduğu belirsizlikler neticesinde SDP kodlarının atanmasında yapılan hatalar, belge yaşam döngüsünün tamamlanamamasına ve bunun neticesinde önemli risklerin ortaya çıkmasına neden olabilmektedir (Binici, 2019, ss. 119-120). Araştırma bulguları (bkz. Tablo 3.21) bu riskler arasında belgelere erişim, tasfiye sürecinde zorluk, yanlış imha ve hukuki riskler olduğunu göstermektedir. Buna göre SDP’nin belge yaşam döngüsünün her aşamasında önemli olduğu, verilen kodların ve yapılan dosyalamaların hem idari hem de yasal riskler barındırdığı ifade edilebilir.

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. Ancak elektronik ortamda tasfiye sürecinin doğru işletilebilmesi için alt yapı sorunları ve önemli belirsizlikler mevcuttur (Çiçek, 2021, ss. 52) Araştırma bulguları (bkz. Tablo 3.25) 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 Başkanlığı'nın yol göstermesi gerekmektedir. Ancak araştırma bulgularından Başkanlığın pasif kaldığı ve yeterli alt yapıya sahip olmadığı anlaşılmıştır. Buna göre EBYS standartlarını ortaya koyan Devlet Arşivleri Başkanlığı'nın eksiklikleri tamamlamak ve belirsizlikleri çözmek için daha aktif çalışması gerekmektedir.



4. SONUÇ VE ÖNERİLER

Yakın geçmişte geleneksel olarak (fiziksel ortamda) sürdürülen belge yönetimi, günümüzde elektronik ortamda gerçekleştirilmektedir. Hem geleneksel ortamdaki elektronik ortama geçiş sürecinde hem de geçiş sonrası uygulamalarda bazı belirsizlikler, eksiklikler ve hatalar nedeniyle çok çeşitli riskler ortaya çıkabilmektedir. Gerek mevzuattaki belirsizlikler ya da politikalardaki eksiklikler gerekse EBYS sistem ve süreçlerinde insan kaynaklı hatalar nedeniyle bu riskler meydana gelebilmektedir. Bir kurumda, EBYS kullanıcıları o kurumun çalışanlarıdır. Bu kişiler aynı zamanda EBYS üzerindeki belge yaşam döngüsünü belirlemektedir. Dolayısıyla belge üstveri tanımlamaları ve SDP kodu gibi alanlarda personel tarafından yapılan hatalar birçok önemli risk meydana getirebilmektedir. Bu nedenle personelin EBYS üzerinde gerçekleştirdiği işlemlerin niteliği, hatalı durumlarda hangi risklerin ortaya çıkabileceği ve bunun sonucunda ne tür yaptırımların uygulanabileceği gibi bilgi ve farkındalık eksikliklerinin giderilmesi, EBYS risk yönetimi açısından oldukça değerli görülmüştür. Böylece EBYS kullanıcıları yaptıkları işlemler sonucunda ne tür risklerin ortaya çıkabileceğini anlayacak ve hatalar azalacaktır. Ayrıca EBYS paydaşlarının elinde olmadan ortaya çıkabilecek riskler (ör. doğal afetler gibi beklenmedik bir zamanda, aniden gelişebilecek riskler) için ne tür önlemler alınması gerektiği, ortaya çıktığında nasıl müdahale edeceği gibi konulardaki bilgi eksikliğinin giderilmesiyle bu tür risklerin meydana getirebileceği zararın azalması sağlanabilecektir.

Personelin söz konusu eksikliklerinin giderilmesi eğitim ile mümkündür. Bu doğrultuda, ülkemizdeki kurum ve kuruluşların personelinin EBYS sistem ve süreçlerinde risk yönetimi konusunda eğitmek için kullanabilecekleri gelişmiş bir eğitim materyalinin hazırlanması son derece önemli görülmüştür. Bu nedenle çalışmada EBYS kullanıcılarının bilgi ve farkındalık eksikliklerinin giderilmesi için yararlanılabilecek bir eğitim materyali geliştirilmiş ve materyalin etkili olup olmadığı sınanmıştır. Bu kapsamda eğitim materyalinin geliştirilmesi aşamasında toplanan veriler ve materyalin test edilmesiyle elde edilen bulgular araştırma sorularına yanıt vermiş ve aşağıdaki sonuçlara ulaşılmıştır:

- Araştırmada merak edilen ilk temel soru, Türkiye’deki kurumların EBYS için kurumsal risk yönetim planları geliştirip geliştirmediğidir. Bu inceleme,

ülkemizdeki EBYS risk yönetimi uygulamalarının mevcut durumunu anlamak açısından önemli görülmüştür. Elde edilen veriler, EBYS risk yönetimi uygulamaları konusunda kurumlar arasında önemli farklılıklar olduğunu ortaya koymaktadır. Araştırmada görüşme yapılan kurumların büyük çoğunluğunun EBYS’de risk yönetimine yönelik kısmi çalışmalar yürüttüğü ya da hiçbir uygulamasının bulunmadığı anlaşılmıştır. Bu nedenle ‘Kurumlarda EBYS’ye yönelik kurumsal risk yönetim planları oluşturulmuş mudur?’ sorusuna, Türkiye’deki kurumların önemli bir kısmında kayda değer bir çalışmanın olmadığı yanıtı verilebilir.

- Bu araştırmanın temel gerekçelerinden biri, EBYS’de risk yönetimini konu edinen bir eğitim materyali aracılığıyla personelin bilgi ve farkındalık düzeylerinin artırılmasının uygulamadaki sorunların çözümüne katkı sağlayıp sağlayamayacağını anlamaktır. Bu nedenle çalışmada “*EBYS sorumluları, belge yönetimi uzmanları ve akademisyenler ile EBYS yazılım firmaları, gelişmiş bir eğitim materyalinin kurumların risk yönetim planlarına katkı sağlayacağını düşünmekte midir?*” soruna yanıt aranmıştır. Kurumlar, akademisyenler, alan uzmanları ve EBYS firma temsilcileriyle gerçekleştirilen görüşmeler neticesinde EBYS paydaşlarının risk yönetimi konusunda hazırlanan gelişmiş bir eğitim materyalinin kurumların risk yönetim planlarına önemli katkılar sağlayacağı konusunda hemfikir oldukları anlaşılmıştır. Paydaşlar, eğitim materyali sayesinde alandaki çalışma eksikliğinin giderileceğine, yöneticilerin, bilgi işlem personelinin ve EBYS kullanıcılarının bilgi/farkındalık düzeylerinin artacağına, sistemin doğru kullanımıyla süreç işleyişine önemli katkılar sağlanacağına dikkat çekmiştir. Bunlar ışığında, EBYS’de risk yönetimini konu edinen bir eğitim materyalinin geliştirilmesinin EBYS risk yönetimi uygulamalarını iyileştirmek için etkili bir yöntem olduğu sonucuna varılmıştır.
- Bu çalışmanın asıl odak noktası geliştirilen eğitim materyalinin etkililik düzeyini belirlemektir. Bu nedenle araştırmada “*EBYS risk yönetimi eğitimi alan ÇAKÜ personelinin, eğitim öncesi ve sonrası bilgi düzeyleri arasında anlamlı bir fark oluşmuş mudur?*” sorusuna yanıt aranmış ve EBYS risk yönetimi eğitim programının, eğitime katılan ÇAKÜ personeli üzerinde önemli bir etki yarattığı anlaşılmıştır. Bu nedenle, söz konusu eğitim

programının EBYS kullanıcılarının bilgi düzeyinde önemli bir iyileşme sağladığı sonucuna varılmıştır.

Araştırmada yanıtı aranan sorular cevap bulmuştur. Bu doğrultuda sınanmak istenen hipotez için şu sonuca varılmıştır:

- Bu araştırmada geliştirilen EBYS risk yönetimi eğitim materyalinin etkililiğini ölçmek amacıyla deneysel bir çalışma yürütülmüştür. Çalışma kapsamında ÇAKÜ’de görev yapan yazışma personeline eğitim materyali temel alınarak bir seminer programı uygulanmıştır. Eğitimin etki düzeyini belirlemek üzere materyalde yer alan konuları kapsayan bir test geliştirilmiştir. Katılımcılar hem seminer öncesinde hem de sonrasında bu teste tabi tutulmuş ve eğitimin bilgi düzeyi üzerindeki etkisi ölçülmüştür. Yapılan karşılaştırmalı analizler, eğitim sonrasında katılımcıların bilgi düzeylerinde istatistiksel olarak anlamlı bir artış olduğunu ortaya koymuştur. Bu durum, *“EBYS risk yönetimi eğitim programının, kullanıcıların bilgi ve farkındalık düzeylerini artırmada ve elektronik belge yönetimi sistem ve süreçlerinde karşılaşılabilecek risk unsurlarını azaltmada anlamlı bir etkisi vardır.”* hipotezini doğrulamaktadır.

Araştırma soruları yanıt bulmuş ve hipotez doğrulanmıştır. Bunun yanı sıra 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, yoğun iş yükü gibi risklere neden olduğu anlaşılmıştır.

- Kurumların pek çoğunda EBYS'ye yönelik politika ve prosedürlerin oluşturulmadığı belirlenmiştir.
- EBYS'lerde risk yönetimine ilişkin kurumsal analizlerin etkin bir şekilde yapılmadığı ve risk yönetim mekanizmalarının işletilmediği anlaşılmıştır.
- Kurumlarda EBYS'ye yönelik yönetim desteğinin, sistemin başarısı ve verimli bir şekilde sürdürülebilmesi için son derece önemli olduğu anlaşılmıştır.
- EBYS sistemlerinin tasarımında ve yapılandırmasında kurumsal analizlerin eksikliği ve firmaya aşırı bağımlılık unsurlarının ciddi riskler meydana getirebileceği 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.
- Çoğu kurumda EBYS ile entegre çalışan bir e-arşiv modülünün bulunmadığı, bazı kurumlarda ise bu modülün verimli bir şekilde kullanılmadığı anlaşılmıştır.

Çalışma kapsamında araştırma soruları yanıt bulmuş, hipotez doğrulanmış ve araştırmada ulaşılan önemli sonuçlar açıklanmıştır. Buna göre araştırma aşağıda sıralanan katkıları sağlamaktadır:

- Araştırma kapsamında geliştirilen eğitim materyalinin EBYS kullanıcılarının risk yönetimi konusunda bilinçlenmesine katkısı vardır.
- Araştırma kapsamında geliştirilen eğitim materyalinin kurumların EBYS risk yönetimi uygulamalarını iyileştirmesine katkısı vardır.
- Bu çalışma literatürdeki boşluğu doldurmaya katkı sağlamaktadır.
- Bu araştırma, ülkemizdeki EBYS’de risk yönetimi uygulamalarının anlaşılmasına katkı sağlamaktadır.
- Bu çalışma, yöneticilerin, bilgi işlem personelinin ve EBYS kullanıcılarının bilgi/farkındalık düzeylerini artırarak sistemin doğru kullanımına ve sürecin verimliliğinin artmasına katkı sağlamaktadır.

Çalışma kapsamında elde edilen bulgular doğrultusunda aşağıdaki öneriler sunulabilir:

- Geliştirilen eğitim materyalinin EBYS kullanıcılarına risk yönetimi konusunda önemli faydalar sağladığı araştırma sonuçlarıyla ortaya konmuştur. Bu durum benzer kurumların da personelinin bu materyalle eğitebileceğine işaret etmektedir. Böylece çalışanların EBYS’de risk yönetimine ilişkin bilgi ve farkındalık düzeyleri artırılırken, sistem ve süreçlerdeki risklere karşı alınan önlemler de güçlenecektir.
- Geliştirilen eğitim materyalinin farklı sektörlere uyarlanması ve daha geniş kitlelere ulaştırılması önerilmektedir.
- Çalışmada bir seferlik verilen bir eğitimin sonuçları değerlendirilmiştir. Ancak bu eğitimlerin periyodik olarak tekrarlanması öğrenilen bilgilerin kalıcılığını artırılabilir. Ayrıca eğitim sonrası katılımcılardaki gelişmelerin izlenmesi ve ihtiyaca göre materyalde güncellemeler yapılması önerilmektedir.
- Katılımcıların bilgi düzeyini ve risk yönetimi deneyimini artırmak için hazırlanan eğitim materyaliyle verilen teorik eğitime ek olarak çeşitli uygulamalar yapılması önerilmektedir.
- Risk yönetiminin kurum kültürünün önemli bir parçası haline gelmesi önemlidir. Bunun için kurumun en üst amiri başta olmak üzere birim amirlerinin süreci sahiplenmesi önkoşuldur. Bu nedenle eğitimlere üst düzey yöneticilerin de dâhil edilmesi gerekmektedir. Bu sayede risk yönetimi, kurumsal düzeyde stratejik bir önem kazanabilir.

- Her kurumun risk profili yapısal olarak farklılık göstermektedir. Bu nedenle risk yönetimi eğitimlerinin kurumun faaliyet alanına, büyüklüğüne ve ihtiyaçlarına uygun şekilde özelleştirilmesinin daha etkili sonuçlar doğuracağı düşünülmektedir.
- Görüşme yapılan kurumların önemli bir kısmında EBYS kapsamında risk yönetimi mekanizmalarının etkin işlemediği görülmüştür. Bu nedenle kurumların mevcut risk yönetimi mekanizmalarını yeniden değerlendirmeleri ve gerekli yapısal iyileştirmeleri yapmaları önerilmektedir.
- Kurumların riskleri etkin bir şekilde yönetebilmesi için bilgi ve belge yönetimi bölümü mezunlarının EBYS ve arşivleme süreçlerinde görevlendirilmesi önerilmektedir. Araştırma bulguları (bkz. Tablo 3.30), 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 tavsiye edilmektedir.
- 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 önerilmektedir.
- Ulusal ölçekte belge yönetimine ilişkin risk yönetim stratejilerinin belirlenmesi büyük önem taşımaktadır. Araştırma bulguları (bkz. Tablo 3.30), 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 işbirliği

yapması gerekmektedir. Bu işbirliği 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. Ancak 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

personelerle 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 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. 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 kodlarının standartlaşmasını sağlayacağı gibi kodların doğruluğunu artırabilir.
- 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 yapılmasına neden olmaktadır. Verimliliği artırmak ve kaynakları daha etkin kullanmak amacıyla Üniversite Yönetim Kurulu tarafından tüm birimlere duyurulacak bir karar ile fiziki belge kullanımının en aza indirilmesi hedeflenmelidir. Bu hedef doğrultusunda caydırıcılığın sağlanması için cezai yaptırımlar belirlenmeli ve uygulanmalıdır.
- Eskimiş veya gereksiz belgelerden kurtulmak, disk alanı açmak gibi nedenlerle gerçekleştirilen silme işlemi, önemli bir belgenin geri dönüşümsüz olarak silinmesine neden olabilir. Bu durum, hukuki sorunlara veya iş

süreçlerinde aksamalara yol açabilir. EBYS, sistem yöneticisinin dahi bir belgeyi silmesine izin vermeyecek şekilde yapılandırılmalıdır.

- Birim, bölüm amirlerinin değişmesi durumunda yeni gelen yöneticinin eski belgelere erişiminin olmaması dosya bütünlüğünü bozmakta, iş akışında sorunlar meydana getirmekte, doğru ve zamanında karar vermeyi zorlaştırmaktadır. Bu nedenle yapılan sevk işlemlerinin, kullanıcılar yerine rollere göre yapılması; yeni atanacak yöneticilerin, kendilerinden önceki yöneticilerin işleriyle ilgili tüm belgelere otomatik olarak erişim sağlamasını sağlayarak iş sürekliliğini destekleyecektir. Ayrıca belge klasörleri oluşturulurken bireysel klasör değil birim klasörü şeklinde tanımlama yapılması herhangi bir amir değişikliğinde yeni gelen kişinin oluşturulmuş klasöre erişimini sağlayacaktır.
- Alanda gözlemlenen bir diğer önemli sorun da dosya tasnif planı ile sisteme dâhil edilen her bir eleman için saklama planında bir saklama süresi ve tasfiye işleminin tanımlanmamış olmasıdır. Bu durum belge yönetiminin gerçekleşmemesine neden olmaktadır. Bu nedenle saklama planları EBYS'ye entegre edilmelidir. 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 ile bütünleşik çalışan bir elektronik arşivleme modülünün bulunmaması ihtiyaç duyulduğunda belgelere erişimi zorlaştıracak 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.

- Elektronik ortamda ayıklama-imha prosedürleri belirlenmemiş olması sistem kapasitesinin dolmasına, sistemin yavaşlamasına ve ihtiyaç anında belgeye erişim sorunlarına neden olmaktadır. Bunun için belgelerin önem ve saklama sürelerine göre sınıflandırılması ve saklanmasına lüzum görülmeyen ve saklama süresini dolduran belgelerin gerekli olur ve onay alındıktan sonra güvenli bir şekilde imha edilmesi gerekmektedir. Tüm imha işlemleri detaylı bir şekilde kayıt altına alınmalıdır. Kurumların bu işlemleri sağlıklı yürütülebilmesi için Devlet Arşivleri Başkanlığı'nın bir talimat yayınlaması ve süreci denetlemesi gerekmektedir.
- Kurumun genel elektronik belge yönetimi performansını ölçmek için herhangi bir planının veya yönteminin bulunmaması, iş süreçlerinin ne kadar sürdüğü, hangi aşamalarda gecikmeler olduğu gibi verilerin elde edilememesine ve bu nedenle süreçlerin iyileştirilmemesine neden olmaktadır. Bu nedenle kurumların belge oluşturma süresi, belge erişim süresi, hata oranı gibi performans göstergelerine ilişkin verileri elde edilebileceği bir yöntem geliştirilmesi gerekmektedir. Elde edilen veriler düzenli olarak analiz edilmeli ve raporlanmalıdır. Ayrıca sistem kullanıcılarının görüşlerine başvurulmalı ve sistemin kullanım kolaylığı ve etkinliği değerlendirilmelidir. İş süreçleri baştan sona incelenerek iyileştirme alanları belirlenmelidir.

Araştırma sonuçları kurum ve kuruluşlarda hali hazırda devam eden EBYS uygulamalarının pek çok potansiyel risk barındırdığını ortaya koymaktadır. Bu nedenle öncelikle ülke çapında eksik görülen mevzuat için çalışmalar yapılması gerekmektedir. Bu çalışmalarda belge yöneticilerinin de rol alması, kurum ve kuruluşlarda uygulamadaki eksikliklerin/hataların giderilmesi ve mevzuat-uygulama uyumsuzluğunun engellenmesi açısından önemlidir. Bu süreçte kurumların da üzerine düşen pek çok sorumluluk vardır. Kurum ve kuruluşlar EBYS uygulamalarını mevzuata uygun bir şekilde yapılandırmalı ve ivedilikle risk planlarını hazırlayarak risk yönetim mekanizmalarını hayata geçirmelidir. Aksi takdirde sorunlu uygulamaların beraberinde getireceği riskler ve bunların ciddi sonuçlarıyla yüzleşmek zorunda kalacaklardır.

Kurum ve kuruluşlarda EBYS'lerin en önemli paydaşı kurum çalışanlarıdır. Personel tarafından gerçekleştirilen hatalı uygulamalar sonucu pek çok ciddi risk ortaya çıkabilmektedir. Bunun nedenini personelin yaptığı hatalı işlemlerin sonucunda meydana gelecek riskler konusunda yeterli bilgiye ve farkındalığa sahip olmamasıdır. Bu nedenle personel tarafından EBYS üzerinde gerçekleştirilen işlemlerin iyileştirilmesi sağlanmalıdır. Ayrıca yapılan hatalı işlemlerin sonucunda ne tür risklerin oluşabileceği detaylı bir şekilde aktarılmalıdır. Bunun en etkili yolu ise kurumlarda düzenli olarak EBYS ve risk yönetimi eğitimlerinin verilmesidir. Bu eğitimlerde belge yönetimi sürecinden maksimum verimin elde edilebilmesine yönelik konular üzerinde durulmalı ve EBYS kullanımı, belgenin üretiminden dosyalanmasına, dağıtımından tasfiyesine kadar olan tüm süreci kapsayacak biçimde ele alınmalıdır. Eğitim, EBYS üzerinde yapılan hatalı işlemlerin sonuçlarında ortaya çıkabilecek riskler üzerine örnek senaryolarla zenginleştirilmeli ve yapılması gereken doğru işlemler detaylıca açıklanmalıdır. Bunun için eğitimcinin konuya hâkim olması, iyi bir eğitim planlaması yapması, sunumunu güçlü tutması ve öğrenenlerin ilgisini çekme beceresi, EBYS paydaşlarının bilgi ve farkındalık seviyelerinin artırılması açısından büyük önem taşımaktadır.

5. KAYNAKÇA

- Akçakanat, Ö. (2012). Kurumsal risk yönetimi ve kurumsal risk yönetim süreci. *Süleyman Demirel Üniversitesi Vizyoner Dergisi*, 4(7), 30-6.
- Akdoğan, U. Z. ve Özdemirci, F. (2017). Standartlar çerçevesinde EBYS ve e-Arşiv uygulamalarında kurumsal yeterlilik gereksinimini ve nitelikli insan gücünü geliştirme faaliyetleri. F. Özdemirci ve Z. Akdoğan (Ed.), *Bilgi sistemleri ve bilişim yönetimi: Beklentiler ve yeni yaklaşımlar içinde* (ss. 251-256). BİL-BEM.https://fahrettinozdemirci.com.tr/wp-content/uploads/2021/01/TSE_Sertifika_Egitim_Gereksinimi_Ozdemirci.pdf
- Albayrak, S. (2020). Türkiye’de kamu personel yönetiminin yeni kurumsal yapısı ve kamu istihdamının yeni görünümü. *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi*, 75(4), 1517-1549. <https://doi.org/10.33630/ausbf.814996>
- Ambira, C. M., ve Kemoni, H. (2011). Records management and risk management at Kenya Commercial Bank Limited, Nairobi. *SA Journal of Information Management*, 13(1), 112-123. doi: 10.4102/sajim.v13i1.475
- Australian/New Zealand Standard. (2004). Risk management (AS/NZS 4360:2004). https://mkidn.gov.pl/media/docs/pol_obronna/20150309_3-NZ-AUST-2004.pdf
- Aydın, F. ve Saydam, V. (2019). Elektronik belge yönetimi sistemlerinde bilgi varlıklarının kullanımı. *Bilgi Yönetimi Dergisi*, 2(1), 1-8.
- Bakkal, H., Tunç, İ. ve Kasımoğlu, A. (2016). *İç kontrol ve kurumsal risk yönetimi*. İdeal Kültür Yayıncılık.
- Bannerman, P. L. (2008). Risk and risk management in software projects: A reassessment. *Journal of Systems and Software*, 81(12), 2118–2133. <https://www.sciencedirect.com/science/article/pii/S0164121208000897>

- Barnawi, A. O. (2013). *Risk management of electronic health record system in hospitals* (Tez No. 1001810) [Doktora tezi, De Montfort Üniversitesi]. ProQuest Dissertations & Theses Global.
- Baybutt, P. (2013). The ALARP principle in process safety. *Process Safety Progress*, 33(1), 36-40. <https://doi.org/10.1002/prs.11599>
- Bearman, D. (2006). Moments of risk: Identifying threats to electronic records. *Archivaria*, (62), 15-46. <https://archivaria.ca/index.php/archivaria/article/view/12912>
- Bektaş Şeker, T. (2005). Bilgi teknolojilerindeki gelişmeler çerçevesinde bilgiye erişimin yeni boyutları. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, (13), 377-391.
- Bıçakçı, Y. S. (2022). *Yönetim bilişim sistemleri* [Çevrimiçi ders içeriği]. <https://www.yunusserhat.com/courses/yonetim-bilisim-sistemleri/>
- 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>
- Blake, R. (2005). *Complying with the records management code: Evaluation workbook and methodology*. The National Archives. https://cdn.nationalarchives.gov.uk/documents/record_management_compliance.rtf
- Bozkurt, C. (2010). Risk, kurumsal risk yönetimi ve iç denetim. *Denetişim*, (4), 17-30. https://dergipark.org.tr/tr/pub/denetisim/issue/22481/240477#article_cite
- Calp, M. H. ve Akcayol, M. A. (2015). Yazılım projelerinde karşılaşılan risk faktörleri ve risk yönetim süreci. *Marmara Fen Bilimleri Dergisi*, 1, 1-13. <https://doi.org/10.7240/mufbed.72223>
- Ceylan, H. ve Başhelvacı, V. S. (2011). Risk değerlendirme tablosu yöntemi ile risk analizi: Bir uygulama. *International Journal of Engineering Research and*

- Cıbaroğlu, M. O. (2019). Elektronik Belge Yönetim Sistemlerinde Taksonomi Geliştirme Çabaları. *E-Beyas 2019 Sempozyumu: Endüstri 4.0 Sürecinde Bilgi Yönetimi ve Bilgi Güvenliği: eBelge-eArşiv-eDevlet-Bulut Bilişim-Büyük Veri-Yapay Zekâ*. Ankara. [https://www.researchgate.net/publication/338159602 Elektronik Belge Yon etim Sistemlerinde Taksonomi Gelistirme Cabalari](https://www.researchgate.net/publication/338159602_Elektronik_Belge_Yonetim_Sistemlerinde_Taksonomi_Gelistirme_Cabaları)
- Clemence, O., Luambano, I., ve Mwantimwa, K. (2025). Adoption and application of electronic records systems in higher learning institutions. *Information Development*, 41(2), 333-352. <https://doi.org/10.1177/02666669231158336>
- Cox, L. A. (2008). What's wrong with risk matrices? *Risk Analysis*, 28(2), 497-512. <https://doi.org/10.1111/j.1539-6924.2008.01030.x>
- Czosseck, C., Ottis, R., ve Talihärm, A. M. (2011). Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 1, 24-34. [https://www.researchgate.net/publication/220143696_Estonia_after_the_2007_Cyber_Attacks_Legal_Strategic_and_Organisational_Changes_in_Cyber_S ecurity](https://www.researchgate.net/publication/220143696_Estonia_after_the_2007_Cyber_Attacks_Legal_Strategic_and_Organisational_Changes_in_Cyber_Security)
- Çeliksa, B. ve Ünlü, N. (2018). Risk değerlendirme karar matrisi yöntemi kullanarak örnek bir risk değerlendirme raporunun oluşturulması. *The Journal of Academic Social Science Studies*, (65), 483-504. https://www.researchgate.net/publication/323835777_RISK_DEGERLENDIRME_KARAR_MATRISI_YONTEMI_KULLANARAK_ORNEK_BIR_RI SK_DEGERLENDIRME
- Çiçek, N. (2016). Elektronik belge yönetimi uygulamalarında bir alt sistem olarak dosya yönetimi. *Türk Kütüphaneciliği*, 30(3), 434-448. <https://www.tk.org.tr/index.php/TK/article/view/2692/2665>
- Çiçek, N. (2020). E-devlet stratejisi bağlamında elektronik belge yönetimi için “yazılı politika”

gereksinimi: Türkiye’deki uygulamalar üzerine bir inceleme. *Türk Kütüphaneciliği*, 34(3), 377-405. doi: 10.24146/tk.739591

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>

Department of Defense, U. S. (2000). *Standard practice for system safety (MIL-STD-882D)*. <https://mail.system-safety.org/Documents/MIL-STD-882D.pdf>

Derici, O., Tüysüz, Z. ve Sarı, A. (2007). Kurumsal risk yönetimi ve Sayıştay uygulaması. *Sayıştay Dergisi*, (65), 151-172. https://www.sayistay.gov.tr/files/4409_der65m12.pdf

Devlet Arşivleri Başkanlığı. (2023). *Yükseköğretim üst kuruluşları ve yükseköğretim kurumları saklama süreli standart dosya planı* (Sürüm 4). Ankara: Devlet Arşivleri Başkanlığı. <https://www.devletarsivleri.gov.tr/Sayfalar/Sayfa.aspx?icerik=20&h=EC4EE38996FE1DD2D040D483800B793116ED6F1FD94ED1E517B581F5E16F395B>

Dilek, E., Talih, Ö. ve Kaya Bensghir, T. (2023). Estonya 2007 siber saldırılarının incelenmesi ve ülkelerin ulusal siber güvenlik politikalarına etkileri. *Bilgi Yönetimi Dergisi*, 6(2).

DiNapoli, T. P. (2016). *Standards for internal control in New York State government*. Division of State Government Accountability. <https://www.osc.ny.gov/files/state-agencies/guidance/pdf/agencies-ictf-docs-int-control-stds.pdf>

Dişli, M. (2019). *Üniversitelerde elektronik belge yönetim sistemlerinin birlikte çalışabilirlik açısından değerlendirilmesi* (Tez No: 554272) [Yüksek lisans tezi, Hacettepe Üniversitesi]. YÖK Tez Kataloğu.

Dişli, M. ve Külçü, 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>

DQS. (2023, 9 Ağustos). *FMEA nedir?-Hata türleri ve etki analizi*. <https://www.dqsglobal.com/tr-tr/egitim/blog/fmea-nedir#:~:text=FMEA%20nedir%20sorusunun%20en%20genel,i%C3%A7in%20yap%C4%B1lan%20sistematik%20%C3%A7al%C4%B1%C5%9Fmalar%C4%B1n%20b%C3%BCt%C3%BCn%C3%BCd%C3%BCr>

Edin, İ., Bakoğlu, R., Can, Z. S., Küçükgül, Ş. G., Özel, S., Dumludağ, D. ve Bulut, E. (2016). Pestle analizi. R. Bakoğlu ve M. L. Yıldız (Ed.), *Üniversitelerde strateji geliştirme sürecinde uygulamalı durum analizleri* içinde (ss. 101-122). Beta Yayıncılık.

Elzamly, A., Hussin, B. ve Salleh, N. (2016). Top fifty software risk factors and the best thirty risk management techniques in software development lifecycle for successful software projects. *International Journal of Hybrid Information Technology*, 9(6), 11-32. <http://dx.doi.org/10.14257/ijhit.2016.9.6.02>

Emhan, A. (2009). Risk yönetim süreci ve risk yönetmekte kullanılan teknikler. *Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi*, 23(3), 209-220.

Ermisket, E. G. (2011). Kamu kurumlarında risk yönetimi: Bir uygulama önerisi. *Denetim*, (7), 58-70. <https://dergipark.org.tr/tr/pub/denetisim/issue/22497/240538>

Eroğlu, N. G. (2019). *Türkiye’de kurum ve kuruluşlarda elektronik belgelerin uzun süre korunması/arşivlenmesi ve erişimi* (Tez No. 587061) [Yüksek lisans tezi, Çankırı Karatekin Üniversitesi]. YÖK Tez Kataloğu.

Erses, N., Balay, M., Şengel, E., Öncü, S., Baltacı Göktalay, Ş., Uzun, A., Çakır, H., Delialioğlu, Ö., Alan, S., Demirer, V. ve Şahin, İ. (2014). *Temel bilgi teknolojileri ve bilgisayar kullanımı*. Ekin Basım Yayın Dağıtım.

