



T.C.
ANKARA SOSYAL BİLİMLER ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

DAYANIKLILIK İLKELERİNİN KURUMSAL RİSK YÖNETİMİ
UYGULAMALARIYLA BÜTÜNLEŞTİRİLMESİ:
DAYANIKLILIK ODAKLI KURUMSAL RİSK YÖNETİMİ MODELİ

Doktora Tezi

Mehmet Baha KARAÇOLAK

Denetim ve Risk Yönetimi Anabilim Dalı

Denetim ve Risk Yönetimi Doktora Programı

Kasım 2025



T.C.
ANKARA SOSYAL BİLİMLER ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

DAYANIKLILIK İLKELERİNİN KURUMSAL RİSK YÖNETİMİ
UYGULAMALARIYLA BÜTÜNLEŞTİRİLMESİ:
DAYANIKLILIK ODAKLI KURUMSAL RİSK YÖNETİMİ MODELİ

Doktora Tezi

Mehmet Baha KARAÇOLAK

Denetim ve Risk Yönetimi Anabilim Dalı

Doç. Dr. Hakan KARABACAK

Kasım 2025

TEŞEKKÜR

Tez yazım sürecinde akademik desteğini esirgemeyen, bilgi, fikir ve deneyimiyle tezin olgunlaşmasını sağlayan değerli danışmanım Doç. Dr. Hakan KARABACAK Hocama teşekkür ederim.

İlgi ve tecrübeleriyle çalışmanın derinleşmesi ve zenginleşmesine katkı sunan Doç. Dr. Halis KIRAL ve Doç. Dr. Yenal ARSLAN Hocalarıma; Tez Savunma Jürisine katılma nezaketi gösteren ve değerli görüşlerini paylaşan Doç. Dr. İzzet ARI ve Dr. Öğretim Üyesi Musab Talha AKPINAR Hocalarıma saygı ve şükranlarımı sunarım.

Kıymetli zamanını, önerilerini ve desteğini paylaşan mesai arkadaşım Muhammet Yaşar ÖZGÜR'e teşekkür ederim.

Doktora programı boyunca sabrı, sevgisi ve koşulsuz desteğiyle yanımda olan, kendinden çok fedakârlık yapan kıymetli eşime minnettarım.

İÇİNDEKİLER

TEŞEKKÜR.....	i
İÇİNDEKİLER.....	ii
ÖZET.....	vi
ABSTRACT	viii
KISALTMALAR.....	x
ŞEKİL LİSTESİ	xii
TABLO LİSTESİ	xiv
GİRİŞ.....	1
BİRİNCİ BÖLÜM.....	6
KURUMSAL RİSK YÖNETİMİ.....	6
1.1. Kurumsal Risk Yönetimi	6
1.2. KRY'yi Zorunlu Kılan Etmenler	8
1.3. Risk Yönetiminde Davranışsal ve Yönetmel Unsurlar	11
1.3.1. Risk Algısı.....	11
1.3.2. Risk Tutumu	12
1.3.3. Risk İştahı.....	13
1.3.4. Risk Toleransı	14
1.3.5. Risk Kapasitesi.....	15
1.3.6. Risk Kültürü	15
1.3.7. Risk İletişimi	16
1.4. Risk Yönetim Süreci.....	17
1.4.1. Risklerin Tanımlanması.....	19
1.4.2. Risklerin Analiz Edilmesi	21
1.4.3. Risk Yanıtlarının Geliştirilmesi	23
1.4.4. Yanıt Planının Uygulanması.....	31
1.4.5. İzleme ve Değerlendirme.....	32
1.5. KRY'nin Sağladığı Faydalar	33
1.6. KRY'nin Uygulanmasındaki Zorluklar	38
İKİNCİ BÖLÜM	42
KURUMSAL DAYANIKLILIK.....	42

2.1. Dayanıklılık Kavramı.....	42
2.1.1. Kavramın Kökenleri.....	44
2.1.2. Kavramın Gelişimi	44
2.1.3. Dayanıklılık Türleri ve Yaklaşımları.....	48
2.2. Kurumsal Dayanıklılık.....	50
2.3. Kurumsal Dayanıklılık Kapasiteleri.....	53
2.3.1. Öngörü (Tahmin) ve Hazırlık Kapasitesi	53
2.3.2. Önleyici Kapasite	54
2.3.3. Özümseme Kapasitesi.....	55
2.3.4. Onarım Kapasitesi	56
2.3.5. Uyum Kapasitesi	57
2.3.6. Dönüşüm Kapasitesi	59
2.4. Kurumsal Dayanıklılık Süreci.....	59
2.5. Kurumsal Dayanıklılığın Unsurları.....	65
2.5.1. Özellikleri	65
2.5.2. İlkeleri.....	66
2.5.3. Boyutları	68
2.5.4. Bileşenleri	69
2.5.5. Unsurların Değerlendirilmesi	71
2.6. Kurumsal Dayanıklılığın Önemi	75
2.7. Kurumsal Dayanıklılığın Güçlendirilmesi	76
2.7.1. Operasyonel ve Yapısal Faktörler.....	78
2.7.2. Kurumsal Öğrenme	81
2.7.3. İnsan Kaynakları, Kültür ve Liderlik Boyutu	81
2.7.4. Sosyal ve Kolektif Dayanıklılık Unsurları.....	83
2.7.5. Stratejik ve Entegre Dayanıklılık Yönetimi	84
2.8. Kurumsal Dayanıklılığın Sağlanmasındaki Zorluklar	88
ÜÇÜNCÜ BÖLÜM	91
RİSK VE DAYANIKLILIĞIN BİRLİKTE YÖNETİLMESİ.....	91
3.1. Olumsuz Durum Kavramı	91
3.2. Olumsuz Durum Türleri.....	91
3.2.1. Riskler	92
3.2.2. Tehditler	93
3.2.3. Muğlaklık ve Belirsizlikler	96
3.2.4. Cehalet (Tam Bilgisizlik).....	100

3.3. Olumsuz Durum Türlerinin Sınıflandırılması.....	100
3.4. Sınıflandırmanın Sağladığı Avantajlar	107
3.4.1. Duruma Özgü Müdahalelerin Geliştirilmesi	107
3.4.2. Hazırlık Süreçlerinin İyileştirilmesi.....	108
3.4.3. Durumların Önceliklendirilmesinin Sağlanması.....	108
3.4.4. Karar Alma Süreçlerinin Desteklenmesi.....	108
3.4.5. Kurum İçi Farkındalık ve Eğitim Kolaylığı.....	109
3.4.6. Stratejik Esneklik ve Adaptasyon	109
3.4.7. Kurumsal Politika ve Strateji Üretimine Katkı Sunulması.....	110
3.4.8. Ortak Bir Terminolojinin Tesis Edilmesi.....	110
3.5. Belirsizlik - Tehdit - Risk - Olay Zinciri.....	110
3.6. Durum Türlerine Yönelik Yönetim Araçlarının Belirlenmesi.....	111
3.7. KRY ve DY Arasındaki İlişkilerin Tanımlanması	115
3.7.1. Amaç ve Odak Bakımından Tamamlayıcılık	118
3.7.2. Zaman Boyutu ile Tamamlayıcılık.....	118
3.7.3. Strateji ve Uygulama Düzeyinde Entegrasyon	121
3.7.4. Belirsizlik Türlerine Yaklaşımda Farklılaşma	122
3.7.5. Araçların Kapsamlarında Farklılaşma	122
3.7.6. Yapısal İlişkiler	122
3.8. Teori ve Pratikteki Sınırlılıklar ve Yetersizlikler.....	124
3.9. DY Kapsamında Değerlendirilmesi Gereken Olumsuz Durumların Tespit Edilmesi	126
DÖRDÜNCÜ BÖLÜM	132
RİSK, TEHDİT VE BELİRSİZLİKLERE KARŞI DAYANIKLILIĞI GÜÇLENDİRME STRATEJİLERİ.....	132
4.1. Dayanıklılık Stratejisi	132
4.2. Literatür Analizi.....	135
4.2.1. Akademik Çalışmalar.....	135
4.2.2. Kurumsal Dayanıklılık Standartları.....	146
4.3. Literatür Bazlı Jenerik Dayanıklılık Stratejileri.....	148
4.3.1. Stratejilerin Konsolide Edilmesi	148
4.3.2. Dayanıklılık Stratejileri	150
4.4. Durum Türüne Göre Risk ve Dayanıklılık Stratejilerinin Belirlenmesi.....	165
4.4.1. Olumsuz Durum Türleri Çerçevesinde Risk Stratejilerinin Seçilmesi....	166
4.4.2. Risk Stratejileri ile Dayanıklılık Stratejilerinin Eşleştirilmesi.....	170

4.4.3. Olay Fazları ve Stratejilerin Devreye Alınması.....	172
4.4.4. Uygulama Örnekleri.....	176
BEŞİNCİ BÖLÜM	187
DAYANIKLILIK ODAKLI.....	187
KURUMSAL RİSK YÖNETİMİ MODELİ ÖNERİSİ	187
5.1. Modelin Amacı.....	187
5.2. Modelin Kapsamı.....	188
5.3. Modelin Teorik Temeli.....	189
5.4. Modelin Öne Çıkan Özellikleri	190
5.5. Modelin Bileşenleri.....	191
5.5.1. Yönetişim ve İlkeler	192
5.5.2. Kurumsal Kapasite.....	193
5.5.3. İletişim ve Koordinasyon	194
5.5.4. Yanıt Stratejileri	194
5.5.5. Olay Fazları.....	194
5.5.6. Eylemler.....	195
5.5.7. Geri Bildirim	195
5.6. Rol ve Sorumluluklar	196
5.7. Modelin İşleyişi ve Uygulama Süreci.....	196
5.7.1. Tanımlama	199
5.7.2. Analiz	202
5.7.3. Planlama	206
5.7.4. Uygulama.....	210
5.7.5. İzleme	212
5.8. Beklenen Değer ve Katkıları.....	214
SONUÇ VE ÖNERİLER.....	218
KAYNAKLAR.....	224
EKLER.....	257

ÖZET

Günümüz iş dünyası giderek artan ölçüde belirsizlik, karmaşıklık ve öngörülemezlik koşullarıyla şekillenmektedir. Bu dinamik ortamda ortaya çıkan siyah kuğu niteliğindeki olaylar, kurumların kontrol kapasitesini aşmakta ve en güçlü senaryoları dahi geçersiz kılabilir. COVID-19 pandemisi, Rusya-Ukrayna Savaşı, küresel tedarik zinciri kesintileri, siber saldırılar ve doğal afetler gibi örnekler, kuruluşların yalnızca hesaplanabilir risklere değil, aynı zamanda öngörülemeyen tehdit ve belirsizliklere karşı da hazırlıklı olması gerektiğini açıkça göstermektedir. Bu tür gelişmeler, geleneksel Kurumsal Risk Yönetimi (KRY) ve Dayanıklılık Yönetimi (DY) yaklaşımlarının tek başına ele alındıklarında yetersiz kaldığını ortaya koymaktadır.

KRY, ölçülebilir ve hesaplanabilir risklere odaklanan yapısıyla kuruluşlara önemli katkılar sunmakla birlikte, ani şoklar, zincirleme etkiler ve sistemik kırılmalıklar karşısında sınırlı bir etki göstermektedir. Benzer biçimde DY, çoğunlukla kriz sonrası toparlanma süreçleriyle sınırlı kalmakta, risk-getiri dengesi gözetilen stratejik bir bakış açısını yeterince içermemektedir. Dolayısıyla her iki yaklaşımın bağımsız kullanımları, olumsuz durumlara karşı parçalı çözümler üretmekte; kuruluşlara bütüncül ve stratejik değer yaratma kapasitesi kazandırmamaktadır. Bu durum, KRY ve DY'nin bütünleştirilerek tek bir çerçeve altında ele alınması, olumsuz durumların olay öncesi, anı ve sonrası evrelerinde bütünsel olarak yönetilmesi ihtiyacını doğurmaktadır.

Bu çalışmanın amacı, KRY'nin sistematik ve ölçülebilir risk yönetimi çerçevesini DY'nin önleme, koruma, uyum ve toparlanma kapasiteleriyle sentezleyen Dayanıklılık Odaklı Kurumsal Risk Yönetimi (DOKRY) Modelini geliştirmektir. Araştırma, nitel ve kavramsal bir yaklaşım benimsemekte; literatür taraması, içerik analizi ve kavramsal sentez yöntemleriyle ilerlemektedir. Bu kapsamda uluslararası standartlar ve akademik literatür incelenmiştir. Analizler sonucunda, her iki yaklaşımın sınırlılıkları, birbirini tamamlayan boyutları ve entegrasyon fırsatları belirlenmiş; DOKRY modelinin ana bileşenleri tanımlanmıştır.

Önerilen model; durum analizi, risk-tehdit-belirsizliklerin sınıflandırılması, strateji seçimi, olay fazlarının (öncesi-anı-sonrası) yönetimi, uygulama, izleme ve geri bildirim aşamalarını içeren döngüsel bir yapıya sahiptir. Bu yapı, her döngüde kurumsal öğrenmeyi, kaynakların etkin kullanımını ve kapasite gelişimini teşvik ederek kurumsal olgunluk düzeyini

yükseltmektedir. Böylece kuruluşlar yalnızca önleyici ve koruyucu mekanizmalarla değil, aynı zamanda uyarlanabilir ve yenilikçi stratejilerle de desteklenmektedir.

Araştırmanın teorik katkısı, KRY ve DY'nin tek başlarına sahip oldukları sınırlılıkları aşacak özgün ve bütünlük bir çerçeve sunmasıdır. Uygulama açısından ise çalışma, kuruluşlara proaktif durum yönetimi, kriz anında etkin müdahale ve kriz sonrası güçlenerek çıkma kapasitesi kazandıran kapsamlı bir yol haritası önermektedir. Bununla birlikte, çalışmanın kavramsal bir model geliştirme amacını taşıması nedeniyle, önerilen modelin ampirik olarak test edilmesi araştırma kapsamı dışında kalmaktadır. Modelin farklı sektörlerde uygulanabilirliği ve etkinliği, gelecekte yapılacak saha araştırmalarında sınanmalıdır.

Sonuç olarak, önerilen Dayanıklılık Odaklı KRY Modeli, risklerin yanı sıra tehdit ve belirsizliklerin de bütünlük bir şekilde yönetilmesini sağlayarak kuruluşlara sürdürülebilirlik, stratejik esneklik ve rekabet avantajı kazandırmayı hedeflemektedir. Bu yönüyle çalışma, belirsizliklerin ve öngörülemeyen olumsuz durumların hâkim olduğu günümüz iş ortamında teorik ve pratik düzeyde katkı sunmaktadır.

Anahtar Kelimeler: Risk, Tehdit, Belirsizlik, Kurumsal Risk Yönetimi, Dayanıklılık, Kurumsal Dayanıklılık.

ABSTRACT

Today's business world is increasingly shaped by conditions of uncertainty, complexity, and unpredictability. In this dynamic environment, black swan events can overwhelm organizations' capacity for control and render even the most robust scenarios obsolete. Examples such as the COVID-19 pandemic, the Russia-Ukraine war, global supply chain disruptions, cyberattacks, and natural disasters clearly demonstrate that organizations must be prepared not only for calculable risks but also for unforeseen threats and uncertainties. Such developments reveal that traditional Enterprise Risk Management (ERM) and Resilience Management (RM) approaches alone are insufficient.

While ERM, with its focus on measurable and calculable risks, provides significant contributions to organizations, it has limited impact in the face of sudden shocks, chain reactions, and systemic vulnerabilities. Similarly, RM is mostly limited to post-crisis recovery processes and does not sufficiently incorporate a strategic perspective that considers the risk-return balance. Therefore, the independent use of both approaches produces fragmented solutions to adverse situations; it does not provide organizations with the capacity to create comprehensive and strategic value. This situation necessitates the integration of KRY and DY under a single framework and the holistic management of adverse situations in their pre-event, during-event, and post-event phases.

The aim of this study is to develop a Resilience-Focused Enterprise Risk Management (RFERM) Model that synthesizes the systematic and measurable risk management framework of ERM with the prevention, protection, adaptation, and recovery capacities of DRM. The research adopts a qualitative and conceptual approach, progressing through literature review, content analysis, and conceptual synthesis methods. In this context, international standards and academic literature were examined. As a result of the analyses, the limitations of both approaches, their complementary dimensions, and opportunities for integration were identified, and the main components of the DOKRY model were defined.

The proposed model has a cyclical structure that includes situation analysis, classification of risks, threats, and uncertainties, strategy selection, management of event phases (pre-event, during event, post-event), implementation, monitoring, and feedback. This structure promotes organizational learning, effective use of resources, and capacity development in each cycle,

thereby raising the level of organizational maturity. Thus, organizations are supported not only by preventive and protective mechanisms but also by adaptable and innovative strategies.

The theoretical contribution of the study is that it offers a unique and integrated framework that overcomes the limitations of ERM and RM when considered separately. In terms of application, the study proposes a comprehensive roadmap that enables organizations to gain the capacity for proactive situation management, effective intervention during crises, and emerging stronger after crises. However, as the study aims to develop a conceptual model, empirical testing of the proposed model is beyond the scope of this research. The applicability and effectiveness of the model across different sectors should be tested in future field studies.

In conclusion, the proposed Resilience-Focused ERM Model aims to provide organizations with sustainability, strategic flexibility, and competitive advantage by enabling the integrated management of risks, threats, and uncertainties. In this respect, the study contributes at both the theoretical and practical levels to today's business environment, which is dominated by uncertainties and unforeseen adverse situations.

Keywords: Risk, Threat, Uncertainty, Enterprise Risk Management, Resilience, Enterprise Resilience.

KISALTMALAR

AICPA	: The American Institute of Certified Public Accountants (Amerikan Yeminli Mali Müşavirler Enstitüsü)
BSI	: The British Standards Institution (İngiliz Standartları Enstitüsü)
BT	: Bilgi Teknolojileri
COSO	: Committee of Sponsoring Organizations of the Treadway Commission (Treadway Komisyonu Sponsorluk Kuruluşları Komitesi)
DKKV	: Deutsches Komitee Katastrophenvorsorge e.V. (Alman Afet Önleme Komitesi)
DOKRY	: Dayanıklılık Odaklı Kurumsal Risk Yönetimi
DS	: Dayanıklılık Stratejisi
DY	: Dayanıklılık Yönetimi
ESG	: Environmental, Social, and Governance (Çevresel, Sosyal ve Yönetişim)
HTEA	: Hata Türleri ve Etkileri Analizi
IMA	: The Institute of Management Accountants (Yönetim Muhasebecileri Enstitüsü)
IPCC	: Intergovernmental Panel on Climate Change (Hükümetlerarası İklim Değişikliği Paneli)
IRGC	: International Risk Governance Council (Uluslararası Risk Yönetişimi Konseyi)
IRM	: Institute of Risk Management (Risk Yönetimi Enstitüsü)
ISO	: International Organization for Standardization (Uluslararası Standardizasyon Örgütü)
İSY	: İş Sürekliliği Yönetimi
KOBİ	: Küçük ve Orta Büyüklükteki İşletmeler
KPI	: Key Performance Indicator (Anahtar Performans Göstergesi)
KRI	: Key Risk Indicator (Anahtar Risk Göstergesi)
KRY	: Kurumsal Risk Yönetimi
KY	: Kriz Yönetimi
ODT	: Olumsuz Durum Tablosu
PECB	: Professional Evaluation and Certification Board (Profesyonel Değerlendirme ve Sertifikasyon Kurulu)

PERT	: Program Evaluation and Review Technique (Program Değerlendirme ve Gözden Geçirme Tekniği)
PESTLE	: Political, Economic, Social, Technological, Legal, Environmental (Politik, Ekonomik, Sosyal, Teknolojik, Hukuki, Çevresel)
PMI	: Project Management Institute (Proje Yönetim Enstitüsü)
RIMS	: Risk and Insurance Management Society (Risk ve Sigorta Yönetimi Topluluğu)
RS	: Risk Stratejisi
RY	: Risk Yönetimi
SES	: Sosyo-Ekonomik Sistemler
SWOT	: Strengths, Weaknesses, Opportunities, Threats (GZFT – Güçlü Yönler, Zayıf Yönler, Fırsatlar, Tehditler)
VUCA	: Volatility, Uncertainty, Complexity, Ambiguity (Değişkenlik, Belirsizlik, Karmaşıklık, Muğlaklık)

ŞEKİL LİSTESİ

Şekil 1: Risk Yönetimi Süreci	18
Şekil 2: Mühendislik Dengesi ve Ekolojik Denge	45
Şekil 3: Dayanıklılık Kavramının İzlediği Evrimsel Patika	47
Şekil 4: α , β , γ Tipi Dayanıklılık Türleri	49
Şekil 5: Şoka Maruz Kalan Bir Sistemin Performansındaki Temel Değişimler.....	61
Şekil 6: Dayanıklılık Sürecine İlişkin Performans - Zaman Eğrisi	62
Şekil 7: Dayanıklılık Sürecine İlişkin Aşamalar, İlgili Kapasiteler ve Senaryolar	64
Şekil 8: Dayanıklılığın Bileşenleri (Graveline & Germain, 2022)	71
Şekil 9: Olumsuz Durum Türlerinin Farkındalık, Etki-Olasılık Bilgisi ve Sonuçların Öngörülebilirliği Temelinde Sınıflandırılması	102
Şekil 10: Cehalet, Belirsizlik, Tehdit, Risk ve Olay Zinciri	111
Şekil 11: Müdahale Araçlarının Etkinleştirilmesine Yönelik Karar Akış Diyagramı	113
Şekil 12: Belirsizlik, Tehdit, Risk, Olay ve Sonuç Zinciri	119
Şekil 13: KRY İle DY Arasında Öncüllük-Ardılık ve Tamamlayıcılık İlişkisi	120
Şekil 14: Kurumsal Dayanıklılıkla İlişkili Uygulamaların Hazırlık, Uygulama ve İzleme Aşamalarının Gösterilmesi	120
Şekil 15: Dayanıklılıkla ilişkili Uygulamalar Arasındaki Öncüllük-Ardılık ve Tamamlayıcılık İlişkileri	121
Şekil 16: KRY ve Kurumsal Dayanıklılık Arasındaki Etkileşimler	123
Şekil 17: Örnek Risk Matrisi	127
Şekil 18: Modelin Bileşenleri ve İşleyişi	191
Şekil 19: Modelin Aşamaları ve Alt Adımları	197
Şekil 20: Modelin İşleyişine Yönelik İş Akış Süreci	198

Şekil 21: Tanımlama Aşaması	199
Şekil 22: Analiz Aşaması.....	203
Şekil 23: Neden (N), Olumsuz Durum (OD) ve Sonuç (S) İlişkilerinin Kurulması.....	205
Şekil 24: Planlama Aşaması	207
Şekil 25: Yanıt Eylemlerinin Neden, Olumsuz Durum ve Sonuçlar ile İlişkilendirilmesi....	209
Şekil 26: Uygulama Aşaması.....	210
Şekil 27: İzleme Aşaması.....	213



TABLO LİSTESİ

Tablo 1: KRY'nin Kuruluşlara Sağladığı Faydalar	37
Tablo 2: KRY'nin Kuruluşlarda Uygulanmasında Karşılaşılan Zorluklar	41
Tablo 3: Dayanıklılığa İlişkin Özellik, İlke, Boyut ve Bileşenler	73
Tablo 4: Dayanıklılığın Kuruluşlar Açısından Önemi	77
Tablo 5: Kurumsal Dayanıklılığın Güçlendirilmesine Yönelik Temel Etmenler	86
Tablo 6: DY'nin Kuruluşlarda Uygulanmasında Karşılaşılan Zorluklar	90
Tablo 7: Risk, Belirsizlik ve Tehdit Türlerinin Bilgi Temelli Karşılaştırılması	105
Tablo 8: Olumsuz Durum Sınıfların ve Olay Fazına Göre Yönetim Araçları	114
Tablo 9: Olumsuz Durumların DY Kapsamında Değerlendirilmesine Yönelik Soru Listesi	131
Tablo 10: Literatürdeki Çalışmalarda Yer Verilen Dayanıklılık Stratejileri.....	143
Tablo 11: Standartlarda Yer Verilen Dayanıklılık Stratejileri ile Strateji Benzeri Unsurlar	148
Tablo 12: Literatürdeki Dayanıklılık Stratejilerinin Değerlendirilmesi	149
Tablo 13: Olumsuz Durum Sınıflarına Yönelik Risk Stratejileri.....	168
Tablo 14: Risk ve Dayanıklılık Stratejilerinin Olay Fazlarına Göre Uygulanması	174
Tablo 15: Olumsuz Durum Türleri ve Ait Oldukları Sınıflar	201
Tablo 16: Olumsuz Durum Sınıflarına Göre Uygulanabilir Risk Stratejileri	208
Tablo 17: Risk Stratejilerini Destekleyen Dayanıklılık Stratejileri.....	208

GİRİŞ

Günümüz iş ortamı giderek daha belirsiz, karmaşık ve değişken bir karakter kazanmıştır. Belirsizlik, değişkenlik ve öngörülemezlik, hem ölçeği hem de etkisi bakımından kurumların kontrol kapasitesini aşan olayları daha görünür hale getirmiştir. Nassim Nicholas Taleb (2007) tarafından ortaya konulan ve nadiren gerçekleşen fakat gerçekleştiğinde yıkıcı sonuçlar doğuran ve önceden öngörülemeyen olayları ifade eden siyah kuğular, kuruluşların en güçlü senaryolarını dahi geçersiz kılabilmektedir.

Bir siyah kuğu olarak 2019 yılının sonlarında ilk kez kendini gösteren COVID-19 pandemisi, bir anda tüm dünyada üretim süreçlerini durma noktasına getirmiş, uzaktan çalışma düzenini zorunlu kılmış ve küresel ekonomide büyük dalgalanmalara yol açmıştır.

Küreselleşme, jeopolitik gerilimler, dijitalleşme, iklim değişikliği ve toplumsal dönüşümler, kuruluşların faaliyetlerini öngörülemez belirsizlikler ile çeşitli ve çok boyutlu tehdit ve risklerle karşı karşıya bırakmaktadır.

Örneğin, Rusya-Ukrayna Savaşı ile birlikte Avrupa enerji piyasasında yaşanan ani arz kesintileri, birçok ülkeyi enerji güvenliği sorunlarıyla yüz yüze bırakmıştır. ABD-Çin ticaret gerilimleri, teknoloji sektöründe tedarik zincirlerini kırılgan hale getirmiş, yarı iletken kıtlığı otomotivden elektroniğe kadar birçok endüstride üretimi aksatmıştır.

Ekonomik dalgalanmalar, tedarik zinciri kırılmaları, düzenleyici çerçevelerdeki ani değişiklikler, siber saldırılar ve kriz niteliği taşıyan toplumsal olaylar, kurumların geleneksel risk yönetimi anlayışıyla baş edemeyeceği kadar dinamik bir çevre yaratmaktadır.

2017’de ABD’li kredi raporlama şirketi Equifax’a yapılan siber saldırı, yaklaşık 147 milyon kişinin kişisel verilerinin açığa çıkmasına neden olmuş ve şirketin itibarına ciddi zarar vermiştir. Benzer şekilde, 2021 yılında Ever Given isimli dev konteyner gemisinin Süveyş Kanalı’nı günlerce kapatması, küresel ticaretin yüzde 12’sinin aksamasına ve milyarlarca dolarlık zarara yol açmıştır.

Toplumsal boyutta ise, 2020’de ABD’de George Floyd protestoları, birçok büyük şirketin operasyonlarını durdurmasına ve tedarik zincirlerinde aksamalar yaşamasına yol açmıştır. Türkiye’de 2023’te yaşanan büyük deprem felaketi ise yalnızca bölgesel değil, ulusal ölçekte

ekonomik, lojistik ve sosyal etkiler yaratmış, birçok kuruluşun iş sürekliliği planlarını sorgulamasına neden olmuştur.

Bu belirsiz, değişken ve öngörülemez ortamda kuruluşlar, olumsuz durumları yönetebilmek için geleneksel Kurumsal Risk Yönetimi (KRY) sistemleri ile dayanıklılığın sağlanmasına yönelik çeşitli uygulamaları benimsemektedir.

KRY, ölçülebilir ve hesaplanabilir risklere odaklanan yapısıyla önemli olmakla birlikte, belirsizlikler, ani şoklar, zincirleme etkiler ve sistemik kırılmalıklar karşısında yetersiz kalmaktadır. Örneğin, pandemi veya ani jeopolitik çatışmalar gibi hesaplanabilirlik sınırlarının ötesine geçen siyah kuğu niteliği taşıyan olaylara karşı, KRY etkili olamamaktadır.

Benzer şekilde, diğer bir araç olan Dayanıklılık Yönetimi (DY) de çoğunlukla operasyonel krizlerden sonra gündeme gelmekte, toparlanma süreçleriyle sınırlı kalmakta ve risk–getiri dengesini gözetken stratejik bir bakış açısı sunmamaktadır. Bu nedenle, dayanıklılık uygulamaları çoğu zaman “tepki verme ve iyileşme” boyutunda yoğunlaşmakta, proaktif risk yönetimiyle yeterince bütünleşmemektedir.

KRY ve DY’nin bağımsız kullanımları, kuruluşların yalnızca belirli yönlerden korunmasını sağlamakta; ancak belirsizliğin, değişkenliğin ve öngörülemezliğin hâkim olduğu günümüz iş ortamında kapsamlı bir güvence üretmekten uzaktır. Bu ikili yapı, bir yanda riskleri sistematik olarak analiz edip önlemeye çalışan, diğer yanda yaşanan şoklardan toparlanmaya odaklanan iki ayrı yaklaşım ortaya çıkarmaktadır. Sonuç olarak, kurumlar parçalı, dağınık ve bütünsel değer yaratma kapasitesinden yoksun bir yönetim anlayışıyla hareket etmektedir.

Ancak, iş ortamının anılan dinamikleri, kuruluşları “önleyici ve koruyucu” yaklaşımlara ilave olarak “uyarlanabilir ve stratejik değer yaratıcı” bir bakış açısıyla riskleri, tehditleri ve belirsizlikleri bütünsel bir yaklaşımla yönetmeye zorlamaktadır.

Bu gerekliliğin karşılanması hususunda her iki aracın yetkinliklerinin araştırılması, bağımsız kullanımlarından kaynaklanan sınırlılık ve yetersizliklerinin ortaya çıkarılması gerekmektedir.

KRY ile DY’nin bütünsel bir sistem çerçevesinde bir araya getirilmesi, risk, tehdit ve belirsizliklerin olay öncesinde ele alınarak değerlendirilmesi ve yönetilmesi ile olay sonrasında toparlanma süreçlerinin daha etkin şekilde yürütülmesine olanak sağlayacaktır. Bu tür bir entegre yapı, yalnızca önleyici ve koruyucu mekanizmaları güçlendirmekle kalmayacak, aynı zamanda uyarlanabilir ve yenilikçi stratejilerin uygulanmasını da mümkün kılacaktır.

Bütünleşik yapı, hem önleyici ve koruyucu mekanizmaları güçlendirecek, hem de uyarlanabilir ve yenilikçi stratejilerin hayata geçirilmesini sağlayacaktır.

Bu doğrultuda, mevcut literatür çerçevesinde hâlihazırda kullanılan KRY ve DY'nin kavramsal çerçeveleri ile pratikteki uygulamaları dikkate alınarak aşağıdaki soruların yanıtları aranacaktır.

- i. Olumsuz durum ve olayların, olay öncesi, anı ve sonrasını bir bütün halinde sürekli olacak şekilde yönetilmesi bağlamında KRY ve DY'nin yetersizlik ve sınırlılıkları nelerdir?
- ii. Literatürde, öncüllük-ardıllık, tamamlayıcılık ve kapsayıcılık gibi hususlar açısından KRY ile DY arasındaki ilişkiler nasıl tanımlanmaktadır?
- iii. Risklerle birlikte tehdit ve belirsizliklere karşı dayanıklılığın güçlendirilmesine yönelik mevcut strateji ve araçlar nelerdir? DY'ye yönelik strateji ve araçlar, KRY çalışmalarına nasıl dâhil edilebilir?
- iv. Kuruluşlarda KRY ve DY'nin birlikte yönetilebilmesi amacıyla 'yeni bir 'Dayanıklılık Odaklı KRY Modeli'nin geliştirilmesi, olumsuz durumların etkin bir şekilde yönetilmesi açısından nasıl bir katma değer yaratabilir?
- v. Dayanıklılık Odaklı KRY Modelinde yer alması gereken ana bileşenler, modelin işleyişi, kullanılabilecek araç ve yöntemler nelerdir?

Bu çalışmada, olumsuz durum ve olayların kuruluşlar tarafından yönetilebilmesi amacıyla kullanılabilecek, KRY ve DY'yi bünyesinde sentezleyen bir aracın geliştirilmesi amaçlanmaktadır. Bu bağlamda, araştırma KRY'nin sunduğu sistematik ve ölçülebilir risk yönetim çerçevesi ile DY'nin önleme, koruma ve toparlanma kapasitelerinin bütünleştirilmesini hedeflemektedir.

Çalışmanın önemi, kuramsal ve uygulama boyutlarında görülmektedir. Kuramsal açıdan, KRY ve DY'nin tek başlarına sahip oldukları sınırlılıkları aşacak özgün bir çerçeve sunulmaktadır. Uygulama boyutunda ise, önerilen model kuruluşlara proaktif durum yönetimi, olay, kriz anında etkin müdahale ve kriz sonrası güçlenerek çıkma kapasitesi hususlarında bütüncül bir bakış açısı ve yönetim imkânı kazandırmaktadır.

Çalışma, bu yönüyle küresel ölçekte artan belirsizlikler, karmaşık tehditler ve öngörülemeyen olumsuz durum ve olaylarla dolu günümüz iş dünyasında kuruluşların

sürdürülebilirliğine, stratejik esnekliğine ve rekabet avantajına katkı sağlayacak bir yol haritası sunmaktadır.

Önerilen Dayanıklılık Odaklı KRY Modeli, geleneksel KRY ve DY yaklaşımlarının sınırlılıklarını aşarak, kurumlara hem belirsizlik ve tehditlere karşı daha güçlü bir koruma hem de rekabet avantajı yaratacak stratejik bir esneklik sağlamayı hedeflemektedir.

Araştırma, kuruluşların risk, tehdit ve belirsizlikler ile krizlerin önlenmesi, gerçekleşmesi durumlarına yönelik olumsuz etkilerinin azaltılması ve toparlanma süreçlerinin yönetilmesi ihtiyacı ve gerekliliğini merkeze alarak KRY, DY, Kriz Yönetimi ve İş Sürekliliği Yönetimi'ne ilişkin (İSY) akademik literatür üzerine inşa edilmiştir.

Teorik altyapı, söz konusu literatüre ilave olarak uluslararası genel kabul gören standart ve çerçevelere dayanmaktadır. Bu kapsamda araştırma, KRY'ye ilişkin COSO KRY (2018) çerçevesi ve ISO 31000:2018 Risk Yönetimi standardına dayanmaktadır. Diğer taraftan araştırma, DY'ye yönelik ANSI/ASIS (2009) tarafından yayımlanan Organizasyonel Dayanıklılık, ISO tarafından yayımlanan ISO 22301:2019 Güvenlik ve Dayanıklılık – İş Sürekliliği Yönetim Sistemleri – Gereklilikler ve BSI tarafından yayımlanan BS 65000:2022 Organizasyonel Dayanıklılık — Uygulama Kodu Standartlarına dayanmaktadır.

Bu araştırma, kavramsal bir model geliştirmeyi amaçlayan nitel bir çalışma olarak tasarlanmıştır. Çalışmanın temel yöntemi literatür taraması, içerik analizi ve kavramsal sentez süreçleri ile modelin geliştirilmesi üzerine kuruludur.

Bu doğrultuda KRY ve DY üzerine akademik araştırmalar ile uluslararası standartlar detaylı analiz edilmiştir. Söz konusu analizden elde edilen kavramlar derlenmiş ve ilkeler, kapasiteler ve stratejiler oluşturulmuştur. Kavramlar arasındaki ilişkiler, benzerlikler ve boşluklar belirlenmiştir.

Bu ilişkiler bağlamında KRY'nin sınırlılıkları ile DY'nin eksiklikleri analiz edilerek karşılaştırılmıştır. İki yaklaşımın birbirini tamamlayan boyutları ortaya konmuştur. Bu analizlerin sonucunda model için gerekli bileşenler tanımlanmıştır. Böylece risk yönetiminin sistematik yapısı ile dayanıklılık bütünleştirilerek özgün bir çerçeve olarak Dayanıklılık Odaklı Kurumsal Risk Yönetimi (DOKRY) modeli geliştirilmiştir.

Araştırma, bu yönüyle kavramsal bir çerçeve sunmakta olup, ampirik doğrulamanın ileride yapılacak saha araştırmalarıyla test edilmesi öngörülmektedir.

Tez çalışması, KRY ve DY'ye yönelik kavramsal çerçevenin çizildiği literatür ağırlıklı ilk iki bölüm ile önerilen modelin alt modüllerinin inşa edildiği ve modelin olgunlaştırıldığı üç uygulama bölümden oluşmaktadır.

Birinci bölümde KRY'nin teorik çerçevesi detaylandırılmakta olup, riske yönelik davranışsal ve yönetsel unsurlar ile risk yönetim süreci açıklanmaktadır. KRY'nin kuruluşlara sağladığı faydalar ile uygulamadaki zorluklar incelenmektedir.

İkinci bölümde DY'ye yönelik literatür analizi kapsamında dayanıklılık ve kurumsal dayanıklılık kavramları ele alınmakta, kurumsal dayanıklılığa ilişkin kapasitelere değinilmektedir. Kurumsal dayanıklılık süreci ile kurumsal dayanıklılığın unsurlarına ilave olarak dayanıklılık kapasitesinin artırılması hususlarına yönelik bilgilere yer verilmektedir. Bu bölümün son kısmında DY'nin uygulamadaki zorlukları araştırılmaktadır.

Üçüncü bölümle birlikte modelin oluşturulmasını teminen risk ve dayanıklılığın birlikte yönetilmesi kapsamında kuruluşların karşılaştığı olumsuz durum türleri ile bu durum türlerine ilişkin yönetim araçları konuları detaylandırılmaktadır. İlave olarak KRY ve DY arasındaki ilişkilerin tanımlanarak bütünsellik arz eden bir durum ve olay yönetiminin sağlanması bakımından araçların yetersizlikleri ve sınırlılıkları ortaya çıkarılmaktadır.

Dördüncü bölüm dayanıklılık stratejilerine yönelik literatür analizi ile başlamakta, analiz sonucunda kuruluşların uygulayabileceği dayanıklılık stratejileri derlenmekte ve açıklanmaktadır. Olumsuz durum türleri doğrultusunda kullanılabilecek risk stratejileri ile bu stratejileri destekleyecek dayanıklılık stratejileri belirlenmektedir. Yine bu aşamada durum ve olaylara yönelik müdahale fazları ile strateji ve eylemlerin devreye alınması hususlarına yönelik bilgiler sunulmaktadır. İlave olarak bu bölümde risk ve destekleyici dayanıklılık stratejilerinin belirlenmesine yönelik örnekler verilmektedir.

Tezin beşinci bölümünde, üçüncü ve dördüncü bölümler dikkate alınarak dayanıklılık odaklı bir kurumsal risk yönetimi modeli oluşturulmaktadır. Modele yönelik amaç ve kapsam bilgileri ile modeli oluşturan bileşenler, modelin işleyişindeki roller ve sorumluluklar açıklanmaktadır. Ardından modelin işleyişi ve uygulama süreci aşama ve alt adımlar şeklinde detaylandırılmaktadır. Modelden beklenen değer ve katkılar aktarılmaktadır.

Sonuç ve Öneriler Bölümü'nde ise önerilen modelin literatür ve uygulamaya katkıları ile uygulanabilirliği, sınırları ve geleceğe dönük yönlerini irdelenmektedir.

BİRİNCİ BÖLÜM

KURUMSAL RİSK YÖNETİMİ

1.1. Kurumsal Risk Yönetimi

Risk kavramı, ISO 31000 Risk Yönetimi standardında (2018) “belirsizliğin hedefler üzerindeki etkisi” şeklinde tanımlanmaktadır. Risk terimi, belirli bir olayın gerçekleşmesiyle öngörülen olumsuz bir sonucun ortaya çıkma olasılığını ifade etmektedir.

Belirsizlik ve risk, tüm kuruluşlar için kaçınılmaz bir gerçektir (Marchetti, 2012). Risk kavramı, hedefleri olumsuz etkileyebilecek sosyal, ekonomik, finansal ve çevresel durumları kapsar. Risklerin niteliği, kuruluşun faaliyet alanlarına göre farklılık gösterir.

Günümüzde işletmeler ve bireyler, bilinçli kararlar almak için yapılandırılmış yaklaşımlar ve araçlar gerektiren çok çeşitli risklerle karşı karşıyadır (Moeller, 2007). Kuruluşlar, belirsizlik ve risklere neden olan çevresel değişikliklerle yüzleşmek zorunda kalmakta; rekabet avantajı elde etmek için uygun yönetim metodolojilerine ihtiyaç duymaktadır (Blanco-Mesa vd., 2019).

Risk yönetimi, riskleri sistematik olarak değerlendirme, ölçme ve bunlara yanıt verme sürecidir (Moeller, 2007). Özellikle birden fazla lokasyona sahip, uluslararası faaliyet gösteren, dış ortaklara bağlı ya da çeşitli iş kollarında faaliyet gösteren kuruluşlar açısından risk yönetimi hayati önem taşır (Gregory, 2003).

Kurumsal Risk Yönetimi (KRY), farklı standartlar ve kuruluşlar tarafından çeşitli şekillerde tanımlanmıştır. Uluslararası İç Denetçiler Enstitüsü (IIA) (2004), KRY’yi “bir kuruluşun stratejik ve finansal hedeflerinin gerçekleştirilmesini etkileyen tüm riskleri değerlendirme ve bunlara yanıt verme konusunda titiz ve koordineli bir yaklaşım” olarak tanımlarken; Risk Yönetim Topluluğu (RIMS) (2011), KRY’yi “bir kuruluşun risklerinin tümünü ele alarak ve bu risklerin birleşik etkisini birbiriyle ilişkili bir risk portföyü olarak yöneterek kuruluşun hedeflerine ulaşmasını destekleyen stratejik bir iş disiplini” olarak tanımlamaktadır. COSO KRY (2018) çerçevesinde kavram, “kuruluşların strateji belirleme ile entegre ettikleri ve bu stratejiyi uygularken, değer yaratma, koruma ve gerçekleştirme sürecinde riskleri yönetmek amacıyla uyguladıkları kültür, yetkinlikler ve uygulamalar” şeklinde açıklamaktadır. ISO 31000 (2018) ise daha genel bir yaklaşımla risk yönetimini, “risklere

ilişkin olarak bir kuruluşu yönlendirmek ve kontrol etmek için gerçekleştirilen koordineli faaliyetler” olarak tanımlamaktadır. KRY tanımları kaynaklara göre kısmen farklılık gösterebilse de, yapılandırılmış bir risk yönetimi süreci, risklere ilişkin birleşik bir bakış açısı ve riskler ile stratejik hedefler arasında bağlantı gibi temel unsurları tutarlı bir şekilde içerir (Marchetti, 2012).

KRY, başlangıçta silo yapısında yürütülen geleneksel risk yönetimi anlayışının sınırlılıklarına bir yanıt olarak gelişmiştir (Chapman, 2012; Ibrahim & Esa, 2017). Silo bazlı risk yönetimi yaklaşımı, her bir riski izole şekilde yönetirken; KRY, riskler arasındaki ilişkileri dikkate alan entegre bir yönetim yaklaşımı sunar (Nocco & Stulz, 2006). KRY, kuruluşun tüm risklerini bütüncül bir sistemle yönetmesini sağlayarak, geleneksel modellerdeki izole risk odaklılıktan farklı olarak kapsamlı bir risk görünümü sunar (Green, 2016).

KRY, operasyonel ve stratejik riskleri yönetmek üzere entegre bir çerçeve olarak 21. yüzyılda gelişmiştir (Masood vd., 2020). KRY, krizler, düzenlemeler ve yatırımcı beklentileri gibi etkenlerle küresel ölçekte benimsenmiş ve zamanla periyodik değerlendirmelerden gerçek zamanlı iç görü sunan dinamik bir yapıya dönüşmüştür (Lam, 2017). Bu yaklaşım, riskleri bütüncül biçimde ele alarak genel kontrolü güçlendirmekte, maliyetleri azaltmakta ve kuruluşun değerini artırmaktadır (Togok & Zainuddin, 2014).

KRY, kuruluş çapında tüm önemli risklerin belirlenmesi, yönetilmesi ve raporlanmasını içerir (Hunziker, 2019). Bu süreç, stratejik, finansal, operasyonel, uyum ve itibar risklerini kapsar (Lam, 2017). Riskler, içsel hatalar ya da dış faktörlerden kaynaklanabilir (Assibi, 2022). Sürekliliği sağlanan bir KRY, değişen risk ortamına uyumu sağlar; bu yolla risk stratejileri dışsal değişimlere hızla uyulanır ve kurumsal dayanıklılık artırılmış olur (Lam, 2017).

KRY, farklı risk kategorilerinin belirlenmesini, risklerin azaltılmasını ve izlenmesini sağlayan strateji ve faaliyetler bütünüdür (Sprčić vd., 2015). Bu bakımdan kapsamlı ve entegre bir çerçeve sunar (Chapman, 2012). Olumlu ve olumsuz sonuçlara sahip belirsizlikleri tespit etmeye odaklanır (Hopkin & Thompson, 2022).

KRY, risk iştahı çerçevesinde potansiyel olayları yöneterek iş hedeflerine ulaşma konusunda makul güvence sağlar (Protiviti, 2006). Risklerin karşılıklı bağımlılıklarını dikkate alarak, kaçınma yerine optimize edilmiş risk alımını destekler (Lam, 2017).

KRY’nin temel amacı, kuruluşun hedeflerine ulaşma şansını artırmaktır. KRY, temelde hissedar değerini korumak ve artırmakla ilgilenir (Sprčić vd., 2015). Marchetti’ye (2012) göre KRY, strateji ile risk iştahını uyumlu hale getirerek kayıpları azaltmayı, risklere bütüncül

yaklaşarak proaktif kararları desteklemeyi ve kaynak kullanımını optimize ederek operasyonel verimliliği artırmayı amaçlar. Bu, yalnızca nicel analizle değil, aynı zamanda yönetsel deneyim ve içgörüyle gerçekleştirilir (Marchetti, 2012).

Lam (2014), başarılı bir KRY programının yedi temel bileşenden oluştuğunu belirtmektedir. Bunlardan ilki, yönetim kurulu ve üst yönetim tarafından yürütülen kurumsal yönetişimdir. Risk yönetimi iş süreçlerine entegre edilirken; portföy yönetimi, risklerin topluca değerlendirilmesini ve çeşitlendirilmesini sağlar. Yüksek maliyetli riskler sigorta veya dış kaynak yoluyla transfer edilir. Risk analitiği, ölçüm ve analiz araçları sunarken; veri ve teknoloji, raporlama ve izleme işlevlerini destekler. Son olarak, paydaş yönetimi risk bilgilerinin şeffaf biçimde iletilmesini amaçlar (Lam, 2014).

Hopkin ve Thompson'a (2022) göre, KRY kabul edilebilir risk seviyelerinin belirlenmesini ve iç iletişim ile denetimin güçlendirilmesini sağlar. Ayrıca, hissedar değerini yükseltir ve risk iletişimini güçlendirir.

Risk eşiklerini tanımlayan, riskleri değerlendiren ve risklere maruz kalma durumunu aktif olarak izleyen ve yöneten kuruluşlar iş performansını genelde daha doğru tahmin edebilir (Marchetti, 2012). Bu yaklaşımda, risklerin belirlenmesi ve azaltılması, kuruluşun açıkça ifade ettiği risk iştahı tarafından şekillendirilir (Masood vd., 2020). Beklenmedik performans farklılıkları ile öngörülemeyen sonuçları ve kayıpları en aza indirmeyi amaçlayan KRY, kuruluşun değerini en üst düzeye çıkarmaya odaklanır (Lam, 2017).

1.2. KRY'yi Zorunlu Kılan Etmenler

Düzenleyici ve kurumsal baskılar, KRY'nin benimsenmesinin başlıca itici güçleri arasındadır. Sarbanes-Oxley Yasası gibi yasal zorunluluklar, kuruluşları uyum amacıyla KRY'yi uygulamaya zorlamıştır (Renault vd., 2016). Özellikle finans sektöründeki düzenleyici gereklilikler bu eğilimi daha da güçlendirmektedir (Bohnert vd., 2019). Bankacılık ve sigortacılık gibi sektörlerde, kurumsal beklentiler ve uyum gereklilikleri KRY'nin benimsenmesini motive etmede kritik bir rol oynamaktadır (Florio vd., 2022).

Ayrıca, COSO gibi zorunlu olmayan çerçeveler KRY'yi iyi yönetim uygulaması olarak teşvik etmekte (Renault vd., 2016); Cadbury ve King Raporları gibi raporlar KRY'nin kurumsal gözetimdeki rolünü vurgulamaktadır (Khan vd., 2016). Bu güçlerin birleşimi, KRY'yi hem

düzenleyici bir gereklilik hem de bir yönetim standardı olarak konumlandırmaktadır (Nocco & Stulz, 2006).

Küresel piyasalardaki artan karmaşıklık ve belirsizlik, kuruluşları daha kapsamlı sistemler olan KRY'ye yöneltmiştir. Hammaddede fiyatları, düzenleyici değişiklikler ve rekabet baskıları gibi küresel istikrarsızlık unsurları, iş sürekliliğini tehdit etmektedir (Renault vd., 2016; Hunziker, 2019). Teknolojik gelişmeler ve piyasa birleşmeleri gibi etkenler de KRY'nin benimsenmesini desteklemektedir (Khan vd., 2016). Kuruluşlar giderek daha dinamik ortamlarda faaliyet gösterirken, özellikle birbiriyle bağlantılı riskler ve finansal yenilikler karşısında, geleneksel, silo benzeri risk yaklaşımlarının sınırları ortaya çıkmaktadır (Nocco & Stulz, 2006).

Kuruluşların iç dinamikleri, KRY'yi benimseme kararlarında belirleyici rol oynamaktadır. Güçlü büyüme beklentileri veya zayıf finansal performans gibi faktörler, riski azaltmak ve yatırımcı güveni sağlamak amacıyla KRY'yi teşvik etmektedir (Khan vd., 2016). Ayrıca, kuruluşun büyüklüğü ve operasyonel karmaşıklığı arttıkça, sistematik ve entegre risk yönetimi ihtiyacı da artmakta, bu da KRY uygulamalarını yaygınlaştırmaktadır (Bohnert vd., 2019).

Yönetişim yapıları ve üst yönetimin katılımı, KRY'nin benimsenmesinde belirleyici rol oynamaktadır. Yönetim kurulu yapısı, risk komiteleri ve iç denetim sistemleri KRY uygulamalarını şekillendirmektedir (Florio vd., 2022). Bağımsız yönetim kurulları ve yerleşik denetim organlarına sahip kuruluşlar daha yapılandırılmış sistemler geliştirme eğilimindedir (Bohnert vd., 2019). Yönetim desteği, KRY'nin uygulanmasında temel bir itici güç olarak öne çıkmakta; yönetim kurullarının risk yönetiminin önemini fark etmesi, uygulamaların kapsamlı şekilde benimsenmesini kolaylaştırmaktadır (Nocco & Stulz, 2006).

KRY'nin benimsenmesinde ücretlendirme yapıları, yönetsel algılar ve sahiplik modeli gibi iç dinamikler belirleyici rol oynamaktadır. Yöneticilerin çıkarlarını uzun vadeli performans hedefleriyle uyumlu hale getiren teşvik sistemleri, risk yönetimini teşvik etmektedir (Bohnert vd., 2019). Yöneticilerin riske ve belirsizliğe yaklaşımlarının yanı sıra sahiplik yapısı da (örneğin aile ve kamu şirketleri gibi farklı paydaş beklentilerine sahip yapılar) KRY'nin gelişimini ve davranışlarını etkilemektedir (Florio vd., 2022). Kurumsal yatırımcıların veya kamu mülkiyetinin varlığı ise daha resmi ve şeffaf KRY sistemlerini teşvik etmektedir (Bohnert vd., 2019).

KRY, farklı risk perspektiflerini entegre ederek parçalı yönetim yaklaşımlarının yarattığı verimsizliklere çözüm sunar. Kuruluşlarda risklerin genellikle hazine, BT veya uyum gibi ayrı birimlerde silolar şeklinde yönetilmesi, koordinasyon eksikliği ve kaynak israfına yol açmaktadır (Protiviti, 2006). Bu durum, tehditlere bütüncül yanıt verilmesini engellerken operasyonel yükü de artırmaktadır (Nocco & Stulz, 2006; Togok & Zainuddin, 2014). COSO KRY (2004) çerçevesi, 11 Eylül ve küresel finansal kriz sonrası geleneksel araçların yetersizliğini ortaya koyarak bütüncül risk yönetimine geçişte önemli bir dönüm noktası olmuştur (Hunziker, 2019). KRY, bu bağlamda kurumsal risklerin koordineli şekilde yönetilmesi için stratejik bir zorunluluk olarak öne çıkmaktadır.

Literatür, KRY'nin değer yaratma ve kurumsal performansı iyileştirmedeki rolünü vurgulamaktadır. KRY, stratejik davranışları risk profiliyle uyumlu hale getirerek açık, risk bilincine sahip bir kültür oluşturur ve çalışanların endişelerini rahatça ifade etmesini sağlar (Protiviti, 2006). Şeffaflığı artırarak paydaş güvenini destekler ve risk raporlaması, kaynak tahsisi ve kontrolü yoluyla memnuniyeti artırır (Renault vd., 2016). Riskler arası bağımlılıkları dikkate alarak stratejik planlamayı geliştirir ve risk iştahına uygun çeşitlendirmeyi mümkün kılar (Hunziker, 2019). Ampirik çalışmalar, KRY'nin yatırımcı güveni, şirket değeri ve finansal performans üzerinde olumlu etkileri olduğunu göstermektedir (Hunziker, 2019). Risklerin ve fırsatların dengeli yönetimi sayesinde karar alma süreçleri gelişir; kazanç oynaklığı azalır ve kârlılık artar (Renault vd., 2016). Krizleri önceden tespit ederek iş sonuçlarında tutarlılık sağlar, dış değişimlere hızlı yanıt verir ve yönetim yapısını güçlendirir (Protiviti, 2006). Son olarak, sermaye maliyetlerini azaltarak ve risk-getiri dengelerini optimize ederek değer maksimizasyonuna katkıda bulunur (Nocco & Stulz, 2006).

KRY'nin benimsenmesi, sektörlerin özgün risk profillerine bağlıdır. Yüksek risk maruziyetine sahip sektörlerdeki kuruluşlar, bu riskleri yönetmek için KRY sistemlerine daha yatkındır (Bohnert vd., 2019). Özellikle belirsizlik ve oynaklığın yüksek olduğu finans ve enerji gibi sektörler, daha kapsamlı KRY çerçeveleri geliştirme eğilimindedir (Florio vd., 2022). Bu durum, sektöre özgü dinamiklerin KRY uygulamalarını motive ettiğini göstermektedir.

Gelişmiş bilgi teknolojileri, KRY'nin benimsenmesini destekleyen önemli bir unsur olmuştur. Risk modelleme ve veri analizine imkân tanıyan BT araçları, belirsizliğin etkin yönetimini kolaylaştırır (Renault vd., 2016). Ancak birçok kuruluş, hızla değişen risklere yanıt vermede yetkinlik eksiklikleri yaşamaktadır (Togok & Zainuddin, 2014). Modern risk ortamının karmaşıklığı, bu ihtiyacı daha da artırarak, teknolojik açıdan gelişmiş ve yetkinlik temelli KRY çerçevelerine olan gereksinimi ortaya koymaktadır.

Büyük yıkıcı olaylar, firmaların KRY'yi benimsemelerinde kritik bir itici güç olmuştur. 11 Eylül (2001), Japonya depremi (2011), Bangkok seli (2011) ve Euro krizi (2009-2012) gibi felaketler, geleneksel yaklaşımların yetersizliğini ortaya koymuş ve entegre, ileriye dönük sistemlere duyulan ihtiyacı artırmıştır (Togok & Zainuddin, 2014). Bu gelişmeler, KRY'nin yalnızca stratejik değil, aynı zamanda sistemik şoklara karşı koruyucu bir araç olarak da görülmesini sağlamıştır.

1.3. Risk Yönetiminde Davranışsal ve Yönetmel Unsurlar

KRY, yalnızca teknik veya prosedürel bir işlev değildir; bireylerin ve grupların davranışlarına, tutumlarına ve karar verme tercihlerine derinlemesine yerleşmiştir. Risk modelleri ve çerçeveleri yapısal ve içsel tutarlılık sağlarken, bunların gerçek etkinliği, risklerin kuruluşun tüm kademelerindeki çalışanlar tarafından nasıl anlaşıldığına, yorumlandığına ve bunlara göre nasıl hareket edildiğine bağlıdır. Kuruluş genelindeki davranışsal ve yönetmel faktörler, risklerin tanımlanma, değerlendirilme ve yanıtlanma şekillerini belirler.

Bu bölümde, risk algısı, risk tutumu, risk iştahı, risk toleransı, risk kapasitesi, risk kültürü ve risk iletişimi dâhil olmak üzere, bir kuruluşun risk yönelimini toplu olarak tanımlayan temel unsurlar ele alınmaktadır. Anılan unsurlar, bireylerin ve kurumların riskleri algılama ve yanıtlama biçimlerinin şekillendirilmesinde birbirleriyle ilişkili farklı roller oynamaktadır.

1.3.1. Risk Algısı

Risk algısı, yaygın bir şekilde çeşitli kişisel, sosyal ve bağlamsal faktörlerin şekillendirdiği öznel bir kavram olarak kabul edilmektedir. Kavram, bireylerin veya grupların kişisel değerleri, endişeleri ve içinde bulundukları durumlardan kaynaklı etkiler temelinde potansiyel tehditleri nasıl değerlendirdiklerini ifade etmektedir (Molak, 1997; Cooper vd., 2005; Lucarelli, 2011; Greiman, 2013). Bu algılar, algılanan risk üzerindeki kontrol gücü, rıza, geçmiş deneyimler, iletişim kalıpları ve risklerin algılanan ciddiyeti veya bilinmezliği gibi unsurlar tarafından etkilenir (Molak, 1997; Cooper, 2003). İki temel psikolojik boyut olan belirsizlik ve korku, risk yargılarını sıklıkla şekillendirir (Lucarelli, 2011). Risk algısı, kuruluşlar içinde büyük farklılıklar gösterir; bu nedenle yöneticilerin önyargıların risk değerlendirmelerini nasıl çarpıtabileceğini ve hatalı kararlara yol açabileceğini anlamaları önem arz etmektedir (AIRMIC, 2018). Bu farklılıkları anlamak, risklerin daha doğru bir şekilde

önceliklendirilmesini ve kaynakların daha doğru tahsis edilmesini sağlar (Greiman, 2013). Bu nedenle öznel algıları, kuruluşun risk gerçekleriyle uyumlu hale getirmek için eğitim ve farkındalık girişimleri ihmal edilmemelidir (Greiman, 2013).

1.3.2. Risk Tutumu

Risk tutumu, algı tarafından şekillendirilen ve iç ve dış faktörlerin etkisiyle belirsizliğe verilen bağlama bağlı ve dinamik bir tepkidir (Hillson, 2009). IRM (2012), risk tutumunu, risk kültürünün üç temel bileşeninden biri olarak “risk algısının etkisiyle bir birey veya grubun risk karşısında benimsediği tutum” şeklinde tanımlamaktadır. Kavram, bir bireyin veya grubun riski almaya, kaçınmaya veya riske karşı tarafsız kalmaya yönelik eğilimini yansıtır (Fraser & Simkins, 2010; Hunziker, 2019). Organizasyonel düzeyde, bir kuruluşun riski nasıl değerlendirdiğini ve riske girmeye veya riskten kaçınmaya nasıl karar verdiğini tanımlar (ISO, 2009; Ketcham & Louisot, 2014) ve riske karşı değişen bireysel tepkiler nedeniyle iş başarısında hayati bir rol oynar (Chong & Brown, 2000).

Risk tutumunu etkileyen temel faktörler arasında kurumsal paydaşların tercihleri (Olson & Wu, 2020), uyumu teşvik eden sosyal baskılar (Cooper, 2003) ve riskten kaçınma veya risk alma davranışı gibi bireysel özellikler sayılabilir (Hunziker, 2019).

Kuruluşların risk tutumları, risk kriterlerinin belirlenmesini ve risklere yönelik kararların alınmasını yönlendirir (Lark, 2015). Risk değerlendirmeleri, bu tutumla uyumlu olmalıdır (Hopkin & Thompson, 2022).

Risk tutumlarının kuruluşun hedeflerine bağlı olmasına istinaden, farklı bağlamlar için ortak bir yaklaşım yoktur. Chong ve Brown (2000) ve Hillson (2009), bireylerin veya grupların belirsizliğe karşı bilişsel ve davranışsal tepkilerine göre risk tutumunu dört ana sınıf altında toplamaktadır.

1. Duygusal Yönelim – Riskten Kaçınma: Bireyler ya da gruplar belirsizliğe karşı duygusal rahatsızlık duyar, istikrar ve rutini tercih eder ve tehditleri abartırken fırsatları küçümseme eğilimindedir.
2. Keşif Yönelim – Risk Arayışı: Potansiyel kazançlar tarafından motive edilen risk arayışında olan bireyler ya da gruplar, belirsizliğe proaktif olarak yaklaşır, genellikle tehditleri küçümser ve büyüme için spekülasyon girişimleri benimser.

3. Bilişsel Yönelim – Risk Bilinci / Risk Tarafsızlığı: Risk bilincine sahip bireyler ya da gruplar, objektif analiz ve uzun vadeli sonuçlara öncelik vererek rasyonel ve duygusal olarak tarafsız bir bakış açısını korur.
4. Pasif Yönelim – Risk Toleransı / Risk Bilinci Yok: Risk toleransı olan bireyler ya da gruplar belirsizliği duygusal tepki göstermeden kabul ederken, risk bilinci olmayan bireyler ya da gruplar riskleri ihmal eder veya farkında olmazlar, bu da rehavete veya güvensiz kararlara yol açabilir.

1.3.3. Risk İştahı

Risk iştahı, bir kuruluşun hedeflerine ulaşmak için kabul etmeye hazır olduğu risk düzeyini ifade etmektedir. Orange Book (2004) ve IRM (2011) bu iştahı, eylem gerektirmeden önce kabul edilebilir risk eşiği olarak tanımlarken; Green (2016), kabul edilebilir riskin boyutu olarak tanımlamaktadır. Chapman (2012) ise tercih, tolerans ve kapasite ile ilişkilendirmektedir.

Stratejik düzeyde risk iştahı, hedeflerin gerçekleştirilmesi için kabul edilebilir risk düzeyini tanımlar ve risk felsefesini eyleme geçirilebilir eşiklere dönüştürür (Marchetti, 2012). Stratejik tutarlılık ve hesap verebilirliği sağlamak için daha geniş karar alma süreçlerine entegre edilmelidir (Hopkin & Thompson, 2022). Strateji formülasyonu, kuruluşun risk iştahını yansıtmalı ve yönetim, hedefler, misyon ve kabul edilen risk düzeyleri arasında uyumu sağlamalıdır (Marchetti, 2012).

Risk iştahı, risk yönetiminin stratejik hedeflerle uyumunu destekler. Bir kuruluşun yeteneklerine ve paydaşlarının beklentilerine göre üstlenilebileceği risk düzeyini yansıtır (IMA, 2011). Risk kriterlerine dâhil olan risk iştahı, değerlendirme ve riske yönelik strateji kararlarına rehberlik eder (Fraser & Simkins, 2010). Risk stratejisinin temel bir parçası olarak, risk iştahını tanımak, hem tehditlere hem de fırsatlara etkili bir şekilde yanıt vermek bakımından oldukça önemlidir (Chapman, 2012).

Risk iştahı, organizasyonel dinamikler ve özellikle üst yönetimin tercihleri doğrultusunda şekillenir (Marchetti, 2012). İstenen getiriler, etik ve stratejik hedefler gibi unsurlar da bu süreci etkiler; finansal riskler genellikle daha tolere edilebilirdir (Green, 2016).

Risk iştahı, genellikle politika temelli sınırlarla niteliksel (örneğin yüksek, orta ve düşük) veya niceliksel (örneğin gelir/gider yüzdesi) biçimlerde ifade edilir (Marchetti, 2012). Her risk,

bu belirlenen eşiklere göre değerlendirilir. Stratejik düzeyde risk iştahı, yönetim kurulu için politika niteliğindedir; operasyonel düzeyde ise yöneticilerin bu sınırlara uyması beklenir (Hopkin & Thompson, 2022).

Kuruluşlar, risklerini kendi kapasiteleri dâhilinde yönetmeli ve kapasitelerini aşan diğer risklerini transfer etmelidir (Wu & Olson, 2008). Dinamik, hedefe yönelik bir risk iştahı, KRY için hayati önem taşımaktadır (Lam, 2017). Risk yanıtları, riskin tanımlanan iştahı aşıp aşmadığına bağlı olarak belirlenir; ancak birçok kuruluş bu sınırları netleştirmekte zorlanmakta ve bazı durumlarda iştahın ötesindeki riskler de kabul edilebilir görülmektedir (Hopkin & Thompson, 2022).

1.3.4. Risk Toleransı

Risk toleransı, “bir kuruluşun hedeflerine ulaşmak için kabul etmeye istekli olduğu veya kabul edebileceği risk düzeyini” ifade eder. Hunziker (2019), tanımında riskin sürdürülemez hale gelmeden önce riskin ne kadar tolere edilebileceğini vurgulamaktadır.

Risk toleransı, organizasyon genelinde kabul edilebilir riskler için kuruluş tarafından kabul edilmiş resmi sınırların belirlenmesini gerektirir (Moeller, 2007). Bu bağlamda tolerans, risklerin kabul edilemez hale geldiği eşiği tanımlar ve kontrol önlemlerinin uygulanıp uygulanmayacağına ilişkin rehberlik eder (Engemann & Henderson, 2012; Greiman, 2013).

Risk toleransı, ihlal edildiğinde eylemi tetikleyen belirli üst ve alt sınırları tanımlar (Lam, 2014; Hopkin & Thompson, 2022). Birimler arasında toleransların uyumlu hale getirilmesi, farklı risklere ilişkin toleransların genel iştah sınırları içinde kalmasını sağlar (IMA, 2011) ve hedeflerin gerçekleştirilme olasılığını artırır (COSO, 2004). İş birimleri içinde belirlenen risk eşikleri, aşıldığında önceden tanımlanmış yanıtlar tetiklenir (Murray-Webster & Williams, 2010).