- Federation of European Risk Management Associations (FERMA). (2011). *Avrupa Risk Yönetimi Dernekleri Federasyonu risk yönetim standardı*. <https://www.ferma.eu/app/uploads/2011/11/a-risk-management-standard-turkish-version.pdf>
- Field, A. (2018). *IBM SPSS ile istatistiksel analiz rehberi* (M. S. Bilir, Çev.; 5. bs.). Nobel Akademik Yayıncılık.
- Gibson, N. (2011). *Risk and records management: Investigating risk and risk management in the context of records and information management in the electronic environment* (Tez No. U639005) [Doktora tezi, University of Northumbria at Newcastle]. ProQuest Dissertations & Theses Global.
- Government Accountability Office (GAO). (2001). *Internal control management and evaluation tool*. <https://www.gao.gov/products/gao-01-1008g>
- Güler, C. (2018). Kamu kurumlarında e-belge yönetimi uygulamalarında karşılaşılan problemler: Teknik şartnamelerin incelenmesi. *Arşiv Dünyası Dergisi*, (21), 1-21. <https://dergipark.org.tr/tr/pub/ad/issue/42284/508762>
- Hamidoviç, H. (2010). *An introduction to digital records management*. ISACA. <https://www.isaca.org/resources/isaca-journal/past-issues/2010/an-introduction-to-digital-records-management>
- 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>
- Henkoğlu, T. (2016). Elektronik ortamlarda bilgi güvenliğinin sağlanması [Bildiri]. F. Özdemirci, N. Özel, T. Çakmak, Z. Akdoğan ve B. Yalçinkaya (Ed.), *E-BEYAS 2015 Sempozyumu: Kurumsal belleklerin geleceği – Dijitalleştirme, elektronik arşiv, elektronik belge yönetimi* (21–22 Ekim 2015) (ss. 109-116). Ankara: Ankara Üniversitesi BEYAS Koordinatörlüğü.
- 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. (2006). *Information and documentation - Records management processes - Metadata for records: Part 1 - Principles* (ISO Standard No. 23081:2006).

International Organization for Standardization. (2010). *Information and documentation - Principles and functional requirements for records in electronic office environments - Part 1: Overview and statement of principles* (ISO Standard No. 16175-1:2010).

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

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

International Organization for Standardization. (2018a). *Information technology - Security techniques - Information security management systems - Overview and vocabulary* (ISO Standard No. 27000:2018).

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

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

International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection - Guidance on managing information security risks* (ISO Standard No. 27005:2022).

International Organization for Standardization. (2024). *Information and documentation - Records risks - Risk assessment for records management* (ISO Standard No. 18128-1:2024).

International Records Management Trust. (2009a). *Training in electronic records management module 1: Understanding the context of electronic records management* (L. Millar, Ed.). IRMT.

International Records Management Trust. (2009b). *Training in electronic records management module 2: Planning and managing an electronic records management programme* (L. Millar, Ed.). IRMT.

International Records Management Trust. (2009c). *Training in electronic records management module 3: Managing the creation, use and disposal of electronic records* (L. Millar, Ed.). IRMT.

International Records Management Trust. (2009d). *Training in electronic records management module 4: Preserving electronic records* (L. Millar, Ed.). IRMT.

İnce, F. (2019). Kurumsal risk yönetim süreci [Bildiri sunumu]. 3. Uluslararası Akdeniz Sempozyumu, Mersin.
<https://libdis.com/index.jsp?modul=page&w=ctaqwIkBnJwnONLTicUr>

İslam, Y. (2019). *Dosyalama ve arşivleme teknikleri: Belge yönetimi - arşiv yönetimi-yönetmelikler*. Seçkin Yayıncılık.

Johare, R. (2006). Education and training in electronic records management (ERM): The need for partnership building. C. Khoo, D. Singh ve A. S. Chaudhry (Ed.), *Proceedings of the Asia-Pacific Conference on Library & Information Education & Practice 2006 (A-LIEP 2006)* (ss. 541-549). School of Communication & Information, Nanyang Technological University.
https://www.researchgate.net/profile/Rusnah-Johare/publication/234072207_Education_and_training_in_electronic_records_management_the_need_for_partnership_building

- Kabakulak, T. (2019). Bir tekstil işletmesinde risk değerlendirme uygulaması: 5x5 matris ve HAZOP. *Karaelmas İş Sağlığı ve Güvenliği Dergisi*, 3(2), 97-111. <https://doi.org/10.33720/kisgd.581677>
- Kalkınma Bakanlığı Bilgi Toplumu Dairesi. (2012). *e-Dönüşüm Türkiye Projesi: Birlikte çalışabilirlik esasları rehberi* (Sürüm 2.1). Kalkınma Bakanlığı. https://afyonluoglu.org/PublicWebFiles/Reports-TR/genel/2012%20Mayis-birlikte_calisabilirlik_esaslari_rehberi_2.1.pdf
- Karaca, M. S. (2006). *Bilgisayar uzmanlığı*. Nobel Yayın Dağıtım.
- Karahan, V. ve Aydoğmuş, E. (2023). Risk analysis and risk assessment in laboratory studies. *European Journal of Science and Technology*, (49), 55-60. <https://doi.org/10.31590/ejosat.1260340>
- Kartal, M. (2022). *Bilimsel araştırmalarda hipotez testleri: Parametrik ve nonparametrik teknikler* (6. bs.). Nobel Akademik Yayıncılık.
- Kaya Bensghir, T. (1996). *Bilgi teknolojileri ve örgütsel değişim* (TODAİE Yayın No: 274). TODAİE. https://www.researchgate.net/publication/290435708_Bilgi_Teknolojileri_ve_Orgutsel_Etkileri_ICT_and_Organizational_Impacts
- Koçiyit, S. ve Ayan, M. (2014). *Stratejik analiz*. York University, Türkiye Temsilciliği İşletme Bölümü. https://www.academia.edu/8638617/Stratejik_Analiz
- Kuzucuoğlu, A. H. (2014). Health-safety risks and precautions at library and archive buildings. *International Journal of Social Science*, (29), 313-338. <http://eprints.rclis.org/24026/>
- Leikums, T. (2012). Managing human factors in implementing electronic document systems in the public sector. *Romanian Review of Social Sciences*, 2, 21-30.
- 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](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).
- McDowall, R. D. (2005). Effective and practical risk management options for computerised system validation. *Quality Assurance Journal*, 9(3), 196-227. Doi: 10.1002/qaj.339
- Miles, M. B., Huberman, A. M. ve Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3. ed.). 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>
- Nalbantoğlu, S. (2018). Bir temel hak olarak unutulma hakkı. *TAAD*, (35), 583-605. <https://dergipark.org.tr/tr/pub/taad/issue/52647/693627>
- Northern Territory Government of Australia. (2024). *Business Classification Scheme (BCS)*. <https://dcdd.nt.gov.au/government-records/business-classification-scheme-bcs>
- Odabaş, H. (2005). Belge yönetimi ve Türkiye’de belge yönetimi gereksinimi. *Bilgi Dünyası*, 6(1), 36-57.
- Odabaş, H. ve Polat, C. (2008). E-devlet bilişim sistemlerinde kurumsal bilgi ve belge yönetimi [Bildiri]. E. Bilar ve Y. Ekinçi (Ed.), *Balkan Ülkeleri Kütüphaneler Arası Bilgi-Belge Yönetimi ve İşbirliği Sempozyumu, 5–7 Haziran 2008* (ss. 236-246). Trakya Üniversitesi. <https://odabashuseyin.wordpress.com/wp-content/uploads/2011/04/e-devlet-bilic59fim-sistemlerinde-kurumsal-bilgi-ve-belge-yc3b6netimi.pdf>

- Oxford University Press. (2023). Risk. *Oxford Learner's Dictionaries*.
https://www.oxfordlearnersdictionaries.com/definition/english/risk_1?q=risk
- Özdemirci, F. (2007). Üniversitelerde belge yönetimi ve arşivler. *Türk Kütüphaneciliği*, 21(2), 218-229.
<https://www.tk.org.tr/index.php/TK/article/view/64/65>
- Özdemirci, F., Bayram, Ö., Torunlar, M., Saraç, S. ve Yalçınkaya, B. (2013). *Elektronik belge yönetimi ve arşivleme sistemi: Geçiş süreci ve uygulama yönetimi*. Ankara.
- Paksu, S. ve Bozdemir, R. (2021). Bilgi güvenliği risk yönetimi. *BİLGEM Teknoloji Dergisi*, 12. <https://bilgem.tubitak.gov.tr/wp-content/uploads/sites/8/bilgem-teknoloji-dergisi-12.pdf>
- Public Record Office Victoria. (2010). *PROS 10/10: Guideline 6: Records & risk management* (Ed. Strategic Management Advisory Group).
<https://lgig.com.au/files/2013/11/Records-Risk-Management-Assessment.pdf>
- Renn, Ortwin. (1998). Three decades of risk research : accomplishments and new challenges. *Journal of Risk Research*, 1(1), 49-71.
<https://doi.org/10.1080/136698798377321>
- Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik. (2020). *T.C. Resmî Gazete*, 31151, 10 Haziran 2020.
- Saffady, W. (2005). Risk analysis and control: Vital to records protection. *Information Management Journal*, 39(5), 62-68. <https://www.proquest.com/scholarly-journals/risk-analysis-control-vital-records-protection/docview/227722863/se-2>
- Sağlık, Ö. (2021a). Arşivlenen elektronik belgelerin güvenilirliğini tehdit eden riskler: Teknolojik koşullar açısından bir inceleme. *Bilgi ve Belge Araştırmaları Dergisi*, (16), 29-47.

- Sağlık, Ö. (2021b). *Elektronik belge yönetimi uygulamalarındaki koşullar ışığında e-imzalı belgelerin delil değerinin arşivsel güvenilirlik açısından incelenmesi* (Tez No. 698268)[Doktora tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü].
- Sayan, H. (2015). Eğitim ve Öğretmen. *Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 6(2), 585-596.
- Shapiro, S. S. ve Wilk, M. B. (1965). An analysis of variance test for normality (complete samples). *Biometrika*, 52(3-4), 591-611.
<https://www.jstor.org/stable/2333709?seq=20>
- 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>
- Şataf, C. (2014). Fayda-maliyet analizinde uygulamada karşılaşılan güçlükler: Fayda ve maliyetin belirlenebilme sorunu. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 19(1), 107-123.
- Şeker, T. B. (2005). Bilgi teknolojilerindeki gelişmeler çerçevesinde bilgiye erişimin yeni boyutları. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi* (13), 377-391.
<https://dergipark.org.tr/en/download/article-file/1722272#923599>-
[1722272.pdf](https://dergipark.org.tr/en/download/article-file/1722272#923599)
- Tahtaloğlu, H. (2018). Türkiye’de Elektronik Belge Yönetim Sisteminin Kamu Personeli Tarafından Benimsenmesinde Eğitim Faktörü. *Yasama Dergisi* (37), 124-147.
- Taşkaya, S. M. (2012). Nitelikli bir öğretmende bulunması gereken özelliklerin öğretmen adaylarının görüşlerine göre incelenmesi. *Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 33(2), 283-298.
- The National Archives. (2017). *Risk assessment handbook*.
<https://cdn.nationalarchives.gov.uk/documents/information-management/Risk-Assessment-Handbook.pdf>

- Türedi, H. ve Koban, A. O. (2016). COSO iç kontrol modelinde risk değerlendirme faaliyetleri. *Marmara Üniversitesi Öneri Dergisi*, 12(46), 155-178.
<https://dergipark.org.tr/tr/pub/maruoneri/issue/23666/252039>
- Türk Dil Kurumu Güncel Türkçe Sözlük. (2024). Risk. *Güncel Türkçe Sözlük*.
<https://sozluk.gov.tr/>
- Türk Standardları Enstitüsü. (2015). *TS 13298 e-belge ve arşiv yönetim sistemi*. Ankara: Türk Standardları Enstitüsü.
- TÜSİAD. (2008). *Kurumsal risk yönetimi*.
<https://tusiad.org.tr/yayinlar/raporlar/item/3637-kurumsal-risk-yonetimi>
- United Nations Development Programme. (2023). *Enterprise risk management guidance: Step 6 – Recording and reporting*.
- Usman, Ö. ve Kaygusuz, S. Y. (2019). Kurumsal risk yönetiminde uygulanması gereken adımlar. *Muhasebe ve Denetime Bakış*, (56),109-128.
- Usta, A. (2018). Organizasyonlarda risk yönetimi süreci: stratejiler, amaçlar ve unsurlar. *Kahramanmaraş Sütçü İmam Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 8(2), 91-110.
<https://dergipark.org.tr/tr/pub/ksuiibf/issue/41823/504759>
- Valipour, A., Yadollahi, M., Rosli, M. Z., Nordin, Y. ve Norhazilan, M. N. (2014). An enhanced multi-objective optimization approach for risk allocation in public–private partnership projects: A case study of Malaysia. *Canadian Journal of Civil Engineering*, 41(2).
- Vaughan, E. J. ve Vaughan, T. (2008). *Fundamentals of risk and insurance*. John Wiley & Sons, Inc. <https://nibmehub.com/opac-service/pdf/read/Fundamentals%20of%20Risk%20and%20Insurance-%2010th%20Edition.pdf>
- Wilk, M. B. ve Gnanadesikan, R. (1968). Probability plotting methods for the analysis of data. *Biometrika*, 55(1), 1-17.

Yalçın, E., Altun Çiftçioğlu, G. ve Güzel, B. (2024). İnsan güvenilirlik analizi metotları. *Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi*, 30(2), 282-292. doi: 10.5505/pajes.2023.33958

Yalçinkaya, B. (2014). Belge yönetim sistemlerinde ve süreçlerinde risk tanımları. *Arşiv Dünyası*, (16-17), 16-24. <https://dergipark.org.tr/tr/pub/ad/issue/55753/762803>

Yalçinkaya, B. (2015). Elektronik belge yönetimi (EBY) uygulamalarında başarıyı olumsuz etkileyen risk unsurları. *Bilgi ve Belge Araştırmaları Dergisi*, (4), 20-40.

Yalçinkaya, 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. <https://www.scribd.com/document/562272672/Alı-Y%C4%B1ld%C4%B1r%C4%B1m-Hasan-%C5%9Eim%C5%9Fek-Sosyal-Bilimlerde-Nitel-Ara%C5%9Ft%C4%B1rma-Yontemleri>

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. *Bilgi yönetimi ve bilgi güvenliği: ebelge-earşiv-edevlet-bulut bilişim-büyük veri-yapay zekâ içinde* (ss. 45-60). Ankara Üniversitesi. <https://akademi.butagrup.com.tr/uploads/BGYS-EBYS.pdf>

Yüksel Ş. (2018). Fiziksel çevre kontrolü: önemi ve iç mimarlık eğitimindeki yeri, *Kent Akademisi*, 11(1), 108-116.

Yüksel, A. N. (2020). Nitel bir araştırma tekniği olarak: Görüşme. *International Social Sciences Studies Journal*, 6(56), 547-552.

https://sssjournal.com/files/sssjournal/241566749_08_56_6_ID2099_Yüksel_547-552.pdf



EKLER

EK 1: Görüşmeler İçin Etik Kurul İzni



T.C.
ÇANKIRI KARATEKİN ÜNİVERSİTESİ
Fen, Matematik ve Sosyal Bilimler Etik Kurulu
DEĞERLENDİRME FORMU



Toplantı No:	49
Araştırmanın Yürütücüsü:	Nagihan Gönül Eroğlu
Araştırmanın Başlığı:	Kurum ve Kuruluşlarda Elektronik Belge Yönetim Sistemi Risk Unsurları Eğitim Rehberi Önerisi: Çankırı Karatekin Üniversitesi Örneği
Karar Tarihi:	20-12-2024
Kurul Görüşü:	Kabul Edilmiştir. Araştırmanın/Projenin uygulanabilirliği konusunda bilimsel araştırmalar etiği açısından bir sakınca yoktur.

SONUÇ: Kabul Edilmiştir. Araştırmanın/Projenin uygulanabilirliği konusunda bilimsel araştırmalar etiği açısından bir sakınca yoktur.

Başkan Profesör Dr. Yavuz Demirel	İMZA
Başkan Yardımcısı Doçent Dr. Süheyla Bozkurt Balcı	İMZA
Üye Doçent Dr. Haydar Koç	İMZA
Üye Doçent Dr. Emine Çeliksoy	İMZA
Üye Doçent Dr. Hüseyin Özdemir	İMZA
Üye Doçent Dr. Bilgehan Tekin	İMZA
Üye Doktor Öğretim Üyesi Bahaddin Demirdiş	İMZA
Üye Doktor Öğretim Üyesi Eray Göç	İMZA
Üye Avukat Aslı Asiye Marmara	İMZA
Üye Doçent Dr. Nazan Kaytez	İMZA

Belge Doğrulama Adresi:
<https://etikkurul.karatekin.edu.tr/dogrulama/d8443f33bccb48f3>



EK 2: Eğitim Materyalinin Etkinliği Testi İçin Etik Kurul İzni



T.C.
ÇANKIRI KARATEKİN ÜNİVERSİTESİ
Fen, Matematik ve Sosyal Bilimler Etik Kurulu
DEĞERLENDİRME FORMU



Toplantı No:	54
Araştırmanın Yürütücüsü:	Nagihan Gönül Eroğlu
Araştırmanın Başlığı:	Kurum ve Kuruluşlarda Elektronik Belge Yönetim Sistemi Risk Unsurları Eğitim Rehberi Önerisi: Çankırı Karatekin Üniversitesi Örneği
Karar Tarihi:	29-05-2025
Kurul Görüşü:	Kabul Edilmiştir. Araştırmanın/Projenin uygulanabilirliği konusunda bilimsel araştırmalar etiği açısından bir sakınca yoktur.

SONUÇ: Kabul Edilmiştir. Araştırmanın/Projenin uygulanabilirliği konusunda bilimsel araştırmalar etiği açısından bir sakınca yoktur.

Başkan Profesör Dr. Yavuz Demirel	İMZA
Başkan Yardımcısı Doçent Dr. Süheyla Bozkurt Balcı	İMZA
Üye Doçent Dr. Haydar Koç	İMZA
Üye Doçent Dr. Emine Çeliksoy	İMZA
Üye Doçent Dr. Hüseyin Özdemir	İMZA
Üye Doçent Dr. Bilgehan Tekin	İMZA
Üye Doktor Öğretim Üyesi Bahaddin Demirdiş	İMZA
Üye Doktor Öğretim Üyesi Eray Göç	İMZA
Üye Avukat Aslı Asiye Marmara	İMZA
Üye Doçent Dr. Nazan Kaytez	İMZA

Belge Doğrulama Adresi:
<https://etikkurul.karatekin.edu.tr/dogrulama/855366fa13e94e87>



EK 3: Kurumlar İçin Soru Formu

Sayın Katılımcı

LÜTFEN BU DOKÜMANI DİKKATLİCE OKUMAK İÇİN ZAMAN AYIRINIZ

Sizi Nagihan Gönül EROĞLU tarafından yürütülen “Kurum ve Kuruluşlarda Elektronik Belge Yönetim Sistemi Risk Unsurları Eğitim Rehberi Önerisi: Çankırı Karatekin Üniversitesi Örneği” başlıklı araştırmaya davet ediyoruz. Bu araştırmaya katılıp katılmama kararını vermeden önce, araştırmanın neden ve nasıl yapılacağını bilmeniz gerekmektedir. Bu nedenle bu formun okunup anlaşılması büyük önem taşımaktadır. Eğer anlayamadığınız ve sizin için açık olmayan şeyler varsa, ya da daha fazla bilgi isterseniz bize sorunuz. Bu çalışmaya katılmak tamamen gönüllülük esasına dayanmaktadır. Çalışmaya katılmama veya katıldıktan sonra herhangi bir anda çalışmadan çıkma hakkında sahipsiniz. Çalışmayı yanıtlamanız, araştırmaya katılım için onam verdiğiniz biçiminde yorumlanacaktır. Size verilen formlardaki soruları yanıtlarken kimsenin baskısı veya telkini altında olmayın. Bu formlardan elde edilecek kişisel bilgiler tamamen gizli tutulacak ve yalnızca araştırma amacı ile kullanılacaktır. Katılımınız, değerli katkı ve geri bildirimleriniz için şimdiden teşekkür ederim.

Nagihan Gönül EROĞLU

Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü

Bilgi ve Belge Yönetimi Bölümü Doktora Öğrencisi

1. Eğitim Materyali ve EBYS’de Risk Farkındalığı/Genel Durum

- **Eğitim Materyali Hakkında**
 - Taslak eğitim materyali (“EBYS Risk Unsurları Eğitim Rehberi”) hakkında eksik veya eklenmesi gereken alanlar olduğunu düşünüyor musunuz?
 - Bu çalışmanın eğitim materyali olarak sunulmasının faydalı olacağını düşünüyor musunuz? (Evet/Hayır – Açıklayınız)
- **Risk Yönetimi Yaklaşımı**
 - Kurumunuzda EBYS ile ilgili riskleri yönetmek için sistematik bir yaklaşımınız var mı?
 - Evet ise: Bu yaklaşım hangi risklere odaklanıyor?
 - Hayır ise: Böyle bir yaklaşım geliştirilmesine yönelik önerileriniz nelerdir?
- **Geçmişteki Sorunlar ve Riskler**
 - EBYS ile ilgili geçmişte karşılaştığınız en büyük sorun neydi?
 - Bu sorunun temelinde yatan risk faktörü sizce neydi?

2. Dış Faktörlere Bağlı Riskler

- **Yasal Düzenlemeler ve Riskler**
 - Yasal düzenlemelerdeki değişikliklerin EBYS üzerinde oluşturduğu riskler nelerdir?
 - Bu risklere karşı alınan önlemler nelerdir?

- **Beklenmedik Olaylar (Doğal Afetler, Siber Saldırıları)**
 - Doğal afetler veya siber saldırılar gibi beklenmedik olaylar verilerinize nasıl zarar verebilir?
 - Bu tür olayların risklerini en aza indirmek için hangi önlemleri aldınız/almayı planlıyorsunuz?
- **Yeni Teknolojilerin Entegrasyonu ve Riskleri**
 - Yapay zekâ, bulut teknolojileri gibi yeni teknolojilerin EBYS'nize entegrasyonu konusunda planlarınız nelerdir?
 - Bu teknolojilerin yaratabileceği riskler nelerdir ve bu risklere karşı nasıl bir yaklaşım benimsiyorsunuz?

3. İç Faktörlere Bağlı Riskler

- **EBYS Politikaları ve Prosedürleri**
 - Kurumunuzdaki EBYS politikaları ve prosedürleri güncel ve etkin mi?
 - Bu politikaların eksikliği veya güncel olmaması hangi riskleri yaratır?
- **Kurumsal Değişiklikler ve Veri Yönetimi**
 - Birleşme, devralma gibi kurumsal değişiklikler EBYS'nizi nasıl etkiler?
 - Uyum süreçlerinde ne gibi zorluklarla karşılaşıyorsunuz?
- **Personel Bilgi ve Eğitim Durumu**
 - Personeliniz EBYS konusunda yeterli bilgi ve becerilere sahip mi?
 - Eğitim yetersizliği sistem kullanımını nasıl etkiliyor?
 - Bu konuda alınabilecek çözüm önerileriniz nelerdir?
- **Personel Devir Hızı**
 - Yeni personel, yönetici değişiklikleri veya vekalet işlemleri gibi durumlar, sistem güvenliği ve sürekliliği açısından hangi riskleri oluşturuyor?
 - Bu risklerin yönetilmesi için hangi adımları atıyorsunuz?
- **Yönetim Desteği**
 - EBYS projelerinin başarısı için yönetimin rolü nedir?
 - Yetersiz yönetim desteği hangi riskleri doğurur?
- **Kurum Kültürü ve Dijital Dönüşüm**
 - Elektronik belgelere kurum kültürünüzde verilen önem nedir?
 - Kâğıt odaklı bir kültürden dijital bir kültüre geçerken ne gibi zorluklar yaşamaktasınız?

4. Sistem Faktörüne Bağlı Riskler

- **Tedarikçi İlişkileri**
 - EBYS tedarikçinizle yaşadığınız herhangi bir sorun var mı?
 - Tedarikçinin sistem üzerindeki erişim yetkileri konusunda endişeleriniz var mı?
- **Teknik Sorunlar**
 - Sisteminizde en sık karşılaşılan teknik sorunlar nelerdir?
 - Bu sorunların çözümüne yönelik uyguladığınız yöntemler neler?
- **Saklama Süreleri ve Yöntemleri**
 - Belgelerinizin saklama süreleri ve saklama yöntemleri yasalara uygun mu?

- Saklama gereksinimlerinin yetersizliği durumunda ne gibi riskler ortaya çıkar?
 - **Yedekleme ve Geri Yükleme**
 - EBYS'nizin yedekleme ve geri yüklenebilirlik durumu nasıl?
 - Bu süreçlerde karşılaşılabilecek riskleri nasıl yönetiyorsunuz?
 - **Uzun Vadeli Kullanılabilirlik**
 - EBYS'nizin belgelerin uzun vadede kullanılabilirliğini sürdürme yeteneği hakkında ne düşünüyorsunuz?
 - **Üstveri Yönetimi**
 - Üstveri (metadata) yönetimi eksikliklerinin karar verme süreçlerine etkileri nelerdir?
 - Bu eksikliklerin oluşturduğu riskleri nasıl değerlendiriyorsunuz?
 - **Güvenlik İhlalleri**
 - Yetkisiz erişim veya veri sızıntısı gibi güvenlik ihlallerinin oluşturduğu riskler nelerdir?
 - Bu risklere karşı alınan önlemler neler?
5. **Elektronik Belge Yönetim Süreçlerindeki Riskler**
- **Belgelerin Doğru Tanımlanması ve Dosya Planı**
 - Belgelerin yanlış tanımlanması veya standart dosya planına uyulmaması hangi sonuçları doğurabilir?
 - Bu durumun belge yönetimi süreçlerine etkileri nelerdir?
 - **Fiziki Belgelerin Elektronik Ortama Aktarımı**
 - Fiziki belgelerin elektronik ortama aktarılması sırasında hangi riskler yaşanabilir?
 - Bu riskleri azaltmak için nasıl bir yöntem uygulanıyor?
 - **Elektronik Belgelerin Tasfiye İşlemleri**
 - Elektronik belgelerin tasfiyesi için belirli bir prosedürünüz var mı?
 - Prosedür eksikliği hangi risklere neden olur?
 - **Elektronik Arşivleme Modülü**
 - Kurumunuzda elektronik arşivleme için EBYS ile entegre bir modül bulunuyor mu?
 - Modül bulunmaması durumunda ne tür risklerle karşılaşıyorsunuz?
 - **Kâğıt ve Elektronik Belge Entegrasyonu**
 - Kâğıt ve elektronik belge arşivleme süreçlerinizin entegrasyonu nasıl sağlanıyor?
- Bu süreçlerin ayrı tutulması ne gibi potansiyel riskler oluşturur?

EK 4: Akademisyenler/Uzmanlar İçin Soru Formu

Sayın Katılımcı

LÜTFEN BU DOKÜMANI DİKKATLİCE OKUMAK İÇİN ZAMAN AYIRINIZ

Sizi Nagihan Gönül EROĞLU tarafından yürütülen “Kurum ve Kuruluşlarda Elektronik Belge Yönetim Sistemi Risk Unsurları Eğitim Rehberi Önerisi: Çankırı Karatekin Üniversitesi Örneği” başlıklı araştırmaya davet ediyoruz. Bu **araştırmaya** katılıp katılmama kararını vermeden önce, araştırmanın neden ve nasıl yapılacağını bilmeniz gerekmektedir. Bu nedenle bu formun okunup anlaşılması büyük önem taşımaktadır. Eğer anlayamadığınız ve sizin için açık olmayan şeyler varsa, ya da daha fazla bilgi isterseniz bize sorunuz. Bu çalışmaya katılmak tamamen **gönüllülük** esasına dayanmaktadır. Çalışmaya katılmama veya katıldıktan sonra herhangi bir anda çalışmadan **çıkma** hakkında sahipsiniz. **Çalışmayı yanıtlamanız, araştırmaya katılım için onam verdiğiniz** biçiminde yorumlanacaktır. Size verilen **formlardaki** soruları yanıtlarken kimsenin baskısı veya telkini altında olmayın. Bu formlardan elde edilecek kişisel bilgiler tamamen gizli tutulacak ve yalnızca araştırma amacı ile kullanılacaktır. Katılımınız, değerli katkı ve geri bildirimleriniz için şimdiden teşekkür ederim.

Nagihan Gönül EROĞLU

Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü

Bilgi ve Belge Yönetimi Bölümü Doktora Öğrencisi

1. Eğitim Materyali ve EBYS’de Risk Farkındalığı/Genel Durum

- **Eğitim Materyali Hakkında**
 - Taslak eğitim materyali (“EBYS Risk Unsurları Eğitim Rehberi”) hakkında eksik veya eklenmesi gereken alanlar olduğunu düşünüyor musunuz?
 - Bu çalışmanın eğitim materyali olarak sunulmasının faydalı olacağını düşünüyor musunuz? (Evet/Hayır – Açıklayınız)
- **EBYS’de Risk Unsurları**
 - EBYS’de sıklıkla karşılaşılan, önemli gördüğünüz risk unsurları nelerdir?
 - Dış, iç, belge yönetim süreci ve teknolojik faktörlerin birleşiminden kaynaklanan karmaşık risklerin tespiti ve yönetimi hakkında ne düşünüyorsunuz?

2. Dış Faktörlere Bağlı Riskler

- **Yasal ve Politik Riskler**
 - Hükümet politikaları veya yasal düzenlemelerdeki değişikliklerin EBYS uygulamalarına etkisi nedir?
 - Yeni standartlar ve uygulamalar EBYS üzerinde ne tür uyumsuzluk riskleri oluşturabilir?
- **Doğal Afet ve Krizler**
 - Doğal afetler veya ekonomik krizlerin EBYS uygulamalarına olası etkileri hakkında ne düşünüyorsunuz?
 - Bu tür durumlara hazırlık için ne tür stratejiler önerirsiniz?
- **Yeni Teknolojiler ve Siber Güvenlik**
 - Yapay zekâ, makine öğrenmesi ve nesnelerin interneti gibi teknolojilerin EBYS’ye entegrasyonu sırasında karşılaşılabilecek riskler nelerdir?
 - Siber saldırılara karşı alınması gereken güvenlik önlemleri konusunda önerileriniz nelerdir?

- **Altyapı ve Teknoloji Sorunları**

- Ülke veya kuruluş içerisindeki teknolojik altyapı sorunlarının EBYS üzerindeki etkileri nelerdir?

3. İç Faktörlere Bağlı Riskler

- **Organizasyonel Değişiklikler**

- Birleşmeler, devralmalar veya yeniden yapılanma gibi durumlarda EBYS uygulamalarında ortaya çıkan riskler nelerdir?

- **Personel ve Eğitim**

- Personel değişiklikleri ve eğitim eksikliklerinin EBYS süreçleri üzerindeki etkileri hakkında ne düşünüyorsunuz?

- **Politikalar ve Prosedürler**

- EBYS politikaları ve prosedürlerindeki eksikliklerin oluşturduğu riskler nelerdir?

- **Teknolojik Değişiklikler**

- Teknolojik değişikliklerin sistem güvenliği veya uyumluluk üzerindeki etkilerini nasıl değerlendiriyorsunuz?

4. Sistem Faktörlerine Bağlı Riskler

- **Tasarım ve Yapılandırma**

- EBYS tasarımında, özellikle belge tanımlama ve sistem yapılandırma süreçlerinde yaşanabilecek riskler nelerdir?

- **Bakım ve Güvenlik**

- EBYS sistemlerinin bakım süreçlerinde karşılaşılan en yaygın güvenlik ve yedekleme sorunları nelerdir?

- **Hukuki ve Standartlarla Uyum**

- Veri gizliliği, imza güvenliği ve belgelerin delil niteliği ile ilgili karşılaşılan hukuki riskleri nasıl değerlendiriyorsunuz?
- Uluslararası belge yönetimi standartlarının Türkiye'deki kurumlar tarafından benimsenmesi hakkındaki görüşleriniz nelerdir?

- **Sürdürülebilirlik ve Süreklilik**

- EBYS'lerin sürdürülebilirliğini tehdit eden en önemli risk faktörleri nelerdir?

5. Belge Yönetim Süreçlerindeki Riskler

- **Belge Oluşturma ve Üstveri**

- Belgelerin oluşturulma sürecindeki eksikliklerin oluşturduğu riskler nelerdir?
- Üstveri yönetimi ve dosya planı uygulamalarındaki eksikliklerin yaratabileceği sorunlar nelerdir?

- **Erişilebilirlik ve Saklama**

- Elektronik belgelerin erişilebilirliği ve saklanması sırasında karşılaşılan riskler nelerdir?
- Saklama süreli belgelerin yönetimi ve imha işlemleriyle ilgili eksikliklerin sonuçları neler olabilir?

6. Yeni Teknolojiler ve Yenilikçi Uygulamalardaki Riskler

- **Teknolojik Dönüşüm**

- Yapay zekâ, makine öğrenmesi ve bulut teknolojilerinin EBYS'ye etkileri hakkında ne düşünüyorsunuz?

- Bu teknolojilerin getirdiđi fırsatlar ve riskler nelerdir?
- **Veri Güvenliđi ve Gizliliđi**
 - Yeni teknolojik entegrasyonların veri güvenliđi, gizlilik ve erişim kontrolü üzerindeki etkilerini nasıl değerlendirirsiniz?
 - Bu etkilerin olası sonuçları neler olabilir?



EK 5: Firmalar İçin Soru Formu

Sayın Katılımcı

LÜTFEN BU DOKÜMANI DİKKATLİCE OKUMAK İÇİN ZAMAN AYIRINIZ

Sizi Nagihan Gönül EROĞLU tarafından yürütülen “Kurum ve Kuruluşlarda Elektronik Belge Yönetim Sistemi Risk Unsurları Eğitim Rehberi Önerisi: Çankırı Karatekin Üniversitesi Örneği” başlıklı araştırmaya davet ediyoruz. Bu **araştırmaya** katılıp katılmama kararını vermeden önce, araştırmanın neden ve nasıl yapılacağını bilmeniz gerekmektedir. Bu nedenle bu formun okunup anlaşılması büyük önem taşımaktadır. Eğer anlayamadığınız ve sizin için açık olmayan şeyler varsa, ya da daha fazla bilgi isterseniz bize sorunuz. Bu çalışmaya katılmak tamamen **gönüllülük** esasına dayanmaktadır. Çalışmaya katılmama veya katıldıktan sonra herhangi bir anda çalışmadan **çıkma** hakkında sahipsiniz. **Çalışmayı yanıtlamanız, araştırmaya katılım için onam verdiğiniz** biçiminde yorumlanacaktır. Size verilen **formlardaki** soruları yanıtlarken kimsenin baskısı veya telkini altında olmayın. Bu formlardan elde edilecek kişisel bilgiler tamamen gizli tutulacak ve yalnızca araştırma amacı ile kullanılacaktır. Katılımınız, değerli katkı ve geri bildirimleriniz için şimdiden teşekkür ederim.

Nagihan Gönül EROĞLU

Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü

Bilgi ve Belge Yönetimi Bölümü Doktora Öğrencisi

1. Eğitim Materyali

- **Eğitim Materyali Hakkında**
 - Taslak eğitim materyali (“EBYS Risk Unsurları Eğitim Rehberi”) hakkında eksik veya eklenmesi gereken alanlar olduğunu düşünüyor musunuz?
 - Bu çalışmanın eğitim materyali olarak sunulmasının faydalı olacağını düşünüyor musunuz? (Evet/Hayır – Açıklayınız)

2. Dış Faktörlere Bağlı Riskler

- **Yasal Düzenlemeler ve Riskler**
 - Hükümet politikaları ve/veya yasal düzenlemelerdeki değişikliklerin EBYS uygulamalarına etkileri konusunda ne gibi riskler öngörüyorsunuz?
 - Veri saklama gereklilikleri, uyum süreçleri vb.
 - Yeni standartlar ve uygulamalar EBYS ile uyumsuzluk riski oluşturabilir mi? Eğer evet, bu risklere nasıl hazırlanıyorsunuz?
- **KVKK Uyumu ve Performans Etkileri**
 - KVKK’ya uyum sağlamanın EBYS performansına etkileri nelerdir?
 - Sistem hızında yavaşlama, veri erişim süreçlerinde karmaşıklık vb.
 - Uyumluluğun maliyeti ve yazılım geliştirme süreçlerine olan etkisi hakkında ne düşünüyorsunuz?
- **Beklenmedik Olaylar (Doğal Afetler, Siber Saldırıları)**
 - Doğal afetler veya ekonomik krizler gibi dışsal olayların EBYS uygulamalarını nasıl etkilediğini gözlemliyorsunuz?
 - Veri kaybı, erişim kesintisi vb.
 - Siber saldırılara karşı önerdiğiniz güvenlik önlemleri nelerdir?
- **Teknolojik Yenilikler ve Entegrasyon**
 - Yeni teknolojilerin (yapay zekâ, nesnelerin interneti vb.) EBYS’ye entegrasyonunda yaşanabilecek riskler nelerdir?

- Mobil cihazlar ve sosyal medya kullanımının belge yönetimine etkileri ve bu süreçlerde oluşabilecek riskleri nasıl değerlendiriyorsunuz?

3. İç Faktörlere Bağlı Riskler

- **Kurumsal Değişiklikler ve Veri Yönetimi**
 - Organizasyonel değişiklikler (birleşme, devralma vb.) sırasında EBYS uygulamalarında hangi risklerle karşılaşılıyorsunuz?
- **Özelleştirme ve Kurum Talepleri**
 - Kurumların farklı taleplerine uyum sağlamak için hangi özelleştirme süreçlerini uyguluyorsunuz?
 - Bu süreçlerde karşılaşılan zorluklar nelerdir?
- **Personel ve Eğitim**
 - Personel değişiklikleri ve eğitim eksiklikleri, EBYS süreçlerini nasıl etkiliyor?
 - (Yeni personel, yöneticiler, eğitim yetersizliği – Örnek veriniz)

4. Sistem Faktörüne Bağlı Riskler

- **Tasarım, Yazılım Mimarisi ve Teknik Riskler**
 - EBYS tasarım süreçlerinde karşılaştığınız en yaygın riskler nelerdir?
 - Belge tanımlama hataları, sistem tasarımı eksiklikleri.
 - EBYS geliştirirken yazılım mimarisi ile ilgili karşılaştığınız en büyük teknik riskler nelerdir?
 - Yazılımın ölçeklenebilirliği, hata toleransı vb.
- **Bakım ve Güvenlik**
 - Sistem bakım süreçlerinde yedekleme veya güvenlik önlemlerinin yetersiz olmasının yol açtığı riskleri nasıl yönetiyorsunuz?
 - EBYS’lerde en sık karşılaşılan güvenlik tehditleri nelerdir?
 - EBYS’nin bulut tabanlı bir versiyonunu geliştiriyorsanız, veri güvenliği ve erişim denetimi ile ilgili önerdiğiniz yöntemler nelerdir?
 - Erişim ve izin kurallarındaki eksiklikler, sistem güvenliğini ne şekilde tehdit eder?
- **Birlikte Çalışılabilirlik**
 - Sistemler arası entegrasyon ve veri uyumsuzluk sorunlarının risklerini nasıl değerlendiriyorsunuz?
- **EBYS’nin Geleceği: Tehditler ve Fırsatlar**
 - EBYS’nin geleceği açısından en büyük tehditleri ve fırsatları nasıl değerlendiriyorsunuz?

5. Elektronik Belge Yönetim Süreçlerindeki Riskler

- **Belge Oluşturma ve Üstveri**
 - Belgelerin oluşturulması sırasında üstveri yönetimindeki eksikliklerin yarattığı riskler nelerdir?
- **Erişilebilirlik ve Saklama**
 - Elektronik belgelerin erişilebilirliği ile ilgili yaşanan sorunların sistemler üzerindeki etkisi nedir?
 - Elektronik belgelerin saklanması ve arşivlenmesinde karşılaşılan en önemli zorluklar nelerdir?

- Saklama süresi dolmuş belgelerin yönetimi ve imha işlemlerinin eksikliğinin oluşturduğu riskler konusunda ne düşünüyorsunuz?



EK 6: Sekreterler İçin Soru Formu

Sayın Katılımcı

LÜTFEN BU DOKÜMANI DİKKATLİCE OKUMAK İÇİN ZAMAN AYIRINIZ

Sizi Nagihan Gönül EROĞLU tarafından yürütülen “Kurum ve Kuruluşlarda Elektronik Belge Yönetim Sistemi Risk Unsurları Eğitim Rehberi Önerisi: Çankırı Karatekin Üniversitesi Örneği” başlıklı araştırmaya davet ediyoruz. Bu **araştırmaya** katılıp katılmama kararını vermeden önce, araştırmanın neden ve nasıl yapılacağını bilmeniz gerekmektedir. Bu nedenle bu formun okunup anlaşılması büyük önem taşımaktadır. Eğer anlayamadığınız ve sizin için açık olmayan şeyler varsa, ya da daha fazla bilgi isterseniz bize sorunuz. Bu çalışmaya katılmak tamamen **gönüllülük** esasına dayanmaktadır. Çalışmaya katılmama veya katıldıktan sonra herhangi bir anda çalışmadan **çıkma** hakkında sahipsizsiniz. **Çalışmayı yanıtlamanız, araştırmaya katılım için onam verdiğiniz** biçiminde yorumlanacaktır. Size verilen **formlardaki** soruları yanıtlarken kimsenin baskısı veya telkini altında olmayın. Bu formlardan elde edilecek kişisel bilgiler tamamen gizli tutulacak ve yalnızca araştırma amacı ile kullanılacaktır. Cevaplamanız için hazırlanmış testte EBYS ve risk unsurlarına yönelik 19 maddeden oluşan seçmeli test ve 6 maddeden oluşan kısa cevap test bulunmaktadır. Cevaplama süresi toplam 30 dakikadır. Katılımınız için şimdiden teşekkür ederim.

Nagihan Gönül EROĞLU

Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü

Bilgi ve Belge Yönetimi Bölümü Doktora Öğrencisi

Katılımcıların Özellikleri

1. **Cinsiyetiniz nedir?**
a) Erkek b) Kadın
2. **Yaşınız nedir?**
a) 18-22 b) 23-27 c) 28-32 d) 33-37 e) 38-42 f) 43+
3. **Mezuniyet dereceniz nedir?**
a) Lise b) Ön lisans c) Lisans d) Yüksek Lisans e) Doktora
4. **Çalıştığınız birim türü nedir?**
a) Akademik birim b) İdari birim
5. **‘Risk Yönetimi’ kavramına aşinalığınız ne düzeydedir?**
a) Hiç aşına değilim
b) Az düzeyde aşınayım
c) Orta düzeyde aşınayım
d) İyi derecede aşınayım
e) Çok iyi derecede aşınayım
6. **Memuriyet süreniz nedir?**
a) 1-3 Yıl b) 4-6 Yıl c) 7-10 Yıl d) 11-15 Yıl e) 16-20 Yıl f) 20+ Yıl
7. **Yazışma personeli olarak mevcut görevinizdeki hizmet süreniz nedir?**
a) 1-3 Yıl b) 4-6 Yıl c) 7-10 Yıl d) 11-15 Yıl e) 16-20 Yıl f) 20+ Yıl
8. **Daha önce kurumsal yazışmalarda riskli durumlarla karşılaştınız mı?**
a) Evet b) Hayır
9. **Daha önce aldığınız benzer bir eğitim oldu mu?**
a) Evet b) Hayır

Sorular

1. Bir üniversitenin öğrenci işleri biriminde, mezuniyet belgeleri “Genel Duyurular” klasörüne kodlanarak arşivlenmiştir. Aradan 5 yıl geçtikten sonra bu belgelerin mezunlara verilmesi gerektiğinde, belgelerin bulunmasında zorluklar yaşanmıştır.
Aşağıdakilerden hangisi yaşanan bu zorlukların temel nedenidir?
 - A) Belgelerin fiziksel olarak saklanması
 - B) Arşiv personelinin eğitimsiz olması
 - C) Standart dosya plan kodlamasında hata yapılması
 - D) Elektronik belge yönetim sisteminin kullanılmaması
 - E) Belgelerin dijital ortamda kopyasının bulunmaması
2. **Elektronik Belge Yönetim Sistemi (EBYS)’de bir belgeye atanan standart dosya plan kodu aşağıdakilerden hangisinin belirlenmesinde rol oynar?**
 - A) Dağıtım listesi
 - B) Elektronik kayıt numarası
 - C) Saklama süresi
 - D) İşlem sırası
 - E) İmza yetkisi
3. **“Unutmayın: E-imza paylaşamaz, devredilemez, emanet bırakılamaz.” ilkesine rağmen bir kurumda bu uygulama yaygın hale gelirse, aşağıdaki hangi önlemin en etkisiz olacağı söylenebilir?**
 - A) E-imza eğitimlerinin artırılması
 - B) Kullanan kişiler için kişisel sorumluluk bilgilendirmesi yapılması
 - C) Kullanıcıların işlem geçmişlerinin rutin olarak denetlenmesi
 - D) E-imza şifrelerinin değişiminin yılda bir yapılması
 - E) İmza kullanımını kimin yaptığına dair çift doğrulama sistemlerinin kurulması
4. **Aşağıdakilerden hangisi SDP’de en fazla hata riskinin bulunduğu alanlardan biri değildir?**
 - A) 020 Olurlar, 030 Anlaşma ve Protokol İşleri kodunun yazışma kodu olarak kullanılması
 - B) ‘99 diğer’ kodunun sıklıkla kullanılması
 - C) Personel dosyaları, dava dosyaları, proje dosyaları gibi tümleşik dosya açılması
 - D) Gelen yazıya cevap oluştururken SDP koduna bakmadan aynı kodla yazı yazma
 - E) Standart Dosya Planının genel kodlarının kullanılması
5. **Sekreterlerin EBYS kullanırken en çok karşılaştığı “gizlilik ihlali” riski hangi durumda oluşur?**
 - A) Yanlış dağıtım
 - B) Yanlış dosyalama kodu kullanımı
 - C) Belgenin sistem dışına çıkarılması
 - D) Yanlış saklama süresi verilmesi
 - E) Belge numaralandırmasının atlanması
6. **Aşağıdakilerden hangisi süresi dolmadan imha edilen belgenin yol açabileceği sorunların başında gelir?**
 - A) Belgeye erişim sorunları
 - B) İmha sürecinde yetki ve rol sorunları
 - C) Yasal sorunlar
 - D) Teknik sorunlar
 - E) İletişim sorunları
7. **Sekreterin EBYS eğitimi almamasının doğurabileceği en büyük risk hangisidir?**
 - A) Gereksiz belge üretimi
 - B) Yanlış dağıtımın getireceği sorunlar
 - C) Yazışma kurallarını bilmemek
 - D) Süreç hatalarının artması
 - E) Ara yüz kullanımında zorlanma

8. Bir kamu kurumunda yapılan iç denetimde, belgelerin büyük bölümünün yanlış dosya plan koduyla işlendiği tespit edilmiştir.

Denetçiler, bu durumun aşağıdakilerden hangisine doğrudan olumsuz etkilemeyeceğini belirtmiştir?

- A) Kurumsal hafızanın sürekliliğine
 - B) Bilgiye erişimin hızına ve doğruluğuna
 - C) Kurumun kamuya hesap verebilirliğine
 - D) Personelin görev tanımlarına
 - E) Yasal saklama sürelerinin doğru uygulanmasına
9. Bir kamu kurumunda, gelen belgelerin “ilgili birimlere dağıtımı” sürecinde sistematik hatalar yapılmaktadır. Örneğin, “İç Denetim Raporu” yanlışlıkla Bilgi İşlem Birimi’ne, “Stratejik Plan Taslağı” ise Personel Daire Başkanlığı’na gönderilmiştir.

Yapılan bu hatalar sonucunda;

- I. Kurumun yasal sürelerde yanıt verememesi
- II. Belge güvenliğinin ve gizliliğinin ihlali
- III. Karar alma süreçlerinin yanlış bilgiye dayanması
- IV. Kurum içi iş yükü ve zaman yönetiminde verimsizlik oluşması
- V. Belgelerin izlenebilirliğinin azalması

Faktörlerinden hangileri uzun vadeli ve yüksek etkili risk oluşturur?

- A) I, II ve III
 - B) I, III ve IV
 - C) II, IV ve V
 - D) I, II, III ve IV
 - E) I, II, III, IV ve V
10. Aşağıdakilerden hangisi EBYS’de yanlış dosya kodu kullanımının oluşturabileceği başlıca aksaklıklardan biridir?
- A) Dağıtım işlemlerinde aksaklık
 - B) İş sürecinde aksaklık
 - C) Belge üretiminde aksaklık
 - D) Tasfiye sürecinde aksaklık
 - E) Yazışma düzeninde aksaklık
11. Birim arşiv sorumlusu, EBYS’de kayıtlı belgelerin üstveri alanlarını denetlerken pek çok belgenin “konu” ve “anahtar kelime” alanlarının boş bırakıldığını fark eder.

Yukarıdaki durumun kurumsal bilgi yönetimi açısından aşağıdakilerden hangisini en çok zayıflatacağı söylenebilir?

- A) Belge imha prosedürlerinin güncelliği
 - B) Kurumsal dijital dönüşüm stratejisi
 - C) Bilginin sınıflandırılarak analiz edilebilirliği
 - D) E-arşiv performansı
 - E) Kurumun fiziksel arşiv kapasitesi
12. Kurum içi bilgi güvenliği politikaları çerçevesinde, bir sekreter EBYS üzerinde gizlilik derecesi “gizli” olarak tanımlanması gereken bir belgeyi yanlışlıkla normal bir belge olarak kaydetmiştir.

Bu durum, aşağıdakilerden hangisine doğrudan neden olarak hem işlem güvenliğini hem de yasal sorumluluğu en üst düzeyde riske atar?

- A) Gizlilik yalıtımı
- B) Dağıtım sorunları
- C) Üstveri hatası sonucu yaşanan erişim sorunları
- D) Bilgi sızıntısı
- E) Kurum içi işleyişte karışıklık

13. Belge dağıtım süreci devam ederken kullanıcının oturumu açık bırakarak ekranı terk etmesi, aşağıdakilerden hangisi açısından **en yüksek düzeyde** yönetsel ve güvenlik riski doğurur?

- A) Zaman damgasının yeniden üretilip sürüm karmaşasına yol açması
- B) Oturumun dış müdahaleye açık hale gelmesi
- C) Belgenin kurum içi güvenlik düzeyine düşüp gizlilik güncellemesinin yapılmaması
- D) Erişim yetkisi askıya alınca belge akışının durması
- E) Belgenin yanlış klasöre otomatik kaydedilmesi

14. Bir kurumda EBYS kullanılarak arşivlenen belgelerde, tarih, konu, dosya plan kodu, anahtar kelime gibi üstverilerin eksik veya yanlış girildiği tespit edilmiştir.

Yapılan bu hataların;

- I. Kurum içi yetki matrislerinin değişmesi
- II. Saklama sürelerinin yanlış belirlenmesi
- III. Belgelerin bulunabilirliğinin ciddi oranda azalması
- IV. Belgelerin bağlamdan kopması ve yanlış yorumlanması
- V. Denetim süreçlerinde bilgi bütünlüğünün zedelenmesi

Yukarıdaki sonuçlardan hangilerini doğurması, kurumsal bilgi yönetimi açısından yüksek düzeyde yönetsel ve yasal risk oluşturur?

- A) I, II ve IV
- B) II, III, IV ve V
- C) II, III ve IV
- D) I, III, IV ve V
- E) I, II, III, IV ve V

15. Sekreterin dağıtım yaptığı belgeyi kontrol etmemesinin neticesinde karşılaşılabilecek en ciddi risk aşağıdakilerden hangisidir?

- A) Belgenin dosyalamasında hata yapılmasına
- B) Belgenin ihtiyaç duyulmayan kişi ya da birimlere iletilmesine
- C) Belge gizliliğinin ihlaline
- D) Belgenin yanlış kurumlara gönderilmesine
- E) Belgenin zamanında tamamlanmamasına

16-20. sorularda yer alan boşluklara uygun ifadeyi yazınız.

- 16. EBYS'de sekreterin yaptığı _____ hatası, belgenin sistemde tanımsız hale gelmesine yol açabilir.
- 17. Yanlış dağıtım yapılan belge, hem işlem süresini uzatır hem de _____ sorunlarına neden olabilir.
- 18. Kurumların hedeflerinden sapmasına neden olan belirsizlikler veya gelecekte zarara uğrama olasılığı olarak tanımlanan kavram _____.
- 19. Saklama planının dikkate alınmaması, belgelerin süresinden önce _____ riskini doğurur.
- 20. Bir kurumun veya bireyin stratejik hedeflerine ulaşmak için ne düzeyde riski kabul etmeye istekli olduğunu belirten kavram _____.

EK 7: Eğitim Materyali



Kurum ve Kuruluşlarda Elektronik Belge Yönetim Sistemi (EBYS) Risk Unsurları Eğitimi

Öğr. Gör. Nagihan Gönül EROĞLU
nagihangonuleroglu@karatekin.edu.tr

- > **Eğitimin Amacı**
- > **Kavramlar**
- > **Elektronik Belge Yönetim Sistemlerinde ve Süreçlerinde Risk**
- > **Elektronik Belge Yönetim ve Süreçlerinde Risk Unsurları**
 - Dış Faktörlere Bağlı**
 - İç Faktörlere Bağlı**
 - Elektronik Belge Yönetim Sistemine Bağlı**
 - Elektronik Belge Yönetim Süreçlerindeki**
- > **Risk Yönetim Süreci**
 - Risk Değerlendirmesi**
 - Risk Müdahalesi (Risklerin Tedavi Edilmesi/Risk İyileştirmesi)**
 - İzleme ve Gözden Geçirme**
 - İletişim ve Danışma**
 - Kaydetme ve Raporlama**





Eğitimin Amacı

Bu sunumda, literatür taraması ve yürütülen görüşmeler (kamu kurumları, EBYS yazılım firmaları ve alanında uzman akademisyen/uzmanlar) sonucunda elde edilen veriler doğrultusunda; kurum ve kuruluşların Elektronik Belge Yönetim Sistemi (EBYS) ve buna bağlı iş süreçlerinde karşılaştıkları ya da karşılaşma potansiyeli taşıyan risk unsurları sistematik bir şekilde incelenecektir.

Sunumun temel amacı, katılımcıların EBYS kapsamındaki riskler hakkında bilgi sahibi olmalarını sağlamak, farkındalıklarını artırmak ve bu risklere karşı uygulanabilecek etkili yönetim stratejileri konusunda yol göstermektir.

Bu amaç doğrultusunda sunum kapsamında aşağıdaki başlıklar ele alınacaktır:

- EBYS ve risk kavramlarına ilişkin temel açıklamalar yapılacaktır,
- Elektronik belge yönetimi süreçlerinde ortaya çıkan risk unsurları ve bu risklerin yönetimine yönelik süreçler detaylı biçimde değerlendirilecektir.



Elektronik Belge Yönetimine Yönelik Kavramlar

Belge,

- Bir şahıs, kurum veya kuruluş tarafından üretilen ya da kuruluşa gelen, fiziksel yapısı ya da üretildiği ortam ne olursa olsun, kültürel, idari ve hukuki nedenlerle gelecekte kullanılma potansiyeli taşıyan ve bu yönüyle kanıt niteliği bulunan her türden kaydedilmiş bilgidir.
- Kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin resmi iş ve işlemleri sonucunda ortaya çıkan; yazılı, çizili, resmedilmiş, görüntülü, sesli ya da elektronik ortamlarda üretilmiş ve hukuki geçerlilik taşıyan bu kayıtlar, belge olarak değerlendirilir (Devlet Arşivleri Başkanlığı, 2024, s.8).
- Bu tanım, Uluslararası Standartlar Örgütü tarafından yayımlanan ISO 15489-1:2016 standardında geçen belge tanımıyla da örtüşmektedir. Söz konusu standarda göre belge; “Bir kuruluş ya da kişi tarafından yasal yükümlülüklerin yerine getirilmesi, iş faaliyetlerinin yürütülmesi ya da karar alma süreçlerinin belgelenmesi amacıyla kanıt ve bilgi içeriği taşımak üzere oluşturulan, alınan ve saklanan kayıtlı bilgi” olarak tanımlanır (ISO, 2016, s. 2).



Elektronik Belge Yönetimine Yönelik Kavramlar

Belge Yönetimi,

Kurum ve kuruluşlarda belge niteliği taşıyan bilgilerin üretiminden nihai tasfiyesine (imha ya da arşivleme) kadar geçen tüm sürecin sistematik ve kontrollü bir biçimde yürütülmesini sağlayan yönetsel faaliyetler bütünüdür.

- Bu süreç; belgelerin oluşturulması, sınıflandırılması, erişimi, kullanımı, saklanması, güvenliği, düzenli olarak gözden geçirilmesi ve gerektiğinde imha edilmesi ya da arşivlenmesini içerir.



Elektronik Belge Yönetimine Yönelik Kavramlar

Elektronik Belge,

Çeşitli bilgisayar ve taşınabilir elektronik araçlarla oluşturulan; kurumlar, birimler ya da kişiler arasında aktarılabilen ve dijital ortamlarda saklanabilen, yazılı, sesli veya görsel bilgi içeren her türlü kayıttır. Bu belgeler, ulusal ve uluslararası mevzuat ve standartlar doğrultusunda güvenli biçimde iletilebilir, saklanabilir veya imha edilebilir (Devlet Arşivleri Başkanlığı, 2024).





Elektronik Belge Yönetimine Yönelik Kavramlar

Elektronik Belge Yönetimi,

- Elektronik belge yönetimi ise, kurumların günlük iş süreçlerinde oluşturdukları bu bilgi ve belgelerin, içerik ve biçim bütünlüğünü koruyarak, elektronik ortamda yönetilmesini sağlayan sistematik bir süreçtir (Türkiye Bilişim Derneği, 2009).
- TS 13298 standardına göre ise elektronik belge yönetimi; Dokümantasyonun içerisinden kurumsal faaliyetlerin yasal delili sayılabilecek belgelerin ayıklanarak, içerik, format ve ilişkisel bağlamları korunmak suretiyle üretimden nihai tasfiyeye kadar tüm yaşam döngüsünün etkin biçimde yönetilmesini kapsamaktadır (TS 13298, 2015).



Elektronik Belge Yönetimine Yönelik Kavramlar

Elektronik Belge Yönetim Sistemi (EBYS),

İdarelerin faaliyetlerini yerine getirirken hazırladıkları ve faaliyetlerinin delili olabilecek e-Yazışma Teknik Rehberi'ne uygun belgelerin içerik, üst veri, format ve ilişkisel özelliklerini koruyan, belgelerin ait olduğu fonksiyon veya işlem için delil teşkil eden ve aidiyet zinciri içerisindeki yönetimini elektronik ortamda sağlayan sistemi(Resmi Yazışma Kuralları, 2020)

Elektronik Belge Yönetimine Yönelik Kavramlar

- Belgelerin, üretim işleminden başlanarak belge yönetim süreci boyunca geçireceği aşamaların bir otomasyon sistemi ile yürütülmesini içeren bilgi sistemidir (Yalçınkaya, 2016: 136-137).
- EBYS, belgeyi dijital ortamlarda kaydedip, belge yönetim esaslarına göre yönetme imkânı sağlayan bir araçtır (Odabaş, 2007: 239).
- Kurum ve kuruluşlar için yönetimin bir unsuru olan belge, yapılan faaliyetlerin kanıtı olduğundan bir sermaye kadar değerlidir. Bu kadar önemli olan belgelerin üretiminden arşivlenmesine kadar geçireceği tüm işlemlerin belirli bir sistem dâhilinde yönetilmesi gerekir (Odabaş ve Polat, 2008, 239-240).



Risk Yönetimine Yönelik Kavramlar

Risk,

- Oxford Languages'a göre 'gelecekte zarara uğrama olasılığı' olarak tanımlanmaktadır (Oxford University Press, 2023).
- Türk Dil Kurumu benzer şekilde 'bir zararla karşılaşma ihtimali' olarak ifade eder (TDK, 2022).
- International Organization for Standardization (ISO) ise riski, 'kurumların hedeflerinden sapmasına neden olan belirsizlikler' olarak açıklamaktadır (ISO 31000, 2018, s. 1).