Genellikle nicel olan tolerans seviyeleri, riskler ile anahtar risk göstergelerinin değerlendirilmesinde bir eşik görevi görür (Lam, 2014) ve riske yönelik müdahale gerekip gerekmediğini gösterir. Toleransın belirlenmesine yönelik standart bir formül bulunmadığından, kuruluşlar stratejik hedefleri, risk tutumları, kapasiteleri ile maliyet-fayda faktörlerini dikkate almalıdır (Fraser & Simkins, 2010). Bu tanımlanan tolerans aralıklarının aşılması, eylem gerekliliğini işaret eder (AICPA, 2018; Yoe, 2019).

Yasal veya düzenleyici gereklilikler, risk tolerans seviyesini etkileyebilmektedir (ISO Kılavuz 73:2009). Hedeflerin açık bir şekilde ifade edilmesine ilave olarak yönetimin yasal yükümlülükleri, yönetişimi, organizasyonel yapıyı ve yetkinlik beklentilerini dikkate alması, risklerin belirlenmesi ve uygun risk tolerans eşiklerinin belirlenmesi için gereklidir (Dinapoli, 2016).

1.3.5. Risk Kapasitesi

Risk kapasitesi genel olarak, bir kuruluşun stratejik ve operasyonel hedeflerine ulaşma yeteneğinden ödün vermeden dayanabileceği maksimum risk seviyesi olarak tanımlanır. Murray-Webster ve Williams’a (2010) göre risk kapasitesi, “bir kuruluşun veya kuruluşun bir alt kümesinin, itibarı, sermayesi, varlıkları ve ek fon sağlama yeteneği gibi faktörlerle bağlantılı olarak taşıyabileceği maksimum risk miktarı”dır. COSO (2018), benzer şekilde risk kapasitesini, “bir kuruluşun strateji ve iş hedeflerini gerçekleştirirken üstlenebileceği maksimum risk miktarı” olarak tanımlamakta ve likidite, paydaş ilişkileri ve kurumsal yetkinlikler gibi belirleyici faktörleri vurgulamaktadır.

Bir kuruluşun risk kapasitesi, finansal gücü, altyapısının sağlamlığı, marka itibarı ve pazar rekabet gücü gibi faktörler tarafından şekillenir (Hopkin & Thompson, 2022). Risk kapasitesinden daha fazla risk iştahına sahip bir kuruluş, önemli bir tehlikeye maruz kalır (Murray-Webster & Williams, 2010). Ayrıca, bir kuruluş yüksek risk iştahı sergileyebilir, ancak potansiyel dalgalanmaları veya etkileri yönetme kapasitesinden yoksun olabilir. Tersine, yüksek kapasiteye sahip olsa bile, stratejik yönelim, yönetim hedefleri veya paydaş beklentileri doğrultusunda kasıtlı olarak daha düşük bir iştah seçebilir (Crickette vd., 2012).

1.3.6. Risk Kültürü

Kültür, organizasyondaki her düzeyde kararların alınma şeklini belirleyen insan davranışlarının bir sentezi olarak tanımlanır (Chappell, 2014). Bu temele dayanarak, risk kültürü, tüm çalışanların günlük davranışlarında ve kararlarında yansıtılan, risklere karşı derin bir farkındalık ve içsel duyarlılık olarak tanımlanır (Banks, 2012).

IRM’ye (2012) göre risk kültürü, bir organizasyon içindeki tutum, davranış ve ortak değerlerin etkileşimi yoluyla gelişir ve ortak bir amacı olan bir grup insan tarafından paylaşılan riskle ilgili değerler, inançlar, bilgi ve anlayış olarak tanımlanır. Bu görüşe paralel olarak,

Banks (2012), risk kültürünü davranışsal, yerleşik, bağlamsal ve kalıcı olarak nitelendirerek, etkinliğinin gerçek liderlik taahhüdüne ve organizasyon genelinde geniş katılımına bağlı olduğunu vurgulamaktadır.

Lam (2014), risk kültürünü organizasyondaki bireylerin riskle ilgili değer, varsayım ve davranışlarını şekillendiren ince ama etkili bir güç olarak tanımlar. Risk kültürünün, KRY'nin başarısında kritik rol oynadığını vurgulayan yazar, çalışanların risk yönetimini benimsemediği zayıf bir kültürün girişimleri zedelediğini; günlük işleyişe entegre edilen risk yönetiminin ise güçlü bir kültürün göstergesi olduğunu belirtir.

Risk kültürü, doğası gereği kuruma özeldir ve kuruluşlar arasında, genellikle üst yönetimin sahiplenmesine bağlı olarak farklılık göstermektedir (Banks, 2012). Kültür, üst yönetim tarafından kasıtlı olarak şekillendirilebilir veya doğal olarak gelişebilir; her iki yaklaşım da organizasyonun ihtiyaçlarına uygun bir kültürün oluşmasında etkilidir (IRM, 2012). Üst yönetimin sahiplenmesi, çalışan eğitimi, teşvik yapılarının devreye alınması, değişim yönetimi ve açık iletişim, risk kültürünü şekillendiren ve sürdüren birbiriyle bağlantılı temel faktörlerdir (Lam, 2014). Risk kültürü, kuruluşun kendine özgü bağlamına uyarlanmalı ve küresel firmalarda ulusal kültürel farklılıkları barındıracak kadar esnek olmalıdır (Banks, 2012).

Risk kültürü, sürekli olarak iyileştirilmesi ve sürdürülmesi gereken, gelişen ve uyarlanabilir bir sistemdir. Carrel (2010), risk kültürünü sürekli geri bildirim, yerleşik süreçler ve dış koşullarla uyum tarafından şekillenen, kendi kendini uyarlayan bir zekâ olarak tanımlamaktadır. Benzer şekilde Banks (2012), risk kültürünün iç ve dış değişikliklerle birlikte değiştiğini ve etkinliğini korumak için sürekli dikkat gerektirdiğini vurgulamaktadır.

1.3.7. Risk İletişimi

Risk iletişimi, genel olarak ilgili taraflar arasında risklerle ilgili bilgilerin bilinçli bir şekilde paylaşılması veya aktarılması olarak tanımlanmaktadır (Lang vd., 2001; Fewtrell & Bartram, 2014). Cooper vd.'ye (2005) göre risk iletişimi, karar vericiler ve paydaşlar arasında risklerin varlığı, niteliği, biçimi, olasılığı, ciddiyeti ve ele alınması gibi hususları kapsayan bilgilerin paylaşılmasını içerir ve paydaşlar arasında karşılıklı yürütülen bir süreç olarak nitelendirilir. Bu bağlamda Molak (1997), risk iletişiminin amacının öznel risk algılarını, risk analizinden elde edilen objektif risklerle uyumlu hale getirmek olduğunu vurgulamaktadır. Gutteling ve Wiegman (1996), risk iletişimini, risk sorunlarını önlemek, çözmek veya azaltmak

için bilimsel araştırmalara dayalı ve belirli hedef kitlelere uyarlanmış bilgi aktarımının sistematik planlanması olarak tanımlanmaktadır.

Etkili risk iletişimi zamanında olmalı, paydaşların ihtiyaçlarına göre uyarlanmalı ve net bulgular ve öneriler içermelidir (Hillson, 2019). Hem uyarılar hem de eğitici içerikle farklı kitlelere hitap etmeli (Lang vd., 2001) ve geri bildirimlere olanak tanıyarak riskleri, belirsizlikleri ve etkileyen faktörleri açıkça açıklamalıdır (Teaf & Kuperberg, 2004).

Marchetti (2012), KRY’de rol ve beklentilerin net aktarılması ve ortak bir risk dili oluşturulmasının, üst yönetimin bağlılığını güçlendirdiğini ve uygulamanın kuruma yayılmasına katkı sağladığını belirtmektedir.

Etkili risk iletişimi, kuruluşların KRY ile ilgili rol, sorumluluk ve beklentileri açıkça iletirken, iç ve dış geri bildirim için açık kanallar sağlamasını gerektirir (Marchetti, 2012). Bu çabalar, kamu kurumları, endüstri grupları ve bireysel vatandaşlar dâhil olmak üzere çok çeşitli paydaşların farklı bilgi ihtiyaçlarını da karşılamalıdır (Fewtrell & Bartram, 2014).

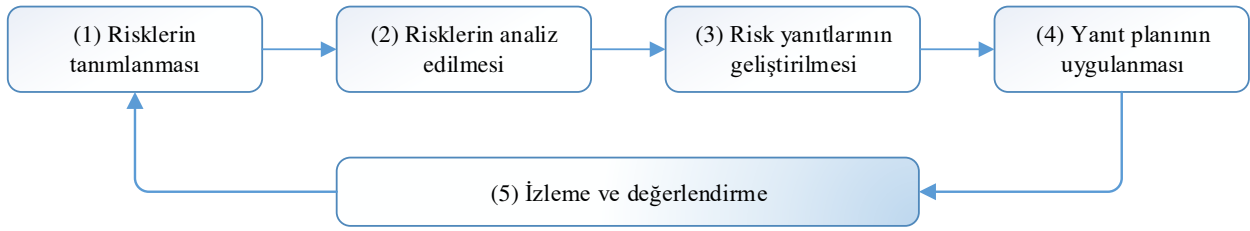
1.4. Risk Yönetim Süreci

KRY yaklaşımı, riskleri değer yaratacak şekilde yönetmek amacıyla risk yönetim sürecinin tutarlı bir şekilde uygulanmasını sağlamaktadır (Fraser & Simkins, 2010). Bu çerçevede, bir kuruluşun stratejik hedeflerine ulaşmasını engelleyebilecek veya destekleyebilecek belirsizlikleri, kurumsal düzeyde ve sistematik bir yaklaşımla tanımlayan, analiz eden, değerlendiren, yanıtlayan ve izleyen entegre bir yönetim süreci olarak tanımlanabilir.

Bu süreç, ISO 31000 (2018) ve COSO (2018) gibi uluslararası standart ve çerçeveler aracılığıyla yapılandırılmıştır. Söz konusu kaynaklarda, KRY sürecine ilişkin uygulama adımları, aşamalandırma ve adlandırma bakımından farklılık gösterse de içerik ve yönetim yaklaşımı bağlamında benzerlik göstermektedir.

KRY, tanımlanan risklere yanıt olarak eylemleri yönlendirmek ve kontrol etmek için tasarlanmış ilkeleri, süreçleri, rolleri, faaliyetleri ve altyapıyı kapsamaktadır (Green, 2016). KRY süreci, genellikle şu ana adımlardan oluşmaktadır. (1) Risklerin tanımlanması, (2) analiz edilmesi, değerlendirilmesi, (3) risklere yanıtların geliştirilmesi, (4) yanıt planının uygulanması ve (5) izleme ve değerlendirme adımlarından oluşmaktadır. Şekil 1’de bahsedilen adımlardan oluşan jenerik bir risk yönetim süreci gösterilmektedir.

Şekil 1: Risk Yönetimi Süreci



Risklerin yönetiminde izlenen süreçte yer alan adımlar, birbirlerini besleyen ve süreklilik gösteren bir döngü şeklinde KRY'nin dinamik doğasını yansıtmaktadır. Kuruluş genelinde KRY'nin başarısı, anılan adımların organizasyonel yapı, kurumsal yetkinlik, kültür ve iletişim süreçleri ile entegre bir şekilde yürütülmesine bağlıdır.

Öte yandan, bahse konu risk yönetim süreçlerine ilave olarak ISO 31000 (2018) Risk Yönetimi Standardı ve COSO KRY (2018) çerçevesi ile çeşitli araştırmalarda (Fraser & Simkins, 2010; Marchetti, 2012; Green, 2016) risklerin tanımlanması aşamasından önce gelmek üzere iş ortamının / bağlamının değerlendirilmesi amacıyla bir adım daha bulunmaktadır.

COSO KRY (2018) çerçevesinde “Strateji ve Hedef Belirleme” bileşeni olarak adlandırılan bu bölümde risk yönetiminin strateji oluşturma ve hedef belirleme süreçlerine entegre edilmesine odaklanılmaktadır. Amaç, bir kuruluşun seçtiği stratejiyi risk iştahı ve iş bağlamıyla uyumlu hale getirmek, böylece risklerin stratejik planlamanın en erken aşamalarından itibaren tanımlanması, değerlendirilmesi ve yönetilmesini sağlamaktır (COSO, 2018).

COSO KRY (2018), dört temel ilke aracılığıyla riski stratejiye entegre eder. İş bağlamını analiz etmek, strateji ve performansı etkileyebilecek iç ve dış faktörleri, ortaya çıkan eğilimleri de dâhil olmak üzere değerlendirmek anlamına gelir. Risk iştahını tanımlamak, kuruluşun değer elde etmek için kabul etmeye hazır olduğu risk miktarını ve türünü belirler ve stratejik hedeflerle uyumu sağlar. Alternatif stratejileri değerlendirmek, bilinçli karar almayı desteklemek için seçenekleri risk-getiri profillerine göre karşılaştırmayı gerektirir. İş hedeflerini formüle etmek, seçilen strateji ve tanımlanan risk iştahıyla uyumlu, ölçülebilir ve ulaşılabilir hedefler belirlemeyi içerir ve performans ve risk yönetimi için bir temel sağlar (COSO, 2018).

Benzer şekilde ISO 31000 (2018) Risk Yönetimi Standardında “Kapsam, Bağlam ve Kriterler” olarak adlandırılan bu bölüm, risk yönetimini etkileyen iç ve dış faktörlerin tanımlanması ile risk yönetimi politikasının uygulanması için kapsam ve risk kriterlerinin

belirlenmesini içermektedir. Standartta dış bağlam, kuruluş dışındaki kültürel, yasal, ekonomik ve teknolojik koşullar ile paydaş algılarını; iç bağlam ise kuruluşun hedeflerine ulaşmasını etkileyen içsel değerler, kültür, yapı ve yetenekleri kapsar. Yönetişim roller, stratejiler, kaynaklar, bilgi, karar alma süreçleri, iç ilişkiler, benimsenen standartlar ve sözleşme düzenlemelerini kapsar (ISO, 2018).

Risk yönetimi bağlamı, iç ve dış faktörlerle birlikte kuruluş genelindeki risk iştahı ve risk yönetimi çerçevesini tanımlayarak, risklerin belirlenmesi, değerlendirilmesi ve yönetilmesi için temel oluşturur (Fraser & Simkins, 2010). Üst yönetim desteği, sürecin planlanması, araç ve belgelerin geliştirilmesi ile eğitim ve farkındalık oturumları gibi temel bileşenlerin eksikliği, değerlendirme sürecinin etkinliğini ve verimliliğini olumsuz etkileyebilir (Lam, 2014).

Riskler sektörel, ekonomik ve politik koşullar gibi dış faktörler ile kültür, süreçler ve strateji gibi iç faktörler dâhil olmak üzere bağlama göre değişir. İç bağlam, kuruluşun hedeflerine ve risk türüne göre değişen risk toleransı ve risk iştahını içerir (Green, 2016).

Bağlam üst yönetimin rolü ile risk yönetimi sürecine dâhil olan paydaşların belirlenmesinde etkilidir (Hallowell vd., 2013). Ayrıca, bağlam içinde açıkça tanımlanmış hedefler, performans beklentilerinin belirlenmesine yardımcı olur ve yönetimin bu hedeflere ulaşmakla ilişkili riskleri değerlendirmesini sağlar (Dinapoli, 2016).

Risk yönetimi bağlamını net bir şekilde belirlemek, tüm sürecin etkinliğini sağlamak için çok önemlidir. İyi tanımlanmış bir bağlam, bilinçli karar almayı destekler, paydaşların katılımını teşvik eder ve risk faaliyetlerini kurumsal hedeflerle uyumlu hale getirir.

1.4.1. Risklerin Tanımlanması

Risk yönetimi faaliyetlerine temel oluşturan risk belirleme adımı, olası tüm risklerin tespit edildiği ve bir risk kaydına işlendiği ilk adım olarak tanımlanır.

Green'e (2016) göre risk belirleme, risklerin kökenlerini, nedenlerini, olası olayları ve sonuçlarını tanımlayarak, kontrol edilebilir ve edilemeyen riskler ile bunların olası zincirleme etkilerini içeren kapsamlı bir risk kaydı oluşturma sürecidir.

Akçakanat (2012), riskleri yönetmek için öncelikle kuruluşun hedeflerinin belirlenmesi, ardından bu hedefleri tehdit eden risklerin tanımlanması gerektiğini vurgulamaktadır. Yönetim, olumsuz etkilere sahip potansiyel olayları belirlemeli ve bunların hedeflerin gerçekleştirilmesini engelleme veya destekleme potansiyeline göre tehdit mi yoksa fırsat mı

oluşturduğunu belirlemelidir. Kuruluş, iş stratejisinin ve hedeflerinin gerçekleştirilmesini etkileyebilecek riskleri belirler (COSO, 2018). Bu riskler, insan hatası, dolandırıcılık veya sistem arızaları gibi içsel riskler veya yasal değişiklikler veya doğal afetler gibi dışsal riskler olabilir (Dinapoli, 2016).

Bu süreç, yönetimin, organizasyonun hedeflerini etkileyebilecek beklenen ve beklenmeyen olaylar da dâhil olmak üzere hem iç hem de dış faktörleri dikkate almasını gerektirir. Dış faktörler arasında ekonomik koşullar, yasal veya düzenleyici eğilimler, siyasi iklim, pazar rekabeti, talep dalgalanmaları ve güvenlik tehditleri yer alırken, iç faktörler organizasyonel kültür, personel yetenekleri, kapasite, teknoloji, süreçler, liderlik etkinliği ve risk iştahını kapsar (Passenheim, 2013).

Risk kaynakları, risk olaylarına yol açabilecek koşullardır. Risk tanımlamanın yaygın kaynakları arasında geçmiş veriler yer alır (Fraser & Simkins, 2010). Gregory (2003), içsel risklerin üç ana kaynaktan beslendiğini vurgulamaktadır. Bunlar kuruluşun misyonu, yapısı ve kültürü, sahip olduğu veya kontrol ettiği varlıklar ve kaynaklar ile iş ortakları gibi dış kuruluşlarla olan ilişkileri olarak aktarılmaktadır.

Marchetti'ye (2012) göre, önceki olaylar veya kayıplar bu aşamada değerli referanslar olup, potansiyel olayların birbirleriyle ilişkili olabileceğini, eşzamanlı gerçekleşebileceğini veya birbirini tetikleyebileceğini anlamak açısından önem taşır. Risk belirleme çalışmaları, tüm önemli iç ve dış riskleri kapsamalıdır (ISO, 2018). Her sorun kurumsal düzeyde risk oluşturmaya da, yöneticiler dış eğilimleri belirli ve değerlendirilebilir risklere dönüştürmelidir (COSO, 2018). Çevresel, Sosyal ve Kurumsal Yönetim (ESG) ile ilgili riskler, genellikle yeni veya ortaya çıkan, bilinmeyen, uzun vadeli, nicel olarak ölçülmesi zor ve tek bir kuruluşun ötesinde toplu eylem gerektirebilen riskler olduğundan, belirlenmesi özellikle zordur (COSO, 2018).

KRY hedeflerinin kapsamlı bir şekilde anlaşılması bakımından paydaşların bu aşamaya katılımı önem taşımakta (Passenheim, 2013); bahse konu paydaşlarla iş birliklerinin gerçekleştirilmesi, risk tanımlanması sürecini desteklemektedir (Akçakanat, 2012).

Risk belirleme teknikleri beyin fırtınasından senaryo analizine ve karar ağaçları gibi yapılandırılmış yaklaşımlara kadar çeşitlilik gösterir. Yaygın ve etkili bir yöntem, personelin katıldığı grup beyin fırtınası oturumlarıdır. Bu oturumlar, operasyonları aksatabilecek potansiyel olaylar hakkında fikir üretilmesini sağlar (Dinapoli, 2016). Uzman veya paydaş görüşmeleri, nominal grup tekniği, Delphi yöntemi ve SWOT analizi gibi nitel yöntemler,

genellikle uygulanması kolay olan yöntemler olup, çeşitli paydaşların katılımı bu uygulamalardan elde edilen faydayı artırmaktadır (Olson & Wu, 2020). Ayrıca, benzer geçmiş projelerden elde edilen tarihsel veriler, özellikle bu veriler iyi belgelenmiş ve erişilebilir olduğunda, risk tanımlamayı destekleyebilir.

Risk belirleme süreci, temelde belirlenen risklerin listesini, risklerin sahibi olan birimleri, risklerin temel nedenleri ve sonuçlarını içeren bir risk kaydının oluşturulmasıyla sonuçlanır.

1.4.2. Risklerin Analiz Edilmesi

Risk analizi, risklerin doğasını anlamak ve önemini belirlemek amacıyla riskin nedenlerini, olasılığını ve potansiyel sonuçlarını sistematik olarak inceleyen analitik bir süreçtir. Risk belirleme aşamasına dayanan risk analizi süreci, nicel ve nitel yöntemleri kullanarak tehditleri sürekli olarak değerlendirir, riskler arasındaki ilişkileri ortaya çıkarır, bunları önceliklendirir ve organizasyonel hedefler üzerindeki etkilerini değerlendirir (Passenheim, 2013). Risk analizi aşaması, karar vericilere riskin ele alınması veya uygulanacak strateji ve kontrollerle ilgili kararları yönlendirmek için yeterli bilgi sağlar. Bu sayede, kuruluşun yapılandırılmış ve bilgilendirilmiş analizlere geçmesine olanak tanır (Gregory, 2003).

Risk analizinin temel amacı, risklerin kaynaklarını ve nedenlerini anlamak, mevcut kontrollerin etkinliğini değerlendirmek ve risk olaylarının olasılığını ve olası sonuçlarını (olumsuz veya olumlu) değerlendirmektir (Green, 2016). Başarılı bir değerlendirme gerçekleştirebilmek için, organizasyonun faaliyetleri ve sektör bağlamı hakkında ayrıntılı bilgiye sahip kişiler analizde yer almalı; iç veriler, sektör karşılaştırmaları ve dış kaynaklardan yararlanılmalıdır (Marchetti, 2012). Açıkça ifade edilmiş hedefler, ilgili risklerin belirlenmesi ve uygun risk tolerans eşiklerinin belirlenmesi konusunda yardımcı olmakla birlikte, kuruluşun misyonunu yerine getirmesine yönelik risklerin yönetilmesi için kapsamlı bir değerlendirme gereklidir (Dinapoli, 2016). Bu analizden elde edilen bilgiler, risklerin önceliklendirilmesi ve uygun müdahale stratejilerinin seçilmesinde kullanılır (Green, 2016).

Riskler belirlendikten sonra, her birinin nasıl ele alınacağına karar vermek için değerlendirme adımı uygulanır (Akçakanat, 2012). Bu adım, doğal ve kalıntı riskleri dikkate alarak her bir riski olasılığı ve etkisi açısından değerlendirmeyi içerir (Marchetti, 2012). Olasılık, riskin meydana gelme olasılığını ifade etmekte; etki ise riskin hedefler üzerindeki

potansiyel etkisini belirtmektedir. Riskin şiddeti, genellikle olasılık ile etkinin çarpılmasıyla elde edilir.

Değerlendirmede, verilerin mevcudiyetine bağlı olarak nitel ve nicel yöntemler kullanılabilir. Uzman görüşü gibi nitel teknikler değerlendirmede esneklik sağlarken, nicel modeller daha fazla kesinlik sunar (Moeller, 2007). Amaç, açık ve tarafsız bir değerlendirmeyi desteklemek için her riske objektif ve ölçülebilir değerler atamaktır (Gregory, 2003).

Mevcut veya planlanan kontrollerden sonra kalan risk olarak tanımlanan kalıntı risk, önceden tanımlanmış risk kriterleriyle karşılaştırılarak söz konusu riskin tolere edilebilir olup olmadığı değerlendirilmelidir. Bir risk kabul edilebilir eşikleri aşarsa, daha ileri yanıt seçenekleri araştırılmalıdır. Risk şiddeti, kuruluşun risk tolerans seviyesinin belirlenmesine yardımcı olur (Dinapoli, 2016); kritik ve düşük öncelikli risklerin ayırt edilmesini sağlar (Moeller, 2007).

Risk değerlendirme teknikleri arasında çok amaçlı değerlendirme analizleri, öznel derecelendirme sistemleri, istatistiksel modelleme, odak grup testleri ve simülasyon gibi teknikler yer almaktadır (Fraser & Simkins, 2010). Analitik yaklaşımlar, gelişmiş nicel modellerden uzman yargısına veya yapılandırılmış sezgiye dayalı nitel değerlendirmelere kadar uzanır. Nicel analiz mümkün olmadığında, nitel yöntemler kullanılmaktadır. Bunlar arasında, özellikle farklı olasılık ve etki koşulları altında riski değerlendirmek için senaryo analizi yaygın olarak kullanılmakla birlikte diğer yaygın olarak kullanılan araçlar arasında risk matrisleri, hata türleri ve etkileri analizi (HTEA) ve program değerlendirme ve gözden geçirme tekniği (PERT) bulunmaktadır (Passenheim, 2013).

Analiz sürecinin kritik bir adımı olarak risk önceliklendirme, kaynakların en önemli tehdit ve risklere verimli bir şekilde tahsis edilmesini sağlar (Lam, 2014). Önceliklendirme, etki ve olasılık gibi kriterler kullanılarak gerçekleştirilir.

Anahtar Risk Göstergeleri (KRI), risklerin varlığı, gelişimi ve düzeylerindeki değişimleri izleyerek risk seviyeleri hakkında genel bir bakış sunan risk analizi araçlarıdır (Fraser & Simkins, 2010). Düzgün bir şekilde geliştirilmiş KRI'lar, proaktif yönetimi mümkün kılar. Etkili KRI'lar, erken uyarı sinyalleri olarak işlev gören ileriye dönük özelliklere sahiptir (Lam, 2014). Örneğin, BT sistemlerinde artan kesinti sayısı, siber güvenlik zafiyetlerinin veya teknolojik altyapıdaki yetersizliklerin erken göstergesi olabilir.

Risk analizi aşaması, önceliklendirilmiş ve kendisine karşı yanıt stratejisi ve eylemi uygulanması gereken risklerin belirlenmesi ile sonuçlanır. Risk değerlendirmesinin sonuçları, üst yönetim ve yönetim kurulunun incelemesi için konsolide bir yapıda belgelenmelidir.

1.4.3. Risk Yanıtlarının Geliştirilmesi

Risk analizinin ardından gelen risk yanıtlarının geliştirilmesi aşaması, kurumların karşılaştıkları risklere karşı sistemli ve stratejik müdahale çerçevesi oluşturmalarını sağlar. Dört adımdan oluşan bu süreç yapılandırılmış bir sıra doğrultusunda ilerler.

Öncelikle risklere karşı izlenecek genel yaklaşımı belirleyen risk yanıt stratejileri belirlenir. Ardından, bu stratejiler doğrultusunda somut ve uygulanabilir yanıt eylemleri ortaya konur. Bu eylemler, kurumsal işleyişe entegre edilecek şekilde detaylandırılarak bir risk yanıt eylem planına dönüştürülür. Sürecin son adımı olarak ise, gerçekleştirmelere karşı hazırlıklı olunmasını sağlayacak alternatif senaryoları içeren Beklenmedik Durum Planları oluşturulur. Böylece, risk yanıt süreci yalnızca önleme değil, aynı zamanda kurtarma ve onarmayı kapsayacak şekilde esneklik ve süreklilik perspektifinden de ele alınmış olur.

1.4.3.1. Yanıt Stratejilerinin Belirlenmesi

Riskler değerlendirildikten sonra, bunları etkili bir şekilde yönetmek üzere uygun yönetim stratejileri formüle edilir (Wu & Olson, 2008). Risk yanıt stratejileri, bir kuruluşun risklerine yönelik farkındalığı ile her bir risk türünü özel bir yaklaşımla yönetme niyetini yansıtan metodolojik tercihleri temsil eder (Karaçolak, 2024).

Risk yanıt stratejileri, “risklerin kabul edilip edilmeyeceği, azaltılacağı, paylaşılacağı ya da tamamen ortadan kaldırılacağına ilişkin temel yönelimleri” tanımlar. Kurumun risklere yönelik iştahı, toleransı, hedefleri ve mevcut kaynakları doğrultusunda şekillenirler. Risklere yönelik stratejilerin doğru bir şekilde tespit edilmesi, KRY’nin etkinliği ile verimliliğini doğrudan etkileyen stratejik seviyede bir karardır.

Kuruluşlar, belirsizlikleri etkili bir şekilde yönetmek için çeşitli risk yanıt stratejileri uygularlar ve belirli bir stratejinin seçimi, riskin niteliği, risk türü ve kuruluşun risk toleransı gibi faktörlere bağlıdır (Cooper vd., 2005).

Tehditlere yönelik risk yanıt stratejilerine ilişkin KRY standart ve çerçeveleri ile çeşitli akademik çalışmalarda, geneli itibariyle benzerlik göstermekle birlikte farklı stratejilere yer verilmektedir. Risk yanıt stratejileri, ISO 31000 (2018) Risk Yönetim Standardı ile COSO KRY (2004) çerçevesinde kaçınma, azaltma, kabul ve transfer stratejileri olarak yer almaktadır. COSO KRY (2018) çerçevesinde farklı olarak paylaşma stratejisine değinilmektedir. Borghesi ve Gaudenzi (2013), söz konusu stratejilere ayırma, kopyalama ve çeşitlendirme stratejilerini ilave etmektedir.

Karaçolak (2024), risk yönetimi ile ilgili çeşitli çalışmalarda, standartlarda ve çerçeve belgelerdeki risk yanıt stratejilerini derlediği araştırmasında tehditlere yönelik stratejileri kaçınma, azaltma, transfer, kabul, paylaşma, ayırma, kopyalama ve çeşitlendirme stratejileri olarak derlemektedir. Söz konusu stratejiler ilerleyen bölümlerde açıklanmaktadır.

a) Kaçınma / Sonlandırma Stratejisi

Riskten kaçınma, risklere müdahale edilemediği veya kabul edilebilir bir düzeye indirilemediği durumlarda, riskli faaliyetten tamamen kaçınmanın veya geri çekilmenin daha maliyet etkin olduğu düşünülen bir stratejidir (BSI, 2011). Bu gibi durumlarda, ilgili faaliyeti sonlandırmak, riski kabul edilebilir bir düzeye indirmenin tek geçerli yolu olabilir (Hopkin & Thompson, 2022). Kaldırma, ortadan kaldırma, hariç tutma veya sonlandırma olarak da adlandırılan bu strateji, özellikle olumsuz bir sonuç beklendiğinde riski tamamen ortadan kaldırmayı amaçlar (Chapman, 2012).

Bir riskin potansiyel etkileri kontrol edilemez olarak algılanırsa, yönetim ilgili faaliyeti tamamen durdurmayı tercih edebilir (Akçakanat, 2012). Örneğin, politik istikrarsızlık nedeniyle belirli bir pazara giriş yapmaktan vazgeçmek, riskin ortaya çıkma ihtimalini sıfıra indirir. Ancak bu strateji, fırsatları da kaçırma riski taşıdığından dikkatle değerlendirilmelidir.

Potansiyel etkinliğine rağmen, belirli faaliyetlerin sürdürülmesine ilişkin yasal ve düzenleyici yükümlülükler nedeniyle, riskten kaçınma uygulamasının kapsamı kamu sektöründe özel sektöre kıyasla önemli ölçüde daha sınırlı olabilir (Hopkin & Thompson, 2022). Bununla birlikte, aşırı ihtiyat veya risk ve getirinin hatalı değerlendirilmesinden kaynaklanan hatalı bir riskten kaçınma stratejisi, fırsatların kaçırılmasına veya diğer risklere maruz kalmanın artmasına neden olabilir (BSI, 2011).

b) Azaltma Stratejisi

Risk modifikasyonu olarak da adlandırılan risk azaltma stratejisi, risk yönetiminin en yaygın kullanılan stratejisidir. Risklerin nedenleri veya sonuçlarında ayarlamalar yaparak olumlu sonuçların olasılığını artırmak ve olumsuz sonuçların olasılığını veya etkilerinin ciddiyetini azaltmak amacıyla uygulanır (BSI, 2011; Hopkin & Thompson, 2022). Bu yaklaşım, riski tamamen ortadan kaldırmayı değil, riski oluşturan faaliyeti sürdürürken, riski kabul edilebilir bir düzeyde yönetmeyi amaçlamaktadır (Hopkin & Thompson, 2022).

Risk azaltma, bir riskin ortaya çıkmasını önlemeye yönelik önleyici kontroller ile riskin ortaya çıkması durumunda etkilerini yönetmek için acil durum planlaması veya potansiyel etkiyi absorbe etmek için ek finansal veya insan kaynakları tahsis edilmesi gibi çeşitli düzeltici kontroller yoluyla hayata geçirilebilir (BSI, 2011). Hassas veya yüksek değerli verileri içeren riskler gibi kabul edilemez risklerin söz konusu olduğu durumlarda, yönetim riske maruz kalmayı kabul edilebilir bir eşiğe indirmek için özel kontroller belirleyebilir (Akçakanat, 2012). Azaltma stratejisinin etkinliği, bu kontrol faaliyetlerinin açıkça tanımlanmış, iyi iletilmiş ve amaçlandığı gibi işleyip işlemediğine bağlıdır (Dinapoli, 2016).

Bu stratejiye örnek olarak bir üretim tesisinde yangın riskinin söz konusu olması durumu verilebilir. Tesise yangın algılama sistemleri ve otomatik söndürücüler gibi fiziksel kontroller yerleştirilmesi, çalışanlara düzenli yangın güvenliği eğitimi verilmesi ve acil durum tatbikatlarının yapılması bu stratejiye dâhildir. Bu tür uygulamalar sayesinde hem yangının çıkma ihtimali azaltılır hem de çıkması durumunda yaratacağı zararlar en aza indirilir. Bu yaklaşım, işletmenin güvenliğini artırarak operasyonel sürekliliği koruma açısından kritik rol oynar.

c) Transfer Etme Stratejisi

Risk transferi, belirli bir riskin yönetim sorumluluğunun başka bir tarafa devredilmesini içerir (BSI, 2011). Risk transferi, finansal veya varlıklarla ilgili risklerin yönetiminde özellikle etkilidir ve genellikle sigorta poliçeleri veya üçüncü taraf sözleşmeleri yoluyla kullanılır (Hopkin & Thompson, 2022). Sigorta, bu stratejinin en yaygın biçimi olarak kabul edilmektedir (Chapman, 2012).

Ancak, risk transferinin de sınırlamaları vardır. Bir riski transfer etmek, riskin varlığını ve potansiyel etkilerini ortadan kaldırmaz; yükü başka bir kuruluşa aktarır (Chapman, 2012).

Ayrıca, riskini karşıya transfer eden kuruluş, “transfer edilen riski alan tarafın bu riski etkili bir şekilde yönetememe olasılığı” şeklinde yeni bir risk türü üstlenmiş olur (BSI, 2011).

Ayrıca, riskin tamamen devredilmesi genellikle mümkün değildir (BSI, 2011). Örneğin, sigortalama bir yangın sonrası yeniden inşa maliyetlerini karşılayabilir, ancak kurtarma süresince iş faaliyetlerinin kesintiye uğramasını önleyemez. Benzer şekilde, BT hizmetlerinin dış kaynak kullanımı, sistem arızası riskini ortadan kaldırmaz veya acil durum planlaması ihtiyacını ortadan kaldırmaz. Üretim veya hizmetlerin bir yükleniciye devredilmesi de, yüklenicinin performansının düşük olması durumunda kuruluşu itibar kaybından korumaz. Risk transferi nadiren tek başına uygulanır ve genellikle diğer risk yanıt stratejileriyle birlikte kullanılır (BSI, 2011).

d) Kabul Etme Stratejisi

Kabul stratejisi, riskin tutulması, absorbe edilmesi veya tolere edilmesi gibi ifadelerle de adlandırılır ve herhangi bir risk azaltma önlemi almaksızın belirli bir kalıntı riski üstlenmeyi kasıtlı olarak seçmeyi içerir. Bu strateji genellikle uygulanabilir veya kabul edilebilir yanıt seçenekleri kalmadığında ya da kontrolü uygulamanın şu anda mümkün olmadığı durumlarda kullanılır (BSI, 2011; Chapman, 2012). Bu gibi durumlarda, riskin kabul edilmesi kararı, önceki risk analizi ve değerlendirme süreçlerinin sonuçlarına dayandırılmalı ve koşullar değişirse revize edilmelidir (BSI, 2011).

Kabul stratejisi, bir riskin potansiyel etkisinin ek müdahale olmadan kabul edilebilir olduğu durumlarda da kullanılabilir (Hopkin & Thompson, 2022). Örneğin, bir riskin sonuçları önemsizse veya azaltma maliyeti beklenen kayıptan fazlaysa, yönetim riski kabul etmeye karar verebilir (Akçakanat, 2012). Söz konusu stratejiye bir kuruluşun ofis ekipmanlarının çalınması gibi düşük olasılıklı ve sınırlı maliyetli riskleri sigorta yaptırmadan kabul etmesi örnek olarak verilebilir. Bu yaklaşım, kaynakların daha kritik risklere yönlendirilmesini sağlar.

Chapman (2012), risk kabul kararının geçerliliğini doğrulamak üzere üç temel testin uygulanması gerektiğini vurgulamaktadır. Bunlar diğer tüm stratejik seçeneklerin (örneğin, ortadan kaldırma, azaltma veya transfer) değerlendirilip değerlendirilmediğinin doğrulanması; risk bağlamının değişen koşullara göre düzenli olarak gözden geçirilmesinin sağlanması ve kuruluşun potansiyel etkiye dayanacak yeterli emilim (özümseme) kapasitesine sahip olduğunun teyit edilmesidir.

e) Paylaşma Stratejisi

Riskin birden fazla taraf arasında bölüşülmesini sağlayan iş birlikçi bir yaklaşım olarak paylaşma stratejisinde, tarafların maruz kalacağı zarar azaltılır. Bu yaklaşım, sorumluluğun tamamen devredilmediği, aksine dağıtıldığı için tam risk transferinden farklıdır (Cooper vd., 2005). Bu strateji, iş birliği sözleşmeleri, finansal anlaşmalar, ortaklıklar veya ortak girişimler gibi mekanizmalar aracılığıyla uygulanabilir; bu yolla hem potansiyel kazançlar hem de yükümlülükler paylaşılır (BSI, 2011; Hopkin & Thompson, 2022).

Örneğin, büyük bir altyapı projesi yürüten bir inşaat firması, proje kapsamındaki finansal riskleri ve zamanlama belirsizliklerini azaltmak amacıyla bir kamu-özel sektör ortaklığı kurabilir. Bu durumda hem kamu kurumu hem de özel sektör firması proje risklerini paylaşmış olur.

f) Ayırma Stratejisi

Ayırma stratejisi, kaynakları ve faaliyetleri mekânsal, işlevsel (Karaçolak, 2024) ya da zaman dilimlerine dağıtarak (Borghesi & Gaudenzi, 2013) hasarın yayılmasını önler. Temel amaç, bir risk gerçekleştiğinde tüm sistemin değil sadece bir kısmının etkilenmesini sağlamaktır. Bu tür önlemler, kayıp olaylarının olasılık ve etkisinin azaltılmasına etkili bir şekilde katkıda bulunur (Borghesi & Gaudenzi, 2013).

Örneğin, tehlikeli kimyasalların, diğer üretim ekipmanlarından ayrı, özel yalıtılmış bir bölümde depolanması bu stratejinin pratik bir uygulamasıdır.

g) Kopyalama Stratejisi

Kopyalama stratejisi, yedeklemelerin, yedek varlıkların veya yedek olarak tutulacak önemli mülklerin, verilerin veya yeteneklerin kopyalarının tutulmasını içerir (Borghesi & Gaudenzi, 2013). Bu strateji ile herhangi bir arızada ya da kesintide, yedek kaynak devreye girerek iş sürekliliği sağlanır. Bilgi teknolojilerinde yedekleme sistemleri ve alternatif veri merkezleri bu stratejinin pratik örneklerindendir. Kopyalama, tek bir varlığa olan bağımlılığı azaltma amacı bakımından ayrıştırma stratejisine benzemektedir (Karaçolak, 2024).

h) Çeşitlendirme Stratejisi

Çeşitlendirme stratejisi, riskleri birden fazla proje, ürün, pazar veya bölgeye dağıtarak tek bir yere bağımlılığı sınırlandırarak kayıpların etkisini azaltır (Borghesi & Gaudenzi, 2013). Farklılaştırılmış ürün portföyleri, çoklu tedarikçilerle çalışmak ya da çeşitli pazarlarda faaliyet göstermek, çeşitlendirme stratejisinin uygulamaları arasında yer alır. Böylece herhangi bir alanda yaşanacak olumsuzluk, tüm organizasyonu etkilemeden kontrol altına alınabilir.

Örneğin, bir üreticinin tüm hammaddeleri tek bir tedarikçiden almak yerine, farklı ülkelerdeki birden fazla tedarikçiden temin etmesi bir çeşitlendirme stratejisidir. Böylece bir ülkedeki, kriz tüm üretimi durdurmaz. Ayrıştırma stratejisi risk etkilerini izole ederek kayıpları azaltırken, çeşitlendirme stratejisi potansiyel etkileri çeşitli alanlara dağıtarak kayıpları hafifletir (Karaçolak, 2024).

1.4.3.2. Yanıt Eylemlerinin Belirlenmesi

Uygun risk yanıt stratejilerinin seçilmesini takiben yönetim, risklerin etkili bir şekilde yönetilmesini sağlamak amacıyla ayrıntılı bir eylem planı oluşturmalıdır. Risk yanıt eylemi (yanıt faaliyeti, kontrol, kontrol eylemi, kontrol faaliyeti), “bir riskin olasılığını azaltmak, etkisini hafifletmek, riskten kaçınmak, riski paylaşmak veya kabul etmek amacıyla yürütülen bilinçli ve planlı faaliyetler bütünü” ifade etmektedir. Risk yanıt faaliyetleri, “belirlenen riskleri ele almak için seçilen yanıt stratejilerine uygun olarak yürütülen eylemler” olarak açıklanmaktadır (Karaçolak, 2024). Chapman (2012), bu kontrolleri “belirlenen bir tehdide yanıt olarak alınan önlemler dizisi” olarak ifade etmektedir.

Kontrol faaliyetleri, organizasyonel planların etkinliğini ve hedeflerin gerçekleştirilmesini sağlamak üzere oluşturulurlar (Akçakanat, 2012). Risk yanıt eylemleri, seçilen risk stratejisi doğrultusunda maliyet, artık risk ve kriterlerle uyum açısından şekillenmekte; riskin kurumsal hedefler üzerindeki olumsuz etkisine ilişkin uygun ve orantılı bir karşılık verilmesini sağlamaktadır.

Eylemler, risklerin türü, şiddeti ve yönetilebilirliğine göre çeşitlendirilerek, KRY çabalarının etkinliğini doğrudan etkileyen esas uygulamalardır. Bu faaliyetler önleyici, yönlendirici, tespit edici ve düzeltici kontroller olmak üzere 4 ana türe ayrılmaktadır (Chapman, 2012; Hopkin & Thompson, 2022).

1. **Önleyici kontroller**, risklerin ortaya çıkmasını önlemeye yönelik uygulamalardır (Akçakanat, 2012). Öncelik zarar oluşmadan önce önlemek olduğunda bu strateji devreye girer ve fiziksel güvenlik, güvenlik duvarları ve görevlerin ayrılması gibi önlemler hayata geçirilir. Ancak, belirli operasyonel ortamlarda yüksek maliyetlere neden olabilir veya pratik olmayabilir (Hopkin & Thompson, 2022).
2. **Yönlendirici kontroller**, istenen sonuçların elde edilmesi için davranışları yönlendirmeyi amaçlar. Kayıpları önlemek veya olay sonrası hasarı en aza indirmek için bireylere nasıl davranmaları gerektiğini öğreten politikalar, prosedürler ve eğitim programlarını içerir. Etkinlikleri, uyuma bağlıdır ve genellikle gözetim mekanizmaları gerektirir (Hopkin & Thompson, 2022).
3. **Tespit edici kontroller**, meydana gelen risklerin etkilerini belirlemeye yönelik mekanizmalardır (Akçakanat, 2012). Tespit edici kontroller, bir risk olayının ne zaman meydana geldiğini belirleyerek geriye dönük olarak çalışır. Olayın kendisini önlemezler, ancak zamanında müdahale ve kurtarma imkânı sağlarlar. Örnekler arasında denetimler, mutabakatlar ve izleme sistemleri sayılabilir.
4. **Düzeltilici kontroller**, hâlihazırda gerçekleşmiş riskleri ele alır ve bunların etkisini azaltmayı veya koşulları eski haline getirmeyi amaçlar. Bunlar arasında olay müdahale planları, sigorta talepleri süreçleri veya hizmetlerin eski haline getirilmesi sayılabilir. Sonuçların yönetilmesine yardımcı olurlar, ancak olayların meydana gelme olasılığını etkilemezler ve etkinlik açısından değerlendirilmesi zor olabilir (Hopkin & Thompson, 2022).

Kontrol faaliyetlerinin geliştirilmesi ve uygulanması, kuruluşun yapısı, kültürü ve çalışma ortamıyla uyumlu olmalıdır (Marchetti, 2012). COSO (2004), kontrol sistemlerinin kuruluşlar arasında standartlaştırılmak yerine özelleştirilmesi gerektiğini vurgulamaktadır. Buna göre, kontrol faaliyetleri, sistem veya süreç geliştirmenin ilk aşamasında tasarlanmalı ve verimlilik ve maliyet etkinliği sağlanmalıdır. Manuel, otomatik ya da her ikisinin birleşimi şeklinde yürütülebilen kontrol faaliyetleri, risk yönetiminin sürdürülebilirliği ve etkinliğinin sağlanması amacıyla KRY çerçevesine entegre edilerek uyum içinde çalışması sağlanmalıdır (Marchetti, 2012).

Kontrol uygulaması maliyet ve risk önemi arasında bir dengeyi yansıtmalıdır. Bir kontrolün maliyetinin, önlemeye çalıştığı potansiyel kaybı aşmaması gerekir. Etki ve olasılık

değerleri yüksek olan risklere yönelik yeterli kontrol geliştirilebilmesini teminen kaynakların önceliklendirilmesi esastır (Dinapoli, 2016).

Tek bir kontrol türü, evrensel olarak yeterli olmadığı için, yönetim, birden fazla kontrolün gerekli olup olmadığını veya bir kontrolün diğerinin yerine geçip geçemeyeceğini belirlemek üzere bağlamı değerlendirmelidir. Hangi kontrollerin seçileceği maliyetlerin ve faydaların kapsamlı bir şekilde değerlendirilmesini gerektirir ve kurumsal risklere özel ve orantılı bir yanıt verilmesini sağlar (Dinapoli, 2016).

1.4.3.3. Risk Yanıt Planının Hazırlanması

Risk yönetimi sürecinin önemli bir aşaması, kuruluşun önceden tanımlanmış stratejileriyle uyumlu risk yanıt planları oluşturmak ve bunların etkili bir şekilde uygulanmasını sağlamaktır. Risk yanıt planlaması, tehditleri ele almak ve azaltmak için stratejiler geliştirmeyi ve bunların maliyet, zamanlama ve kalite üzerindeki etkilerini değerlendirerek uygun şekilde yönetmeyi amaçlar (Olson & Wu, 2020).

Risk yanıt planı, “kuruluşun belirli riskler için seçtiği yanıt stratejilerinin nasıl uygulanacağını ayrıntılı şekilde açıklayan plan” olarak tanımlanabilir. Risk yanıt planı, seçilen eylemlerin uygulanma yöntemini, sorumluları, kaynakları ve beklenen faydaları açıkça ortaya koymalı; performans ölçütleri, kısıtlamalar, izleme ve raporlama gerekliliklerini içermelidir. Eylemlerin önceliklendirilmesi ve sürekli izleme, tedavi etkinliği açısından kritiktir (ISO, 2009). Bu planlar, risklerin niteliğine göre uyarlanır ve kuruluşun genel hedefleriyle uyumludur.

Etkili yanıt planları, tanımlanan eylemlerin yanı sıra sorumlulukların dağıtılması, gerekli kaynakların tahsisi, uygulama zaman çizelgeleri ve izleme mekanizmalarını da içerir. Bu kapsamlı yapı, planların sadece teorik yapılar olmamasını ve operasyonel olarak uygulanabilir olmasını sağlar.

Risklerin değişken doğası göz önüne alındığında, yanıt planları sürekli izlenmeli ve ortaya çıkan veriler ışığında güncellenmelidir. Risk ortamındaki değişiklikler, stratejilerin ve yanıt mekanizmalarının ilgi ve etkinliğini korumak için periyodik olarak yeniden değerlendirilmesini gerektirir. Bu yinelemeli yaklaşım, kuruluşun dinamik tehditlere ve belirsizliklere uyum sağlama kapasitesini artırır.

1.4.3.4. Beklenmedik Durum Planlarının Hazırlanması

Beklenmedik durum yaklaşımı, belirli bir riskin gerçekleşmesi halinde ortaya çıkan olumsuz etkisini azaltmayı amaçlamaktadır (Ecsite, 2015). PMI (2018), Beklenmedik Durum Planını, “riske ilişkin tercih edilen stratejinin tam olarak etkili olmadığına anlaşılmaması ya da önceden tanımlanmış bir riskin meydana gelmesi durumunda, uygulanmak üzere geliştirilen plan” olarak tanımlamaktadır. Söz konusu plan, ISO 22301 (2019) standardında “belirli bir riskin ya da olayın gerçekleşmesi durumunda devreye girmek üzere hazırlanan, önceden tanımlanmış bir eylem planı” olarak ifade edilmektedir.

Beklenmedik durum planı, kuruluşun hızlı ve etkili şekilde tepki verebilmesini sağlayan yedek plandır. Risk yönetimi ve kurumsal dayanıklılık bağlamında kritik öneme sahiptir. Plan, en sorunlu senaryoların gerçekleşmesi durumunu dikkate alarak oluşturulur.

Operasyonel sürekliliği etkileyen herhangi bir olay, olay önceden tanımlanmışsa Beklenmedik Durum Planı; olay önceden tanımlanmamışsa Acil Durum Planı gibi iş sürekliliğine yönelik planlar aracılığıyla yönetilir.

1.4.4. Yanıt Planının Uygulanması

Risk yanıt planının uygulanması, riskler için belirlenen yanıt stratejilerinin pratikte hayata geçirilmesidir. Uygulama sürecinde, belirlenen kontrol faaliyetlerinin sistematik biçimde yürütülmesi önem arz etmektedir. Anılan kontrol önlemlerinin uygulanması genellikle bölüm yöneticilerinin katılımını gerektirir (Gregory, 2003). Risk yanıtlarının uygulanması genellikle bir zaman çizelgesine göre yürütülmekte; faaliyetler bahse konu çizelgeye göre gerçekleştirilmektedir.

Uygulama sırasında, kuruluşun yönetsel, yapısal ve kültürel bağlamlarını dikkate almak önemlidir. Uygulama, tüm ilgili paydaşların aktif katılımıyla, açıkça tanımlanmış rol ve sorumluluklarla desteklenmelidir.

Risk yanıtlarının uygulanması sırasında elde edilen bulgular, artık riskin yeniden değerlendirilmesine olanak tanır ve bu sayede önceden kabul edilebilir görülen bir risk, değişen koşullarda yeniden ele alınabilir. Ayrıca, uygulama süreci boyunca ortaya çıkabilecek ikincil risklerin belirlenmesi ve mevcut planla entegre bir şekilde yönetilmesi gerekir.

1.4.5. İzleme ve Değerlendirme

KRY sürecinin başarısı, risk yanıt planlarının uygulanmasına, izlenmesine, değerlendirilmesine ve gerektiğinde güncellenmesine bağlıdır. Süreçte risk yanıtlarının uygulanmasını takiben, kuruluşlar risk yanıt eylemlerinin etkinliğini, uygunluğunu ve yeterliliğini sağlamada önemli rol oynayan sürekli izleme ve değerlendirme aşamasına geçerler. Bu aşama, karar vericilerin seçilen yanıtların amaçlandığı gibi işleyip işlemediğini, değişen iç ve dış koşullara uyumlu olup olmadığını ve riskleri kabul edilebilir eşikler içinde tutmak için herhangi bir ayarlamaya gerek olup olmadığını belirlemelerine olanak tanır.

İzleme ve değerlendirme aşaması, kontrol başarısızlıklarının veya verimsizliklerin zamanında tespit edilmesini ve riskler artmadan önce düzeltici önlemlerin alınmasını sağlayarak bir erken uyarı sistemi işlevi görür. Etkili izleme rutin işlemler, değerlendirme araçları veya dış girdiler yoluyla tespit edilen eksikliklerin hızlı bir şekilde belirlenmesi, değerlendirilmesi ve çözüme kavuşturulmasını gerektirir (Marchetti, 2012). Kontrol sistemleri düzenli olarak izlenmeli, kuruluşlar kontrollerin yeni riskler getirip getirmediğini değerlendirmelidir (BSI, 2011).

Risk ölçütleri ve gösterge tabloları, performansı izlemeye ve stratejik uyumu desteklemeye yardımcı olur (Ketcham & Louisot, 2014). Göstergeler ve eşikler, yönetimin risk yanıtlarının etkinliğini değerlendirmesini ve risklerin kabul edilebilir seviyelerde kalmasını sağlayarak stratejilerin zamanında ayarlanmasına olanak tanır (COSO, 2018). Risk yanıt planlarındaki ilerleme, bir performans göstergesi olarak işlev görür ve daha kapsamlı raporlama için bilgi sağlar (ISO, 2009).

İzleme ve değerlendirme aşaması, tüm KRY sürecinin etkinliğini ve uyarlanabilirliğini sağlar. Risk yönetimi strateji ve eylemlerinin kurumsal değişiklikler, düzenleyici değişiklikler, paydaş beklentileri ve daha geniş risk ortamı ile uyumlu olarak gelişmesini sağlar. Sürekli izleme, stratejilerin etkinliğini güçlendirir ve üst yönetime güvence sağlar (Ketcham & Louisot, 2014). Aynı zamanda gerçekleşen olaylardan beslenerek öğrenmeyi destekler ve organizasyonel dayanıklılığı artırır (Akçakanat, 2012; Green, 2016).

İzleme, doğası gereği süreklilik arz etmektedir; tek seferlik, kapalı döngü bir süreç olarak işlev görmekten ziyade sürekli iyileştirmeyi teşvik etmektedir (Ketcham & Louisot, 2014). Değerlendirmelerin sıklığı, değişikliklerin ölçeğine, risk düzeyine ve mevcut izleme mekanizmalarından gelen bilgilere bağlıdır.

Etkili izleme, geçmiş risk değerlendirmelerinin doğruluğunu gözden geçirip gerekli revizyonları belirleyerek öğrenmeyi ve uyumu destekler, böylece risk yönetiminin dinamik ve geçerli kalmasını sağlar (Fraser & Simkins, 2010).

Kapsamlı bir izleme ve gözden geçirme süreci, kontrol etkinliğini değerlendirmek ve yeni riskleri belirlemek için tüm risk yönetimi aşamalarını kapsamalıdır. KRY'nin, personel, yapı veya hedeflerdeki değişikliklerle birlikte evrilerek gelişmesi, zaman içinde geçerliliğini ve performansını korumak amacıyla sürekli izleme ve bağımsız değerlendirmelerin bir kombinasyonunu gerektirmektedir (COSO, 2004; BSI, 2018). İzleme ve gözden geçirme sonuçları belgelenmeli, gerektiğinde paydaşlara raporlanmalı ve çerçevenin iyileştirilmesinde kullanılmalıdır (ISO, 2018).

Olumsuz olaylar meydana geldiğinde, etkiyi azaltmak için acil durum planlarını devreye almak veya alternatif stratejiler uygulamak gibi düzeltici önlemler alınmalıdır (Olson & Wu, 2020).

1.5. KRY'nin Sağladığı Faydalar

Yüksek ölçekli kurumsal başarısızlıklar, genelde değişimi tetikleyen birer katalizör olarak işlev görmektedir; yetersiz risk yönetiminin etkilerini ortaya koyarak kuruluşları daha stratejik ve kapsayıcı KRY uygulamalarına yönlendirmektedir. KRY'nin benimsenmesi, yönetimi güçlendirme ve paydaş güvenini yeniden tesis etme çabalarını yansıtmaktadır (Khan vd., 2016). Kuruluşlar, hızla değişen ve belirsizliklerle dolu ortamlarda faaliyet gösterirken, bu zorluklara karşı etkin bir çözüm olarak KRY'yi benimsemektedir (Akçakanat, 2012).

KRY, stratejik hedefleri engelleyebilecek riskleri belirleyerek, risk yönetimini kurumsal stratejiyle uyumlu hale getirir ve karmaşık ortamlarda bilinçli karar almayı sağlar (İbrahim & Esa, 2017). Bu bağlamda KRY, risk iştahını iş stratejileriyle uyumlu hale getirerek karar süreçlerini desteklemekte (Chapman, 2012); risk değerlendirmesini iyileştirmekte ve strateji ile risk iştahı arasındaki bağı kuvvetlendirmektedir (Marchetti, 2012). Aynı zamanda, stratejik kararlara risk düşüncesini entegre ederek kaynak ve maliyet optimizasyonuna katkı sağlamaktadır (Lam, 2014). Bu yönüyle KRY, sürdürülebilir rekabet avantajı elde edilmesine, risk yönetimi maliyetlerinin azaltılmasına ve genel iş performansının artırılmasına hizmet etmektedir. Risk sahipliğini, zamanında müdahaleyi ve stratejik planlamaya riskin entegre edilmesini teşvik ederken, dinamik karar alma süreçlerini desteklemektedir (Protiviti, 2006).

KRY, risk-getiri eğrisi gibi araçlarla beklenen sonuçlarla olası olumsuzluklar arasında denge kurarak, risk-getiri profilini optimize eder (Lam, 2017) ve bu sayede zaman ile sermayenin etkin tahsisini mümkün kılar (Chapman, 2012). Ayrıca finansal, fiziksel ve entelektüel varlıkları koruyarak rekabet gücünü sürdürmeye katkı sağlar (Gregory, 2003), kurumsal kaynakların daha verimli kullanılmasını destekler (Hallowell vd., 2013).

KRY, risklerin şeffaf iletimini destekleyerek paydaş güvenini ve şirket değerini artırır (Hallowell vd., 2013); finansman ve sermaye maliyetlerini azaltır, kârlılığını artırır. Finansal raporlamanın doğruluğunu geliştirir ve kurumsal yönetişimi güçlendirir (Hopkin & Thompson, 2022). İlave olarak, silo temelli araçlara bağımlılığı azaltarak artık ve istenmeyen risklere odaklı portföy bazlı bir yaklaşım sunar (Lam, 2014) ve tahmin süreçlerini iyileştirerek daha bilinçli karar alınmasını sağlar (Marchetti, 2012).

Diğer taraftan KRY, yalnızca olumsuzlukları azaltmakla kalmaz; aynı zamanda fırsatların belirlenmesini ve yönetilmesini sağlayarak kârlılığını artırır (Chapman, 2012) ve yeni fırsatların ortaya çıkmasına imkân tanır. KRY, erken müdahale ile beklenmeyen kayıpları azaltır ve performans hedeflerine ilişkin belirsizliklerin öngörülmesini kolaylaştırır (Hopkin & Thompson, 2022).

KRY, operasyonel verimliliği ve kurumsal dayanıklılığı artırarak risk ve maliyetleri düşürür, süreçlerin önceliklendirilmesini sağlar ve kritik kontrollere odaklanarak gereksiz tekrarları azaltır (Hopkin & Thompson, 2022). Bu doğrultuda, değişime hazırlığı artırır, yasal uyumu destekler, belirsizlikleri daha iyi öngörmeye ve risk değerlendirmelerine duyulan güveni artırmaya yardımcı olur (Akçakanat, 2012). Ayrıca, proaktif risk yönetimini mümkün kılarak aksaklıkların azaltılmasını, operasyonel süreçlerin iyileştirilmesini ve iç kontrollerin güçlendirilmesini sağlar (Fraser & Simkins, 2010).

KRY, iş birimleri arasındaki karşılıklı bağımlılıkları fark ederek birimler arası iletişim ve koordinasyonu geliştirir (Gregory, 2003) ve böylece silo yaklaşımının aksine, risklerin bütüncül biçimde kurumsal düzeyde yönetilmesini sağlar.

KRY'nin uygulanması, risk verilerinin toplanmasına ve analizine dayanarak yöneticilerin sezgileri yerine deneyim ve verilere dayalı kararlar almasını sağlar, böylece yönetim etkinliğini artırır (İbrahim & Esa, 2017). Güvenilir bilgilerle zamanında karar almayı kolaylaştırır, performans öngörülebilirliğini artırır (Hopkin & Thompson, 2022). Ayrıca, geçmiş deneyimlerden öğrenmeyi ve kurumsal bilgi birikiminin gelişimini destekler (Chapman, 2012).

KRY, kuruluşların yasal, düzenleyici ve içsel yükümlülüklerini anlamasını ve bu yükümlülüklerle uyum sağlamasını kolaylaştırır (Fraser & Simkins, 2010). KRY, düzenleyici kurumlar veya savunucu kuruluşlar tarafından açılacak yasal süreçlerin riskini azaltırken, iş kazaları ve çalışanlarla ilgili yasal talepleri en aza indirerek sigorta maliyetlerini düşürür; ayrıca hatalı ürünlerden kaynaklı tüketici zararlarını önleyerek olası yasal yaptırımları engeller (Gregory, 2003).

Kurumsal yönetim açısından değerlendirildiğinde, risk rollerinin ve sorumluluklarının açık şekilde tanımlanması, hesap verebilirliği ve bilinçli risk azaltımı uygulamalarını desteklemektedir (İbrahim & Esa, 2017). Üst yönetim ve yönetim kurulu, KRY sayesinde belirsizlikleri yönetme, fırsatları değerlendirme ve paydaşlara güvence sunma yetkinliğine ulaşır (Protiviti, 2006). Ayrıca KRY, yönetim kurulu düzeyinde katılımı teşvik ederek aşırı risk alma eğilimini engellemekte, karar alma süreçlerinde öngörü ve sorumluluk bilincini artırmaktadır (Chapman, 2012).

Aynı zamanda KRY, yatırımcılar, düzenleyici kurumlar ve derecelendirme kuruluşları nezdindeki güvenilirliği güçlendirerek, kurumsal itibarı yükseltmektedir. Marka değerinin ve kuruluş imajının korunmasına yardımcı olmakta, pazar konumunun sürdürülmesi ya da güçlendirilmesini sağlamaktadır (Gregory, 2003). İlaveten, hissedar değerini artırmakta, kuruluşa ilişkin paydaş algısını pozitif yönde etkilemektedir (Hopkin & Thompson, 2022).

KRY, kuruluşların değişen risk ortamına karşı hazırlıklı olmasını ve bu değişimlere proaktif şekilde uyum sağlamasını sağlar (İbrahim & Esa, 2017), üretim kesintilerini önler, yasal sorumluluk riskini azaltır, operasyonel güvenilirliği artırır ve iş sürekliliğini korur (Gregory, 2003).

KRY, düşük olasılıklı ancak yüksek etkili risk senaryolarına karşı hazırlığı teşvik eder; senaryo analizi ve acil durum planlaması gibi araçlar kullanarak kurumsal dayanıklılığı artırır (Hallowell vd., 2013).

KRY, risk farkındalığını organizasyonun tüm seviyelerine ve işlevlerine yerleştirir (Chapman, 2012). Aynı zamanda, liderlik taahhüdü, performans teşvikleri ve risk profesyonellerinin kilit iş süreçlerine entegrasyonu aracılığıyla stratejik risk almayı destekleyen bir risk farkındalığı kültürü oluşturur (Hallowell vd., 2013).

KRY uygulamaları genellikle üst yönetim ve yönetim kurulu gözetiminde, çoğu zaman bir risk yöneticisi liderliğinde yapılandırılan merkezi bir sistem aracılığıyla yürütülür (Lam, 2014). Proaktif ve sistematik şekilde risk yönetimine yatırım yapan liderler, daha fazla verimlilik

kazancı elde eder ve kayıpları azaltırken; bu alanda yatırım yapmayan liderler krizlere tepkisel ve parçalı biçimde yaklaşmak zorunda kalmaktadır (Lam, 2014). KRY, iç denetim, düzenleme ve süreç iyileştirme faaliyetlerini entegre ederek yinelemeleri azaltmakta ve kontrol mekanizmalarına ilişkin hesap verebilirliği artırmaktadır (Marchetti, 2012).

KRY'nin kuruluşlara sağladığı faydalara ilişkin literatürde yer verilen hususlar tematik olarak Tablo 1'de özetlenmektedir.



Tablo 1: KRY'nin Kuruluşlara Sağladığı Faydalar

Fayda	Açıklama	Kaynak
1. Stratejik Uyum ve Risk-Getiri Dengesi	KRY, stratejik hedeflerle risk yönetimini bütünleştirir; risk iştahını stratejilerle uyumlu hale getirerek kaynak ve sermaye tahsisini optimize eder, kurumsal stratejiye bütüncül bir yön kazandırır.	Chapman (2012); Marchetti (2012); Ibrahim ve Esa (2017); Lam (2014, 2017)
2. Bilinçli ve Veri Dayalı Karar Alma	KRY, risk analizlerini karar süreçlerine entegre eder; veriye dayalı öngörülerle stratejik seçimlerin kalitesini artırır, belirsizlik ortamında rasyonel ve zamanında karar vermeyi kolaylaştırır.	Marchetti (2012); Lam (2014); Ibrahim ve Esa (2017)
3. Kurumsal Yönetişim ve Hesap Verebilirlik	KRY, risk rollerini ve sorumluluklarını netleştirerek yönetişimi ve hesap verebilirliği güçlendirir; yönetim kurulu gözetiminde risk bilinci ve kontrol disiplini kurumsallaştırır.	Protiviti (2006); Chapman (2012); Ibrahim ve Esa (2017); Hopkin ve Thompson (2022)
4. Paydaş Güveni ve Kurumsal İtibar	KRY, şeffaf risk iletimi ve doğru finansal raporlama yoluyla paydaş güvenini artırır; yatırımcılar, düzenleyici kurumlar ve toplum nezdinde güvenilirliği ve itibarı güçlendirir.	Gregory (2003); Hallowell vd. (2013); Khan vd. (2016); Hopkin ve Thompson (2022)
5. Operasyonel Verimlilik ve Süreç İyileştirme	KRY, süreçleri entegre ederek tekrarları ortadan kaldırır, kritik kontrollere odaklanır, operasyonel verimliliği artırır ve maliyetleri düşürür; proaktif müdahalelerle aksaklıkları önler.	Fraser ve Simkins (2010); Marchetti (2012); Hallowell vd. (2013); Hopkin ve Thompson (2022);
6. Risk Kültürü, Farkındalık ve İletişim	KRY, organizasyon genelinde risk farkındalığı ve öğrenme kültürü oluşturur; birimler arası koordinasyonu güçlendirir, silo yaklaşımını aşarak bütüncül bir risk iletişim ağı kurar.	Gregory (2003); Chapman (2012); Hallowell vd. (2013); Lam (2014)
7. Rekabet Avantajı ve Performans Artışı	KRY, risk fırsatlarını yöneterek sürdürülebilir rekabet avantajı sağlar; kurumsal varlıkları korur, performans öngörülebilirliğini artırır ve paydaş değerini yükseltir.	Gregory (2003); Chapman (2012); Lam (2014); Hopkin ve Thompson (2022)
8. Yasal Uyum ve Kurumsal Güvence	KRY, düzenleyici gerekliliklere uyumu kolaylaştırır, yasal ve operasyonel riskleri azaltır; kurumsal güvenilirlik ve meşruiyetin güçlenmesine katkı sağlar.	Gregory (2003); Fraser ve Simkins (2010)
9. Dayanıklılık, Süreklilik ve Proaktif Uyum Yeteneği	KRY, düşük olasılıklı fakat yüksek etkili olaylara karşı hazırlığı artırır; senaryo planlaması ve erken uyarı mekanizmalarıyla iş sürekliliğini ve kurumsal dayanıklılığı güçlendirir.	Gregory (2003); Hallowell vd. (2013); Lam (2014); Ibrahim ve Esa (2017); Hopkin ve Thompson (2022)

1.6. KRY'nin Uygulanmasındaki Zorluklar

Kurumsal Risk Yönetimi (KRY), teoride güçlü bir çerçeve olmakla birlikte kuruluşlarda uygulanmasında bir takım sınırlılıklar ve zorluklar yaşanmaktadır.