Risk Yönetimine Yönelik Kavramlar

- Kamu Risk Yönetimi Rehberine göre risk, sözlük anlamıyla «zarara uğrama tehlikesi» olarak tanımlanırken bu tanımda geçen tehlike ise gerçekleşme ihtimali olan ama istenmeyen, sakıncalı durumları ifade etmektedir. Bu bağlamda risk:
 - Belirli bir amaç veya faaliyet söz konusu olduğunda ortaya çıkan,
 - Olumlu etkiler **fırsat**,
 - Olumsuz etkiler ise **tehdit** olarak değerlendirilmektedir.
- Kamu yönetimi açısından risk, idarelerin stratejik amaç ve hedeflerine ulaşmalarını olumlu ya da olumsuz yönde etkileyebilecek olay veya durumlar olarak tanımlanmaktadır.
- Günümüzde küreselleşme, teknolojik gelişmeler, mevzuat değişiklikleri ve artan paydaş beklentileri gibi faktörler, kamu idarelerinin hedeflerine ulaşma sürecini karmaşıktırmaktadır. Bu nedenle idarelerin, karar alma süreçlerinde riskleri önceden belirleyip değerlendirmeleri; riskler gerçekleşmeden önce önlem almaları veya gerçekleşme durumunda zararı azaltacak plan ve yöntemler geliştirmeleri gerekmektedir. (Hazine ve Maliye Bakanlığı,2024, s.8)



Risk Yönetimine Yönelik Kavramlar

Risk Yönetimi,

- Bir kuruluşun stratejik hedeflerini etkileyebilecek olay veya durumları bütüncül bir bakış açısıyla tanımlaması, bu risklerin olasılık ve etkilerini analiz etmesi, önem derecelerine göre önceliklendirmesi ve uygun yanıt stratejilerini belirlemesi sürecidir.
- Ayrıca risklerin izlenmesi ve raporlanmasını da içeren bu süreç; sistematik, sürekli ve uyarlanabilir bir yapıya sahiptir. Etkin risk yönetimi, olumsuz etkilerin azaltılmasını ve ortaya çıkabilecek fırsatların kurumsal değere dönüştürülmesini mümkün kılmaktadır (Hazine ve Maliye Bakanlığı,2024, s.8)



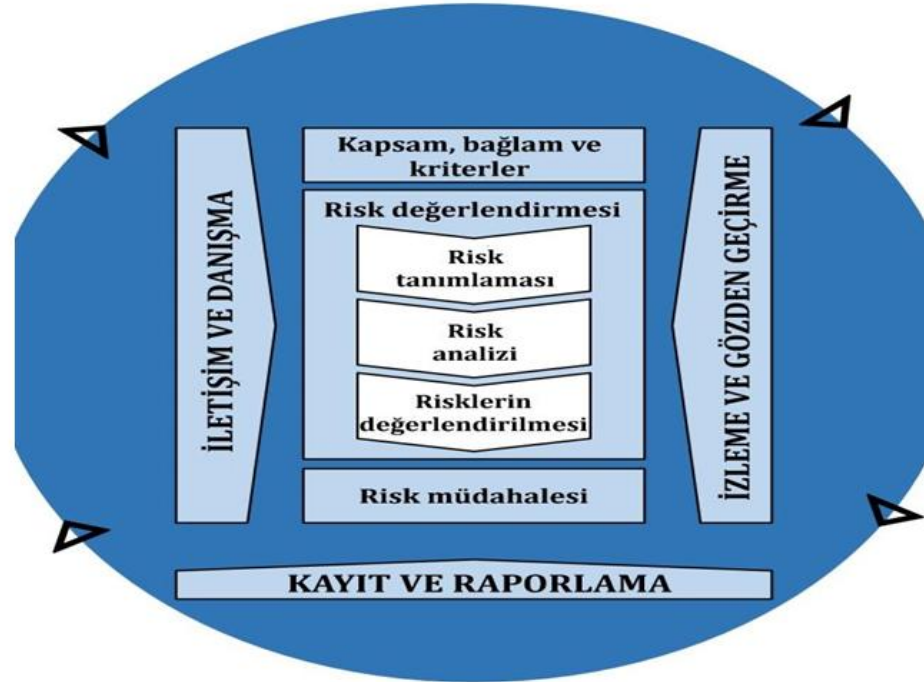
Risk Yönetimine Yönelik Kavramlar

Risk İştahı,

- Bir kuruluşun stratejik hedeflerine ulaşmak amacıyla kabul edebileceği risk düzeyini ifade etmektedir. Kurumsal risk yönetiminin temel unsurlarından biri olan bu kavram, risk ile getiri arasındaki dengeyi yansıtmaktadır. Üst yönetim tarafından belirlenmekte ve kuruluşun genel stratejisiyle uyumlu olması beklenmektedir.
- Çevresel faktörler, sektör koşulları ve paydaş beklentileri gibi unsurlar risk iştahını etkilemektedir. Yüksek risk iştahı, daha yüksek getiri potansiyeli ile birlikte daha büyük kayıpları da beraberinde getirebilmektedir. Düşük risk iştahı ise zararları sınırlamakla birlikte fırsatların kaçırılmasına yol açabilmektedir. Bu nedenle, risk iştahının dengeli biçimde yönetilmesi, kurumsal sürdürülebilirlik açısından kritik bir rol oynamaktadır (Hazine ve Maliye Bakanlığı, 2024, s.30).



Risk Yönetimine Yönelik Kavramlar



Kaynak: ISO 31000, 2018, s.9

Risk Yönetimine Yönelik Kavramlar

Süreç	Açıklama
Risk Değerlendirmesi	Risklerin tanımlanması, analizi ve değerlendirilmesi süreçlerini içerir. Potansiyel riskler belirlenir, olasılık ve etki değerleri analiz edilir, riskler önceliklendirilerek kabul edilebilirliği değerlendirilir.
Risk Müdahalesi	Belirlenen risklere yönelik aksiyonların alınması.
İzleme ve Gözden Geçirme	Risklerin sürekli olarak izlenmesi.
İletişim ve Danışma	Risk yönetim süreçlerine dair bilgilendirme ve danışma faaliyetlerinin yürütülmesi.
Kaydetme ve Raporlama	Risk yönetim süreçlerinin belgelenmesi ve raporlanması.



Elektronik Belge Yönetimi Sistem ve Süreçlerinde Risk

- EBYS, yalnızca belgelerin dijital ortama aktarılmasını sağlayan bir araç değil; aynı zamanda kurumsal hafızayı oluşturan, yasal sorumlulukları belgeleyen ve bilgi güvenliğini sağlayan stratejik bir sistemdir. Bu yapı, doğal olarak çok katmanlı riskleri de beraberinde getirmektedir.
- Uluslararası Belge Yönetimi Standardı ISO 15489, bir belgenin taşınması gereken temel nitelikleri özgünlük (authenticity), güvenilirlik (reliability), bütünlük (integrity) ve kullanılabilirlik (usability) olarak tanımlamaktadır.
- Bu nitelikler, belgenin sadece içeriğiyle değil, aynı zamanda üretildiği bağlam, ilişkili olduğu süreçler ve kullanım amacı ile birlikte değerlendirilmesini zorunlu kılmaktadır.

- TS 13298 Elektronik Belge ve Arşiv Yönetimi Standardı ise, dijital ortamda üretilen belgelerin taşınması gereken daha ayrıntılı özellikleri belirlemektedir:
Tanımlanabilirlik, bütünlük, onay ve kayıt bilgisi, yapısal özellikler, üretim sorumluluğu, mülkiyet hakları ve teknolojik nitelikler.

Belge Kriteri	Tanım / Açıklama	Uygulama Örneği
Tanımlanabilirlik	Elektronik belgenin üretici, yazar, alıcı, tarih gibi kimlik bilgileriyle tanımlanabilir olması gerekir.	Bir e-yazışmada üretici kurumun adı, yazarı olan memurun kimliği, iletim ve arşivleme tarihleri EBYS'de kayıtlıdır.
Bütünlük	Belgenin içeriği, tanımlayıcı bilgileri ve fiziksel yapısının bozulmadan korunması gerekir. Entelektüel, tanımsal ve fiziksel bütünlük sağlanmalıdır.	Elektronik imza ile imzalanan bir belgeye sonradan müdahale edilirse, sistem bu durumu tespit ederek uyarı verir.
Onay ve Kayıt Bilgisi	Belgenin yetkili kişilerce onaylanması ve kayıt altına alınması; elektronik imza, mühür, zaman damgası gibi araçlarla belgelemesi gereklidir.	Resmî bir karar yazısı, yetkili amir tarafından güvenli elektronik imza ile onaylanarak kayıt sistemine işlenir.
Yapısal Özellikler	Belgenin ürettiği andaki sunum biçimi, formu ve dosya formatı korunmalıdır.	Rapor formatında hazırlanan bir belge, PDF/A formatında saklanarak sunum özellikleri sabitlenir.
Üretim Sorumluluğu ve Mülkiyet Hakları	Belgenin üretiminden tasfiyesine kadar geçen süreçte sahiplik, ilişkili kurum ve belgelerle olan bağ korunmalı; provenans bilgisi izlenebilir olmalıdır.	Bir ihaleye ait belge, ilgili dairenin ürettiği, işlem süreci boyunca izlenen ve sonunda arşive devredilen bir kayıttır.
Teknolojik Özellikler	Belgeyle ilişkili donanım, yazılım, veri/dosya formatı, sistem yönetimi gibi teknolojik altyapı unsurları kayıt altına alınmalıdır.	Belgeyi oluşturan sistemde kullanılan işletim sistemi, yazılım sürümü ve veri tabanı formatı sistem loglarında tutulur.



- Bu özellikler, elektronik belgelerin hem uzun vadeli korunmasını hem de yasal geçerliliğini doğrudan etkilemektedir. Nitekim Akgün ve Çiçek (2022, s.36) bu niteliklerin belgenin dijital kimliğini ve sürdürülebilirliğini doğrudan belirlediğini belirtirken, Kandur (2011, s. 4–5), elektronik belgelerin yalnızca içerikleriyle değil, bağlamsal ve ilişkisel bütünlükleriyle birlikte korunmasının zorunlu olduğunu, aksi takdirde belgelerin hukuki açıdan geçerliliğinin tartışmalı hâle gelebileceğini vurgulamaktadır.
- Bu çerçevede, elektronik belge yönetimi; yalnızca fiziksel belgelerin dijital ortama aktarılması süreci değil, aynı zamanda kurumsal bellek, yasal sorumluluk ve bilgi güvenliği açısından yeniden yapılanmayı gerektiren stratejik bir alandır.

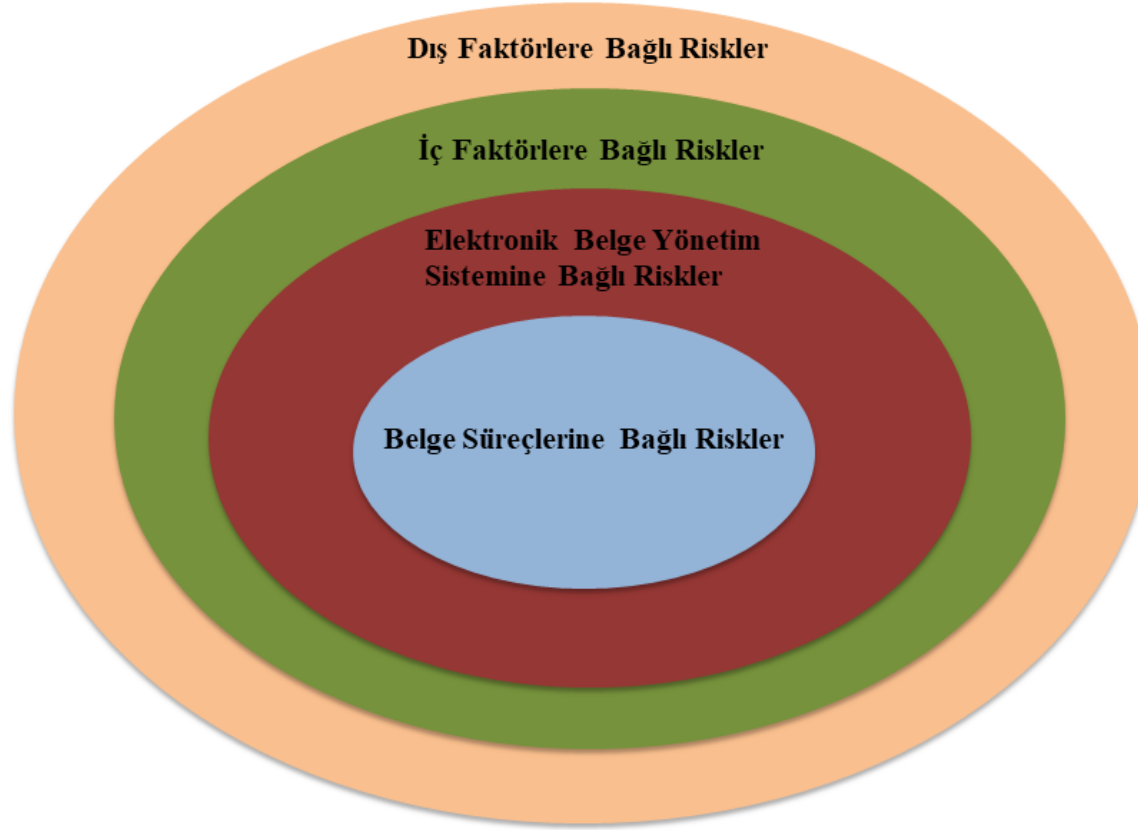


- Tanımlayıcı unsurların eksikliği, bütünlük zincirinin kırılması, onay ve kayıt mekanizmalarının yetersizliği ya da teknolojik altyapının güvenilir olmaması, belgelerin geçerliliğini doğrudan tehdit eden başlıca risk alanları arasında yer almaktadır.
- Ayrıca, dijital sistemlerdeki hızlı teknolojik dönüşüm, veri formatlarının zamanla geçersiz hâle gelmesi, yazılım ve donanım uyumsuzlukları gibi etkenler de belgelerin uzun vadeli erişilebilirliğini ve kullanılabilirliğini riske atmaktadır.



- Bu noktada, ISO 15489 ve TS 13298 gibi standartlarda tanımlanan belge niteliklerinin kurumsal düzeyde eksiksiz bir biçimde uygulanabilmesini engelleyen tüm risklerin tanımlanması ve yönetilmesi gerekmektedir.
- Kamu Risk Yönetim Rehberi, bu tür kurumsal risklerin yalnızca bilgi güvenliği bağlamında değil, aynı zamanda hesap verebilirlik, şeffaflık ve kurumsal süreklilik açısından da değerlendirilmesi gerektiğini vurgulamaktadır.
- Rehberin önerdiği yaklaşıma göre:EBYS'ye ilişkin tüm potansiyel risklerin tanımlanması,stratejik amaç ve hedeflerin yasal düzenlemelerle uyumlu ve risk temelli belirlenmesi,kurumun misyon, vizyon ve değerlerine uygun bir risk iştahı ve risk kapasitesi tanımlanması,risklerin birim, faaliyet ve süreç düzeyinde analiz edilmesiöncelikli adımlar olarak görülmektedir.

Bu çerçevede, Elektronik Belge Yönetim Sistemlerinde ve Süreçlerinde ortaya çıkan risk unsurları, kaynaklarına ve etki alanlarına göre dört ana başlık altında ele alınacaktır:



Elektronik Belge Yönetim Sistemlerinde ve Süreçlerinde Risk Unsurları

RİSKLER	
1. Dış Faktörlere Bağlı	Siyasi-Toplumsal Bağlamdaki Değişiklikler
	Makro Ekonomik ve Teknolojik Çevre
	Fiziksel Çevre ve Altyapı
2. İç Faktörlere Bağlı	Organizasyonel Değişim
	İnsan Kaynakları, Yetkinlikler ve Finansman
3. Elektronik Belge Yönetim Sistemine Bağlı	EBYS Tasarımı
	EBYS Bakımı
	Güvenlik
	Birlikte Çalışabilirlik
	Sürdürülebilirlik ve Süreklilik
4. Elektronik Belge Yönetim Süreçlerindeki	Elektronik Belgenin Oluşturulması
	Elektronik Belgenin Kullanımı/Paylaşılması
	Kullanılabilirliğin Sürdürülmesi
	Elektronik Belgeye Erişim
	Elektronik Belgenin Saklanması-Arşivlenmesi
	Elektronik Belgelerde Arama İmke



Dış Faktörlere Bağlı Riskler:Siyasi, hukuki, ekonomik ve teknolojik çevredeki değişimlerden kaynaklanan ve kurumsal kontrol alanı dışında gelişen riskleri kapsamaktadır.

İç Faktörlere Bağlı Riskler:Kurumun kendi yapısı, kaynakları, personeli, yönetim anlayışı ve iş süreçlerinden kaynaklanan sistem içi riskleri ifade etmektedir.

EBYS'ye Bağlı Sistemsel Riskler:Sistem tasarımı, teknik altyapı, yazılım özellikleri, tedarikçi ilişkileri ve dijital uyumluluk gibi faktörlerden kaynaklanan yapısal risklerdir.

EBYS Süreçlerine Bağlı Operasyonel Riskler:Belge üretimi, erişimi, sınıflandırılması, dosyalanması, saklanması ve arşivlenmesi gibi süreçlerde karşılaşılan uygulama kaynaklı riskleri içermektedir.

Bu sınıflandırma, EBYS kapsamındaki risklerin daha sistematik bir biçimde analiz edilmesini ve her bir risk alanı için stratejik yönetim adımlarının belirlenmesini mümkün kılmaktadır.

1. Dış Faktörlere Bağlı Riskler

- Kurumun faaliyet gösterdiği siyasi, ekonomik, sosyal ve teknolojik çevredeki değişimler, doğal afetler, ekonomik krizler, yasal düzenlemeler gibi dış etkenlere bağlı risk faktörlerini beraberinde getirir.
- Bu faktörler, kurumun strateji, operasyon, itibar ve finansal performansı üzerinde olumsuz etkiler yaratabilmektedir (Usman ve Kaygusuz, 2018, s.115).



1. Dış Faktörlere Bağlı Riskler

1.1.Siyasi-Toplumsal Bağlamdaki Değişiklikler

EBYS, siyasi istikrar, yönetim anlayışı ve toplumsal beklentiler gibi dışsal faktörlerden doğrudan etkilenebilmektedir. Hükümet politikalarında, mevzuatta veya teknik standartlarda meydana gelen değişiklikler, EBYS'nin işleyişinde belirsizliklere ve uyum sorunlarına yol açarak kurumsal bilgi yönetiminde stratejik riskler oluşturabilmektedir.





Hükümet Politikaları

- Siyasal otoritenin bilgi yönetimi, dijital dönüşüm ve e-devlet uygulamaları konusundaki yaklaşımındaki değişiklikler, EBYS uygulamalarını doğrudan etkileyebilmektedir.
- Yönetim anlayışındaki dönüşüm, belge yönetimi sistemlerinin kurumsal öncelik sıralamasında geri plana itilmesine veya bütçe ve kaynak tahsislerinde kesintilere yol açarak stratejik belirsizliklere neden olabilmektedir.



Yasal ve Düzenleyici Değişiklikler

- Belge yönetimi süreçlerini etkileyen mevzuatta meydana gelen değişiklikler (örneğin; arşiv mevzuatı, kişisel verilerin korunması, bilgi edinme hakkı gibi düzenlemeler), mevcut sistemin işleyişiyle çelişebilir ve uyum gereksinimini doğurabilmektedir.
- Bu tür düzenlemelere uyum sağlanamaması, kurumların yasal sorumluluklarını yerine getirememesi riski ile karşı karşıya kalmalarına neden olmaktadır.



Yeni Standartlar ve Teknik Uygulamalar

- Ulusal veya uluslararası düzeyde yayınlanan yeni teknik standartlar ve uygulama çerçeveleri (örneğin; ISO, TS 13298 güncellemeleri, ELAS/RM gibi) EBYS'nin yapısal ve işlevsel düzeyde güncellenmesini gerektirebilir.
- Bu standartlara uyum sağlanamaması, sistemin geçerliliğini ve güvenilirliğini zayıflatmakta; dış denetimlerde uyumsuzluk ve kalite kaybı risklerini ortaya çıkarmaktadır.



Yasal düzenlemelerdeki değişiklikler veya hükümet politikalarındaki yön değişimlerin oluşturabileceği riskler:

Oluşabilecek Riskler		
Personel Alışkanlıkları/Uyum Sorunu	Sistemin Uyum Sorunu	Mevzuat Eksikliği/Belirsizliği
Hizmetlerin Aksaması	İş Yüktü	Belge Sürekliliğinin Sağlanamaması
Kurumsal Hazırlık Eksikliği	Belge Güvenliği	Belgenin Delil Değerini Kaybetmesi
Bilgilendirme Eksikliği	Erişim	Maliyet
Personel/Sistem Değişikliği	Planlama Eksikliği	Sistemin Yeniden Yapılanması
Standartlaşmama	Teknoloji Üretimi	Uygulama ve Denetleme Eksikliği
Uzman Personel Eksikliği	Yazılımcıların Bilgi Eksikliği	



Örnek: Uyum Sorunu

EBYS’de yapılan güncelleme ile sık kullanılan “**SDP-713**” kodu kaldırılmıştır. Ancak uzun süredir bu kodu kullanan Ayşe Hanım, yeni kodlara alışmakta zorlanmakta ve sistemde “713” kodunu bulamayınca, benzer ama yanlış bir kod olan “721” kodunu kullanmaya başlamıştır.

Sonuç:

Bu durum, belgelerin yanlış sınıflandırılması ve arşivleme-tasfiye süreçlerinde karışıklığa neden olmuştur.

Değerlendirme:

Düzenlemelerde yapılan değişiklikler kullanıcı alışkanlıkları ve yetersiz bilgilendirme ile, ciddi uyum sorunları ve operasyonel riskler doğurabilir.

Katılımcı Görüşü:

- TS 13298:2015 standardının güncellenmesiyle birlikte bütünleşik arşiv yönetim sistemi devreye alınmıştır. Yeni düzenlemeyle, kamu kurumları belgelerini, içerik,format ve sunum özelliklerini koruyarak arşiv yönetim sistemine aktarmalıdır. Ancak yapılan gözlemler ve görüşmelerde bazı kurumların bu değişikliğe hazırlıksız yakalandığı görülmüştür. Belgelerin ileride arşivleneceği düşünülmediği için:

Önceden değerlendirme yapılmamış,
Belgeler için saklama süresi belirlenmemiş,
Saklama planı oluşturulmamıştır.

- Yeni standart, sadece belge devrini değil, sistem içinde belirli uygulamaların yapılmasını da zorunlu kılmaktadır. Örneğin, kurumun belgeyi dosya formatında oluşturması ve belirli bir arayüz üzerinden arşiv sistemine aktarması gerekmektedir.Ancak bazı kurumlar:

Dosya formatında üretim yapmadıkları,
Gerekli teknik uygulamaları sistemlerinde kurmadıkları içinbu değişikliklere uyum sağlayamamakta, bu da önemli bir uyumsuzluk ve operasyonel risk oluşturmaktadır.



Paydaş Beklentileri

- İç ve dış paydaşların bilgiye hızlı erişim, kurumsal şeffaflık ve hizmet kalitesi konularındaki artan beklentileri, EBYS sistemlerine yönelik performans ve etkililik baskısını artırmaktadır.
- Sistemin bu beklentileri karşılamada yetersiz kalması, kurumsal güvenin sarsılmasına ve kullanıcı bağlılığının azalmasına neden olabilir.



Taleplerin ve Kullanıcı Davranışlarının Değişmesi

- Teknolojik gelişmeler ve dijital kullanıcı alışkanlıklarındaki dönüşüm, EBYS sistemlerinin daha esnek, entegre ve kullanıcı odaklı hale gelmesini zorunlu kılmaktadır.
- Kullanıcı ihtiyaç ve taleplerine hızlı yanıt veremeyen sistemler, resmi süreçlerin dışında alternatif yolların gelişmesine neden olabilir; bu da kurumsal bilgi yönetiminde kayıt dışılık ve denetimsizlik gibi ciddi riskler doğurur.



1. Dış Faktörlere Bağlı Riskler

1.2.Fiziksel Çevre ve Altyapı

- Fiziksel çevre ve altyapıya bağlı riskler; doğal afetler, insan kaynaklı felaketler ve altyapı bozukluklarından kaynaklanarak belge yönetimi sistemlerini doğrudan etkileyebilecek ciddi tehditlerdir. Bu tür olaylar, belgelerin fiziksel bütünlüğünü ve erişilebilirliğini tehlikeye atabilir.

Başlıca risk kaynakları şunlardır:

- **Deprem, yangın, sel, fırtına gibi doğal afetler**, belgelerin depolandığı alanlarda yıkıcı etkilere neden olabilir.
- **Savaş ve terör eylemleri**, özellikle kamu kurumlarında hizmet kesintilerine ve bilgi kaybına yol açabilir.
- **Altyapı arızaları** (su, enerji, bilişim sistemleri, ulaşım vb.), belge yönetimi süreçlerinin aksamasına neden olabilir.



Katılımcı Görüşleri-Beklenmedik Olayların Oluşturduğu Riskler

- Kurumsal bilgi sistemlerinde karşılaşılan en kritik tehditlerden biri, beklenmedik olaylar sonucu ortaya çıkabilecek **veri kaybı riski**dir. Katılımcı görüşleri doğrultusunda yapılan değerlendirmelerde, bu riskin yalnızca teknik bir problem olarak değil, aynı zamanda **kurumsal süreklilik, hizmet güvenliği ve bilgi bütünlüğü** açısından stratejik bir öneme sahip olduğu açıkça ortaya konulmaktadır.
- Ekonomik, çevresel veya teknolojik nedenlere bağlı olarak meydana gelebilecek olağanüstü durumlar karşısında, **veri yedekleme altyapısının eksikliği** veya **felaket kurtarma merkezlerinin (FKM) yetersizliği**, kurumsal sistemlerin tüm verilerini geri döndürülemez biçimde kaybetme riskiyle karşı karşıya bırakmaktadır. Bu bağlamda, Olağanüstü Durum Merkezleri (ODM) ve sistem replikasyonları gibi yapıların önceden planlanması ve kurumsal sistemlere entegre edilmesi, **iş sürekliliğinin sağlanması bakımından elzemdir**.



Katılımcı Görüşleri-Beklenmedik Olayların Oluşturduğu Riskler

- Katılımcılar, özellikle veri depolama cihazlarının yedekleme mekanizmalarının ulusal ve uluslararası standartlara uygun biçimde yapılandırılmaması hâlinde, afet veya saldırı senaryolarında veri güvenliğinin ciddi şekilde tehlikeye gireceğini ifade etmektedirler. Ayrıca, afet sonrası müdahale süreçlerinin önceden tanımlanmaması, hizmetlerin yeniden başlatılmasında **ciddi operasyonel aksamalara** ve **maliyet kayıplarına** neden olabilmektedir.



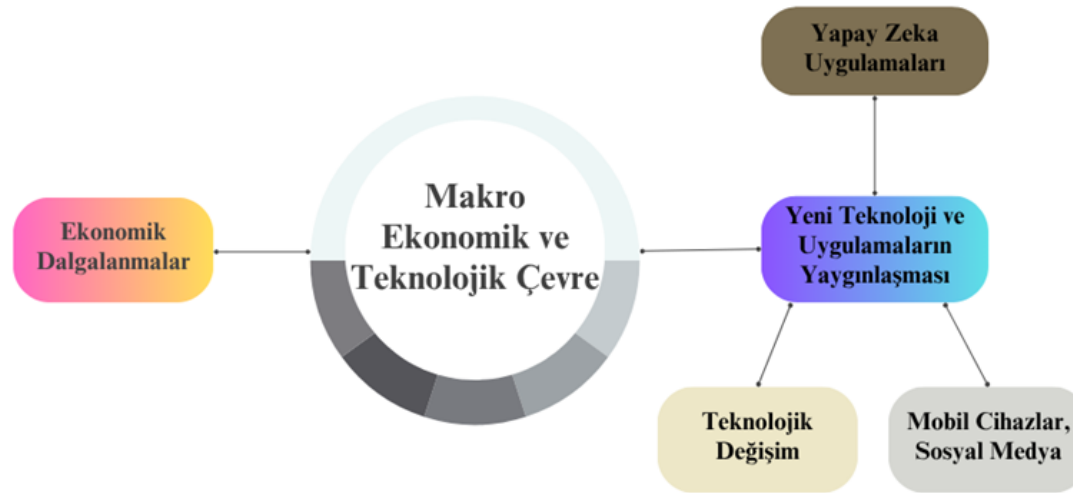
Katılımcı Görüşleri-Beklenmedik Olayların Oluşturduğu Riskler

- Türkiye’de doğal afet kaynaklı risklere karşı yeterli önlem alınmaması, bilgi ve belge yönetimi açısından önemli bir zafiyet alanı olarak değerlendirilmektedir. Katılımcıların görüşleri doğrultusunda, afet risklerine yönelik veri güvenliği planlamasında temel ilkenin “**birden fazla coğrafi ve teknik kopya, riski azaltır**” yaklaşımı çerçevesinde ele alınması gerektiği vurgulanmaktadır.
- Bu kapsamda, verilerin yalnızca tek bir fiziksel lokasyonda değil; farklı afet risk senaryoları göz önünde bulundurularak, **coğrafi olarak ayrıştırılmış ve güvenli bölgelerde** yedeklenmesi gerektiği belirtilmektedir. Örneğin, sel riski yüksek bir bölgede (örneğin Bartın) bulunan verilerin yedeği, hem sel hem de deprem riski düşük olan başka bir bölgeye aktarılmalıdır. Benzer şekilde, deprem riski yüksek alanlarda faaliyet gösteren kurumlar, veri yedeklerini daha düşük riskli bölgelere fiziksel olarak taşımalı ya da bu bölgelerde veri merkezi hizmeti almalıdır. Nitekim, birçok kamu kurumunun deprem sonrası Ankara gibi görece daha güvenli bölgelerde sunucu ve disk altyapısını konumlandırması bu stratejik yaklaşımın uygulandığını göstermektedir.
- Katılımcılar, bu tür önlemlerin afet meydana geldikten sonra değil, **afet öncesinde proaktif şekilde planlanması gerektiğini** ifade etmektedir. Kurumların, faaliyet gösterdikleri bölgenin risk haritasına göre **hangi afet türlerinin kabul edilebilir düzeyde risk içerdiğini** belirlemeleri ve buna uygun **yedekleme politikaları geliştirmeleri** gerektiği vurgulanmaktadır.

1. Dış Faktörlere Bağlı Riskler

1.3. Makro Ekonomik ve Teknolojik Çevre

EBYS, makro ekonomik koşullar ve teknolojik gelişmelerden doğrudan etkilenmektedir. Ekonomik belirsizlikler, bilgi teknolojileri alanına ayrılan bütçelerde kısıtlamalara yol açarak sistem yenileme, bakım ve eğitim gibi temel ihtiyaçların karşılanmasını zorlaştırabilmektedir. Öte yandan, hızla gelişen dijital teknolojiler, EBYS'nin mevcut yapısını zorlamakta ve güvenlik, uyumluluk ile erişilebilirlik açısından yeni riskler doğurmaktadır. Bu nedenle, ekonomik ve teknolojik çevredeki değişimlerin dikkatle izlenmesi, EBYS'nin sürdürülebilirliği açısından kritik önem taşımaktadır.