KRY'nin etkili bir şekilde uygulanması, net bir şekilde tanımlanmış sorumluluklar ve hesap verebilirlik mekanizmalarına sahip bir yönetim yapısı gerektirmektedir (Galloway & Funston, 2000). Risk Yönetimine ilişkin rol ve sorumlulukların belirsizliği, risklerin belirlenmesi ve azaltılmasında verimsizlik ve boşluklar yaratarak etkili bir KRY sürecinin yürütülmesini engellemektedir (Moshesh vd., 2018; Alawattegama, 2022). Ayrıca, bazı yöneticiler riskle ilgili sorumluluklarının yeteri kadar farkında ve bilincinde değildir, bu durum KRY süreçlerinin etkin bir şekilde ilerlemesine engel olmaktadır (Marchetti, 2012).

Risk yönetimi tüm çalışanların sorumluluğu olmakla birlikte, KRY'ye özel risk görevlilerinin atanmaması, bu işlevin diğer görevlerle birleşmesine ve bağımsız şekilde gözetilmemesine yol açmaktadır (Vhanda vd., 2023). Riskle ilgili rollerin iç denetimden ayrı tutulması, etkili gözetim ve açık iletişim için gereklidir (Fraser vd., 2024). Ancak birçok kuruluş, KRY'yi geleneksel denetim ve risk yönetimi işlevleriyle karıştırarak uygulamada tutarsızlığa neden olmaktadır (Fraser & Simkins, 2016).

KRY'nin stratejik hedeflerle uyumlu yürütülmesi için yönetimin desteği kritiktir. Ancak birçok kuruluşta üst yönetim gerekli beceri ve önceliğe sahip değildir (Fadun, 2013). Yönetim katılımı olmadan KRY stratejik kararlardan kopar, meşruiyet ve kaynak desteği azalır (Moshesh vd., 2018). Liderlik eksikliği KRY'nin otoritesini ve sürdürülebilirliğini zayıflatır, tutarsız uygulamalara neden olur (Kerstin vd., 2014; Renault vd., 2016).

KRY'nin etkili uygulanmasında kaynak ve yetenek eksiklikleri önemli bir engeldir. Bütçe kısıtları ve kurumsal öncelikler, KRY'ye yeterli zaman, maliyet ve dikkat ayrılmasını engeller. Nitelikli personel, teknoloji ve altyapı eksikliği yaygındır (Moshesh vd., 2018; Vhanda vd., 2023). Bu bağlamda KRY, birçok kuruluşta hâlâ maliyetli ve sürdürülemez görülmekte, bu da risk yönetimine olan temel yatırımları kısıtlamaktadır (Marchetti, 2012; Kerstin vd., 2014).

Parçalanmış yapılar ve silo yaklaşımı, KRY'nin etkinliğini azaltmaktadır. Renault vd. (2016), birçok kuruluşun hâlâ merkezi bir sistem yerine proje tabanlı risk anlayışına bağlı olduğunu belirtmektedir. Yazarlar, farklı disiplinlerdeki terminoloji farkının ortak risk dili geliştirilmesini zorlaştırdığını, bu durumun iletişimi zayıflattığını ve sonuç olarak zayıf iletişim ve sınırlı bilgi paylaşımının, risk bilgisinin akışını kısıtladığını ifade etmektedir. Risk

sorumluluklarının izole birimlerde kalması, bütüncül gözetimi engeller ve tutarsız değerlendirmelere yol açar (Hunziker, 2019).

Kuruluşlardaki katı işleyiş yapıları ve yerleşik kültürel normlar, KRY'ye direnç oluşturmakta ve özellikle hiyerarşik ve geleneksel sektörlerde uygulamayı zorlaştırmaktadır (Renault vd., 2016). KRY'nin stratejik bir değer yerine uyum yükü olarak algılanması, kurumsallaşmayı engeller (Fadun, 2013). Bu durum, güç dengelerini ve konfor alanlarını tehdit ettiği için savunmacı tepkilere yol açabilir (Kerstin vd., 2014). Geleneksel yöntemlere bağlılık ve hesap verebilirlik kaygısı, çalışan ve yöneticilerde direnci artırır (Moshesh vd., 2018). Oysa başarılı bir KRY uygulaması, yalnızca güçlü kontrolleri değil; aynı zamanda inovasyon, dürüstlük ve sorumlu risk almayı destekleyen bir kültürü de gerektirir (Galloway & Funston, 2000).

KRY ilkelerine yönelik düşük farkındalık ve anlayış, çalışanlar ile yöneticilerin risk yönetimini sahiplenmesini zayıflatmakta ve katılımı sınırlamaktadır (Zhao vd., 2015). Birçok kuruluş, tüm riskleri olumsuz olarak değerlendirip stratejik risk almaktan kaçınmakta; bu durum özellikle KOBİ'lerde stratejik entegrasyonu engellemektedir (Fadun, 2013).

KRY'nin stratejik ve operasyonel süreçlerden ayrıştırılması, karar alma süreçlerinde bilgi üretimini zayıflatmakta ve risk yönetiminin etkisini azaltmaktadır. Birçok kuruluş, KRY'yi planlama ve performans sistemleriyle entegre etmekte zorlanmakta, bu da potansiyel katma değeri sınırlamaktadır (Fraser & Simkins, 2016). Özellikle kısa vadeye odaklanarak çalışan sektörlerde KRY, operasyonlardan kopuk ve bürokratik bir yük olarak görülmektedir (Zhao vd., 2015; Renault vd., 2016). Bu durum, KRY'nin stratejik bir araçtan çok bir uyum aracı olarak algılanmasına yol açmaktadır (Fadun, 2013).

KRY uygulamalarında uyum amaçlı raporlamaya aşırı odaklanması, KRY'nin stratejik bir araç olma işlevini zayıflatmaktadır (Fraser vd., 2024). Kayıt tutma ve denetim odaklı raporların öncelik kazanması, KRY'yi bürokratik bir sürece indirgemektedir. Raporlama, karar alma süreçlerini destekleyen ve paydaş katılımını sağlayan bir yan ürün olarak ele alınmalıdır.

Düşük veri kalitesi ve zamanında bilgiye erişim eksikliği, risklerin doğru belirlenmesini, analizini ve müdahale stratejilerinin geliştirilmesini zorlaştırmaktadır (Fraser & Simkins, 2016). Bu durum, risk yönetiminin gerçeklerden kopmasına ve karar süreçlerinin zayıflamasına yol açmaktadır (Alawattegama, 2022; Vhanda vd., 2023). Ayrıca, iletişim eksiklikleri ve yetersiz bilgi paylaşımı, risklerin birimler arasında parçalı bir şekilde ele alınmasına neden olmaktadır (Moshesh vd., 2018).

Günümüzde kuruluşlar, dinamik, karşılıklı bağımlı ve ölçülmesi güç risklerin hâkim olduğu karmaşık bir ortamla karşı karşıyadır. Karar alma özerkliği ile tanımlı risk toleransı arasındaki dengeyi kurmak zorluk yaratmakta (Alawattegama, 2022); risk modelleri ise çoğunlukla destekleyici araçlar yerine nihai değerlendirme araçları olarak kullanılmaktadır (Fraser vd., 2024). Bu durum, belirsizliklerin ve bağımlılıkların göz ardı edilmesine neden olurken, bilişsel ve motivasyonel önyargılar da risk analizlerinde büyük ölçüde ihmal edilmektedir (Hunziker, 2019).

KRY'ye ilişkin bilgi eksikliği, kuruluşların kendilerine uygun çerçeveyi seçmelerini zorlaştırmakta; seçilen çerçeveler ise çoğu zaman yetersiz uygulanmakta ve stratejik süreçlerle yeterince bütünleşmemektedir (Fadun, 2013; Moshesh vd., 2018). Mevcut çerçevelerdeki katı ve statik prosedürler, ani ve gelişen riskleri yakalamakta yetersiz kalmakta, bu da risk profillerinin güncelliğini yitirmesine yol açmaktadır (Fraser vd., 2024). Risk yönetimi açısından olgunlaşmış kuruluşlar ise KRY'yi kendi karar alma ihtiyaçlarına göre uyarlamakta ve şeffaf, kullanıcı dostu araçlarla desteklemektedir (Galloway & Funston, 2000).

KRY, temel süreçlere entegre edilmediğinde performans yönetimi ve kaynak tahsisi gibi alanlardaki etkisi azalır (Kerstin vd., 2014). Sürekli değerlendirme ve izleme gerektirse de, idari yük, personel eksikliği ve finansal kısıtlar bu işlevlerin yerine getirilmesini zorlaştırmakta ve müdahaleleri geciktirmektedir (Galloway & Funston, 2000; Vhanda vd., 2023).

Stratejik ve operasyonel risklerin sayısallaştırılamaması, KRY süreçlerinde bu risklerin yeterince temsil edilmemesine neden olmaktadır (Alawattegama, 2022). Kuruluşlar, maddi olmayan veya karmaşık riskleri ölçmekte zorlanmakta, bu da ihmal edilmelerine ve stratejik hedeflerle uyumun sağlanamamasına yol açmaktadır (Fraser & Simkins, 2016). Araçlar mevcut olsa da (örneğin senaryo analizi, HTEA), yeterince kullanılmamaktadır (Hunziker, 2019).

Dijital teknolojilere bağımlılığın artması, karmaşık siber tehditlerle karşı karşıya kalma riskini artırmakta ve KRY'yi zorlaştırmaktadır (Wang, 2024). Küresel faaliyetler ve farklı düzenleyici sistemler KRY sürecini karmaşıklarlaştırırken (Wang, 2024), zayıf kurumsal yapılar ve ekonomik dalgalanmalar entegrasyonu engellemektedir (Vhanda vd., 2023). Ayrıca, uzun vadeli değer yaratma ile kısa vadeli hissedar beklentileri arasındaki denge, stratejik risk uyumunu zorlaştırmaktadır (Galloway & Funston, 2000).

KRY'nin uygulanmasında kuruluşlarda karşılaşılan zorluklara ilişkin literatürde yer verilen hususlar tematik olarak Tablo 2'de özetlenmektedir.

Tablo 2: KRY'nin Kuruluşlarda Uygulanmasında Karşılaşılan Zorluklar

Zorluk	Açıklama	Kaynak
1. Rol, Sorumluluk ve Yönetişim Belirsizlikleri	KRY uygulamalarında rollerin, sorumlulukların ve hesap verebilirlik mekanizmalarının net tanımlanmaması ve gözetim, iç denetim ve risk yönetimi fonksiyonlarının karıştırılması süreci zayıflatmakta, tutarsız uygulamalara ve boşluklara yol açmaktadır.	Galloway ve Funston (2000); Fraser ve Simkins (2016); Moshesh vd. (2018); Alawattagama (2022); Vhanda vd. (2023); Fraser vd. (2024)
2. Liderlik Eksikliği ve Üst Yönetim Desteğinin Zayıflığı	Üst yönetimin stratejik vizyon, farkındalık ve öncelik eksikliği, KRY'nin kurumsal kararlardan kopmasına, meşruiyet kaybına ve kaynak yetersizliğine yol açmakta; liderlik eksikliği uygulamaların otoritesini ve sürdürülebilirliğini zayıflatmaktadır.	Fadun (2013); Kerstin vd. (2014); Renault vd. (2016); Moshesh vd. (2018)
3. Kaynak, Yetenek ve Altyapı Kısıtları	KRY alanında nitelikli uzman eksikliği ile teknolojik kaynakların yetersizliği ve maliyet algısı nedeniyle birçok kuruluşta KRY süreçleri yüzeysel, kesintili veya sürdürülemez biçimde yürütülmektedir.	Marchetti (2012); Kerstin vd. (2014); Moshesh vd. (2018); Vhanda vd. (2023)
4. Silo Yaklaşımı, Parçalı Yapılar ve Zayıf İletişim	KRY'nin farklı birimler arasında bütünleştirilememesi, proje tabanlı ve silo temelli yaklaşımlar, ortak risk dili eksikliği ve zayıf bilgi paylaşımı nedeniyle bütüncül gözetim ve öğrenmeyi engellemektedir.	Renault vd. (2016); Moshesh vd. (2018); Hunziker (2019)
5. Kurumsal Kültür, Direnç ve Farkındalık Sorunları	Hiyerarşik, geleneksel ve savunmacı kültürler KRY'ye direnç göstermekte; risk yönetimi bir uyum yükü veya kontrol aracı olarak algılandığında, katılım, sahiplenme ve stratejik değer yaratma potansiyeli azalmakta; düşük farkındalık, KRY'nin yaygınlaşmasını sınırlandırmaktadır.	Galloway ve Funston (2000); Fadun (2013); Kerstin vd. (2014); Zhao vd. (2015); Renault vd. (2016); Moshesh vd. (2018)
6. Stratejik Entegrasyon ve Bürokratikleşme	KRY'nin planlama, performans ve stratejik yönetim sistemlerine entegre edilememesi ve aşırı raporlama, denetim odaklı süreçler ve kısa vadeli bakış açısı nedeniyle KRY'nin stratejik bir araç yerine uyum odaklı bürokratik bir işlev kazanmasına yol açmaktadır.	Fadun (2013); Zhao vd. (2015); Fraser ve Simkins (2016); Renault vd. (2016); Fraser vd. (2024)
7. Bilgi, Veri ve Analitik Yetersizlikleri	Düşük veri kalitesi, zamanında bilgiye erişim eksikliği ve yetersiz analitik kapasite, risklerin doğru belirlenmesini ve önceliklendirilmesini zorlaştırmakta, bilişsel önyargıların etkisiyle değerlendirmelerin öznel hale gelmesine yol açmaktadır.	Fraser ve Simkins (2016); Hunziker (2019); Alawattagama (2022); Vhanda vd. (2023); Fraser vd. (2024)
8. Karmaşık Ortam, Teknolojik ve Düzenleyici Zorluklar	Dijitalleşme, siber tehditler, küresel düzenlemeler ve ekonomik dalgalanmalar KRY süreçlerini karmaşıklaştırmakta; katı çerçeveler ve statik prosedürler yeni risk türlerini yakalamakta yetersiz kalmaktadır. Uzun vadeli değer yaratma ile kısa vadeli performans baskıları arasındaki gerilim stratejik uyumu zorlaştırmaktadır.	Galloway ve Funston (2000); Fraser vd. (2024); Vhanda vd. (2023); Wang (2024)

İKİNCİ BÖLÜM

KURUMSAL DAYANIKLILIK

2.1. Dayanıklılık Kavramı

Dayanıklılık kavramı, geçmişten günümüze yüklendiği anlam ve kullanıldığı disiplinler bakımından çeşitli değişimlere uğramıştır. Dayanıklılık kavramı, başlangıçta psikoloji ve malzeme bilimiyle sınırlıyken, zamanla afet, iklim, sosyo-ekolojik ve kurumsal alanlarda da kritik bir unsur haline gelmiştir.

Kökeni Latince esneklik, sıçrama, geri gelme anlamlarına gelen resilire kelimesine dayanan dayanıklılık (resilience) terimi, günümüzün modern İngilizce-Türkçe sözlüklerinde aşağıdaki şekillerde tanımlanmaktadır.

- 1. İnsanların veya nesnelerin şok, yaralanma vb. gibi hoş olmayan bir olaydan sonra hızla iyileşme yeteneği, 2. Bir maddenin büküldükten, gerildikten veya bastırıldıktan sonra orijinal şekline geri dönme yeteneği (Oxford English Dictionary Online, t.y.).
- 1. Bir maddenin büküldükten, gerildikten veya bastırıldıktan sonra normal şekline dönme yeteneği, 2. Zor veya kötü bir şey olduktan sonra tekrar mutlu, başarılı vb. olma yeteneği (Cambridge Dictionary Online, t.y.).
- 1. Kauçuk gibi bir maddenin preslendikten veya büküldükten sonra orijinal şekline dönme yeteneği, 2. Zor bir durum veya olaydan sonra tekrar güçlü, mutlu veya başarılı olma yeteneği (Longman Dictionary Online, t.y.).
- 1. Bir maddenin veya nesnenin büküldükten, gerildikten veya bastırıldıktan sonra orijinal şekline dönme yeteneği, 2. Bir kişinin bir hastalık, hayal kırıklığı veya başka bir sorundan sonra yeniden sağlıklı, mutlu veya güçlü olma yeteneği (Macmillan English Dictionary, 2004).

Sözlük tanımlarına bakıldığında, kavramın fiziksel (nesne) ve psikolojik (insan) dayanıklılığına yönelik olduğu görülmekle birlikte, tanımlarda (1) fiziksel, (2) psikolojik veya sosyal dayanıklılık ile (3) uyum ve yeniden yapılanma hususlarına ortak vurgu yapıldığı görülmektedir.

Dayanıklılık, farklı düzeylerde esneklik, uyum ve yeniden yapılanma kapasitesini ifade eden, giderek önem kazanan disiplinler arası bir kavramdır. En genel haliyle, belirsizlik ve zorluklara karşı ayakta kalma ve dönüşerek güçlenme sürecini temsil etmektedir.

Resilience kavramı Türkçeye çoğunlukla dayanıklılık olarak çevrilmekle birlikte, kimi çalışmalarda dirençlilik olarak kullanıldığı da görülmektedir. Direnç kelimesi, Türkçede “dayanma, karşı koyma gücü; dayanırlık, mukavemet” anlamlarını taşımakta; dirençlilik kelimesi “karşı koyma, mukavemet etme gücüne sahip olma durumu” olarak tanımlanmaktadır. Tanımlar, dirençlilik kelimesinin tek yönlü bir tepkiyi ifade ettiğini ve mevcut durumun korunmasına yönelik olduğunu göstermektedir.

Buna karşılık, dayanıklılık (resilience) kavramı mevcut durumun korunmasına ilave olarak, hazırlık, yeni duruma uyum ve dönüşüm gibi çok aşamalı ve çok yönlü bir kapasiteyi ifade etmektedir. Lake (2013), resistance kavramını “bir ekosistemin bir bozucu etkiyi kayıp yaşamadan atlatabilme kapasitesi”; resilience kavramını “bir ekosistemin, önemli düzeyde kayıplar yaşamış olsa bile, bir bozucu etkiden sonra toparlanabilme kapasitesi” olarak tanımlamaktadır. Yazarın tanımlarından yola çıkarak, resistance ile *bozucu etkiye karşı koyma, etkilenmeme, yapısını koruma kapasitesine*; resilience ile *toparlanma kapasitesi, kayıplardan sonra geri dönme yetisine* vurgu yapıldığı görülmektedir.

Bu noktadan hareketle, iklim ve enerji gibi olumsuz durumların absorbe edilerek, mevcut durumun korunmasının söz konusu olduğu çalışma alanlarında dirençlilik ifadesinin, olumsuz durumun gerçekleşmesi ve akabinde toparlanma süreçlerinin aktif olacağı toplumsal ve kurumsal yönetim gibi çalışma alanlarında dayanıklılık ifadesinin kullanılmasının uygun olacağı söylenebilir. Bu bağlamda, tezde resilience kavramının Türkçe karşılığı olarak “dayanıklılık” kelimesi tercih edilecektir.

Öte yandan Conz ve Magnani (2020), literatürde dayanıklılık kavramının, çok çeşitli yorum ve tanımlarla karakterize edilebilen soyut bir kavramı temsil ettiğini vurgulamaktadır. Dayanıklılık konusu birçok farklı alanda çalışılmış ve alana özgü dayanıklılık tanımları geliştirilmiştir; ancak disiplinler arası farklılıklar nedeniyle kavramın ortak bir tanımı bulunmamaktadır. Kavramın tanımı, genellikle çalışmayı gerçekleştiren yazarın bakış açısına göre şekillenmekte olup, kabul edilmiş ortak bir tanımı bulunmamaktadır (Conz & Magnani, 2020; Mentges vd., 2023). Bu kapsamda, örneğin Banahene vd. (2014) çalışmasında 12 farklı tanıma yer vermiştir. Davidson vd.’nin (2016) çalışmasında 15, Wied vd.’nin (2020) çalışmasında 251, Nipa’nın (2023) çalışmasında 23 adet tanıma yer verildiği görülmektedir.

2.1.1. Kavramın Kökenleri

Dayanıklılık kavramının kökeni Latince “geri sıçramak, geri tepmek” anlamlarına gelen *resilire* kelimesine dayanmaktadır. Seneca, Pliny the Elder, Ovid ve Cicero gibi antik dönem (MÖ 8. yy. ile MS 5. yy. arası) yazarları, *resilire* ifadesini sıçrama, küçülme ve geri tepme durumlarını aktarmak üzere kullanmışlardır (Alexander, 2013; Williams vd., 2017).

Resilire terimi, Fransızcaya “geri çekilmek, iptal etmek” anlamlarına gelen *résiler* olarak geçmiş ve 16. yüzyılda İngilizceye geri çekilmeyi veya eski haline dönmeyi ifade eden *resile* kelimesi olarak girmiştir (Graveline & Germain, 2022).

Sir Francis Bacon, 1625 yılında yayımladığı “*Sylva Sylvarum*” adlı eserinde sesin geri tepmesini tanımlamak için “dayanıklılık” kelimesini kullanarak, terimin bilimsel anlamda ilk kullanımlarından birini gerçekleştirmiştir (Alexander, 2013). Dayanıklılık kavramının bilimsel literatüre girmesi 1800’lü yıllara kadar uzanmaktadır. Dayanıklılığın, sistemler üzerine ilk uygulaması 19. yüzyılın ortalarında mekanikte (fizik) yapılmıştır (Pimm, 1984).

2.1.2. Kavramın Gelişimi

19. yüzyılın sonlarına doğru İskoç mühendis William J. M. Rankine, bilimsel bir bakış açısıyla yaklaşarak kavramın ilk tanımını mekanik üzerine yayımladığı “*A Manual of Civil Engineering*” isimli kitabında yapmıştır. Rankine (1862) dayanıklılığı, “bir malzeme, parça ya da yapının deforme olmaksızın absorbe edebileceği enerji kapasitesi” olarak tanımlamıştır. Timoshenko ve Goodier (1951), malzemelerin elastik davranışlarını, stres (gerilme) ve strain (şekil değiştirme) arasındaki ilişkileri kullanan matematiksel modellerle açıklamış ve elastisite teorisini genişleterek dayanıklılık kavramının modern mühendislikte kullanılmasının yolunu açmıştır.

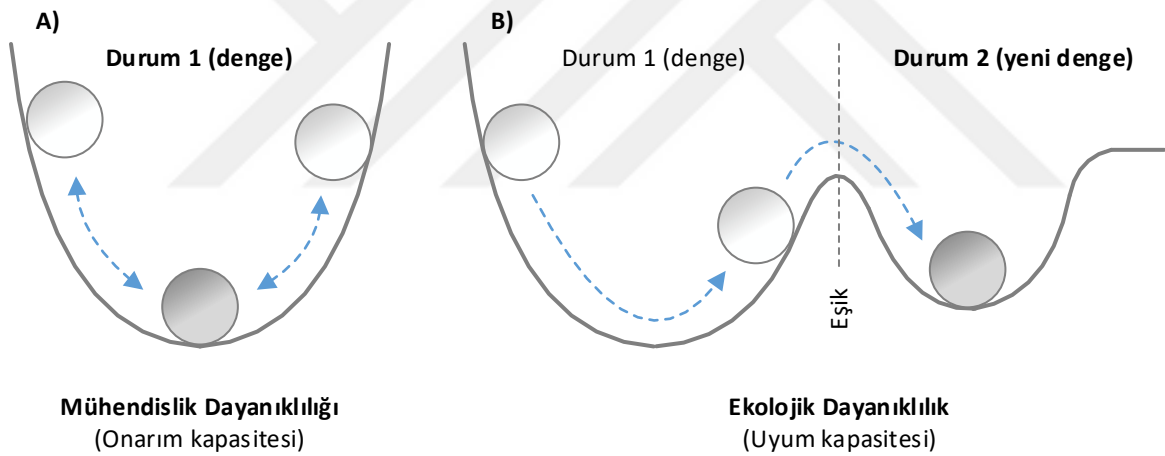
Psikoloji alanında dayanıklılık, ilk olarak İkinci Dünya Savaşı kaynaklı travma yaşayan çocukların duygusal tepkileri üzerinden ele alınmış (Freud & Burlingham, 1944) ve kavram, Werner vd. (1971) tarafından olumsuz koşullarda sağlıklı gelişimi tanımlamak için kullanılmıştır. Werner ve Smith (1982), dayanıklılığı zorluklarla başa çıkmayı sağlayan özellikler olarak tanımlamıştır.

C. S. Holling (1973) “Ekolojik Sistemlerin Esnekliği ve İstikrarı” başlıklı öncü makalesinde geleneksel denge temelli modellerini, doğal sistemlerin karmaşıklığını göz ardı

ettikleri için eleştirmiş; durağanlık ile dayanıklılığı birbirlerinden ayırarak, dayanıklılığı ekolojik bir çerçevede yeniden yorumlamıştır. Çalışmada kararlılık; “bir sistemin geçici bir rahatsızlıktan sonra önceki denge durumuna geri dönme kabiliyeti” olarak tanımlarken dayanıklılık; “önceki duruma dönmek yerine, değişikliklere veya stres faktörleri karşısında uyum sağlayarak yeni bir denge noktasında varlığını sürdürebilme kabiliyeti” olarak ifade edilmiştir.

Şekil 2’de Holling (1973) tarafından tanımlanan iki temel dayanıklılık yaklaşımı gösterilmektedir. Mühendislik dayanıklılığı¹, sistemin tek bir kararlı denge noktasına sahip olduğu varsayımına dayanmakta ve sistemin, bir dış şok sonrasında anılan dengeye ne kadar hızlı geri dönebildiğini ifade etmektedir. Buna karşılık ekolojik dayanıklılık, sistemin birden fazla kararlı duruma sahip olabileceğini ve sistemin dış etkiler altında mevcut dengesinden farklı olarak yeni bir kararlı duruma geçiş yapabilme kapasitesini vurgulamaktadır.

Şekil 2: Mühendislik Dengesi ve Ekolojik Denge



Kaynak: Thoms vd., (2018)

Holling (1973), doğal sistemlerin dinamik ve dış etkenlere açık olduğunu vurgulayarak, değişime uyum sağlama kapasitesine odaklanmış ve süreklilik temelli modelin daha açıklayıcı olduğunu savunmuştur. Süreklilik temelli modellerde uyarlanabilirlik ve esneklik perspektifleri önem arz etmektedir. Bu doğrultuda Holling’in çalışması sonucunda, ekosistemlerin kararlı varlıklar olarak kabul edildiği bakış açısından, zaman içinde değişen ve dönüşen dinamik

¹ Holling’in 1973 yılındaki çalışmasında “mühendislik dayanıklılığı” şeklinde bir ifade kullanmamıştır. Bu ifade sonraki yıllarda Pimm (1984) ve Holling (1996) tarafından gerçekleştirilen çalışmalarda kavramsallaştırılmaktadır.

kapasiteye sahip varlıklar olarak değerlendirilmesi şeklinde bakış açısında bir değişim söz konusu olmuştur (Alexander, 2013; Graveline & Germain, 2022).

Sonraki yıllarda Holling'in bu temel çalışması referans alınarak antropoloji, ekolojik-ekonomi ve çevre psikolojisi gibi farklı alanlarda çeşitli çalışmalar gerçekleştirilmiştir (Folke, 2006). Bu çalışmalarda dayanıklılık kavramı farklı yönleriyle ele alınarak kavrama ilişkin çeşitli tanımlar önerilmiş (Hosseini vd., 2016) ve kavrama yeni anlamlar yüklenmiştir. Böylece dayanıklılık kavramı, çok çeşitli disiplindeki bilgiler ile beslenen ve gelişen bilimsel bir disiplin olarak yol kat etmiştir (Xue vd., 2018).

1980'lerde afetlere yönelik dayanıklılık, sosyal, ekonomik ve fiziksel boyutlarıyla ele alınmış; O'Brien ve Mileti (1980) sosyal bağların ve afet öncesi hazırlığın önemine dikkat çekerken, Cutter vd. (2008) afet dayanıklılığını hazırlık, direnç ve toparlanma kapasitesi olarak tanımlamıştır.

20. yüzyılın sonlarında, kurumsal dayanıklılık, kuruluşların krizlere karşı direnç gösterme ve uyum sağlama yeteneği olarak yönetim çalışmalarında önem kazanmıştır. Mallak (1999), kurumsal dayanıklılığı, dışsal streslerin etkisini en aza indirirken değişime hızlı yanıt verebilme kapasitesi olarak tanımlamış ve uygulamaya yönelik yönetim stratejileri sunmuştur. Lengnick-Hall vd. (2011) kavramın, aksaklıklara karşı yanıt olarak emilim, uyum ve öğrenmeyi kapsayan dinamik bir kapasite olduğunu vurgulamaktadır. Annarelli ve Nonino (2016) ise dayanıklılığı, şokları öngörme ve yönetme kapasitesi olarak tanımlamıştır.

Kavramın sosyal bilimlerde ilk kullanan yazarlardan olan Timmerman (1981), dayanıklılığı "bir toplumun stres veya kesinti yaşadıktan sonra etkili bir şekilde 'kendini toparlama' yeteneği" şeklinde tanımlamıştır. Adger (2000), sosyal dayanıklılığın temel bileşenlerini sosyal ağlar, dayanışma ve kaynaklara erişim olarak tanımlamıştır.

Dayanıklılık kavramı, 1990'lardan itibaren ekonomi alanında afet ve krizlerin etkilerine karşı sistemlerin toparlanma kapasitesini açıklamak için kullanılmaya başlanmıştır. Holling (1996), ekonomik dayanıklılığı mühendislik ve ekolojik yaklaşımlarla ele alırken; Rose (2004), şoklara direnç, toparlanma ve adaptasyon kapasitesi olarak tanımlamıştır. Kavram, tehlikelere direnme ve toparlanma kapasitesiyle afet risk azaltmada önemli bir rol oynamaktadır (UNISDR & WMO, 2009).

Dayanıklılık, sürdürülebilirlik alanında ilk kez Brundtland Raporu'nda (1987) ele alınmış ve ekolojik sistemlerin dayanıklılığı, sürdürülebilir kalkınmanın temel koşulu olarak

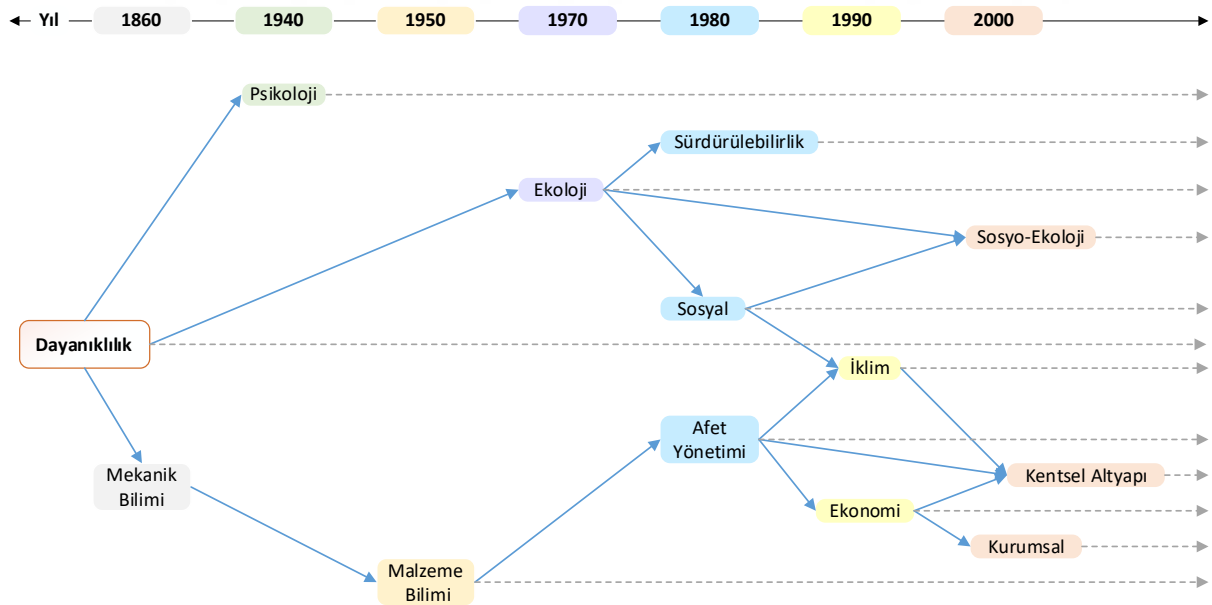
görülmüştür. Folke (2006), sosyal ve ekolojik dayanıklılığın artırılmasının sürdürülebilir kalkınmayı desteklemedeki rolünü vurgulamıştır.

Berkes ve Folke (1998), dayanıklılık kavramını sosyal ve ekolojik sistemlerin etkileşimini temel alan sosyo-ekolojik sistemler (SES) bağlamında ele alarak dayanıklılık ile sürdürülebilirliğin bir arada olduğu entegre bir yönetim yaklaşımı önermiştir. SES dayanıklılığı, insan davranışları ve yönetişimin ekosistem dayanıklılığı üzerindeki etkisine dikkat çekmektedir (Walker vd., 2004).

İklim değişikliği bağlamında Hükümetlerarası İklim Değişikliği Paneli (IPCC) (1990), dayanıklılığı, direnç ve değişime uyum kapasitesi olarak tanımlamıştır. Gay ve Sinha (2013), mühendislik, sosyal bilimler, ekoloji ve ekonominin altyapı dayanıklılığına katkı sağladığını belirtmiştir. Meerow vd. (2016) kentsel altyapı dayanıklılığının fiziksel, sosyal ve ekonomik sistemlerin bütüncül yaklaşımıyla güçlendirilebileceğini vurgulamıştır.

Dayanıklılık kavramı 2000'lerden itibaren çevre bilimi, sağlık, sinirbilim ve güvenlik gibi çok çeşitli alanlarda araştırılmıştır. Şekil 3'te, kavramın gelişim ve değişim sürecine ilişkin ana patikalar gösterilmektedir.

Şekil 3: Dayanıklılık Kavramının İzlediği Evrimsel Patika



Kaynak: Béné vd.'den (2018) uyarlanmıştır.

Günümüzde dayanıklılık kavramı, başlangıçtaki fiziksel esneklikten psikolojik, çevresel, toplumsal ve kurumsal uyarlanabilirliğe kadar değişen yorumlarla, sistemlerin bozulmaları absorbe etme ve bunlara uyum sağlama kapasitesi olarak tanımlanmaktadır (Mokline & Ben

Abdallah, 2021; Graveline & Germain, 2022). Kavramın disiplinler arası doğası, yaygın bir şekilde uygulanmasını sağlamıştır.

2.1.3. Dayanıklılık Türleri ve Yaklaşımları

Handmer ve Dovers (1996), bozucu tehditlere verilen yanıt stratejileri bakımından dayanıklılığın (1) direnç ve mevcut durumun sürdürülmesi, (2) sınırlı değişimin gerçekleştirilmesi ile (3) açıklık ve uyumluluk şeklinde sınıflandırılmasını önermektedir. Proag (2014) çalışmasında, Handmer ve Dovers (1996) tarafından geliştirilen yanıt stratejilerini açıklamaktadır. Yazar, söz konusu stratejileri; değişimi reddeden *direnç stratejisi*, sınırlı uyum sağlayan minör *değişim stratejisi* ve yüksek esneklikle değişimi benimseyen proaktif *uyum stratejisi* olarak tanımlamaktadır.

Walker vd. (2004), dayanıklılık kavramı için 4 önemli parametre olduğunu ifade etmektedir. Bunlardan *tolerans* (1) “bir sistemin iyileşme kabiliyetini kaybetmeden (aşılması halinde iyileşmeyi imkânsız hale getiren bir eşiği geçmeden) önce, değiştirilebileceği maksimum miktarı” ifade etmektedir. *Direnç* (2) “bir sistemi değiştirmenin kolaylığı veya zorluğu; sistemin değiştirilmeye ne ölçüde imkân tanıdığı”; anlamına gelmektedir. *Değişime yakınlık* (3), “bir sistemin mevcut durumunun bir sınıra veya anılan “eşiğe” ne kadar yakın olduğunu” göstermektedir. *Panarşi* (4), “sistemlerin nasıl büyüdüğünü, kriz yaşadığını, çöktüğünü ve nasıl yeniden yapılandığını” açıklamaktadır. Panarşi çok ölçekli, döngüsel ve uyarlanabilir bir sistem teorisidir.

Woods (2015), dayanıklılık kavramını karmaşık adaptif sistemler bağlamında ele alarak dört ana tema altında yapılandırmıştır. İlk olarak *geri tepme*, sistemlerin yıkıcı olaylardan sonra hızla toparlanarak eski dengesine dönmesini ifade eder; örneğin, bir topluluğun doğal afet sonrası altyapısını hızla onarması bu kapsamdadır. *Sağlamlık*, sistemlerin rahatsızlıklara rağmen işlevselliğini sürdürebilme kapasitesine işaret eder; bu da aşırı hava koşullarına dayanıklı yapıların varlığıyla örneklendirilebilir. Üçüncü olarak, *kontrollü genişletilebilirlik*, sistemlerin beklenmedik zorluklar karşısında uyum sağlama ve performanslarını artırma yeteneğidir. Dinamik ulaşım sistemleri, bu kapasitenin tipik bir örneğidir. Son olarak, *sürdürülebilir uyarlanabilirlik*, sistemlerin çok katmanlı ağ yapıları (bilgi akışı ağı, lojistik ağı, tedarik zinciri ağı, teknoloji ağı gibi birçok alt ağın üst üste gelerek oluşturduğu katmanlı yapı) aracılığıyla değişen koşullara uyum sağlama ve gelişme yetkinliğini ifade eder. Bu bağlamda,

çok merkezli yönetim yapılarıyla kaynak yönetiminde gerçekleştirilen paydaş iş birlikleri öne çıkar.

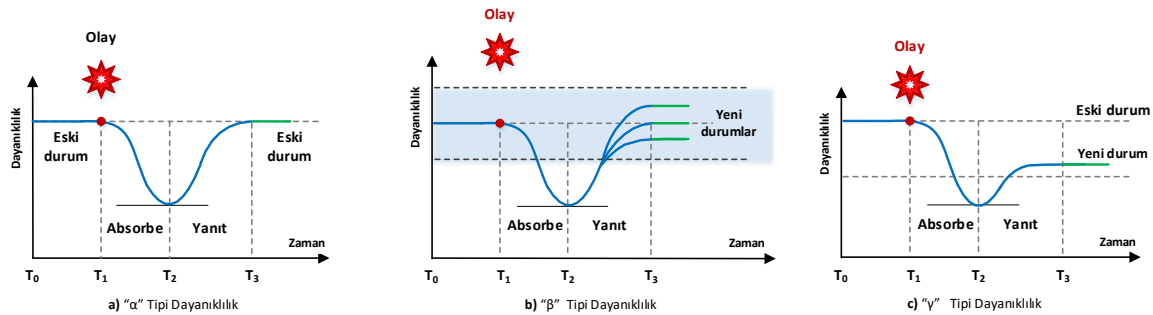
Davidson vd. (2016), dayanıklılığı bozulma düzeyine göre üç türde sınıflandırmıştır: *Temel dayanıklılık* (Tip 1) düşük kırılabilirlikle dengiyi koruma; *uyarlanabilir dayanıklılık* (Tip 2) değişimlere yapı ve işlev kaybı olmadan uyum sağlama; *dönüştürücü dayanıklılık* (Tip 3) ise geri döndürülemez değişimlere tepki verme kapasitesidir. Çalışmada uygulama ve politikaların bu düzeylere uygun olması gerektiği vurgulanmaktadır.

Williams vd. (2017), dayanıklılığı çevreye uyum ve gelişme yeteneğine dayalı etkileşimli bir adaptasyon süreci olarak tanımlamaktadır. Yazarlar, bu etkileşimin yalnızca değişime yanıtı değil, aynı zamanda yeni kaynakların korunması, kazanılması ve geliştirilmesini de kapsadığını belirtmektedir. Bu dayanıklılık sürecinin sonucu, iyileşerek eski duruma dönülmesi ya da yeni kararlı bir duruma adaptasyon sağlanması olarak ifade edilmektedir.

Clement vd. (2021) çalışmalarında, Davidson vd.'nin (2016) çalışmasına benzer şekilde dayanıklılık kavramına yönelik üç ana tür belirlemişlerdir. Şekil 4'te gösterildiği üzere,

- α tipi dayanıklılık*, sistemin hafif bozulmaları absorbe edip eski performans seviyesine dönebilme yeteneğini;
- β tipi dayanıklılık*, sistemin bozulma sonrası kabul edilebilir bir performans aralığına dönebilme kapasitesini;
- γ tipi dayanıklılık*, sistemin bozulma sonrası yeni duruma uyum sağlayarak istikrarlı şekilde performansını sürdürmesi ve yeni bir dengeye geçiş yapmasını ifade etmektedir.

Şekil 4: α , β , γ Tipi Dayanıklılık Türleri



Kaynak: Clement vd., (2021)

Tanner vd. (2017), dayanıklılığı işlevsel ve dinamik dayanıklılık şeklinde iki başlıkta ele alır. Bunlardan *işlevsel dayanıklılık*, sistemlerin şoklara rağmen temel işlevlerini koruyarak dengeye dönmesini ifade eder; örneğin, sel yönetim sistemleri, düzenli bakım ve önlemlerle su baskınlarına karşı işlevselliğini sürdürebilir. *Dinamik dayanıklılık* ise sistemlerin değişen koşullara uyum sağlayarak yeniden yapılanabilme kapasitesidir; örneğin, iklim değişikliğine karşı çiftçilerin tarımsal uygulamalarını çeşitlendirme yoluyla uyarlaması bu kapsamdadır. Yazarlar, dinamik dayanıklılığın sistemik değişim gerektirdiği için daha zor olduğunu belirtir.

2.2. Kurumsal Dayanıklılık

Günümüzün hızla değişen iş dünyasında, belirsizliklerden kaynaklanan geçmişe kıyasla daha yoğun ve kapsamlı yeni tehditler bir anda ortaya çıkmaktadır. Örneğin, son zamanlarda yaşanan siber güvenlik ihlalleri, terör saldırıları, iklim değişikliğine bağlı doğal afetler, küresel ekonomik krizler ve beklenmeyen felaketler gibi tehditler gerçekleşmiştir. Beklenmedik ani ve hızlı değişimlere istinaden, kuruluşlar bu dinamik ve çalkantılı ortamda ayakta kalabilmek, gelişebilmek ve söz konusu belirsizlik ve tehditleri yönetmek üzere etkili çözümlerin arayışındadır. Önceki bölümde değinildiği üzere, kurumsal risk yönetimi bu çözümlerden birisi olmakla birlikte, bu zorluklara karşılık gelen bir başka yaklaşım, kurumsal dayanıklılığın yönetilmesi ve güçlendirilmesidir.

Kurumsal bağlamda dayanıklılık; beklenmedik tehditler, şoklar, krizler veya uzun süreli baskılar karşısında kuruluşun varlığını sürdürebilmesi amacıyla hazırlıklı olması, gerçekleştirmelere uyum sağlayabilme ve gelişmeye devam edebilmesidir. Literatürde kurumsal dayanıklılık kavramı, çeşitli perspektiflerden ele alınmaktadır. Theocharidou vd. (2016) kavramın bir sonuç, süreç, kapasite ve durum olarak değerlendirildiği çalışmalardan bahsetmektedir. Farklı olarak Khin Khin Oo ve Rakthin (2022), kurumsal dayanıklılığa yetenek olarak atıfta bulunulan çalışmalara; Hillmann ve Guenther (2021) ise kavramın özellik, davranış, strateji veya yaklaşım, performans türü veya bunların bir karışımı olarak nitelendirildiği çalışmalara değinmektedir.

Bir yetenek olarak kurumsal dayanıklılık, Vogus ve Sutcliffe (2007) tarafından “bir kuruluşun, olumsuzluklara rağmen gerilimi absorbe etme ve işleyişini iyileştirme yeteneği olarak tanımlanmaktadır. Lengnick-Hall vd. (2011) kavramı “kuruluşun hayatta kalmasını tehdit edebilecek yıkıcı sürprizlerden yararlanmak için bunları etkili bir şekilde absorbe etme, duruma özel yanıtlar geliştirme ve nihayetinde dönüştürücü faaliyetlerde bulunma yeteneği”

olarak ifade etmektedir. Chen (2016), kurumsal dayanıklılığa “bir kuruluşun hayatta kalmak ve gelişmek için artan değişiklikleri ve ani kesintileri öngörme, bunlara hazırlık yapma, bunlara yanıt verme ve bunlara uyum sağlama yeteneği” olarak ele almaktadır.

Literatürdeki kurumsal dayanıklılık kavramını yetenek olarak açıklayan diğer tanımlarla (Hamel, 2007; Mahaboob vd., 2022; Durst vd., 2024) birlikte ele alındığında dışsal şokları absorbe etme, değişim ve bozulmalara karşı proaktif ve adaptif davranış, olaylardan öğrenerek kendini geliştirme ve yeniden yapılandırma öne çıkan ortak vurgulardır.

Kurumsal dayanıklılığın bir süreç olarak tanımlanması, dayanıklılığın sabit bir özellik ya da statik bir çıktı olmadığını, aksine zaman içinde gelişen, sürekli işleyen ve olaylar karşısında aktif biçimde devreye giren bir dizi faaliyet ve yetkinlik bütünü olduğu görüşünü desteklemektedir.

Sutcliffe ve Vogus (2003), kurumsal dayanıklılığın öğrenme ve esnek kaynak yönetimi yoluyla krizlerle başa çıkma becerisini geliştiren süreçlere dayandığını ifade etmektedir. Benzer şekilde, Mondragón vd. (2022) de dayanıklılığı, belirsizlik ortamında bireyleri ve grupları yenilikçi uyuma yönlendiren dinamik bir örgütsel süreç olarak tanımlayarak, sürecin çok katmanlı ve yenilikçi yönüne vurgu yapmaktadır. Bu yaklaşım, kurumsal dayanıklılığın sadece kriz anlarında ortaya çıkan bir tepki değil, kriz öncesi hazırlık, kriz anında başa çıkma ve kriz sonrası iyileşme ve öğrenme aşamalarını kapsayan döngüsel ve dinamik bir süreç olduğunu vurgular.

Hamel ve Valikangas (2003), kurumsal dayanıklılığı kurumsal değerlerin, süreçlerin ve davranışların korunmasıyla birlikte yenilikçilik yoluyla sürekli yeniden yapılanmayı mümkün kılan bir kapasite olarak tanımlamaktadır. Benzer şekilde Herbane (2013), kuruluşların iç ve dış tehditlere karşı dayanıklılık oluşturma kapasitelerinin, kriz baskısını absorbe ederek önceki durumlarına geri dönebilmelerini sağladığını vurgulamaktadır. Bu bakış açısı, dayanıklılığı sadece bir tepki veya sonuç değil, aynı zamanda mevcut ve geliştirilebilir bir yetkinlik seti olarak ele alır.

Öte yandan, Jung ve Song (2015), kavramı “kritik acil durum işlevlerini yerine getirmekten sorumlu bir kuruluşun harekete geçme ve karar verme sürecini başlatma yetkinliği” olarak açıklamaktadır. Home ve Orr (1997), kurumsal dayanıklılığı “beklenen olay düzenini bozan önemli değişikliklere, uzun süreli gerileme davranışına girmeden verimli bir şekilde yanıt vermek için temel bir nitelik olarak tanımlarken; McManus vd. (2008) ise “karmaşık, dinamik ve birbirine bağlı bir ortamda, kuruluşun genelindeki durum farkındalığı, temel

zayıflıkları ve uyum kapasitesinin bir fonksiyonu şeklinde ifade etmektedir. Burnard ve Bhamra'ya (2011) göre kurumsal dayanıklılık, “bir kuruluşun çalkantılı dönemlerde uyum sağlama kapasitesini mümkün kılan, içsel ve uyarlanabilir nitelik ve yeteneklerle ilişkili, kurumsal sistemlerin ortaya çıkan bir özellik olarak tanımlanabilir.

Kavram, çeşitli standartlarda farklı yönleriyle ele alınmakta ve farklı vurgularla tanımlanmaktadır. Kurumsal dayanıklılık, ASIS SPC.1-2009 standardında, bir olaydan etkilenmeme veya olay sonrası kabul edilebilir sürede kabul edilebilir performans düzeyine geri dönme yeteneği olarak tanımlanır (ANSI, 2009). BSI 65000:2014 standardı ise, kuruluşun hayatta kalmak ve gelişmek için ani ve artan değişiklikleri öngörme, hazırlık yapma, yanıt verme ve uyum sağlama yeteneğine vurgu yapar (BSI, 2014). ISO 22316:2017 standardı da, dayanıklılığı hedeflere ulaşmak ve gelişmek için değişen ortama uyum sağlama kapasitesi olarak ele alır (ISO, 2017). Her üç standart, kurumsal dayanıklılığı stratejik hedeflerle ilişkilendirerek, uzun vadeli uyum ve gelişim kapasitesine odaklanmaktadır.

Yer verilen tanımlar incelendiğinde, kurumsal dayanıklılık kavramının farklı bakış açılarıyla ele alınmasına rağmen, birçok tanımda kesişen bazı temel unsurlar öne çıkmaktadır. Bu ortak vurgular kavramın çok boyutlu doğasını yansıtarak, dayanıklılığın kurumsal yapı ve işleyişe nasıl entegre edildiğine dair önemli ipuçları sunmaktadır. Aşağıda, öne çıkan söz konusu unsurlara kısaca değinilmektedir.

1. Organizasyonun şokları, krizleri veya beklenmeyen olayları absorbe etme ve faaliyetlerini sürdürebilme kapasitesi.
2. Ani ve sürekli değişimlere karşı proaktif ve reaktif uyum becerisi.
3. Sadece eski duruma dönmekle kalmayıp, durumdan öğrenme ve dönüşüm fırsatları yaratma.
4. Dayanıklılığın, kuruluşun kültürü, değerleri, süreçleri ve kaynak yönetimiyle şekillenen bir sistem özelliği olması.
5. Dayanıklılığın, bireysel ve kolektif aktörlerin etkileşimiyle gelişen, öğrenme ve esneklik barındıran çok katmanlı ve sürekli bir süreç olması.
6. Dayanıklılığın sadece kriz anıyla değil, aynı zamanda uzun vadeli hedeflere ulaşma ve kurumsal gelişimle ilişkilendirilmesi.

Bu doğrultuda kurumsal bağlamda dayanıklılık, “bir kuruluşun iç ve dış çevresinden kaynaklanan beklenmedik şok ve değişimler karşısında temel işlevlerini sürdürerek stratejik

hedeflerine uyumlu şekilde faaliyetlerine devam edebilme ve bu süreçten öğrenerek gelişebilme yeteneği, süreci, kapasitesi ve özelliği” olarak ifade edilebilir.

Anılan nitelikler, kesinti ve aksaklıkları absorbe ederek başlangıç durumuna dönmekle birlikte, belirsizlikler içinde öngörülü davranma, hazırlıklı olma, yenilikçi ve olumlu bir uyum stratejisi geliştirme ve gerektiğinde kendini yeniden yapılandırarak daha dirençli hale gelme yeteneğini de kapsar. Dayanıklılık, kuruluşun hayatta kalma, rekabet gücünü sürdürme ve uzun vadeli değer yaratma becerisini destekleyen dinamik bir süreçtir.

2.3. Kurumsal Dayanıklılık Kapasiteleri

Dayanıklılık kapasitesi, “bir sistemin kesinti ve aksaklıklara direnme, bunlara uyum sağlama ve işlevselliğini geri kazanma yeteneğini artıran unsurlar” olarak tanımlanır (Hosseini & Barker, 2016). Bu kapasiteler, bir kuruluşun veya sistemin risk ve belirsizliği etkili bir şekilde yönetme yeteneğinin temelini oluşturur. Kurumsal dayanıklılık literatüründe farklı isimlerle adlandırılan çeşitli kapasite türleri yer almaktadır. Söz konusu kapasiteler, altı farklı dayanıklılık kapasitesinde (öngörü, önleyici, özümseme, onarıcı, uyum ve dönüştürücü) konsolide edilebilmektedir. Aşağıda anılan kapasite türlerinin ayrıntılı açıklamasına yer verilmektedir.

2.3.1. Öngörü (Tahmin) ve Hazırlık Kapasitesi

Öngörü kapasitesi, “bir sistemin veya kuruluşun gelecekteki riskleri tahmin etme ve orta-uzun vadeli olaylara hazırlık yapma yeteneğini” ifade etmektedir (Mentges vd., 2023). Bu kapasite, ortaya çıkan riskleri belirlemek, bunların dinamik doğasını kabul etmek ve sürekli yeniden değerlendirme yapmak için ufuk taramasının önemini vurgular (Manyena vd., 2019). Şimdiki zaman ve yakın geleceğe odaklanan durum farkındalığından farklı olarak, öngörü kapasitesi, uzun vadede ortaya çıkabilecek potansiyel aksaklıkları anlamaya ve uygun proaktif eylemleri belirlemeye yöneliktir (Mentges vd., 2023). Bu kapasite, kısa vadeli reaktif kararlardan, katılımcı yaklaşımları ve bilginin ortak üretimini içeren uzun vadeli politika vizyonlarına stratejik bir geçişi gerektiren bir yönetim yaklaşımıyla yakından bağlantılıdır (Manyena vd., 2019).

Öngörü kapasitesinin artırılması amacıyla risk senaryoları, erken uyarı sistemleri, trend ve çevresel tarama gibi araçlar kullanılmaktadır. Olasılık-etki matrisleriyle riskler

önceliklendirilir; büyük veri ve yapay zekâ destekli analizlerle geleceğe yönelik senaryolar geliştirilebilir.

Öngörü, geleneksel dayanıklılık tanımlarında sıklıkla yer almamakla birlikte, sadece tahmin yapmaktan öte, gelecekteki zorluklara yönelik potansiyel yanıtların analitik değerlendirmesini de içerir ve böylece kuruluşun hazırlıklı olmasını sağlar (Mentges vd., 2023). Bu doğrultuda öngörme kapasitesiyle eşanlı kullanımları hazırlık kapasitesi, bir kuruluşun yapılandırılmış planlama ve erken müdahaleler yoluyla potansiyel yıkıcı olayları öngörme ve bunlara hazırlık yapma yeteneğini yansıtır (Sanchis vd., 2020). Hazırlık kapasitesi, kapsamlı risk değerlendirmelerini ve kesintilerin etkisini en aza indirmeye yönelik önleyici tedbirlerin alınmasını içerir (Sanchis vd., 2020). Sonuç olarak, öngörü kapasitesi ve hazırlık kapasitesi, kuruluşların öngörülemeyen zorlukları önceden görmeleri, bunlara yönelik planlar yapmaları ve bunları etkili bir şekilde yönetmelerinin sağlanmasında önemli roller oynar.

2.3.2. Önleyici Kapasite

Önleyici kapasite, bir sistemin veya kuruluşun, potansiyel tehditleri ve olumsuz olayları henüz gerçekleşmeden önce tespit ederek, bu tehditlerin ortaya çıkmasını engelleme ya da etkilerini en aza indirme yeteneğini vurgulamaktadır. DKKV (2023) tarafından “mevcut riskleri azaltmak ve yeni risklerin ortaya çıkmasını önlemek için faaliyet yürütme ve önlem alma yeteneği” olarak tanımlanmaktadır. Bu kapasite, proaktif bir yaklaşıma dayanır ve risklerin gerçekleşmesinden önce harekete geçmeyi amaçlar. Bu kapasite, risk değerlendirmeleri, düzenleyici çerçeveler ve altyapı iyileştirmeleri gibi proaktif stratejileri vurgular (Manyena vd., 2019).

Kozine ve Andersen (2015), önleyici kapasitenin sistemin, öngörme ve buna hazırlık yapma derecesini yansıttığını vurgulamaktadır. Hazırlık kavramı, dayanıklılık bağlamında kimi çalışmalarda öngörü ve tahminleme ile potansiyel olumsuz olayların gerçekleşmesinin engellenmesi ya da gerçekleştiğindeki etkisinin azaltılmasına yönelik çalışmalar şeklinde geniş bir kapsamla tanımlanmaktadır. Bu bağlamda hazırlık kapasitesi kavramı, öngörü ve önleyici kapasiteleri bütüncül bir şekilde kapsayan bir üst çerçeve olarak değerlendirilebilir.

DKKV (2023), önleyici kapasitenin tamamen ortadan kaldırılamayan kurumsal kırılganlığı ve maruz kalınan kritik risklerin azaltılmasını amaçladığını vurgulamaktadır. Önleyici kapasite, kırılganlıkları önceden ele alarak, dayanıklılığın desteklenmesi ve yıkıcı olayların olasılığı ile sonuçlarının en aza indirgenmesi bakımından hayati bir rol oynamaktadır.

Kurumsal risk yönetiminin tesis edilmesi, iç kontrol ve süreç iyileştirme çalışmaları, yedeklilik ve çeşitlilik uygulamaları, eğitim ve farkındalık programları, teknik sistemlerde düzenli bakım ile erken uyarı ve izleme sistemleri önleyici kapasitenin artırılması için kullanılmaktadır. Ayrıca, sürdürülebilir altyapı yatırımları, güvenli yerleşim ve kaynak yönetimi politikaları da bu kapsamda değerlendirilebilir.

2.3.3. Özümseme Kapasitesi

Özümseme (absorbe etme, emme, emilim, soğurma) kapasitesi, sistemin kesinti ve aksaklıklara karşı ilk savunma hattı olarak kabul edilmekte; şoklara dayanarak ve minimum çabayla olumsuz sonuçları en aza indirerek sistemi korumaktadır. (Biringer vd., 2013; Keshavarz vd., 2024). Bu, sistemin önemli yapısal veya işlevsel değişiklikler yaşamadan kesintilere tolerans gösterme veya direnme yeteneğini temsil eder (Manyena vd., 2019; Abimbola & Khan, 2019). Vugrin'e (2010) göre, özümseme kapasitesi, depolanan kaynakları kullanarak kesintiler sırasında performansı korumaya yardımcı olan sağlamlık ve yedeklilik gibi özellikleri içerir. Francis ve Bekera (2014) bu kapasiteyi, bir sistemdeki bozulmaların etkilerini emerek, olumsuz sonuçların etkilerini belirgin şekilde hissettirmeksizin sistemin çalışmaya devam etme yeteneği olarak tanımlar ve bu kapasitenin, yapılandırmalar, kontroller ve prosedürlere bağlı olduğunu vurgular.

Hosseini ve Barker (2016) tarafından vurgulandığı üzere, emme kapasitesi, şok etkilerini önlemek veya azaltmak için bir kesinti öncesinde alınan tüm hazırlık önlemlerini de içerir. Bu anlamda operasyonel sürekliliği destekleyen genel bir tampon işlevi görür (Mentges vd., 2023).

Yu vd. (2020) ve Keshavarz vd. (2024) de bu kapasiteyi envanter tamponları, tedarikçi çeşitlendirmesi ve alternatif ulaşım kanalları gibi risk azaltma stratejileriyle ilişkilendirmektedir. Bu stratejiler, bir sistemin önemli ölçüdeki uyum veya onarım müdahalelerine gerek kalmaksızın şokları emmesini sağlar (Biringer vd., 2013; Keshavarz vd., 2024).

Özümseme kapasitesi genellikle fiziksel ve operasyonel sistemlere uygulanırken, Zahra ve George (2002) özümseme kapasitesini “kuruluşların dinamik bir örgütsel yetenek üretmek için bilgiyi edinme, özümseme, dönüştürme ve kullanma süreçlerinden oluşan bir dizi örgütsel rutin” olarak yorumlamaktadır. Yazarlar, potansiyel emici kapasite (bilgi edinme ve asimilasyon) ile gerçekleşmiş emici kapasite (bilgi dönüşümü ve kullanımı) arasında ayrım yaparak, kavramın farklı dayanıklılık alanlarında geçerliliğini genişletmektedirler.

Bu kapasitenin kapsamına sađamlık (depreme dayanıklı bina yapıları), yedeklilik (yedek jeneratörler veya alternatif tedarikçiler), otomatik koruma sistemleri (otomatik yangın söndürme sistemleri), önceden yapılan hazırlıklar (afet tatbikatları ve acil durum planları), hızlı müdahale yeteneđi (acil bakım-onarım ekipleri) girmektedir. Ayrıca hazır kaynak bulundurma (stratejik gıda veya yakıt stokları) ve basit sistem yapıları (modüler üretim hatları) gibi unsurlar da bu kapasitenin geliştirilmesine yönelik hazırlıklardır.

2.3.4. Onarım Kapasitesi

Onarım (restorasyon, kurtarma) kapasitesi, bir sistemin kesintiye neden olan bir olaydan sonra performansı, mümkün olan en hızlı ve verimli şekilde yeniden tesis etme yeteneđini ifade eder (Mentges vd., 2023). Vugrin (2010), restoratif kapasitenin, işlevselliğın olay öncesi seviyelere geri getirilmesi ile gelecekteki kesintilere daha iyi dayanabilecek yeni yapıların kurulmasına yönelik çalışmaları kapsadığını belirtmektedir. Bu kapasite, hasarlı altyapının onarılması, bileşenlerin değıştirilmesi ve acil durum planlarının uygulanması gibi somut eylemleri kapsar.

Francis ve Bekera (2014) çalışmalarında onarım kapasitesini, kurtarma faaliyetlerinin etkinliđi ve zamanında gerçekleştirilmesini içeren, bir sistemin istikrarlı bir duruma geri dönme yeteneđi olarak tanımlamaktadır. Mentges vd. (2023), bu kapasiteye onarım ekiplerinin görevlendirilmesini, yedek parçaların temini ve acil durum operasyonlarının başlatılmasını dâhil etmektedir. Kurtarma çabaları, genellikle paydaşların çelişen çıkarları ve restorasyonun maliyet ve faydalarının nicel olarak belirlenmesinin güç olmasında dolayı zorluklarla karşılaşmaktadır (Francis & Bekera, 2014). Ayrıca, restoratif kapasite, sistemlerin adaptif veya emilim kapasitelerini aşan olumsuz etkilerini nötr hale getirmesine olanak tanıdığından, hizmet sürekliliğının korunması bakımından kritik öneme sahiptir (Biringer vd., 2013). Nan vd.'ye (2014) göre, gerçek zamanlı izleme sistemlerinin kurulması, kesintilerin erken tespiti ve hatta tahminini mümkün kılarak onarım süreçlerini iyileştirir ve böylece genel tepki hızını artırır.

Onarım kapasitesi, havacılık ve uzay sanayii, nükleer enerji santralleri ve ağır sanayi ve metal işleme tesisleri gibi yüksek riskli ortamlarda geniş kapsamlı ve güçlü olmalıdır. Restoratif kapasite, bu tür ortamlarda kesinti süresini kısaltarak kritik işlevlerin sürekliliğini sağlar (Abimbola & Khan, 2019). Tedarik zincirlerinde, kesintilerin ardından işgücü geri kazanımı ve teknolojik iyileştirme gibi stratejilerle faaliyetlerin yeniden başlatılabilme yeteneđini ifade eder (Keshavarz vd., 2024).

Restoratif kapasite, uyum kapasitesinden farklıdır. Uyum tepkileri genellikle geçici ve esnekken, restoratif kapasite, dayanıklı sistemlerin daha kalıcı, yapısal bir özelliği olarak görülür. Bu durum, geçici hizmet sürekliliği çözümleri ile altyapının kalıcı onarımı arasındaki farkla örneklenebilir (Hosseini & Barker, 2016). Mentges vd. (2023), restoratif kapasitenin “normal” duruma geri dönmeyi vurgulasa da, bu durumun kesinti öncesi durumun tam olarak aynısı olmayabileceğini ve sisteme özgü olarak tanımlanması gerektiğini belirtmektedir. Restoratif kapasitenin etkinliği, geçmişteki kurtarma deneyimlerinin gelecekteki planların ve müdahalelerin gelişimine bilgi sağladığı kurumsal öğrenme yoluyla güçlendirilebilir (Sanchis vd., 2020), böylece kuruluşların sürekli iyileştirme yoluyla dayanıklılık kazanmalarına olanak tanır.

2.3.5. Uyum Kapasitesi

Uyum (adaptasyon, uyarlanma) kapasitesi, bir sistemin değişen koşullara veya kesintilere yanıt olarak kendisini ayarlama ve yeniden düzenleme yeteneğini temsil eder ve sadece dışsal desteklere bağlı kalmadan işlevselliğini sürdürmesini veya geri kazanmasını sağlar (Francis & Bekera, 2014; Abimbola & Khan, 2019). Bu kapasite, olumsuz olaylar sırasında ve sonrasında sistemin kendini organize etme ve dinamik değişiklikleri uygulama potansiyelini yansıtır (Vugrin, 2010) ve kıt kaynakların ikame edilmesi, davranışların değiştirilmesi veya yenilikçi yanıtların uygulanması gibi eylemlerle kendini gösterir (Biringer vd., 2013; Sanchis vd., 2020). Bu iç kapasite, kesinti ve aksaklıklardan kaynaklanan etkilerin özümseme sınırlarını aştığında işlevselliğin devamı için ilave çaba ve uyum gerektirdiğinde özellikle önemlidir (Hosseini & Barker, 2016; Yu vd., 2020).