Ekonomik Dalgalanmalar

- Küresel ve ulusal ölçekte yaşanan ekonomik belirsizlikler, kamu kurumlarının bilgi teknolojilerine ayırdığı kaynaklarda kısıtlamalara yol açabilmektedir. Enflasyon, döviz kuru artışları ve bütçe daralmaları gibi ekonomik göstergeler, EBYS'ye ilişkin lisans yenilemeleri, teknik bakım, donanım güncellemeleri ve kullanıcı eğitimi gibi maliyet kalemlerinin karşılanmasını güçleştirebilir. Bu durum, sistemin güncelliğini yitirmesi, hizmet kesintileri yaşanması ve stratejik planlamaların aksaması gibi yapısal riskleri beraberinde getirmektedir.
- *“Ekonomik krizler, sahip olduğumuz teknolojik koşulların devam ettirilmemesi gibi bir riske sebep oluyor. Buna kurum ne kadar çözüm getirebilir ciddi bir mesele. Öncelikle bazı firmalar bakım sözleşmesi yapmayabilir ya da bakım sözleşmesinin içeriğini düşürebilir. Aldığı anlık yedeklemelerde sayıyı azaltabilir, teknolojiyi yenilemeyebilir böyle risklere de sebep olabilir.”*



Yeni Teknoloji ve Uygulamaların Yaygınlaşması

Yapay Zekâ, Makine Öğrenmesi ve Nesnelerin İnterneti (IoT):

- Yapay zekâ, makine öğrenmesi ve nesnelerin interneti gibi yeni nesil teknolojilerin kurumsal sistemlere entegrasyonu; iş süreçlerinin otomasyonu, işlem hızının artırılması ve karar destek mekanizmalarının güçlendirilmesi açısından önemli fırsatlar sunmaktadır. Bu teknolojiler, özellikle belge sınıflandırma, içerik tanıma ve dijital arşiv süreçlerinde yenilikçi uygulamaların önünü açmaktadır.
- Ancak, söz konusu teknolojilerin belge yönetimi sistemlerine entegrasyonu, beraberinde çeşitli güvenlik, gizlilik ve uyum risklerini de getirmektedir. Özellikle yapay zekâ algoritmalarının eğitildiği veri setlerinin içeriği ve kaynağı çoğu zaman belirsizdir.
- Bu belirsizlik, hassas ve gizli belgelerin farkında olunmadan dış sistemlerle paylaşılması gibi ciddi riskleri doğurabilir. Örneğin, sağlık, adli ya da kamu güvenliğine ilişkin belgelerin yer aldığı veri kümelerinin dış kaynaklı yapay zekâ modelleriyle paylaşılması, belge ifşası ve yetkisiz erişim gibi sorunlara yol açabilir.



«Kullandığımız derin öğrenme algoritmalarının arka planında, geliştiricisine eğitim verisi gönderilip gönderilmediğini çoğu zaman kesin olarak bilemiyoruz. Bu durum, özellikle hassas verilerin işlendiği alanlarda ciddi güvenlik ve gizlilik risklerini beraberinde getirmektedir. Örneğin, tıp alanında bu tür risklerin somut örneklerine rastlanmaktadır. Bir senaryoya göre, kötü niyetli bir ilaç şirketi, bir hastanenin MR görüntülerini doğrudan değil, sonuç raporları düzeyinde manipüle edebilen bir zararlı yazılım (virüs) geliştirerek, teşhis verilerini kendi geliştirdiği ilacın kullanımını teşvik edecek şekilde değiştirebilmektedir. Bu tür örnekler, gelecekte karşılaşılmaması muhtemel tehditlerin boyutunu gözler önüne sermektedir. Yapay zekâ teknolojileri üzerinden yürütülebilecek bilgi savaşları olasılığı, artık göz ardı edilemeyecek düzeydedir. Bu bağlamda, gizli kalması gereken belge setlerine yapay zekâ algoritmalarının erişme ihtimali de önemli bir güvenlik açığı oluşturmaktadır. Çünkü belirli bir kurumun gizli belge türlerinde kullandığı yapısal kalıplar (örüntüler), yapay zekâ tarafından öğrenilebilir ve bu örüntüler taklit edilerek, sanki o kurumdan çıkmış gibi görünen sahte belgeler üretilir. Bu nedenle, yapay zekâ tabanlı uygulamalarda kullanılacak algoritmaların da tıpkı yazılım sistemlerinde olduğu gibi, Birlikte Çalışabilirlik Esasları Rehberi benzeri bir denetim ve onay sürecinden geçirilmesi gerektiğini düşünüyorum..»



- Bu bağlamda, kurumların dış kaynaklı yapay zekâ çözümlerini kullanırken veri mahremiyeti ve güvenilirliği konularında yüksek düzeyde denetim ve kontrol mekanizmaları oluşturması zorunlu hâle gelmektedir.
- Yapay zekâ algoritmalarının nasıl çalıştığı, hangi verilere dayandığı ve bu verilerin ne şekilde işlendiği şeffaf biçimde izlenmelidir.
- Tıpkı yazılım kaynak kodlarında olduğu gibi, yapay zekâ algoritmalarının da bağımsız ve akredite denetim kuruluşları tarafından periyodik olarak denetlenmesi, kamu kurumlarında güven tesis edilmesi açısından kritik bir gerekliliktir.



Veri kalitesi de yapay zekâ uygulamaları açısından önemli bir risk olarak öne çıkmaktadır. Belgelerin nitelikli olmaması, eksik veya hatalı kodlanmış dosyalar, yetersiz üst veri kullanımı gibi durumların yapay zekânın doğru ve güvenilir çıktılar üretmesini engellediği belirtilmektedir. Uluslararası düzeyde yürütülen güvenilir yapay zekâ projelerinde de bu veri yetersizliğinin süreci yavaşlattığı gözlemlenmiştir. Bu nedenle, teknolojik altyapı kadar, verinin içeriğinin ve yapısının da yapay zekâ uygulamaları öncesinde iyileştirilmesi gerektiği ifade edilmektedir.



Yeni Teknoloji ve Uygulamaların Yaygınlaşması

Teknolojik Değişim

- Yapay zeka, makine öğrenmesi ve nesnelerin interneti gibi yeni teknolojilerin EBYS süreçlerinde yarattığı risklerin ardından, kullanılan teknolojinin kendisindeki değişim ve dönüşümün de önemli risk unsurları oluşturduğu görülmektedir. Teknolojik altyapının sürekli evrilmesi, sistemlerin güvenliği, erişilebilirliği, delil değeri ve belgelerin bütünlüğü üzerinde doğrudan etkiler meydana getirmektedir.
- Teknolojik altyapının sürekli değişmesi, belgelerin uzun vadeli geçerliliği ve delil değeri açısından önemli riskler doğurmaktadır. Katılımcılar, özellikle belge formatları ve depolama ortamlarındaki dönüşümlerin belge yönetimi süreçleri üzerindeki etkilerine dikkat çekmektedir.
- Geçmişte kullanılan disket, CD gibi ortamların yerini bugün SSD ve NVMe gibi daha gelişmiş teknolojiler almıştır. Bu tür teknolojik geçişler sırasında, belgelerin yeni sistemlere **zamanında ve uygun formatta aktarılmaması**, ilerleyen dönemlerde **erişim ve uyumluluk sorunlarına** yol açabilmektedir. Belgelerin güncel formatlara dönüştürülmemesi durumunda, gelecekte o belgelere ulaşmak zorlaşabilir; bu da hem **belgenin varlığını hem de hukuki delil niteliğini** riske atabilir.
- Bu nedenle, kurumların teknolojik değişim süreçlerinde son derece **dikkatli ve temkinli** hareket etmesi gerekmektedir. Risk yönetimi açısından, belge güvenliği söz konusu olduğunda herhangi bir açığın kabul edilmemesi ve **düşük risk iştahıyla** hareket edilmesi gerektiği vurgulanmaktadır.

- 
- Kurumlarda gerçekleşen teknolojik dönüşüm süreçleri, EBYS üzerinde yeni güvenlik risklerini de beraberinde getirmektedir. Katılımcılar, özellikle dış kaynaklı hizmet alımlarında yalnızca teknolojinin değil, aynı zamanda **güvenlik altyapısının da eş zamanlı ve eksiksiz şekilde transfer edilmesi** gerektiğini vurgulamaktadır. Bu noktada, teknik tedbirlerle birlikte **hukuki güvenlik mekanizmalarının**, örneğin iyi yapılandırılmış akıllı sözleşmelerin, sürece entegre edilmesi gerekliliği dile getirilmektedir.
 - Teknolojik değişimlerin hızlı yaşanması, sistemlerin güvenlik sürekliliğini tehdit edebilecek boyutlara ulaşabilmektedir. Yeni sistemlere uyum sağlama süreci, sadece operasyonel değil aynı zamanda **bir güvenlik meselesi** olarak değerlendirilmektedir.
 - Ayrıca, donanım ve yazılım güncellemeleri sırasında gerekli sistem yapılandırmalarının (konfigürasyonların) tam olarak yapılmaması, **siber saldırı riski ve veri kaybı** gibi ciddi sonuçlara yol açabilir. EBYS gibi kurumsal bilgi sistemlerinde, teknolojik değişikliklerin ardından yapılandırma eksikliklerinin giderilmemesi, sistemlerin dayanıklılığını zayıflatmakta ve kurumsal verilerin bütünlüğünü tehlikeye atmaktadır.



Yeni Teknoloji ve Uygulamaların Yaygınlaşması

Mobil Cihaz Kullanımı

Kurum çalışanlarının mobil cihazlar aracılığıyla EBYS'ye erişim taleplerinin artması, sistemin mobil uyumluluğu ve siber güvenlik altyapısı açısından yeni gereksinimler doğurmaktadır. Mobil uyumlu olmayan sistemler işlem gecikmelerine neden olurken, kişisel cihazlar üzerinden erişim ise yetkisiz erişim, veri sızıntısı ve bilgi bütünlüğü ihlali gibi riskleri artırmaktadır. Kurumsal kontrol dışında kalan cihazlara yönelik sınırlı denetim, mevcut teknik önlemlere rağmen güvenlik açıklarını tamamen ortadan kaldıramamaktadır. Bu nedenle, mobil erişim süreçlerinde hem sistem hem cihaz düzeyinde çok katmanlı güvenlik politikalarının geliştirilmesi gerekmektedir.



Yeni Teknoloji ve Uygulamaların Yaygınlaşması

Sosyal Medya ve Yeni İletişim Kanalları

- Dijital iletişim araçlarının yaygınlaşması, kurumsal bilgilerin geleneksel yolların dışında sosyal medya ve mesajlaşma uygulamaları üzerinden dolaşıma girmesine neden olmaktadır. EBYS'nin bu iletişim kanallarını kapsayacak şekilde tasarlanmaması, kayıt dışı belge üretimi, bilgi kaybı ve güvenlik açıkları gibi riskleri artırmaktadır.
- Ayrıca resmi belgelerin ekran görüntüsü alınarak sosyal medya ya da kişisel uygulamalarda paylaşılması, belge bütünlüğünü bozmakta ve kurumsal itibarı zedeleyebilmektedir. Bu risklerin önlenmesi için, mobil cihaz politikaları, sosyal medya farkındalık eğitimleri ve güvenli erişim önlemleri büyük önem taşımaktadır.

2. İç Faktörlere Bağlı Riskler

- Risk yönetimi çalışmalarına başlamadan önce, kurumun kapsamlı bir değerlendirmesi yapılmalıdır. Bu değerlendirme, kurum kültürü, yönetim, çalışanlar, paydaşlar, organizasyonel yapı, mevcut insan, sistem, süreç ve finansal kaynaklar ile stratejik hedefler gibi tüm iç etkenlerin detaylı bir analizini içerir.
- Kurumu tam anlamıyla anlamak ve risk yönetimi çalışmalarına uygun bir çerçeve çizmek, başarılı bir risk yönetimi uygulamasının temelini oluşturur. Bu sayede kurum, olası risklere karşı daha hazırlıklı hale gelir ve stratejik hedeflerine daha etkin bir şekilde ulaşabilir.





2. İç Faktörlere Bağlı Riskler

2.1. Organizasyonel Değişim

- Organizasyonel değişimler, literatürde hem içsel dinamiklerden hem de dışsal faktörlerden kaynaklanabilen çok boyutlu bir olgu olarak değerlendirilmektedir. Ancak bu çalışmada, organizasyonel değişimlerin sınıflandırılmasında değişimin kaynağından ziyade, kurumun iç işleyişine olan etkisi temel alınmıştır.
- Bu bağlamda, her ne kadar bazı organizasyonel değişimler makroekonomik koşullar, teknolojik gelişmeler ya da merkezi düzeyde alınan yönetsel kararlar neticesinde ortaya çıksa da —örneğin üniversitelerin ayrılması, bazı kamu kurumlarının kapatılması ve görevlerinin başka kurumlara devredilmesi, ya da bazı kurumların birleşmesi ve ayrılması gibi durumlar— söz konusu değişiklikler kurumların organizasyonel yapısında ve belge yönetim süreçlerinde doğrudan dönüşümlere neden olmaktadır.
- Nitekim 2018 yılında Cumhurbaşkanlığı Hükümet Sistemi'ne geçişle birlikte Devlet Personel Başkanlığı, Kalkınma Bakanlığı ve Bütçe ve Mali Kontrol Genel Müdürlüğü gibi kurumların kapatılarak işlevlerinin farklı kurumlara devredilmesi, bu tür yapısal değişimlerin somut örnekleri arasında yer almaktadır

- 
- Bu tür deęişiklikler her ne kadar merkezi otorite tarafından alınan kararlarla şekillenmiş olsa da, sonuçları itibarıyla kurumların içsel süreçlerini ve organizasyonel bütünlüğünü derinlemesine etkilemektedir (Albayrak, 2020, s. 1519). Ayrıca, kamu kurumlarında stratejik yönetim uygulamalarının yaygınlaşmasıyla birlikte, organizasyonel deęişimlerin risk yönetimi süreçleri içerisinde sistematik biçimde ele alınması gerektięi çeşitli çalışmalarda vurgulanmaktadır. Kurumların stratejik planlama ve performans yönetimi süreçlerinde, organizasyonel deęişimlerin etkilerini dikkate alarak risklerin tanımlanması, deęerlendirilmesi ve yönetimine yönelik yapıların oluşturulması gereklilięi ortaya konulmaktadır (Ermişket, 2011, s. 59).
 - Bu çerçevede, yalnızca kurum yönetiminin inisiyatifiyle gerçekleştirilen deęişiklikler deęil, aynı zamanda dışsal faktörlerin etkisiyle meydana gelen yapısal dönüşümler de kurumun iç işleyişine olan etkileri açısından deęerlendirilmiş ve bu kapsamda organizasyonel deęişimler **iç faktörler** kategorisinde ele alınmıştır. Bu yaklaşım, organizasyonel deęişimlerin doğurduğu risklerin daha bütüncül bir yaklaşımla yönetilmesine katkı sağlamayı amaçlamaktadır.

Aşağıdaki tabloda, organizasyonel değişimlerin EBYS ve süreçlerine etkileri doğrultusunda tespit edilen başlıca risk alanları yer almaktadır. Bu riskler, hem operasyonel hem de yönetsel düzeyde çeşitli sorunlara yol açabilecek potansiyele sahiptir. Belge bütünlüğünün korunamaması, veri erişiminin kesintiye uğraması, iş yükünün artması gibi başlıklar, kurumların yeniden yapılanma süreçlerinde karşılaşılabileceği temel kırılganlık alanlarını göstermektedir.

RİSKLER	
Erişim	Adaptasyon
İş Yüğü	EBYS'nin Hantallık ve Uyum Sorunları
Veri Kaybı	Ortak Sistemlerin Kullanılmaması
Yönetsel Karmaşıklık	Prestij Kaybı
Firma Değişikliği	Veri Güvenliği
İş Sürecinin Aksaması	Veri Uyuşmazlığı
Belge Bütünlüğünün Bozulması	Yasal Yükümlülüğün Sağlanamaması
DETSİS Kodlarının Güncellenmemesi	Uzun Süreli Sorunlar

- 
- Kurumsal yapılanmalarda yaşanan birleşme, ayrılma veya yeniden yapılanma süreçleri, bilgi ve belge yönetimi açısından çeşitli belirsizlikler doğurmakta; bu durum özellikle **veri ve belge kaybı riski** açısından önemli bir sorun alanı olarak değerlendirilmektedir.
 - Birleşme durumlarında belgelerin ortak bir sistem altında toplanması nispeten daha az sorun yaratmakta iken, kurumun iki ayrı birime bölünmesi ya da bir birimin başka bir kuruma devredilmesi gibi durumlarda **belge ve veri sahipliğinin muğlaklaşması** ciddi sorunlara yol açabilmektedir. Bu tür yeniden yapılanmalarda belgelerin hangi kuruma veya birime ait olduğunun açık şekilde belirlenmemesi, belgelerin yanlış sınıflandırılması ya da hatalı şekilde taşınması riskini artırmaktadır.
 - Özellikle üst düzey kurumsal dönüşümlerin (örneğin bakanlık düzeyindeki yeniden yapılanmaların) sık yaşandığı durumlarda, bilgi yönetim süreçlerinin bu yapısal değişimlere uyum sağlamada yetersiz kalabildiği; dolayısıyla belgelerin kaybolması, yetkisiz erişime açılması ya da yanlış yerde konumlandırılması gibi sonuçlar doğurabileceği belirtilmektedir.

2. İç Faktörlere Bağlı Riskler

2.2. İnsan Kaynakları, Yetkinlikler ve Finansman

EBYS sürdürülebilirliği ve kurumsal işleyişe entegrasyonu, çok boyutlu insan ve kaynak yönetimini gerektirmektedir. Sistemsel başarının sağlanmasında personelin yetkinliği, yönetim desteği, kurumsal farkındalık, finansal kaynakların sürekliliği ve açık politika-prosedür yapısı kritik rol oynamaktadır. Bu unsurlardaki zayıflıklar, EBYS'nin yalnızca teknik değil, aynı zamanda organizasyonel ve stratejik düzeyde de aksamasına neden olabilmektedir. Bu başlık altında, insan kaynağı niteliği, eğitim süreçleri, yönetsel sahiplenme ve mali planlamaya ilişkin riskler bir bütün olarak ele alınmaktadır.





EBYS'nin Kurum Kültüründeki Yeri

- EBYS'nin kurumsal kültür içerisinde yeterince yer edinmemesi, sistemin yalnızca teknik bir araç olarak algılanmasına ve kurumsal işleyişten izole edilmesine yol açmaktadır.
- EBYS'nin bilgi yönetimi, hesap verebilirlik ve kurumsal hafıza açısından stratejik bir araç olduğu bilinci oluşmadığında, yanlış uygulamalar artmakta, kurumsal bütünlük zarar görmektedir.



- Elektronik belgelere kurum kültüründe verilen önem ile kâğıt odaklı bir kültürden dijital bir kültüre geçişin riskleri:

RİSKLER	
E-Belgenin Çıktısının Alınması	EBYS Ekibinin Sorun Çözme Yetisi
Yeniliklere/Değişikliklere Direnç	Yöneticinin Tutumu
EBYS'ye Ait Birimin Olmaması	Adaptasyon
Jenerasyon Farkı	Islak İmzalı Belge Üretiminin Devam Etmesi
Teknik Bilgi Yetersizliği	



Yönetim Desteği

- Yönetim kademesinin EBYS'ye yönelik açık desteği, sistemin kurumsal önceliklere entegre edilmesi ve tüm birimlerce benimsenmesi açısından belirleyicidir.
- Yönetim desteğinin yetersiz olması durumunda, sistemin uygulamaya geçirilmesinde direnç artmakta, bütçe ve kaynak tahsisi zayıflamakta, stratejik hedeflerle bütünleşme sağlanamamaktadır. Bu durum, sistemin sürdürülebilirliğini doğrudan tehdit etmektedir.

- EBYS, kurum genelinde etkin ve sürdürülebilir bir şekilde uygulanabilmesi, üst yönetimin sürece olan yaklaşımı ve desteğiyle doğrudan ilişkilidir. Yönetim desteği yalnızca karar alma süreçlerini değil, aynı zamanda kurum genelindeki işleyişi, personel tutumunu ve sistemin stratejik düzeyde benimsenmesini de etkilemektedir. Bu bağlamda, katılımcı görüşlerine dayalı olarak yönetim desteğinin yetersizliğinin açabileceği riskler:

Sistemin Geliştirilmesi/Sürdürülebilirliği	Yazışmaların Yanlış Yapılması
Desteğin Diğer Birimlere/Personele Yansıması	Belge Bütünlüğü
Kurum Hizmetlerine Etkisi	Dijital Çöplük
Politika Geliştirme	Erişim
Sistemin Yanlış İşletilmesi	Geçerlilik
Standart Olmayan Evrak Akışı	Güvenilirlik
Kurumsallaşamama	Hedeflere Ulaşma
Kurum İmajı	Yöneticilerin Eğitim Eksikliği



Personel

- EBYS'nin etkin ve sürdürülebilir bir şekilde işlemesi, sistemle doğrudan etkileşimde bulunan personelin bilgi, beceri ve farkındalık düzeyine doğrudan bağlıdır. Belge yönetimi süreçlerine yeterince hâkim olmayan, teknik altyapıya uyum sağlayamayan veya dijital dönüşüme direnç gösteren personel; sistem hatalarına, süreçlerin verimsizliğine ve bilgi güvenliği açıklarına neden olabilmektedir.
- EBYS, yalnızca belirli birimlerde değil, kurumun tüm birimlerinde ve farklı düzeylerde görev yapan personel tarafından aktif olarak kullanılan bir yapıya sahiptir. Bu durum, sistemin başarısını kurumsal ölçekte etkileyen temel faktörün insan kaynağı olduğunu göstermektedir. Personelin sistemi doğru, tutarlı ve standartlara uygun şekilde kullanabilmesi, belge yönetimi süreçlerinin sağlıklı yürütülmesini ve sistemin kurumsal işleyişe entegre edilmesini mümkün kılmaktadır.
- Ayrıca, kamu kurumlarında yaygın olarak gözlemlenen yüksek personel devri, bilgi birikiminin kurumsallaşamamasına, deneyim aktarımının kesintiye uğramasına ve operasyonel risklerin artmasına neden olmaktadır.



Eğitim/Denetim

- Sistemsel yeterlilik kadar önemli olan bir diğer unsur, kullanıcıların EBYS'yi doğru ve standartlara uygun şekilde kullanabilmelerini sağlayacak **sürekli ve kapsamlı eğitim programlarının** varlığıdır. Eğitimin yetersiz olması, sistemin yanlış kullanılmasına, işlemlerin eksik veya hatalı yürütülmesine neden olabilmektedir.



- EBYS etkin bir şekilde kullanılabilmesi, yalnızca teknik altyapıya değil, aynı zamanda kullanıcıların bilgi ve yetkinliğine de bağlıdır. Bu kapsamda personelin sistemle ilgili bilgi düzeyi, verilen eğitimlerin niteliği ve kurum içindeki personel hareketliliği gibi faktörler önemli risk alanları oluşturmaktadır.
- Eğitim faaliyetleri, bilgi ve belge yönetimi sistemlerinin etkin kullanılmasında temel bir unsur olarak görülmekle birlikte, **eğitimin tek başına yeterli olmadığı**, buna eşlik eden denetim ve yaptırım mekanizmalarının eksikliğinin sürecin başarısını ciddi biçimde zayıflattığı katılımcılar tarafından özellikle vurgulanmaktadır.
- Eğitim sonrasında edinilen bilgilerin kurumsal uygulamalara yansıtılmasında **sürekli denetim** yapılmadığı takdirde, personelin hatalı uygulamalara devam ettiği ve farkındalığın istenilen düzeye ulaşmadığı ifade edilmektedir. Özellikle birim yöneticilerinin belge kontrol süreçlerinde yalnızca içerik doğruluğuna odaklanmaları, ancak **dosya planı kodlamasına hiç bakmadıkları** vurgulanmaktadır.

Katılımcı Yorumları:

Maalesef yöneticilerin ne burada ne de diğer kurumlarda bu noktada en ufak bir inisiyatif almadıkları gibi almaya niyetleri de yok. Şunu diyorlar: Biz dosya kodlarını mı öğreneceğiz ya?

Öğrenme, senin biriminde kullandığın zaten 5-10 tane dosya kodu var; 1500 kod olabilir ama senin birimini ilgilendiren 5 tane kod var. O 5 tane kodu da öğreniver ve o 2 tane yazıyı ben hâlâ iddia ediyorum 2 tane yazıyı sırf dosya plan kodu yanlış verilmiş diye gönder; o çalışan bir daha o hatayı yapmaz kesinlikle. Yani farkındalık olması lazım ve sürekli denetim olması lazım.

Burada en zayıf halka insan, dolayısıyla EBYS'yi hatta diğer bilgi sistemlerini kullanan insanlar. Dolayısıyla insanlardaki farkındalığın artması gerekmektedir. İnsana dayalı güvenlik zafiyetlerini azaltmak için çok sık eğitim verilmeli; yani bu işlemi yapan insanlara eğitim verilmeli. Ayrıca birimler denetlenmeli. Yani yerinde nasıl işlem yapıyorlar, ne tür sorunları var, yaptıkları hatalar varsa bunları süre verilerek düzeltmeleri istenmeli. Denetim olmazsa insanlar yanlış yapmaya devam eder.

Politika ve Prosedürler

- Belge yönetimi süreçlerinin kurum genelinde tutarlılık içinde yürütülebilmesi için açıkça tanımlanmış politika, prosedür ve yönergelerin varlığı gerekmektedir.
- Bu tür düzenlemelerin bulunmaması ya da güncel olmaması, belge üretimi, dosyalama, saklama ve erişim işlemlerinde standardın bozulmasına, uygulamada keyfiliğe ve kurumsal uyumsuzluğa yol açabilmektedir. Ayrıca, denetim süreçlerinde açıklık ve hesap verebilirlik sağlanamamasına neden olabilmektedir. Oluşabilecek riskler:

Yetki ve Sorumluluk Belirsizliği	Sürdürülebilir Hizmet
Belge Erişimi	Yanlış Uygulamalar
Elektronik ve Fiziksel Arşivleme Entegrasyonu	Bilgi Eksikliği
İş Etkinliği	Donanım ve Sistem Değişiklikleri
Personel Hataları	Kurumlararası Belge Entegrasyonu
Standart Olmayan Evrak Akışı	Firma Bağımlılığı (N=1)
Kurumsallaşamama	Teknolojik İlerleme



Finansal Kaynaklar

- EBYS'nin kurulumu ve sürdürülebilirliği, güçlü bir finansal planlama ve kaynak tahsisi gerektirmektedir. Yetersiz bütçe, teknik altyapının güncellenememesi, lisans yenilemeleri, kullanıcı eğitimi, bakım ve destek hizmetleri gibi temel ihtiyaçların karşılanamamasına neden olabilmektedir.. Bu durum, sistemin zamanla işlevsiz hale gelmesine ve kurumsal bilgi yönetimi süreçlerinin aksamasına yol açabilmektedir. Finansal süreklilik, dijital arşivleme stratejilerinin de başarısı açısından belirleyici bir faktördür.

3. Elektronik Belge Yönetim Sistemine Bağlı Riskler

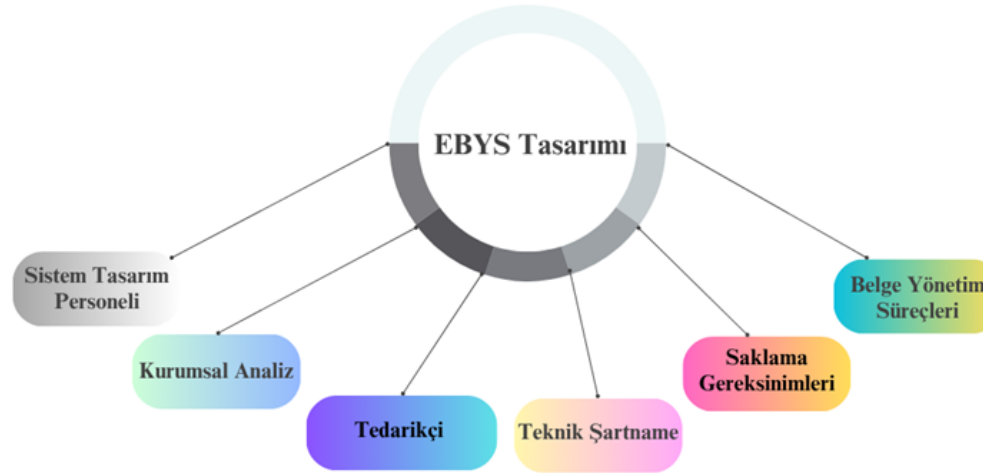
- Bilgi toplumu ve e-devlet stratejilerinin bir yansıması olarak Türkiye'deki birçok kamu kurumu, çeşitli yazılımlar kullanarak elektronik belge yönetimine (EBYS) geçiş yapmıştır. Ne var ki, bu EBYS projelerinin bazıları, teknik altyapı sorunları başta olmak üzere, yazılım geliştirme süreci boyunca karşılaşılan çeşitli risk faktörleri yüzünden öngörülen başarıya ulaşamamaktadır.
- Elzamly (vd. 2016) tarafından yapılan bir araştırmaya göre, bu risk faktörlerinin sayısı 50'yi aşmaktadır. Bu durum, EBYS projelerinin başarısız olmasının yanı sıra kurumların dijital dönüşüm süreçlerinde gecikmelere ve maliyet artışlarına neden olabilmektedir (Çiçek, 2020, 381).



3. Elektronik Belge Yönetim Sistemine Bağlı Riskler

3.1. EBYS Tasarımı

EBYS başarısı, sistemin kurumsal ihtiyaçlara uygun, bütüncül ve sürdürülebilir bir şekilde tasarlanmasına bağlıdır. Tasarım sürecinde yapılan hatalar; teknik yetersizlikler, mevzuata uyumsuzluk, kullanıcı beklentilerinin karşılanamaması ve sistemin zamanla işlevsiz hale gelmesi gibi riskleri beraberinde getirmektedir. Bu nedenle, tasarım aşamasında personel yetkinliği, kurumsal analiz süreçleri, tedarikçi seçimi, teknik şartname hazırlığı ve belge yönetimi gereksinimlerinin dikkatle ele alınması gerekmektedir.





Sistem Tasarım Personeli:

- EBYS'nin etkili bir şekilde yapılandırılabilmesi için tasarım sürecinde görev alan personelin hem teknik hem de belge yönetimi konularında yetkin olması gerekmektedir. Uzmanlık eksiklikleri, sistemin işlevsel yetersizliklerine, kullanıcı ihtiyaçlarını karşılamayan modüllerin geliştirilmesine ve sürdürülebilir olmayan bir yapının ortaya çıkmasına neden olabilir.

Kurumsal Analiz:

- Kurumsal analiz sürecinin eksik veya hatalı yürütülmesi, EBYS'nin kurumun iş akışlarına, belge türlerine ve yasal yükümlülüklerine uygun şekilde tasarlanmamasına yol açabilir. Bu durum, belge yönetimi süreçlerinin uygulanmasını engelleyerek mevzuata uyumsuz, işlevsiz ve sürdürülemez bir sistemin ortaya çıkmasına neden olur.