Olay öncesi durumlara geri dönmeye odaklanan restoratif kapasitenin aksine, adaptif kapasite geçmişteki kesintilerden ders almayı ve ileriye dönük iyileştirmeler yapmayı vurgular (Mentges vd., 2023). Bu iyileştirmeler, yeni teknolojilerin benimsenmesi, operasyonel prosedürlerin revizyonu ve gelişen krizlere yanıt vermek için stratejik esnekliği içerebilir (Sanchis vd., 2020; Keshavarz vd., 2024). Ayrıca, uyum kapasitesi, emilim ve restoratif kapasiteleri güçlendirerek gelecekteki şoklara hazırlıklı olmayı sağlar; bu da uzun vadeli dayanıklılığa katkı sağlar (Francis & Bekera, 2014; Mentges vd., 2023).

Cedergren ve Hassel (2024) tarafından vurgulandığı üzere, uyum kapasitesi esneklik, yanıt verme yeteneği ve örgütsel öğrenme tarafından şekillendirilir ve durum farkındalığı, kırılganlık yönetimi, liderlik ve karar alma yetenekleri gibi bileşenlerle desteklenir. Bu

unsurlar, kurumların potansiyel zorlukları öngörmesini ve buna göre yanıt stratejileri geliştirmesini sağlar. Sonuç olarak, etkili bir şekilde geliştirildiğinde, uyum kapasitesi kriz yönetimini kolaylaştırır; uzun vadeli örgütsel dönüşümü teşvik eder (Cedergren & Hassel, 2024).

Uyum kapasitesi büyük ölçüde insan odaklıdır ve güçlü liderlik, iletişim, iş birliği ve kurumsal öğrenme ile desteklenir, bu da kuruluşların sadece başa çıkmakla kalmayıp gelişmesine de yardımcı olur.

Uyum kapasitesinin temel unsurları aşağıdaki şekilde özetlenebilir.

1. Durumsal farkındalık, iç ve dış risklerin erken tespit edilmesine yardımcı olur. Örneğin, COVID-19 sırasında bazı kurumlar uyum sağlamak amacıyla önceliklerini yeniden değerlendirmiş ve bu çerçevede hareket etmiştir.
2. Esneklik, operasyonlarda hızlı ayarlamalara olanak tanır. Kesinti durumlarında tedarik zincirinin yeniden yönlendirilmesi veya tedarikçilerin değiştirilmesi bir örnek olarak verilebilir.
3. Zayıf altyapının güçlendirilmesi veya kritik personelin yedeklenmesi gibi uygulamalar aracılığıyla kırılganlıkların yönetilmesi kapasitenin geliştirilmesi açısından önem arz etmektedir.
4. Dayanıklılık odaklı liderlik ve karar verme yetkinliği, krizler sırasında zamanında ve bilgilendirilmiş yanıtlar verilmesini sağlar. Örneğin, COVID-19 sırasında okulların hızla çevrimiçi eğitime geçmesi buna bir örnek teşkil etmektedir.
5. Kurumsal öğrenme, geçmiş deneyimlerden yararlanmayı gerektirir. Önceki başarısızlıkların ardından sel uyarı sistemlerinin güncellenmesi, kurumsal öğrenmenin sağladığı bir katkıdır.
6. Davranışsal ve yapısal değişiklikler, yeni teknolojilerin benimsenmesi veya kaynakların yeniden tahsis edilmesi uyum kapasitesinin kapsamına dâhildir. Buna yönelik örnek, bir fabrikanın pandemi sırasında hijyen malzemeleri üretimine geçmesidir.

2.3.6. Dönüşüm Kapasitesi

Dönüşüm (transformasyon) kapasitesi, dayanıklılığı artıran ve kırılganlığın temel nedenlerini hedef alan sistemik ve yapısal değişikliklere odaklanarak, iyileşme ve uyumun ötesine geçer. Sadece değişen koşullara uyum sağlamak yerine, gelecekte daha sürdürülebilir sonuçlar elde etmek için sistemlerin ve yapıların yeniden şekillendirilmesini gerektirir (Manyena vd., 2019).

MacLeman vd. (2016), dönüştürücü kapasiteyi şokların etkilerini tamamen ortadan kaldırmak üzere yeni sistemler kurma yeteneği olarak tanımlamaktadır.

Jeans vd. (2016), dönüştürücü kapasitenin risk ve kırılganlığın nedenlerini ele almaya yönelik kasıtlı eylemlerin uygulanmasını sağladığını belirtmektedir. Sistem perspektifinden bakıldığında, dönüştürülebilirlik, mevcut ekolojik, ekonomik veya politik düzenlemeler sürdürülemez hale geldiğinde temelden yeni bir sistem yaratma yeteneği olarak tanımlanır (Walker vd., 2004). Bu dönüşüm, yeni stratejileri veya bileşenleri getirerek sistem dinamiklerini yeniden tanımlamayı içermektedir.

Mochizuki vd.'ye (2018) göre dönüştürücü kapasite, değer sistemlerinden bürokratik veya yasal rejimlere, finansal kurumlardan teknolojik altyapılara kadar bir sistemin temel unsurlarında meydana gelen değişiklikleri kapsar. Bu tür kapsamlı dönüşümler sayesinde sistemler sadece yeniden inşa edilmez, aynı zamanda mevcut ve gelecekteki zorluklara daha iyi yanıt verebilmek için yeniden tasarlanır.

Bu kapasiteye; yönetsel ve işleyişe ilişkin kural ve düzenlemeler, altyapı dönüşümleri, kültürel değişimler ve işleyiş tarzına yönelik değişim ve yapılandırmalara, dijitalleşme ve teknolojik dönüşüm gibi uygulamalar dâhildir. Amaç, sistemi sürdürülebilir biçimde yeniden kurmaktır. Örneğin finans sektöründe dijital bankacılığa geçilmesi, sanayide esnek üretim yapısına geçilmesi ve enerji sektöründe yenilenebilir enerji yatırımları, dönüşüm kapasitesinin çıktılarına örnek olarak verilebilir.

2.4. Kurumsal Dayanıklılık Süreci

Kurumsal dayanıklılığa ilişkin literatürdeki bazı çalışmalarda, dayanıklılığın bir süreç olarak evrimi vurgulanmıştır. Söz konusu sürecin aşamalarının, farklı terim ve kapsamlar doğrultusunda kavramsallaştırılması amacıyla çerçeveler belirlenmiştir.

Burnard ve Bhamra (2011), tanımlanmamış kesintilere karşı dayanıklı kurumsal tepkiler için sundukları çerçevede dayanıklılık sürecini tespit ve aktivasyon, dayanıklı yanıt ve örgütsel öğrenme şeklinde üç aşamada ele almıştır. Çerçeve tehdit tespiti ve müdahale aktivasyonu kritik aşamalar olarak vurgulanmaktadır.

Linkov vd. (2016), dayanıklılığı planlama, özümseme, iyileşme ve adaptasyon aşamalarından oluşan dinamik bir süreç olarak tanımlamaktadır. Planlama aşaması, risk değerlendirmesi ve önleyici stratejilere; özümseme aşaması, kesinti sırasında operasyonların sürdürülmesine; iyileşme aşaması, işlevselliğin yeniden kazanılmasına; adaptasyon aşaması, öğrenilen derslerle sürecin geliştirilmesine odaklanır.

Cato vd. (2018), askeri alanda birim dayanıklılığını hazırlık, müdahale ve iyileşme olmak üzere üç aşamada ele alır. Hazırlık, olay öncesi planlama ve kaynak kazanımını; müdahale, şokların absorbe edilmesini ve uyum sağlamayı; iyileşme ise öğrenme ve gelişimi kapsar. Süreç, kuruluşun daha güçlü şekilde toparlanmasını hedefler ve işlevsellik düzeyiyle dayanıklılık gösterilir.

Klimek vd. (2019) tarafından gerçekleştirilen çalışmada şoka maruz kalan bir sistemin performansındaki değişimlere ve bunun sonucunda ortaya çıkan tepki davranışlarına yer verilmektedir. Söz konusu değişimler, Kaynak: 'te gösterilmektedir. Buna göre (1) numaralı patika sağlam (çökmeden emilim), (2)) numaralı patika esnek (eksik iyileşme), (3)) numaralı patika çökme veya (4)) numaralı patika uyarlanabilir davranış (yapıları, işlevleri ve geri bildirim döngülerini değiştirerek dönüşüm) gibi farklı tepki davranışlarını temsil etmektedir.

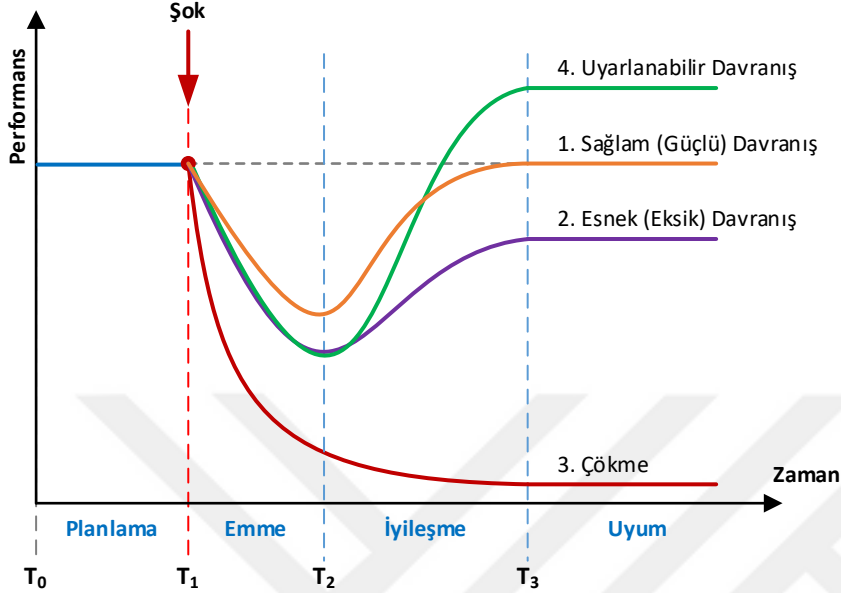
Aldea vd. (2020), dayanıklılığı dört aşamada tanımlamaktadır: kaçınma, bozulmalardan etkilenmeden kaçınmayı hedefler; özümseme, performans düşüşüyle birlikte işlevlerin sürdürüldüğü aşamadır; uyarlama, performans korumak için yapılan ayarlamaları içerir ve iyileşme, sistemin operasyonel seviyelerini geri yüklemesini sağlar.

Duchek (2020) dayanıklılığı, olayların öncesinde, sırasında ve sonrasında etkili bir yanıt olarak tanımlamış ve üç aşamaya ayırmıştır: beklenti, başa çıkma ve adaptasyon. Çalışmada dayanıklı kuruluşların, geçmişe, mevcut sorunlara ve geleceğe yanıt verebilme kapasitesine sahip olması gerektiği savunulmaktadır.

Jovanović vd. (2020), dayanıklılık sürecini beş aşamada ele alır: riskleri anlama, tehditlerin önceden tanımlanması; öngörme/hazırlanma, proaktif planlama ve adaptasyon; absorbe etme/dayanma, operasyonların stabil tutulması ve hasarın azaltılması; yanıt ver/kurtar, işlevselliğin geri kazanılması; ve adaptasyon/dönüşüm, uzun vadeli sürdürülebilirlik için

öğrenilen derslerin entegre edilmesidir. Bu aşamalar, kesintilere karşı dinamik ve sürekli bir yaklaşımı ifade eder.

Şekil 5: Şoka Maruz Kalan Bir Sistemin Performansındaki Temel Değişimler



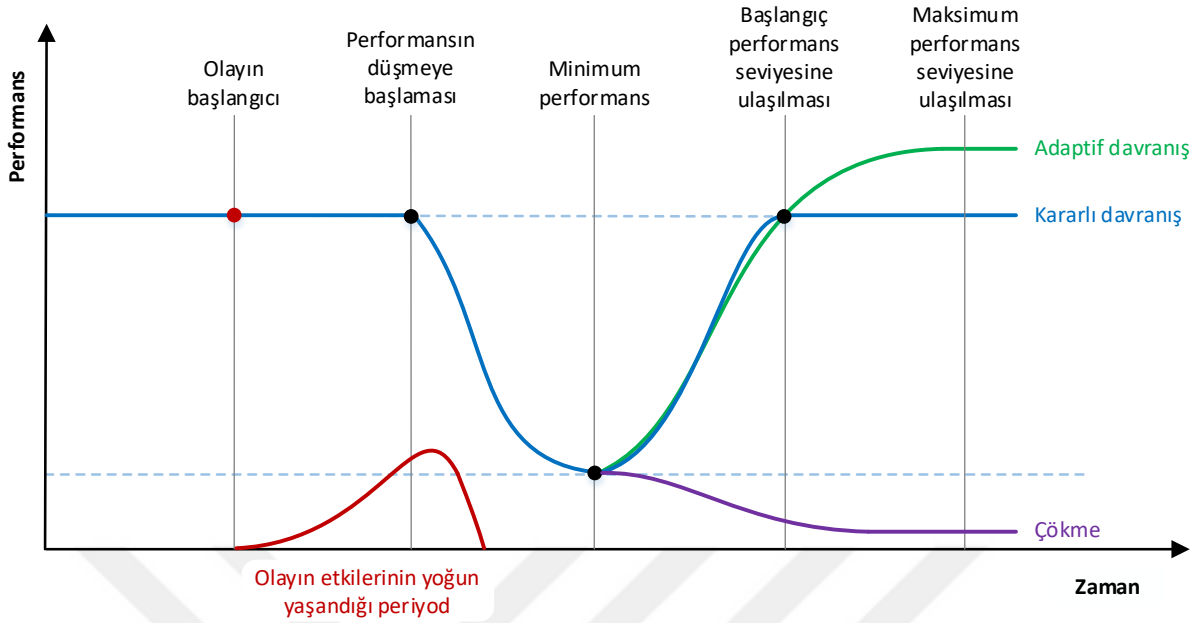
Kaynak: Klimek vd. (2019)

Mokline ve Ben Abdallah (2021), kurumsal dayanıklılığı dört aşamada ele alır: Aksaklık aşaması, krizlerin erken tespitini ve kök nedenlerin azaltılmasını hedefler. Özümseme aşaması, liderlik ve kaynaklarla şoklara direnmeye odaklanır. Yenileme aşaması, inovasyon ve büyüme fırsatlarını araştırır. Sahiplenme aşaması, geçmişten öğrenilen derslerin geleceğe entegrasyonunu vurgular.

Mentges vd. (2023), dayanıklılığı, genellikle kesinti öncesi, sırası ve sonrasındaki aşamaları gösteren bir performans eğrisi (Kaynak:) ile tasvir edilen dinamik bir süreç olarak tanımlamaktadır. Yazarlar, gerçekleştirdikleri literatür analizinde, performans eğrisini kullanan çalışmalardaki dayanıklılık aşamalarını derlemişler, adlandırmadaki farklılıklara rağmen aşamaların genel sırası ve süresi hakkında genel bir uzlaşı olduğunu belirtmektedir.

Bu çerçevede, Mentges vd.'ye (2023) göre dayanıklılık, riskleri azaltmak için yapılan hazırlıkları, krizler sırasında alınan önlemleri ve gelecekteki dayanıklılığı artıran dönüştürücü adaptasyonları bir araya getirmektedir.

Şekil 6: Dayanıklılık Sürecine İlişkin Performans - Zaman Eğrisi



Kaynak: Mentges vd. (2023)

Karunaratne (2022), kurumsal dayanıklılığı üç aşamalı bir çerçevede açıklar: Proaktif aşama, potansiyel tehditlerin öngörüldüğü ve güvenlik açıklarının azaltıldığı dönemdir. Eşzamanlı aşama, kesinti anında operasyonların sürdürülmesi ve kaynakların esnek yönetimini içerir. Reaktif aşama ise iyileşme, uyum sağlama ve öğrenilen derslerle dayanıklılığı artırma sürecidir. Bu çerçeve, kurumsal kabiliyetler arasındaki etkileşimleri ve aksaklıklar karşısında başarılı olabilmek için öncelikleri dengeleme gerekliliğini vurgular.

Su ve Junge (2023), kurumsal dayanıklılığı olumsuzluk öncesi, olumsuzluk anı ve olumsuzluk sonrası olarak üç aşamalı bir süreçte ele almaktadır. Olumsuzluk öncesi aşama, tahmin ve hazırlık, riskleri izleme, senaryo planlama ve simülasyon gibi stratejilerle proaktif öngörü ve hazırlığı vurgular. Olumsuzluk anı, algılama, özümseme, adaptasyon ve koordinasyonu içeren gerçek zamanlı tepkilerle kriz etkilerini yönetmeye odaklanır. Olumsuzluk sonrası aşama ise öğrenme, süreç iyileştirme ve yenilik yoluyla dayanıklılığı artırır, ayrıca olumsuzlukları stratejik büyüme ve uzun vadeli iyileştirme fırsatlarına dönüştürmeyi hedefler.

Dahmen (2023), dayanıklılığı beklenti, başa çıkma ve adaptasyon aşamalarıyla çerçevelemiştir. Beklenti aşaması, risk farkındalığını artırmaya ve proaktif hazırlığa odaklanırken, başa çıkma aşaması kriz yönetimini ve etkili kaynak kullanımını içerir.

Adaptasyon aşaması ise kriz sonrası öğrenilen derslerle dayanıklılığı güçlendirmeye vurgu yapar.

Tekletsion vd. (2024) ise dayanıklılığı kriz öncesi planlama, kriz sırası başa çıkma ve kriz sonrası iyileşme ve öğrenme olarak üç temel aşamada ele almıştır. Bu çalışmalar genel olarak, dayanıklılığın hazırlık, müdahale ve iyileşme aşamalarında dinamik bir süreç olarak ele alınması gerektiğine dikkat çekmektedir.

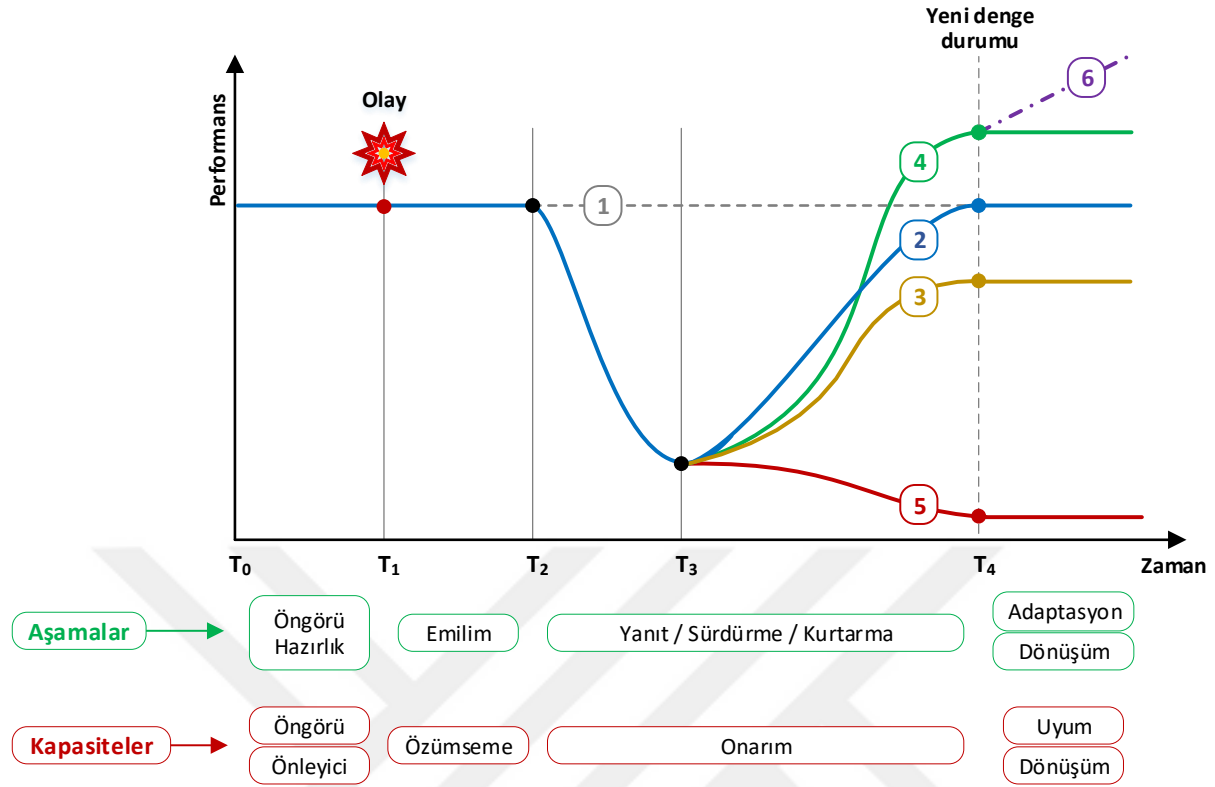
Literatürdeki çalışmalar ve konuya ilişkin analizler çerçevesinde, Şekil 7’de olay öncesi, anı ve sonrasına ait aşamalar ile her bir aşamaya yönelik ilgili dayanıklılık kapasitelerine ilişkin patikalar gösterilmektedir. Şema kurumsal dayanıklılık sürecini zaman ve işlevsellik eksenlerinde göstermekte ve açıklamaktadır. Süreç, öngörü ve hazırlık, emilim, yanıt/kurtarma ve adaptasyon/dönüşüm olmak üzere dört ana aşamadan oluşmaktadır. Şemada yer verilen senaryolar, kuruluşun dayanıklılık kapasitesine göre şekillenen alternatif gelişim yollarını temsil etmektedir.

Olay öncesi dönemde kuruluşlar, tehditleri önceden tahmin etmek ve etkilerini azaltmak amacıyla senaryo planlama, farkındalık artırma ve kaynak hazırlığı gibi faaliyetlerle öngörü ve önleyici kapasitelerini geliştirir. Olay anında ise sistemin sarsıntıyı absorbe etmesi beklenir. Bu aşama, kuruluşun özümseme kapasitesiyle ilgilidir ve hasarın minimuma indirilmesi hedeflenir. Olay sonrası erken dönemde devreye giren onarım kapasitesi sayesinde kuruluş, işlevlerini sürdürebilir hale gelmeye çalışır. Son aşamada ise kurumun mevcut yapıya uyum sağlayarak toparlanması (adaptasyon) ya da daha ileri bir dönüşümle yapısal gelişim göstermesi (dönüşüm) beklenir. Bu süreçte uyum ve dönüşüm kapasiteleri kritik rol oynar.

Bir numaralı senaryoda (1 numara - gri yol), kuruluş olayın gerçekleşmesinden etkilenmemiştir. Herhangi bir kesinti ya da performans düşüklüğü söz konusu değildir. Bu senaryoda kuruluşun önleyici kapasitesi ve emilim (özümseme) kapasiteleri güçlüdür. Olay gerçekleşmiş ya da gerçekleşmemiş olabilir.

Eski performansa geri dönüş (2 numara - mavi yol) senaryosunda kuruluş, yaşanan kesinti sonrası kısa süreli ve sınırlı bir performans düşüşü yaşamakta, ardından hızla toparlanarak olay öncesindeki performans seviyesine geri dönmektedir. Bu patika, bir "bouncing back" durumudur. Kesintiyle birlikte kurtarma, sürdürme, yanıt aşaması başlamaktadır. Kuruluşun emilim ve onarım kapasitesi yüksektir.

Şekil 7: Dayanıklılık Sürecine İlişkin Aşamalar, İlgili Kapasiteler ve Senaryolar



Sınırlı iyileşme (3 numara - sarı yol) senaryosunda kuruluş, kesintinin ardından tam olarak eski durumuna dönemese de belli bir işlevsellik düzeyine ulaşır. Ancak bu seviye olay öncesinden daha düşüktür. Bu durum, sınırlı özümseme ve onarım kapasitesine sahip sistemlerin izlediği patikadır.

Gelişerek iyileşme (4 numara - yeşil yol) senaryosu, kuruluşun yalnızca toparlanmakla kalmayıp, krizi fırsata çevirdiği ve olaydan ders çıkararak önceki durumdan daha güçlü bir pozisyona geldiğini gösterir. Adaptif toparlanma söz konusudur. Bu senaryo, “bouncing forward” yani ileriye doğru sıçrama örneğidir. Uyum kapasitesi gelişmiştir.

Çöküş (5 numara - kırmızı yol) senaryosunda kuruluş, kesintinin etkilerini yeterince absorbe edemez, toparlanma sürecinde başarısız olur ve işlevselliğini sürdüremez. Bu yol, hazırlık, özümseme ve onarım kapasitelerinin zayıf ve yetersiz olması nedeniyle sistemin kalıcı olarak bozulduğunu veya ortadan kalktığını ifade eder.

Dönüşüm (6 numara - mor noktalı yol) senaryosunda kuruluş, yaşanan olayı müteakiben uzun vadeli, stratejik ve kalıcı değişiklikler aracılığıyla, öncekinden farklı özgün bir rota izler. Dönüşümde kuruluşun değerleri, yapısı, iş modeli ya da kültürü gibi temel bileşenleri değişmektedir. Artık olay öncesi sabit durumu sağlayan temel koşullar ile bileşenlerin

bulunduğu düzlemden ayrılarak, koşulları ve işleyişi farklı olan yeni bir düzleme geçilmesi söz konusudur. Şemada gösterim kolaylığı olması amacıyla, altı numaralı yol yüksek performansa sahip olarak gösterilmektedir; ancak içinde bulunduğu düzlem farklıdır. Bu senaryo, “build back better” yani daha iyisini inşa etme örneğidir.

Yer verilen altı senaryo, kuruluşların kriz karşısında göstereceği tepkinin ne kadar hazırlıklı, esnek, öğrenen ve dönüştürücü olduğunu yansıtan genelleştirilmiş dayanıklılık senaryolarıdır. Her biri kurumsal dayanıklılığın farklı düzeylerini ve sonuçlarını somutlaştırmaktadır.

Şekildeki taralı alan, olayın (şokun) gerçekleşmesiyle birlikte sistem performansında meydana gelen kaybın büyüklüğünü ve süresini temsil etmektedir. Başka bir ifadeyle bu alan:

- Performans düşüşünün derinliğini (etki şiddeti) ve
- Sistemin bu düşüşten toparlanma süresini (iyileşme hızı)

birlikte göstermektedir. Dolayısıyla taralı alan ne kadar genişse, olayın kurumsal sistem üzerindeki toplam etkisi (yani “dayanıklılık kaybı” veya “zarar maliyeti”) o kadar büyüktür. Tersine, alanın küçük olması, kuruluşun emilim, yanıt ve onarım kapasitelerinin daha etkin çalıştığını ve sistem performansının daha hızlı toparlandığını ifade etmektedir.

2.5. Kurumsal Dayanıklılığın Unsurları

Kurumsal dayanıklılık, belirli ilke, bileşen, özellik ve boyutların bir araya gelmesiyle şekillenir. Literatürde farklı terimlerle ifade edilen bu yapısal unsurlar, kurumların dayanıklılık kapasitesini belirleyen temel öğeleri temsil eder. Kuruluşlar, bu unsurlar aracılığıyla mevcut sistemlerini güçlendirebilir; gelecekte karşılaşılabilecekleri olumsuzluklara karşı daha hazırlıklı hale gelebilir. Kurumsal dayanıklılık kavramının anlaşılması bakımından anılan unsurların bütüncül bir bakış açısıyla ele alınması önem arz etmektedir.

2.5.1. Özellikleri

McManus vd. (2008), kurumsal dayanıklılığın özelliklerini durum farkındalığı (çevresel ve paydaş dinamiklerini anlama), temel kırılganlıkların yönetimi (kritik zayıflıkların ele alınması) ve adaptif kapasite (kesintilere yanıt olarak stratejik ayarlamalar) olarak kategorize etmektedir.

Lengnick-Hall vd. (2011) ve Carvalho vd. (2012), kurumsal dayanıklılığın esneklik, çeviklik, uyarlanabilirlik ve bütünlük temellerine dayandığını vurgulamaktadır. Mochizuki vd. (2018) bu özelliklere, başa çıkma kapasitesi (kısa vadeli işlevselliği sürdürmek için kaynakları kullanma), uyum kapasitesi (olumsuz etkilere hazırlanma ve azaltma) ve dönüşümsel kapasiteyi (yeni zorlukların üstesinden gelmek için sistem özelliklerini temelden değiştirme) eklemektedir.

Lovell vd. (2016), dayanıklı sistemler için beş kritik özelliği ana hatlarıyla belirtmektedir. Bunlardan (1) farkındalık, proaktif risk tanımlamasını ve ortaya çıkan tehditlere adaptasyonu teşvik etmekte, (2) çeşitlilik, arızalar sırasında işlevsellik için yedeklilik ve alternatif seçenekler sağlamaktadır. Yazarlar, paydaşlar arasında iş birliğini vurgulayan (3) entegrasyonu diğer bir özellik olarak ele almaktadırlar. Kesintilere yanıt olarak kaynakların dönüştürülmesini ifade eden (4) uyarlanabilirlik, yeniden kullanma yeteneğini vurgularken; (5) öz düzenleme yerel arızaların artmasını önler.

Francis ve Bekera (2014), dayanıklılığı absorbe etme, adaptasyon, restorasyon ve öğrenme olmak üzere dört temel özellik ile açıklar. Absorbe etme, sistemin hazırlık ve uyum yoluyla aksaklıklara direnmesini sağlar; adaptasyon, sistemin özerk olarak işlevselliğini yeniden kazanmasıdır. Restorasyon kesinti ve aksaklıklardan kaynaklanan hasarların onarılması ve sistemin yeni bir normal duruma geri döndürülmesini ifade ederken; öğrenme, geçmiş deneyimlerden faydalanarak gelecekteki müdahalelerin geliştirilmesini sağlar.

2.5.2. İlkeleri

Dayanıklılık, ekolojik sistemlerden kurumsal yapılara kadar birçok alanda işleyen bir dizi ilkeye dayanır. Bu ilkeler, sistemlerin işlevselliğini sürdürmek veya uzun vadeli sürdürülebilirliği sağlamak üzere kesinti ve aksaklıkları absorbe etme, uyum sağlama ve dönüşüm geçirme gibi çeşitli mekanizmaları yansıtır.

İlke, “bir inanç veya davranış sisteminin veya bir akıl yürütme zincirinin temelini oluşturan temel bir gerçek veya önerme olarak tanımlanmaktadır (Oxford Online Dictionary, t.y.). İlkeler, davranış veya değerlendirme için rehberlik görevi üstlenmektedir. Dayanıklılık ilkeleri, sistemlerin, kuruluşların veya bireylerin aksaklıklara veya olumsuzluklara dayanmasına, bunlara uyum sağlamasına ve bunlardan kurtulmasına yardımcı olan temel yönergeler veya stratejilerdir.

Proaktiflik ve öngörü ilkesi, kuruluşların tehdit ve belirsizlikleri önceden algılayarak bunlara karşı hazırlıklı olması amacıyla erken önlem almasını ifade eder. Kurumsal dayanıklılık, kesintileri öngörme ve bunlara hazırlık yapma becerisine dayanır. Tehditlerin etkisini azaltmak için proaktif bir risk yönetimi gerekir (Kahan vd., 2009). Risk radarı, erken uyarı ve fırsat farkındalığı sağlar (Goffin vd., 2014). Riske ilişkin tolerans seviyelerine yönelik marjların hata payı bırakılacak şekilde yönetilmesi, en kötü senaryolara hazırlıklı olmayı sağlarken (Johnsen, 2010), farklı düzeylerdeki aksaklıkların farkında olmak, dayanıklılığın gerekliliklerindendir (Quendler, 2017).

Uyum sağlama ve esneklik ilkesi, değişen koşullara ve beklenmedik durumlara karşı hızla uyum sağlama ve alternatif yollarla çözüm üretme yeteneğidir. Dayanıklı kuruluşlar, kesintilere rağmen işlevselliğini sürdürebilmelidirler. Esnek ve hata tolere eden yapılar, yenilikçi çözümleri destekler (Johnsen, 2010). Uyum sağlayan ve öğrenen kültürler, değişim karşısında çevikliği artırır (Posch vd., 2024).

Dirençlilik ve güç ilkesi, sistemin şoklara ve baskılara karşı dirençli olmasını ve kritik işlevlerin alternatif yollarla sürdürülebilirliğini güvence altına almasını ifade eder. Sağlamlık, ani streslere karşı direnç sunarken (Kahan vd., 2009), yedeklilik alternatif yollarla iş sürekliliğini güvence altına alır (Johnsen, 2010). Farklı kaynakların dâhil edilmesi, sistemik gücü pekiştirir (Posch vd., 2024).

Krize yanıt verilmesi ve toparlanma ilkesi, kriz anında etkili tepki vererek sistemi koruma ve kesintiden sonra hızla işlevselliği yeniden sağlama becerisidir. Dayanıklı sistemler, kesintileri hızla onaracak planlara sahip olmalıdır (Kahan vd., 2009). Hazırlıklı personel ve hızlı müdahale süreçleri, krizin büyümesini engeller (Goffin vd., 2014).

Kaynak yönetimi ve problem çözme ilkesi, kısıtlı kaynaklar altında yaratıcı çözümler üretme ve kriz anında mevcut kaynakları etkin bir şekilde seferber edebilme kapasitesidir. Kısıtlı koşullarda yaratıcı çözümler üretebilmek ve kaynakları etkili şekilde seferber edebilmek dayanıklılık için kritiktir (Kahan vd., 2009). Geniş kaynak çeşitliliği, tehditlere ve fırsatlara daha esnek yanıtlar verilmesini sağlar (Goffin vd., 2014).

Öğrenme, değerlendirme ve uyarılama ilkesi, geçmiş deneyimlerden öğrenerek sistemlerin sürekli olarak kendini geliştirmesi ve yeni koşullara uygun şekilde uyarlanmasıdır. Kurumsal dayanıklılık, sürekli öğrenme ve geçmiş deneyimler üzerine sistematik düşünme yoluyla güçlenir (Kahan vd., 2009). Değişen koşullara ilişkin sürekli farkındalık ve kıl payı

kurtulma deneyimlerinden çıkarılan dersler, uyarlanabilir iyileştirmeleri destekler (Posch vd., 2024).

İletişim, iş birliği ve katılımcılık ilkesi, farklı paydaşlar arasında açık iletişim ve iş birliğini sağlayarak dayanıklılığı kolektif bir çaba haline getirmeyi ifade eder. Kurumsal dayanıklılık, sistemler arasındaki karşılıklı bağımlılıkları yönetme kapasitesiyle yakından bağlantılıdır ve zincirleme arızaların öngörülmesini ve kontrol altına alınmasını sağlar (Kahan vd., 2009). Ortak anlayış ve şeffaflık, koordinasyonu kolaylaştırır (Johnsen, 2010). Kapsayıcı katılım ve bireysel katkılar, dayanıklılık kültürünü pekiştirir (Quendler, 2017).

Sistemsal sadelik ve bağımsızlık ilkesi, aşırı karmaşıklıktan kaçınarak süreçleri sadeleştirmek ve sistem bileşenleri arasındaki bağımlılıkları azaltarak yaygın arızaların önüne geçmektir. Basitleştirilmiş yapılar, hata riskini düşürür (Johnsen, 2010). Çok boyutlu çevresel etkileşimlerin farkında olunması ve dış sistemlerle açık etkileşimde bulunulması, kuruluşun esnekliğini artırır (Quendler, 2017).

2.5.3. Boyutları

Dayanıklılığın boyutları, bir kuruluşun dayanıklılığını oluşturan temel yönleri veya perspektifleri temsil eder. Bu boyutlar, dayanıklılığın stratejik, kültürel, sosyal, operasyonel, öğrenme ve zaman gibi farklı düzlemlerdeki doğasını ortaya koyar.

Rubim ve Borges (2017), dayanıklılığın boyutlarını strateji (özümseme, uyum, dönüşüm), planlama (proaktif veya reaktif) ve eylem (bireysel veya kolektif) gibi boyutlar üzerinden incelemiştir.

Chen vd. (2021) çalışmasında, kurumsal dayanıklılığın beş boyutuna değinmektedir. Bunlardan ilki olan sermaye dayanıklılığı, krizlerden önce finansal hazırlığı sağlar. Stratejik dayanıklılık, uyarlanabilir planlamayı destekler. Kültürel dayanıklılık, ortak değerler aracılığıyla uzun vadeli çalışan bağlılığını teşvik eder. İlişkisel dayanıklılık, güçlü, güvene dayalı iç ve dış ilişkiler kurar ve öğrenme dayanıklılığı, kuruluşların krizlerden ders almasını ve uyum sağlamasını sağlar. Bu bileşenler birlikte, firmaların kesintilere dayanmasını ve büyümeyi sürdürmesini sağlar.

Namdar vd. (2021), dayanıklılık kavramını öngörü, hazırlık, sağlamlık ve iyileşme olmak üzere dört eyleme geçirilebilir boyuta indirgemıştır. Bu boyutlar, bir sistemin kesintileri erken

tespit etme, yanıt stratejileri hazırlama, operasyonel kapasiteyi sürdürme ve işlevselliği hızla geri kazanma becerisini yansıtmaktadır.

Graveline ve Germain (2022), dayanıklılığı geri sıçrama, ileriye sıçrama ve daha iyi inşa etme olmak üzere üç tamamlayıcı boyutta sentezlemekte; dayanıklılığın iyileşme ve adaptasyon sürecinde geçmiş, şimdiki ve gelecekteki düşüncelerin nasıl bütünleştirdiğini göstermektedir.

Dayanıklılığın çok boyutluluğu sektöre özgü yorumlarla da desteklenmektedir. Örneğin, Cimellaro vd. (2010), sağlık ve altyapı ağlarında dayanıklılık boyutlarını (sağlamlık, beceriklilik, yedeklilik ve hızlilik) tanımlayarak toparlanma sürecinin niceliksel yönlerine odaklanmıştır.

2.5.4. Bileşenleri

Dayanıklılığın bileşenleri, anılan boyutların içinde yer alan ölçülebilir, yönetsel ya da davranışsal unsurlardır. Genellikle bir kuruluşun dayanıklılığını geliştirmek için sahip olması gereken temel kapasiteleri, süreçleri veya prensipleri tanımlar.

Weick ve Sutcliffe (2007) dayanıklılığı; (1) zorlukları absorbe etme ve işlevselliği sürdürme kapasitesi, (2) aksaklıklardan kurtulma veya geri dönme yeteneği ve (3) önceki deneyimlerden öğrenme ve büyüme kapasitesi şeklinde üç temel bileşen üzerinden tanımlamaktadır. Bu bileşenler dayanıklılığın dinamik doğasını yansıtmakta olup, hayatta kalma ve ilerlemedeki rolünü vurgulamaktadır. Örneğin, dayanıklı sistemler kesinti öncesi durumlarına tam olarak geri dönmeyebilir, ancak gelişmiş yeteneklerle değişmiş bir duruma evrilebilir.

Conz ve Magnani (2020), bu alanda yapılan çalışmalara yönelik gerçekleştirdikleri literatür analizinde elde ettikleri bulgulara dayanarak dayanıklılığın üç farklı temel bileşenine değinmektedir. Bunlardan (1) proaktivite, kuruluşların krizlere etkili bir şekilde yanıt vermesini sağlayan öngörülü önlemleri; (2) yedeklilik ve beceriklilik, varlıkların ve çeşitlendirilmiş kaynakların önemini; (3) kolektiflik içeride ve dışarıda iş birliğine dayalı dinamiklerin ve güven inşasının değerini vurgular (Conz & Magnani, 2020).

Caza vd. (2020), kurumsal dayanıklılığın iki temel bileşeni olarak zorluklar ve olumlu uyumu vurgulamaktadır. Zorluklar, kuruluşun işleyişini tehdit eden akut veya kronik sorunları ifade eder ve etkileri bağlama göre değişir. Olumlu uyum ise, bu zorluklar karşısında işleyişin

korunması, yeniden kazanılması veya dönüşüm yoluyla gelişim sağlanmasıdır; bu uyumun zamanı ve kapsamı kurumsal düzeylerde farklılık gösterebilir.

Bonime-Blanc'a (2020) göre kurumsal dayanıklılık, sekiz temel altyapı unsuru tarafından desteklenir. Yönetişim, en üst düzeyde proaktif liderliği vurgular. Kültür, şeffaf, iş birliğine dayalı ve odaklanmış bir ortamı teşvik eder. Paydaşlarla iletişim, kuruluşun en önemli paydaşlarını belirleme ve onlarla etkileşim kurma yeteneğini ifade eder. Risk zekâsı, risk yönetim sistemlerinin uygun şekilde uyarlanması ve dengelenmesini sağlar. Strateji, çevresel, sosyal, yönetim ve teknolojik hususların kurumsal stratejilere entegre edilmesini ifade etmektedir. Performans dengesi, adil ve değer odaklı performans yönetim sistemlerinin önemini vurgular. Kriz hazırlığı, risk sistemlerine bağlı sağlam acil durum planlarının olmasının gerekliliğini vurgular. Son olarak, inovasyon, sürekli iyileştirme kültürünü teşvik ederek riski yeni fırsatlara ve değer yaratmaya dönüştürür.

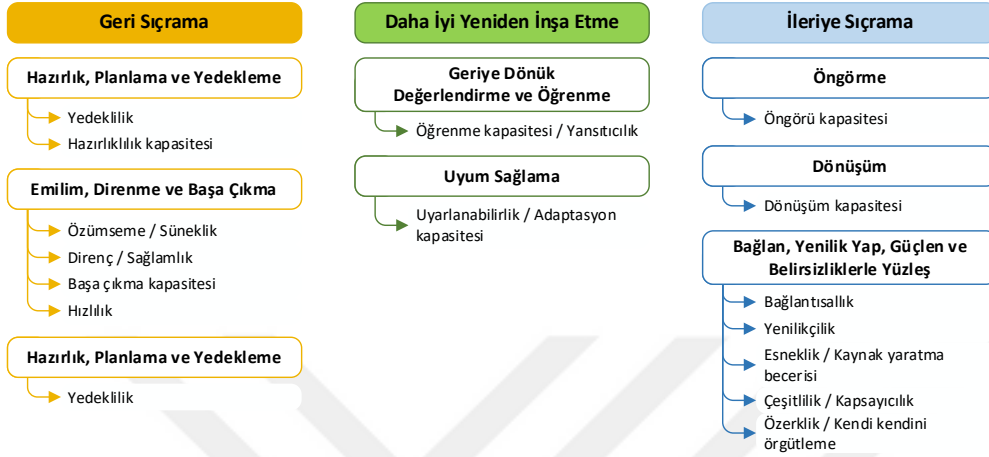
Kantabutra ve Ketprapakorn (2021) tarafından önerilen kurumsal dayanıklılık çerçevesi, örgütlerde dayanıklılığı toplu olarak tanımlayan ve yönlendiren yedi temel bileşeni belirleyerek birbirleriyle ilişkilendirir. Yedi bileşen şunları içerir:

1. Girdiler (insan kaynakları, sosyo-kültürel değerler, kurumsal ortamlar ve sosyal ve çevresel konular vb.)
2. Kurumsal yapının sağlanması
3. Değer ve inanç alt sistemi (kurumsal değerler)
4. Dayanıklılık düşünce yapısı (proaktif, inovasyon ve öğrenme odaklı tutum vb.)
5. Kurumsal sürdürülebilirlik uygulamaları (sosyal sorumluluğu ve çevre yönetimini teşvik eden somut eylemler bir kuruluşun dayanıklılık taahhüdünü yansıtır)
6. Kurumsal uyarlanabilirlik ve tamponlama (buffering) kapasiteleri
7. Sürdürülebilirlik performansı (bir kuruluşun baskı altında operasyonel istikrarını korurken uzun vadeli sosyal, çevresel ve ekonomik hedeflere ne ölçüde ulaştığının ölçülmesi)

Çerçeve, bu bileşenler arasındaki dinamik etkileşimi vurgulayarak etkili entegrasyonun uyum kabiliyetini nasıl artırabileceğini, sürdürülebilirliği nasıl teşvik edebileceğini ve kuruluşları zorlukların ortasında nasıl başarılı olacak şekilde konumlandırabileceğini ortaya koymaktadır (Kantabutra ve Ketprapakorn, 2021).

Graveline ve Germain (2022), risk ve afet yönetiminde, çözümleme kapasitesi, uyarlanabilirlik, yedeklilik ve beceriklilik gibi 25 farklı dayanıklılık bileşeni tanımlamakta (Şekil 8) ve bu bileşenleri dayanıklılık türleri ve süreçleri altında sınıflandırmaktadırlar.

Şekil 8: Dayanıklılığın Bileşenleri (Graveline & Germain, 2022)



Kaynak: Graveline ve Germain (2022)

2.5.5. Unsurların Değerlendirilmesi

Kurumsal dayanıklılığa ilişkin literatürde yer verilen unsurlar incelendiğinde, dayanıklılığı oluşturan "özellik", "ilke", "boyut" ve "bileşen" gibi kavramların kullanımında belirgin bir kavramsal örtüşme olduğu görülmektedir. Farklı çalışmalarda benzer içerikteki kavramların farklı başlıklar altında sınıflandırıldığı dikkat çekmektedir.

Öğrenme kavramı, hem bir özellik (Francis & Bekera, 2014) hem de bir ilke (Kahan vd., 2009; Posch vd., 2024) olarak ele alınmakta; ayrıca kimi çalışmalarda boyut (Chen vd., 2021) ve bileşen (Graveline & Germain, 2022) olarak da değerlendirilmektedir.

Yedeklilik, Cimellaro (2010) tarafından ilke olarak, Johnsen (2010) tarafından özellik olarak, Conz ve Magnani (2020) tarafından bileşen olarak tanımlanmaktadır. Benzer şekilde, esneklik, hem özellik (Lengnick-Hall vd., 2011), hem ilke (Johnsen, 2010), hem de bileşen (Graveline & Germain, 2022) olarak nitelendirilmektedir.

İlave olarak, beceriklilik, çeşitlilik, dayanıklılık kapasiteleri, durum farkındalığı, esneklik, hazırlık, hızlılık, kapsayıcılık, kültür, öğrenme, öngörü, özerklik, proaktivite, sağlamlık, yedeklilik kavramları benzer biçimde birden fazla kavramsal başlık altında tekrar edilmektedir.

Kurumsal dayanıklılığın unsurlarına ilişkin gerçekleştirilen literatür analizi sonucunda elde edilen dayanıklılığa ilişkin özellik, ilke, boyut ve bileşenler tematik olarak Tablo 3’te sunulmaktadır.

Tablodaki kavramlar incelendiğinde, kurumsal dayanıklılığın aşağıdaki sekiz temel ilke etrafında şekillendiği söylenebilir.

1. Dayanıklılık odaklı liderlik ve yönetim ilkesi,
2. Kaynakların etkin yönetimi ve dağıtımı ilkesi,
3. Açıklık ve şeffaflık İlkesi,
4. İşbirliği ilkesi,
5. Kapsayıcılık ilkesi,
6. Sistemsel sadelik ve bağımsızlık ilkesi,
7. Sürekli iyileştirme ilkesi ve
8. Hazırlıklılık ilkesi

Diğer taraftan, tabloda yer alan kavramlardan durumsal farkındalık, sağlamlık, dayanıklılık kapasitesi, çeviklik, esneklik, hızlilik, temel kırılganlıkların yönetimi, öğrenme yeteneği ve inovasyon odaklılık unsurlarının, dayanıklılığa ilişkin özellikler olarak nitelendirilebileceği değerlendirilmektedir.

Tablo 3: Dayanıklılığa İlişkin Özellik, İlke, Boyut ve Bileşenler

Özellik	İlke	Boyut	Bileşen
• Bütünlük (Lengnick-Hall vd., 2011; Carvalho vd., 2012) • Çeşitlilik (Lovell vd., 2016) • Çeviklik (Lengnick-Hall vd., 2011; Carvalho vd., 2012) • Dayanıklılık kapasiteleri (McManus vd., 2008; Francis & Bekera, 2014; Mochizuki vd., 2018) • Durum farkındalığı (McManus vd., 2008; Lovell vd., 2016) • Entegrasyon (Lovell vd., 2016) • Esneklik (Lengnick-Hall vd., 2011; Carvalho vd., 2012) • Öğrenme (Francis & Bekera, 2014) • Özerk hareket edebilme (Lovell vd., 2016)	• Çeşitlilik (Goffin vd., 2014; Posch vd., 2024) • Esneklik (Johnsen, 2010) • Durum farkındalığı (Quendler, 2017) • Hazırlıklılık (Goffin vd., 2014) • Hızlı toparlanma (Kahan vd., 2009) • Kapsayıcılık (Quendler, 2017) • Karşılıklı bağımlılıkları yönetme (Kahan vd., 2009) • Kaynak yönetimi ve problem çözme (Kahan vd., 2009) • Ortak anlayış ve şeffaflık (Johnsen, 2010) • Öğrenme, değerlendirme ve uyarlama (Kahan vd., 2009; Posch vd., 2024) • Proaktiflik (Kahan vd., 2009) ve öngörü (Goffin vd., 2014)	• Beceriklilik (Cimellaro vd., 2010) • Eylem (Rubim & Borges, 2017) • Geri sıçrama, ileriye sıçrama ve daha iyi inşa etme (Graveline & Germain, 2022) • Hazırlık (Namdar vd., 2021) • Hızlılık (Cimellaro vd., 2010) • İlişkisel (Chen vd., 2021) • İyileşme (Namdar vd., 2021) • Kültürel (Chen vd., 2021) • Öğrenme (Chen vd., 2021) • Öngörü (Namdar vd., 2021) • Planlama (Rubim & Borges, 2017) • Sağlamlık (Cimellaro vd., 2010; Namdar vd., 2021) • Sermaye (Chen vd., 2021)	• Bağlantılılık (Graveline & Germain, 2022) • Beceriklilik (Graveline & Germain, 2022; Conz & Magnani, 2020) • Çeşitlilik (Graveline & Germain, 2022) • Dayanıklılık kapasiteleri (Weick & Sutcliffe, 2007; Caza vd., 2020; Kantabutra & Ketprapakorn, 2021; Graveline & Germain, 2022) • Dirençlilik / Sağlamlık (Graveline & Germain, 2022) • Esneklik (Graveline & Germain, 2022) • Geri dönme yeteneği (Weick & Sutcliffe, 2007) • Hazırlıklılık (Bonime-Blanc, 2020) • Hızlılık (Graveline & Germain, 2022) • İnovasyon (Bonime-Blanc, 2020; Kantabutra & Ketprapakorn, 2021; Graveline & Germain, 2022) • İnsan Kaynağı (Kantabutra & Ketprapakorn, 2021) • Kapsayıcılık (Graveline & Germain, 2022) • Kolektiflik (Conz & Magnani, 2020) • Kurumsal değerler (Kantabutra & Ketprapakorn, 2021) • Kurumsal sürdürülebilirlik uygulamaları (Kantabutra & Ketprapakorn, 2021) • Kurumsal yapı (Kantabutra & Ketprapakorn, 2021) • Kültür (Bonime-Blanc, 2020) • Öğrenme (Weick & Sutcliffe, 2007; Kantabutra & Ketprapakorn, 2021; Graveline & Germain, 2022) • Öngörü (Graveline & Germain, 2022)

Tablo 3: Dayanıklılığa İlişkin Özellik, İlke, Boyut ve Bileşenler (Devam)

Özellik	İlke	Boyut	Bileşen
• Temel kırılganlıkların yönetimi (McManus vd., 2008) • Uyarlanabilirlik (Lengnick-Hall vd., 2011; Lovell vd., 2016; Carvalho vd., 2012)	• Sağlamlık (Kahan vd., 2009) • Sistemsel sadelik ve bağımsızlık (Johnsen, 2010) • Tolerans (Johnsen, 2010) • Yedeklilik (Johnsen, 2010)	• Strateji (özümseme, adaptasyon, dönüşüm) (Rubim & Borges, 2017; Chen vd., 2021) • Yedeklilik (Cimellaro vd., 2010)	• Örgütlenme (Graveline & Germain, 2022) • Özerklik (Graveline & Germain, 2022) • Paydaşlarla iletişim (Bonime-Blanc, 2020) • Performans dengesi (Bonime-Blanc, 2020) • Proaktivite (Conz & Magnani, 2020; Kantabutra & Ketprapakorn, 2021) • Risk zekâsı (Bonime-Blanc, 2020) • Stratejik entegrasyon (Bonime-Blanc, 2020) • Sürdürülebilirlik performansı (Kantabutra & Ketprapakorn, 2021) • Yedeklilik (Conz & Magnani, 2020; Graveline & Germain, 2022) • Yönetişim (Bonime-Blanc, 2020)

2.6. Kurumsal Dayanıklılığın Önemi

Kurumsal dayanıklılık, sürekli ve hızlı, ani değişimlerin yaşandığı ve belirsizliğin yoğun olduğu iş ortamında, kuruluşlar bakımından süreklilikle birlikte uzun vadeli başarının sağlanması açısından kritik hale gelmiştir.

Dayanıklılık, kuruluşların kesintilere dayanmasını, hızlı değişime uyum sağlamasını ve sürekliliğinin kesintisiz devam etmesini sağlar (Friedman & Lewis, 2021). Sürekli değişen bir dünyada, kuruluşlar sürdürülebilirliklerini ve yaşayabilirliklerini sınavan zorluklarla her an karşı karşıyadır (PECB, 2025).

Uzun vadeli sürdürülebilirlik ve finansal dayanıklılık, olumsuz koşullara rağmen operasyonel istikrarın korunması ve kalıcı değer yaratılması açısından kritik öneme sahiptir. Dayanıklılık, uzun vadeli sürdürülebilirliği teşvik ederek kuruluşların hayatta kalmasını ve olumsuz olaylardan ders alıp büyümelerini sağlar (Hollands vd., 2024). Rekabetçi ve kâr edebilir bir şekilde var olmak için, kuruluşlar ani değişiklikler ile etkileri uzun vadeli olabilecek olayları yönetebilmelidir (PECB, 2025).

Stratejik çeviklik ve inovasyon yeteneği, kuruluşların beklenmedik değişikliklere yaratıcı ve hızlı yanıtlar vermesini sağladığından, kurumsal yenilenme ve rekabet avantajı için kritik öneme sahiptir. Dayanıklı kuruluşlar, kesintilere yaratıcı bir şekilde yanıt vermek için daha donanımlıdır (Caza vd., 2020). Kuruluşlar çevik olmalı, değişen iş koşullarına hızlı bir şekilde yanıt verebilmeli ve yeniliğe açık olmalıdır (Friedman & Lewis, 2021). İnovasyon ve öğrenmenin iyileştirilmesi, stratejik yenilenme kapasitelerini artırır (Ortiz-de-Mandojana & Bansal, 2016).

Paydaşların güveni ve itibar yönetimi, kriz zamanlarında güven oluşturmak, sadakati sağlamak ve sosyal sermayeyi güçlendirmek için gereklidir. Anılan durumlarda kuruluşun dayanıklılık gösterebilmesi, paydaşlar nezdindeki güveni güçlendirir (Caza vd., 2020); bunu başarabilen kuruluşlar, müşterilerin, yatırımcıların ve halkın güvenini kazanma eğilimindedir (Ortiz-de-Mandojana & Bansal, 2016). Dayanıklılık, çalışanların refahına ve kurumsal bağlılığa katkıda bulunur (Hollands vd., 2024).

Hazırlık ve müdahale kabiliyeti, kuruluşların karşılaştığı aksaklık, kesinti ve krizlerin yönetilmesi açısından önem arz eder. Dayanıklı kuruluşlar, nadiren meydana gelen büyük krizlere ve sık sık yaşanan küçük zorluklara daha iyi hazırlıklıdır (Unit4, 2023). Kurumsal dayanıklılık, kuruluşların bu tür durumlarda işlevselliğini sürdürmesini sağlar (Hollands vd.,

2024). COVID-19 pandemisi, yalnızca hızlı ve yenilikçi bir şekilde uyum sağlayabilen kuruluşların hayatta kalabileceğini göstermiştir (Friedman & Lewis, 2021).

Diğer taraftan, dayanıklılık, başarısızlıktan kaçınmaya ilaveten, zorluklardan daha güçlü çıkılmasıyla da ilgilidir (Caza vd., 2020). Kuruluşlar, kısa vadeli eylemlerini uzun vadeli hedeflerle uyumlu hale getirerek kalıcı değere katkıda bulunur (Ortiz-de-Mandojana & Bansal, 2016). Dayanıklı kuruluşlar, kriz dönemlerinde önemli ölçüde daha yüksek hissedar getirisi elde eder (Unit4, 2023).

Yapısal ve kültürel esneklik, hızlı karar alma, iletişim, iş birliği ve sürekli öğrenmeyi destekleyen bir kurumsal tasarım ve kültürel ortam oluşturulması bakımından önemlidir. Friedman ve Lewis'e (2021) göre dayanıklı kuruluşlar, departmanlar arası iş birliğini teşvik eder. Yazarlar, dayanıklılığın sağlanması için inovasyonu destekleyen, başarısızlığı tolere eden, çeşitliliğe değer veren ve öğrenmeyi teşvik eden bir kültür ile değişimi kucaklayan bir liderlik anlayışının gerekli olduğunu ifade etmektedir.

Kurumsal dayanıklılığa yatırım yapmak, bir şirketin kesintilere karşı dayanıklılığını ve kesintilerden kurtulma kapasitesini artırır; kuruluşu sürekli değişen bir ortamda uzun vadeli değer yaratma, paydaşların güvenini sürdürme ve rekabet avantajı elde etme konusunda avantajlı bir konuma getirir.

Bu bölümde değinilen kurumsal dayanıklılığın kuruluşlar açısından önemine ilişkin literatür incelemesinden elde edilen sonuçlar Tablo 4'te özetlenmektedir.

2.7. Kurumsal Dayanıklılığın Güçlendirilmesi

IPCC (2014), kapasite geliştirme kavramını, “bir bireyin, topluluğun, toplumun veya kuruluşun değişime yanıt verebilme gücünü, özelliklerini ve mevcut kaynaklarını artırma uygulaması” olarak tanımlamaktadır. Kurumsal bağlamda dayanıklılık kapasitesinin geliştirilmesi, kuruluşların beklenmedik tehditlere karşı koyabilmesi, hızla uyum sağlayabilmesi ve uzun vadeli sürdürülebilirliği koruyabilmesi için önem arz etmektedir. Bu süreç, öngörü, uyum sağlama, hızlı tepki ve yedeklilik gibi temel yetkinliklerin güçlendirilmesini ve aynı zamanda liderlik, öğrenme, iş birliği, teknolojik altyapı ve karar alma sistemleri gibi unsurların bu hedefe yönelik olarak entegre edilmesini gerektirir.

Tablo 4: Dayanıklılığın Kuruluşlar Açısından Önemi

Tema	Açıklama	Kaynaklar
1. Süreklilik ve Uzun Vadeli Başarı	Kurumsal dayanıklılık, belirsizliklerin yoğun ve değişimin sürekli olduğu ortamlarda kuruluşların varlığını sürdürmesi, iş sürekliliğini sağlaması ve uzun vadeli başarısını koruması açısından kritik bir unsurdur. Dayanıklılık, kuruluşların ani değişiklikler karşısında operasyonlarını sürdürebilmesini ve uzun vadeli sürdürülebilirliklerini güvence altına almasını sağlar.	Friedman ve Lewis (2021); PECB (2025); Hollands vd. (2024)
2. Sürdürülebilirlik ve Değer Yaratımı	Dayanıklılık, sürdürülebilirliği destekleyen bir temel olarak kuruluşların olumsuz koşullar altında bile operasyonel istikrarı korumasına, finansal dayanıklılığı sürdürmesine ve kalıcı değer yaratmasına olanak tanır. Aynı zamanda kuruluşların krizlerden öğrenmesini ve büyümesini teşvik eder.	Hollands vd. (2024); PECB (2025)
3. Stratejik Çeviklik	Stratejik çeviklik, kuruluşların beklenmedik değişimlere hızlı, yaratıcı ve esnek biçimde yanıt verebilme kapasitesidir. Dayanıklı kuruluşlar, değişen koşullara uyum sağlayarak rekabet avantajı elde eder ve çevik karar alma süreçleriyle sürdürülebilir performans sergiler.	Friedman ve Lewis (2021); Caza vd. (2020)
4. Yenilenme ve İnovasyon Yeteneği	Yenilenme ve inovasyon kapasitesi, dayanıklılığın dinamik boyutunu oluşturur. Kuruluşlar, krizlerden öğrenerek yeni stratejiler geliştirme, süreçlerini yenileme ve inovasyon yoluyla büyüme fırsatlarını değerlendirme becerisine sahiptir.	Ortiz-de-Mandojana ve Bansal (2016); Caza vd. (2020)
5. Paydaş Güveni ve İtibar Yönetimi	Dayanıklılık, kriz dönemlerinde paydaş güvenliğini koruyarak müşteri, yatırımcı ve kamu nezdinde itibarı güçlendirir. Güven temelli ilişkiler, kuruluşun itibarını sürdürmesine ve kriz sonrası toparlanma hızını artırmasına yardımcı olur.	Caza vd. (2020); Ortiz-de-Mandojana ve Bansal (2016)
6. Sosyal Sermaye ve Çalışan Refahı	Kurumsal dayanıklılık, çalışan bağlılığı, örgütsel güven ve içsel dayanıklılığı destekleyerek sosyal sermayeyi güçlendirir. Dayanıklı kuruluşlar, çalışan refahını ve dayanışma kültürünü teşvik ederek kurumsal sürekliliğe katkıda bulunur.	Hollands vd. (2024); Caza vd. (2020)
7. Kültürel ve Yapısal Esneklik	Kurumsal dayanıklılığın sağlanması, iletişim, iş birliği, öğrenme ve çeşitliliği destekleyen bir kültürel yapıyı gerektirir. İnovasyonu teşvik eden, başarısızlıktan öğrenmeyi destekleyen ve değişimi kucaklayan liderlik anlayışı, örgütsel esnekliği güçlendirir.	Unit4 (2023); Friedman ve Lewis (2021); Hollands vd. (2024)
8. Krizlere Hazırlık ve Müdahale Yeteneği	Kurumsal dayanıklılık, kuruluşların hem nadir görülen büyük krizlere hem de sık yaşanan küçük kesintilere hazırlıklı olmasını, bu olaylara etkin şekilde yanıt vermesini ve fonksiyonlarını sürdürmesini sağlar. Özellikle COVID-19 gibi krizlerde, hazırlıklı ve yenilikçi kuruluşlar ayakta kalabilmiştir.	

Kurumsal dayanıklılığın güçlendirilmesinde çeşitli boyutlar öne çıkmaktadır. Operasyonel ve yapısal etmenler, hazırlıklılık, hızlı yanıt verebilirlik, erken uyarı, kaynak esnekliği, yedeklilik, uyum ve dönüşüm yeteneği kurumların beklenmedik durumlara karşı direnç kazanmasını sağlar. Bilişsel kapasite, kurumsal öğrenme, bilgi yönetimi ve sürekli gelişim süreçleriyle dayanıklılığı destekler. İnsan kaynakları, kültür ve liderlik boyutunda ise dayanıklılık odaklı liderlik, psikolojik güvenlik, etkin insan kaynağı yönetimi ve katılımcı karar alma önemlidir.

Ayrıca, sosyal ve kolektif unsurlar kapsamında iş birliği ağları, paydaş katılımı ve dış aktörlerle koordinasyon dayanıklılığı pekiştirir. Son olarak, stratejik entegrasyon aracılığıyla strateji-yapı-operasyon uyumu, dayanıklılık odaklı tasarım ve KRY entegrasyonu kurumsal kapasiteyi bütüncül biçimde güçlendirir. İlerleyen bölümlerde anılan hususlar açıklanmaktadır.

2.7.1. Operasyonel ve Yapısal Faktörler

2.7.1.1. Hazırlıklılık ve Proaktif Planlama

Bu faktörlerden ilki kuruluşların potansiyel olaylara karşı hazırlıklı olması ve söz konusu olaylara yönelik planlama yapmasıdır. Kurumsal dayanıklılığın temeli olan hazırlıklılık, sistemler ve personel genelinde yapılandırılmış planlama ve risk öngörülerini içerir. Koronis ve Ponis (2018), hazırlıklılığın çalışanların kriz protokolleri hakkında bilgilendirilmesini ve bu protokolleri uygulamaya koymasını sağlamak üzere planlama, risk değerlendirmesi, kriz prosedürleri ve yoğun eğitim gibi temel unsurları kapsadığını belirtmektedir. Dayanıklı kuruluşlar, kesinti ve aksaklıklara karşı proaktif olarak planlama ve yatırım yaparlar, bu da onların uyum sağlamasına, dayanmasına ve hızla toparlanmasına olanak tanır. Böylece krizlerden sonra gelişip daha güçlü bir gelecek oluşturabilirler (Deloitte, 2021).

2.7.1.2. Yanıt Verebilirlik ve Hızlı Tepki

Yanıt verebilirlik faktörü, kuruluşların krizler karşısında cevap vermeye hazır olma durumunu, hızlı cevap oluşturma yeteneğini ifade eder. Yanıtlayabilirlik, sorunları çerçevelendirmeyi, etkileri analiz etmeyi ve uyumu sürdürmeyi içerir. Gerçek zamanlı ve yapıcı tepkiler verilmesi, kuruluşun dayanıklılığı bakımından önemli bir kapasite ve yetkinliktir (Koronis & Ponis, 2018).

2.7.1.3. Farkındalık ve Erken Uyarı

İç ve dış ortamlarını sürekliliği sağlayacak şekilde tarayan kuruluşlar, tehditleri önceden görme ve azaltma konusunda daha donanımlıdır. Farkındalık, zayıf sinyallerin erken tespit edilmesini sağlar ve reaktif tepkiler yerine proaktif eylemlerin hayata geçirilmesini mümkün kılar. Değişen koşulları ve paydaşların beklentilerini aktif olarak izleyen kuruluşlar, krizleri önleme veya etkilerini azaltma becerilerini geliştirir (Khan vd., 2019).

Proaktif algılama ve durumsal farkındalık, kurumsal dayanıklılık kapasitesinin temelini oluşturur. Bu noktada çevresel tarama, proaktif düşünme ve güçlü bir bilgi tabanının sürdürülmesi yoluyla tehditlerin erken fark edilmesi sağlanır (Duchek, 2020). Söz konusu yetkinliklerin geliştirilmesi, dayanıklılığın sağlanması bakımından bir gerekliliktir.

İş analitiği ve gerçek zamanlı veri analizi, algılama ve farkındalık çabalarına destek olur; krizler sırasında daha hızlı ve daha kesin kararlar alınmasını sağlar (Sincorá vd., 2018). Risk izleme sistemleri kullanarak her an takipte olan kuruluşlar, risklerin tespitini etkin bir şekilde gerçekleştirerek risk körlüğünü aşabilir (Hopkin, 2015). Ayrıca, gerçek zamanlı durum farkındalığı araçlarıyla kurumsal mimarinin güçlendirilmesi, dinamik ortamlarda çevikliği ve yanıt verme yeteneğini artırır (Jnitova vd., 2021).