Katılımcı Yorumları:

- *“Sistemi yapılandırmada modellemenin çok iyi yapılması modüllerin yerinde ve gerektiği şekilde tasarlanması çok önemlidir. Hazır paket EBYS uygulama yazılımlarının temininde sistem yeni uygulanacağı kuruma göre yeniden tasarlanıp yapılandırılmalı. Kurum kültürü, organizasyonel yapı, yetkiler, fonksiyon ve iş süreçleri o örgütün kurum kültürü, iş yapma stratejisi ve iş modeline göre tekrar gözden geçirilmeli. Bu süreç satın alma sözleşmesinde çok akılcıca tasarlanıp yazılmalı. Aksi halde satın alınan ama uygulanamayan bir programla yüz yüze kalma riski hep olacaktır.*
- *“Birçok yazılım firması vardı, kimi yürütemedi iflas etti, kimi çok az kurumla iş yapıyor, kimisi de el değiştirdi. Bunlar kurumlar için çok büyük risk. Kurumun kullandığı firmanın değişmesi, belgelerin sürdürülebilirliğini, kullanıcı erişim yetkilerinin yeniden tasarlanmasını gibi birçok riski beraberinde getirir.*



Tedarikçi Seçimi:

- EBYS'nin geliştirme ve entegrasyon sürecinde görev alacak tedarikçinin yalnızca teknik yeterliliği değil, aynı zamanda belge yönetimi alanındaki uzmanlığı, kurumsal süreçlerle uyumu ve güvenilirliği de dikkate alınmalıdır. Belge yönetimi konusunda deneyimsiz firmalar, sistemi yalnızca teknik bir yazılım aracı olarak kurgulayabilir ve yönetsel işlevleri göz ardı edebilir.
- Ayrıca, tedarikçinin kurumsal süreklilik sağlamaması, yani firmanın el değiştirmesi, iş bırakması ya da destek hizmetlerini kesintiye uğratması gibi durumlar, sistemin bakım, güncelleme ve sürdürülebilirliğini ciddi biçimde riske atabilir. Bu nedenle tedarikçi ile yapılacak sözleşmelerin uzun vadeli iş birliğini güvence altına alacak şekilde yapılandırılması büyük önem taşımaktadır.



- Katılımcılar, hizmet alan kurumlarda EBYS konusunda yetkin personel eksikliğinin, sistemin kurulum ve işletim süreçlerini büyük ölçüde tedarikçi firmanın inisiyatifine bıraktığını ifade etmektedir. Bu durumun, firmanın sistemi teknik gereklilikler ve standartlardan ziyade kendi önceliklerine göre şekillendirmesine yol açarak kurumun ihtiyaçlarını karşılamayan işlevsellikte planların sisteme entegre edilmesine ve çok yönlü risklerin ortaya çıkmasına neden olmaktadır.
- Diğer yandan katılımcı bu riski daha doğrudan bir şekilde şu sözlerle ifade etmektedir:

“Birçok yazılım firması vardı, kimi yürütemedi iflas etti, kimi çok az kurumla iş yapıyor, kimisi de el değiştirdi. Bunlar kurumlar için çok büyük risk. Kurumun kullandığı firmanın değişmesi, belgelerin sürdürülebilirliğini, kullanıcı erişim yetkilerinin yeniden tasarlanmasını gibi birçok riski beraberinde getirir.”



Teknik Şartname:

- Teknik şartnamelerin, kurumun özgün ihtiyaç analizine dayalı olarak ve ulusal/uluslararası belge yönetimi standartlarıyla uyumlu şekilde hazırlanması, EBYS'nin işlevsel, sürdürülebilir ve kurumsal yapıya entegre biçimde tasarlanabilmesi açısından kritik öneme sahiptir.
- Yetersiz, yüzeysel veya hatalı hazırlanan şartnameler; sistemin işlevselliğinde eksikliklere, farklı sistemlerle entegrasyon zorluklarına ve mevzuata uyumsuzluklara neden olabilir.
- Ayrıca, detaylı tanımlamalar ve açık teknik kriterler içermeyen şartnameler, tek bir firmaya bağımlı bir yapı oluşmasına yol açabilir. Bu durum, sistemin bakım, güncelleme, destek ve geliştirme süreçlerinde alternatif üretilmemesi, maliyetlerin artması ve teknolojik esnekliğin kaybedilmesi gibi riskleri beraberinde getirmektedir. Bu nedenle teknik şartnameler, hem fonksiyonel hem de stratejik gereksinimleri kapsayacak biçimde dikkatle hazırlanmalıdır.



Saklama Gereksinimleri:

- EBYS'nin tasarım sürecinde belge türlerinin saklama sürelerinin ve saklama planlarının dikkate alınmaması, hem yasal yükümlülüklerin yerine getirilmesini engelleyebilir hem de bilgi güvenliği, veri yığılması ve ayıklama süreçlerinde ciddi sorunlar doğurabilir. Saklama gereksinimleri göz ardı edilen sistemler, arşiv devri aşamasında uyumsuzluk riski taşır.

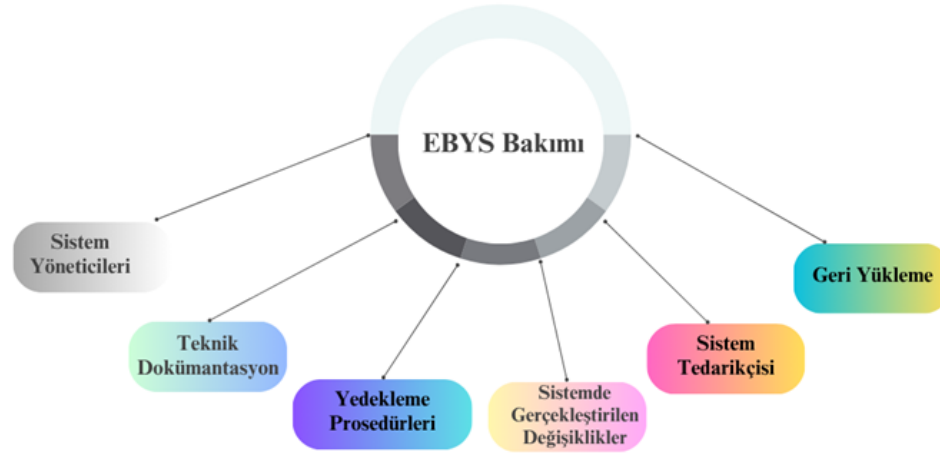
Belge Yönetim Süreçleri:

- EBYS'nin, belge üretiminden tasfiyeye kadar tüm belge yaşam döngüsünü kapsayacak şekilde yapılandırılmaması, sistemin sadece depolama amaçlı kullanılmasına neden olabilir. Belge yönetim süreçlerinin sistem içinde tanımlı olmaması, işlem bütünlüğünü ve kurumsal hafızayı zedelerken, denetlenebilirliği de ortadan kaldırmaktadır.

3. Elektronik Belge Yönetim Sistemine Bağlı Riskler

3.2. EBYS Bakımı

Elektronik Belge Yönetim Sistemlerinin (EBYS) uzun vadeli işlevselliği, yalnızca sistemin ilk kurulum aşamasına değil; aynı zamanda düzenli ve profesyonel şekilde yürütülen **bakım süreçlerine** de bağlıdır. EBYS'nin sürdürülebilirliği açısından bakım faaliyetleri stratejik öneme sahiptir ve bu süreçte meydana gelen aksaklıklar sistem güvenliği, belge bütünlüğü ve hizmet sürekliliği üzerinde ciddi riskler oluşturabilmektedir.





Sistem Yöneticileri

- Sistem yöneticilerinin yetkinliği ve sürekliliği, EBYS'nin güvenli ve kesintisiz çalışması açısından kritik bir faktördür. Yetersiz eğitim almış ya da sistemin tüm bileşenlerine hâkim olmayan yöneticiler, hatalı yapılandırmalar, veri kayıpları veya güvenlik açıklarına neden olabilir. Personel devri, bilgi birikiminin kurum dışına çıkmasına ve sistem sürekliliğinin sekteye uğramasına yol açabilir.

Teknik Dokümantasyon

- Güncel ve erişilebilir teknik dokümantasyonun bulunmaması, özellikle sistemde görev alan yeni personelin süreçlere uyumunu zorlaştırmakta, bakım ve müdahale süreçlerinde gecikmelere yol açmaktadır. Dokümantasyon eksiklikleri, aynı zamanda denetim süreçlerinde belge izlenebilirliğini ve sistemin hesap verebilirliğini de zayıflatmaktadır.



Yedekleme Prosedürleri

- Veri kaybını önlemeye yönelik yedekleme politikalarının olmaması ya da düzenli olarak uygulanmaması, sistem arızası, siber saldırı veya kullanıcı hatası durumlarında **geri döndürülemez bilgi kayıplarına** neden olabilir. Yedekleme frekansının düşük olması ya da yedeklerin güvenli olmayan ortamlarda tutulması da bu riski artırmaktadır.

Sistemde Gerçekleştirilen Değişiklikler

- EBYS üzerinde yapılan güncellemeler, modül eklemeleri veya yapılandırma değişiklikleri, yeterli test sürecinden geçirilmeden uygulanırsa; sistemin mevcut işleyişini bozabilir, verilerin bütünlüğünü tehlikeye atabilir ve sistemler arası uyumsuzluklara yol açabilir. Ayrıca bu tür değişikliklerin izlenebilir olmaması, sorunların kaynağının tespitini güçleştirir.



Sistem Tedarikçisi

- Tedarikçi firmanın kurumsal sürekliliği, teknik destek sağlama kapasitesi ve belge yönetimi konusundaki uzmanlığı, bakım sürecinin başarısını doğrudan etkiler. Tedarikçinin el değiştirmesi, hizmeti sonlandırması ya da teknik desteği aksatması durumunda kurum, kritik sistem bileşenlerinde müdahale edemez hâle gelebilir. Bu da **firma bağımlılığı kaynaklı yapısal riskleri** gündeme getirir.

Geri Yükleme (Recovery) Süreçleri

- Olası veri kaybı ya da sistem çökmesi durumunda kullanılacak geri yükleme mekanizmalarının önceden test edilmemesi, sistemin eski hâline döndürülmesini geciktirebilir veya imkânsız hâle getirebilir. Bu süreçlerin kurumsal olarak tanımlanmamış ve dokümante edilmemiş olması, kriz anlarında büyük bilgi kayıplarına ve hizmet kesintilerine neden olabilir.

3. Elektronik Belge Yönetim Sistemine Bağlı Riskler

3.3. Güvenlik

EBYS, kurumsal bilginin dijital ortamda saklandığı, erişildiği ve yönetildiği sistemler olduğundan, **güvenlik** bu sistemlerin en kritik bileşenlerinden birini oluşturmaktadır. Güvenlik zafiyetleri, sadece belge kaybına değil, aynı zamanda kurumun yasal ve itibarî sorumluluğuna da doğrudan etki edebilecek riskler barındırır.





Güvenlik Politikaları

- Kurumsal düzeyde tanımlı, yazılı ve güncel güvenlik politikalarının bulunmaması, belge güvenliğini kurumsal yaklaşımdan ziyade bireysel inisiyatiflere bırakır. Bu durum, standart dışı uygulamalara, farkında olmadan gerçekleştirilen ihlallere ve olaylara müdahalede yetersizliklere neden olabilir.

Bilgi Güvenliği Standartları

- ISO/IEC 27001 gibi uluslararası bilgi güvenliği standartlarına uyum sağlanmaması, EBYS'nin güvenlik altyapısında zafiyetler doğurabilir. Şifreleme, kimlik doğrulama, erişim kayıtlarının izlenmesi gibi kontrollerin eksikliği, sistemin dış tehditlere ve iç suistimallere açık hale gelmesine neden olur.



Yedekleme

- Düzenli, otomatik ve güvenli yedekleme süreçlerinin olmaması; sistem arızası, siber saldırı ya da kullanıcı hatası durumlarında **geri döndürülemez belge kayıplarına** yol açabilir. Ayrıca, yedeklerin bütünlüğünün doğrulanmaması veya erişimin güvence altına alınmaması, yedekleme sisteminin kendisini bir zafiyet kaynağı haline getirebilir.

Bakım

- EBYS'nin güvenlik açıklarını giderecek bakım faaliyetlerinin düzenli olarak yapılmaması, güncellenmeyen sistemlerin saldırılara açık hale gelmesine neden olabilir. Kritik sistem bileşenlerinde yaşanan gecikmiş müdahaleler, veri kaybı veya hizmet kesintisi ile sonuçlanabilir.

Depolama

- Belgelerin şifrelenmemiş biçimde saklanması, güvenliği tehdit eden temel sorunlardan biridir. Ayrıca, belgelerin güvenli olmayan fiziksel ya da dijital ortamlarda tutulması, hem dış müdahaleye açık hale gelmesine hem de uzun vadeli bütünlüğünün bozulmasına neden olabilir.



Eriřim

- Yetkisiz erişimlerin engellenmesi kadar, yetkili erişimlerin **izlenebilir ve sınırlı** olması da kritik öneme sahiptir. Erişim kontrol mekanizmalarının yetersiz olması, belge içeriklerinin kötüye kullanılmasına, sızdırılmasına veya manipüle edilmesine zemin hazırlayabilir.

Yetkilendirme

- Kullanıcılara verilen yetkilerin açık, sınırlı ve iş tanımlarına uygun biçimde tanımlanmaması, bilgi güvenliği ihlallerine davetiye çıkarabilir. Fazla yetkilendirme veya atıl kullanıcı hesapları, özellikle iç tehditler açısından ciddi güvenlik riskleri oluşturur.



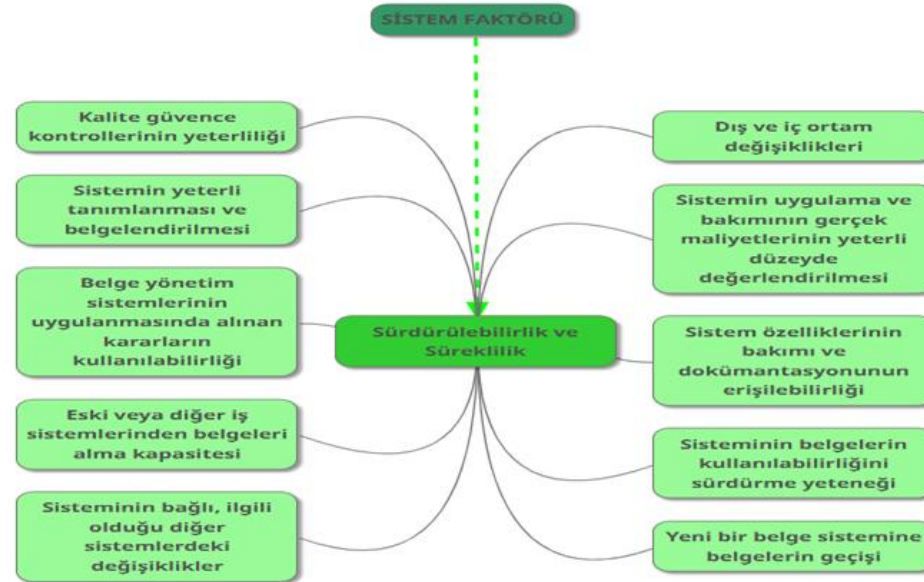
Bakım ve Güvenlik Riskleri/Katılımcı Görüşleri

Veri Güvenliği	E-imzanın Paylaşılması
Yedekleme ve Geri Yükleme Riskleri	Hizmet Aksaması
Veri Kaybı	Veri Kaybı
Hizmet Kesintisi	İmzalama Süreci
Fiziksel Cihazların Deforme Olması	Firma Bağımlılığı
Alt Yapı	Maliyet
Güven Kaybı	Firma Değişikliği
Teknik Şartname	Bakım Süreçlerinin Dokümantasyonu
İnsan Faktörü	Firmanın Güvenilirliği
Belge Bütünlüğü	Versiyon Geçişleri

3. Elektronik Belge Yönetim Sistemine Bağlı Riskler

3.4. Sürdürülebilirlik ve Süreklilik

EBYS, yalnızca belgelerin kısa vadeli işlevselliğiyle değil, uzun vadeli erişilebilirlik, kurumsal hafızanın korunması, yasal yükümlülüklerin yerine getirilmesi ve bilgi sistemleriyle entegrasyonun devamlılığı açısından da değerlendirilmektedir. Bu bağlamda sistemin sürdürülebilirliği, kurumsal risk yönetimi stratejileri içinde kritik bir yer tutmaktadır. Aşağıda, EBYS'nin sürdürülebilirlik ve süreklilik bağlamında karşı karşıya kalabileceği temel risk alanları açıklanmaktadır





Kalite Güvence Kontrollerinin Yetersizliği

- EBYS süreçlerinde kalite ve uygunluk kontrollerinin kurumsal bir sistematığa bağlanmamış olması, uzun vadeli sistemsel hataların erken dönemde tespit edilememesiyle sonuçlanabilir. Bu durum, belge bütünlüğünün bozulması, işlem gecikmeleri ve bilgi güvenliği açıklarının ortaya çıkmasına neden olmaktadır.

Sistemin Tanımlanması ve Belgelendirilmesindeki Eksiklikler

- Sistemin teknik yapısının, işlevsel bileşenlerinin ve süreç akışlarının yeterince tanımlanmamış ya da belgelendirilmemiş olması, özellikle personel değişiklikleri ve dış kaynak kullanımında kurumsal bilgi kaybı riski doğurmaktadır. Bu eksiklik, sistemin sürdürülebilir yönetimini zayıflatır.



Belge Yönetim Kararlarının Uygulanabilirliğinde Tutarsızlık

- Kurumsal kararların belge yönetim süreçlerine bütüncül biçimde entegre edilememesi; sistemsal dağınıklığa, süreçlerin şeffaf biçimde izlenememesine ve kurumsal hesap verebilirliğin zedelenmesine neden olmaktadır. Kararların dijital sistemle senkronize olmaması, belge yönetiminin stratejik yönünü etkisiz kılar.

Eski ve Diğer Sistemlerden Veri Aktarımı Riskleri

- Eski sistemlerden belge aktarımında yaşanan teknik ve semantik uyumsuzluklar, belgelerin bağlamından kopmasına, veri kaybına ya da yasal geçerliliğin tartışmalı hale gelmesine yol açabilir. Özellikle bütünsel arşiv yönetiminde bu tür kopukluklar, kurumsal hafızada boşluklar yaratabilir.



Bağlantılı Sistemlerdeki Değişikliklere Karşı Uyumsuzluk

- EBYS'nin entegre çalıştığı kurum içi sistemlerdeki (örneğin insan kaynakları veya finans uygulamaları) güncellemelerin EBYS'ye yansıtılamaması, veri senkronizasyonunun bozulmasına, belge akışının kesintiye uğramasına ve sistemler arası tutarsızlığa neden olur.

İç ve Dış Ortam Değişikliklerine Uyum Yetersizliği

- Hukuki, teknolojik ya da kurumsal ortamdaki değişimlere sistemin yeterince hızlı ve esnek uyum sağlayamaması; belge yönetim süreçlerinin güncelliğini yitirmesine, yasal sorumlulukların ihlal edilmesine ve kurumun dijital dönüşüm sürecinde geri kalmasına neden olabilir.



Sistemin Gerçek Maliyetlerinin Göz Ardı Edilmesi

- EBYS uygulamalarında yalnızca kurulum maliyetlerinin değil, bakım, güncelleme, lisans, entegrasyon, eğitim ve destek hizmetlerine ilişkin tüm maliyetlerin uzun vadeli planlamaya dahil edilmemesi, sistemin sürdürülebilirliği açısından ciddi risk oluşturmaktadır. Yetersiz kaynak planlaması, sistemin zamanla işlevsizleşmesine neden olabilir.

Teknik Özelliklerin Sürdürülmesi ve Dokümantasyonun Erişilebilirliği

- Yazılım güncellemeleri, konfigürasyon değişiklikleri ve kullanıcı yetkilendirmeleri gibi teknik işlemlerin uygun şekilde belgelenmemesi ve bu bilgilere zamanında erişilememesi, sistem bakımının sürdürülebilirliğini zayıflatır. Bu durum, özellikle denetim süreçlerinde bilgi eksikliklerine ve yönetim sorunlarına neden olabilir.



Belgelerin Kullanılabilirliğini Sürdürme Yetersizliği

- Zaman içinde belge formatlarının eskimesi, yazılım ve donanım uyumsuzlukları ya da yedekleme hataları, belgelerin erişilemez hale gelmesine yol açabilir. Bu durum, yalnızca arşiv değerinin kaybına değil, aynı zamanda kurumsal şeffaflık ve denetlenebilirlik açısından da ciddi sorunlara neden olur.

Yeni Sistemlere Geçişte Uyum Riskleri

- EBYS'den başka bir belge sistemine geçiş sırasında yaşanan üstveri uyumsuzluğu, dosya formatı farklılıkları ve yetersiz geçiş planlaması; veri kayıpları, erişim problemleri ve sistemsel kopukluklar doğurabilir. Bu risk, sistemler arası geçişin etkili bir stratejiye dayanmaması halinde büyür ve kurumsal işleyişi sekteye uğratabilir.

Sürdürülebilirlik ve Süreklilik Riskleri/Katılımcı Görüşleri

RİSKLER	
Teknoloji Değişimi	Belge Saklama Formatındaki Belirsizlik
Kurumsal Sorumluluk	Bilgi/Bilinç Eksikliği
E-imza Durumu	Veri Güvenliği
Firma Bağımlılığı	Nitelikli Üst Veri
Yetkin Personel	Eğitim
Maliyet	Firmalar Arası Rekabet
Yetkili Kurumların Sorumluluğu	Firmanın Yetkinliği
	Bütünlüğün Bozulması



Katılımcı Görüşleri:

- Teknolojiye bağlı sürdürülebilirlik riskleri özellikle teknolojik eskime, dijital ortamın kırılganlığı ve uzun vadeli erişilebilirlik gibi alanlarda ortaya çıkmaktadır.

“En önemli risk faktörü burada EBYS lerin dijital ortamda olması aslında. Çünkü dijital ortam biraz daha kırılgan fiziksel ortama göre. Belli yıl sonra EBYS’de PDF’leri görüntüleyebileceğiniz konusunda şüpheler var. Mesela teknoloji eskimesi diye bir tabir vardır. Burada özellikle belgelerin hem PDF görüntüsü hem üst verilerinin hiçbir şekilde bozulmadan saklanmasına dair bir güvenilirlik garantisi şu an yok. Çünkü sürekli yazılımlar değişiyor, güncelleniyor. 20, 30 yıl sonra word ya da pdf diye bir şey kalmayabilir. Bu durumda da özellikle tarihi araştırmacılar ve hukuki anlamda geriye dönük araştırmalar için çok büyük risk. EBYS’lerin bu ilk oluşturulduğu andaki gibi uzun süreli korunmasını sağlanması lazım.

3. Elektronik Belge Yönetim Sistemine Bağlı Riskler

3.5. Birlikte Çalışabilirlik

- 2009/4 Sayılı Başbakanlık Genelgesi'ne göre, kamu bilgi sistemlerinde birlikte çalışabilirliğin sağlanması; kamu hizmetlerinin **etkin, hızlı ve entegre** biçimde sunulabilmesi amacıyla temel bir gereklilik olarak tanımlanmıştır.
- Bu amaca yönelik olarak geliştirilen *Birlikte Çalışabilirlik Esasları Rehberi*, kamu kurumları ile kamuya dijital ortamda hizmet sunan tüm paydaşlar arasında:
 - Teknik,
 - Yönetimsel ve
 - Anlamsal uyum temelinde birlikte çalışabilirliği teşvik eder.
- Rehber, bu kapsamda yetki ve sorumluluklar, yöntem ve ilkeler ile kullanılacak teknik standartları tanımlamakta; veri entegrasyonu, içerik yönetimi, dosya formatları, protokol uyumu ve güvenlik gibi çok boyutlu alanlarda kurumsal uyumu desteklemektedir.

Türkiye’de Birlikte Çalışabilirlik İçin Uyulması Gerekenler

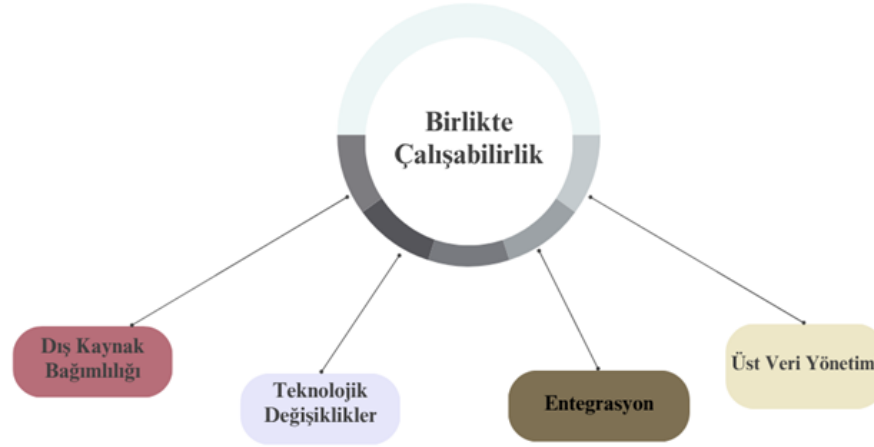
Dosya formatları	PDF/A, .gif, .jpeg
Hipermetin aktarım protokolleri	HTTP 1.1 RFC 2616, RFC 2817, RFC 2818
Kurum kimlik ve haberleşme kodları	DEVLET TEŞKİLATI MERKEZİ KAYIT SİSTEMİ
EBYS standardı	TS 13298
Bilgi güvenliği yönetimi standardı	ISO 27001
Sayısal imza	XML Signature
Elektronik imza formatı	CAdEs, XAdEs, PAdES. CAdES-XLong (Kamu kurumları için)
e-posta taşıma	SMTP / MIME
e-posta taşıma güvenliği	RFC 3207
Veri değişimi	XML
Web servisleri	SOAP RFC 4277 / WSDL v1.1/ UDDI



Türkiye’de EBYS’lerin birlikte çalışabilirliği üzerine genelge ve rehberin yanı sıra;

- TSE 13298 Elektronik Belge ve Arşiv Yönetim Standardı,
- e-Yazışma Teknik Rehberi,
- Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik,
- Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik gibi önemli rehber, standart ve yasal düzenlemeler yapılmaktadır.

Ancak, tüm bu düzenleyici çerçeveye rağmen uygulamada birlikte çalışabilirliğe ilişkin önemli sorunlar yaşanmaktadır. Dişli ve Külçü (2020, s. 38), bu alandaki sorunlara dikkat çekerek, **sistemler arası veri uyumsuzluğu, teknik standartlara yalnızca kısmi uyum, tedarikçi bağımlılığı, entegrasyon eksikliği** gibi birçok problemlerin sürdüğünü ortaya koymaktadır. Birlikte çalışabilirlik, EBYS'nin kurum içi ve kurumlar arası bilgi sistemleriyle entegre, tutarlı ve sürdürülebilir bir yapıda çalışmasını sağlayan temel bir ilkedir. Ancak bu yapının kurulması ve sürdürülmesi, beraberinde çok boyutlu riskleri de getirmektedir.





Dış Kaynak Bağımlılığı

- EBYS yazılımının dış tedarikçiler tarafından geliştirilmesi, güncellenmesi veya entegre edilmesi durumlarında firma bağımlılığı riski doğmaktadır. Özellikle birlikte çalışabilirlik için gereken teknik uyumun sadece tedarikçi kontrolünde olması, kurumun sistem üzerinde sınırlı kontrol sahibi olmasına ve alternatif çözümler geliştirememesine yol açabilir.

Teknolojik Değişiklikler

- Birlikte çalışabilirliği sürdürebilmek için sistemin sürekli olarak güncel teknolojilere adapte olması gerekir. Ancak yazılım, format ve protokol değişikliklerine zamanında yanıt verilememesi, EBYS'nin diğer sistemlerle uyumunu bozabilir. Bu durum, veri kaybı, erişim sorunları ve arşiv süreçlerinde kesinti gibi riskleri beraberinde getirir.



Entegrasyon Sorunları

- EBYS'nin diğer kurumsal sistemlerle (örneğin KEP, e-Yazışma, DETSİS, belge yönetim modülleri) tam entegrasyonunun sağlanamaması, belge akışında kesintilere, iş tekrarlarına ve veri tutarsızlıklarına neden olabilir. Entegrasyon eksikliği, aynı zamanda belgeye dayalı karar alma süreçlerinin yavaşlaması ve hatalı işlem yapılması riskini artırır.

Üst Veri (Metadata) Yönetimi

- Birlikte çalışabilirliğin sağlanabilmesi için belgelerle ilişkili üst verilerin standartlara uygun, eksiksiz ve doğru şekilde yönetilmesi gerekmektedir. Ancak farklı sistemler arasında üst veri tanımlarının uyumsuz olması veya eksik aktarılması, belge bütünlüğünü ve izlenebilirliğini tehlikeye atar. Bu da hem arşivsel geçerliliği hem de hukuki güvenilirliği riske sokar.

4. Elektronik Belge Yönetim Süreçlerindeki Riskler

- 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 üretilmesinden imhasına kadar, oluşturulmasını, saklanmasını, erişilmesini ve geri alınmasını, bakımını, güvenliğini ve imhasını içeren bilgisayar teknolojisi ve sistemleri aracılığıyla yönetilmesini gerektirmektedir.
- 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).



4. Elektronik Belge Yönetim Süreçlerindeki Riskler

4.1. Belgenin Oluşturulması

- Belge yönetim sürecinin ilk adımı olan belge oluşturma, EBYS'nin bütünlüğü, güvenilirliği ve kurumsal işleyişle uyumu açısından kritik bir aşamadır. Bu aşamada yapılan hatalar ya da ihmal edilen adımlar, belgenin yaşam döngüsünün tamamında sorunlara ve belge yönetimi risklerine yol açabilir.





Sorumluluk

- Belgeyi üretmekle yükümlü olan personelin açık şekilde tanımlanmaması veya belge oluşturma sürecinde sorumlulukların netleştirilmemesi, belge üretiminde yetki karmaşası, eksik belge üretimi veya resmiyet kazanmayan belgelerin dolaşıma girmesi gibi riskler doğurabilir. Bu durum, hem belgeye dayalı karar süreçlerini zayıflatır hem de denetlenebilirliği olumsuz etkiler.



Fiziki Belge Üretimi

- Dijital süreçlerin hâkim olduğu bir ortamda fiziki belge üretimine devam edilmesi, belge bütünlüğünün korunmasını zorlaştırır. Belgelerin hem dijital hem fiziksel versiyonlarının oluşturulması durumunda, sürüm kontrolü sağlanamazsa **tutarsızlık**, **karışıklık** ve **güvenlik açıkları** ortaya çıkabilir. Ayrıca fiziki belgelerin arşivlenmesi, erişilmesi ve izlenmesi dijital belgelere kıyasla daha riskli ve maliyetlidir.

Belge Doğruluğu ve Tutarlılığı

- Belge içeriklerinin eksik, hatalı veya güncel olmayan bilgilerle oluşturulması, hem kurumsal karar alma süreçlerini yanlış yönlendirebilir hem de belgeye dayalı işlemlerde hukuki ve yönetsel hatalara yol açabilir. İçerik tutarsızlığı, aynı konuyla ilgili birden fazla ve çelişkili belge üretilmesine sebep olabilir; bu da kurum içi güvenilirliği zedeler.



Üstveri (Metadata)

- Üstveri, belgenin kimliği niteliğindedir. Üstveri bilgilerinin eksik, yanlış veya standart dışı girilmesi; belgenin arandığında bulunamaması, sınıflandırılamaması veya bağlamından kopuk değerlendirilmesi gibi riskler oluşturur. Ayrıca sistemler arası veri alışverişinde **anlamsal uyumsuzluk** ve **belge bağlamının kaybı** gibi sonuçlar doğabilir.

Standart Dosya Planı (SDP)

- Üstverinin önemli bir bileşeni olan Standart Dosya Planı'nın yanlış veya eksik uygulanması, belge sınıflandırmasında tutarsızlık yaratır. Belgelerin yanlış konu altında açılması, belgeler arası ilişkiselliğin bozulmasına ve arşivleme/erişim süreçlerinde hatalara yol açar. Bu durum, kurumun bilgiye hızlı ve doğru erişimini engelleyerek riskleri artırır.



Katılımcı Görüşleri:

- Belge üretim süreci, doğru ve tutarlı verilerin kaydedilmesi açısından kritik bir aşama olup bu sürecin etkin bir şekilde yönetilmesi, sonraki belge saklama, erişim, güvenlik ve yönetim süreçlerinin sağlıklı bir şekilde işlemesini sağlamaktadır. Katılımcılardan elde edilen bulgular, bu süreçte belirli risk unsurlarının ortaya çıkabileceğini göstermektedir. Özellikle, üst veri ve üst veri alanlarından biri olan SDP hataları, önemli risk faktörleri arasında yer almaktadır

- 
- Personelin dosya planı kodlarını kullanmasıyla ilgili katılımcıların görüşleri, bu sürecin potansiyel risklerini ortaya koymaktadır. Katılımcılar, standart dosya planı kodlarının kullanıcılar tarafından doğru bir şekilde kullanılmamasının en büyük risklerden biri olduğunu vurgulamaktadır. Özellikle, evrak ayıklama ve imha süreçlerinde yanlış dosya planı kodu kullanılması durumunda, belgelerin yanlışlıkla imha edilme olasılığının yüksek olduğunu ifade etmektedir. Bu bağlamda, ilk onay akışında birim amirlerinin denetim yapmasının önemli bir önlem olarak önerildiği belirtilmiştir. Amirlerin, evrakların doğru dosya planına ve doğru klasöre yönlendirilip yönlendirilmediğini kontrol etmeleri gerektiği, bu sürecin etkinliğini artıracak bir yaklaşım olarak öne çıkmaktadır.
 - Ayrıca dosya planlarının güncel olmamasını ve örgütün sahada yürüttüğü işlerle ilgili gerçek fonksiyonların planda yer almamasını eleştirmektedir. Bunun yanı sıra, dosya planında mevcut olan kodların doğru kullanılmaması, örneğin "99-Diğer" kodu ile belgelerin geçici olarak işaretlenmesi, ana konu kodlarının kullanılması önemli bir sorun olarak ortaya çıkmaktadır. Bu durum, kodların doğru kullanılmaması ve güncellenmemesi nedeniyle belgelerin doğru şekilde sınıflandırılmaması riskini artırmaktadır.

- 
- “Dosya planı, tanımlama belge üretirken önemli değilmiş gibi gözükse de belgenin erişimini, saklanmasını, imhasını etkileyen bir şey. Bu yüzden çok önemli. Yanlış, eksik olması belgenin yok olmasına kadar gidebilir.”
 - “Şu ana kadar bildiğim kadarıyla hiçbir kurumda elektronik belgeler üzerinde bir ayıklama imha yapılmadı. Elektronik imza kanunu 2005te çıktı, 2025 oldu 20 sene geçti. Saklama planına baktığımız zaman 5 sene 10 sene gibi kavramlar var bu 5 sene 10 sene olanların imha edilmesi lazım hiçbir kurumda ben duymadım bununla ilgili bir çalışma da yok. Çünkü kimse güvenemiyor. Fiziksel belgeye masanın üstünde yayıyorsunuz; bu önemliymiş ya buraya koymuş ama bunu ayırayım diyorsunuz. Yani sistem ne yapacak 060, 5 sene sonra imha bütün 060lar getirecek ama o "kod gerçekten 060 mı değil onun için kimse cesaret etmiyor. ”

4. Elektronik Belge Yönetim Süreçlerindeki Riskler

4.2. Elektronik Belgenin Kullanımı/Paylaşımı

Elektronik belge yönetiminde, oluşturulan belgelerin iç ve dış paydaşlarla paylaşılması süreci; erişim, güvenlik, standartlara uygunluk ve yetkilendirme gibi kritik başlıklarda çeşitli riskleri barındırmaktadır. Bu aşamadaki zafiyetler, belge güvenliğini ve kurumsal iletişimin etkinliğini doğrudan etkiler.





Kurum Kodlarının Kullanılması

- Elektronik yazışmalarda kurum kodlarının yanlış, eksik ya da standart dışı kullanılması; belge yönlendirme hatalarına, yanlış muhataba iletimine ve işlem gecikmelerine yol açabilir. Bu durum, özellikle kurumlar arası iletişimde belge bütünlüğünün ve izlenebilirliğin bozulmasına neden olur.

Kayıtlı Elektronik Posta (KEP)

- KEP sistemi, resmi yazışmalarda güvenli iletim altyapısı sunmakla birlikte, teknik bilgi eksikliği ya da format uyumsuzlukları nedeniyle kullanımı sırasında çeşitli riskler doğabilir. Belgelerin **.eyp formatında gönderilmemesi, belgenin açılmaması** veya **sisteme entegre edilememesi**, belge işleme süreçlerinin sekteye uğramasına ve kurumsal gecikmelere neden olabilir.



Elektronik Yazışma Paketi (EYP)

- EYP'nin yanlış yapılandırılması ya da standartlara uygun kullanılmaması, belge bütünlüğünün bozulmasına ve sistemler arası uyumsuzluğa yol açar. Paketleme hataları, gönderilen belgenin muhatap sistemde açılmamasına ya da içeriğinin eksik görüntülenmesine neden olabilir. Bu durum, yazışmanın geçerliliğini hukuki ve yönetsel açıdan tartışmalı hale getirir.

Güvenlik İhlalleri

- Paylaşım sürecinde belgelerin yetkisiz kişilerle paylaşılması, içeriklerinin sızdırılması ya da erişim kayıtlarının izlenememesi gibi durumlar, ciddi bilgi güvenliği ihlallerine neden olabilir. Özellikle hassas içeriklerin dış ortamlarda izinsiz paylaşılması, kurumun itibarına ve yasal sorumluluğuna zarar verebilir.



Personel Eğitimi

- Personelin elektronik yazışma standartlarına, güvenlik prosedürlerine ve belge paylaşım protokollerine yeterince hâkim olmaması, yanlış işlem yapılmasına, güvenlik açıklarının fark edilmemesine ve belge süreçlerinde hatalara neden olabilir. Bu eksiklik, hem iç hem dış paydaşlarla yürütülen yazışmalarda iletişim kesintilerine ve hata oranlarının artmasına zemin hazırlar.



Katılımcı Görüşleri

Katılımcılar belge gönderme sorunları konusunda, iş akış belirsizliği, mevzuata uygun olmayan durumların yaşandığı ve DETSİS kaynaklı risklerin olduğunu belirtmektedir.

- Katılımcı, kurumlarında aktif bir elektronik yazışma yönetmeliği bulunmaması nedeniyle, yazışma süreçlerinin standardize edilemediğini ve bu belirsizliğin ciddi sorunlara yol açtığını ifade etmektedir. Özellikle, kimlerin vekaletle kime yetki verebileceği, kimlerin vekaletleri onaylayabileceği ve izinlerin kimler tarafından onaylanabileceği gibi temel iş akışlarının netleşmemesi, yazışmaların düzensiz ve standart dışı olmasına neden olmaktadır. Bu belirsizlik, belge gönderme ve dağıtım sürecinde zorluklar yaşanmasına yol açmakta ve evrakların doğru yerlerde işleme alınmaması gibi önemli riskler doğurmaktadır. Ayrıca, arşiv modülünün devreye girmesiyle birlikte, evrakların standart hale getirilmemesi, arşivleme süreçlerinde de sorun yaratmaktadır. Kurum içindeki yazışma düzeninin belirsizliği, başkanlık ve daire başkanlıkları arasındaki yazışmaların nasıl ve hangi düzende yapılacağına dair net bir yol haritasının olmaması, iş akışındaki bu belirsizliğin belge gönderme sürecinde ciddi aksaklıklara yol açtığını göstermektedir.

- 
- Katılımcılar, Resmi Yazışma Usul ve Esasları Hakkındaki Yönetmeliğe uyulmamasının belge yönetim sistemlerinde ciddi güvenlik ve işlem riski doğurduğunu ifade etmektedir. Öne çıkan örneklerde, bazı kamu kurumlarının kendilerini bu yönetmeliğin dışında görmeleri, standart dışı belge gönderimlerine yol açmaktadır. EYP paketine uygun olmayan, gizlilik derecelendirmesi yapılmamış veya doğrulanabilirliği olmayan belgeler, **alıcı kurumlar tarafından işleme alınmamakta**; bu durum hem zaman kaybına hem de hukuki sorumlulukların ihlaline neden olabilmektedir.
 - Verilen somut bir olayda, **bir belediyeden gelen sahte bir yetki belgesi**, doğrulama yapılmadan işleme alınmış ve bu belge ile bir taşınmaz satışı gerçekleştirilmiştir. Belgede yer alan karekodun doğrulama sayfası çalışmadığı halde belge geçerli sayılmış, bu da ciddi bir **mal varlığı güvenliği zafiyetine** yol açmıştır.
 - Benzer şekilde, hak sahipliğiyle ilgili bir kadastro yazısının sahte bir kopyası oluşturularak farklı bir kuruma sunulmasıyla, **yetkisiz işlemler yapılmış**; böylece belge sahteciliği üzerinden kamu zararına neden olunmuştur.
 - Katılımcılar, bu gibi durumların yalnızca eğitim eksikliğinden değil, aynı zamanda yönetsel zaafiyet, denetim yetersizliği ve keyfi uygulamalardan kaynaklandığını belirtmektedir. Fiziksel evrakla baskı kurmaya çalışan kurumlar, KEP gibi yasal yolları devre dışı bırakarak **yönetmelik dışı taleplerle belge güvenliğini riske atmaktadır**.

4. Elektronik Belge Yönetim Süreçlerindeki Riskler

4.3. Kullanılabilirliğin Sürdürülmesi

Elektronik belgelerin yalnızca oluşturulması değil, **zaman içinde bütünlük, erişilebilirlik ve bağlamsal anlamını koruyarak sürdürülebilir şekilde kullanılabilir olması** da belge yönetiminin temel amaçlarından biridir. Bu süreçte yaşanacak herhangi bir aksaklık, belgeye dayalı işlemlerin, denetimlerin ve kurumsal hafızanın zarar görmesine neden olabilir.





Belge Gerçekliği ve Güvenilirliği

- Belgenin orijinallliğini ve doğruluğunu teyit edebilecek teknik ve yönetsel kontrollerin eksikliği, belgelerin **sahte, değiştirilmiş ya da geçersiz hale gelmesi** riskini artırır. Elektronik imza, zaman damgası ya da onay mekanizmalarının yetersizliği, belge güvenilirliğini zedeler ve kurumlar arası anlaşmazlıklara neden olabilir.

Versiyon Yönetimi

- Bir belgenin birden fazla sürümünün oluşturulması durumunda bu sürümlerin doğru şekilde yönetilmemesi, **karışıklığa, eski belgelerin yanlışlıkla kullanılmasına** veya **hatalı kararların verilmesine** neden olabilir. Versiyon kontrol sistemlerinin eksikliği, özellikle belge üzerinde çok sayıda kullanıcı işlem yaptığında belge bütünlüğünü riske sokar.



Eskime Sorunları (Obsolescence)

- Elektronik belgelerin uzun vadeli saklama sürecinde, **veri formatlarının eskiyerek kullanılamaz hale gelmesi**, **yazılım-donanım uyumsuzluğu** gibi teknik nedenlerle belgelerin erişilememesi riski söz konusudur. Bu durum, arşivlerdeki bilgilere ulaşmayı imkânsız hale getirebilir ve bilgi kaybına neden olabilir.

Üst Veri Anlamlılığı

- Üstveri alanlarının yanlış, eksik ya da bağlamından kopuk biçimde girilmesi, belge ile ilişkilendirilmiş bilgilerin **zaman içinde anlamını yitirmesi** riskini doğurur. Bu da belgenin kurum içindeki sınıflandırılması, aranması, bağlamsal olarak yorumlanması ve denetlenmesi süreçlerini olumsuz etkiler.



Şifreleme Yönetimi

- Belgelerin erişim güvenliği açısından şifrlenmesi olumlu bir uygulama olsa da, **şifreleme anahtarlarının güvenli biçimde yönetilmemesi, anahtarların kaybolması** ya da **şifreli belgelerin zamanla açılmaz hale gelmesi**, belgelere erişimi kalıcı olarak engelleyebilir. Bu durum, kritik belgelerin işlevsiz hale gelmesine yol açar.

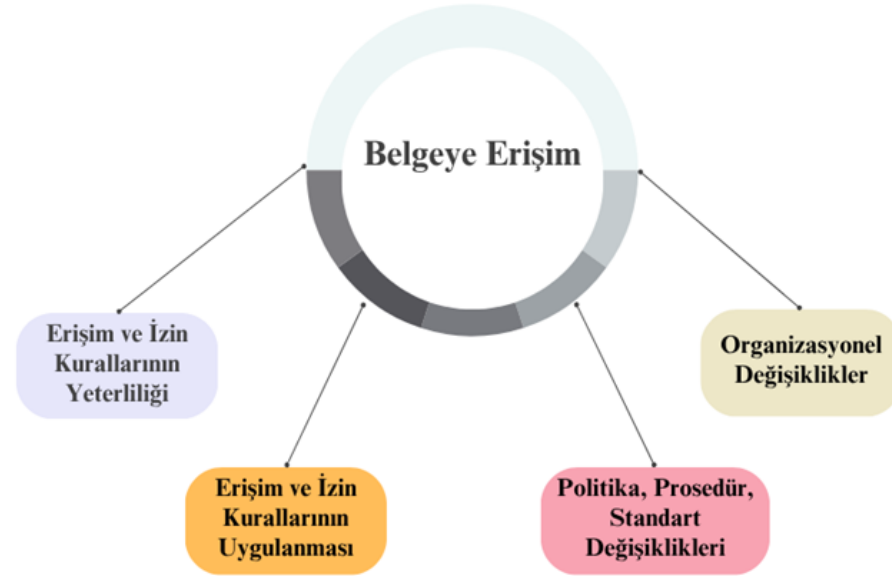
Olay Geçmişi Belgeleri (Audit Trail)

- Belge üzerinde yapılan işlemlerin, kullanıcı müdahalelerinin ve değişikliklerin **izlenebilir olmaması**, belge yaşam döngüsünün kontrol dışı kalmasına neden olur. Olay geçmişi kayıtlarının bulunmaması veya tutarsız olması, denetim süreçlerini etkisizleştirir ve sorumluluk zincirini zayıflatır.

4. Elektronik Belge Yönetim Süreçlerindeki Riskler

4.5. Elektronik Belgeye Erişim

Elektronik belgelerin yalnızca oluşturulması ve saklanması değil, aynı zamanda **yetkili kişiler tarafından doğru zamanda, güvenli şekilde erişilebilmesi** de etkili belge yönetiminin temel unsurlarındandır. Erişim süreçlerindeki zafiyetler, hem bilgi güvenliğini hem de kurumsal verimliliği olumsuz etkileyebilir.





Erişim ve İzin Kurallarının Yeterliliği

- Belgelere kimlerin, hangi düzeyde erişeceğine dair açık tanımlı erişim ve izin kurallarının bulunmaması ya da bu kuralların yetersiz olması; **yetkisiz erişim**, **veri sızıntısı** veya **bilgiye erişim engeli** gibi kritik güvenlik risklerine yol açar. Ayrıca belgeye erişim sınırlamalarının belirsiz olması, kurum içi görev ve sorumlulukların netliğini de zedeler.

Erişim ve İzin Kurallarının Uygulanması

- Mevcut erişim politikalarının EBYS üzerinde etkin şekilde uygulanmaması ya da kullanıcılar tarafından bilinmemesi, sistem üzerinde tanımlı roller ile gerçek uygulama arasında **uyumsuzluklar** doğurabilir. Bu durum, ya belgenin yetkisiz kişiler tarafından görüntülenmesine ya da ihtiyaç duyan personelin belgeye ulaşamamasına neden olabilir.



Politika, Prosedür ve Standart Değişiklikleri

- Erişim politikaları, kurumsal prosedürler ve yasal standartlarda meydana gelen değişikliklerin EBYS sistemine zamanında entegre edilmemesi; **güncel olmayan erişim kısıtlamalarının yürürlükte kalmasına**, bu nedenle sistemin kurumsal yapı ve mevzuatla uyumunu kaybetmesine neden olabilir.

Organizasyonel Değişiklikler

- Birimin taşınması, kapatılması, başka kuruma devredilmesi ya da görev değişiklikleri gibi yapısal dönüşümlerde erişim izinlerinin **yeniden tanımlanmaması** veya güncellenmemesi, belgelerin **yanlış kişilerin erişimine açılması** ya da **ilgili birimlerin belgelerden dışlanması** gibi güvenlik ve süreklilik riskleri doğurabilir.

Katılımcı Görüşleri

- *“Erişilebilirliğin sağlanmasında erişim uçları çok önemli. EBYS’lerde belge temelli arama yapılıyor ama arşivlerde bilgi temelli bir arama var. Yani arşivde belgeyi aramıyoruz ama bilgiyi arıyoruz. O bilgiye ihtiyaç duyuyoruz. Dolayısıyla erişim uçlarının üst verilerin ona göre belirlenmesi gerekiyor. Erişilebilirliği ancak o şekilde sağlayabiliriz. Doğru üst verilerin atanması, üst veriyi yönetiminin doğru yapılması, mevcut üst veriler belki de arşiv için yeterli olmayacak, yeni üst verilerin eklenmesi gibi üst veri yönetimi çok önemli.*
- *“Saklamada şimdilik sıkıntı yok gibi ama erişimde problemler yaşanıyor. İmha hemen hemen hiç yapılmıyor. Özellikle dijital malzeme için imha düşünülmüyor. Oysa arşivlenen her belgenin bir saklama, arşivleme ve tekrar erişim maliyeti var. Bu şimdilik pek göz önünde bulundurulmuyor. Bugün 0,25 cent üretim maliyeti olan bir e-belgenin 100 yıl sonraki erişim ve kullanım maliyeti bugünkü teknolojik değişim ve dönüşüm göz önünde bulundurulduğunda ortalama 94 dolar olarak hesap edilmektedir.”*



- Erişimi etkileyen teknik risklerle ilgili çeşitli endişeler dile getirilmektedir. Belgelerin uzun süreli korunması önemli bir teknik risk olarak öne çıkmakta; belgeler bozulduğunda, erişilebilir olsalar bile delil değerlerini yitirebilecekleri vurgulanmaktadır. Bu durumda, bozulmuş belgelerin herhangi bir mahkemeye sunulamayacağına dikkat çekilmektedir. Ayrıca, belgelerin yeni donanım ve sistemlere aktarımındaki eksikliklerin erişim üzerinde ciddi olumsuz etkiler yaratabileceği belirtilmektedir.

4. Elektronik Belge Yönetim Süreçlerindeki Riskler

4.6. Elektronik Belgenin Saklanması-Arşivlenmesi

Elektronik belge yönetimi sürecinde belgelerin yalnızca oluşturulması ve kullanılması değil, uzun vadeli olarak güvenli biçimde saklanması ve erişilebilirliğinin sürdürülebilmesi kritik önemdedir. Bu süreçte hem kağıt hem de elektronik belgelerin farklı ihtiyaç ve zafiyetleri bulunmakta; arşivleme stratejisinin bu ayrımları gözeterak yapılandırılmaması çok boyutlu riskler doğurmaktadır.





Kağıt ve Elektronik Belgelerin Arşivlenmesi

- Kağıt belgeler, fiziksel koşullara duyarlıdır. Nem, ısı, yangın, haşere ve yanlış dosyalama gibi riskler belgenin bütünlüğünü tehdit eder. Sayısallaştırılmamış belgelerin erişim ve paylaşım süreçlerinde gecikmelere yol açması, arşiv yükünü artırır. Elektronik belgelerde ise donanım eskimesi, veri formatlarının zamanla geçersiz hâle gelmesi (dijital obsolescence) ve üstveri kayıpları gibi teknik riskler ön plana çıkar. Kağıt ve dijital kayıtların paralel tutulması, belge bütünlüğü ve tutarlılık açısından senkronizasyon sorunları doğurabilir.



Dijitalleştirme Sürecine İlişkin Riskler

- **Standart dışı tarama işlemleri**, belgenin okunabilirliğini ve arşivsel değerini azaltır.
- **Eksik ya da hatalı sayısallaştırma**, belge içeriğinin kaybolmasına veya bağlamın bozulmasına neden olabilir.
- **Asıl belge ile dijital kopya arasında tutarsızlık**, yasal geçerliliği tartışmalı hale getirebilir.
- **Üstveri eksiklikleri**, dijital belgenin sınıflandırılamamasına ve bulunamamasına yol açar.
- **Belirsiz sorumluluklar ve süreç yönetimi**, dijital arşivde belge kayıplarına neden olabilir.
- **Gereksiz belgelerin de dijital ortama aktarılması**, sistemin performansını ve arşiv verimliliğini düşürür.
- **Güncel formatlara dönüştürülmeyen taramalar**, uzun vadede erişim sorunlarına yol açar.



Saklama Süresi ve Planlaması

- Kurumun belgeleri ne kadar süre saklayacağına dair net ve standartlara dayalı saklama planlarının olmaması, belgelerin ya gereğinden kısa süre saklanmasına ya da gereksiz şekilde arşiv yükü oluşturmalarına neden olabilir.
- Standart Dosya Planı ile ilişkilendirilmemiş belgeler arşiv sürecinde doğru şekilde konumlandırılmaz, bu da belge kayıplarına veya arşiv içi erişim sorunlarına neden olur.



Dosya Formatları ve Dijital Eskime (Obsolescence)

- Uzun dönemli arşivleme için uygun olmayan formatların (ör. .docx, .jpg) kullanılması, ilerleyen yıllarda belgelerin açılmamasına yol açabilir. PDF/A, XML gibi arşiv dostu formatlara geçişin sağlanmaması, hem içerik kaybı hem de belge geçerliliği açısından risk doğurur.

Depolama Ortamı ve Erişilebilirlik

- Belgelerin bulunduğu fiziksel ya da dijital depolama ortamlarının güvenli, sürdürülebilir ve erişilebilir olmaması, kalıcı veri kaybı riskini artırır.
- Yedekleme sistemlerinin eksikliği ya da geri yükleme testlerinin yapılmaması, felaket senaryolarına karşı hazırlıksızlığa yol açar.



Arşivleme Stratejisi Eksiklikleri

- Kurumsal arşivleme stratejisinin olmaması ya da belirsizliği; görev, yetki ve sorumluluk karmaşasına, standart dışı uygulamalara ve arşiv sistemlerinin sürdürülemezliğine neden olabilir.

Arşivleme Standartlarına Uyum

- TS 13298, ISO 15489 gibi standartlara, Devlet Arşivleri Başkanlığı tarafından belirlenen teknik ve yönetsel kriterlere uyulmaması, belgelerin resmî geçerlilik, hukuki delil niteliği ve denetlenebilirlik açısından sorunlu hale gelmesine neden olur.
- Elektronik belgelerin bütünleşik Arşiv Yönetim Sistemi'ne (AYS) aktarımında teknik uyumsuzluklar, üstveri eksiklikleri ve belge formatı hataları sık karşılaşılan risklerdendir.
- Belgelerin ne zaman arşivleneceği, hangi kriterlere göre ayrılacağı, ne zaman imha edileceği gibi kararların kurumsal düzeyde netleştirilmemesi; hem yasal riskler hem de bilgi güvenliği sorunları yaratır.



Kağıt ve Elektronik Belgelerin Arşivlenmesi

Katılımcı Görüşleri

- Belge ve dosya bütünlüğünün sağlanamaması, EBYS kapsamında önemli bir risk olarak değerlendirilmektedir. Fiziksel ortamda oluşturulan belgelerin, elektronik ortamda üretilen devam belgeleriyle ilişkilendirilmemesi durumunda arşivsel bağlamın kaybolduğu ifade edilmektedir. Sistem ilk kullanılmaya başlandığında fiziksel belgelerin taranarak elektronik ortama aktarılması ve bu belgelerle elektronik belgeler arasında bağlantı kurulması gerekirken, bu ilişkinin çoğu zaman kurulmadığı ve belgeler arasında olması gereken sürekliliğin sağlanamadığı belirtilmektedir.
- Belge ve dosya bütünlüğü sağlanmadığında, eksik ya da kopuk bilgilere ulaşılabileceği ve bunun da veri bütünlüğünü olumsuz etkilediği vurgulanmaktadır. Belge yönetim sürecine sahiplenici bir yaklaşım benimsenmediği sürece kullanıcıların yalnızca EBYS üzerinden yapılan sorgularla yetinip daha geniş belge setlerine ulaşma çabası göstermediği, bunun da önemli bir risk oluşturduğu dile getirilmektedir.



Kağıt ve Elektronik Belgelerin Arşivlenmesi

Katılımcı Görüşleri

- Bütüncül belge ilişkilendirmesinin ve belgeler arası bağın hem arşivsel değer hem de kurumsal bilgi güvenliği açısından kritik önemde olduğu belirtilmektedir. Yaşanan bir örnekte, fiziksel ve dijital ihale dosyaları arasında farklar tespit edildiği; fiziksel dosyalar eksiksizken, dijital dosyaların neredeyse boş olduğu ifade edilmektedir. Bu durumun nedeninin, belgelerin dijital ortama aktarılması için fazladan zaman harcanması gerekliliği olduğu anlaşılmıştır. Ancak dijital belgelerin güvenli saklama açısından avantaj sağladığı, dolayısıyla artık öncelikle dijital dosyaların esas alınması gerektiği konusunda ortak bir görüşe varıldığı belirtilmektedir. Fiziksel ve elektronik belgelerin ayrı yürütüldüğü bir sistemde dosya bütünlüğünden söz edilemeyeceği vurgulanmaktadır.



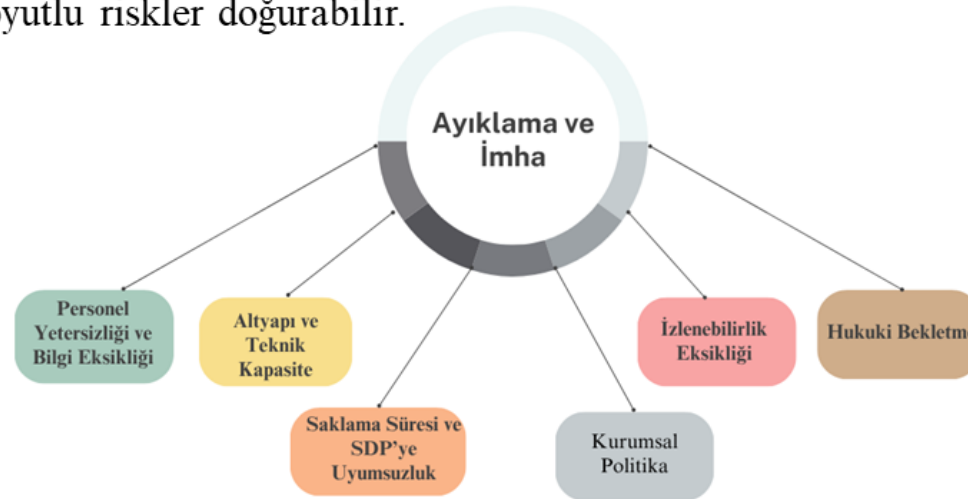
E-Arşiv Modülü -*Katılımcı Görüşleri*

- EBYS kapsamında kurumsal bilgi ve belge yönetiminin sürekliliği, güvenliği ve erişilebilirliği açısından e-arşiv modülünün varlığı kritik bir unsur olarak değerlendirilmektedir. Ancak kurumlar arasında bu modülün kullanımına ilişkin farklılıklar dikkat çekmektedir.
- Bazı kurumlar, arşiv modülüne sahip olmadıklarını ve bu eksikliğin gerekçesini “Prosedürler netleşmediği ve zorunlu olmadığı için şu aşamada bütçe ayırmak istemedik. Her şey netleştğinde almayı planlıyoruz.” şeklinde ifade etmektedir.
- Arşiv modülüne sahip olup etkin şekilde kullanmayan kurumlar ise, prosedürlerin belirsizliğini gerekçe göstererek şunları belirtmektedir: “Modül var ama kullanmıyoruz çünkü arşiv süreçleri net değil. Belgeler şu an bir havuzda toplanıyor, bu da ciddi bir problem. Süreçler netleştğinde belgelerin dosyalanması, klasör yapılarının incelenmesi, arşive aktarılacak belgelerin belirlenmesi gibi yoğun bir iş yükü oluşacak.”
- Öte yandan, arşiv modülünü aktif olarak kullanan kurumlar, bu sistemin kullanılmaması durumunda belgelerin kontrolsüz biçimde bir havuzda birikeceğini ve bunun erişim zorluklarına, iş akışında aksamaya, hukuki risklere, sistem performansında yavaşlamaya ve belge yönetiminde karmaşaya yol açabileceğini vurgulamaktadır. Ayrıca farklı belge türlerinin yönetiminin güçleşeceği ve iş yükünün artacağı da belirtilmektedir.

4. Elektronik Belge Yönetim Süreçlerindeki Riskler

4.7. Elektronik Belgelerde Ayıklama ve İmha

Elektronik belgelerin yaşam döngüsü yalnızca oluşturulma, kullanım ve saklama süreçlerinden ibaret değildir; sürecin doğal bir uzantısı olarak belgelerin belirli aralıklarla ayıklanması ve uygun yöntemlerle imha edilmesi de gereklidir. Bu işlemler, bilgi güvenliğinin sağlanması, yasal yükümlülüklerin yerine getirilmesi ve sistemin sürdürülebilirliği açısından kritik rol oynamaktadır. Ancak ayıklama ve imha süreçlerinin plansız, denetimsiz veya standartlara aykırı yürütülmesi çok boyutlu riskler doğurabilir.