2.7.1.4. Kaynak Esnekliği ve Yedeklilik

Dayanıklılık, kuruluşun yeterli ve esnek kaynaklara sahip olmasına önemli ölçüde bağlıdır. Kuruluşlar, krizler sırasında zaman, finans ve insan sermayesini tahsis etmek için çeşitli araçlara ve çevik hareket edebilme kapasitesine ihtiyaç duyar. Bu tür kaynakların mevcudiyeti, risk taraması, hazırlık ve stres altında çevik eylemleri mümkün kılar (Duchek, 2020). Kaynakların esnek bir şekilde dağıtılması, hızlı ve etkili yanıtlar verilmesini sağlarken (Khan vd., 2019), yedek kaynaklar ve fazlalıklar, kuruluşun olumsuz olayı özümseme kapasitesini artıran koruyucu tampon görevi görür (Duchek, 2020).

Esneklik, uyarlanabilirlik ve yedeklilik gibi dayanıklılık özelliklerinin kurumsal mimari çerçevelere dâhil edilmesi, kuruluşların şoklara daha iyi dayanmasını ve bunlara daha iyi yanıt vermesini sağlar (Jnitova vd., 2021). Dijital teknolojilere ve altyapıya yapılan yatırımların, kısıtlayıcı koşullar altında operasyonların sürdürülmesinde etkili olduğu bilinmektedir (Aksay & Şendoğdu, 2022). Uzaktan çalışma ve dijital hizmet sunumu gibi yeni iş modellerine hızlı

adaptasyon sağlanması, dayanıklılığın sürdürülmesi bakımından önem arz etmektedir (Nosike vd., 2024).

Analitik araçlar ve iş sürekliliği planlaması, proaktif yönetimi mümkün kılarak dayanıklılığa katkıda bulunur. İş sürekliliği planlamasının kurumsal mimariye entegre edilmesi, kritik bağımlılıkların ortaya çıkarılmasını ve operasyonel sürekliliği sağlar (Jnitova vd., 2021). Sistemler arasında yedeklilik ve çeşitliliğin teşvik edilmesi, şoklara karşı emilim kapasitesini artırır (Tasic vd., 2020).

2.7.1.5. Uyum ve Dönüşüm Yeteneği

Uyum yeteneği, kuruluşların sadece toparlanmakla kalmayıp, zorlukları aşarak gelişmelerini sağlayan ve dayanıklılık açısından belirleyici bir faktördür. Uyum yeteneği, baskı altında dönüşümü mümkün kılan dinamik ve gelişen bir kapasite olarak tanımlanır (Koronis & Ponis, 2018). Kantur ve Iseri-Say (2012), ampirik ve teorik araştırmaların, dayanıklı kuruluşların hızlı uyum sağlayabilen, uyumunu koruyabilen ve yenilikçi düşünebilen kuruluşlar olduğunu ve bu özelliklerinin rekabetin yüksek olduğu ve öngörülemez iş ortamlarında dayanmalarını ve başarılı olmalarını sağladığını belirtmektedir. Dayanıklı kuruluşlar, kriz öncesi koşullara geri dönmelerin yanında, zorlukları inovasyon ve dönüşüm için bir katalizör olarak kullanarak ileriye doğru sıçrayabilirler. Dış baskılara veya iç dinamiklere yanıt olarak yeniden organize olma (dönüşüm) yeteneği, dayanıklılığın temel direklerinden birini oluşturur (Khan vd., 2019). Bu bağlamda dönüşüm faktörü, toparlanmanın yanında, gelecekteki aksaklıklarla daha iyi başa çıkabilmek için kuruluşun, sistemlerin ve süreçlerin yeniden yapılandırılmasını da ifade eder (Roberts, 2023).

2.7.1.6. Dinamik Yetenekler

Dinamik yetenekler, bir kuruluşun fırsatları veya tehditleri algılama, stratejik eylemler yoluyla bunları değerlendirme ve değişen ortamlara uyum sağlamak için içyapılarını ve süreçlerini dönüştürme becerisini ifade etmektedir (Teece vd., 1997). Dinamik yeteneklere yatırım yapılması kurumsal dayanıklılığın sağlanması açısından lokomotif bir faktördür. Aldianto vd. (2021) söz konusu yeteneklerin belirsizlik ortamında inovasyonu destekleyerek uzun vadeli dayanıklılığı artırdığını ifade etmektedir.

2.7.2. Kurumsal Öğrenme

Kurumsal öğrenme, bilgi yönetimi ve sürekli gelişim süreçleri, dayanıklılığı güçlendiren bilişsel temelli kapasitelerin merkezinde yer almaktadır. Krizlerden ders çıkarma ve bilgiyi etkin bir şekilde yönetme kapasitesini ifade eden kurumsal öğrenme ve bilgi yönetimi, dayanıklılığı güçlendiren bir faktördür. Dayanıklı kuruluşlar, dışarıdan gelen bilgileri özümseme ve bunları eyleme geçirilebilir bilgiye dönüştürme konusunda açık sistemler gibi işlev görür (Koronis & Ponis, 2018). Özellikle geçmişteki olumsuz durum ve olaylardan elde edilen bu tür bilgileri edinme, paylaşma ve uygulama becerisi, gelecekteki belirsizliklere hazırlıkta önem arz etmektedir (Khan vd., 2019).

Geniş ve çeşitli bir bilgi tabanı, risklerin erken tespitini, etkili müdahaleyi ve sürekli öğrenmeyi destekler (Duchek, 2020), iyi gelişmiş bir bilgi birikimi ise inovasyonu ve bilinçli karar almayı teşvik eder (Aldianto vd., 2021). Tatbikat, simülasyon ve olay sonrası incelemelerden yeni bilgilerin edinilmesi, kuruluşların zayıflıklarını belirlemelerine, operasyonel prosedürlerini iyileştirmelerine ve uyum kapasitelerini geliştirmelerine yardımcı olur (Crichton vd., 2009).

Kurumsal öğrenme mekanizmalarının kurulması, geçmişteki kesinti ve aksaklıkların ileriye dönük planlama ve yapısal iyileştirmelere entegre edilmesini sağlar (McManus vd., 2008). Sürekli öğrenme odaklı bir yaklaşım benimseyen kuruluşlar, gelecekteki zorluklara daha iyi uyum sağlayabilir (Gover & Duxbury, 2018). İlave olarak, bilgi aktarımı ve geri bildirim mekanizmalarının kurumsallaştırılması, reaktif tepkilerin proaktif planlamaya dönüştürülmesinde kritik bir rol oynar. İzleme sistemleri ve geri bildirim döngüleri, stratejilerin dinamik olarak belirlenmesine imkân tanır (Sincorá vd., 2018). Pandemi gibi krizlerden öğrenilenler, kuruluşların planlama yöntemleri ile planlarını revize etmelerine ve genel dayanıklılıklarını artırmalarına olanak sağlamıştır (Aksay & Şendoğdu, 2022).

2.7.3. İnsan Kaynakları, Kültür ve Liderlik Boyutu

2.7.3.1. Liderlik ve Kurumsal Kültür

Liderlik tarzı ve kurumsal kültür, tüm düzeylerde dayanıklılığın benimsenmesi bakımından bir temel niteliğindedir. Güvene dayalı, çevik liderlik, hızlı karar alma ve uyum sağlama ortamı yaratır (Aldianto vd., 2021). Ortak amaçları teşvik eden ve çalışanları

güçlendiren liderler, kurumsal uyumu ve çevik yanıt verebilirliği destekler (Khan vd., 2019). Ayrıca, sürekli öğrenme ve inovasyona yönelik bir kültür, kuruluşu olası zorluklara karşı hazırlar. Yetkinin dağıtılması ve uzmanlığa dayalı bir karar alma yapısı, çevikliği ve öğrenmeyi güçlendirir (Duchek, 2020).

Deloitte (2021) tarafından gerçekleştirilen, kamu ve özel sektörden 21 ülkede 2.260 üst düzey ve kıdemli yöneticiyi kapsayan araştırma, liderlerin dayanıklı kuruluşların özelliklerini nasıl algıladıklarını ve şirketlerinin yeni operasyonel zorluklara, stratejik değişikliklere ve “yeni normale” nasıl uyum sağladıklarını incelemiştir.

Bu özelliklerden ilki olan *hazırlık*, liderlerin kısa ve uzun vadeli planlamasıyla krizlere karşı yapılandırılmış bir duruş sağlar. Bu özellik, *uyum yeteneğiyle* birleştiğinde, esnek ve çok yönlü çalışabilen personel sayesinde ani değişimlere hızlı yanıt verilmesini sağlar. Kuruluş içi *iş birliği* kararları hızlandırır, riskleri azaltır ve yeniliği teşvik eder. *Güvenilirlik*, lider ve çalışanlar arasında şeffaf iletişim ve güvene dayanır. *Sorumluluk*, kârın ötesine geçerek paydaş ihtiyaçlarını gözetken çevik tepkiler verilmesini mümkün kılar. Bu beş unsur birlikte kurumsal dayanıklılığı bütüncül bir şekilde güçlendirir.

Dayanıklılık konusunda öncü rol üstlenen lider, farkındalığı yüksek bir kuruluş kültürü oluşturmalıdır. Lider, bu doğrultuda dayanıklılığı günlük karar alma süreçlerine, risk algısına ve sorumluluk yapılarına yerleştirerek, proaktif ve uyum sağlayabilen bir kuruluş kültürünü oluşturur (Longstaff vd., 2014). Bu bağlamda, üst yönetim tarafından iletişim ve eğitim yoluyla motive edilen risk bilincine sahip bir kültür, kurumsal farkındalığı artırır (Woon vd., 2011). Ayrıca, liderler çalışanların refahını aktif olarak desteklediklerinde ve zorluklar sırasında ekiplerine güven aşıladıklarında, kuruluşun dayanıklılığı artar (Gover & Duxbury, 2018).

2.7.3.2. Psikolojik Güvenlik

Kurumsal dayanıklılık, açık iletişim, güven ve çalışan bağlılığını teşvik eden bir liderlik aracılığıyla güçlendirilir (Aksay & Şendoğdu, 2022). Liderler, çalışanların ortak değerler ve karşılıklı destek yoluyla iş birliği yaptığı, kaynaklara erişebildiği ortamlar oluşturarak dayanıklılığın kurum geneline yayılmasına katkıda bulunur (Lengnick-Hall vd., 2011). Ayrıca, çalışanların olumsuz sonuçlardan korkmadan endişelerini ifade etme, risk alma ve hatalarından ders alma özgürlüğünü ifade eden psikolojik güvenlik, dayanıklılığın temel unsurlarından biridir (Gover & Duxbury, 2018). Psikolojik güvenlik, açık iletişim kurulabilen, ortak amaç

güdülen ve suçlama yapılmayan bir ortam aracılığıyla kurumsal kültür tarafından pekiştirilir ve olumsuzluk dönemlerinde güven ve iş birliğini toplu olarak güçlendirir (Hopkin, 2015).

2.7.3.3. Stratejik İnsan Kaynakları Yönetimi

Stratejik insan kaynakları yönetimi, çalışanlarda kilit yetenekleri geliştirerek kurumsal dayanıklılığı güçlendirir. Lengnick-Hall vd.'ye (2011) göre, İK uygulamaları çalışanların dayanıklılığını bilişsel ve davranışsal boyutlarda desteklemelidir. Davranışsal dayanıklılık, esneklik yetkinliği ile durumsal ve doğaçlama davranış ve inisiyatif kullanma yetkinliklerini teşvik eden rutinlerle geliştirilir. Bilişsel dayanıklılık, zorlukları yeniden çerçeveleme ve yeni zihinsel modeller oluşturma yoluyla desteklenir (Lengnick-Hall vd., 2011).

2.7.3.4. Karar Alma Sürecinde Katılımcılık

Katılımcı mekanizmalar, kararların daha kapsamlı ve uygulanabilir olmasını sağlar. Karar alma süreçlerine farklı düzeylerden çalışanların katılımı, sahiplenme duygusunu artırır. Çevik karar verme süreçleri, kuruluşların değişen koşullara hızlı ve etkili bir şekilde yanıt vermesini sağlayarak, kesinti dönemlerinde uyum kapasitelerini artırır (Nosike vd., 2024). KRY'nin günlük karar alma süreçlerine dâhil edilmesi, dayanıklılığın tüm operasyon düzeylerinde yerleşik hale getirilmesini sağlar (Woon vd., 2011). Ayrıca, kriz durumlarında çalışanları kararlara dâhil eden katılımcı yaklaşımlar, personelin bilinçli kararlar almasını sağlayarak yeni koşullara uyum yeteneği (Gover & Duxbury, 2018) ile kurumsal bağlılığı ve yanıt verme yeteneğini artırır (Aksay & Şendoğdu, 2022). Çalışanların karar alma süreçlerine katılmalarının sağlanması, sahiplenme ve bağlılık duygusunu besleyerek kriz durumlarında verilen yanıtların etkisini artırır (Nosike vd., 2024). Daha geniş düzeyde, ortaklar arasında iş birliğine dayalı karar alma, koordinasyonu iyileştirir ve dayanıklılığa katkıda bulunur (Andrés & Poler, 2013).

2.7.4. Sosyal ve Kolektif Dayanıklılık Unsurları

Diğer bir faktör, özellikle krizler esnasında kuruluşun iç ve dış ağlar ile bu ağlarla olan iletişiminin gücüdür. İşbirliğine dayalı ilişkiler, kolektif zekâyı teşvik eder, durumsal farkındalığı artırır ve karşılıklı yardımı kolaylaştırır. Bu ağlar, kaynakların ve bilgilerin hızlı bir

şekilde paylaşılmasına yardımcı olur ve karmaşık ve beklenmedik senaryoları yönetme kapasitesini artırır (Khan vd., 2019).

İş birliği ve paydaşların katılımı, özellikle karmaşık ve dinamik ortamlarda kurumsal dayanıklılığın oluşturulmasında merkezi bir rol oynar. Ortaklar arasında güven ve karşılıklı taahhütlerin oluşturulması, uzun vadeli dayanıklılığı artırır (Andrés & Poler, 2013). Ayrıca, krizler sırasında temel insan, mali ve teknolojik kaynaklara erişimin sağlanması, dayanıklı müdahalelerin gerçekleştirilmesinde kritik bir faktördür (Gover & Duxbury, 2018). Dayanıklılık planlamasına çeşitli paydaşların aktif katılımı, tehditlerin, rollerin ve karşılıklı bağımlılıkların kolektif olarak anlaşılmasına katkıda bulunur ve böylece koordineli ve kapsayıcı eylemleri teşvik eder (Crichton vd., 2009).

Kuruluşlar, farklı bölümler ve fonksiyonlar arasındaki iş birliğini geliştirerek dayanıklılıklarını güçlendirebilir. Andrés ve Poler (2013), kurum içi dayanıklılığın, çeşitli birimlerin bilgi, yetkinlik ve kaynaklarını bir araya getirerek sistemin bütünü güçlüleştirdiğini belirtmektedir. Bu iş birliği, özellikle operasyonel bağımlılıklar içeren büyük ölçekli sistemlerde kritik önem taşır.

Kurumlar arası stratejik ittifaklar, özellikle tedarik zinciri yönetimi, kamu-özel iş birlikleri veya kriz sonrası toparlanma dönemlerinde dayanıklılığı güçlendiren unsurlardır. Bu tür ittifaklar bilgi paylaşımını, kaynak erişimini ve ortak müdahaleyi kolaylaştırır (Tasic vd., 2020).

2.7.5. Stratejik ve Entegre Dayanıklılık Yönetimi

Kurumsal dayanıklılığın stratejik düzeyde ele alınması, uzun vadeli yönetim mekanizmalarıyla uyum içinde yürütülmelidir. Strateji, yapı ve operasyonel süreçler arasındaki entegrasyon, dayanıklılığın organizasyon genelinde sürdürülebilir kılınmasını sağlar (Sanchis vd., 2020).

Modülerlik, çeşitlilik, ademi merkeziyetçilik ve yedeklilik ilkeleri, sistemsel dayanıklılığın mimari temellerini oluşturur (Tasic vd., 2020). Bu ilkelerin organizasyonel tasarıma entegre edilmesi, olumsuz olayların yayılımını sınırlar, adaptasyon hızını artırır ve kriz sonrası toparlanmayı kolaylaştırır.

Dayanıklılık yaklaşımının KRY süreçleriyle entegrasyonu, risklerin yalnızca önlenmesi değil, aynı zamanda fırsatların da yakalanmasını sağlar. Risk yönetimi süreçleri, sürekli

iyileştirme ve öğrenme döngüleriyle desteklendiğinde, performans ve dayanıklılık hedefleri arasında denge kurulabilir (Woon vd., 2011; Hopkin, 2015).

Kurumsal dayanıklılığın artırılması, yalnızca belirli faktörlerin varlığına değil, bu faktörlerin sistematik olarak geliştirilmesine bağlıdır. Hazırlık, öğrenme, liderlik, kaynak esnekliği ve iş birliği gibi unsurlar, kapasite geliştirme yaklaşımlarıyla bütünleştğinde dinamik, sürdürülebilir ve çok katmanlı bir dayanıklılık mimarisi ortaya çıkar.

Kurumsal dayanıklılığın güçlendirilmesine yönelik gerçekleştirilen ve yukarıda yer verilen literatür analizi sonucunda derlenen etmenler tematik olarak Tablo 5’te sunulmaktadır.



Tablo 5: Kurumsal Dayanıklılığın Güçlendirilmesine Yönelik Temel Etmenler

Ana ve Alt Etmenler	Açıklama	Anahtar Unsurlar	Kaynaklar
Operasyonel ve Yapısal Etmenler			
Hazırlıklılık ve Proaktif Planlama	Kuruluşların olası olaylara karşı yapılandırılmış planlama ve eğitim yoluyla önceden hazırlanması dayanıklılığın temelini oluşturur.	Planlama, Risk Değerlendirmesi, Kriz Prosedürleri, Eğitim	Koronis ve Ponis (2018); Deloitte (2021)
Yanıt Verebilirlik ve Hızlı Tepki	Kuruluşun kriz anında hızlı, bilinçli ve etkili yanıt verme kapasitesini ifade eder.	Hızlı Tepki, Kriz Yönetimi, Uyarlanabilir Kararlar	Koronis ve Ponis (2018)
Farkındalık ve Erken Uyarı	Çevresel tarama, erken sinyal algılama ve veri analizi yoluyla tehditleri önceden tespit etmeyi sağlar.	Durumsal Farkındalık, Proaktif Algılama, Veri Analitiği	Khan vd. (2019); Duchek (2020); Hopkin (2015)
Kaynak Esnekliği ve Yedeklilik	Kriz anlarında kaynakların esnek biçimde yönetilmesi ve dijital altyapıların süreklilik sağlaması dayanıklılığı destekler.	Yedek Kaynaklar, Dijitalleşme, İş Sürekliliği Planlaması	Duchek (2020); Jnitova vd. (2021); Tasic vd. (2020)
Uyum ve Dönüşüm Yeteneği	Kuruluşların baskı altında yenilenme ve sistemlerini yeniden yapılandırma kapasitesidir.	Adaptasyon, Yeniden Yapılanma, İnovasyon	Khan vd. (2019); Roberts (2023)
Dinamik Yetenekler	Tehditleri algılama, fırsatları değerlendirme ve süreçleri dönüştürme yeteneğiyle uzun vadeli dayanıklılığı güçlendirir.	Fırsat Algısı, Stratejik Dönüşüm	Teece vd. (1997); Aldianto vd. (2021)
Kurumsal Öğrenme			
Kurumsal öğrenme, bilgi yönetimi ve sürekli gelişim	Kuruluşların geçmiş deneyimlerden öğrenerek geleceğe yönelik planlamalarını iyileştirmesi, öğrenme ve geri bildirim mekanizmaları kurarak bilgiye dayalı karar alma yetkinliğini artırmasıdır.	Kurumsal Öğrenme, Geri Bildirim Döngüleri, Bilgi Paylaşımı, Tatbikat	McManus vd. (2008); Crichton vd. (2009); Sincorá vd. (2018); Aksay ve Şendoğdu (2022)

Tablo 5: Kurumsal Dayanıklılığın Güçlendirilmesine Yönelik Temel Etmenler (Devam)

Ana ve Alt Etmenler	Açıklama	Anahtar Unsurlar	Kaynaklar
İnsan Kaynakları, Kültür ve Liderlik Boyutu			
Liderlik ve Kurumsal Kültür	Güvene dayalı, çevik ve vizyoner liderlik; öğrenen kültürün yerleşmesini sağlar.	Liderlik, Risk Bilinci, Kurumsal Uyum	Duchek (2020); Woon vd. (2011)
Psikolojik Güvenlik	Açık iletişim ve güven ortamı, çalışan bağlılığı ve kolektif dayanıklılığı güçlendirir.	Psikolojik Güvenlik, İşbirliği, Açık İletişim	Hopkin (2015); Gover ve Duxbury (2018)
Stratejik İKY	Stratejik İK uygulamalarıyla çalışanların kilit yetenekleri geliştirilerek kurumsal dayanıklılık güçlendirilir.	Yetenek, Durumsal Yanıt Verebilme, İnisiyatif Kullanma	Lengnick-Hall vd. (2011); Nosike vd. (2024)
Karar Alma Sürecinde Katılımcılık	Çalışanların karar alma süreçlerine katılmalarının sağlanması, sahiplenme ve bağlılık duygusunu besler.	Katılım, Bağlılık, Ortak Sorumluluk	Nosike vd. (2024); Aksay ve Şendoğdu (2022)
Sosyal ve Kolektif Dayanıklılık Unsurları			
İş Birliği Ağları ve Paydaş Katılımı	Krizler esnasında iç ve dış ağların gücü, kaynak paylaşımı ve kolektif müdahale kapasitesi sağlar.	Paydaş Katılımı, Bilgi Paylaşımı, Ortak Eylem	Gover ve Duxbury (2018); Crichton vd. (2009)
Kurum İçi ve Fonksiyonlar Arası İşbirliği	Farklı birimlerin bilgi ve kaynaklarını bir araya getirerek sistemin bütünsel dayanıklılığını artırır.	Disiplinlerarası İşbirliği, Koordinasyon, Bilgi Akışı	Andrés ve Poler (2013)
Stratejik İttifaklar ve Dış Aktörlerle Koordinasyon	Tedarik zinciri, kamu-özel ortaklıkları ve dış aktörlerle koordinasyon yoluyla dayanıklılığı güçlendirir.	Stratejik İttifaklar, Kaynak Erişimi, Ortak Müdahale	Tasic vd. (2020)
Stratejik ve Entegre Dayanıklılık Yönetimi			
Strateji-Yapı-Operasyon Entegrasyonu	Strateji, yapı ve operasyon süreçlerinin dayanıklılık ilkeleriyle uyumlu hale getirilmesi gerekir.	Stratejik Uyum, Yönetişim, Süreklilik	Sanchis vd. (2020)
Dayanıklılık Odaklı Tasarım İlkeleri	Modülerlik, çeşitlilik ve ademi merkeziyetçilik ilkeleri krizlerin etkisini azaltır ve sistemin toparlanmasını kolaylaştırır.	Modülerlik, Çeşitlilik, Yedeklilik	Tasic vd. (2020)
KRY ile Entegrasyon ve Performans Uyumlaştırması	KRY süreçlerinin dayanıklılıkla bütünleşmesi, hem risklerin önlenmesini hem fırsatların yakalanmasını sağlar.	Risk-Performans Dengesi, Sürekli İyileştirme	Hopkin (2015); Woon vd. (2011)

2.8. Kurumsal Dayanıklılığın Sağlanmasındaki Zorluklar

Dayanıklılık kavramı sık kullanılan ancak net ve yaygın kabul görmüş bir tanımı olmayan bir terimdir; bu nedenle farklı anlayışlar disiplinler ve sektörler arasında tutarlı uygulamayı güçleştirmektedir. Bu durum, uygulayıcıların kavramı teoriden uygulamaya aktarmalarını zorlaştırmaktadır (Burnard & Bhamra, 2019). Kavramın çok boyutlu ve ölçeklenebilir doğasının çeşitli düzeyler ve sektörler arasında koordinasyon gerektirmesi nedeniyle, uygulama süreci daha karmaşık hale gelmektedir (Folke vd., 2009). Diğer taraftan, kavramın kapsamının fazla genişletilmesi, her şeyi açıklama iddiasıyla hiçbir şeyi yeterince açıklayamama riskini doğurmaktadır (Macrae & Wiig, 2019).

Dayanıklılığı ölçmeye ve uygulamaya yönelik çabalar da benzer biçimde çeşitli güçlüklerle karşı karşıyadır. Kavramın soyut ve çok katmanlı doğası, ölçülebilir hale getirilmesini zorlaştırmakta; standart ölçütlerin eksikliği nedeniyle uygulamalarda ortak bir yaklaşım geliştirilememektedir (Folke vd., 2009). Kavramın somut stratejilere ve sonuçlara dönüştürülmesindeki güçlükler, dayanıklılığın işlevselleştirme sürecini sekteye uğratmaktadır (Kahan vd., 2009).

Dayanıklılığın stratejik yönetime ve karar alma süreçlerine entegre edilmesi de önemli bir zorluk alanıdır. Birçok kuruluş, dayanıklılığı önemli bir hedef olarak tanımlamasına rağmen, bu hedefi stratejik ve operasyonel kararlara yansıtmakta yetersiz kalmaktadır (Fotinos-Ventouratos vd., 2023). Mevcut kurumsal yapıların, planlama süreçlerinin ve uygulama pratiklerinin bu kavramı içselleştirmekte zorlanması ve çoğu zaman direnç göstermesi, bütünsel bir yaklaşımın gelişmesini engellemektedir (Kahan vd., 2009). Ayrıca anılan zorluklar, doğru, zamanında ve kapsamlı verilere erişimin sınırlı olmasıyla daha da artmakta ve bu da kuruluşların kırılganlıkları değerlendirme ve bilinçli karar alma yeteneklerini zayıflatmaktadır (Nnaji vd., 2024).

Yapısal ve kurumsal engeller de uygulamada önemli sınırlılıklar yaratmaktadır. Görev ve sorumlulukların farklı birimler arasında dağınık olması, koordinasyonu zorlaştırmakta, hesap verebilirliği azaltmaktadır (Dalgaard-Nielsen, 2017). Dayanıklılığın birey, ekip, kuruluş ve sektör içi diğer kuruluşlar arası düzeylerde inşa edilmesi gerekliliği, çok katmanlı bir yönetim yaklaşımını zorunlu kılmaktadır (Burnard & Bhamra, 2019). Özellikle büyük ve köklü bir tarihi olan kurumlarda görülen atalet ve teamüller, değişime karşı direnci artırmakta ve uyarlanabilirliği sınırlamaktadır.

Kuruluşların dayanıklılık stratejileri geliştirirken karşılaştığı bir diğer zorluk, istikrar (kararlı durum) ile esneklik arasındaki dengenin sağlanmasıdır. Etkili bir dayanıklılık yönetimi, bu iki kavramı aynı anda sürdürebilen liderlik becerilerini gerektirir; ancak bu davranışların tutarlılıkla sürdürülmesi uygulamada kolay değildir (Macrae & Wiig, 2019). Ayrıca, dayanıklılığı güçlendirecek kapasite, sistem ve yedeklemelerin oluşturulması maliyetli ve çoğu zaman finansal hedeflerle çatışmaktadır (Burnard & Bhamra, 2019). Buna ek olarak, detaylı planlama ve kontrol süreçlerine aşırı güven, kriz anlarında gerekli doğaçlama ve esnek müdahaleleri sınırlandırarak dayanıklılık uygulamalarının etkinliğini azaltabilmektedir (Dalgaard-Nielsen, 2017).

Dayanıklılığın kurumsal kültüre yerleşmesi, güçlü bir liderlik ve kurumsal kapasitenin varlığına bağlıdır. Belirsizlikle başa çıkabilen, aşağıdan yukarıya geri bildirim teşvik eden liderlik biçimlerinin yokluğu, katı hiyerarşik yapılarda sıkça görülmektedir (Dalgaard-Nielsen, 2017). Bunun yanında, aktörler arası güven ve şeffaflık eksikliği, dayanıklılığı ortaklaşa inşa etme çabalarını ciddi biçimde olumsuz etkilemektedir (Fotinos-Ventouratos vd., 2023).

Diğer taraftan, kaynak sınırlamaları ve ekonomik baskılar, uzun vadeli dayanıklılık yatırımlarını sekteye uğratmaktadır. Özellikle zaman, eğitim ve altyapı yatırımı gerektiren stratejilerin uygulanması, mali açıdan zorlayıcı olmakta ve küçük ya da kısıtlı bütçeli kuruluşlarda tercih edilmemektedir (Kahan vd., 2009). Ayrıca, proaktif izleme ve hızlı tepki verebilme yeteneği sunan sistemlerin kurulması, yüksek maliyet ve kaynak ihtiyacı nedeniyle birçok kuruluş tarafından sürdürülemez görülmektedir (Macrae & Wiig, 2019). Çoğu kuruluş, uzun vadeli dayanıklılık yerine kısa vadeli verimlilik ve karlılığı önceliklendirme eğilimindedir ve kurumsal sağlamlığa yönelik temel yatırımları ertelemektedir (Nnaji vd., 2024).

Kurumsal dayanıklılığın uygulanmasında kuruluşlarda karşılaşılan zorluklara ilişkin literatürde yer verilen hususlar, tematik Tablo 6’da özetlenmektedir.

Tablo 6: DY'nin Kuruluşlarda Uygulanmasında Karşılaşılan Zorluklar

Zorluk	Açıklama	Kaynak
1. Kavramsal Belirsizlik ve Tutarsızlık	Dayanıklılığın disiplinler arası farklı şekillerde yorumlanması, net bir tanımın olmaması nedeniyle uygulamada ortak bir anlayış geliştirilememektedir. Bu durum teoriden uygulamaya geçişi zorlaştırmakta ve kavramın aşırı geniş yorumlanması işlevselliğini zayıflatmaktadır.	Burnard ve Bhamra (2019); Folke vd. (2009); Macrae ve Wiig (2019)
2. Ölçümleme ve İşlevselleştirme Güçlüğü	Kavramın soyut ve çok katmanlı doğası nedeniyle ölçülebilir göstergelerin geliştirilmesi zordur. Standart ölçütlerin olmaması, dayanıklılığın somut stratejilere ve sonuçlara dönüştürülmesini güçleştirmektedir.	Folke vd. (2009); Kahan vd. (2009)
3. Stratejik Entegrasyon Eksikliği	Kuruluşlar dayanıklılığı hedef olarak tanımlasa da, stratejik ve operasyonel kararlara entegre etmekte zorlanmaktadır. Mevcut yapılar kavramı içselleştirmekte direnç göstermekte, veri eksikliği karar alma süreçlerini zayıflatmaktadır.	Fotinos-Ventouratos vd. (2023); Kahan vd. (2009); Nnaji vd. (2024)
4. Yapısal ve Kurumsal Engeller	Görevlerin farklı birimler arasında dağınık olması koordinasyonu zorlaştırmakta, hesap verebilirliği azaltmaktadır. Kurumsal atalet ve teamüller, değişime direnci artırmakta ve uyarlanabilirliği sınırlamaktadır.	Dalgaard-Nielsen (2017); Burnard ve Bhamra (2019)
5. İstikrar-Esneklik Dengesinin Kurulamaması	Dayanıklılık yönetimi, hem kararlılığı hem esnekliği aynı anda gerektirir; ancak bu iki kavram arasında denge kurmak uygulamada zordur. Aşırı planlama, kriz anında doğaçlama ve esnek müdahaleleri kısıtlamaktadır.	Macrae ve Wiig (2019); Dalgaard-Nielsen (2017)
6. Maliyet, Kaynak ve Altyapı Kısıtları	Yedekleme sistemleri, kapasite artırımı ve altyapı yatırımları yüksek maliyet gerektirir. Uzun vadeli dayanıklılık yerine kısa vadeli verimliliğin önceliklendirilmesi, stratejik yatırımların ertelenmesine yol açmaktadır. Eğitim, teknoloji ve proaktif izleme sistemlerine yapılan yatırımların yetersizliği, krizlere hızlı ve etkili yanıt verme kapasitesini düşürmektedir.	Burnard ve Bhamra (2019); Nnaji vd. (2024); Kahan vd. (2009); Macrae ve Wiig (2019)
7. Liderlik ve Kültürel Kısıtlar	Katı hiyerarşik yapılar, aşağıdan yukarıya geri bildirimi engellemekte; güven ve şeffaflık eksikliği dayanıklılığı kolektif olarak inşa etme çabalarını zayıflatmaktadır.	Dalgaard-Nielsen (2017); Fotinos-Ventouratos vd. (2023)

ÜÇÜNCÜ BÖLÜM

RİSK VE DAYANIKLILIĞIN BİRLİKTE YÖNETİLMESİ

3.1. Olumsuz Durum Kavramı

Durum kavramı, “belirli bir zamanda ve yerde gerçekleşen şeyler ve var olan koşullar kümesi” olarak tanımlanmaktadır (Cambridge, t.y.). Kavram yönetsel bağlamda, bir kuruluşun “belirli bir zaman diliminde içinde bulunduğu iç ve dış koşulların bütünü” olarak değerlendirilebilir. Söz konusu koşullar, kuruluşun stratejik ve operasyonel kararları, faaliyetleri ve bu faaliyetleri yürütmek amacıyla kullandığı kaynaklar ile kaynakların dağıtımı üzerinde doğrudan etkilidir.

Kuruluşlar, gündelik iş hayatlarında fırsat olarak nitelendirilen olumlu durumlarla karşılaşabildikleri gibi, sonuçları itibarıyla kuruluşun yönetimini, işleyişini ve faaliyetlerini etkileyen olumsuz durumlarla da mücadele etmek zorundadırlar. Kurumsal risk yönetimi ve dayanıklılık bağlamlarında ele alınan cehalet, muğlaklık ve belirsizlikler ile tehdit türleri ve riskler olumsuz durumlardır.

Kuruluşlar, karşılaştıkları çeşitli olumsuz durumları, farklı yönetim araçları doğrultusunda durumun mahiyetine özgü stratejiler geliştirerek yönetmek zorundadırlar. Olay öncesi, anı ve sonrasını kapsamak üzere süreklilik arz eden bir önleme, koruma ve toparlanma çerçevesinin oluşturulması, kuruluşun olası belirsizlik, tehdit ve risklere yönelik en az zararla varlığını devam ettirebilmesi açısından önem taşımaktadır.

3.2. Olumsuz Durum Türleri

Kuruluşlar, günümüzün dinamik iş ortamında varlıklarını sürdürmek ve stratejik hedeflerine ulaşabilmek amacıyla çevrelendikleri olumsuz durumları yönetmek zorundadırlar. Bu doğrultuda bahse konu durumlara ilişkin mahiyetin mümkün olduğunca netleştirilmesi ve tanımlanması, kuruluşun olumsuzluklara hazırlıklı olması açısından önem taşımaktadır.

3.2.1. Riskler

Risk terimi, etkileri bakımından olumsuz bir sonucun ortaya çıkması olasılığını ifade etmektedir. Risk, “bir tehdidin, belirli bir güvenlik açığı üzerinden bir varlığa başarılı bir şekilde saldırmasının olasılıksal bir fonksiyonu” olarak tanımlanır (Tatar & Karabacak, 2012). Riskler, olumsuz durumların varlıklarının farkında olunması ile tanımlanabilir ve etkileri ile olasılık değerleri bilinebilir hâle gelmiş durumları ifade eder. Bu tür riskler bilinen riskler olarak isimlendirilir.

Tehditlerin tanımlanabilir ve tahmin edilebilir olduğu, ölçülebildiği durumlara risk denmektedir (Hillson, 2003). Riskler, tehdidin gerçekleşme olasılığı ile gerçekleştiğinde yaratacağı etkinin birleşimidir. Riskin varlığı, bir tehdidin varlığıyla mümkündür. Risk unsurunda, gerçekleşmesi durumunda yaratacağı sonuçlara ilişkin küme bilinmekte olup, ortaya çıkacak negatif sonuçların kuruluşu ne kadar etkileyeceği ve gerçekleşme olasılıkları hakkında bilgi söz konusudur. Ancak, söz konusu kümeden hangi sonucun gerçekleşeceği bilinmemektedir.

Knight (1921), olasılıkların nesnel bir şekilde belirlenebilme durumuna göre risk ve belirsizliği ayrıştırarak, risklerin olasılıkların önceden bilindiği ve ölçülebildiği durumları temsil ettiğini belirtmektedir. Belirsizlik durumlarında bu olasılığın tam olarak belirlenebilmesi söz konusu değildir (Brouwer & De Blois, 2008).

Risk analizi, belirsizlik ve belirsizliğe ilişkin bilgiye dayalıdır (Thekdi & Aven, 2024). Risk yönetim stratejilerinin belirlenmesi, belirsizliğin niteliğine bağlı olduğundan, belirsizliğin tanımlanması ve sınıflandırılması risklerin etkili bir şekilde değerlendirilmesi açısından önemlidir (Alleman & Quigley, 2024).

Diğer taraftan, risk belirleme çalışmaları çok kapsamlı ve derin yapılsa dahi, sürecin sonunda bazı riskler hâlâ bilinemeyebilir (Fraser & Simkins, 2010). Henüz fark edilmeyen ve mevcut risk yönetimi çerçevelerinde ele alınmayan bu riskler, “bilinmeyen riskler” olarak ifade edilir (Lindhout vd., 2020). İkincil riskler, zincirleme riskler, beliren riskler ve gizli riskler, bilinmeyen risklerdir.

3.2.2. Tehditler

Tehdit, basitçe belirsizliklerin farkında ve tanımlanabilir olduğu durumlar olarak değerlendirilebilir. Kavram, Cambridge Sözlükte (t.y.) “zarar veya hasara neden olması muhtemel biri veya bir şey” olarak tanımlanmaktadır. Kurumsal yönetim bağlamında ise tehdit, “gerçekleşmesi halinde kuruluşun normal şekilde çalışmasını engelleyecek bir olay ya da durum” anlamına gelmektedir (Okolita, 2016). Tehditler, kuruluşun iş yapma biçimi, süreçleri, çalışanları ve sistemleri gibi kuruluş içi kaynaklı olabileceği gibi; pazar koşullarının değişimi, doğal afetler ve siber saldırılar ile çevresel, yasal değişiklikler gibi dış kaynaklı da olabilmektedir. Tehditler kasıtlı ya da kasıtsız olabilir.

Scholtz (2000), çalışmasında tehdit kavramının öncülleri olarak belirsizlik ve yetersiz bilgiyi işaret etmekte, kavramın kritik özellikleri arasında (1) gerçekleşme potansiyeli taşıması, (2) geleceğe yönelik olması ve (3) zarar verme kapasitesine sahip olmasını saymaktadır. Bu noktadan hareketle, tehdit kavramı “kurumsal hedefleri olumsuz etkileyebilen, kendisine karşı harekete geçilmesi gereken durumlar” olarak tanımlanabilir. Tehditler, bir kuruluşun, sürecin ya da kurumsal hedefin olumsuz etkilenmesine yol açabilecek potansiyel kaynaklardır.

Tehditlerin varlıkları, herhangi bir koşula ya da başka bir unsura, değişkene bağlı olmak zorunda değildir. Kuruluşların kırılgan olduğu noktaları suiistimal edebilecek herhangi bir değişken, unsur vb. tehdit olarak değerlendirilebilir (Rausand, 2011).

Kurumsal düzeyde karşılaşılabilecek tehdit türlerine ilişkin literatürde kısıtlı bilgi bulunmaktadır. Bu kapsamda sadece zincirleme, bileşik ve beliren tehditlerden bahsedilmektedir. Ancak etkin yönetilebilmeleri bakımından, doğaları, yapısal özellikleri ve etkileme biçimleri çerçevesinde tehdit türlerinden de söz edilmesi gerekmektedir. Aşağıda, çeşitli tehdit türleri² ile bunlara yönelik açıklamalara yer verilmektedir.

1. **Genel (tanımlı) tehditler:** Etkisi ve doğası açıkça bilinen, ancak olasılığı kesin olarak ölçülemeyen tehditlerdir. Tehdidin gerçekleşmesi durumunda yaratacağı sonuçlara ilişkin küme bilinmektedir. Bir veri merkezinin, bulunduğu bölgedeki altyapı zafiyetleri nedeniyle zaman zaman elektrik kesintisi yaşaması, genel (tanımlı) bir tehdittir.

² Zincirleme, bileşik ve beliren tehdit türleri literatürde yer almakla birlikte, diğer tehdit türleri bu çalışma kapsamında tez yazarı tarafından kavramsallaştırılmıştır.

2. **Zincirleme tehditler**, birden fazla sistemde birbiriyle bağlantılı bir tehdidin diğer birini tetiklemesi sonucu meydana gelen tehditler silsilesi olarak tanımlanabilir (Pescaroli & Alexander, 2016). Örneğin, fabrikadaki enerji kesintisinden kaynaklı üretimin durması ve ardından pazara ürün arz edilememesi bir zincirleme tehdittir.
3. **Bileşik tehditler**, eş zamanlı ya da ardışık bir şekilde gerçekleşen ve aynı anda gerçekleştiklerinde daha büyük etkiler meydana getirebilen en az 2 olay olarak tanımlanmaktadır (IPCC, 2012). Örneğin, pandemi tehdidi ile ekonomik krizin aynı ya da yakın dönemlerde gerçekleşmesi, bileşik tehditlere örnek olarak verilebilir. Çarpan etkisi sonucunda bütünleşik ve iki tehdidin etkileri toplamından daha yüksek bir etki yaratmışlardır.
4. **Birikimli tehditler**, başlangıçta çok küçük etkiye sahip olan ancak zaman içerisinde bu küçük etkilerin birikmesiyle meydana gelen ve etkileri giderek büyüyen tehditlerdir. Bu tehditler, etkilerini zaman içerisinde yavaş yavaş gösterir ve uzun vadede yıkıcı sonuçlara neden olurlar. İklim değişikliği ve su kıtlığı örnek olarak verilebilir.
5. **Uyuyan tehditler**, kendisini göstermesi için belirli koşulların oluşması gereken ve aktifleşene değin uzun bir süre boyunca örtük bir şekilde pasif kalan tehditlerdir. Örneğin, çalışanlar arasındaki iletişimde görülen eksiklikler ya da kurumsal aidiyette yaşanan zafiyetler bir kriz çıkana değin arkada uyumaktadır. Krizle birlikte bu tehdit gerçekleşir ve çalışanların bir kısmı aynı anda işi bırakabilir.
6. **Beliren (ortaya çıkan) tehditler**, henüz kendisini tam olarak ortaya çıkarmamış, yeni trend ya da gelişmeler aracılığıyla şekil alan tehditlerdir. Başlangıçta bilinemezler, ancak zaman ve gözlemlerle giderek tanımlanabilir veya öngörülebilir hale gelirler. Bu tehditlerden kaynaklanan riskler, “hızlı, beklenmedik ya da her iki şekilde” kendisini gösterebilir (Salim vd., 2021). COVID-19’un ilk ortaya çıkışı beliren tehditlere örnek olarak verilebilir.
7. **Gizli tehditler**, mevcut durumda sistemin içinde bulunmakta olup mevcut gözlem araçlarıyla henüz tespit edilememiştir. Ancak bu tehdit, varsayılabilir veya dolaylı olarak sezilebilir. Tehdidin gizliliği, algısal sınır sorunu veya modelleme yetersizliği ile ilgilidir. Siyah kuğu olarak nitelendirilen olaylar, gizli tehditlere örnek olarak verilebilir.

Tehditler önceden fark edilebilirlikleri ve sonuçlarının öngörülebilirlikleri, gelişme hızları (belirme ve gelişme hızı), yayılım ve domino etkisi yaratma potansiyelleri (yayılım ve sistemik risk), yanıt verilmesi için ihtiyaç duyulan zaman ve imkân durumu (müdahale penceresi) ile diğer karmaşıklık ve çoklu etki yaratma potansiyellerine (karmaşıklık ve bağlantılılık) göre sınıflara ayrılabilir. Bu bağlamda yapılan sınıflandırma, kurumların hangi tehdit türlerine karşı ne tür önlemler alması gerektiğine dair daha isabetli ve duruma özgü kararlar vermesine olanak tanır. Aşağıda, bu amaç doğrultusunda geliştirilen tehdit gruplarına yer verilmektedir.

3.2.2.1. Genel (Tanımlı) Tehditler

Bu tür tehditler, doğası bilinebilir ve anlaşılır olan, tanımlanması ve fark edilmesi kolay tehditlerdir. Olası sonuçlar kümesi öngörülebilir niteliktedir. Tehdidin potansiyel etkisi hakkında yeterli bilgi mevcuttur; ancak gerçekleşme olasılığı konusunda kesin ve güvenilir bir bilgi bulunmamaktadır.

Genel tehditler, diğer tehdit türlerine göre daha kolay algılanabilir ve yüksek belirginliğe sahip tehditlerdir. Başlangıçta potansiyel etkileri bilinebilir. Zaman içinde etki alanının genişlemesi, etkilerinin belirginleşmesi gibi durumlar söz konusu değildir.

3.2.2.2. Genişleyen Tehditler

Bu tehdit grubu, bir sistemin yalnızca belirli bir bileşenini değil, birden fazla alt sistemini veya dış paydaşla bağlantılı yapıları da etkileyebilecek düzeyde yayılma potansiyeline, artan karmaşıklığa ve zaman içinde büyüyen etkilere sahiptir. Genellikle bir noktada başlayan bu tehditler, sistemler arası bağımlılık ve etkileşimler yoluyla domino etkisi yaratarak genişler.

Anılan tehditler sadece anlık müdahalelerle değil, modüler yapıların kurulması, yayılımının sınırlandırılması, etki zincirlerinin kopartılması gibi strateji ve uygulamaları gerektirir. Karmaşıklıkları nedeniyle, etkileri önceden kestirilemeyebilir ve müdahale edilmezse hızla kontrol dışına çıkabilir. Zincirleme, bileşik ve birikimli tehditler bu grupta yer almaktadır.

3.2.2.3. Örtük Tehditler

Bu grup, sistem içinde uzun süre fark edilmeden varlığını sürdürebilen, algılanması zor, düşük görünürlükle hareket eden ve genellikle potansiyel tehdit olarak varlığını koruyan durumları kapsar. Bu tür tehditler, mevcut izleme ve analiz mekanizmalarının ötesinde kalabilmekte; yalnızca özel koşullarda, tetikleyici bir unsurun etkisiyle görünür hale gelmektedir.

Yönetilmeleri için proaktif gözetim, çok kaynaklı veri analitiği ve erken uyarı sistemleri gibi ileri düzey izleme ve analiz yetkinlikleri gerekir. Bu tehditlerin geç fark edilmesi, müdahale sürecinin zamanlamasını kritik hale getirir ve riskin etkisini büyütebilir. Uyuyan ve gizli tehditler bu grupta yer almaktadır.

3.2.2.4. Beliren Tehditler

Beliren tehditler, aniden ortaya çıkan, henüz sistemde tanımlanmamış ve bilinmeyen, etkileri ve olasılıkları netleşmemiş, ancak gelişim eğilimi gösteren ve zamanla daha ciddi hale gelebilecek tehditlerdir. Öncesinde net sinyal vermeyebilir, çoğu zaman beklenmedik şekilde görünür hale gelir.

3.2.3. Muğlaklık ve Belirsizlikler

Muğlaklık, iş dünyasında bir durumun veya olayın başlangıçta tanımlanabilir olmasına rağmen, sonuçlarının yorumlara açık, farklı anlamlar çıkarılabilir ve kesin öngörülemeyecek nitelikte olmasıdır. Bodenhausen ve Peery'ye göre (2009), muğlaklık, ilgili bilgiler mevcut olmasına rağmen bunların anlamı ve yer aldığı bağlam net olmadığı durumlarda oluşur. Muğlaklık durumlarında mevcut bilgiler vardır, ancak bu bilgiler farklı paydaşlar tarafından farklı şekillerde yorumlanabilir (Sharif & Irani, 2017). Bader vd. (2019), muğlaklığı durumun tam olarak anlaşılmasındaki zorluk olarak açıklamakta ve nedensel ilişkilerin tamamen net olmamasının bu duruma yol açtığını belirtmektedir.

Söz konusu durumda etki kısmen tahmin edilebilir olsa da, olasılık ve sonuçların netliği düşük düzeydedir. Bu nedenle muğlaklık, karar verme süreçlerinde belirsizlikten farklı olarak, bilgi eksikliğinden değil, bilginin çoklu anlam taşımasından ve net yorum yapılamamasından kaynaklanır. Robbins (2018), kavramı karar vericinin dışarıdan gelen sinyalleri net, kesin veya

doğru bir şekilde okuma kapasitesinin eksikliğiyle ilişkilendirir. Muğlak ortamlarda karar alıcılar, verilerin ve sinyallerin tutarsızlığı, piyasa göstergelerinin çelişkili olması, farklı senaryoların eş zamanlı geçerli olabilmesi gibi durumlarla karşı karşıya kalır.

Knight (1921), belirsizlik durumunu “gelecekteki olayların gerçekleşme olasılığının tanımlanamaz ve hesaplanamaz olmasıyla karakterize edilen bir durum” olarak ifade etmektedir. Belirsizlik kavramı, literatürde “mevcut veya gelecekteki koşullara ilişkin eksik veya kusurlu bilgi” olarak tanımlanmaktadır (Brouwer & De Blois, 2008). Kavram, Bouyssou vd. (2010) tarafından “eksik bilgi durumu”; Gansch ve Adee (2020) tarafından “bilinmeyen ve yetersiz bilgi durumu” şeklinde ifade edilmektedir. Faber ve Proops (1990), bilgisizlik durumunun olası sonuçlar hakkında herhangi bir fikre sahip olunmaması anlamına geldiğini ifade etmektedir. Durumun benzersiz ve kendine özgü olması nedeniyle olasılık dağılımı ve gerçekleşme şeklinin bilinmesi mümkün değildir (Amoroso vd., 2017). Belirsizlik, verinin yeterli ve net olmaması, durumun öngörülemezliği ile ortamın karmaşıklığından kaynaklı olabilir (Alleman & Quigley, 2024). 2020-2022 yılları arasında küresel ölçekte yaşanan ve hakkında bilgi sahibi olunmayan bir virüsün bir anda ortaya çıkması sonucunda gerçekleşen COVID-19 pandemisi belirsizliğe örnek olarak verilebilir.

Belirsizliklerin yönetilmesi, tanımlanması ve niteliklerinin tespit edilmesiyle mümkün olur (Skinner vd., 2014). Bilinmeyen, eksik ya da kusurlu bilginin kavramsallaşmış hali olarak, belirsizlikler literatürde farklı şekillerde sınıflandırılmıştır (Gansch & Adee, 2020).

Bevan (2022), belirsizlik ve belirsizlik türlerine ilişkin çerçevelerini incelediği çalışmasında altı temel sınıflandırma yönteminden bahsetmektedir. Yazar, anılan sınıflandırmalardan ilki olan belirsizliğin doğası kaynaklı sınıflandırmada aleatorik ve epistemik belirsizlik türlerinden bahsederken, Bronk (2011) bu sınıflandırma yöntemine ontolojik belirsizliği eklemiştir.

3.2.3.1. Aleatorik Belirsizlikler

Aleatorik belirsizlik, bir olgudaki içsel belirsizliğin doğal rastlantılardan kaynaklandığı durumları ifade etmekte olup, genellikle stokastik süreçlerle ilişkilendirilmektedir (Kiureghian & Ditlevsen, 2009). Bu rastlantısal belirsizlik, insan ve doğal sistemlerde görülen doğal rastlantısallıktır (Skinner vd., 2014). Aleatorik belirsizlikler tesadüfilikten kaynaklanır (Howell, 2016); ek bilginin elde edilmesi ya da belirsizliğin analiz edilmesi yoluyla azaltılamaz (Kiureghian & Ditlevsen, 2009). Olasılıksal dağılımlar yoluyla tahmin edilebilir (Gansch &

Adee, 2020). Zar atma oyunu aleatorik bir belirsizlik örneğidir. Her zar atışının sonucu rastgele olup, atışlar önceki atışlardan bağımsızdır ve etkilenmezler. Dolayısıyla kesin sonuç bilinemez.

Aleatorik belirsizliklerde, kuruluşun belirsizliğin kaynağı üzerindeki kontrol düzeyine göre gerçekleşme olasılığının azaltılması mümkün olabilir.

- İçsel kaynaklı durumlarda (örneğin makine arızası, insan hatası, süreç aksaklıkları) proaktif bakım, eğitim ve süreç iyileştirme yoluyla gerçekleşme olasılıkları düşürülebilir.
- Dışsal nedenlerde (doğal afetler, tedarik zinciri sorunları, ekonomik dalgalanmalar) olasılığı azaltmak genellikle mümkün değildir. Bununla birlikte, etkileri azaltmak için önceden hazırlık ve planlama yapılabilir. Aleatorik belirsizlikler, risk analizi ile olasılık bazlı strateji ve araçların kullanımına uygundur.

Aleatorik belirsizlikler, olasılığı bilinen ancak zamanı öngörülemeyen olaylara dayanır. Bu tür durumlarda kuruluşlar, önceden tanımlanmış senaryolar ve protokollere dayalı hazırlıklar yapar.

3.2.3.2. Epistemik Belirsizlikler

Epistemik belirsizlik, bilgi eksikliğinden kaynaklanan ve sahip olunan bilginin artması ya da modelin geliştirilmesi yoluyla azaltılabilen belirsizliği ifade eder (Kiureghian & Ditlevsen, 2009). Teorik olarak, daha fazla veri elde edilerek, daha hassas ölçüm yapılarak ya da daha iyi model kullanılarak azaltılabilir ya da ortadan kaldırılabilir. Belirsizliğe ilişkin araştırma ve kök neden analizinin yapılması, uzman görüşüne başvurulması aracılığıyla eksik bilginin giderilmesi ve böylece belirsizliğin yönetilmesi sağlanabilir (Alleman & Quigley, 2024). Herhangi bir coğrafi alandaki yer altı suyunun varlığı ya da miktarı hakkında başlangıçta bilgi sahibi olunmaması epistemik belirsizliğe örnektir. Ancak, sondaj ve çeşitli ölçümlerle bu belirsizlik azaltılabilir. Muğlaklık durumu (anlam belirsizliği), epistemik belirsizliğin bir özel türüdür (Enserink vd., 2013).

Epistemik belirsizlikler, karar verilebilmesi amacıyla değerlendirme ve yargı oluşturulmasını gerektirir (Howell, 2016). Eksik ya da yetersiz bilgi ile nitelendirilen epistemik belirsizlikte, karar verici bu durumun farkındadır. Bu açıdan, epistemik belirsizlik bilinen-bilinmeyeni ifade etmektedir (Taleb, 2007). Bu tür belirsizliklerde bilgi artırımı, senaryo analizleri ve deneyimli personel görüşlerinden yararlanılır; kapasite geliştirme ve esnek karar

yapıları ön plana çıkar. Kuruluşlar, bilgi toplama ve çeşitli ortaklıklar kurma gibi belirsizliği azaltma stratejileri ile esneklik, inovasyon ve çeşitlendirme gibi başa çıkma stratejilerini kullanmaktadırlar (Sharma vd., 2020).

Epistemik belirsizlik ilke olarak bilgi artırımıyla azaltılabilir, ancak bazı durumlarda bilgiye zamanında erişim mümkün olmayabilir. Örneğin, siber güvenlik açıkları düzenli testler ve eğitimle kontrol altına alınabilirken; tedarikçinin ani üretimden çekilmesi gibi dışsal ve bilinmeyen durumlarda önleyici müdahale imkânı yoktur.

Olay anında duruma özgü çözümler geliştirme, karar destek sistemlerinden yararlanma ve yönetsel esneklik kritik hale gelir. Örneğin, yeni bir düzenlemenin etkileri hakkında belirsizlik yaşayan bir banka, farklı senaryolar altında olası mali etkileri modelleyebilir. Olay sonrasında kuruluşun, yaşanan olaydan öğrenerek mevcut halinden daha gelişmiş bir duruma evrilmesi (*bounce forward*) söz konusudur. Olay sonrasında kurumsal öğrenme ve sistem iyileştirme süreçleri devreye girerek kurumsal hafıza oluşturulur. Bu belirsizlik türünde öğrenme ve uyum kapasitesi önem arz etmektedir.

3.2.3.3. Ontolojik Belirsizlikler

Ontolojik belirsizlik, “sistemin ilgili bir yönünün modelinde tam bir bilgisizlik durumu” olarak tanımlanabilir (Gansch & Adeo, 2020). Rastlantısallık ya da bilgi eksikliğinden bağımsız olarak var olan bir belirsizlik türüdür. Amoroso vd. (2017), ontolojik belirsizlikte, olayların doğası ile bundan kaynaklı gerçekleşme olasılıklarının bilinemediği durumların söz konusu olduğuna vurgu yapar. Benzer şekilde Bronk (2011), bu belirsizlik türü için “henüz yaratılmamış veya henüz evrimleşmemiş olanın kategorilerini ve olası doğasını bile bilmenin imkânsızlığını” dile getirir ve gerçekleşene kadar önceden ölçülmesinin mümkün olmadığını ifade eder.

Bilinmeyen-bilinmeyen olarak ontolojik belirsizlik, cehalet durumuna karşılık gelmektedir. Karar verici bilmediğinin farkında değildir (Taleb, 2007). Ontolojik belirsizliklere karşı genel dayanıklılığın artırılması hedeflenir. Esneklik, adaptasyon kapasitesi, çeşitlilik ve öğrenen organizasyon yapısı ön plana çıkar. Sezgi, gözlem ve durumsal farkındalık yetkinlikleriyle kurumsal esneklik ve kapasite güçlendirilmelidir. Bu tür belirsizliklerde etki ve olasılığı azaltmak genellikle mümkün değildir.

Kuruluşlar, ontolojik belirsizliklere karşı olay öncesinde esnek, yenilikçi ve kapsayıcı kültürler oluşturarak hazırlık yapar. Olay anında doğaçlama, hızlı yeniden yapılandırma ve liderlik ön plana çıkar. Olay sonrasında ise kurumsal dönüşüm (*build back better*) ve yeniden yönelim gerçekleşir. Kurumlar “eski normale” dönmek yerine, yeni koşullara uyum sağlayan daha dirençli bir yapı oluşturur. Bu tür belirsizliklerde *dönüştürücü kapasite*, kurumların sadece hayatta kalmasını değil, aynı zamanda gelişmesini sağlar.

3.2.4. Cehalet (Tam Bilgisizlik)

Cehalet durumu, kuruluş açısından henüz bilinmeyen, gündeme girmeyen herhangi bir olgu ya da durumun varlığı ya da yokluğu hakkında bilgi sahibi olunmaması durumunu ifade etmektedir. Aven ve Steen (2010), cehaleti, “belirli olayların, sonuçların veya sonuçların olasılığı hakkında farkındalık eksikliği olan bir durum” olarak tanımlamaktadır. Yazarlar, karar vericinin bilmediğinin farkında olmamasına istinaden cehaleti, belirsizlik veya riskten ayırır. Roy ve Zeckhauser (2015), kavramı “hem bilinmeyen hem de bilinmeyen bir durum” şeklinde açıklamaktadır.

Cehalet durumu, kuruluşun herhangi bir riskin, tehdidin, belirsizliğin ya da farklı bir olumsuz durumun varlığından tamamen habersiz olduğu ve bu duruma ilişkin farkındalığının dahi bulunmadığı bir durumu ifade eder. Proaktif değil, ancak olay gerçekleştikten sonra öğrenilebilir. Oehmen vd. (2020) dayanıklılığı, kuruluşların cehalet (tam bilgisizlik) durumunu yönetme yetkinliği olarak tanımlamaktadır. Bu doğrultuda cehaletin ontolojik bir bilinmezlik olduğu söylenebilir.

Örneğin, bilim dünyası, insan sağlığına tehdit olabilecek henüz keşfedilmemiş mikroorganizmalar hakkında tam bilgisiz olup, bu durum bilim dünyası adına cehalet durumudur. Faaliyet alanına yönelik küresel eğilimleri izlemeyen bir kuruluşun, sürpriz bir mevzuat ya da düzenleme güncellemesi durumunda ciddi uyum sorunları yaşayabilmesi de örnek olarak verilebilir.

3.3. Olumsuz Durum Türlerinin Sınıflandırılması

Durum türlerine ilişkin önceki bölümde sunulan açıklamalar ve türlerin özgün nitelikleri çerçevesinde olumsuz durumları birbirinden ayırt edebilmek için üç temel kriterin belirleyici

olduğu görülmüştür. Bunlar; (1) durumun varlığına ve gerçekleşmesine ilişkin farkındalık düzeyi, (2) etki ve olasılık değerlerinin bilinebilirliği ve (3) sonuçların öngörülebilirliğidir.

İlk kriter olan belirsizliğin var olup olmadığının fark edilmesi hususu, “belirsizliğin mevcut olmasına rağmen kurum, birey ya da sistem tarafından fark edilmemesi, edilememesi” olarak değerlendirilebilir. Bir durumun farkına varılamaması halinde, sonraki aşamalara geçilmesi mümkün değildir. Bu nedenle başlangıç ölçütü olarak belirlenmiştir.

Farkındalık, “olayları, nesneleri veya duyuşsal kalıpları algılama, hissetme veya bunların bilincinde olma durumu veya yeteneği” olarak tanımlanmaktadır (Gafoor, 2012). Bu durumun karşıtı olan farkında olmama durumunda, algılama ve bilinç yoktur. Belirsizliğin varlığına ilişkin farkında olmama durumu, Faber ve Proops (1990) tarafından “olası durumların, koşulların veya sonuçların farkında olunmaması” olarak ifade edilmektedir. Belirsizlik ölçeğinde, bilinmeyen bilineni olarak determinizmin diğer uç noktasıdır (Walker vd., 2003). Örneğin, 2000 yılı öncesinde yapay zekânın ilerleyen zaman içerisinde bir tehdit yaratabileceği düşünülmemiş ve bu duruma ilişkin herhangi bir bilgi üretilmemiştir. Bu nedenle, yapay zekâ tehditleri 2000 yılı öncesinde farkında olunmayan bir belirsizlik, yani farkındasızlık, cehalet (ignorance) durumunu yansıtır.

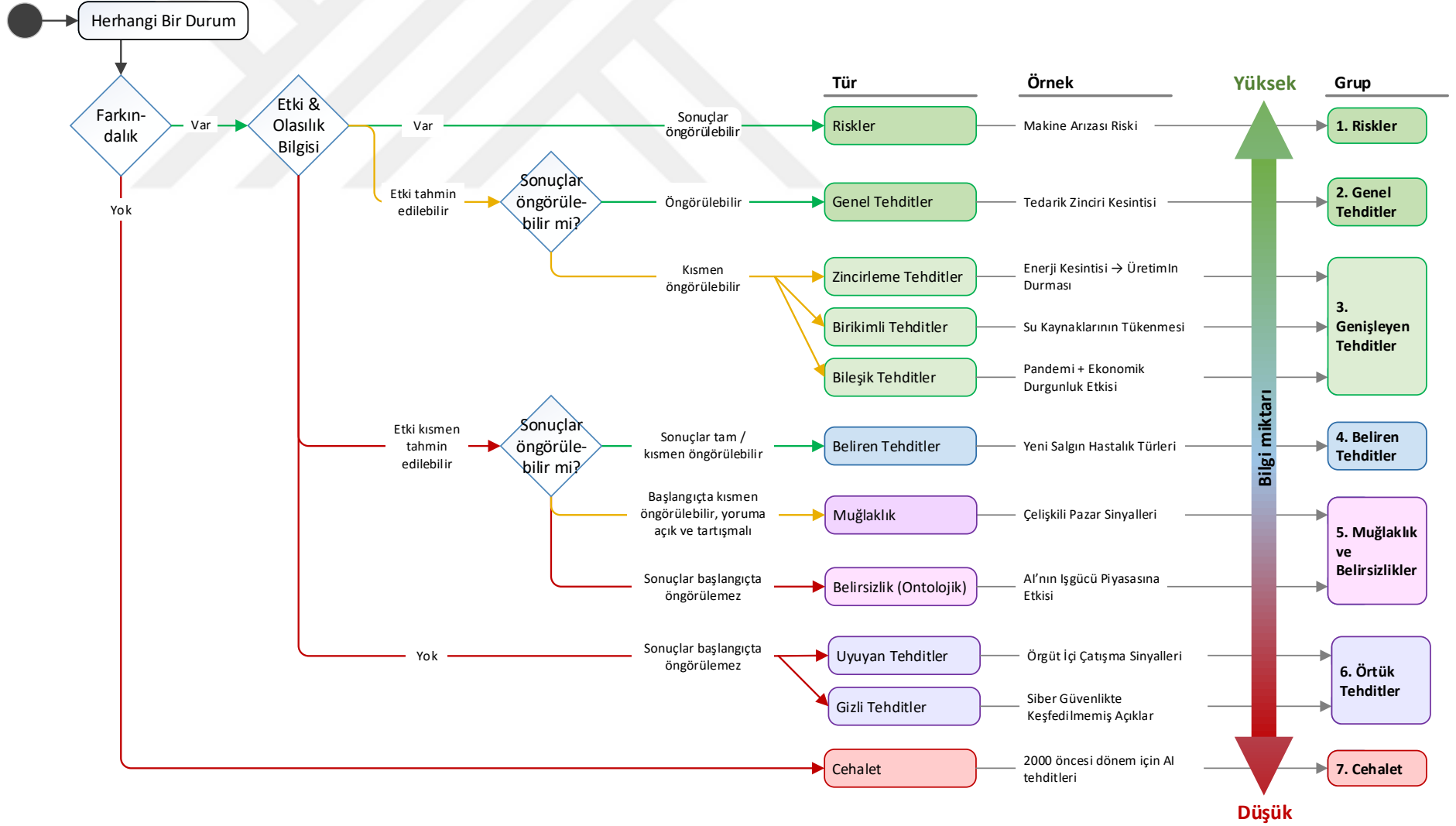
İkinci adım, farkında olunan bir durumun etki ve olasılık değerlerinin bilinebilirliğidir. Bu aşamada, söz konusu olayın tahmin edilip edilemeyeceği, olasılık dağılımları ya da senaryolar üzerinden değerlendirilmektedir.

Son aşama ise, tanımlanmış veya kısmen tanımlanmış bir durumun sonuçlarının öngörülebilirliğidir. Risklerde sonuçlar çoğunlukla öngörülebilirken, beliren tehditlerde bu kısmi düzeyde gerçekleşmekte, ontolojik belirsizliklerde ise tamamen öngörülemez hale gelmektedir.

Bu sıralama, kuruluşların olumsuz durumları anlamlandırma ve yönetme sürecinde, önce farkındalık, ardından ölçüm ve tahmin ve nihayetinde öngörme adımlarını takip etmeleri gerektiği mantığına dayanmaktadır.

Bu çerçevede, durum türlerine ilişkin yer verilen bilgiler çerçevesinde olumsuz durum ve bu durumun yer alacağı sınıfın belirlenmesinde kullanılabilecek bir karar akış diyagramı oluşturulmuştur. Şekil 9’da gösterilen söz konusu diyagram, henüz mahiyeti bilinmeyen olumsuz bir durumun türü ile sınıfının belirlenme sürecini farkındalık, etki-olasılık bilgisi ve öngörülebilirlik karar noktaları doğrultusunda adım adım açıklayan çok katmanlı bir karar akışıdır.