Personel Yetersizliđi ve Bilgi Eksikliđi

- Ayıklama ve imha işlemlerini yürüten personelin belge türleri, saklama süreleri ve yasal sorumluluklar konusundaki bilgi eksikliđi, belgelerin yanlışlıkla imha edilmesine ya da gereksiz belgelerin sistemde tutulmaya devam etmesine neden olabilir. Kurum içi eğitimlerin yetersiz olması veya bu sürecin belirli birimlerin inisiyatifine bırakılması, belge yönetiminde kurumsal bütünlüğü zedeler.

Altyapı ve Teknik Kapasite Sorunları

- İmha işlemlerinin sistematik ve güvenli şekilde yürütülmesi için gerekli olan dijital altyapının eksikliđi, özellikle büyük veri kümeleriyle çalışan kurumlarda süreci yavaşlatabilir ya da başarısız kılabilir. Yedekleme sistemleriyle senkronizasyon sağlanamaması durumunda, silinmiş belgelerin geri yüklenmesi imkânsız hale gelebilir.



Saklama Süresi ve Standart Dosya Planına Uyumsuzluk

- Belgelere ait saklama sürelerinin Standart Dosya Planı'na uygun biçimde belirlenmemesi ya da bu planın sistemle entegre çalışmaması, belgelerin erken ya da geç imha edilmesine neden olabilir. Bu durum, hem yasal yükümlülüklerin ihlali hem de arşivleme maliyetlerinin artması gibi sonuçlar doğurabilir.

İzlenebilirlik Eksikliği (Audit Trail Sorunları)

- Hangi belgenin, kim tarafından, hangi gerekçeyle imha edildiğine ilişkin yeterli kayıt tutulmaması, denetim ve hesap verebilirlik açısından ciddi bir risk oluşturur. Denetim izi bulunmayan imha işlemleri, özellikle kamu kurumlarında kurumsal şeffaflığa zarar verir ve hukuki sorumluluk doğurabilir.



Hukuki Bekletme Riskleri

- Dava, denetim veya disiplin soruşturmaları gibi süreçlerde “imha edilmemesi gereken” belgelerin ayıklama sürecinde yanlışlıkla silinmesi, ciddi hukuki yaptırımlara yol açabilir. Bu risk, EBYS sistemlerinin yasal süreçlerle entegre çalışmaması durumunda daha da artmaktadır.

Kurumsal Politika Eksikliği

- Ayıklama ve imha işlemlerine ilişkin kurum genelinde kabul edilmiş, yazılı ve güncel bir politika olmaması, sürecin birimler arasında farklı şekillerde yürütülmesine yol açar. Bu durum, belge yönetiminde dağınıklığa, standart dışı uygulamalara ve bilgi güvenliğinde zafiyetlere neden olabilir.

Katılımcı Görüşleri

- Saklama süreli belgelerin yönetimi, belgelerin yasal olarak belirli bir süre boyunca saklanması ve bu süre sonunda doğru şekilde imha edilmesi sürecini kapsamaktadır. Bu süreçlerin eksiklikleri ve tasfiye işlemlerinin belirsizliği, kurumlar için ciddi riskler yaratmaktadır.

Belge/Veri Kaybı	Erişim
Yetkili Kurumların Sorumsuzluğu	Yönetilemez Yapı
Gereksiz Saklama	Maliyet
Süreci İşletememe	Veri Gizliliği
Yasal Riskler	Yetkin Personel
Yanlış İmha	Kurum İmajı
Enerji Kaybı	Kurumsal Benliğin Kaybolması
Bütünlüğün Bozulması	Arşivlemenin Yapılamaması
	Sistemin Yavaşlaması



4. Elektronik Belge Yönetim Süreçlerindeki Riskler

Katılımcı Görüşleri:

- “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 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”
- “Fiziki belge yönetimini düşünün belgeler üretildi idari mali hukuki süreçlere göre saklama süreleri tayin edildi ve arşiv belgesi saklama süresi sonunda Devlet Arşivleri’ne gönderilir denildi. Fiziki olarak bunu yapıyor kurumlar ama elektronik olarak yapıldı mı? Kurumların devlet arşivlerine göndereceği belgeler var peki devlet arşivleri bunu alabilecek teknolojik altyapıya sahip mi? Hepsi soru işareti.

- 
- *İmha yaptığımızı düşünelim, eğer imha yapıyoruz. Saklama süremizi tayin etmedik. Saklama süremizi doğru tayin etmedik ama işte aradan 10 yıl geçtiği için bunu imha ettiğimizi düşünüyorum. O zaman delil değeri taşıyan bir belgeyi imha etmiş olabilme ihtimalimiz var ve doğal olarak davalarda sıkıntı yaşayabilme ihtimalimiz oluyor. Mesela fiziki belgeler için söylerler. Devlet kamulaştırmış mesela bazı demir yolu arazilerini fakat kamulaştırdığına dair belgeleri tutmadığı için tekrardan kamulaştırma parası vermiş. Devlet Demiryollarının arşivinde bu belgeler tutulmadığı için orada durumu bilen kişiler de tayin olmuş vesaire oranın kamulaştırıldığını haberdar değiller. Tekrar tekrar kamulaştırma ücreti veriliyor. Bunun elektronik ortamdaki meselesini düşünelim. Eğer siz bu belgeyi onun gibi düşünüp imha ederseniz, 30, 40 yıl sonra bu belge size lazım olduğunda bunu sunamayacak ve bir hak yetki ve sorumluluğu da ispatlayamayacaksınız. Böyle bir sıkıntımız var. Böyle bir sorununuz var. Belge yönetimi, saklama süreleri ve imha işlemleriyle ilgili. Burada esas olan yine dediğim gibi saklama süreli dosya planını oluşturmak.*



- Katılımcılar, elektronik belgelerin tasfiyesi ve uzun vadeli arşivlenmesi sürecine ilişkin kurumsal düzeyde hazırlık bulunmasına rağmen, uygulamada ciddi belirsizliklerin devam ettiğini ifade etmektedirler. Özellikle belgelerin **e-arşiv sistemi mi yoksa EBYS üzerinden mi devredilmesi gerektiği** konusunda kurum içinde farklı yaklaşımların bulunduğu; bu nedenle, sürecin hangi sistem üzerinden yürütülmesi gerektiğine dair ortak bir standardın henüz oluşturulmadığı belirtilmektedir.
- Bu çerçevede, Devlet Arşivleri Başkanlığı tarafından süreçle ilgili net yönlendirmelerin ve teknik standartların yayımlanmasına ihtiyaç duyulduğu vurgulanmaktadır. Elektronik ortamda saklanması gereken belgeler ile arşive devredilmesi gereken belgelerin ayrımının açık biçimde yapılmaması da uygulamada karışıklığa yol açmaktadır.
- Katılımcı görüşlerine göre, kurumlar teknik olarak belgeleri uygun format ve yapıda aktarabilecek kapasiteye sahip olsa da, **merkezi düzeyde yeterli kurumsal altyapı ve standart bütünlüğünün** henüz sağlanamamış olması nedeniyle uygulama süreci belirsizlik taşımaktadır. Bu durumun çözümü için, yalnızca Devlet Arşivleri değil, gerekirse **Cumhurbaşkanlığı ya da başka yetkili bir üst merci tarafından** sürece yön verilmesi gerektiği dile getirilmektedir.

Risk Analizi

- Risk unsurları belirlendikten sonra, risk analizi aşaması devreye girer. Bu aşamada amaç, risklerin kapsamlı bir şekilde anlaşılması ve gerekli durumlarda iyileştirilmesi için stratejiler geliştirilmesidir. Risk analizi, AS/NZS 4360:2004 standardına göre risk kaynaklarının, bunların olası olumlu ve olumsuz sonuçlarının ve bu sonuçların ortaya çıkma olasılığının değerlendirilmesini içerir. Bu sayede risklerin niteliği ve seviyesi belirlenerek, risk değerlendirmesi ve risk tedavisi için sağlam bir zemin hazırlanır. ISO 27005 (2022, s. 5) standardında da vurgulandığı gibi, risk analizi kısaca risk tahmini olarak özetlenebilir.
- Risk analizi, ISO 31000:2018 standardına göre, riskin niteliğini ve uygun olduğunda risk seviyesini de içeren tüm özelliklerini anlamaya odaklanan bir süreçtir. Bu kapsamlı analiz, belirsizlikler, risk kaynakları, olası sonuçlar, her bir olayın gerçekleşme olasılığı, olası senaryolar, mevcut kontroller ve bu kontrollerin etkinliği gibi unsurların detaylı bir şekilde değerlendirilmesini içerir.





Risk Analiz Teknikleri

- **İş Etki Analizi:** Bir olay veya kesintinin kuruluşun belge ve belge yönetimi fonksiyonlarını nasıl etkileyebileceğini değerlendirmeye yönelik bir tekniktir. Analiz kapsamında, olası olaylar ve bunların gerçekleşme olasılıkları, her bir olayın belge ve belge yönetimi üzerindeki potansiyel etkileri, bu etkilerin şiddeti ve süresi, kritik belgelerin ve süreçlerin tanımlanması ve bu riskleri yönetmek için gerekli kaynakların ve yeteneklerin belirlenmesi yer alır.
- **İnsan Güvenilirliği Analizi (İGA):** Bir kişinin sistem güvenilirliğine ve güvenliğine katkısını değerlendirmektir. Bu değerlendirme, yanlış eylem potansiyelini belirleyip analiz ederek gerçekleştirilir. Özellikle doğru performansın kritik önem taşıdığı görevlere taktik düzeyde uygulanır. Bu sayede belge yönetiminin tasarım, uygulama ve değişiklik aşamalarında hataları en aza indirecek şekilde tasarlanması ve korunması sağlanır.
- **Papyon Analizi:** Bir olayın nedenlerinden sonuçlarına uzanan yolları ve bu yolları etkileyen kontrolleri görselleştiren güçlü bir risk analizi aracıdır. Karmaşık riskleri basit ve anlaşılır bir şekilde sunarak, farklı senaryoların değerlendirilmesini kolaylaştırır.



Risklerin Değerlendirilmesi

Risklerin değerlendirilmesi, potansiyel tehlikelerden kaynaklanabilecek risklerin büyüklüğünü tahmin etme ve mevcut kontrol mekanizmalarının bu riskleri bertaraf etmede ne kadar yeterli olduğunu değerlendirme sürecidir. Bu sayede, risklerin kabul edilebilir olup olmadığına karar verilebilir ve kabul edilemez riskler için gerekli önlemler belirlenebilir. Ceylan ve Başhelvacı'ya (2011, ss. 26-27) göre risk değerlendirmesinin iki temel amacı vardır:

- *Risklerin Kabul Edilebilirliği:* Mevcut risklerin kabul edilebilir bir seviyede olup olmadığını belirlemek.
- *Risk Azaltma Tedbirleri:* Kabul edilemez riskler için gerekli önlemleri ve tedbirleri tanımlamak.



Risklerin Değerlendirilmesi

- Ceylan ve Başhelvacı'nın (2011) ortaya koyduğu risk değerlendirme yaklaşımı, risklerin kabul edilebilirliğini belirlemeyi ve kabul edilemez riskler için uygun önlemleri tanımlamayı amaçlarken, bu yaklaşım Kamu Risk Yönetim Rehberi ile de uyumludur.
- Rehberde (2024, s.s. 36-37) vurgulandığı üzere, riskler yalnızca kurumsal düzeyde değil, aynı zamanda birim, faaliyet ve süreç seviyelerinde de ele alınmalı; belge yönetimi gibi operasyonel alanlarda da bu bakış açısıyla değerlendirilmelidir.
- Özellikle belge üretim, kullanım ve saklama süreçlerinin kişilere bağımlı yürütülmesi, kontrol mekanizmalarının yetersizliği ya da standartlara uyumsuzluk gibi durumlar, süreç temelli risklerin tipik örneklerini oluşturur.
- Bu nedenle, belge yönetiminde karşılaşılan potansiyel risklerin sistematik biçimde süreç kartları ve iş akışları üzerinden tanımlanması, hem kontrol eksikliklerinin giderilmesini sağlar hem de kurumsal hedeflerle uyumlu risk azaltma stratejilerinin geliştirilmesine katkıda bulunur.



Riski Değerlendirme Teknikleri

- *Makul Olarak Uygulanabilir En Düşük Seviye (As Low As Reasonably Practicable) (ALARP):* ALARP ilkesi, riskleri kabul edilebilirlik seviyelerine göre üç kategoriye ayırmaktadır. ALARP ilkesi, risklerin kabul edilebilir seviyelerini(1. Kabul Edilemez Bölge, Tolere Edilebilir Bölge, Kabul Edilebilir Bölge) belirlemede ve uygun risk yönetimi stratejileri geliştirmede önemli bir araçtır (Baybutt, 2014).
- *Güvenilirlik Merkezli Bakım (GMB):* Makinelerin, ekipmanların ve diğer varlıkların en üst düzeyde güvenilir ve kullanılabilir olmasını sağlayan bir yöntemdir.



Riski Değerlendirme Teknikleri

- *Risk Değerlendirme Matrisleri:* İki veya daha fazla değişken arasındaki ilişkiyi analiz etmek için kullanılmaktadır. Bu matrislerden L Tipi Matris (LTM) yönteminde tehlikelerin oluşma olasılığı ile meydana gelme olasılığı arasındaki ilişki analiz edilmektedir (Department of Defence, 2000).
- Genel olarak 5x5 Matris yöntemi olarak bilinen ve L tipi matris olarak da adlandırılan metot, kolay anlaşılıp kolay uygulanabilir olmasından dolayı ülkemizde en çok tercih edilen risk değerlendirme yöntemidir (Saffady, 2005; Bannerman P. L. 2008, Cox, 2008, Ceylan ve Başhelvacı, 2011; Kuzucuoğlu, 2014; Hazine ve Maliye Bakanlığı,2024, s.44).

“Risk = Tehlikeli Bir Olayın Meydana Gelme İhtimali (Olasılık) * Tehditin Etkisi/Şiddeti”

- *Fayda-Maliyet Analizi:* Farklı projelerin ekonomik açıdan karşılaştırılmasını sağlayan güçlü bir risk değerlendirme aracıdır. Bu teknikte, projenin ömrü boyunca yapılacak tüm harcamalar ve elde edilecek tüm faydalar, bugünkü değerlerine indirgenerek maliyet-fayda analizi hesaplanır.

Risk Müdahalesi (Risklerin Tedavi Edilmesi/Risk İyileştirmesi)

Riskler tanımlanıp değerlendirildikten sonraki adım, risklerle başa çıkmak için kullanılabilecek yaklaşımların değerlendirilmesi ve her biri için kullanılması gereken tedavi seçeneğinin belirlenmesidir. Risk tedavisi, riskleri tedavi etmek için çeşitli seçeneklerin belirlenmesini, bu seçeneklerin değerlendirilmesini ve tedavi planlarının uygulanmasını içermektedir. Burada amaç, tüm risklerin ortadan kaldırmak değil risklerin kabul edilebilir seviyelere indirilmesi veya risklerin kabul edilebilir düzeyde tutulması için gerekli olan tedavi seçeneklerine karar vermektir (McDowall, 2005).

- **Azaltma:** Risklerin kabul edilebilir bir seviyeye indirilmesi için önceden belirlenmiş kontrol faaliyetlerinin uygulanmasını içerir (Derici, Tüystüz ve Sarı, 2007, s.162).
- **Riski Transfer Etme:** Kabul edilebilir risk seviyesinin altına düşürülmesi mümkün olmadığında veya gerekli kontrollerin uygulanması yüksek maliyet gerektirdiğinde, riskin üçüncü bir tarafa devri gündeme gelir. Sigorta yaptırmak bu yöntemin bir örneğidir. Riski transfer etmeyi seçerken, güvenlik ihtiyaçlarının, kontrol hedeflerinin ve ilgili kontrollerin sözleşmelerde açıkça belirtilmesine dikkat edilmelidir (Paksu ve Bozdemir, 2021, s. 65).



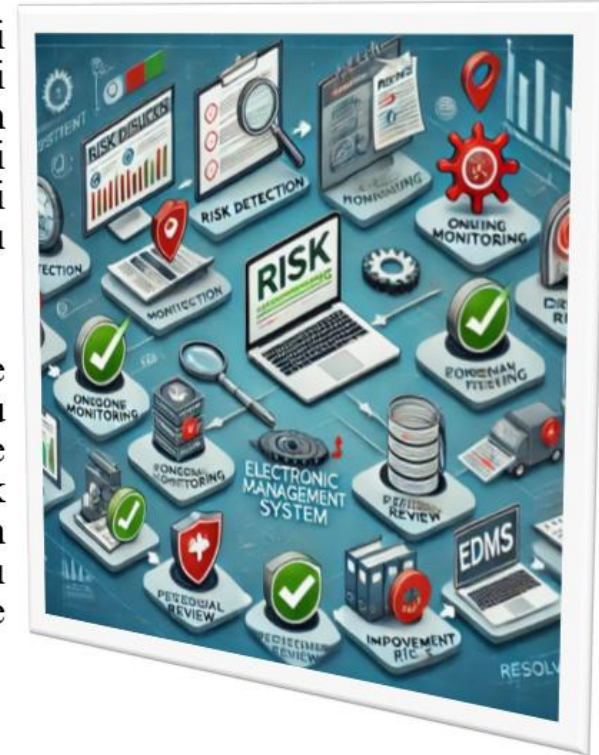
Risk Müdahalesi (Risklerin Tedavi Edilmesi/Risk İyileştirmesi)

- **Riskle Mücadele Etmek:** Olayların olumsuz etkileri azaltılarak potansiyel kayıpların giderilmesi için gerekli kontrollerin belirlenmesi ve uygulanması hedeflenmektedir. Riskin etkilerinin azaltılmasına yönelik kontroller ve faaliyetler olay öncesi (örneğin; deprem öncesi yapılanlar) ve olay sonrası (deprem sonrası yapılanlar) olabilmektedir (Bozkurt, 2010, s.21).
- **Riskten Kaçınma:** Riskin ortaya çıkmasına veya artmasına neden olan faaliyetlerden kaçınmayı veya bunları sonlandırmayı ifade eder (TÜSİAD, 2008, s. 60). Riskten kaçınma yöntemi, riskin felaket potansiyeline sahip olduğu ve riskin azaltılamadığı veya transfer edilemediği durumlarda kullanılmalıdır. Bu durumlar genellikle hem sıklığı hem de şiddeti yüksek olan ve azaltılamayan riskler için geçerlidir. Her ne kadar kaçınma, bazı risklerle başa çıkmanın tek alternatifi olsa da olumlu olmaktan çok olumsuz bir yaklaşım olarak değerlendirilir (Vaughan ve Vaughan, 2008, s. 18).



İzleme ve Gözden Geçirme

- Değişen risk ortamına ayak uydurmak için risk yönetimi programlarının da sürekli güncellenmesi ve gözden geçirilmesi gerekir. Yeni risklerin ortaya çıkması ve eski risklerin ortadan kalkması, geçmişte uygun olan çözümlerin günümüzde de yeterli olmayabileceği anlamına gelir. Bu nedenle, risk yönetimi programının düzenli olarak gözden geçirilmesi ve izlenmesi, olası felaketlerin önlenmesine yardımcı olur.
- Gözden geçirme süreci, geçmiş risk değerlendirmelerinin ve uygulama seviyelerinin güncelliğini sorgulamayı içerir. Bu sayede, risk yönetimi sürecinin her adımı, değişen koşullara ve yeni tehditlere karşı kontrollü biçimde ele alınacaktır. Düzenli risk yönetimi gözden geçirmeleri ve izleme faaliyetleri, kuruluşların değişen risk ortamına ayak uydurmasına ve olası tehditlere karşı kontrollü bir şekilde korunmasına yardımcı olur (Vaughan ve Vaughan, 2008, s.30-31).



İzleme ve Gözden Geçirme

İzleme ve gözden geçirme sürecinin başarılı olması için birtakım yöntemler belirlenmekte ve buna yönelik faaliyet alanları oluşturulmaktadır. Public Record Office Victoria (2010)'da sürece ilişkin yöntem ve faaliyet alanları özetlenmektedir. Yöntemler şu şekilde listelenebilir:

- **Sürekli İzleme:** Mevcut ve gelecekteki olası belge yönetimi risklerinin, devam eden belge yönetimi operasyonlarının bir parçası olarak sürekli olarak kontrol edilmesi ve izlenmesi.
- **Değerlendirmeler ve Denetimler:** Belge yönetimi uygulamaları ve belge yönetimi programlarıyla ilişkili risklerin belirlenmesi ve raporlanması için öz değerlendirmeler ve iç denetimler.
- **Dış Denetimler:** Kurumda belge yönetiminin hangi yönlerinin risk altında olabileceğini belirlemeye yardımcı olmak için Ombudsman, Genel Denetçi, Gizlilik Komiseri veya Sağlık Komiseri gibi dış denetimler.
- **Kısa Öz Değerlendirme:** Kurumda belge yönetiminin hangi yönlerinin risk altında olabileceğini belirlemeye yardımcı olmak için kısa bir öz değerlendirme formunun geliştirilmesi.



İletişim ve Danışma

- Risk yönetimi sürecinin başarısı için etkili bir iletişim ve danışma stratejisinin geliştirilmesi önemli görülmektedir. Bu strateji çerçevesinde, risk farkındalığını ve anlayışı artırmaya odaklanan iletişim, paydaşlara risklerin doğası, potansiyel etkileri ve olası sonuçları hakkında bilgi sunarak şeffaflığı ve katılımı teşvik etmektedir.
- Danışma ise farklı uzmanlık alanlarından gelen paydaşların görüşlerini toplayarak, risk kriterlerinin belirlenmesi ve değerlendirilmesinde çeşitli bakış açılarının dikkate alınmasını sağlar. Bu sayede daha kapsamlı ve sağlam bir risk analizi gerçekleştirilebilir ve risklerin kontrollü bir biçimde yönetilmesine imkân tanınır (ISO 31000, 2018).



İletişim ve Danışma

Başarılı bir iletişim ve danışma stratejisi için ise uygulanması gerekenler şu şekilde sıralanabilir (Hazine ve Maliye Bakanlığı, 2024, s.82; ISO 31000, 2018, s.9; TÜSİAD, 2008, s.64):

- *Net rol ve sorumluluk tanımlama:* Risk yönetimi sürecindeki her paydaşın rolü ve sorumluluğu açıkça tanımlanmalı ve görev tanımlarına işlenmelidir.
- *Kapsamlı iletişim planı oluşturma:* Hem kurum içi hem de kurum dışı paydaşlarla iletişimi düzenleyen bir plan oluşturulmalı ve bu plan riskler ve risk yönetimi süreciyle ilgili tüm dikkate değer konuları kapsamalıdır.



İletişim ve Danışma

- *Karşılıklı diyalog ve takım çalışması:* Tek yönlü bilgilendirmeden ziyade, karar alıcılar ve menfaat sahipleri arasında karşılıklı bir diyalog ortamı teşvik edilmelidir. Farklı bakış açılarının risk analizine dahil edilmesi ve değerlendirilmesi önemlidir.
- *Geri bildirim ve iyileştirme:* İletişim ve danışma faaliyetlerinin kayıt altına alınması ve karar alma sürecine entegre edilmesi, paydaşların geri bildirimlerinin toplanmasına ve risk yönetimi sürecinde gerekli iyileştirmelerin yapılmasına olanak sağlar.



Kaydetme ve Raporlama

- Kuruluşlar, risk yönetimi faaliyetlerinin ve elde edilen sonuçların tüm paydaşlara iletilmesi, karar verme süreçleri için bilgi sağlanması, risk yönetimi sisteminin sürekli geliştirilmesi ve risklerden sorumlu olanlar da dahil olmak üzere tüm paydaşlarla etkileşimin teşvik edilmesi gibi kritik nedenlerden dolayı risk yönetim sürecini ve elde edilen sonuçları belgelemeli ve raporlamalıdır (ISO 31000:2018, s.14-15).



Kaydetme ve Raporlama

- Raporlamadan elde edilen veriler, sadece bir sonraki risk belirleme sürecinin girdilerini oluşturmakla kalmayacak, aynı zamanda risk yönetimi döngüsünü de besleyecek bir geri bildirim mekanizması görevi görecektir. Her raporlama döngüsü, geçmişte alınan önlemlerin riskleri ne kadar azalttığını, yeni risklerin ortaya çıkıp çıkmadığını ve mevcut risklerin nasıl değiştiğini anlamamızı sağlayarak risk profilinin sürekli güncellenmesine ve iyileştirilmesine katkıda bulunacaktır. Bu sayede, risk yönetimi kontrollü ve dinamik bir hale gelerek, kuruluşun hedeflerine ulaşmasını engelleyebilecek tehditlere karşı her zaman hazırlıklı olmasını sağlayacaktır (İnce, 2019, s.290).



Kaynakça

- Albayrak, S. (2020). Türkiye’de kamu personel yönetiminin yeni kurumsal yapısı ve kamu istihdamının yeni görünümü. *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi*, 75,4, 1517–1549.
- Australian/New Zealand Standard (2004). Risk Management. (Standart No: AS/NZS 4360:2004). http://mkidn.gov.pl/media/docs/pol_obronna/20150309_3-NZ-AUST-2004.pdf
- Baybutt, P. (2013). The ALARP principle in process safety. *Process Safety Progress* 33, 1, 36-40. <https://doi.org/10.1002/prs.11599>
- Bozkurt, C. (2010). Risk, kurumsal risk yönetimi ve iç denetim, *Denetışim*,4, 17-30.
- Ceylan, H. ve Başhelvacı, V. S. (2011). Risk değerlendirme tablosu yöntemi ile risk analizi: bir uygulama. *International Journal of Engineering Research and Development*, 3, 2, 25-33.
- Çiçek Akgün, A., & Çiçek, N. (2022). Dijital Çağda Değişen Belge Olgusunun Arşivcilikte Düzenleme ve Tanımlamaya Etkisi: Literatüre Dayalı Bir İnceleme. *Bilgi Ve Belge Araştırmaları*(17), 33-58. <https://doi.org/10.26650/bba.2022.17.1127615>
- Çiçek, N. (2020). E-devlet stratejisi bağlamında elektronik belge yönetimi için “yazılı politika” gereksinimi: Türkiye’deki uygulamalar üzerine bir inceleme. *Türk Kütüphaneciliği*, 34, 3, 377-405

Kaynakça

- Department of Defence, U. S. (2000). Standard Practice for System Safety, DoD, MILSTD-882D. Erişim adresi: <https://mail.system-safety.org/Documents/MIL-STD-882D.pdf>
- Derici, O., Tüysüz, Z. ve Sarı, A. (2007). Kurumsal risk yönetimi ve sayıştay uygulaması, *Sayıştay Dergisi* 65,151-172
- Devlet Arşivleri Başkanlığı. (2024). *Belge ve arşiv yönetimi temel kavram ve terimler*. T.C. Cumhurbaşkanlığı Devlet Arşivleri Başkanlığı.
- Dişli, M. ve Külçü, Ö. (2020). Üniversitelerde elektronik belge yönetim sistemlerinin birlikte çalışabilirlik açısından değerlendirilmesi. *Bilgi Dünyası*, 21 (1), 35-63
- Türkiye Bilişim Derneği. (2009). *Elektronik belge yönetimi sürüm 0.2*. Türkiye Bilişim Derneği.
- Elzamly, A., Hussin, B. ve Salleh, N. (2016). Top fifty software risk factors and the best thirty risk management techniques in software development lifecycle for successful software projects. *International Journal of Hybrid Information Technology* 9, 6, 11-32 Erişim adresi: <http://dx.doi.org/10.14257/ijhit.2016.9.6.02>
- Ermisket, E. G. (2011). Kamu kurumlarında risk yönetimi: Bir uygulama önerisi. *Denetim*, 7, 58–70.



Kaynakça

- 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 Organization for Standardization (2022). *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. (ISO Standard No. 27005:2022).
- International Organization for Standardization. (2016). *ISO 15489-1:2016 – Information and documentation – Records management – Part 1: Concepts and principles*. ISO.
- International Organization for Standardization. (2018). *Risk management guidelines* (ISO Standard No. 31000:2018).
- International Organization for Standardization. (2024). *ISO 18128:2024 – Information and documentation – Records risks – Risk assessment for records management* [Standard]. ISO.
- İnce, F. (2019). Kurumsal risk yönetim süreci. 3. Uluslararası Akdeniz Sempozyumu, Mersin.
- Kandur, H. (2011). Türkiye’de kamu kurumlarında elektronik belge yönetimi: Mevcut durum analizi ve farkındalığın artırılması çalışmaları. *Bilgi Dünyası*, 12(1), 2-12.



- 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
- McDowall, R. D. (2005). Effective and practical risk management options for computerised system validation. *Qual Assur Journal*, 9, 196–227.
- Odabaş, H. (2005). Belge yönetimi ve Türkiye’de belge yönetimi gereksinimi. *Bilgi Dünyası* 6,1, 36-57.
- Odabaş, H. (2007). *Elektronik Belge Yönetimi ve Kamu Kurum ve Kuruluşları*. Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Doktora Tezi, Ankara.
- Oxford University Press. (2023). Risk. In *Oxford learner's dictionaries*. Retrieved March 18, 2023, from https://www.oxfordlearnersdictionaries.com/definition/english/risk_1?q=risk
- Paksu, S. ve Bozdemir, R. (2021). Bilgi güvenliği risk yönetimi, *BİLGEM Teknoloji Dergisi*, 12. Erişim adresi: <https://bilgem.tubitak.gov.tr/wp-content/uploads/sites/8/bilgem-teknoloji-dergisi-12.pdf>
- Public Record Office Victoria. (2010). PROS 10/10: Guideline 6: Records & Risk Management. Ed. Strategic Management Advisory Group.



- Türk Dil Kurumu (2022). Risk. İçinde *Güncel Türkçe sözlük*. Erişim 20 Mart 2023, erişim: <https://sozluk.gov.tr/>
- Türk Standardları Enstitüsü. (2015). *TS 13298: Elektronik belge ve arşiv yönetim sistemi standardı* [Standard]. TSE.
- TÜSİAD (2008). Kurumsal risk yönetimi. İstanbul
- Usman, Ö. ve Kaygusuz, S. Y. (2019). Kurumsal risk yönetiminde uygulanması gereken adımlar. *Muhasebe ve Denetime Bakış*, 56,109-128.
- Vaughan, E.J. ve Vaughan, T. (2008) *Fundamentals of risk and insurance*. John Wiley & Sons, Inc. Erişim adresi: <https://nibmehub.com/opac-service/pdf/read/Fundamentals%20of%20Risk%20and%20Insurance-%2010th%20Edition.pdf>
- Yalçınkaya, B. (2016). Elektronik belge yönetim sistemi (ebys) uygulamalarında başarı faktörü ve fayda analizi. *AJIT-e: Online Academic Journal of Information Technology*, 7,23 DOI: 10.5824/1309-1581.2016.2.006.x