Şekil 9: Olumsuz Durum Türlerinin Farkındalık, Etki-Olasılık Bilgisi ve Sonuçların Öngörülebilirliği Temelinde Sınıflandırılması



Duruma ilişkin bilgi, anılan karar noktalarından elde edilen değerlendirmelerin birleşiminden oluşmaktadır. Bu çerçevede diyagramda ele alınan durumlar, sahip olunan bilgi miktarı doğrultusunda değerlendirilmektedir. Risk durumunda bilgi seviyesi yüksek olmaktadır. Cehalet durumlarında sahip olunan bilgi çok eksiktir ya da hiç yoktur. Bilgi miktarı kuruluşların anılan durumlara vereceği yanıtların proaktif, adaptif, reaktif ya da kapasitif olması üzerinde doğrudan etkilidir.

Diyagram, karar vericiler açısından gri alan olarak değerlendirilen muğlaklık durumunu da kapsamaktadır. Muğlaklık durumunda, sahip olunan bilgi seviyesi yüksek olsa da farklı yorumlara açık olması nedeniyle net bir sonuca ulaşılamamaktadır. Ara seviyedeki tehdit türlerinde ise sahip olunan bilginin kısmen, yaklaşık ya da eksik olduğu, ancak bazı türlerde zaman, deneyim, gözlem ve analizle bilgi seviyesinin artırılabilceği durumları ifade etmektedir. Bu durum, olumsuzlukla başa çıkılmasında teknik bilginin yanı sıra kurumsal öğrenmenin önemini de göstermektedir. Kurumsal öğrenme edinilen bilginin kuruluş içerisinde dağıtıldığı, yorumlandığı ve sonradan kullanılması amacıyla muhafaza edildiği bir süreç olarak tanımlanmaktadır (Huber, 1991). Deneyim, gözlem ve analizler yoluyla edinilen bilginin kurumsallaşması, yaşanacak olası olumsuz durumların önüne geçilmesi, etkisinin azaltılması gibi açılardan önem arz etmektedir.

Diyagram, her bir duruma yönelik olay öncesi hazırlık ile olay sonrası müdahale stratejileri ve eylemlerinin belirlenmesi bakımından altyapı niteliği taşımaktadır. Bu bağlamda, akış şeması kurumsal dayanıklılığın sağlanması sürecine yönelik bir başlangıç aşaması olarak düşünülebilir.

Akış diyagramında görüldüğü üzere, sınıflandırma yapısı farklı durumların kavramsal ayrıştırılmasına ilave olarak, sahip olunan bilgiye dayalı bir şekilde durumların önceliklendirilmesi ile hangi seviyede ve ne tür araçlarla karşılık verileceği hususlarının değerlendirilebilmesi de mümkün hale gelmektedir.

Sınıflandırmanın uygulamaya dönüştürülebilmesini teminen diyagramdaki her duruma yönelik, duruma ilişkin bilgi ile etki-olasılık seviyesi ve öngörülebilirlik kriterleri açısından yapılan karşılaştırmalar Tablo 7’de sunulmaktadır. Böylece, akış diyagramındaki soyut sınıflandırma, tablo vasıtasıyla karşılaştırmalı olacak şekilde somutlaştırılmış ve her durumun farklı araçlarla yönetilmesi gerekliliği netleştirilmiştir.

Kurumsal risk yönetimi etki-olasılık bilgisine dayanmaktayken, tabloda bilgi, farkındalık ve öngörülebilirlik kriterleri ilave edilerek daha geniş bir perspektiften tüm durumlar detaylı bir

şekilde sınıflandırılmaktadır. Bu yönüyle kuruluşun amaç ve hedefleri üzerinde olumsuz etki yaratabilecek olası tüm durumlar kapsanmakta ve klasik risk matrisi pratiğinin ötesinde farklı açılardan bilgileri içermektedir.

Hata! Yer işareti başvurusu geçersiz. incelendiğinde, bir durumu yönetilebilir hale getiren ilk eşik noktasının farkındalık olduğu görülmektedir. Farkındalığın olmadığı cehalet hali ise kuruluş açısından oldukça risklidir. Kimi tehdit türleri, zamanla tanımlanabilir ve öngörülebilir hale gelebilmektedir.

Bununla birlikte gizli ve uyuyan tehditler ile cehalet durumlarının bilgi eksikliği, örtüklüğü ya da yokluğu nedeniyle tespit edilmeleri zor olmaktadır. Dolayısıyla bu durumlar için dayanıklılık yönetimi ve araçlarının kullanılması gerekmektedir.

Görüldüğü üzere tüm durumlar için standart bir yaklaşım benimsenmesi olanaklı değildir. Risk temelli araçların kullanılması sadece belirli durumlar için söz konusuysa, bilgi seviyesi azaldıkça durumların yönetilmesinde öngörü, adaptasyon ve organizasyonel öğrenme gibi dayanıklılık temelli araçlar ön plana çıkmaktadır. Dolayısıyla, farklı durumları belirsizlik ve tehdit türleri ile risk olarak sınıflandırmak, hangi durumlarda hangi yaklaşım, araç ve kapasite türlerinin ele alınması hususunda kritik öneme sahiptir.

Tablo 7: Risk, Belirsizlik ve Tehdit Türlerinin Bilgi Temelli Karşılaştırılması

Olumsuz Durum	Bilgi	Farkındalık	Etki - Olasılık	Sonuçların Öngörülebilirliği
Risk	Bilgi mevcut.	Var	Etki & olasılık biliniyor.	Sonuçlar öngörülebilir.
Genel Tehditler	Bilgi mevcut.	Var	Etki tahmin edilebilir.	Sonuçlar öngörülebilir.
Zincirleme Tehditler	Sınırlı bilgi, olaylar ilerledikçe açığa çıkar.	Var	Etki kısmen bilinir.	Kısmen öngörülebilir, etkileri olaylarla birlikte gelişir.
Birikimli Tehditler	Bilgi mevcut ama etkileri zamana yayılmış.	Var	Etki kısmen bilinir, büyüklük ve hız zamana bağlı belirsiz.	Kısmen öngörülebilir, zamana bağlı değişken.
Bileşik Tehditler	Sınırlı bilgi, bileşenler bilinir ama birleşince karmaşılaşır.	Var	Etki kısmen bilinir.	Kısmen öngörülebilir, bileşik etkiler karmaşık.
Beliren Tehditler	Başlangıçta bilgi yok, zamanla, deneyim ve gözlemle kazanılır.	Var	Etki kısmen tahmin edilebilir.	Sonuçlar tam/kısmen öngörülebilir, zamanla, deneyim ve gözlemle görülebilir.
Uyuyan Tehditler	Başlangıçta bilgi sınırlı / yok, ne zaman tetikleneceği bilinmez.	Sinyal düzeyinde	Etki başta bilinmez.	Sonuçlar başta öngörülemez, tetikleyici olaylarla görülebilir.
Gizli Tehditler	Başlangıçta bilgi yok, zaman ve gözlemle kazanılır. Tehdit varlığı ortaya çıkana kadar bilinmez.	Yok	Etki & olasılık bilinmez.	Sonuçlar başta öngörülemez, zaman içinde sistemik analiz veya sezgiyle görülebilir.
Muğlaklık	Bilgi kısmen mevcut, ancak çok anlamlı ve yorum farklılıkları söz konusu.	Var	Etki yoruma açık.	Sonuçlar tartışmalı, kısmen öngörülebilir.

Tablo 7: Risk, Belirsizlik ve Tehdit Türlerinin Bilgi Temelli Karşılaştırılması (Devamı)

Olumsuz Durum	Bilgi	Farkındalık	Etki - Olasılık	Sonuçların Öngörülebilirliği
Belirsizlik (aleatorik)	Tam bilgiye yakın; doğaya dair değişkenlik bilinir. Rastlantısallık kaynaklı, olasılıksal modellerle kısmen yönetilebilir.	Var	Rastlantısallık kaynaklı, olasılıksal modellerle kısmen yönetilebilir.”	Sonuçlar öngörülebilir ama kesin değil.
Belirsizlik (epistemik)	Eksik bilgi (bilgi eksikliğinden kaynaklı).	Var	Bilgi eksikliğinden kaynaklı, araştırma ve veri artırımıyla azaltılabilir.	Sonuçlar kısmen öngörülebilir, bilgi artırımı ve modelleme yoluyla.
Belirsizlik (ontolojik)	Başlangıçta bilgi yok. Gözlemler arttıkça artabilir.	Var	Etki & olasılık bilinemez.	Sonuçlar başlangıçta öngörülemez, zaman içinde sistemik analiz veya sezgiyle öngörülebilir.
Cehalet (tam bilgisizlik)	Olayın varlığı bilinmiyor.	Yok	Bilgi yok	Sonuçlar öngörülemez.

3.4. Sınıflandırmanın Sağladığı Avantajlar

Olumsuz durumların belirsizlik, tehdit ve risk türleri ekseninde sınıflandırılması, kurumsal dayanıklılığın sağlanmasında önemli avantajlar sağlar. Bu sınıflandırma yaklaşımı, öncelikle kuruluşların karmaşık ve belirsizliğin hâkim olduğu ortamlarda bilinçli, hedefe yönelik ve stratejik hareket etmelerine imkân tanır. Bir durumun, analiz edilerek sınıflandırılması, söz konusu durumun doğası ve etkilerinin daha iyi anlaşılması, böylece etkin bir şekilde yönetilebilmesi açısından önem taşımaktadır.

Ayrıca, sınıflandırma doğru aracın, zamanın ve stratejinin seçilerek durumun hem gerçekleşme öncesinde hem de gerçekleşme sonrasında başarılı yönetilebilmesine destek sağlar. Bu proaktif yaklaşım, önemli kayıpları önleyebilir ve iş sürekliliğini sağlamada etkili olabilir (Mousavi & Gigerenzer, 2014).

Belirsizlik durumunda, olumsuz sonuç doğuracak nitelikteki bir belirsizliğin henüz gerçekleşmeden önlenmesi; gerçekleşmesi halinde ise yaşanacak olumsuz sonuçlara, dayanıklılık kapasitesi ve beraberinde dayanıklılık uygulamaları aracılığıyla müdahale edilmesi söz konusudur.

Bir tehdit durumu söz konusuysa, tehdidin izlenmesi ve gerçekleşmesi durumuna yönelik kaynak planlamasının yapılması, kriz durumuna yönelik senaryo çalışmalarının yapılması; tehdidin gerçekleşmesi halinde müdahale şekli açısından tehdidin türünün belirlenmesi önem arz eder.

Risk durumunda ise yanıt kontrol faaliyetleri aracılığıyla, kurumsal kapasitenin artırılarak gerçekleşmenin önlenmesi amaçlanmaktadır. Risk yanıtları, riskin gerçekleşme olasılığı ile gerçekleşmesi halindeki potansiyel olumsuz sonuçları en aza indirmeyi amaçlar (Richman, 2012).

Söz konusu sınıflandırmaların sunduğu başlıca faydalara aşağıda değinilmektedir.

3.4.1. Duruma Özgü Müdahalelerin Geliştirilmesi

Sınıflandırma, her bir belirsizlik türü için en uygun müdahale yaklaşımını belirlemeyi sağlar. Epistemik ve aleatorik belirsizliklere ilave olarak ontolojik olarak ayrıştırılması, belirsizliklerle mücadeleye ilişkin strateji ve yöntemlerin belirlenmesini sağlar (Gansch & Adeo, 2020).

Aleatorik belirsizlikler ile ontolojik belirsizlikler farklı yapısal ve yönetsel cevaplar gerektirir. Aleatorik belirsizlikler için emilim ve tamponlama stratejileri öne çıkarken, ontolojik belirsizlikler için doğaçlama, inovasyon ve yapısal dönüşüm gereklidir.

Örneğin, aleatorik belirsizlikte bir üretim tesisi, olası deprem riskine karşı yedek güç sistemleri, güvenli tahliye planları ve acil durum eğitimleri uygular. Ontolojik belirsizlikte ise bir banka, kripto para teknolojisinin sektörü dönüştürme ihtimaline karşı stratejik inovasyon ekipleri kurarak ve yeni dijital iş modellerini test ederek dönüşüme hazırlanır.

3.4.2. Hazırlık Süreçlerinin İyileştirilmesi

Olay öncesi dönemde hangi tür belirsizlik ya da tehdide karşı hangi kapasite ve mekanizmaların geliştirilmesi gerektiği daha net belirlenebilir. Bu hazırlıklar, erken uyarı sistemlerinden farkındalık eğitimlerine kadar çeşitlenebilir. Bu sayede kurumsal kaynaklar, olası olaylara karşı en verimli şekilde seferber edilir.

Örneğin, bir siber saldırı tehdidi karşısında olay öncesinde erken uyarı sistemleri kurulması, düzenli sızma testleri yapılması ve çalışanlara farkındalık eğitimi verilmesi, hazırlık süreçlerinin iyileştirilmesine örnektir.

3.4.3. Durumların Önceliklendirilmesinin Sağlanması

Olumsuz durumlar, türüne göre önceliklendirme yapılarak, yüksek belirsizlik ve etki potansiyeline sahip olanlara karşı daha güçlü kontroller ve izleme mekanizmaları kurulabilir.

Örneğin, enerji arz kesintisi (zincirleme tehdit) gibi yüksek etki ve yayılma potansiyeline sahip olaylar, tedarikçi teslimat gecikmeleri gibi daha sınırlı etkili durumlara göre önceliklendirilir ve daha güçlü kontrol mekanizmalarıyla takip edilir.

3.4.4. Karar Alma Süreçlerinin Desteklenmesi

Olumsuz durumların türlerine göre sınıflandırılması, karar vericilere olayın doğası hakkında net bir kavrayış sağlar. Bu sayede hangi stratejik veya operasyonel kararların hangi koşullar altında alınması gerektiği daha açık hale gelir. Böylece hızlı, tutarlı ve durumun gerektirdiği uygun kararlar alınabilir.

Optimal kaynak dağıtımının sağlanması ile doğru ve net risk değerlendirmelerinin gerçekleştirilebilmesini teminen belirsizliğin, epistemik ya da aleatorik belirsizlik şeklinde ayrılması karar alınması sürecini iyileştirir (Fox & Ulkumen, 2011).

Örneğin, sağlık sektöründe faaliyet gösteren bir hastane, büyük bir deprem sonrası yaralı sayısındaki artış gibi aleatorik belirsizlikler karşısında önceden oluşturulmuş acil müdahale durumlarındaki tedavi protokollerini ve yedek malzeme planlarını hemen uygulamaya alabilir. Hastane, daha önce görülmemiş bir hastalık türünün ani ortaya çıkışı gibi bir ontolojik belirsizlik karşısında karar alıcılar, klasik karar verme protokollerinin ötesine geçerek yaratıcı ve emprovize kararlar alarak çözümler üretebilir.

3.4.5. Kurum İçi Farkındalık ve Eğitim Kolaylığı

Sınıflandırma, karmaşık kavramları sadeleştirerek kurum içi eğitim ve farkındalık faaliyetlerinde kullanılabilecek güçlü bir çerçeve sunar. Bu da kültürel dönüşüm ve ortak bir anlayışın gelişmesini destekler.

Uyuyan tehditler örneğinde, örgüt içi çatışma sinyalleri veya çalışan memnuniyetindeki düşüşler, eğitim ve farkındalık programlarıyla görünür hale getirilebilir. Bu tür sınıflandırmalar, çalışanların günlük işlerinde tehditlerin doğasını daha iyi kavramasına yardımcı olur.

3.4.6. Stratejik Esneklik ve Adaptasyon

Tehditleri ve belirsizlikleri türlerine göre anlamak, organizasyonun değişen koşullara daha hızlı ve esnek biçimde yanıt vermesini sağlar. Bu da rekabet üstünlüğü ve uzun vadeli dayanıklılık açısından önemli bir avantajdır.

Örneğin, yarı iletken krizinin (bileşik tehdit) otomotiv sektöründe üretim durmalarına yol açması, şirketleri çeşitlendirilmiş tedarik ağlarına yöneltmiştir. Bu sayede, kuruluşlar değişen koşullara daha hızlı adapte olmuşlardır.

3.4.7. Kurumsal Politika ve Strateji Üretimine Katkı Sunulması

Belirsizliklerin (aleatorik, epistemik, ontolojik) sistematik biçimde sınıflandırılması, organizasyonların daha bilinçli, kapsayıcı ve hedef odaklı politikalar geliştirmesine olanak tanır. Bu sınıflama sayesinde, her bir belirsizlik türüne özgü stratejik öncelikler, kaynak tahsisleri ve uzun vadeli hedefler daha doğru biçimde belirlenebilir.

Örneğin, donanım tedarik sürecinde gecikmelerin yaşanması gibi bir aleatorik belirsizlik durumunda, yedek tedarikçilerle anlaşmalar yapılır ve stok politikaları oluşturularak süreklilik sağlanır. Pandemi sonrası küresel dağıtım sistemlerindeki yapısal kırılmaların görülmesi gibi ontolojik belirsizliklerde yerelleşme, yüksek düzeyde otomasyon, dijital tedarik ağı gibi dönüşümsel stratejiler uygulanabilir.

3.4.8. Ortak Bir Terminolojinin Tesis Edilmesi

Belirsizlik ve riskin sınıflandırılması, karmaşık sistemlerdeki belirsizliklerin tanımlanması ve yönetilmesi amacıyla “ortak bir dil” sağlar, böylece paydaşlar arasındaki iletişim geliştirir (Brouwer & De Blois, 2008). Sınıflandırmanın net bir şekilde yapılmasıyla yanlış anlaşılmanın önüne geçilir ve karar vericilerin değerlendirme etkinliklerinin artırılarak yönetim iyileştirilmiş olur (Orderud & Naustdalslid, 2018).

Tablo 8’de durum türleri doğrultusunda müdahale yöntemleri sunulmaktadır. Bu şekilde proaktif bir yaklaşım, önemli kayıplara engel olabilir ve iş sürekliliğini sağlayabilir (Mousavi & Gigerenzer, 2014).

3.5. Belirsizlik - Tehdit - Risk - Olay Zinciri

Olay kavramı, olumsuz sonuçlara yol açan, kuruluş tarafından gerçekleşmesi planlanmamış veya beklenmedik gelişmeleri ifade etmektedir. Bir diğer bakış açısıyla kurumsal varlıkları ve hizmetleri önemli ölçüde olumsuz etkileyen ve kurumun yanıt vermesini gerektiren bir gelişmedir (Caralli vd., 2011). Bu istisnai koşulların sonucunda ortaya çıkan olay, meydana getirdiği etkinin büyüklüğü ölçüsünde yıkıcıdır.

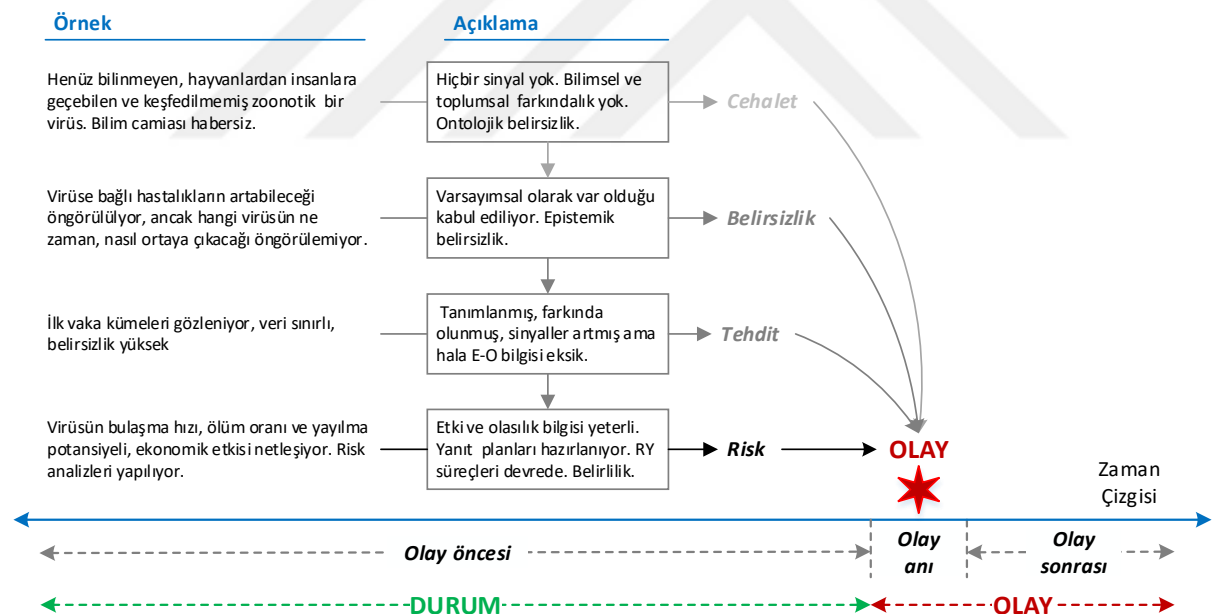
Hata! Başvuru kaynağı bulunamadı.’da cehalet, belirsizlik, tehdit, risk ve olay arasında sahip olunan bilgi miktarı ve bağlamsal ilişkiler gösterilmektedir. Belirsizlikler, bir

anda gerçekleşerek sonuçları itibariyle olumsuz olan bir olaya neden olabileceği gibi, zaman içerisinde hakkında sahip olunan bilginin miktarına göre tehdit ya da riske dönüşebilirler. Benzer şekilde tehditler, doğrudan gerçekleşebileceği gibi, hakkında bilgi sahibi olunmasıyla risk özelliği kazanabilirler. Risklerin gerçekleşmesi durumunda olay durumu ortaya çıkar.

Cehalet, belirsizlik, tehdit ve riskler, olayın gerçekleşmesinden önceki durumlara karşılık gelmektedir. Zaman çizgisi (1) olay öncesi, (2) olay anı ve (3) olay sonrası olmak üzere 3 bölüme ayrılmaktadır.

Olay öncesinde hazırlık amacıyla gerçekleştirilen her türlü eylem proaktif nitelikli olup, olumsuz sonuçları olan durumların gerçekleşmesinin önlenmesi ile gerçekleşmesi durumunda yaratacağı etkinin azaltılmasını amaçlar. Olay anı ve sonrasında kurtarma ve sürekliliği sağlama amaçlı gerçekleştirilen eylemler ise reaktif nitelik taşımaktadır. Dayanıklılık çalışmaları, söz konusu durumları henüz olaya dönüşmeden dayanıklılık kapasitesi aracılığıyla ele alır.

Şekil 10: Cehalet, Belirsizlik, Tehdit, Risk ve Olay Zinciri



3.6. Durum Türlerine Yönelik Yönetim Araçlarının Belirlenmesi

Kurumsal yönetim, farklı durum türleri doğrultusunda farklı müdahale yaklaşımlarının uygulanabilir olmasını teminen yapılandırılmış, somut ve sistematik yaklaşımları gerektirmektedir. Bu doğrultuda olası durumlara yönelik, belirsizlik türleri de dikkate alınarak

olay öncesinde, anında ve sonrasında farklı yönetim yaklaşımlarının devreye girmesi gerekliliği doğmaktadır.

Grote'un (2004) ifade ettiği üzere, belirsizliğin sistematik ve planlı bir şekilde azaltılması ya da belirsizlikle mücadele edilmesi için durumun karakteristiğine göre merkezi ya da yerinden yönetim, merkezi planlama, yetkilendirme ve otonomi gibi araç ve yöntemlere başvurulmalıdır. Gansch ve Adeo (2020) tarafından ortaya konulan çerçevede "belirsizliğin türünün yalnızca bilgiyle değil, aynı zamanda kurumun sahip olduğu müdahale araçlarının türü ve uygulanmasına ilişkin zamanlamayla da yakından ilişkili" olduğu vurgulanmaktadır. Bu bağlamda bir durumun türü netleştirildiğinde yönetim yaklaşımı ve müdahale araç ve uygulamaları belirgin hale gelmektedir.

Kuruluşların karşılaştığı belirsizlik, tehdit ve risk durumları, olay öncesinde durumun fark edilmesinden başlayarak olay öncesi, olay anı, esnası ve sonrasındaki kurtarma, iyileşme süreçlerine kadar süreklilik arz eden bir müdahale döngüsünü gerektirmektedir. Bu çerçevede, kuruluşların yaşam döngülerini kesintisiz kapsayacak şekilde tasarlanan, birbirlerini tamamlayarak sistematik biçimde aktifleşen müdahale araçlarına ihtiyaç bulunmaktadır.

Bu çalışmada, anılan ihtiyacı karşılamak amacıyla temel yönetim araçları olarak kurumsal risk yönetimi (KRY) ve dayanıklılık yönetimi (DY) kullanılmıştır. İlave olarak KRY'nin bir parçası olarak beklenmedik durum planı (BDP), DY kapsamında iş sürekliliği yönetimi (İSY) ile kriz yönetimine (KY) destekleyici araçlar olarak yer verilmektedir.

Bahse konu araçlar, olay döngüsündeki farklı aşamalara odaklanarak zaman ekseninde birbirlerini tamamlamaktadırlar. KRY; risklerin tanımlanması, analiz edilmesi ve yönetilmesi aracılığıyla olay öncesinde aktif olarak işlemektedir. DY, kurumsal kapasitenin geliştirilmesiyle olay öncesi; öngörü, adaptasyon ve dönüşüm mekanizmaları yoluyla olay anı ve sonrası arasındaki yapısal köprüyü kurmaktadır. KY, olay anında duruma yönelik hızlı bir müdahale gerçekleştirerek paydaşların yönetimi ve hasarın sınırlandırılması şeklinde reaktif olarak süreci yönlendirir. İSY, olayın gerçekleşmesini müteakiben iş süreçlerinin devamlılığının sağlanması amacıyla planlama ve kurtarma faaliyetlerini gerçekleştirmektedir. BDP ise "belirli bir riskin ya da olayın gerçekleşmesi durumunda devreye girmek üzere hazırlanan, önceden tanımlanmış bir eylem planı" olarak ifade edilmektedir (ISO, 2019).

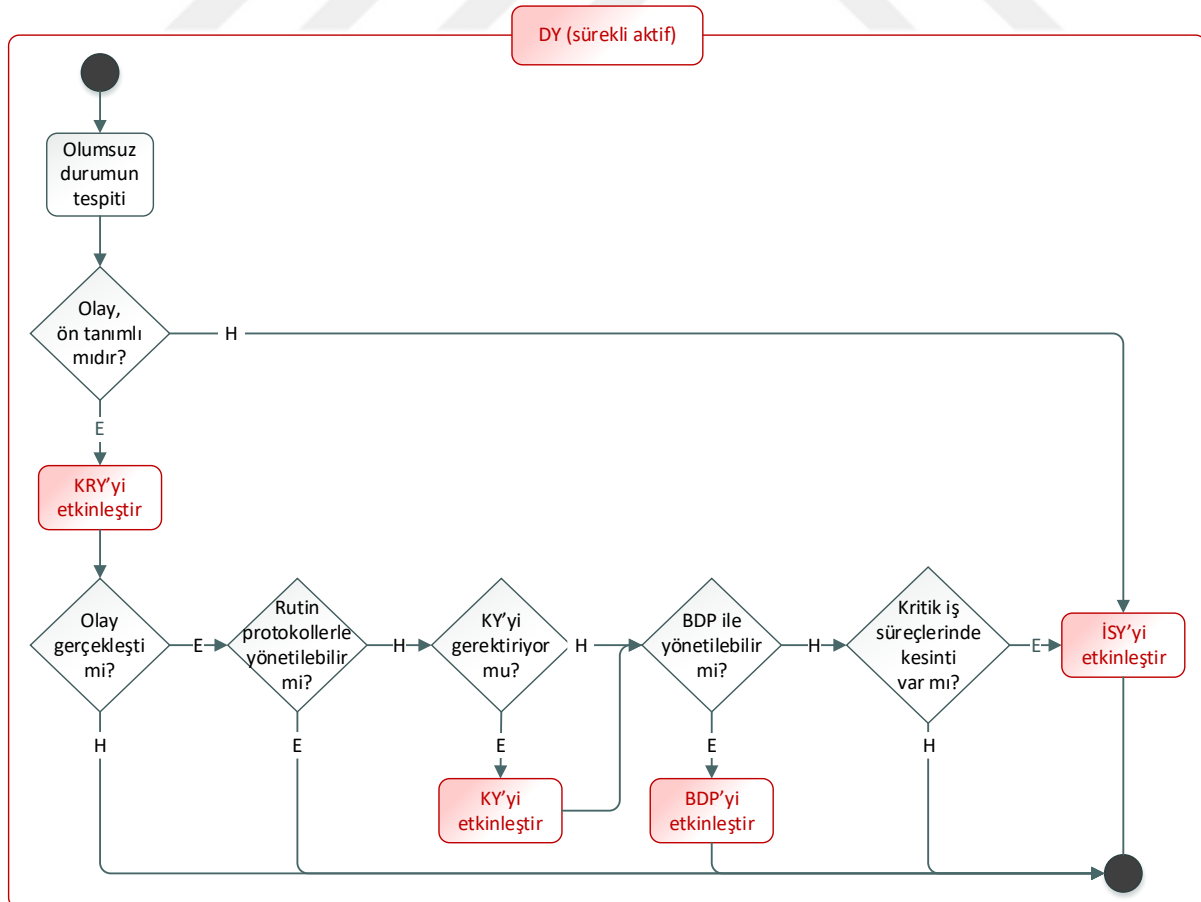
Diğer taraftan bahsi geçen araçlar, kuruluşların proaktif, reaktif ya da adaptif kapasitelerini bütüncül bir şekilde desteklemektedir. KRY aracılığıyla öngörü ve önleme; İSY ile kurtarma; KY ile olayın anının yönetilmesi; BDP ile risklerin gerçekleşmesi durumuna

yönelik eylemlerin hayata geçirilmesi ve DY ile tüm sürecin dayanıklılık kazanması sağlanmaktadır.

Bu doğrultuda, çalışmada anılan araçların kullanılması, kuruluşların yaşamları boyunca koruma ve müdahale çerçevesi içerisinde kalması ve müdahale yöntemlerinin zaman ekseninde modellenmesi amacıyla kapsam bakımında yeterli olarak değerlendirilmektedir. Bir durumun gerçekleşme öncesi, anı ve sonrasında ilişkin hangi araçların aktifleştirilmesi gerektiğine dair karar akış diyagramı Şekil 11’de sunulmaktadır.

Karar akışı, olumsuz bir durumun tespit edilmesiyle başlamakta ve bahse konu durumun rutin protokol ve prosedürlerle yönetilebilme durumunu irdelenmektedir. Yönetilmesi mümkünse ilave bir müdahaleye gerek yoktur; ancak yönetilemiyorsa KRY aktifleştirilmektedir. Olay gerçekleşirse, kriz niteliği taşıma durumu ile operasyonel sürekliliği etkileyip etkilemediği ve BDP ile yönetilebilme hususları değerlendirilerek buna göre KY, İSY ve BDP’den hangisi ya da hangilerinin aktifleştirileceği karar verilir ve ilgili araçlar etkinleştirilir. DY, sürecin başlangıcından sonuna kadar her aşamada sürekli aktif olmakta ve onarım, uyum ve dönüşüm kapasitelerini desteklemektedir.

Şekil 11: Müdahale Araçlarının Etkinleştirilmesine Yönelik Karar Akış Diyagramı



Söz konusu araçların kurumsal seviyede uygulanabilir hale getirilmesi amacıyla, Şekil 11'deki karar akışı diyagramından faydalanılarak, ele alınan her bir durum için olay öncesi, anı ve sonrası aktifleşmesi gereken yönetim yaklaşımları Tablo 8'de gösterilmektedir.

Olay fazlarını dikkate alarak hazırlanan Tablo 8, proaktif ve reaktif müdahale yaklaşımlarının kurumsal düzeyde uygulanabilirliğini görünür hale getirmektedir. Tabloda, durum türü çerçevesinde DY'nin ilgili aşamada ağırlıklı olarak hangi kapasitesinin etkin olacağı gösterilmektedir. Öngörü ve hazırlık kapasitesi ile önleyici kapasite, ağırlıklı olarak olay öncesi aşamada etkindir. Özümseme kapasitesi, genellikle olay anında devreye girer. Onarım, uyum ve dönüşüm kapasiteleri, olay anında başlar, olay sonrasında daha belirgin hale gelir.

Öte yandan dayanıklılık kapsamında belirsizlik türleri, olay fazları ve kullanılan yönetim araçları çerçevesinde aktifleştirilen, gerçekleştirilen uygulamalar farklılaşmaktadır.

Tablo 8: Olumsuz Durum Sınıfların ve Olay Fazına Göre Yönetim Araçları

Olumsuz Durum Sınıfları	Yönetim Araçları		
	Olay Öncesi	Olay Anı	Olay Sonrası
1. Riskler	DY (öngörü ve hazırlık, önleyici)+ KRY	DY (özümseme) + KY + BDP	DY (onarım, uyum dönüşüm) + BDP + İSY
2. Genel Tehditler	DY (öngörü ve hazırlık, önleyici)	DY (özümseme) + KY	DY (onarım, uyum dönüşüm) + İSY
3. Genişleyen Tehditler	DY (öngörü ve hazırlık, önleyici)	DY (özümseme) + KY	DY (onarım, uyum dönüşüm) + İSY
4. Beliren Tehditler	DY (Hazırlık)	DY (özümseme) + KY	DY (onarım, uyum dönüşüm) + İSY
5. Muğlaklık ve Belirsizlikler	DY (Hazırlık)	DY (özümseme) + KY	DY (onarım, uyum dönüşüm) + İSY
6. Örtük Tehditler	DY (Hazırlık)	DY (özümseme) + KY	DY (onarım, uyum dönüşüm) + İSY
7. Cehalet	DY (Hazırlık)	DY (özümseme) + KY	DY (onarım, uyum dönüşüm) + İSY

Tabloda her duruma ilişkin olay anı ya da sonrası için KY ya da İSY'ye yer verilmesi mutlaka aktifleştirileceği anlamına gelmemektedir. Kriz yönetimi, gerçekleşen olayın etkisinin büyüklüğü, yayılma alanı vb. hususlar doğrultusunda; İSY ise sürekliliği etkileyen bir durumun gerçekleşmesi durumu dikkate alınarak, ihtiyaç halinde aktifleştirilir.

3.7. KRY ve DY Arasındaki İlişkilerin Tanımlanması

Risk ve dayanıklılık sistem düşüncesi bağlamında birbirleriyle ilişkili kavramlardır (Aven, 2017). COSO (2017) çerçevesi, kurumsal risk yönetiminin uzun vadede kurumsal dayanıklılığı artıracığını vurgulamaktadır. Kurumsal dayanıklılık kavramı, risk ve kriz yönetimi süreçlerini birlikte kapsayan bütüncül bir bakış açısını ifade eder (Aksay & Şendoğdu, 2022).

Dayanıklılık yönetimi, geniş anlamda içerisinde risk yönetimi, iş sürekliliği uygulamaları, kriz yönetimi gibi araçları barındıran ve bunların birbirleriyle entegre çalışmasını sağlayan disiplinler arası bir yaklaşımdır (Häring, 2015). Dayanıklılık yönetimi, dışsal değişimlerin öngörülmesi, mümkün olduğunca önlenmesi ve gerçekleşmesi durumuna yönelik yanıt eylem planlarının hazırlanmasını sağlayan, olayı müteakiben karar verme süreçlerine yardımcı olan bir çerçevedir (Leflar & Siegel, 2013). Bu çerçeve, arzu edilmeyen olayların gerçekleşmesinin önlenmesi ve gerçekleştiğinde durumun yönetilerek kuruluşların varlıklarını sürdürmelerine yönelik kapasitelerini güçlendirir. Dayanıklılık, tek seferlik ve rutin olmayan olayların yanında risklerin süreklilik ve güncellik sağlayacak şekilde yönetilmesi ve yanıt olarak kaynakların etkin kullanım becerisiyle kendini gösterir (Sutcliffe & Vogus, 2003).

Kuruluşlarda KRY'nin varlığı risklerin etkin bir şekilde yönetildiğinin göstergesi olarak paydaşlarının güvenini kazanılmasını sağlar. Bu güven, kuruluşların uzun vadeli dayanıklılıklarına olumlu olarak yansır (Assibi, 2022). Risklerin kurumsal düzeyde yönetilmesi sürecine kuruluşun yanında insan kaynakları, pay sahipleri, tedarikçiler ve sendikalar gibi paydaşlar dâhildir. Bu çerçevede kuruluşun paydaşları ile olan iş birliklerinin artırılması dayanıklılığın güçlendirilmesini sağlar (Häring, 2015).

Risk değerlendirmeleri, kuruluşun gelecekte karşılaşacağı olayları, belirsizlik, tehdit ve riskler olarak tanımlayarak, risklere ve beklenmedik senaryolara hazırlıklı olmasını sağlar (Aven, 2017). Risklere yönelik mevcut bilgi, daha iyi anlaşılmasının sağlanmasını teminen varsayım ve düşüncelerin incelenmesi vasıtasıyla olası negatif sürprizlerin önceden bilinmesine ve araştırılması gereken alanların belirlenmesine katkıda bulunur (Aven, 2017). Kuruluşlar, önemli iş faaliyetlerinin tanımlanmasına yönelik risk değerlendirme ile kontrol öz değerlendirme gibi araçları kullanarak, kritik faaliyet alanlarına odaklanırlar (PWC, 2021). Risk odaklı yaklaşım, tehditlerin özellik ve kapsamı ile etkilerinin tanımlanması ve değerlendirilmesini sağlayan yapılandırılmış bir yaklaşımdır (Bosetti vd., 2016).

Dayanıklılık yönetimi, risk deęerlendirmeleri sonucunda elde edilen bilgileri kullanarak kaynakların etkin kullanılması amacıyla hangi alanlara yönelik güçlendirmelerin öncelikli olacağına karar verir (Aven, 2017). Kuruluşların tüm birim ve fonksiyonlarının birbirleriyle iletişim içinde iş yapmalarının sağlanarak risklerin azaltılması ve fırsatların artırılmasını sağlamak üzere kaynakların optimizasyonunun sağlanması, dayanıklılık yönetiminin sağlayacağı oldukça önemli bir faydadır (Leflar & Siegel, 2013).

KRY, kurumsal hedef ve stratejilerin belirlenmesi sürecinde, kuruluş açısından önem arz eden risklere yönelik anlayışı güçlendirir ve böylece karar alma süreçlerinin iyileştirilmesinde rol oynar (Amuah, 2023). Operasyonel risklere yönelik çerçeveler, kuruluşların faaliyetleriyle ilişkili kontrol edilemeyenleri de kapsayacak şekilde tüm risklerini tanımlamalarında kılavuzluk yapar.

Risk yönetimi, sistemleri etkileyen temel olay ve stresleri tanımlayarak analiz eder. Bu analiz sonucunda dayanıklılığın artırılmasına ihtiyaç duyulan alanlar belirlenerek stratejiler geliştirilir (OECD, 2014). Risk yönetimi, şok ve stresin sistem üzerindeki etki ve olasılığını analiz ederek riskleri önceliklendirir, bu yolla odaklanılması gereken alanlara işaret eder (OECD, 2014). Etkin bir KRY, öngörü kapasitesini artırarak, dayanıklılığı artırır (Tjahyono vd., 2024).

Proaktif bir risk yönetimi, kuruluşlarda dayanıklılık kültürünün oluşmasına ve risk yönetiminin operasyonların doğal bir bileşeni olarak görülmesine destek sağlar. Kuruluşların dayanıklılık kapasitesini artırmak üzere hedefe odaklı karar almalarına katkı sunar (Assibi, 2022). Kuruluşlar, proaktif bir risk yönetimi aracılığıyla olası finansal istikrar ve itibara yönelik olası riskleri öncesinde tespit edebilir, böylece önleyici tedbirler alınması sağlanır. Bu tedbirlerin uygulanması, yıkıcı olayların önlenmesi, iş sürekliliğinin sağlanması ve paydaş çıkarlarının güvence altına alınması bakımından önem arz etmektedir. Risk yönetimi, kuruluşun öngörü kapasitesinin artırılarak olası krizleri yönetmesine imkân sağlar (Amuah, 2023).

Belirsizlik ve risklerin proaktif yönetimi, olası krizlerin önlenmesi ya da etkilerinin azaltılması bakımından genel dayanıklılığın artırılmasında etkilidir (Tjahyono vd., 2024). Risk yönetimi, proaktif davranarak kuruluşların olası tehditleri öngörerek bunlara yönelik hazırlık yapmalarına destek sağlayarak yıkıcı olaylara yanıt verme yetkinliklerini artırmaktadır (Häring, 2015).

Kurumsal risk yönetimi, uyguladığı risk yanıt eylemleri aracılığıyla kurumsal kapasiteyi artırarak, kuruluşların dinamik ve belirsiz bir ortamda başarıya ulaşmalarına katkı sağlar (Häring, 2015). Risk yönetimi, geri beslemeli bir süreç olarak sürekli izleme ve değerlendirmeler sonucunda tecrübelerden elde edilen kazanımların hayata geçirilmesini sağlayarak kurumsal kapasitenin ve dayanıklılığın artırılmasında rol oynamaktadır (Häring, 2015). Risk yönetimi, uyguladığı önleyici ve olayın hemen ardından derhal yanıt verilmesini sağlayan tepki verici kontroller aracılığıyla sistemin dayanıklılık kapasitesine katkı sağlar (Logan vd., 2022).

Sistemlerin şokları absorbe etme ve uyum sağlama kapasitelerinin analiz edilmesi, kuruluşun zayıf ve güçlü olduğu noktaların tespit edilmesi sağlanır. Bu noktalara yönelik eylemlerin tanımlanması dayanıklılığın sağlanmasına katkıda bulunur (OECD, 2014).

KRY, çok disiplinli bir yaklaşım olarak, kuruluşların risklerini yönetmek üzere uyum kapasitelerinin geliştirilmesinde rol oynar (Leflar & Siegel, 2013). Etkin çalışan ve sürekli güncelliği sağlanan bir KRY, kuruluşların dışsal değişikliklere karşı yanıt vermelerindeki çevikliği ve uyum kapasitelerini artırması yoluyla dayanıklılıklarını artırır (Tjahyono vd., 2024).

Risk yönetimine ilişkin çerçeveler, risk çalışmaları, risk kültürü ve farkındalığı gibi KRY uygulamaları, dayanıklılığın sağlanmasına yönelik kurumsal kaynak ve kabiliyetler üzerinde etkilidir (Monazzam & Crawford, 2024). Bu etki, KRY'nin dinamik bir yetkinlik olarak değerlendirilmesine ilişkin anlayışa katkı sağlamaktadır. Bu dinamizm, KRY'nin mevcut risklerin yönetilmesine ilave olarak kuruluşların değişen çevre, şart ve belirsizliklere uyumunun güçlendirilmesine yardımcı olur. Dayanıklılığın artırılmasında kullanılan kaynaklar; risklerin etkin yönetilmesine destek olan yerleşik çerçeve ve kontrollerden oluşan yapısal kaynaklar, iş birliği ve ağ oluşturmayı teşvik eden ilişkisel kaynaklar, risk ve belirsizliklere yönelik anlayışın güçlendirilmesini destekleyen bilişsel kaynaklardır (Monazzam & Crawford, 2024).

KRY, kapsamlı risk değerlendirmesi vasıtasıyla kuruluşun kırılgan, iyileştirilmesi gereken alanlarını tanımlar (Assibi, 2022). KRY uygulamaları, sağladığı koruma katmanı aracılığıyla kuruluşlardaki kırılganlıkların azaltılmasına katkı sunmakta, böylece dayanıklılığa katkı sağlamaktadır (Otun vd., 2023). Kuruluşlar, olası risk ve kırılganlıklarını tespit ederek, değerlendirmeli ve bunları azaltmak ya da yönetmek üzere çeşitli stratejiler geliştirmelidir.

Etkin çalışan bir KRY, kurumsal dayanıklılığın teşkil edilmesi bakımından esastır (Monazzam & Crawford, 2024).

Kuruluşlarda inovasyon kültürü ve yenilikçi uygulamalara açık olunması, tehditlere yanıt verilmesi bakımından önem taşımaktadır (Otun vd., 2023). Dayanıklılık yönetimi, canlı ve etkin bir uyum ve inovasyon kültürü oluşturarak, kuruluşun kendisiyle birlikte çevresinin bu değişime uyum sağlama hususundaki çevikliğini artırır (Leflar & Siegel, 2013).

Literatürde görüldüğü üzere KRY ve DY, kuruluşların belirsizlikler karşısında sürdürülebilirliğini güvence altına almak amacıyla geliştirilmiş iki temel yönetsel araçtır. Her iki araç da olumsuz durumların öngörülmesi, önlenmesi ve yönetilmesi ortak hedeflerini takip etmekte olup, kapsam, zamanlama ve uygulama düzeyleri bakımından birbirleriyle kimi açılardan farklı, kimi açılardan tamamlayıcı olmak üzere çeşitli ilişkilere sahiptir. Söz konusu ilişkiler aşağıdaki tematik başlıklar halinde özetlenebilir.

Bu bölümde “Literatürde, öncüllük-ardıllık, tamamlayıcılık ve kapsayıcılık gibi hususlar açısından KRY ile DY arasındaki ilişkiler nasıl tanımlanmaktadır?” şeklindeki ikinci araştırma sorusu yanıtlanmış olacaktır.

3.7.1. Amaç ve Odak Bakımından Tamamlayıcılık

KRY, yapılandırılmış süreçleriyle risklerin tanımlanması, analiz edilmesi ve stratejik yanıtlar geliştirilmesi üzerine odaklanırken; DY, kuruluşun özümseme, onarım, uyum sağlama ve dönüşme kapasitelerini güçlendirilmesi yaklaşımı vasıtasıyla olayların öncesine ilave olarak olay anı ve sonrasında da ilgilenir.

KRY, DY’nin ön aşamasını oluşturur; DY ise KRY’nin ötesine geçerek olumsuzluklara ve şoklara rağmen varlığını sürdürebilen, uyum sağlayabilen ve gelişebilen bir yapı inşa eder.

3.7.2. Zaman Boyutu ile Tamamlayıcılık

KRY, risklerin ortaya çıkmasından önce olasılık ve etki temelli planlamalar yapar. DY, olay öncesi hazırlık ile olay anı ve sonrasına yönelik müdahale ve toparlanma kapasitesini içerir.

Hata! Başvuru kaynağı bulunamadı.’de görüldüğü üzere belirsizlik, tehdit ve risk durumları olayın gerçekleşmesinden önceki durumu ifade etmektedir. Zaman çizgisi (1) olay

öncesi, (2) olay anı ve (3) olay sonrası olmak üzere 3 aşamaya ayrılmaktadır. Olay sonrasında, gerçekleşmenin yarattığı sonuçlar görülmektedir.

Şekil 12: Belirsizlik, Tehdit, Risk, Olay ve Sonuç Zinciri



Olay öncesinde hazırlık amacıyla gerçekleştirilen her türlü eylem proaktif nitelikli olup, olumsuz sonuçları olan olayın gerçekleşmesini önlemeyi amaçlar. Bu eylemler arasında tehdit ve risk analizlerinin yapılması, risklerin yönetilmesi, iş sürekliliğini sağlamaya yönelik hazırlıkların yapılması ve kurumsal kapasitenin artırılmasına yönelik çalışmalar yer almaktadır.

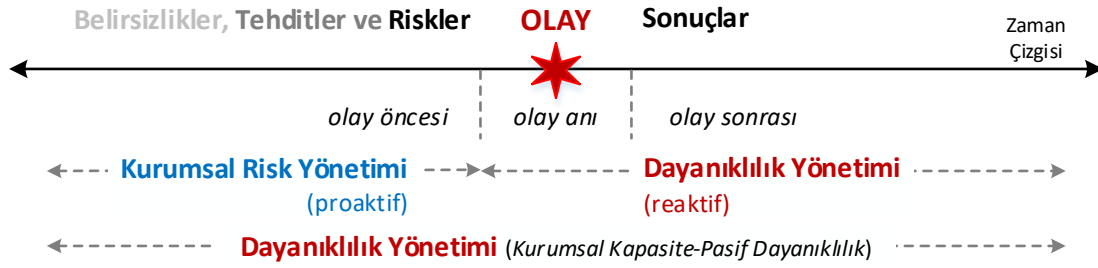
Olay, bir belirsizliğin, tehdidin ya da riskin gerçekleşmesi sonucunda ortaya çıkmıştır. Olay anı ve sonrasında kurtarma ve sürekliliği sağlama amaçlı gerçekleştirilen eylemler ise reaktif nitelik taşımaktadır.

Kurumsal risk yönetimi, olay henüz gerçekleşmeden kullanılan bir araçtır. KRY, bir kuruluşun karşılaşılabileceği riskleri belirleme, analiz etme, değerlendirme ve bu riskleri yönetme sürecidir. Amaç, risklere ait etki ve olasılıkları minimize ederek, herhangi bir sorun, aksaklık, kesinti vb. olmaksızın organizasyonun hedeflerine ulaşmasını sağlamaktır. KRY, risk farkındalığını artırır, kaynakların etkin kullanımını sağlar ve beklenmedik olaylara karşı hazırlıklı olmayı destekler. Kurumsal risk yönetiminin temel görevi uzun vadede kuruluşun dayanıklılığının güçlendirilmesidir (Louisot, 2015).

Şekil 13 'te görüleceği üzere, olay öncesi gerçekleştirilen proaktif eylemler, KRY; olayın gerçekleşmesi ve sonrasında kurtarma ve süreklilik sağlama amaçlı reaktif eylemler DY kapsamında yer almaktadır. İlave olarak, olayın öncesinden başlayarak sonuna değin dayanıklılık kapasitesi arka planda pasif bir dayanıklılık sağlamaktadır. Bu bağlamda KRY ile DY arasında öncüllük-ardıllık ilişkisi olduğu gibi tamamlayıcılık ilişkisi de bulunmaktadır.

Kurumsal dayanıklılık, kuruluşların krizlere ve belirsizliklere karşı dirençli olmasını sağlayan, sürekli gelişen ve adaptasyon gerektiren canlı bir süreçtir. Olay yönetimi, acil durum yönetimi, kriz yönetimi, felaket kurtarma yönetimi ve iş sürekliliği, bu süreç içerisinde aktif olarak yer alan operasyonel sürekliliği sağlayan araçlardır.

Şekil 13: KRY İle DY Arasında Öncüllük-Ardıllık ve Tamamlayıcılık İlişkisi

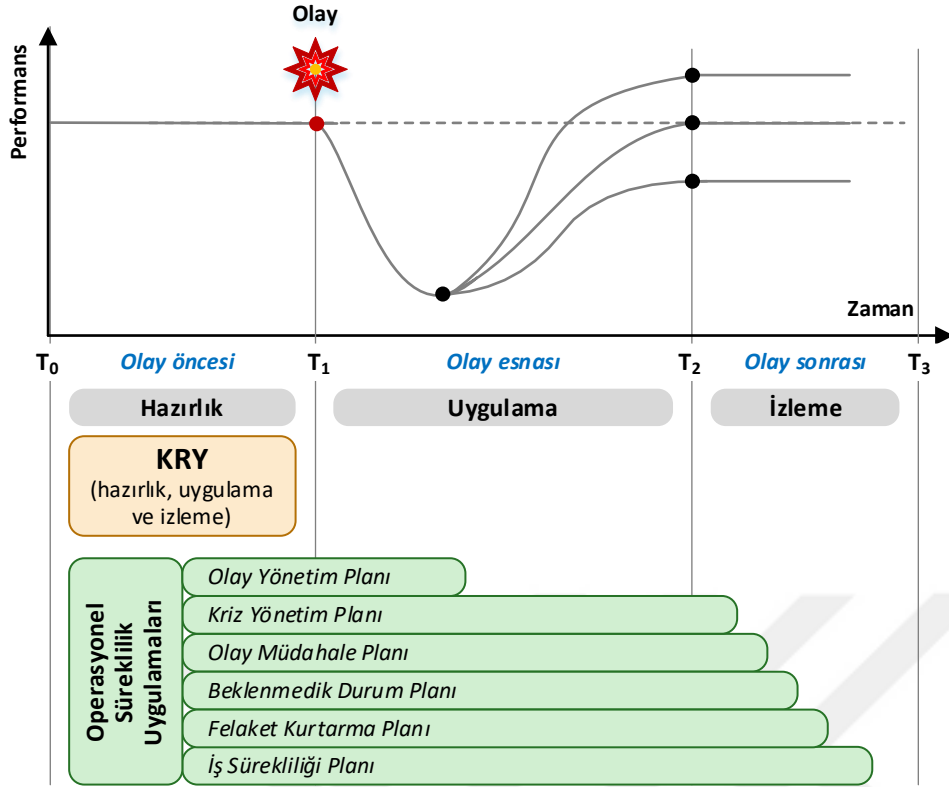


Söz konusu araçların olay öncesi, olay esnası (anı) ve sonrası süreçlerdeki hazırlık, uygulama ve izleme evreleri Şekil 14'te gösterilmektedir. Şekilde **Hata! Başvuru kaynağı bulunamadı.**görüldüğü üzere sürekliliğin sağlanmasına ilişkin dayanıklılık uygulamalarının tümüne ait hazırlık süreci olay öncesinde tamamlanmakta ve cevap verilmesini gerektirecek herhangi bir olayın gerçekleşmesi durumunda aktifleştirilmek üzere hazır olarak beklemektedir. Olay gerçekleştiğinde, olayın türü, kapsamı ve şiddeti gibi çeşitli kriterler vb. çerçevesinde yer verildiği aksiyon planı doğrultusunda işlerlik kazanmaktadır.

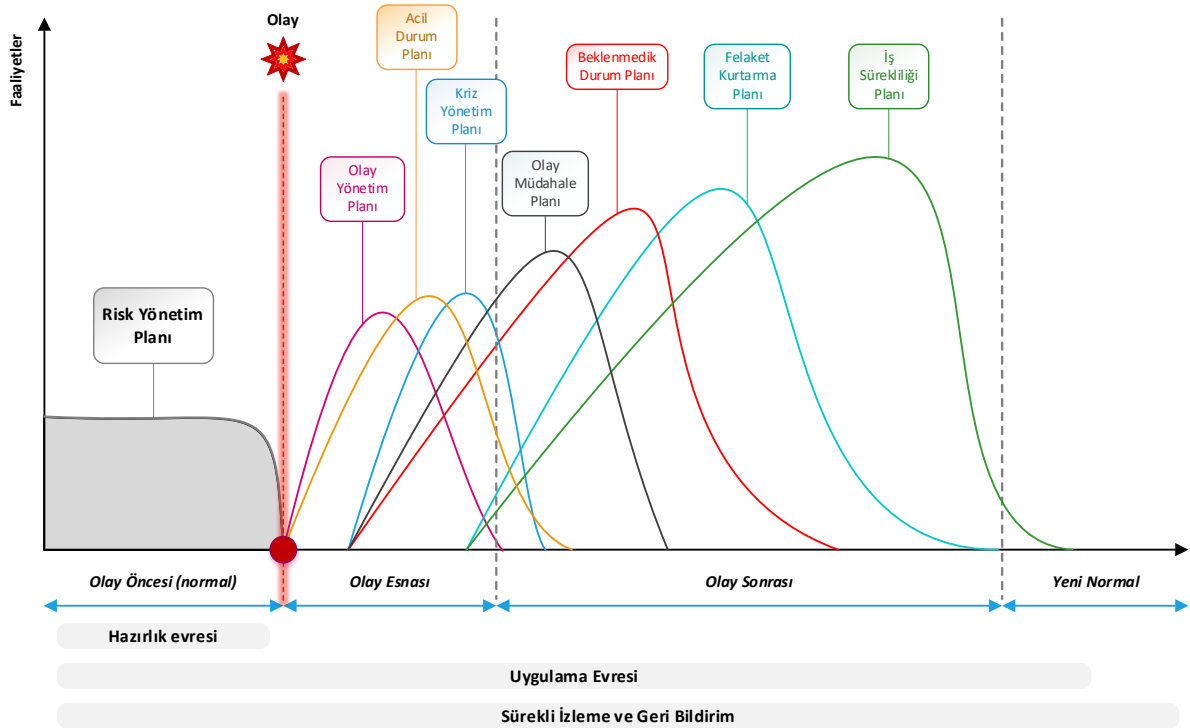
Diğer taraftan KRY, hazırlık, uygulama ve izleme aşamalarını olay öncesinde tamamlamakta ve sürekli geri bildirimlerle canlılığını korumaktadır. KRY tarafından alınan önlemler, olayın öncelikle gerçekleşmesini engellemek, bunun başarmaması durumunda ise olasılık ve etkisinin azaltılmasını amaçlamaktadır. Bu bakımdan KRY çalışmaları kurumsal kapasitenin gelişimine önemli katkılar sağlamaktadır.

KRY ile dayanıklılık uygulamaları arasındaki öncüllük-ardıllık ve tamamlayıcılık ilişkileri Şekil 15'te gösterilmektedir. Kurumsal Risk Yönetimi, dayanıklılık süreçlerini beslemekte ve anılan süreçlerin güncel ve canlı tutulmasına destek olma görevini üstlenmektedir. Dayanıklılık uygulamalarında ise olay gerçekleştiğinde, olayın niteliğine göre olay yönetim, kriz yönetim, acil durum, olay müdahale, beklenmedik durum, felaket kurtarma ve iş sürekliliği planlarından bir veya birkaçı aktifleşmekte ve söz konusu olaya yanıt verilmesi süreci başlatılmaktadır.

Şekil 14: Kurumsal Dayanıklılıkla İlişkili Uygulamaların Hazırlık, Uygulama ve İzleme Aşamalarının Gösterilmesi



Şekil 15: Dayanıklılıkla ilişkili Uygulamalar Arasındaki Öncüllük-Ardıllık ve Tamamlayıcılık İlişkileri



3.7.3. Strateji ve Uygulama Düzeyinde Entegrasyon

KRY, kaçınma, azaltma, transfer ve kabul etme gibi risk yanıt stratejileri ve seçilen stratejiye uygun eylemler geliştirerek riskleri kontrol altına almayı hedefler. DY, bu stratejileri hazırlık, modülerlik, çeşitlilik ve esneklik gibi kurumsal kapasitelere dönüştürerek kalıcı bir direnç geliştirir. Bu noktadan hareketle KRY'nin teknik ve sistematik analizlerinin, DY'nin kültürel ve yapısal dönüşüm mekanizmalarını beslediği söylenebilir.

3.7.4. Belirsizlik Türlerine Yaklaşımda Farklılaşma

Aleatorik belirsizliklerde kesin ya da tahmini yaklaşık bir etki-olasılık değerlendirmesi yapılabilmektedir. Bir aleatorik belirsizlik olarak riskler, KRY yaklaşımı çerçevesinde izlenmektedir. DY, bu belirsizlik türüne ek olarak ontolojik belirsizlikler gibi öngörülemeyen ve tanımsız tehditlerle baş edebilecek esneklik ve öğrenme kapasitesini kapsamaktadır. Ayrıca epistemik belirsizlikler de yine DY kapsamında ele alınmaktadır. Bu doğrultuda, DY, KRY'nin alanı dışındaki olumsuz durumlarla da ilgilenmekte ve KRY'yi tamamlamaktadır.

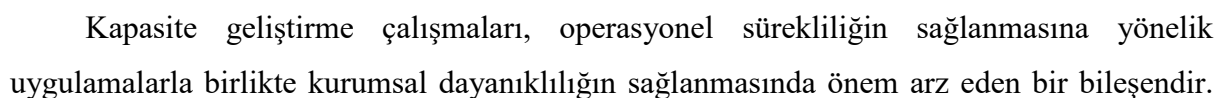
3.7.5. Araçların Kapsamlarında Farklılaşma

KRY, belirli ve yapılandırılmış patikayı izleyen genellikle teknik ve süreç bazlı bir araçtır. DY, organizasyonel kültür, liderlik, psikolojik dayanıklılık ve sosyal sermaye gibi insan odaklı öğeleri de kapsamakla birlikte yapılandırılmış ve belli bir kurala bağlı bir yaklaşım değildir. KRY süreçleri, DY'ye veri ve yapı sağlarken, DY kültürel dönüşüm ve davranışsal adaptasyonu güçlendirir.

3.7.6. Yapısal İlişkiler

Kurumsal risk yönetimi, risklerin tanımlanması sürecinde ortaya konulan tehditleri somutlaştırarak, etki ve olasılık değerlendirmelerini gerçekleştirir. Tehdidin önlenmesine yönelik bir kontrol faaliyetinin geliştirilememesi ya da kurumsal kabiliyetin bu kontrolü uygulamada yetersiz kalması gibi nedenlerden dolayı, kuruluş tehdidin gerçekleşme ihtimalini kabul eder. Bu noktadan sonra gerçekleşmesi durumunda tehdidin olumsuz etkilerine karşı koyma ve azaltma benzeri stratejilerle devam edilir. Bu çerçevede KRY, tehditler konusunda kurumsal dayanıklılık çalışmalarını besleyerek, tehditlerin dayanıklılık bağlamında değerlendirilmelerini mümkün kılar.

Şekil 16: KRY ve Kurumsal Dayanıklılık Arasındaki Etkileşimler



Olayın gerçekleşmesini müteakiben aktifleştirilen kurumsal dayanıklılık araçları vasıtasıyla olay yönetilmeye çalışılır.

Kuruluşun iş süreçlerinin normale dönmesiyle birlikte, yaşanan olaydan ve bu süreçte gerçekleştirilen eylemler, karşılaşılan sorunlar ve kazanılan tecrübe, dayanıklılık kapasitesinin geliştirilmesine geri bildirim sağlar. Artan kapasite hem kurumsal dayanıklılık süreçlerinin hem de kurumsal risk yönetiminin başarısını artırmaktadır. Diğer taraftan yaşanan tecrübeye yönelik riskin farklı bir perspektiften ele alınması ve tekrar gerçekleşmesinin önlenmesi açısından geri bildirim sağlar.

KRY kapsamında hayata geçirilen risk yanıtları, dayanıklılık kapasitesinin geliştirilmesine katkı sağlar. KRY kapsamında yürütülen izleme ve erken uyarı uygulamaları olası tehdit ve risk sinyalleri bakımından tehdit analizi ile KRY'ye bilgi sağlar.

Şemada, öğeleri KRY, kurumsal dayanıklılık uygulamaları ve dayanıklılık kapasitesi olan kapalı bir sistem gösterilmektedir. Bu sistemdeki bileşenler, birbirlerinin etkinliğini etkilemektedir. Ayrıca sistem sürekli öğrenen, gelişen ve adapte olan canlı bir yapıdır.

3.8. Teori ve Pratikteki Sınırlılıklar ve Yetersizlikler

KRY ve DY'nin uygulanmasında kuruluşlarda karşılaşılan zorluklara ilişkin literatürde yer verilen hususlar tezin birinci ve ikinci bölümlerinde detaylı olarak ele alınmıştır.

Söz konusu zorluklara ilave olarak, anılan araçların karşılaşılan olumsuz durum ve olayların, olay öncesi, anı ve sonrasını bir bütün halinde sürekli olacak şekilde yönetilmesi hususunda, müstakil olarak uygulandıklarında kapsam ve fonksiyon bağlamında çeşitli yetersizlik ve sınırlılıkları bulunmaktadır.

Bu çerçevede KRY'nin kapsam ve fonksiyon bakımından sınırlılıkları ve yetersizlikleri aşağıda kısaca özetlenmektedir.

- KRY çoğunlukla ölçülebilir ve hesaplanabilir risklere odaklanır; belirsizlik, tehdit ve ani şoklar ile karmaşık olay zincirleri gibi ölçülmesi zor ya da ölçülemeyen durumlar için etkin çözümler sunma kapasitesine sahip değildir.
- İtibar gibi maddi olmayan veya karmaşık risklerin ölçülmesindeki zorluklar ile mevcut analiz araçlarının bu konudaki sınırlılıkları, risk analizi sürecinin sağlamlık ve güvenilirliğini zayıflatmaktadır.

- KRY, olay öncesinde aktif olmakta ve rolü çoğunlukla risklerin önlenmesi ve azaltılması ile sınırlıdır. Sadece tanımlanabilen risklerin gerçekleşmesi durumunda gerçekleştirilecek eylemlerin yer aldığı ve olay öncesinde hazırlanması gereken beklenmedik durum planları genelde söz konusu değildir. Ancak, kurumlar, gerçekleşen olaydan sonra onarım, uyum ya da dönüşüm gibi toparlanma süreçlerini yönetmek durumundadır.
- KRY, her ne kadar silo-bazlı yaklaşımdan kaçınmış olsa da riskleri müstakil olarak ele alır; riskler arası etkileşimleri, zincirleme etkileri veya sistemsel kırılganlıkları yeterince dikkate almaz.
- KRY, genellikle statik çerçevelere dayanmakta ve hızlı değişen koşullara karşı yavaş tepki vermektedir.
- KRY çoğu zaman bir uyum ve kontrol mekanizması olarak görülmektedir. Oysa kurumların rekabet avantajı elde edebilmesi için risk yönetiminin değer yaratıcı işlevinin görünür olması gerekmektedir.
- Dijitalleşme, siber tehditler, küresel düzenlemeler ve ekonomik dalgalanmalar KRY süreçlerini karmaşıktırmakta; katı çerçeveler ve statik prosedürler yeni risk türlerini yakalamakta yetersiz kalmaktadır.
- Uzun vadeli değer yaratma ile kısa vadeli performans beklentisi arasındaki dengenin kurulması zordur.

Diğer taraftan, aşağıda değinildiği üzere DY'nin de kapsam ve fonksiyon bakımından çeşitli sınırlılıkları ve yetersizlikleri söz konusudur.

- Dayanıklılık farklı disiplinlerde farklı şekillerde tanımlandığından, kuruluş ya da sektör içinde ortak bir uygulama standardı oluşturmak güçtür. Bu durum, “nasıl ölçülür, nasıl yönetilir?” sorularına net yanıt verilmesini engellemektedir.
- Dayanıklılık kavramı çoğunlukla soyut ve çok boyutlu olup, KRY’de olduğu gibi sistematik bir metodoloji sunmaz. Pratikte farklı yorumlar söz konusu olmakta ve bu nedenle kuruluş içinde dağınık, parçalı ve operasyonel karşılığı zayıf kalmaktadır.
- DY, çoğunlukla operasyonel boyutta ele alınmakta olup, iş sürekliliği planları, kriz yönetimi faaliyetleri ve olay sonrası toparlanma gibi pratik süreçlere odaklanmaktadır. Ancak kurumların uzun vadeli stratejik kararlarında kritik olan risk–getiri dengesi (örneğin belirli bir belirsizliği, tehdidi ya da riski kabul etmenin

yaratacağı fırsat ya da maliyeti) yeterince dikkate alınmamaktadır. Dayanıklılık uygulamaları daha çok “kesintiden kurtulma” ile sınırlı kalırken, stratejik düzeyde değer yaratma kapasitesi sınırlı kalmaktadır.

- Dayanıklılık çoğu zaman “uzun vadeli sürdürülebilirlik” kavramı altında konumlanır, fakat kurumların kısa vadeli öncelikleri ve kaynak kısıtları nedeniyle uygulamada geri planda kalır.
- Dayanıklılık genellikle operasyonel krizlerden sonra gündeme gelir ve “toparlanma” ile sınırlandırılır; risk yönetimi süreçleriyle doğrudan bütünleşmediğinde proaktif bir değer yaratamaz.

Görüldüğü üzere KRY ve DY’nin kapsam ve fonksiyon bağlamında çeşitli yetersizlikleri söz konusudur. Bu nedenle, her iki yaklaşımın güçlü yanlarını bütünleştiren ve zayıflıklarını giderecek bir yapıya ihtiyaç duyulmaktadır.

3.9. DY Kapsamında Değerlendirilmesi Gereken Olumsuz Durumların Tespit Edilmesi

Risklerin belirlenmesini müteakiben gerçekleştirilen risk değerlendirme aşamasında, her bir riske nesnel ve ölçülebilir bir etki ve olasılık değeri atanır (Gregory, 2003). Risklerin etkin bir şekilde değerlendirilmesi, risk yanıtlarının belirlenmesi (Protiviti, 2006) ile bu riskler kritikse dayanıklılık kapsamında ele alınıp alınmayacağı hususlarının netleştirilmesi açısından önem arz etmektedir. Kuruluşun iş yaptığı ortam ve koşulların sürekli değişim içinde olmasına bağlı olarak risk değerlendirmesi de süreklilik arz eden bir süreçtir (Barton vd., 2002).

Riskler, olasılık ve etki değerlendirmelerine dayalı olarak risk matrisi üzerinde sıralanır (Hardy, 2015). Matris üzerinde riskin konumlandığı nokta riskin şiddetini (etki x olasılık) gösterir. Riskler etki ve olasılık değerleri kullanılarak önceliklendirilir. Öncelikli olarak kabul edilen risklere yönelik yanıt strateji ve kontrolleri geliştirilir. Amaç, kontroller aracılığıyla etki ve/veya olasılık değerlerinin mümkün olduğunca düşürülmesidir.

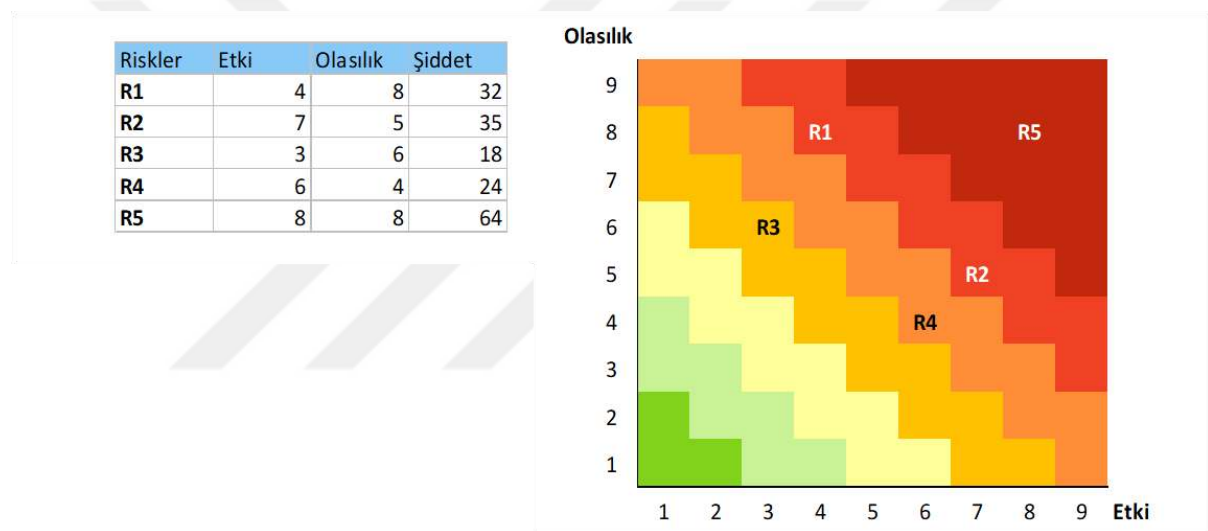
Risklerin dayanıklılık kapsamında önceliklendirilmesi amacıyla riskin kalıntı etki değerleri esas alınır. Kontrollere rağmen etki değerleri arzu edilen seviyeye indirilemeyen riskler için olası gerçekleştirmelere yönelik dayanıklılığın sağlanması çalışmaları devreye girer. Etkisi bakımından makul seviyede kontrol altına alınabilen riskler için KRY süreci yeterlidir,

kaynakların optimal kullanımı açısından söz konusu riskler için ilave olarak dayanıklılık kapasitesi gerçekleştirilmesine ihtiyaç yoktur.

Aşağıda risklerin etki ve olasılık değerleri çerçevesinde konumlandırıldığı bir risk matrisi (**Hata! Başvuru kaynağı bulunamadı.**) örnek olarak verilmektedir. Matrisin sağ üst köşesine y aklaştıkça risklerin şiddeti artmaktadır. Bu doğrultuda Risk 1, Risk 2 ve Risk 5 için risk yanıt strateji ve kontrolleri geliştirilirken, Risk 2, Risk 4 ve Risk 5 dayanıklılık yönetimi kapsamında değerlendirilmeli ve olay öncesi, sonrası uygun kontrol ve faaliyetler tanımlanmalıdır.

Öte yandan, etkisi düşük olsa dahi riskler ikincil ya da zincirleme riskleri tetikleme ya da yaratma potansiyeli, stratejik hedefler üzerindeki etkisi gibi açılardan değerlendirilmelidir.

Şekil 17: Örnek Risk Matrisi



Dayanıklılık kapsamına alınması gereken risklerle birlikte tehditler için kriter olarak sadece (1) etki belirleyici değildir. Tehdit ve riskler, ilave olarak (2) yayılma etkisi, (3) kurtarma zorluğu, (4) kurumsal zayıf noktaları etkileme durumu, (5) itibar üzerindeki etkisi, (6) olayın gerçekleşmesini müteakip hızlı bir şekilde karşılık verilmesi gerekliliği, (7) düzenlemelere yönelik uyum üzerindeki etkisi, (8) riskin, dışa bağımlılık üzerindeki etkisi, (9) ikincil ya da zincirleme risk yaratma potansiyeli ve (10) stratejik etki yaratma potansiyeli gibi kriterlerden birkaçı ya da tamamı aracılığıyla bir kez daha ele alınmalıdır.

Yayılma (dalgalanma) etkisi, “olumsuz durumların diğer süreçler ve paydaşlar üzerindeki domino etkisi” olarak tanımlanabilir. Duong vd. (2024) çalışmalarında bu etkiyi, dışsal kaynaklı risklerin içsel kaynaklı risklerin ortaya çıkmasına neden olması şeklinde

tanımlamaktadır. Yayılma etkisi, zincirleme ya da sistemik risklerin oluşmasına neden olabilir. Kaufman (1995), sistemik riski “başlangıçtaki bir olayın, bir sistem içindeki birbirine bağlı kurumlar veya piyasalar üzerinde bir dizi zararı tetikleme olasılığı” şeklinde ifade etmektedir (Akt. Pacelli, 2025).

Sistemdeki tek bir olay, dalgalanma etkisiyle birden fazla sonuç doğurabilir, bu sonuçların olumsuz etkilerini artırabilir ya da daha şiddetli bir noktaya tırmanabilir (Green, 2016). Örneğin, enerji kesintisi üretimin durmasına, bu durum da teslimatın gecikmesine neden olabilir ya da tedarikçinin iflas etmesi sonucunda üretim durabilir ve bunun sonucunda müşteri kaybı yaşanabilir.

Kurtarma zorluğu, tehdit ya da riskin gerçekleşmesiyle meydana gelen olumsuzluğun giderilerek, kuruluşun yeniden normale dönmesi sürecindeki işgücü ve zaman gereksinimi ile kurtarmanın maliyeti gibi nedenlerden ötürü sürecin zorluğunu belirtmektedir. Çera vd. (2023), kuruluşun büyüklüğü, faaliyet gösterdiği sektör ve alan, coğrafi konumu gibi faktörlerin kurtarma süreci üzerinde etkili olduğunu ifade etmektedir.

Chang vd. (2022) yaşanan bir afet sonrasında çalışan ve parasal hareketlilik bakımından küçük, tedarik zinciri sorunlarına açık, pazar sorunu yaşayan ya da ağır zarar görmüş lokasyonlarda hizmet veren yerel kuruluşlarda toparlanmanın zor olduğunu belirtmektedir. Yaşanan bir deprem sonrasında iş göremez hale gelen fabrikanın yeniden inşa edilmesi aylarca, belki de yıllarca sürebilmesi durumu kurtarma zorluğuna yönelik bir örnektir. Benzer şekilde makroekonomik krizleri müteakiben kuruluşların finansal açıdan toparlanma süreci uzun ve maliyetli olabilir.

Kuruluşun kırılganlıkları ve zayıf yönleri üzerinde etkili olan olumsuz durumlara yönelik dayanıklılık geliştirilmelidir. Dayanıklılık, bir koruyucu strateji olarak “sistemin, tehdit ve risklerin olumsuz sonuçlarına karşı kırılganlıklarının azaltılması ve sistemin güçlendirilmesi” rolünü üstlenir (Aven & Renn, 2010). Kuruluşun olumsuz durumlardan hangilerinin hangi zafiyet noktalarını etkilediğini tespit etmek üzere, kırılganlık analizleri gerçekleştirilebilir. Kırılganlık analizi, söz konusu durumların nedenlerini belirlemeye, bunları öncelik sırasına koymaya ve uygun yönetim araç ve yöntemleriyle dayanıklılığın nasıl artırılabileceğini veya kırılganlık ve zayıf yönlerin nasıl azaltılabileceğini belirlemeye yardımcı olur (Haddow vd., 2021). Analiz sonucunda elde edilen kırılganlıklar, üzerinde çalışılması amacıyla KRY tarafından ele alınır.

Gerçekleşmesi halinde kuruluşun itibarını olumsuz etkileme potansiyeli, olumsuz durumların dayanıklılık kapsamına alınması açısından önemli bir kriterdir. Kurumsal itibar, “bir kuruluşun zaman içinde paydaşlar tarafından genel olarak değerlendirilmesi, onların deneyimleri, iletişimleri, sembolleri ve rakiplerle karşılaştırmaları sonucu oluşan algı” olarak tanımlanmaktadır (Gotsi & Wilson, 2001). Bu bağlamda risk ve tehditlerin yanlış yönetilmesi, kuruluşun itibarının zedelenmesine ve bazı durumlarda işletmenin yok olmasına sebep olabilmektedir (Barton vd., 2002).

Zaman baskısı, risk ve tehditlerin gerçekleştiğinde müdahale için kalan zaman ve müdahalenin aciliyetini ifade etmektedir. Kuruluşlar, kimi tehdit ve risklere, gerçekleştirmelerine müteakip hızlı bir şekilde karşılık vermek durumundadırlar. Siber saldırılara vakit kaybetmeksizin müdahale edilmesi gerekliliği, riskin yarattığı zaman baskısına bir örnektir. Bu tür acil yanıt gerektiren riskler, dayanıklılık kapsamına alınmalıdır.

Uyumluluk etkisi, bir olumsuz durumun gerçekleşmesi sonucunda kuruluşun düzenleyici uyumluluk yükümlülüklerinin ihlal edilmesi ya da uyum durumunun zedelenmesini ifade etmektedir. Uyumluluk, “iş süreçlerinin, operasyonların ve uygulamaların öngörülen ve/veya kabul edilen bir dizi normla uyumlu olmasını sağlamak” şeklinde tanımlanmaktadır (Sadiq & Governatori, 2010). Risk ve tehditlerin gerçekleştirmeleri halinde kuruluşun yasa ve düzenlemelere uyumuna ilişkin olumsuz sonuçlar doğurması, bir riski ya da tehdidi yaratma ya da tetikleme durumu bir başka kriterdir.

Uyumluluk etkisine örnek olarak, bilgi işlem altyapısında yaşanacak bir kesinti nedeniyle, ilgili düzenlemelere uygun bir şekilde zamanında finansal raporlama yapılamaması ve sonucunda uyum kurallarının ihlal edilmesi verilebilir.

Dışa bağımlılık etkisi, bir olumsuz durumun gerçekleşmesi sonucunda kuruluşun dışsal unsurlara olan bağımlılığının oluşması ya da var olan bağımlılığını artırması durumunu belirtmektedir. Dışa bağımlılık, kuruluşların temel faaliyetlerini devam ettirebilmesi için dışsal sistem, kaynak, tedarikçi, altyapılara ve hizmet sağlayıcılara olan bağımlılık durumudur. Bağımlılığın artması, kuruluş açısından yeni kırılganlık alanlarının doğmasına neden olacaktır.

Kuruluşun ana veri merkezinin çökmesi sonucunda, bulut hizmet sağlayıcılarına olan bağımlılığı artar. Bu durumda söz konusu sağlayıcılarda meydana gelebilecek herhangi bir olumsuzluk doğrudan kuruluşu etkileyecektir.

İkincil risk yaratma potansiyeli, bir riskin gerçekleşmesi sonucunda ikincil ya da zincirleme risklerin meydana gelmesi durumunu ifade etmektedir. İkincil riskler, birincil

risklere verilen yanıtlardan kaynaklanan ya da birincil risklerin gerçekleşmesine bağlı olarak meydana gelen risklerdir (Cooper vd., 2005). Örneğin, kuruluşun bilgi sistemlerinde yaşanacak bir siber saldırı sonucunda müşterilere ait kimlik ve ödeme bilgilerinin açık edilmesi, kuruluşun itibarını etkilemekle birlikte kişisel verilerin korunması açısından ilgili düzenlemelerin ihlal edilmesi kuruluşu cezai yaptırımlara maruz bırakacaktır.

İkincil ya da zincirleme risk yaratma potansiyeli, PMI (2018) tarafından proje risklerinin, yanıt verilmek üzere önceliklendirilmesi amacıyla sunduğu bağlantılılık kriteri ile benzeşmektedir. Bağlantılılık kriteri, “bir riskin diğer riskle olan ilişkisi düzeyini” ifade etmekte olup, bu düzey arttıkça bağlantılılık artacaktır. Dayanıklılık kapsamında değerlendirildiğinde ise bağlantılılık arttıkça riskin gerçekleşmesi durumuna yönelik dayanıklılığın da artırılması değerlendirilmelidir.

PMI (2018) tarafından proje risklerinin, yanıt verilmek üzere önceliklendirilmesi amacıyla bir başka kriter olarak sunduğu stratejik etkinin, dayanıklılık gerektiren risklerin belirlenmesi amacıyla kullanılabileceği değerlendirilmektedir. Stratejik etki, bir riskin kuruluşun stratejik amaç ve hedefleri üzerindeki etki potansiyeli olarak tanımlanmaktadır (PMI, 2018). Riskin, gerçekleşmesi halinde stratejik amaç ve hedefleri üzerindeki olumsuz etkisinin yüksek olması dayanıklılık gereksinimi de artırmaktadır.

Olumsuz durumların, DY kapsamına alınıp alınmayacağının belirlenmesi amacıyla bahse konu kriterlerden oluşan bir kontrol listesi kullanılabilir. Kontrol listeleri, “hiçbir adımın unutulmamasını sağlamak üzere tamamlanması gereken öğelerin veya eylemlerin bir listesi” şeklinde sistematik ve pratik bir denetim aracıdır (Alspach, 2017). Olumsuz durumlara yönelik olarak on kriterden oluşan bir kontrol listesi Tablo 9’da sunulmaktadır. Listedeki sorular, dayanıklılıkla ilişkili olumsuz durumların tespiti, önceliklendirilmesi ve uygun stratejilerle yönetilmesi açısından işlevsel bir çerçeve sunmaktadır.

Tablo 9: Olumsuz Durumların DY Kapsamında Değerlendirilmesine Yönelik Soru Listesi

#	Kriter	Sorular	Değerlendirme
1	Etki Büyüklüğü	Olumsuz durum gerçekleştiğinde kurum üzerinde yaratacağı etki ne büyüklüktedir?	(Düşük / Orta / Yüksek)
2	Yayılma Etkisi	Riskin diğer süreçler, paydaşlar veya sistemler üzerinde domino etkisi var mı?	(Evet / Hayır)
3	Kurtarma Zorluğu	Olumsuz durum gerçekleştiğinde toparlanma süreci ne kadar zor ve maliyetlidir?	(1, 2, 3, 4, 5)
4	Kurumsal Zayıflık	Olumsuz durum, kurumun mevcut zayıf noktalarını etkiliyor mu veya yeni zayıflık yaratıyor mu?	
5	İtibari Etki	Olumsuz durumun kurumsal itibara zarar verme potansiyeli nedir?	
6	Zaman Baskısı	Olumsuz durum gerçekleştiğinde hızlı müdahale gerektiriyor mu?	
7	Düzenlemelere Uyum Etkisi	Olumsuz durumun gerçekleşmesi, düzenleyici uyum yükümlülüklerini ihlal eder mi?	
8	Dışa Bağımlılık	Olumsuz durum gerçekleştiğinde dışa bağımlılığı artırır mı veya yeni dışa bağımlılıklar yaratır mı?	
9	İkincil Risk Yaratma Potansiyeli	Riskin gerçekleşmesi, başka risklerin ortaya çıkmasına yol açar mı?	
10	Stratejik Etki	Olumsuz durum kurumun stratejik hedeflerine zarar verir mi? Stratejik planları sekteye uğratar mı?	

DÖRDÜNCÜ BÖLÜM

RİSK, TEHDİT VE BELİRSİZLİKLERE KARŞI DAYANIKLILIĞI

GÜÇLENDİRME STRATEJİLERİ

4.1. Dayanıklılık Stratejisi

Strateji, “bir kuruluşun uzun vadeli yönünü belirleyen, temel faaliyetlerini yönlendiren ve koordine eden kararlar dizisi” olarak tanımlanmaktadır (Aliekperov, 2021). Kavram, bir kuruluşun hedeflerini ve bu hedeflere ulaşmak için alınacak önlemleri belirlemesi ile söz konusu önlemlerin uygulanması amacıyla sınırlı kaynakların seferber edilmesini kapsar (Barad, 2018).

Başka bir ifadeyle stratejiler, kuruluşların belirsizlik, tehdit, risk ve krizler karşısında nasıl hareket edeceklerinin belirlenmesi amacıyla geliştirilen yol haritalarıdır. Stratejilerin uygulanması, yönetsel kararlar verilmesini gerektirmektedir. Amaç, rekabette avantaj elde edilmesi ve katma değer sağlanmasıdır.

Devinney ve Dowling (2020), strateji kavramını kuruluşların uzun vadeli yönlerini belirleyen kararların bütünü olarak ifade etmektedir. Stratejiler, bir seferde uygulanan ve biten bir yöntem ya da eylem değil, geçerli olduğu müddetçe süreklilik arz eden unsurlardır. Kararlaştırılan strateji çerçevesinde yeni kararlar alınması, uygulanması, gözden geçirilmesi ve güncellenmesi söz konusu olabilmektedir.

Bir ifadenin strateji sayılabilmesi için, bu yönelim doğrultusunda özgün kaynak tahsisi veya yetenek geliştirme ihtiyacı doğurması gerekmektedir (Prahâlâd & Hamel, 1990). İlave olarak stratejiler, somut ve uygulamaya yönelik olmakla birlikte seçicidir, ilgili alternatifler içerisinde en kritik ve önemli olanı seçer. Ayrıca kuruluşların iş yapma biçimleri üzerinde etkilidir. Stratejiler, kuruluşlara geleceklerini şekillendirmeleri bakımından yön tayin eder.

Diğer taraftan, Teece vd.’nin (1997) çalışmasında strateji kavramına ilişkin özellik ve gerekliliklere yönelik aşağıdaki hususlara değinilmektedir.

- Strateji, kaynaklara sahip olmanın yanında, bu kaynakların nasıl yapılandırılacağı ve dağıtılacağıyla ilgilidir.

- Strateji belirsizlik, hızlı deęişim ve dönüşüm ortamında rekabet açısından avantaj yaratmaya odaklı olmalıdır.
- Strateji, bir örgütün benzersiz kaynaklarının ve yeteneklerinin üzerine inşa edilmelidir.

Dayanıklılık stratejileri, kuruluşların karşılaşılabileceęi olumsuz durumlara karşı hazırlıklı olmaları, olaylar gerçekleştiğinde hızlı bir şekilde eski hallerine dönmeleri, yeni duruma uyum sağlamaları ya da başka bir yapıya, duruma dönüşmeleri amacıyla hazırlanan ve hayata geçirilen plan, yöntem ve uygulamaları kapsamaktadır. Dayanıklılık stratejileri, Uluslararası Risk Yönetişimi Konseyi (IRGC) tarafından, risklerin etkilerinin belirsiz olduęu durumlar ile kesintiyle sonuçlanabilecek potansiyel durumlarda gereksinim duyulan stratejiler olarak tanımlanmaktadır (Florin & Linkov, 2016). Olay öncesi, anı ve sonrası olmak üzere tüm aşamalarda uygulanmak amacıyla çeşitli dayanıklılık stratejileri bulunmaktadır. Bu stratejiler, kuruluşların iç ve dış faktörlerden kaynaklanan olumsuz etkilerin bertaraf edilmesine yönelik güçlü ve esnek bir yapıya sahip olmalarına odaklanmaktadır. Bu yolla, kuruluşlar kısa vadeli şok ve olumsuzluklara en az düzeyde maruz kalarak, sürekliliklerini sağlayabilirler.

Dayanıklılık stratejilerinin öncelikli amaçları, olumsuz etkilere maruziyet ile kırılganlık ve zayıflıkların azaltılmasıdır (Florin, 2016). Bu doğrultuda dayanıklılık stratejileri, karar vericilerin olası tehditlerden kaynaklanabilecek olumsuz etkilerin şiddet ve süresini en az maliyetle azaltabilecek seçimler yapabilmelerini hedefler (Trump vd. 2018). Yanı sıra, dayanıklılık stratejileri, kuruluşların karşılaştıkları krizleri aşabilmelerinde önemli bir rol üstlenmektedir (Kokkranikal vd., 2024).

Literatürde dayanıklılık stratejileri konusu, tedarik zinciri, sağlık sektörü, kurumsal yönetim ve yükseköğretim gibi çeşitli alanlar bazında ele alınmaktadır. Dayanıklılık stratejileri, tedarik zinciri yönetimine ilave olarak, müşteri ilişkileri yönetimi, bilgi yönetimi, İK yönetimi, bütçeleme ve yeni ürün geliştirilmesini kapsayacak şekilde kuruluşun işlevleri açısından önem arz etmektedir (Florin & Linkov, 2016). IRGC, belirsizlik içeren sistemik ve ani ortaya çıkan riskler için dayanıklılık stratejileri geliştirilmesini önermektedir (Florin, 2016).

Dayanıklılık stratejileri, farklı durumlara göre deęişkenlik gösterebilir. Dayanıklılık stratejileri, zaman çizgisi üzerinde olayın gerçekleştięi noktaya göre konumlandıkları yer doğrultusunda literatürde genellikle aktif ve pasif stratejiler, *proaktif* ve *reaktif* stratejiler ile durumsal stratejiler olarak sınıflandırılmaktadır.

Aktif stratejiler, proaktif ve reaktif stratejileri kapsamaktadır. Proaktif stratejiler, olay henüz gerçekleşmeden önceki aşamada karşılaşılan olumsuz durumu kontrol altına almayı amaçlamaktadır. Bu stratejiler, uygun önlemlerin alınarak olumsuz durumun önlenmesine odaklanırlar (Wieland & Wallenburg, 2013). Önleyici ve hazırlık odaklı stratejilerdir. Kurumun çeşitli kriz senaryoları üzerine tatbikat yapması ve eylem planları oluşturması ile tedarik zincirinde gecikmeler ya da siber saldırılar için otomatik izleme yazılımları ve erken uyarı sistemlerinin oluşturulması proaktif stratejilerdir.

Reaktif stratejiler, olayın gerçekleşmesini müteakiben verilecek yanıt eylemler üzerinde durmaktadır (Lengnick-Hall & Beck, 2005). Bu stratejiler, olay anında ve hemen sonrasında devreye girer. Sorun ortaya çıktıktan sonra hasarın azaltılması ve toparlanmasının sağlanması amacıyla kullanılırlar. Reaktif yaklaşımlar, olumsuz etkileri en aza indirmek üzere hızlı bir şekilde yanıt verilmesini gerektirmektedir (Jum'a vd., 2024). Kriz anında fiziksel ve dijital müdahale amacıyla acil durum kurtarma ekiplerinin görevlendirilmesi ile olay sonrası kritik süreçlerin alternatif yollarla yürütülmesi amacıyla iş sürekliliği planlarının uygulanması reaktif stratejilerdir.

Pasif stratejiler, olay öncesinde sistemin hâlihazırdaki yapısal dayanıklılığı ve kapasitesini ifade eden, önceden yerleştirilmiş koruyucu önlemlerdir. Belirsiz ve öngörülemeyen olumsuzluklara karşı genel dayanıklılık yoluyla koruma sağlanır. Olay öncesinde hayata geçirilmelerine istinaden olay anında etkin konumdadırlar. Pasif stratejiler, etkinin absorbe edilmesine odaklanırlar. Örneğin, talep dalgalanmalarında üretimin aksamaması için fazladan stok (buffer) bulundurulması, pasif bir dayanıklılık stratejisidir.

Söz konusu türlere ilaveten, proje yönetimindeki beklenmedik olaylara yönelik uygulanan durumsal stratejiden (“etrafından dolanma” stratejisi) hareketle, beklenmedik olumsuz bir durumun gerçekleşmesi halinde doğaçlama ve anlık çözümlerin uygulandığı bir *durumsal* strateji de dayanıklılık stratejisi olarak değerlendirilebilir.

Durumsal stratejiler, olayın kaynağının belirsizlik ya da cehalet kaynaklı olduğu; olaylara verilen yanıtların çevik, emprovize, dinamik ve bağlamsal olduğu stratejilerdir. Olay anında, mevcut planların yetersiz kaldığı belirsiz durumlarda uygulanırlar. Yüksek belirsizlikte anlık karar verilmesi ve hareket edilmesi söz konusudur. COVID-19 gibi öngörülemeyen bir pandemide hızlı dijital dönüşüm sağlanarak evden çalışma altyapısının birkaç gün içinde kurulması ve kriz anında kurum dışından uzmanlarla doğrudan iş birliği yaparak yeni çözümler geliştirilmesi durumsal stratejilere örnek olarak verilebilir.

4.2. Literatür Analizi

Literatürde dayanıklılık stratejisi ifadesinin formal anlamıyla kullanıldığı ve bu stratejilerin açıklandığı sınırlı sayıda çalışma bulunmaktadır. Bu başlık altında bahse konu stratejiler araştırılarak, ortak bir zeminde toplulaştırılması yoluyla kurumsal dayanıklılığın sağlanmasına yönelik jenerik stratejilerin belirlenmesi hedeflenmektedir.

Literatür analizi ile birlikte “Risklerle birlikte tehdit ve belirsizliklere karşı dayanıklılığın güçlendirilmesine yönelik mevcut strateji ve araçlar nelerdir? DY’ye yönelik strateji ve araçlar, KRY çalışmalarına nasıl dâhil edilebilir?” şeklindeki üçüncü araştırma sorusunun yanıtı aranacaktır.

4.2.1. Akademik Çalışmalar

Kurumların krizler, kesintiler ve belirsizlik karşısında ayakta kalabilmeleri, izledikleri dayanıklılık stratejilerinin türü ve kapsamına bağlıdır. Literatürde, kurumsal dayanıklılığı artırmak amacıyla geliştirilen stratejiler oldukça çeşitlidir. Bu stratejiler; operasyonel ve yapısal yaklaşımlardan kültürel ve yönetsel müdahalelere, bireysel girişimcilik hamlelerinden dijital ve teknolojik uygulamalara kadar geniş bir yelpazeye yayılmaktadır.

Gibson ve Tarrant (2010) tarafından rutin olmayan ve iş sürekliliğinde kesintiye neden olan risklerin yönetilmesine ilişkin bir model geliştirilmesi amacıyla yaptıkları çalışmada direnç, güvenilirlik, yedeklilik ve esneklik olmak üzere 4 temel dayanıklılık stratejisine yer vermektedirler.

Lee vd. (2013), kuruluşların güçlü ve zayıf yönlerini belirlemek, dayanıklılık stratejilerinin ve yatırımlarının etkinliğini geliştirmek ve ölçmek üzere kullanabilecekleri bir anket aracı geliştirmek amacıyla gerçekleştirdikleri çalışmada dayanıklılık stratejileri öngörü, izleme, tepki, öğrenme, sağlamlık olarak açıklanmaktadır.

Erkip vd. (2014), ülkemizde perakende sektörü tarafından kullanılan ana dayanıklılık stratejilerinin ürün bazında uzmanlaşmanın sağlanması, hijyen ve ilgili standardizasyonun artırılması, promosyon ve indirim kampanyalarının yapılması ile çalışma saatlerinin uzun olması ile eve teslim hizmeti olduğunu aktarmaktadır.

Hatton vd. (2018), sektörel dayanıklılık stratejileri ile yatırımlarının etkinliğini geliştirmek ve değerlendirmek amacıyla bir model ve ölçüm aracı geliştirmeyi amaçladıkları

alışmalarında kurumsal dayanıklılık konusunda literatürü taramışlardır. Yazarlar, tarama kapsamında literatürde yer verilen dayanıklılık stratejilerini strateji ve planlama, liderlik ve kültür, kaynakların kullanılabilirliği ile ağlar ve ilişkiler olarak belirtmektedir.

Granig ve Hilgarter (2020), tarafından kuruluşların iş modelleri üzerinde etkili olan yeni gelişme ve eğilimlerden kaynaklı zorluklarla nasıl başa çıktıklarını araştırdıkları çalışmada proaktif ve reaktif dayanıklılık stratejileri ele alınmaktadır. Proaktif dayanıklılık, trendlerden kaynaklanan etkilerin öncesinde tahmin edilmesi, hazırlık yapılması ve paydaşlarla iletişim halinde kalarak iş modellerinin şekillendirilmesi ve bu yolla uyum sağlanmasını ifade etmektedir. Reaktif dayanıklılık ise olumsuz durumun gerçekleşmesini müteakiben olaya yanıt verilmesine odaklanmaktadır.

Melián-Alzola vd. (2020), yakın zamandaki COVID-19 pandemisinde de görüldüğü üzere yaşanan kırılganlıkların azaltılması amacıyla otellerin dayanıklılıklarını inceleyerek kurumsal dayanıklılığın ölçülmesine yönelik bir model önermişlerdir. Yazarlar, dayanıklılığın sağlanmasında liderlik ve kültür stratejileri ile iç ve dış paydaşlarla kurulan ağ ve ilişkiler, yeniliklere açıklık, durumsal farkındalık, çeşitli senaryo ve stres testlerinin yapılması, finansal, insan ve operasyonel kaynakların erişilebilir olması ve gerektiğinde yeniden tahsis edilebilmesi stratejilerine değinmektedir.

Folake (2021), uzun yıllar faaliyet göstermiş kuruluşların şoklara karşı dayanıklılıklarını artırmak için benimsedikleri stratejileri dört tema altında incelemiştir. Çevik ve uyarlanabilir kültür temasında inovasyon, deneme, karar yetkisi ve belirsizliği benimseme; teknoloji ve inovasyona yatırım temasında teknoloji ortaklıkları, Ar-Ge ve yeni teknolojilerin benimsenmesi, eğitim stratejilerine yer verilmektedir. Finansal planlama ve yönetim temasında kaynak çeşitlendirme, acil durum fonları ve bütçe planlaması yer alırken, hazırlık ve planlama temasında ise afet müdahale planları, altyapı yatırımları ve yerel iş birlikleri stratejilerine yer verilmiştir.

Baghersad ve Zobel (2022), kuruluşların kesintilere karşı dayanıklılık performanslarının değerlendirilmesi amacıyla gerçekleştirdikleri çalışmada kurumsal dayanıklılığı artırmak amacıyla operasyonel bolluk ve kapsam stratejilerini ele almaktadır. Yazarlar, operasyonel bolluk kavramını kuruluşun, gerçekleşen olumsuz olayların etkisinin absorbe edilmesini desteklemek amacıyla kuruluşun hazırda beklettiği ilave kaynaklar olarak tanımlamaktadır. Operasyonel kapsam, kuruluşun faaliyet alanı ile faaliyet gösterdiği coğrafi konumların genişliği ile ilgilidir.

Sinniah vd. (2022), organizasyonel dayanıklılığın operasyonel performansı ne ölçüde etkilediğini belirlemek ve firma büyüklüğünün organizasyonel dayanıklılık ile operasyonel performans arasındaki ilişkiye nasıl etki ettiğini tespit etmeyi amaçladığı çalışmada çeşitli dayanıklılık stratejilerinden bahsetmektedir. Söz konusu stratejiler arasında nakit akışının güçlendirilmesi, alternatif tedarik zinciri patikalarının kullanılması, dijital dönüşüm, ürün ve pazar çeşitlendirme, çalışan eğitimi ve bağlılığı, senaryo planlama ile esnek organizasyon yapısı gibi dayanıklılık stratejileri yer almaktadır.

Sadeqi-Arani ve Ghahfarokhi (2022), COVID-19 pandemisi krizinde spor işletmelerinin karşılaştığı zorlukları değerlendirmek ve dayanıklılık çözümlerini tanıtmak amacıyla gerçekleştirdikleri çalışmalarında COVID ve COVID sonrası dönemler için pazarlama, süreç yönetimi, organizasyonel kaynak yönetimi ve stratejik eylem yönetimi olmak üzere dört kategoride 94 spor işletmeciliği dayanıklılık stratejisi belirlenmiştir. Bu operasyonel stratejiler, stratejik planlama ve kriz yönetimi, organizasyonel kültür ve liderlik, finansal esneklik ve kaynak yönetimi, dijital dönüşüm ve pazara uyumla ilgili stratejiler şeklinde gruplanmıştır.

Pertheban vd.'nin (2023) çalışmasında yedeklilik, esneklik, çeviklik, iş birliği ve bilgi alışverişi gibi stratejilerin uygulanması yoluyla kuruluşların dayanıklılıklarını artırdıklarını ve performanslarını sürdürebildikleri ifade edilmektedir.

Richardson (2023), kurumsal dayanıklılığın güçlendirilmesini teminen ihtiyaç duyulan stratejileri finansal bağlamda çeviklik, adaptif tedarik zincirleri, stratejik teknolojilerin edinilmesi ve kullanılması ile proaktif risk yönetimi olarak ifade etmektedirler.

Förster vd. (2023), krizin süresi ve şiddetine göre kabullenme dayanıklılığı ve stratejik dayanıklılık olmak üzere iki farklı dayanıklılık stratejisi belirlemiştir. Kabul dayanıklılığı, kısa süreli, kaynakları koruyan, kısa ve küçük krizlere uygun, dayanıklılık ve enerji tasarrufuna odaklanan bir yaklaşımdır. Buna karşılık stratejik dayanıklılık, şiddetli veya uzun süreli olumsuzluklara uyum sağlamak ve dönüşüm gerçekleştirmek amacıyla uygulanan, kaynakları artıran uzun vadeli bir stratejidir. Yazarlar, liderlerin stratejilerini, krizin süresine göre uyarlama ve koşulların değişmesine bağlı olarak değiştirme gerekliliklerini vurgulamaktadır.

Pescaroli vd. (2023), acil durum yönetimi, kurumsal dayanıklılık ve iklim değişikliğine uyum konularını bir araya getirerek kentsel sistemlerdeki büyük riskleri yönetmek üzere yeni bir yaklaşımın önerilmesi amacıyla gerçekleştirdikleri çalışmada kurumsal dayanıklılığın sağlanmasına yönelik stratejilere yer verilmektedir. Bahse konu stratejiler sistemik risk yönetimi, kurumsal tepki verebilirlik, öngörülü yönetim, dayanıklılığın örgütsel karar alma

süreçlerine dâhil edilmesi, kurumsal öğrenme ve uyum yeteneğinin teşvik edilmesi, yedeklilik ve esnekliğin oluşturulması ile farklı yönetim düzeyleri ve sektörler arasında iş birliği ve koordinasyon olarak belirtilmektedir.

Valbuena vd. (2023), COVID pandemisi döneminde Kolombiya'nın başkenti Bogotá'daki işletmelerde izlenen dayanıklılık stratejilerini araştırmışlardır. Yazarlar, anılan işletmelerin beklenmedik durumlara karşı hızlı yanıt verilmesi amacıyla doğaçlamaların yapılması, kararlı liderlik yönetimi, insan kaynaklarının etkinliği, kurumsal yönetim alanında şeffaflık, katılım ve iş birliği ile inovasyon, deneyim ve kurumsal kültürü dayanıklılık stratejileri olarak kullandıklarını ortaya çıkarmıştır.

Khuan (2024), literatür analizi yoluyla kurumsal dayanıklılığın sağlanmasında rol oynayan temel unsurları incelediği çalışmada dayanıklılık stratejilerini, liderin kuruluşu yönlendirmesi ve kuruluşun gelişimini sağlaması, insan kaynağının geliştirilmesi, maliyet optimizasyonuna önem verilmesi ile öngörü ve tahmin gibi proaktif önlemlerin alınması ve iş birliği ve ortaklıkların kurulması olarak belirtmektedir.

Enwereji vd.'nin (2024) Güney Afrika'daki VUCA ortamında girişimlere ilişkin dayanıklılık hususunun ele alındığı çalışmada uyum yeteneği, beceriklilik, risk yönetimi, inovasyon ve stratejik planlama, kaynak dağıtımının optimizasyonu, inovasyon, çeşitlendirme, iş birliği ve ağ oluşturma, kriz yönetimi ve risk azaltma dayanıklılık stratejileri olarak ifade edilmektedir.

Kokkranikal vd. (2024), tur operatörlerinin COVID-19 pandemisi döneminde karşılaştıkları zorlukları aşmak amacıyla kuruluş genelinde dayanıklılık oluşturulması üzere çeşitli stratejiler önermişlerdir. Bu stratejiler arasında müşteri odaklı yaklaşımların benimsenmesi, güven artırıcı önlemler alınması, personel etkinliğinin sağlanması, sunulan hizmetlerdeki eksiklik ve hataların telafi edilmesi, yenilikçilik ve mevzuata uyum sağlanması yer almaktadır.

Nosike vd. (2024), dayanıklılık stratejilerinin kuruluşlar üzerine etkileri üzerine gerçekleştirdikleri çalışmada, pandemi dönemleri gibi küresel belirsizlikler ve krizlerin daha iyi yönetilebilmesi amacıyla kuruluşların inovasyon stratejisi ile adaptif stratejilerine odaklandıkları sonucuna ulaşmıştır.

Singh (2024), COVID-19 pandemisi sırasında Hindistan'daki turizm ve konaklama sektöründe insan kaynakları uygulamalarını dayanıklılık açısından analiz etmiştir. Yazar, İK bağlamında dayanıklılık stratejilerini şeffaf ve zamanında iletişim, çalışan bağlılığı ve

motivasyonu, eğitim ve beceri geliştirme, işgücü planlaması ve esneklik, sağlık ve güvenlik protokolleri, liderlik desteği ve duygusal dayanıklılık geliştirme olarak ifade etmektedir.

Lu ve Chan (2024) tarafından gerçekleştirilen çalışma, Çin'in güneydoğusundaki 13 bakım evinin COVID-19 pandemisinin getirdiği zorluklara nasıl yanıt verdiğini incelemektedir. 38 personel ile gerçekleştirilen görüşmelerde bakım evlerinin önemli zorluklarla karşılaştığını, ancak hizmetlerin basitleştirilmesi, insan kaynaklarının yeniden yapılandırılması ve sakinler ile aileleri arasındaki sosyal iletişimi sürdürmek üzere teknolojinin kullanılması gibi çeşitli başa çıkma stratejileri benimsenerek dayanıklılığın sağlandığını göstermektedir.

Dehghani Sadrabadi vd. (2024), tedarik zincirinde yaşanan kırılganlıkların ve kesintilerin azaltılması amacıyla tedarik zinciri dayanıklılığının oluşturulması ile iş sürekliliği planlamasını uygulamanın büyük önem taşıdığını ifade etmektedir. Yazar anılan kesintilerin önlenmesi amacıyla çok amaçlı bir optimizasyon modeli önermektedir. Çalışmada dayanıklılığın artırılmasına yönelik yedeklilik, çeşitlendirme, esneklik, envanterin güçlendirilerek tamponlama yapılması ve iş sürekliliği planlaması stratejilerine yer verilmektedir.

Plaček vd. (2025) tarafından gerçekleştirilen çalışmada Slovakya ve Çek Cumhuriyeti'nde sosyal hizmet sunan sosyal girişimler (tüzel kişiliğe sahip iş modeli) ve kamu sektörü kuruluşlarının uyguladığı dayanıklılık stratejilerini incelemişlerdir. Makalede, sosyal girişimler açısından *ofansif dayanıklılık stratejileri*, yeni finansal kaynaklar ile pazarların aranması, faaliyetlerin çevrim içi ortama taşınması ve pazara yeni hizmet ve ürün çeşitlerinin sunulması; *defansif dayanıklılık stratejileri*, personele psikososyal destek sağlanması; karma dayanıklılık stratejisi ise operasyon ve görevlerin yeni koşullara uyarlanması şeklinde açıklanmaktadır. Kamu kuruluşlarında ise koruyucu önlemlerin aktifleştirilmesi, takım çalışmasına yoğunlaşılması ve iş rutinlerinin güncellenmesi ve acil durum planları ile risk planlarının güncelliğinin sağlanması, defansif dayanıklılık stratejileri olarak aktarılmaktadır.

Jiang vd. (2025), toplumsal sermaye çerçevesini kullanarak, çeşitli sermaye türlerinin organizasyonel dayanıklılık oluşturmada nasıl kullanıldığını geriye dönük ve ileriye dönük bir bakış açısıyla incelemektedir. Bangladeş'teki 30 konaklama işletmesinin sahibi/yöneticisi ile örnekleme yoluyla derinlemesine görüşmeler yapılmıştır. Araştırma sonucunda kurumsal seviyede 10 dayanıklılık stratejisi elde edilmiştir. Bunlar; çalışan beceri ve deneyimlerinden yararlanılması, şeffaf ve anlık iletişim, merkezi olmayan yetkilendirme, teknolojiyi uzaktan iş birliği için kullanma, paydaş ilişkilerini güçlendirme, kurumsal dayanıklılık anlayışı geliştirme,

yapısal ve organizasyonel yeniden tasarım, sürekli eğitim ve beceri geliştirme, dış iş birliği ve acil durum planlarının birlikte hazırlanması, sektör düzeyinde kriz koordinasyonudur.

De Waal vd.'nin (2025) çalışmasında, savaş ekonomisi içinde faaliyet gösteren Ukrayna şirketleri arasında örgütsel dayanıklılığın sağlanmasına yönelik dinamik yollar araştırılmaktadır. Araştırma, silahlı çatışmaların ticaret üzerindeki derin etkisini vurgulamakta ve işletmelerin riskleri azaltmak ve faaliyetlerini sürdürmek için dayanıklılık stratejileri geliştirmeleri gerektiğini vurgulamaktadır. Bu çerçevede operasyonel esneklik, modülerlik ve esneklik, iş birliği ve ağların oluşturulması ile dijital dönüşüm ve teknolojinin benimsenmesi dayanıklılık stratejileri olarak belirtilmektedir.

Literatürde KOBİ'lerin dayanıklılığı üzerine gerçekleştirilen çalışmalarda operasyonel, yönetsel, yapısal ve kültürel dayanıklılık stratejilerine değinilmektedir. Conz vd. (2017), çalışmasında aynı coğrafi alanda kümelenen KOBİ'lerin dayanıklılıklarını nasıl geliştirebileceklerini araştıran bir model sunmaktadır. Model, örgütsel, yenilikçi, iş birliğine dayalı ve girişimci olmak üzere dört farklı dayanıklılık stratejisini kapsamaktadır.

Bachtiar vd. (2023), Endonezya'daki KOBİ'lerin COVID-19 pandemisi sonrasında nasıl bir dayanıklılık geliştirdikleri ve büyüme stratejilerini yeniden şekillendirdiklerini araştırdıkları çalışmalarında bu işletmelerin farkındalık, uyum sağlama ve eyleme geçme olmak üzere üç ana dayanıklılık stratejisini uyguladıklarını belirlemiştir.

Park ve Seo (2024), çalışmalarında kriz dönemlerinde KOBİ'lerde kurumsal dayanıklılığın tesis edilmesine yönelik brikolaj stratejisini benimsemenin fayda sağladığını ifade etmektedir.

Biyela ve Utete (2024) çalışmalarında COVID-19 salgınının yaşandığı 2020-2022 yıllarında yayınlanan 35 makaleyi tarayarak Güney Afrika'daki tüm sektörlerde KOBİ'leri etkileyen ortak bir dizi işgücü, sermaye ve toplam faktör verimliliği sorununu ortaya koymuştur. Yazarlar, söz konusu kriz durumlarına yönelik iş sürekliliği planlaması, çeviklik ve esneklik, dijital dönüşüm ve teknoloji benimseme, finansal kaynak yönetimi, insan kaynakları geliştirme ve iş gücü dayanıklılığı, liderlik ve yönetim, inovasyon ve girişimcilik odaklılık, risk yönetimi ve senaryo planlama ile paydaş katılımı ve iş birliğini dayanıklılık stratejileri olarak tanımlamaktadır.

Adebiyi vd. (2025), ABD'deki küçük ölçekli kuruluşlarda çalışanların, çalıştıkları işletmenin hisselerine veya mülkiyet haklarına sahip olduğu çalışan sahipliği modelinin kurumsal dayanıklılığı artırmak amacıyla bir strateji olarak kullanıldığını aktarmaktadır.

Tedarik zinciri bağlamında yapılan çalışmalarda farklı strateji türlerinin kullanıldığı görülmektedir. Wieland ve Wallenburg'un (2013), tedarik zinciri yönetiminde dayanıklılığı inceledikleri çalışmalarında proaktif bir strateji olarak sağlamlık, "potansiyel kesinti veya şoklara rağmen tedarik zincirinin sürekliliğini sağlamak üzere hazırlık yapılmasını" ifade etmektedir. Çeviklik, "reaktif bir beklenmedik değişikliklere hızlı uyum sağlama ve yanıtlama yetkinliği" olarak tanımlanan reaktif bir stratejidir.

Hohenstein vd. (2015) tarafından tedarik zinciri dayanıklılığı üzerine literatür analizi yöntemiyle gerçekleştirilen araştırmada kesinti öncesine yönelik dayanıklılık stratejileri iş birliği, stok yönetimi, İK yönetimi, çoklu tedarik zinciri, yedekli çalışma, acil durum planlarının hazırlanması ile erken uyarı mekanizmalarının devreye alınması ve izleme faaliyetlerinin gerçekleştirilmesi olarak ifade edilmektedir. Çeviklik, esneklik, iş birliği, yedeklilik ve İK yönetimi kesinti sonrasına yönelik stratejiler olarak aktarılmaktadır. İşbirliği ile İK yönetimi ve yedeklilik stratejileri olay öncesi ve sonrasında aktif olarak izlenen stratejiler olarak ön plana çıkmaktadır.

Rabbani vd. (2020) tarafından senaryo tabanlı tedarik zinciri ağı tasarımı modeli üzerine gerçekleştirilen çalışmada proaktif ve reaktif dayanıklılık stratejilerinden bahsedilmektedir. Yazarlar, tedarik zincirinin görünürlüğünün artırılması, tedarik zincirindeki aktörler arasında iş birliğinin sağlanması ile envanter yönetimi ve bilgi teknolojilerinin hayata geçirilmesini proaktif stratejiler olarak aktarmaktadır. Diğer taraftan çeviklik, esneklik ve yedeklilik reaktif dayanıklılık stratejileri olarak belirtilmektedir.

Afifa ve Santoso (2022), çalışmalarında gıda tedarik zincirlerinde yer alan riskleri azaltmak üzere proaktif nitelikli tedarik zincirinin (yeniden) tasarımı, iş birliği, çeviklik, risk farkındalığının artırılması stratejilerini önermektedir.

Singh vd. (2023), tedarik zinciri dayanıklılığına yönelik önerdikleri çerçevede iş birliği, İşbirliğine dayalı teknolojiler, geri dönüşüm yoluyla kaynak yaratılması, coğrafi konumlanma ve kaynak çeşitlendirmesi ile yedekliliği dayanıklılık stratejileri olarak açıklamaktadırlar.

Mızrak'ın (2024) pandemi sonrasında ülkemizdeki çeşitli sektörlerde yaşanan tedarik zinciri kesintileriyle mücadelede kullanılan dayanıklılık stratejilerini araştırdıkları çalışmada tedarik kaynaklarının çeşitlendirilmesi, risk yönetiminin iyileştirilmesi ve teknolojinin entegrasyonunun sağlanması ortak stratejiler olarak aktarılmaktadır. İlave olarak araştırmada çeviklik kavramının ön plana çıktığına değinilmektedir.

Pont ve Simon (2024) çalışmalarında, aile işletmelerinin tedarik zinciri yönetimi stratejileri aracılığıyla krizler sırasında dayanıklılıklarını nasıl artırdığını araştırmaktadır. Dokuz aile işletmesinin vaka çalışmalarından yola çıkılarak envanterin yeniden düzenlenmesi, güçlü tedarikçi ilişkileri kurulması, ürün kalitesine ve müşteri sadakatine öncelik verilmesi ve maliyet azaltma önlemlerinin uygulanması olmak üzere dayanıklılığı destekleyen dört temel tedarik zinciri yönetimi stratejisi belirlenmektedir.

Tablo 10, ağırlıklı olarak kurumsal yönetim ve tedarik zinciri alanlarında gerçekleştirilmiş akademik çalışmalarda “dayanıklılık stratejisi” olarak ifade edilmiş kavramları kapsamaktadır. Çalışmalarda dayanıklılığın artırılması hususunda benzer stratejileri ifade eden kavramlara yer verildiği görülmektedir.

Anılan kavramlar arasında, operasyonel esneklik ve kriz durumundaki tepki kapasitesini güçlendirmeye yönelik yedeklilik, çeşitlilik, esneklik ve çeviklik; kurum içi ve dışı koordinasyon ve kaynak paylaşımına yönelik iş birliği ve ağ oluşturma stratejileri öne çıkmaktadır. Değişen koşullara ilişkin kuruluşun hızlı ve yaratıcı nitelikte yanıtlar oluşturabilmesini teminen inovasyon ile adaptasyon ve teknolojik dönüşüm stratejileri sıkça belirtilmektedir. Ayrıca, kurumsal risklerin planlı bir şekilde yönetilebilmesi amacıyla hazırlıklılık, öngörü, proaktif risk yönetimi, üzerine yoğunlaşılacak stratejiler olarak yer almaktadır.

Tablo 10’da sunulan literatürde, dayanıklılık stratejilerine ilişkin çeşitliliğin olduğu, ancak anılan stratejilerin toplulaştırılarak ortak tematik kavramlara indirgenebileceği, böylece jenerik ve tematik dayanıklılık stratejilerinin belirlenebileceği görülmektedir.

Tablo 10: Literatürdeki Çalışmalarda Yer Verilen Dayanıklılık Stratejileri

Kaynak	Çalışma Alanı	Çalışmada Yer Alan Dayanıklılık Stratejileri
Gibson ve Tarrant (2010)	Kurumsal Yönetim	Direnç, güvenilirlik, yedeklilik ve esneklik
Wieland ve Wallenburg (2013)	Tedarik zinciri	Sağlamlık, çeviklik
Lee vd. (2013)	Kurumsal Yönetim	Öngörü, izleme, tepki, öğrenme, sağlamlık
Erkip vd. (2014)	Perakende sektörü	Ürün bazında uzmanlaşma, hijyen ve ilgili standardizasyonun artırılması, müşteri memnuniyetinin sağlanması, uzun çalışma saatleri ve eve teslimat
Hohenstein vd. (2015)	Tedarik zinciri	İşbirliği, stok yönetimi, İK yönetimi, çoklu tedarik zinciri, yedekli çalışma, acil durum planlarının hazırlanması ile erken uyarı mekanizmalarının devreye alınması ve izleme faaliyetleri, çeviklik, esneklik, yedeklilik
Conz vd. (2017)	Kurumsal Yönetim	Örgütsel, yenilikçi, iş birliğine dayalı, girişimci stratejiler
Hatton vd. (2018)	Kurumsal Yönetim	Strateji ve planlama, liderlik ve kültür, kaynakların kullanılabilirliği ile ağlar ve ilişkiler
Granig ve Hilgarter (2020)	Kurumsal Yönetim	Öngörü ve tahmin, hazırlık, iletişim, uyum sağlama ve yanıt verme
Rabbani vd. (2020)	Tedarik zinciri	Tedarik zincirinin görünürlüğünün artırılması, iş birliği, envanter yönetimi, dijitalleşme, çeviklik, esneklik ve yedeklilik
Melián-Alzola vd. (2020)	Kurumsal Yönetim	Liderlik ve kültür stratejileri ile iç ve dış paydaşlarla kurulan ağ ve ilişkiler, yeniliklere açıklık, durumsal farkındalık, çeşitli senaryo ve stres testlerinin yapılması ile finansal, insan ve operasyonel kaynakların erişilebilir olması ve gerektiğinde yeniden tahsis edilebilmesi
Folake (2021)	Kurumsal Yönetim	İnovasyon, deneme, karar yetkisi ve belirsizliği benimseme, teknoloji ortaklıkları, Ar-Ge ve yeni teknolojilerin benimsenmesi, eğitim, kaynak çeşitlendirme, acil durum fonları ve bütçe planlaması, afet müdahale planları, altyapı yatırımları ve yerel iş birlikleri stratejileri
Afifa ve Santoso (2022)	Tedarik zinciri	Yeniden tasarım, iş birliği, çeviklik, risk farkındalığı
Baghersad ve Zobel (2022)	Kurumsal Yönetim	Operasyonel bolluk, operasyonel kapsam

Tablo 10: Literatürdeki Çalışmalarda Yer Verilen Dayanıklılık Stratejileri (Devam)

Kaynak	Çalışma Alanı	Çalışmada Yer Alan Dayanıklılık Stratejileri
Sinniah vd. (2022)	Kurumsal Yönetim	Nakit akışının güçlendirilmesi, alternatif tedarik zinciri patikalarının kullanılması, dijital dönüşüm, ürün ve pazar çeşitlendirme, çalışan eğitimi ve bağlılığı, senaryo planlama ile esnek organizasyon yapısı
Sadeqi-Arani ve Ghahfarokhi (2022)	Kurumsal Yönetim	Stratejik planlama ve kriz yönetimi, organizasyonel kültür ve liderlik, finansal esneklik ve kaynak yönetimi, dijital dönüşüm ve pazara uyum
Pertheban vd. (2023)	Kurumsal Yönetim	Yedeklilik, esneklik, çeviklik, iş birliği ve bilgi alışverişi
Richardson (2023)	Kurumsal Yönetim	Finansal çeviklik, adaptif tedarik zincirleri, stratejik teknolojilerin edinilmesi ve kullanılması ve proaktif risk yönetimi
Valbuena vd. (2023)	Kurumsal Yönetim	Gerektiğinde emprovize yanıt verebilme, kararlı liderlik yönetimi, insan kaynaklarının etkinliği, kurumsal yönetim bağlamında şeffaflık, katılım ve iş birliği, inovasyon, deneyim ve kurumsal kültürü
Bachtiar vd. (2023)	Kurumsal Yönetim	Farkındalık, uyum sağlama ve eyleme geçme
Singh vd. (2023)	Tedarik zinciri	İşbirliği, iş birliğine dayalı teknolojiler, geri dönüşüm yoluyla kaynak yaratılması, coğrafi konumlanma ve kaynak çeşitlendirmesi ile yedeklilik
Förster vd. (2023)	Kurumsal Yönetim	Kabul dayanıklılığı ve stratejik dayanıklılık
Pescaroli vd. (2023)	Kurumsal Yönetim	Sistemik risk yönetimi, kurumsal refleksivite, öngörülü yönetim, dayanıklılığın örgütsel karar alma süreçlerine dâhil edilmesi, kurumsal öğrenme ve uyum yeteneğinin teşvik edilmesi, yedeklilik ve esnekliğin oluşturulması ile farklı yönetim düzeyleri ve sektörler arasında işbirliği ve koordinasyon
Mızrak (2024)	Tedarik zinciri	Tedarik kaynaklarının çeşitlendirilmesi, risk yönetiminin iyileştirilmesi, dijitalleşme, çeviklik
Khuan (2024)	Kurumsal Yönetim	Etkin liderlik, insan kaynağının geliştirilmesi, maliyet optimizasyonu, öngörü ve tahmin, iş birliği ve ortaklıkların kurulması
Enwereji vd. (2024)	Kurumsal Yönetim	Uyum yeteneği, beceriklilik, risk yönetimi, inovasyon ve stratejik planlama, kaynak dağıtımının optimizasyonu, çeşitlendirme, iş birliği ve ağ oluşturma, kriz yönetimi ve risk azaltma
Kokkranikal vd. (2024)	Kurumsal Yönetim	Müşteri odaklılık, güven artırıcı önlemler alınması, personel etkinliğinin sağlanması, sunulan hizmetlerdeki eksiklik ve hataların telafi edilmesi, yenilikçilik ve mevzuata uyum
Nosike vd. (2024)	Kurumsal Yönetim	İnovasyon, adaptif stratejiler

Tablo 10: Literatürdeki Çalışmalarda Yer Verilen Dayanıklılık Stratejileri (Devam)

Kaynak	Çalışma Alanı	Çalışmada Yer Alan Dayanıklılık Stratejileri
Singh (2024)	Turizm sektörü	Şeffaf ve zamanında iletişim, çalışan bağlılığı ve motivasyonu, eğitim ve beceri geliştirme, işgücü planlaması ve esneklik, sağlık ve güvenlik protokolleri, liderlik desteği ve duygusal dayanıklılık geliştirme
Lu ve Chan (2024)	Kurumsal Yönetim	Hizmetlerin basitleştirilmesi, insan kaynaklarının yeniden yapılandırılması ve sakinler ile aileleri arasındaki sosyal iletişimi sürdürmek üzere teknolojinin kullanılması
Park ve Seo (2024)	Kurumsal Yönetim	Brikolaj (elde mevcut olan araç, malzeme ve imkânlarla yeni bir şey üretme, bir problemi çözme ya da ortaya yaratıcı bir çözüm koyma süreci)
Dehghani Sadrabadi vd. (2024)	Tedarik zinciri	Yedeklilik, çeşitlendirme, esneklik, envanterin güçlendirilerek tamponlama yapılması ve iş sürekliliği planlaması
Biyela ve Utete (2024)	Tüm sektörler	İş sürekliliği planlaması, çeviklik ve esneklik, dijital dönüşüm ve teknoloji benimseme, finansal kaynak yönetimi, insan kaynakları geliştirme ve iş gücü dayanıklılığı, liderlik ve yönetim, inovasyon ve girişimcilik odaklılık, risk yönetimi ve senaryo planlama ile paydaş katılımı ve iş birliği
Pont ve Simon (2024)	Tedarik zinciri	Envanterin yeniden düzenlenmesi, güçlü tedarikçi ilişkileri kurulması, ürün kalitesine ve müşteri sadakatine öncelik verilmesi ve maliyet azaltma önlemlerinin uygulanması
Plaček vd. (2025)	Kurumsal Yönetim	Sosyal Girişimlerde: Yeni finansal kaynak ve pazarlar, dijitalleşme, hizmet ve ürün çeşitliliği, personele psikososyal destek sağlanması, operasyon ve görevlerin yeni koşullara uyarlanması Kamu Kuruluşlarında: Koruyucu önlemlerin aktifleştirilmesi, takım çalışmasına yoğunlaşılması, iş rutinlerinin güncellenmesi, acil durum planları ve risk planlarının güncelliğinin sağlanması
Adebiyi vd. (2025)	Kurumsal Yönetim	Çalışan sahipliği modelinin uygulanması
Jiang vd. (2025)	Kurumsal Yönetim	Çalışan beceri ve deneyimlerinden yararlanılması, şeffaf ve anlık iletişim, merkezi olmayan yetkilendirme, teknolojiyi uzaktan iş birliği için kullanma, paydaş ilişkilerini güçlendirme, kurumsal dayanıklılık zihniyeti geliştirme, yapısal ve organizasyonel yeniden tasarım, sürekli eğitim ve beceri geliştirme, dış iş birliği ve acil durum planlarının birlikte hazırlanması, sektör düzeyinde kriz koordinasyonu
De Waal vd. (2025)	Kurumsal Yönetim	Operasyonel esneklik, modülerlik ve esneklik, iş birliği ve ağların oluşturulması ile dijital dönüşüm ve teknolojinin benimsenmesi

4.2.2. Kurumsal Dayanıklılık Standartları

Kurumsal dayanıklılığın geliştirilmesine yönelik stratejiler, literatürün yanında dayanıklılıkla ilgili çeşitli uluslararası standartlarda yer alabilmektedir. Bu standartlarda, kuruluşların olumsuz durumlar karşısında hazırlıklı olmasını, olay anında etkin bir şekilde tepki verebilmesini ve sonrasında sürdürülebilir bir şekilde toparlanmasını sağlayacak stratejik yönelimler açık ya da örtük bir şekilde sunulmaktadır.

Bu bağlamda ANSI/ASIS (2009) tarafından yayımlanan Organizasyonel Dayanıklılık Standardı'nda dayanıklılık stratejileri açık bir şekilde belirtilmemiş, bunun yerine yönetim sistemi gereklilikleri aracılığıyla örtük bir şekilde stratejilere atıfta bulunulmuştur. Standartta yer alan örtük yaklaşımlar entegrasyon, hazırlık, uyarlanabilirlik, sürekli iyileştirme, paydaş iş birliği ve kaynak sürdürülebilirliği olarak ifade edilebilir.

ISO (2017) tarafından yayımlanan ISO 22316: Güvenlik ve Dayanıklılık - Organizasyonel Dayanıklılık – İlkeler ve Özellikler Standardı'nda, açıkça dayanıklılık stratejilerine değinilmemiş olup, dayanıklılık stratejileriyle örtüşen ilkeler ve özellikler açıklanmaktadır. Standartta dayanıklılık ilkeleri olarak aşağıdaki hususlara değinilmektedir.

- a. Dayanıklılık, davranışların ortak bir vizyon ve amaçla uyumlu olmasıyla artar.
- b. Dayanıklılık, kuruluşun bağlamına ilişkin güncel bir anlayışa dayanır.
- c. Dayanıklılık, değişimi özümseme, uyum sağlama ve etkili tepki verme becerisine dayanır.
- d. Dayanıklılık, iyi yönetim ve yönetime dayanır.
- e. Dayanıklılık, beceri, liderlik, bilgi ve deneyim çeşitliliği ile desteklenir.
- f. Dayanıklılık, yönetim disiplinleri arasında koordinasyon ve teknik/bilimsel alanlardan katkılarla güçlenir.
- g. Dayanıklılık, risklerin etkin yönetimine dayanır.

Söz konusu ilkeler kapsamında kurumsal kapasite geliştirme, hazırlık, bağlantı, kapsayıcılık, çeşitlendirme, yedeklilik, modülerlik, öğrenme, uyarlanabilirlik, dönüşüm ve ağ oluşturma ve iş birliği hususlarına atıfta bulunulduğu görülmektedir.

Diğer taraftan ortak vizyon ve amaç netliği, bağlamı anlama ve etkileme, etkili ve yetkilendirilmiş liderlik, örgütsel dayanıklılığı destekleyen bir kültür, paylaşılan bilgi ve bilgi

birikimi, kaynakların kullanılabilirliği, yönetim disiplinlerinin geliştirilmesi ve koordinasyonu, sürekli iyileştirmeyi destekleme, değişimi öngörme ve yönetme becerisi dayanıklılığın özellikleri olarak sunulmaktadır. Söz konusu özellikler aracılığıyla yönetim ve liderlik, hazırlıklılık, bilgi paylaşımı ve öğrenme, kaynak yönetimi ve yedeklilik, entegrasyon ve koordinasyon, öğrenme ve adaptasyon ile uyum ve dönüşüm hususlarına atıfta bulunulduğu görülmektedir.

ISO (2019) tarafından yayımlanan ISO 22301: Güvenlik ve Dayanıklılık – İş Sürekliliği Yönetim Sistemleri – Gereklilikler Standardı’nda dayanıklılık stratejileri açıkça belirtilmemiştir. Bunun yerine, kuruluşların sürekliliği ile dayanıklılığını sağlayan stratejiler tasarımları ve uygulamaları için bir çerçeve sunulmaktadır. Standarda göre kesintileri yönetebilmek için uygun seçenekler belirlenip uygulanarak süreklilik stratejileri ve çözümleri oluşturulmalı, bu kapsamda yanıt, kurtarma ve faaliyetlerin devamını destekleyen iş sürekliliği planları ve prosedürleri geliştirilip uygulanmalıdır. Ayrıca, stratejilerde esneklik ve ölçeklenebilirlik sağlanarak farklı türde kesintilere ve kurumun değişen ihtiyaçlarına uyumlanabilir olmaları güvence altına alınmalıdır. Söz konusu gereklilikler yedeklilik, çeşitlilik, modülerlik, uyumlanabilirlik ve hazırlık hususlarına atıfta bulunmaktadır.

BSI (2022) tarafından yayımlanan BS 65000: Organizasyonel Dayanıklılık — Uygulama Kodu Standardı’nda dayanıklılık stratejileri açıkça belirtilmekte ve kuruluşların bu stratejileri hayata geçirmeleri önerilmektedir.

Standart, kuruluşların benimsemesi gereken dört tasarım stratejisini vurgular. Yedeklilik, kesintilerin telafi edilmesi için yedekler, yedek kapasite, sistemler, stoklar ve gölge personel sağlanmasını ifade etmektedir. Çeşitlilik, kırılganlığın azaltılması için kaynakların, tedarikçilerin, ürünlerin ve lokasyonların çeşitlendirilmesini; modülerlik, organizasyonel unsurları birbirine taşınabilir bir şekilde bağlayarak, bir parçadaki arızanın sistem genelinde çökmeye neden olmaması, yerel arızaların ve daha hızlı kurtarma işleminin mümkün olmasının sağlanmasını belirtmektedir. Uyumlanabilirlik, kesintilerle karşı karşıya kalındığında kaynakları hızla yeniden bir araya getirilmesi, yeni çözümlerin üretilmesi ve stratejilerin uygulanması amacıyla esneklik ve becerikliliğin korunmasını açıklamaktadır.

Dayanıklılık stratejilerinin açık ve örtük bir şekilde ifade edildiği standartlar ile strateji ve strateji benzeri hususlar Tablo 11’de gösterilmektedir.

Tablo 11: Standartlarda Yer Verilen Dayanıklılık Stratejileri ile Strateji Benzeri Unsurlar

Standart	Açık / Örtük	Standartta Yer Alan Dayanıklılık Stratejileri
ANSI/ASIS SPC.1-2009 Organizasyonel Dayanıklılık	Örtük	Entegrasyon, hazırlık, uyarlanabilirlik, sürekli iyileştirme, paydaş iş birliği, kaynak sürdürülebilirliği
ISO 22316:2017 Güvenlik ve Dayanıklılık – Organizasyonel Dayanıklılık – İlkeler ve Özellikler	Örtük	Kurumsal kapasite geliştirme, hazırlık, bağlantı, kapsayıcılık, çeşitlendirme, yedeklilik, modülerlik, öğrenme, uyarlanabilirlik, dönüşüm ve ağ oluşturma ve iş birliği, yönetim ve liderlik, hazırlıklılık, bilgi paylaşımı ve öğrenme, entegrasyon ve koordinasyon, öğrenme ve adaptasyon, uyum ve dönüşüm
ISO 22301:2019 Güvenlik ve Dayanıklılık – İş Sürekliliği Yönetim Sistemleri – Gereklilikler	Örtük	Yedeklilik, çeşitlilik, modülerlik, uyarlanabilirlik, hazırlık
BS 65000:2022 “Organizasyonel Dayanıklılık — Uygulama Kodu” Standardı	Açık	Yedeklilik, çeşitlilik, modülerlik, uyarlanabilirlik

4.3. Literatür Bazlı Jenerik Dayanıklılık Stratejileri

4.3.1. Stratejilerin Konsolide Edilmesi

Literatür ve standartlarda benzer stratejik yönelimlerin farklı terminolojilerle ifade edilmesi, kavramsal dağınıklığa yol açmaktadır. Bu nedenle, işlev ve anlam bakımından örtüşen stratejiler jenerik kavramlar altında konsolide edilmiş; böylece farklı bağlamlara uyarlanabilir, sade, uygulanabilir ve genelleştirilebilir bir strateji seti oluşturulmuştur. Bu yaklaşım, hem kavramsal tutarlılık sağlamakta hem de önerilecek modelin önemli bir bileşenini oluşturmaktadır. Bu noktada “jenerik strateji” ifadesiyle “belli bir sektöre, kurumsal yapıya ya da bağlamsal duruma özgü olmayan; farklı örgütsel yapılarda benzer sorunlara karşı benzer çözümler sunabilecek, esnek ve uyarlanabilir yönetsel stratejilere” vurgu yapılmaktadır. Söz konusu ifade, dayanıklılıkla ilişkili literatürde farklı kavramlar olarak ele alınan ortak stratejik yönelimlerin temsil edilmesi ve uygulanabilir bir şekilde sunulması amacıyla kullanılmaktadır.

Öncelikle, literatürde açık bir şekilde “dayanıklılık stratejisi” olarak tanımlanan ve Tablo 10’da yer verilen unsurlar ayrıştırılarak 176 adet strateji ve strateji benzeri ifade tespit edilmiştir. Benzer şekilde ilgili standartlarda “dayanıklılık stratejisi” olarak açıkça bahsedilen ya da örtük bir şekilde değinilen ve Tablo 11’de yer verilen unsurlar ayrıştırılarak 19 adet strateji ve strateji benzeri ifade elde edilmiştir.

Ardından söz konusu unsurlar, farklı sektör ve kurumlara uyarlanabilirlik durumları açısından değerlendirilmiş ve unsurlara yönelik jenerik adlandırmalar yapılmıştır. Son aşamada, bahse konu jenerik ifadeler, strateji olarak nitelendirilebilme durumları çerçevesinde incelenmiş ve 34 adet ana unsur; yönetim aracı, ilke, kapasite, özellik ve strateji açısından gruplandırılmıştır. Tablo 12’de bu gruplandırmaya yer verilmektedir.

Tablo 12: Literatürdeki Dayanıklılık Stratejilerinin Değerlendirilmesi

Dayanıklılığın Sağlanmasında Kullanılan Araçlar	Dayanıklılık İlkeleri	Dayanıklılık Kapasitesi Kapsamındaki Unsurlar	Dayanıklılık Özellikleri	Dayanıklılık Stratejileri
• İş sürekliliği yönetimi • Kriz yönetimi • Risk yönetimi	• Dayanıklılık odaklı liderlik ve yönetim • Açıklık • İletişimde etkinlik • Şeffaflık • Bilgi Paylaşımı ve Öğrenme • Entegrasyon ve Koordinasyon • Sürekli İyileştirme • Kapsayıcılık • Hazırlıklılık	• Çalışan dayanıklılığının artırılması • Farkındalığın güçlendirilmesi • Hazırlıklılık kapasitesi • Kaynak yönetimi • Kurumsal itibarın korunması • Öngörü / tahmin kapasitesi • Uyum kapasitesi • Dönüşüm kapasitesi • Dayanıklılık kültürünün oluşturulması • Kurumsal öğrenmeye ağırlık verilmesi • Yanıt verebilirlik kapasitesinin artırılması	• Dirençlilik • Çeviklik • Esneklik • Sağlamlık • Bağlantısallık • Hazırlıklılık	• Yedeklilik • Çeşitlilik • Modülerlik • Kurumsal ağlar / iş birliği ve ortaklık • Kapasite geliştirme

4.3.2. Dayanıklılık Stratejileri

Literatüre yönelik analiz, konsolidasyon ve değerlendirme aşamalarının sonucunda (1) yedeklilik, (2) çeşitlilik, (3) modülerlik, (4) kurumsal ağlar / iş birliği ve ortaklık ve (5) kapasite geliştirme olmak üzere beş ana dayanıklılık stratejisi belirlenmiştir.

Diğer taraftan, tabloda yer alan unsurların tümü, dayanıklılık kapasitesinin geliştirilmesi stratejisi kapsamında değerlendirilebilir ve bu unsurlara ilişkin eylemler tanımlanabilir.

4.3.2.1. Yedeklilik

Yedeklilik (redundancy), sistemlere kesintiler sırasında çalışmaya devam etmeleri için yedek kaynaklar sağlayarak esnekliğin artırılmasında kritik bir kavram olarak hizmet eder.

Yedeklilik, kesintiler sırasında operasyonların devamlılığını sağlayan birden fazla tedarikçiye veya yedek sisteme sahip olunmasıyla sağlanabilir (Azadeh vd., 2016). Bu kavram, yedekliliğin bir sigorta poliçesi görevi görerek sistemlerin önemli bir işlevsellik kaybı olmadan şokları absorbe etmesine olanak tanımaktadır (Lai & Hsu, 2018). Bu bağlamda Sheffi (2015), yedekliliğin envanter tamponları yoluyla kuruluşların dış belirsizliklerin üstesinden gelmesini sağladığını ifade ederek, kasırga sezonu öncesinde işletmelerin stok seviyelerini artırmalarını buna örnek olarak vermektedir.

Dalziel ve McManus (2004), yedekliliğin sistemlerin, gelişen risklere yanıt vermesini ve stres altında bile işlevselliğini sürdürmesini sağladığını öne sürmektedir. Yedeklilik, bu anlamda bir koruma sağlarken, operasyonel karmaşıklığı ve tek bir olay ya da arızadan kaynaklanan çoklu arızalara karşı kırılganlığı da artırabilir, bu da kuruluşların yedeklilik seviyelerini verimlilikle dikkatli bir şekilde dengelemesini gerekli kılar (Bresch vd., 2014).

Sheffi ve Rice'ın (2005) vurguladığı üzere, yedeklilik esneklikle birlikte çalışarak dayanıklılığı artırır ve birincil sistemler kesintiye uğradığında sürekliliği sağlar. Haines vd. (2008), yedekliliği dayanıklılığın temel özelliklerinden biri olarak konumlandırarak genişletmekte, kavramı sistemde yer alan elemanlardan birisinin arızalanarak işlevini yitirdiği durumlarda, sistemdeki diğer bileşenlerin, anılan elemanın işlevini üstlenerek sistemin genel sistem performansının önemli ölçüde etkilenmemesini sağlaması durumunu ifade ettiğini belirtmektedir.

Literatürde, envanter yedekleme dışında yedekliliğin yapısal, işlevsel ve operasyonel yedeklilik gibi çeşitli türlere altında ele alındığı görülmektedir. Bu kapsamda (1) yapısal yedeklilik, güç sistemlerindeki yedek jeneratörler gibi, diğerleri arızalandığında işlevleri devralabilen fiziksel bileşenleri ifade eder (Cuadra vd., 2015). İş ekosisteminde istikrarın korunması için hayati önem taşıyan benzer rolleri yerine getirebilen birden fazla personel veya sürece sahip olunması (2) işlevsel yedeklilik olarak adlandırılabilir (Sundstrom vd., 2018). Son olarak, (3) operasyonel yedeklilik, çalışanların birden fazla rolü yerine getirmek üzere çapraz eğitime tabi tutulması gibi kurumsal uygulamalarla ilgilidir ve kritik işlevlerin her türlü senaryoda devam edebilmesini sağlar (Lai & Hsu, 2018). Her bir yedeklilik türü, farklı sistemlerde dayanıklılığın artırılmasında farklı bir rol oynar.

Yüksek düzeyde yedeklilik, sistemlerde maliyetlerin ve karmaşıklığın artmasına neden olabilir, altta yatan verimsizlikleri gizleyebilir (Sheffi, 2005) ve yanıt verebilirliği engelleyebilir (Shi vd., 2018). Örneğin, kuruluşlar yedekli kaynakları etkili bir şekilde yönetmekte zorluklarla karşılaşabilir ve bu da potansiyel çakışmalara ve verimsizliklere yol açabilir (Linnenluecke & Griffiths, 2010). Bu nedenle, kuruluşların esnekliği sağlamak için yeterli yedekliliği sürdürmek ile operasyonları zorlaştırabilecek aşırı yedeklilikten kaçınmak arasında bir denge kurması çok önemlidir. Kimi işletmeler, fayda maliyet açısından yedekliliği değerlendirmekte ve yedeklilik maliyetlerini ölçmektedir (Sheffi, 2005; Sheffi, 2015).

Yedeklilik stratejisine ilişkin kurumsal uygulama örneklerine aşağıda yer verilmektedir.

- Bilgi teknolojileri altyapısında bir kesinti yaşanması durumuna karşı, verilerin yedeklendiği farklı lokasyonlarda veri merkezleri kurulması.
- Üretim süreçlerinde kullanılan makinelerin arızalanması durumuna karşı, aynı işlevi görebilecek yedek makinelerin bulundurulması.
- Anahtar pozisyonundaki çalışanların yerine geçebilecek çalışanların önceden eğitilerek hazır tutulması.
- Elektrik kesintilerine karşı acil enerji sistemlerinin kurulması.
- Ani gelir kaybı, piyasa dalgalanması veya kriz dönemlerinde faaliyetleri sürdürebilmek için finansal tampon (acil durum fonu, finansal rezerv) oluşturulması.

4.3.2.2. Çeşitlilik

Çeşitlilik stratejisi, kurumun ürün, hizmet, kaynak, insan kaynağı, tedarikçi, fikir, bilgi ve süreçler bakımından farklı kanallara sahip olmasını amaçlar. Çeşitlilik, tekil bir unsurun arızalanması, kaybedilmesi, kesintiye uğraması vb. durumunda alternatif seçeneklerin varlığını ifade eder.

Tierney (2014) ile Graveline ve Germain (2022), çeşitliliği maddi, insani ve bilgi varlıkları da dâhil olmak üzere bir dizi kaynağı kapsayacak şekilde kavramsallaştırmaktadır. Jackson vd. (2003), kurumsal bağlamlarda çeşitliliğin farklı bakış açıları getirerek daha iyi sorun çözmeyi teşvik ettiğini ve yaratıcılığı artırdığını, daha yüksek uyum kabiliyetine ve krizlere daha etkili yanıtlar verilmesine katkıda bulunduğunu savunmaktadır.

Harrison ve Klein (2007), çeşitlilik terimini işgücü bağlamında, bir grup ya da kuruluşun üyeleri arasında değişik açılardan farklılıkların bulunması olarak tanımlanmaktadır. Çeşitliliğin çok yönlü doğası, ekip, takım içi etkileşimlerini ve uzun vadeli ekip uyumunu şekillendirmede önemli roller oynayan (1) yüzeysel çeşitlilik (yaş, cinsiyet, etnik köken gibi gözlemlenebilir özellikler) ve (2) derin çeşitlilik (değerler, inançlar, kişilik özellikleri) gibi türler aracılığıyla daha fazla araştırılmaktadır (Harrison vd., 2002).

Bresch vd. (2014), çeşitliliğin dayanıklılığı artırmadaki rolünü “bir sistem veya kuruluş içindeki çeşitli bileşenlerin (örneğin çalışanlar, tedarikçiler ve üretim yöntemleri) kesintilere farklı şekilde yanıt verme becerisini” ifade eden duyarlı çeşitlilik kavramı ile açıklamaktadır. Palin’in (2016) tanımladığı işlevsel çeşitlilik, bir kurum içinde çoklu, birbirinin yerine geçebilen roller aracılığıyla yedeklilik yaratarak dayanıklılığı güçlendirir, bu da stres altında etkili yanıtlar verilmesini ve operasyonların devamlılığını sağlar.

Conz ve Magnani (2020), çeşitliliğin finansal, insani ve teknolojik varlıklar da dâhil olmak üzere kurumsal kaynak havuzlarına entegre edildiğinde, kuruluşları değişen koşullara yanıt vermek için gereken esneklikle donattığını vurgulamaktadır. Alternatif kaynak ve yöntemlerin planlanması, heterojen yapıların benimsenmesi, farklı senaryolara uyum kabiliyeti ve kurum içi ve dışı fikir çeşitliliği çeşitlilik stratejisinin özellikleri arasında yer almaktadır.

Öte yandan Yu vd. (2020), aşırı çeşitliliğin verimsizliklere yol açabileceği ve sistemin uyarlanabilir kapasitesinin olumsuz etkilenmemesi için yönetilmesi gereken ödünleşimler (trade-offs) yaratabileceği konusunda uyarılmaktadır. Yazarlar çeşitliliğe, sistemleri aşırı karmaşık veya maliyetli hale getirmeyecek şekilde dengeli bir yaklaşımı önermektedirler.

Çeşitlilik stratejisine ilişkin çeşitli uygulama örnekleri aşağıda yer almaktadır.

- Birden fazla lojistik kanal ve tedarikçinin kullanılması
- Farklı sektörlerle hizmet sunarak pazar çeşitlendirmesi yapılması
- Ürün ve hizmet portföyünün çeşitlendirilmesi yoluyla talep dalgalanmalarına karşı esneklik sağlanması.
- Aynı işlevi gören alternatif teknolojilerin hazır bulundurulması
- Farklı bölgesel pazarlara hitap eden ürün varyasyonları
- Farklı coğrafi bölgelerde operasyonlar yürüterek bölgesel risklerin dengelenmesi.
- Çalışan çeşitliliğini (yaş, cinsiyet, deneyim, uzmanlık) artırarak organizasyonel yaratıcılığın ve adaptasyon yeteneğinin güçlendirilmesi.

4.3.2.3. Modülerlik

Modülerlik, bir sistemin veya organizasyon yapısının, işlevsel olarak bağımsız, ancak birlikte çalışabilir bileşenlere (modüllere) ayrılabilme derecesini ifade eder. Kurumlar açısından modülerlik, operasyonel, yapısal ya da teknolojik birimleri birbirinden ayırıştırarak karmaşık sistemleri daha yönetilebilir hale getiren bir yaklaşımdır.

Biggs vd. (2012) ağ teorileri bağlamında, modülerlik kavramını “diğer düğüm alt kümelerine gevşek bir şekilde bağlı olan, ancak birbirlerine yoğun bir şekilde bağlı düğüm alt kümelerinin varlığının derecesi” olarak ifade eder. Jackson ve Ferris (2013), mühendislik sistemlerine yönelik dayanıklılık ilkelerinin sağladıkları faydaları inceledikleri çalışmalarında modülerlik ilkesini “bir sistemin işlevselliğinin, tek bir düğümün hasar görmesi veya tahrip olması durumunda kalan düğümlerin çalışmaya devam edebilmesi için o sistemin çeşitli düğümlerine dağıtılması gerekliliği” şeklinde açıklamaktadırlar.

Modülerlik stratejisi, organizasyonun esnekliğini ve müdahale kapasitesini artırarak beklenmedik olaylara daha hızlı yanıt verilmesini sağlar. Modüler tasarım, sistemi oluşturan bileşenlerden birisinde bir aksaklık, arıza gerçekleştiğinde, işlevsel sürecin devam edebilmesi ve böylece arızanın yayılımını engeller (Carpenter vd., 2012; Jackson, 2016). Kriz durumlarında yalnızca ilgili modüller durdurulup yeniden yapılandırılabilirken, sistemin geri kalanı işlevini sürdürebilir. Bu da operasyonel sürekliliği destekler. Anılan izolasyon durumu,

arızanın ya da aksaklığın lokal olarak o bölgede kalmasını sağlarken, diğer bölge, süreç, fonksiyona vb. bulaşmasını önler. İlave olarak yarıda kalan sürecin, başka bir nokta, konum ya da sistem üzerinden devam etmesine imkân verir.

Modüler sistemler (ya da kuruluşlar) çeşitli özellikleri ile modüler olmayan yapılardan ayrılmaktadır. Bunların ilki her bir modülün kendi başına çalışabilir, bağımsız olarak geliştirilebilir, güncellenebilir ya da değiştirilebilir olmasıdır. Ayrı modüller bir araya getirildiğinde sistemin bütünsel işlevi bozulmadan korunur. Diğer bir özellik ise bir sorunla karşılaşıldığında yalnızca ilgili modüle müdahale edilmesinin yeterli olmasıdır. Ayrıca değişen koşullara ya da ihtiyaçlara göre sistemin tamamını etkilemeden yalnızca ilgili modül değiştirilebilir.

Modülerlik, sistem karmaşıklığını azaltarak karar alma süreçlerini hızlandırır, öğrenmeyi kolaylaştırır ve değişime uyum yeteneğini artırır. Bu yönüyle, uyumluluk kapasitesiyle doğrudan ilişkilidir.

Bu strateji, belirsizliğin yüksek olduğu durumlar, farklı birbirinden bağımsız iş birimlerinin koordinasyon içinde çalışması gereken durumlar ve kriz anlarında etkilenen bölümün izole edilip diğerlerinin çalışmasının sürdürülmesi gereken durumlarda kullanılabilir. Modülerlik stratejisine ilişkin çeşitli uygulama örnekleri aşağıda yer almaktadır.

- Departmanların, projelerin veya şubelerin birbirinden ayrıştırılmış ama merkezi hedeflere hizmet eder şekilde organize edilmesi.
- Tedarik, üretim ve dağıtım fonksiyonlarının birbirinden bağımsız çalışabilecek biçimde yapılandırılması.
- Yazılım sistemlerinin modüller halinde geliştirilmesi ve yönetilmesi
- Çalışan rollerinin esnek tanımlanması, farklı görevler için geçici ekiplerin oluşturulması.
- Operasyonel süreçlerin parçalarına ayrılması (örneğin sipariş, üretim, sevkiyat gibi bölümlerin ayrı ayrı optimize edilmesi).

4.3.2.4. Kurumsal Ağlar / İşbirliği ve Ortaklık

Kurumsal ağlar oluşturulması ve mevcut ağlara dâhil olunması, kuruluşların benzer hedefleri paylaşan farklı aktörlerle geniş bir ilişki ağı kurmasını ve bu ağlarda yer almasını

ifade eder. Ağ oluşturma, kaynak paylaşımı, koordinasyon ve bilgi entegrasyonu ile güçlü kurumsal ilişki bağları kurulmasını gerektirmekte olup, kurulan bağlar ağın bütününde iş birliğini ve dayanıklılığı güçlendirmektedir (Helaakoski vd., 2007). Kurumsal ağlar oluşturulması ve mevcut ağlara dâhil olunması stratejisi, dayanıklılık kapasitesinin artırılmasına hizmet etmekle birlikte, bir hazırlık çalışmasıdır. Süreklilik arz eden bu ağlar geniş ve çok aktörlü bir yapıya sahip olup, olay öncesinde kurulurlar.

Ağ oluşturma; diğer kuruluşlarla ilişkiler kurmayı, birlikte öğrenmeyi ve birlikte hareket edebilmeyi kapsar. Ağlara dâhil olma ise mevcut sektörel, yerel, ulusal veya uluslararası platformlara katılarak kurumun daha geniş bir dayanıklılık ekosistemi içinde yer alması şeklinde ifade edilebilir. Bu stratejinin amacı dayanıklılık için uzun vadeli, çok taraflı ilişkiler geliştirmek ve bu ilişkiler aracılığıyla bilgi, deneyim, kaynak ve öngörülere erişimi artırmaktır. Ağdaki düşünce ve bakış açısındaki çeşitlilikler, yeni değerlendirme becerileri ile yaratıcılık ve yenilikçiliği tetikleyebilir (Liddle, 2022).

Roberts vd. (2022), iş dayanıklılığı ve ilerlemenin sağlanabilmesini teminen dört temel ağ stratejisine değinmektedir. Bunlardan ittifaklar, rekabet gücünü artırmak amacıyla kaynakları paylaşmak, yeni pazarlara erişmek veya ortak ürünler geliştirmek için diğer kuruluşlarla ortaklık kurmayı içerir. Portföyler, çıktıları ayrı ayrı yönetirken bilgi veya patent paylaşımı yoluyla ortak yaratım için bağımsız firmalarla yapılan anlaşmaları ifade eder. İnovasyon ağları, ürünleri, hizmetleri ve organizasyonel refahı iyileştirmek için kuruluşlar arasında paylaşılan Ar-Ge çabalarına odaklanır. Ekosistemler, tek bir organizasyonun tek başına başaramayacağı müşteri değerini birden fazla aktörün ortaklaşa yarattığı gelişmiş iş birlikleridir.

Ağ oluşturma ve ağlara dâhil olma stratejisine ilişkin uygulama örneklerine aşağıda yer verilmektedir.

- Kuruluşun faaliyet gösterdiği sektördeki çatı kuruluşlara veya meslek birliklerine üye olması.
- Ulusal ve uluslararası düzeyde sürdürülebilirlik, iklim riski, kriz yönetimi gibi tematik ağlara dâhil olması.
- Bilgi, teknoloji ve kaynak paylaşımı için inovasyon kümeleri veya teknoloji merkezleri ile ağ oluşturma.
- Kriz sonrası toparlanma süreçlerinde sosyal sermayeye dayalı ağlardan destek alması.

Diğer taraftan, kurumsal iş birlikleri ve ortaklık stratejisi, belirli bir amaç, proje veya kriz bağlamında iki ya da daha fazla aktör arasında kurulan aktif iş yapma ilişkilerini ifade eder. Bu strateji, yalnızca bilgi ve kaynak paylaşımını değil, aynı zamanda ortak risk algısı geliştirmeyi, karşılıklı destek mekanizmaları oluşturmayı ve kriz anlarında koordineli hareket etmeyi de kapsar.

Soosay vd. (2008), iş birliğini “ortak yatırım, karşılıklı hedefler, ortak karar alma ve problem çözme gibi unsurları içeren, kuruluşlar arasında kurulan bağlılık ilişkisi” olarak tanımlamaktadır. Bu tür iş birliği ortaklıkları, rekabet avantajı sağlar ve kuruluşların performansını artırır. Jüttner ve Maklan (2011), iş birliğini “ortak bir proje üzerinde başkalarıyla birlikte çalışma” olarak tanımlamakta ve iş birliğinin, aktörlerin bireysel olarak sistemin etkili tepki verme yeteneğini sektöre uğratabilecek nitelikteki fırsatçı davranışlarını önlediğini vurgulamaktadır.

Meredith vd. (2017), iş birliğini kuruluş üyelerinin “değerleri, normları ve çalışma yöntemlerini paylaştığı, organizasyonel konuları tartıştığı, bilgi paylaştığı, birbirlerine rehberlik ettiği, ortak deneyimleri üzerinde düşündüğü ve birlikte organizasyonel programlar oluşturduğu” bir süreç olarak tanımlamaktadır.

Kuruluşlarda birbirinden farklı görüşlerin ortaya konulabilmesi ve tartışılabilmesini sağlayan iş birliği ile ortak çalışma, kuruluşların dayanıklılıklarına yönelik temel bir özelliktir. Deloitte tarafından 2021 yılında gerçekleştirilen çalışmada, iş birliğinin dayanıklı kuruluşların temel özellikleri arasında yer aldığı ortaya konulmaktadır. Araştırmada liderlerin, iş birliklerinin karar alma süreçlerini geliştirdiğini, riskleri minimize ettiğini ve inovasyonu desteklediğini ifade ettikleri vurgulanmaktadır (Mondragón vd., 2022).

Nasab vd. (2023), ağ oluşturma, dış kaynak kullanımı ve kaynak paylaşımını kapsayan iş birliklerinin, kurumsal dayanıklılığı artırarak krizlerle mücadelede kuruluşları destekleyebileceğini ifade etmektedir. Andrés ve Poler’e (2013) göre, ağ iş birliği, küresel rekabet gücünün artırılması, inovasyon ve ortaklar arasında uyum gibi birçok fayda sağlar. Kuruluşlar arası ilişkileri güçlendirir, verimsizlikleri en aza indirerek maliyetleri düşürür, işgücü becerilerini ve rol dağılımını netleştirir, dinamik süreçler ile karar alma süreçlerinin daha iyi anlaşılmasını sağlar ve nihayetinde teslimat sürelerini ve maliyetleri azaltarak son kullanıcılara fayda sağlar (Poler, 2010).

İşbirliği, farklı sektör, proje ve takımlar arasında ortak çalışmayı sağlayarak, kuruluşların beceri ve kaynak eksikliklerinin karşılanmasına yardımcı olmaktadır. Bu karşılıklı etkileşim,

kuruluşlarda yeni fikirlerin gün yüzüne çıkmasını, yenilikçi yaklaşımı ve personel bağlılığını desteklemektedir (Kemp, 2022). İşbirliği, personelin kurumda tutulabilmesini teminen kuruluş içerisinde farklı iş deneyimlerine imkân sağlayarak personelin değişim oranını azaltır. Böylece bilgi, yetkinlik ve deneyimin kurum içinde sürekliliği korunarak kuruluşun dayanıklılığında rol oynar (Kemp, 2022).

Camarinha-Matos ve Afsarmanesh (2005), iş birliği süreçlerinin kurulmasının ortaklar arasında iletişimi, koordinasyonu ve iş birliğini geliştirdiğini ve bunun da kesintiye neden olan olayların yönetilmesini kolaylaştırdığını savunmaktadır. İşbirliği içinde çalışan ekipler, farklı iş faaliyetlerinin daha hızlı entegrasyonunu kolaylaştırabilir, iletişimi iyileştirebilir, bilgi paylaşımını artırabilir ve diğer avantajların yanı sıra iş görevlerinde esneklik sağlayabilir (PMI, 2018). İşbirliği, kendi başına dayanıklılığı sağlayamaz; bunun olması için iş birliğini gerçekleştiren aktörler arasında dayanıklılık bakış açısının da ağ genelinde benimsenmesi ve uygulanması gerekmektedir (Arizzi vd., 2014).

Kurumsal iş birlikleri ve ortaklık stratejisi, uluslararası düzeyde, sektörel düzeyde ya da kuruluşlar düzeyinde, aynı ya da çapraz düzey bağlantılar kurulmasını desteklemektedir. Aktörler arasında karşılıklı güvene dayalı bilgi paylaşımı ve karar alma süreçlerinde şeffaflık söz konusudur. İşbirlikleri yalnızca ortak bir amaç üzerine oluşturulmakla birlikte, başka alanlardaki iş birlikleri aracılığıyla uzun soluklu da devam edebilir. Taraflar açısından insan kaynağı, bilgi, teknoloji ve hammadde ve malzeme bakımından çeşitliliği sağlar. Ayrıca iş birliğine dâhil olan aktörler birlikte öğrenerek ve deneyimlerini paylaşarak kurumsal kapasitelerini geliştirirler.

İş birlikleri ve ortaklık stratejisine ilişkin çeşitli uygulama örnekleri aşağıda yer almaktadır.

- Üniversiteler ve araştırma kurumlarıyla bilgi geliştirme ortaklıkları kurulması.
- Büyük çaplı projelerde finansman, bilgi ve işgücü bağlamında iş birliği ve ortaklıklar kurulması.
- Tedarikçiler ve lojistik firmalarıyla alternatif planlama üzerine mutabakat anlaşmaları yapılması.
- Sektörel çatı örgütlerle afet ve kriz yönetimi konularında iş birliği protokolleri oluşturulması.

- Finansal kuruluşlarla kriz zamanlarında kullanılabilecek kredi kolaylıkları veya destek paketleri üzerinde mutabakata varılması.
- Teknoloji firmalarıyla dijital dönüşüm ve uzaktan çalışma altyapısının güçlendirilmesine yönelik ortak çalışmalar yapılması.
- Enerji ve altyapı sağlayıcılarıyla hizmet sürekliliğini sağlamak üzere risk senaryolarına dayalı iş birliklerinin yapılandırılması.

4.3.2.5. Kapasite Geliştirme

Eisinger (2002), kurumsal kapasiteyi bir kuruluşun misyonunu gerçekleştirmesini sağlayan özellikler kümesi olarak tanımlamakta ve her kuruluşun, bu özelliklerden oluşan benzersiz bir “kapasite profili”ne sahip olduğunu ifade etmektedir. Singh vd. (2024), anılan kapasiteyi kuruluşların hedeflerine ulaşabilmek amacıyla değişen koşullara uyum sağlayarak “kaynak, yapı ve süreçlerini etkin ve verimli bir şekilde kullanabilme kabiliyetleri” şeklinde tanımlamaktadır.

Söz konusu kabiliyetlerin geliştirilmesi, kurumsal kapasite geliştirmeye yönelik çalışmalarla sağlanır. Teknolojik altyapı, operasyonel prosedürler, insan kaynakları, finansal istikrar ile kurumsal kültürden oluşan bu kapasite kuruluşun karşılaştığı zorluklara yanıt verebilmesi ile uzun vadeli başarısına destek olur. Kapasite geliştirme faaliyetleri yetenek geliştirme, bilgi birikimi ve ilave olarak süreç optimizasyonu aracılığıyla bu alanları güçlendirir, böylece kuruluşların karşılaştıkları belirsizlik ve karmaşıklık durumlarını yönetebilmelerine ilişkin gerekli olan donanımı edinmelerinde rol oynar (Michaela, 2023). Kapasite geliştirme, kuruluşların değişim ve yeniliğe uyumu ile zorlukları aşabilmesi perspektifinden önemli bir konumdur (Singh vd., 2024).

Lengnick-Hall ve Beck (2009), dayanıklılık kapasitesini “kuruluşun kesintileri absorbe etme, kesintilerden kurtulma ve kesintilere uyum sağlama yeteneği” olarak tanımlamakta ve dayanıklılık kapasitesinin, kuruluşların operasyonel süreklilik ile uzun vadede görünebilir olmalarına imkân tanıdığını belirtmektedir. Dayanıklılık kapasitesi, kuruluşların sahip olduğu kaynakları, stratejik planlamalarını ve uyum çalışmalarını güçlendirmekte; beklenmedik sorunları aşmalarını sağlamaktadır (Lengnick-Hall vd., 2011). Geliştirilmiş bir dayanıklılık kapasitesi, yaşanan olumsuz durumları kuruluşun yenilenmesi ve büyümesi bakımından fırsatlara dönüştürebilir (Pessina, 2021).

Zhou vd. (2023), dayanıklılık kapasitesini geri ve ileri yönlü sıçrama yetkinliği şeklinde açıklamaktadır. Yazarlar, bahse konu yetkinlikleri “kesintilerden hızlı bir şekilde kurtulmayı” sağlayan geri yönlü dayanıklılık ile “krizlerin ardından kuruluşların gelişmesini ve rekabet konumunu güçlendirmesini” sağlayan ileri yönlü dayanıklılık olarak açıklamaktadır.

Esneklik, dayanıklılık kapasitesini etkileyen bir faktör olarak, kuruluşların kendi yapı, strateji ve faaliyetlerini dışsal zorluklara karşı hizalamalarını sağlaması bakımından önem arz etmektedir (Nasab vd., 2023). Etkin bir risk yönetimi, kuruluşların olası tehditlere karşı hazırlıklı olmalarını sağlayarak kurumsal dayanıklılığı güçlendirmektedir (Tjahyono vd., 2024).

Tedarik zincirinin çeşitlendirilmesi ve acil durum rezervlerinin oluşturulması ile operasyonel sistemler gibi kaynaklara yönelik yedekliliğin sağlanması, kuruluşların kriz durumlarında iş sürekliliğini sağlama kabiliyetlerini artırır (Nasab vd., 2023). Güçlü liderlik yapısı, hazırlık ve öngörü süreçleri ile uyum kültürünü destekleyerek dayanıklılığın sağlanmasında rol oynar (Douglas, 2021). İşbirliği ve sektörel ağlara katılım sağlanmasını kapsayan sosyal sermaye, kuruluşların kesinti ve aksaklıklar sırasında dış kaynak ile desteğe ulaşmalarını sağlar (Khin Khin Oo & Rakthin, 2022). Dijital yetkinlikler, kuruluşların riskleri tespit etme, krizlere müdahale etme becerileri ile operasyonel verimliliklerini artırır (Singh, 2022).

Öğrenme ve bilgi yönetimi, kuruluşların geçmişteki başarısızlıklarından edindikleri bilgileri korumalarına, kriz sonrasında değerlendirmeler yapmalarını ve müdahale yetkinliklerini geliştirmelerini mümkün kılarak dayanıklılık kapasitesinin güçlendirilmesine katkıda bulunur (Khan vd., 2019).

Kuruluşlar, hazırlık ve uyum kabiliyetlerini güçlendiren proaktif stratejileri izleyerek dayanıklılık kapasitelerini iyileştirebilir. Yapılandırılmış rutinler ile acil durum planları kuruluşların aksaklık ve kesintilere etkili yanıtlar vermelerini sağlar.

Dış çevrenin taranması ve risk değerlendirme yetkinliklerinin geliştirilmesi, kuruluşların tehditleri öngörebilmesini ve bunlara yönelik önleyici kontroller geliştirmesini sağlar (Lengnick-Hall & Beck, 2009). Hizmet içi eğitime ağırlık verilmesi, çalışanların krizleri yönetmeleri, bilinçli kararlar almaları ve dayanıklılığa katkı sunmalarına yönelik ihtiyaç duyulan becerileri kazandırır (Siddiqui, 2017).

Alternatif tedarikçiler ile çeşitlendirilmiş gelir akışlarının sürekliliğinin sağlanması gibi uygulamalar yoluyla kaynak yedekliliğinin güçlendirilmesi, operasyonel kesintilerin önüne

geçilmesi açısından önem taşır (Nasab vd., 2023). Sektördeki diğer aktörler ile devlet ve araştırma kurumlarıyla dış ortaklıkların güçlendirilmesi, ihtiyaç duyulan kaynaklara erişime imkân tanır (Pinkwart vd., 2022).

Kurumsal iş birliği ve ağları ile risk farkındalığı ve inovasyonu destekleyen bir kurumsal kültürün oluşturulması, belirsizlik durumlarında kararlılığı sağlar. Senaryo çalışmaları ile kriz sonrası değerlendirmeler gibi kurumsal öğrenmeyi güçlendiren uygulamalar, kuruluşların dayanıklılık stratejileri ile olumsuz olaylara verecekleri yanıtların geliştirmelerinde destekleyici bir rol üstlenir (Khan vd., 2019). Kuruluşlar, söz konusu stratejiler vasıtasıyla, kesinti ve aksaklıkları başarılı bir şekilde yönetmeleri, risklerini azaltmaları ve uzun vadede başarılarını sürekli kılmaları için gerekli dayanıklılık kapasitesini geliştirebilirler (Lengnick-Hall & Beck, 2009).

Kurumsal kapasite geliştirme stratejisi, kuruluşun şoklara karşı hazırlıklı olmasını, mevcut kaynaklarını etkin yönetebilmesini ve olağanüstü durumlarda daha az zararla toparlanabilmesini sağlar. Bu strateji, dayanıklılığın “özümseme”, “uyum sağlama” ve “dönüşüm” boyutlarını doğrudan destekler. Ayrıca uzun vadeli rekabet avantajı, iş sürekliliği, kurumsal güven ve paydaş memnuniyeti açısından da yüksek katma değer üretir.

Dayanıklılık kapasitesinin geliştirilmesi stratejisi, çok geniş kapsamlı bir stratejidir. Nihayetinde gölge personel uygulamasından finansal risklerin azaltılmasına yönelik swap işlemlerine, kuruluşa yedek su deposu konulmasından kalite yönetim sistemlerinin uygulanmasına ve düzenli ekipman bakımından teknolojinin güncellenmesine değin her türlü eylem, bu stratejinin kapsamına girmektedir.

Aşağıda tematik başlıklar altında bu strateji kapsamında uygulama örneklerine yer verilmektedir.

1. Liderlik ve Yönetişim Gelişimi

- Liderlik gelişim programlarının uygulanması.
- Orta ve alt kademe yöneticilere stratejik karar yetkisi verilerek merkeziyetin azaltılması.
- Kriz dönemlerinde hızlı karar alma yetkisi olan liderlik ekiplerinin oluşturulması.
- Şeffaf, hesap verebilir ve kapsayıcı karar alma mekanizmalarının kurulması.
- Kurum içi yönetişimde esnek hiyerarşik yapının teşvik edilmesi

- Afet ve acil durumlara yönelik yönetim yapılarının belirlenmesi.

2. İnsan Kaynaklarının Güçlendirilmesi

- Kriz dönemlerinde görev kaydırmalarına imkân sağlayacak esnek iş gücü yapısının oluşturulması.
- Personelin kriz yönetimi ve stresle başa çıkma becerileri üzerine eğitilmesi.
- Kritik görevlerde görev alabilecek yedek insan kaynağının belirlenmesi.
- Çalışanlara psikososyal destek hizmetlerinin sunulması.

3. Bilgi ve İletişim Sistemlerinin Güçlendirilmesi

- Kriz anlarında tüm paydaşlarla hızlı bilgi paylaşımını sağlayan sistemlerin kurulması.
- Erken uyarı sistemlerinin geliştirilmesi ve entegre edilmesi.
- İç iletişimi destekleyecek dijital platformların kullanılması.
- Gerçek zamanlı veri toplama ve analiz kapasitesinin oluşturulması.
- Kriz iletişim protokollerinin yazılı hale getirilerek düzenli tatbikatlarla test edilmesi.

4. Fiziksel ve Teknolojik Altyapının Geliştirilmesi

- Kurum içi altyapının modernize edilmesiyle hizmet ve üretim kapasitesinin artırılması.
- Afet ve acil durumlara karşı dayanıklı bina ve tesislerin inşa edilmesi.
- Kritik sistemler için jeneratör, su depoları gibi yedek altyapıların sağlanması.
- Teknolojik altyapının uzaktan erişim ve çalışma sistemlerine uygun hale getirilmesi.
- Güvenlik açıklarını azaltmak için bilgi teknolojileri altyapısının güçlendirilmesi.
- Fiziksel altyapıda alternatif ulaşım ve iletişim yollarının planlanması.

5. Kurumsal Yapının Gözden Geçirilmesi

- Organizasyon yapısının karmaşıklığını azaltacak şekilde yalınlaştırılması (hiyerarşi basamaklarının azaltılması).

- Görev tanımlarının netleştirilmesiyle iş tekrarlarının ve sorumluluk belirsizliklerinin önüne geçilmesi.
- Kriz anlarında hızlı hareket etmeyi sağlayacak esnek organizasyon yapılarının tasarlanması.
- Birimler arası koordinasyonu güçlendirecek yatay yapılanmaların teşvik edilmesi.
- Yetki ve sorumlulukların yeniden dağıtılmasıyla karar süreçlerinin hızlandırılması.
- Kurum içi görev tanımlarının kriz dönemlerine uygun olarak revize edilmesi.

6. Kurum İçi Unsurlar Arasında Bağlantıların Güçlendirilmesi

- Yatay ve dikey iletişim kanallarının güçlendirilmesi, kolaylaştırılması
- Ortak kurumsal hafıza oluşturulmasını teminen bilginin dokümente edilmesi ve paylaşılması
- Bilgi teknolojileri, insan kaynakları, tedarik ve operasyon birimlerinin ortak kriz senaryoları üzerinde çalışması.
- Farklı departmanlar arası veri paylaşımını sağlayacak entegre dijital platformların kullanılması ve birbirleriyle entegre çalışmasının sağlanması
- Kurum içi iş akış süreçlerinin yatay bağlantılar kuracak şekilde yeniden düzenlenmesi.
- Çalışan rotasyon sistemleriyle farklı birimlerin işleyişi hakkında bilgi edinilmesinin sağlanması.

7. Yönetim Araçlarının Kullanılması

- İSY, KRY, iç kontrol vb. sistemlerinin kurulması ve işler hale getirilmesi
- GZFT, PESTLE ve risk matrisi gibi analiz yöntemleriyle dayanıklılık açıklarının sistematik biçimde belirlenmesi.
- Risk değerlendirme araçlarının, tedarik zinciri sürekliliği ve personel yönetimi gibi alanlara uygulanması.
- Karar destek sistemlerinin senaryo analizleriyle desteklenerek belirsizlik ortamında rehberlik etmesi.

8. Süreç Geliştirme ve Standardizasyon

- Kritik iş süreçlerinin analiz edilerek sadeleştirilmesi ve hızlandırılması.
- Afet ve kriz senaryolarına özel operasyonel süreçlerin standartlaştırılması.
- Yedekli süreçlerin oluşturularak operasyonel sürekliliğin sağlanması.
- Süreç iyileştirme çalışmaları için iç denetim ve geri bildirim mekanizmalarının kurulması.
- Ulusal ve uluslararası standartlara uygun süreç yönetimi uygulamalarının benimsenmesi.

9. Performans ve İzleme Sistemlerinin Kurulması

- Krizlere hazırlık ve müdahale performansını ölçen göstergelerin geliştirilmesi.
- Kurum genelinde faaliyetlerin izlenmesini sağlayacak performans göstergeleri ve geri bildirim mekanizmaları geliştirilmesi.
- Sürekli geri bildirim toplanarak performans değerlendirme süreçlerinin güncellenmesi.
- Süreç iyileştirmeye katkı sağlayacak iç denetim ve öz değerlendirme sistemlerinin hayata geçirilmesi.
- Kurumsal stratejik hedeflerle uyumlu performans kriterlerinin belirlenmesi.
- İzleme sistemlerinin erken uyarı mekanizmalarıyla entegre çalışmasının sağlanması.

10. Finansal Kapasitenin Artırılması

- Acil durum fonlarının oluşturulması ve güncellenmesi.
- Nakit akışı senaryoları ile kriz hazırlığı yapılması.
- Finansal kaynak çeşitliliğinin artırılması (kredi, finansal araçlar vb.).
- Esnek bütçeleme sistemlerinin geliştirilmesi.

11. İşbirlikleri ve Dış Paydaş Katılımı

- Yerel yönetimlerle afet planlama iş birlikleri yapılması.
- Alternatif tedarik zinciri senaryolarının birlikte planlanması.

- Mevzuat deęiřikliklerinin takibi ve kurumsal uyum iin kamu ile iř birlięi yapılması.

12. Kurumsal ğrenme ve Bilgi Yönetimi

- Kriz sonrası deęerlendirme toplantıları düzenlenmesi.
- Geri bildirimlerin deęerlendirilmesi ve dokümanite edilerek gereklerinin yerine getirilmesi.
- Dijital bilgi yönetimi sistemlerinin kurulması.
- Kurumsal hafıza arřivlerinin oluřturulması.
- Sürekli ğrenmeye yönelik kurum ii eęitim platformlarının kurulması

13. Kurumsal Kltr ve Deęerlerin Gçlendirilmesi

- Dayanıklılık odaklı kurum ii deęerlerin tanımlanması.
- Kurum iinde gvene dayalı iletiřimi teřvik eden liderlik uygulamaları.
- alıřan katılımını artırmaya yönelik politikalarının uygulanması.
- Dayanıklılıęı vurgulayan i iletişim kampanyaları hazırlanması.

14. Mevzuat ve Düzenlemelere Uyumun Gçlendirilmesi

- Kriz zamanlarında deęiřen yasal yükümlölüklerin yakından takip edilmesi ve iř süreçlerinin hızla güncellenmesi.
- Zorunlu sertifikasyon ve standartlara uyumun saęlanması.
- alıřanlara yönelik periyodik uyum eęitimi düzenlenmesi.
- Faaliyetlerin yasal risk analizine tabi tutulması.
- Dijital dönüşüm sürecinde kiřisel verilerin korunması ve bilgi gvenlięi aısından yasal yükümlölüklere tam uyum saęlanması.
- Uyum kontrollerinin i denetim sürecine entegre edilmesi.

15. Tedarik ve Lojistik Kapasitesinin Geliřtirilmesi

- Alternatif tedarik zincirlerinin planlanması
- Kritik malzemeler iin minimum stok seviyelerinin artırılması

- Tedarikçilerle esnek sözleşme modellerinin uygulanması
- Lojistik firmalarıyla acil durum planlarının koordine edilmesi

4.4. Durum Türüne Göre Risk ve Dayanıklılık Stratejilerinin Belirlenmesi

Olumsuz durumların türü, kuruluşların hangi risk ve dayanıklılık stratejilerini ne şekilde kullanmaları gerektiğini doğrudan etkiler. Çünkü her tehdit, risk veya belirsizlik türü, farklı dinamiklere, yayılım biçimlerine ve kontrol edilebilirlik düzeylerine sahiptir. Bu nedenle strateji seçimi aynı zamanda olumsuz durumun niteliğine ve öngörülebilirliğine göre şekillenmelidir.

Bu bölümde, olumsuz durumlar yedi temel sınıfa ayrılarak her bir sınıfa uygun risk stratejileri (RS) ve bu stratejileri destekleyici dayanıklılık stratejileri (DS) sistematik biçimde ele alınmaktadır. Amaç, her durum türüne özgü müdahale yaklaşımlarının ortaya konulması ve karar vericilere uygulamaya yönelik yönlendirmenin sağlanmasıdır. Ancak anılan durum ve strateji eşleştirmelerinin, karşılaşılan olumsuz durumun özgün mahiyeti doğrultusunda esneyerek farklı eşleştirme kombinasyonlarına da imkân tanıyacağı hususu göz ardı edilmemelidir. Bu bölümde yapılan eşleştirmeler jenerik olmakla birlikte, planlayıcıların daha kapsamlı bir bakış açısına sahip olmalarını sağlamak üzere gerçekleştirilmektedir.

Durum türüne göre risk ve dayanıklılık stratejilerinin belirlenmesi süreci, organizasyonların karşılaştıkları olumsuz durumlara yönelik en uygun yanıtları seçmelerini sağlayarak kaynakların etkin kullanımını ve müdahalelerin başarısını artırır. Farklı olumsuz durum sınıfları; sahip olunan bilgi düzeyi, öngörülebilirlik, etki hızı ve yayılım kapasitesi bakımından farklı özellikler taşır. Bu nedenle her durum türü için tek tip bir strateji kullanmak yerine, bağlama özgü risk stratejileri ve bunları destekleyen dayanıklılık stratejilerinin seçilmesi gerekir. Sistematik bir belirleme süreci, strateji seçiminde subjektif yargılardan kaynaklanabilecek hataları azaltır, karar verme sürecini standartlaştırır ve olay öncesi, anı ve sonrası fazlarda stratejilerin doğru zamanda devreye alınmasını kolaylaştırır. Ayrıca, bu yaklaşım olumsuz durumlara karşı proaktif planlama yapılmasını destekleyerek kurumun genel dayanıklılık kapasitesini güçlendirir.

Durum türüne göre risk ve dayanıklılık stratejilerinin belirlenmesi süreci, karar vericilerin farklı olumsuz durum tiplerine uygun, etkili ve uyumlu stratejileri seçerek uygulamasını sağlayan sistematik bir yaklaşımdır. Sürecin ilk adımında olumsuz durumlar

sınıflandırılarak, her sınıf türü için en uygun risk stratejileri belirlenmektedir. Ardından seçilen risk stratejileri ile bu stratejileri destekleyecek dayanıklılık stratejileri eşleştirilmektedir. Üçüncü adımda belirlenen stratejilerin olayın üç temel fazında—olay öncesi (hazırlık), olay anı (müdahale) ve olay sonrası (toparlanma)—nasıl devreye alınacağı planlanmaktadır. Son olarak teorik çerçeve uygulama örnekleriyle desteklenerek farklı olumsuz durum senaryolarında stratejilerin nasıl hayata geçirileceği gösterilmektedir.

4.4.1. Olumsuz Durum Türleri Çerçevesinde Risk Stratejilerinin Seçilmesi

Kuruluşların karşı karşıya kaldığı olumsuz durumların niteliği, bu durumlara karşı geliştirilecek stratejilerin belirlenmesinde kritik rol oynamaktadır. Bu bağlamda risklerin yanında, genel tehditler, genişleyen tehditler, örtük tehditler, beliren tehditler, muğlaklık ve belirsizlik ile cehalet gibi kuruluşların karşılaşabileceği olumsuz durum sınıflarının da dikkate alınması gerekmektedir.

Literatür, ilgili standart ve çerçeveler ile iş hayatında, risk bağlamında ele alınmalarından ötürü “risk stratejileri” olarak adlandırılan stratejiler, temelde kuruluşların karşılaşabileceği olumsuz durumlarla başa çıkmalarında yol gösterici olması amacıyla geliştirilmişlerdir. Ancak bu stratejilerin yalnızca risklerle sınırlı kalmayıp, farklı türdeki olumsuz durumlara karşı da önleyici ve koruyucu işlev görebileceği değerlendirilmektedir. Bu bölümde, anlaşılabilirliğin sağlanması ve yerleşik terminolojinin korunması amacıyla söz konusu stratejiler yine “risk stratejileri” ifadesiyle anılacaktır; fakat kapsam itibarıyla tüm olumsuz durum türlerine uygulanacaktır.

Olumsuz durum sınıflarında, karar vericinin durum hakkında sahip olduğu bilginin niteliği ve miktarı değişkenlik göstermektedir. Örneğin, risk ve genel tehdit sınıflarında mevcut bilgi düzeyi genellikle yüksek olup, geçmiş veriler, istatistikler ve önceki olay deneyimleri karar sürecini destekler. Buna karşın, beliren tehditler, örtük tehditler veya muğlaklık ve belirsizlikler gibi sınıflarda mevcut bilgi seviyesi giderek azalmaktadır.

Karar vericinin geçmiş veriler, istatistikler, olay kayıtları ve deneyimlerle desteklenen kapsamlı bilgiye sahip olduğu durumlarda, sekiz risk stratejisi de (kaçınma/sonlandırma, azaltma, transfer, kabul, paylaşma, ayırma, kopyalama ve çeşitlendirme) uygulanabilir. Bu bilgi seviyesi, risk ve genel tehditlerin niteliği, olasılığı ve etkisi hakkında güvenilir öngörüler yapılmasını sağlar; böylece strateji seçiminde geniş bir esneklik elde edilir. Örneğin, riskin tamamen ortadan kaldırılabilirdiği durumlarda kaçınma, etkilerin hafifletilebileceği durumlarda

azaltma, yükün paylaşılabileceği veya devredilebileceği durumlarda transfer ve paylaşma stratejileri tercih edilebilir. Ayrıca sistemin yeniden yapılandırılmasını gerektiren durumlarda ayırma, kopyalama ve çeşitlendirme stratejileri de kolaylıkla planlanabilir ve uygulanabilir.

Mevcut bilgi kısmen yeterli olsa da olumsuz durumun yayılma hızı, etki alanının büyüklüğü veya çoklu etkiler yaratma potansiyeli nedeniyle belirsizlik oranı artar. Bu seviyede genellikle azaltma, transfer, paylaşma, çeşitlendirme ve ayırma stratejileri ön plana çıkar. Azaltma, tehdidin etkilerini yayılmadan önce sınırlamak için kritik olurken; transfer ve paylaşma, yükün başka taraflara dağıtılmasına ve müdahale kapasitesinin artırılmasına olanak tanır. Çeşitlendirme, tek bir kaynağa veya sürece bağımlılığı azaltarak olası yayılma etkilerini sınırlarken; ayırma stratejisi ise kritik bileşenlerin birbirinden izole edilerek tehditte etkilenme riskinin düşürülmesini sağlar. Ancak, tehdidin hızla değişebilen doğası nedeniyle kaçınma veya kabul stratejileri bu seviyede daha az uygulanabilir hale gelir.

Düşük bilgi seviyesi durumunda, mevcut bilgi sınırlı, sinyaller zayıf veya hiç yoktur. Bu durumlarda, belirsizlik yüksek olduğundan strateji seçimi daha çok esneklik ve adaptasyon kapasitesine dayanır. Azaltma, etkilerin olası en kötü senaryolara göre sınırlandırılmasına yönelik önlemleri içerir; paylaşma, belirsizlikten doğan yükün farklı aktörler arasında bölünmesine imkân verir. Ayırma, sistemin potansiyel tehditte korunacak kısımlarını izole ederek kritik işlevlerin devamlılığını sağlar. Kopyalama, kritik unsurların birebir yedeklerini oluşturarak ani kayıplara karşı hızlı toparlanma kapasitesi kazandırır. Çeşitlendirme, alternatif kaynak, süreç ve pazarlar üzerinden belirsizliğin etkilerini dağıtarak riski yayar. Bu seviyede, bilgi eksikliğinin yüksek olması nedeniyle kaçınma veya transfer stratejileri sınırlı fayda sağlar; çünkü tehdidin veya riskin doğası tam olarak bilinmediği için bu stratejilerin uygulanabilirliği düşer.

Söz konusu durum sınıfları çerçevesinde kullanılabilecek jenerik risk strateji önerileri ile bu önerilerin dayanak noktaları Tablo 13'te kısaca açıklanmaktadır. Tabloda her bir sınıf için önerilen strateji seti içerisinden uygun olanının mümkün olduğunca objektif kurallar ve temel değerlendirme kriterleri doğrultusunda belirlenmesi önem arz etmektedir.

Bu doğrultuda olumsuz durumun yaratacağı etkinin seviyesi, bir tercih kriteri olarak değerlendirilebilir. *Etki seviyesi*, bir olumsuz durumun gerçekleşmesi halinde kuruluş üzerinde yaratacağı etkinin büyüklüğünü ifade eder. Bu etki; finansal kayıplar, operasyonel kesintiler, itibar zedelenmesi veya stratejik hedeflerden sapma gibi farklı boyutlarda ortaya çıkabilir. *Kontrol edilebilirlik düzeyi* ise olumsuz durumun meydana gelme süreci üzerindeki içsel veya

dışsal kontrol imkânlarını tanımlar. Bu kriter, kuruluşun söz konusu duruma ne ölçüde müdahale edebileceğini, risklerin gerçekleşme olasılığını azaltacak önlemlerin ne kadar etkin uygulanabileceğini ortaya koyar.

Tablo 13: Olumsuz Durum Sınıflarına Yönelik Risk Stratejileri

Olumsuz Durum Sınıfları	Kullanılabilecek Risk Stratejileri	Gerekçe
1. Risk ve 2. Genel Tehditler	Kaçınma / Sonlandırma, Azaltma, Transfer Etme, Kabul Etme, Paylaşma, Ayırma, Kopyalama, Çeşitlendirme	Bu sınıflar genellikle tanımlanabilir, ölçülebilir ve yönetilebilir niteliktedir. Önleyici olarak olumsuz durumdan tamamen kaçınmak veya sona erdirmek mümkündür. Etki azaltma ve transfer yoluyla yük paylaşılabilir. Kabul etme stratejisi, düşük etkili ve yönetilebilir durumlarda uygulanabilir. Ayırma ve kopyalama ile etkilenebilecek bileşenler korunur. Çeşitlendirme, tek bir kaynağa bağımlılığı azaltarak direnç sağlar.
3. Genişleyen Tehditler	Azaltma, Transfer, Paylaşma, Çeşitlendirme, Ayırma,	Bu tehditler yayılma, büyüme ve çoklu etki yaratma potansiyeli taşır. Azaltma ile büyüme hızı ve etki çapı sınırlanır. Transfer ve paylaşma, yükün tek bir noktada yoğunlaşmasını engeller. Çeşitlendirme ile etkilenen alan dışındaki alternatifler kullanılarak süreklilik sağlanır. Ayırma, tehditten etkilenen kısmın izole edilerek yayılmanın önlenmesini mümkün kılar.
4. Beliren Tehditler	Azaltma, Paylaşma, Ayırma, Kopyalama, Çeşitlendirme	Bu tehditler aniden ortaya çıkar ve hızlı etki yaratır. Azaltma ile doğrudan etki kontrol altına alınır. Paylaşma, yükün dağıtılmasını sağlar. Ayırma, tehdit alanının sistemden izole edilmesine olanak tanır. Kopyalama, kritik unsurların yedekleriyle süreklilik sağlar. Çeşitlendirme, farklı kaynaklar veya yollar üzerinden operasyonun devamını mümkün kılar.
5. Muğlaklık ve Belirsizlikler	Kaçınma / Sonlandırma, Azaltma, Kabul Etme	Muğlaklık ve belirsizlikler tanımlanabilirler, ancak ölçülemezler. Önleyici olarak durumdan tamamen kaçınmak veya sona erdirmek mümkündür. Kuruluş, elinde başka seçenek olmadığında, bu durumu kabul edebilir. Belirsizliğin mahiyeti, zaman içinde duruma ilişkin sahip olunan bilginin artması yoluyla öngörülebilir hale gelebilir. Böyle durumlarda diğer stratejiler de değerlendirilebilir.
6. Örtük Tehditler	Azaltma, Paylaşma, Çeşitlendirme	Bu tehditler uzun süredir var olan ancak fark edilmeyen olumsuz durumlardır, önleyici olarak bilinç artırma ve kapasite geliştirme gerekir. Tespit edilebilirlerse, azaltma, tespit sonrası etkisini en aza indirir. Paylaşma, etkilerin tek bir kurum/alan üzerinde yoğunlaşmasını engeller. Çeşitlendirme, tek bir kritik kaynağa bağımlılığı azaltarak tehdidin tetiklenmesi halinde zarar boyutunu sınırlar.
7. Cehalet	Azaltma, Paylaşma, Kabul	Cehalet durumunda olumsuz durumun farkında olunmadığından önleyici olarak bilinç artırma ve kapasite geliştirme gerekir.

Etki yayılımı ve zincirleme risk yaratma potansiyeli, bir olayın sadece kendi sınırları içinde kalmayıp sistemin diğer bölümlerine yayılma ve ikincil riskleri tetikleme kapasitesini gösterir. Bu tür olaylar genellikle domino etkisiyle daha geniş kapsamlı ve karmaşık bir risk zinciri yaratabilir. *Kaynak yeterliliği* ise olumsuz durumun yönetilmesi için gerekli insan gücü, zaman, finansman, teknik altyapı ve organizasyonel kapasitenin mevcut olup olmadığını ortaya koyar. Yetersiz kaynak, doğru stratejiler belirlense dahi etkin uygulamanın önünde ciddi bir engel oluşturabilir.

Etkilerin kalıcılığı, olumsuz bir durumun etkisinin kısa vadeli ve geri döndürülebilir mi, yoksa uzun vadeli ve kalıcı mı olduğunun belirlenmesini sağlar. Kısa süreli etkiler çoğu zaman sınırlı müdahalelerle ortadan kaldırılabilirken, kalıcı etkiler kuruluşun yapısal dönüşümler gerçekleştirmesini zorunlu kılabilir. *İştah ve tolerans seviyeleri* ise kuruluşun olumsuz duruma yönelik yaklaşımını somutlaştırır. Risk iştahı, hangi ölçüde risk üstlenilebileceğini belirlerken; risk toleransı, kabul edilebilir sınırları ortaya koyar ve bu sınırların aşılması halinde hangi stratejik yanıtların verilmesi gerektiğini belirler.

Öngörülebilirlik, bir olayın sonuçlarının ne ölçüde öngörülebilir olduğunu gösterir. Öngörülebilirliği yüksek olaylar için önceden hazırlık yapmak mümkünken, öngörülemez olaylar daha esnek ve senaryo tabanlı stratejiler gerektirir. *Yasal zorunluluklar* ise strateji seçiminde bağlayıcı dışsal faktörlerdir. Bazı olumsuz durum türlerinde, mevzuat veya düzenleyici kurumlar nedeniyle belirli stratejilerin uygulanması kuruluşun tercihindan bağımsız olarak zorunludur.

Bir diğer kriter olan *dışa bağımlılık yaratma potansiyeli*, bir olayın kuruluşun dış kaynaklara olan bağımlılığını artırma riski taşıyıp taşımadığını değerlendirmeyi mümkün kılar. Bu durum özellikle tedarik zinciri, teknoloji altyapısı veya kritik hizmet sağlayıcılar açısından stratejik kırılganlık yaratabilir. Strateji belirleme sürecinde dışa bağımlılığı artıran seçeneklerden kaçınılması veya bu bağımlılığın çeşitlendirme yoluyla dengelenmesi, uzun vadeli sürdürülebilirlik için kritik bir gerekliliktir.

Risk stratejilerinin seçiminde kullanılan kriterler, karar sürecinin doğruluğunu ve uygulanacak stratejinin etkinliğini doğrudan etkiler. Söz konusu kriterler, olumsuz durumun özelliklerini çok boyutlu analiz ederek rastgele veya tek boyutlu yaklaşımların önüne geçer. Böylece strateji seçimi öznel değerlendirmelerden arındırılarak olgusal temellere dayandırılır. Bu sayede belirlenen stratejiler hem teorik olarak doğru hem de pratikte uygulanabilir hale gelir.

4.4.2. Risk Stratejileri ile Dayanıklılık Stratejilerinin Eşleştirilmesi

RS'lerin tek başına uygulanması çoğu zaman olumsuz durumun tüm etkilerini yönetmek için yeterli değildir. Bu nedenle, her bir RS'nin, onu güçlendirecek destekleyici DS'ler ile birlikte tasarlanması kritik öneme sahiptir. Bahse konu eşleştirme süreci, belirli bir risk stratejisinin uygulanabilirliğini destekleyecek, güçlendirecek ve etkinliğini artıracak uygun dayanıklılık stratejilerinin sistematik olarak tanımlanmasına dayanmaktadır. Amaç, karar alma sürecinde belirsizlikleri azaltmak, stratejik uyumu güçlendirmek ve olay öncesi, olay anı ile olay sonrası aşamalarda uygulanabilecek tutarlı çözüm setleri oluşturmaktır.

Aşağıda her bir risk stratejisini destekleyecek uygun dayanıklılık stratejileri eşleştirilmekte ve bu eşleşmenin dayandığı temel açıklanmaktadır.

a) RS: Kaçınma Sonlandırma Stratejisi + DS: Çeşitlilik, Modülerlik Stratejileri

Kaçınma / sonlandırma stratejisi, olumsuz durumun kaynağının tamamen ortadan kaldırılması veya ilgili faaliyetlerin durdurulması yoluyla durumun bertaraf edilmesini hedefler. Bu strateji uygulanırken *çeşitlilik*, alternatif tedarikçi, pazar veya süreçlerin devreye alınarak belirli bir olumsuz durumun kaynağına olan bağımlılığı azaltır. *Modülerlik*, olumsuz durum oluşturma potansiyeli taşıyan unsurların sistemin geri kalanından ayrılmasını sağlayarak hem operasyonel devamlılığı korur hem de olumsuz durumun diğer birim, süreç ve faaliyetlere yayılmasını engeller. Böylece kaçınma kararı, kuruluşun genel işleyişinde minimum bozulma ile hayata geçirilebilir.

b) RS: Azaltma Stratejisi + DS: Yedeklilik, Modülerlik, Kapasite Geliştirme Stratejileri

Azaltma stratejisi, olumsuz durumun olasılığını veya etkisini kabul edilebilir seviyeye indirmeyi amaçlar. *Yedeklilik*, kritik varlık ve süreçlerin alternatiflerini hazır tutarak olası kayıpların telafi edilmesini sağlar. *Modülerlik*, hasarın sistemin tamamına yayılmasını engelleyerek yalnızca etkilenen bölümün devre dışı bırakılmasına imkân tanır. *Kapasite geliştirme*, insan kaynağı, teknik altyapı ve süreç yetkinliklerini artırarak organizasyonun olay anındaki tepki hızını ve etkinliğini yükseltir. Bu kombinasyon, hem proaktif hem de reaktif önlemleri güçlendirir.

c) RS: Transfer Stratejisi + DS: Ağ / İşbirliği ve Ortaklık, Çeşitlilik Stratejileri

Transfer stratejisi, olumsuz durumun etkilerini finansal, operasyonel veya hukuki yollarla üçüncü taraflara devretmeyi hedefler. *Ağ / İşbirliği ve Ortaklık*, güvenilir iş ortakları ve tedarikçiler ile kurulan stratejik ilişkiler sayesinde olumsuz durumun paylaşımını ve yük dağılımını kolaylaştırır. *Çeşitlilik*, tek bir aktarım kanalına bağımlılığı azaltarak transfer sürecinde alternatif çözümler sunar. Bu sayede transfer edilen olumsuz durumun, tek bir tarafın başarısına veya kaynaklarına bağımlı kalmadan yönetilmesi mümkün olur.

d) RS: Kabul Stratejisi + DS: Kapasite Geliştirme, Yedeklilik Stratejileri

Kabul stratejisi, olumsuz durumun organizasyonun iştah ve toleransı içinde kalarak üstlenilmesini ifade eder. Bu durumda *kapasite geliştirme*, olası etkiler gerçekleştiğinde hızlı toparlanma ve adaptasyon için kritik önemdedir. *Yedeklilik*, kabul edilen olumsuz durumun yaratabileceği kayıpların telafisi için hazır yedek kaynaklar sunar. Böylece olumsuz durum kabul edilse bile organizasyonun direnç seviyesi korunur.

e) RS: Paylaşma Stratejisi + DS: Ağ / İşbirliği, Çeşitlilik Stratejileri

Paylaşma stratejisi, olumsuz durumun etkilerinin birden fazla taraf arasında bölüştürülmesini hedefler. *Ağ / iş birliği ve ortaklık*, ortak müdahale kapasitesini, kaynak paylaşımını ve maliyet bölüşümünü mümkün kılar. *Çeşitlilik*, olumsuz durumun farklı alanlara dağıtılmasını sağlayarak herhangi bir tekil paydaşın aşırı yük altında kalmasını önler. Bu yaklaşım, özellikle uzun süreli veya çok boyutlu risklerde dayanıklılığı artırır.

f) RS: Ayırma Stratejisi + DS: Modülerlik, Yedeklilik Stratejileri

Ayırma stratejisi, riskli unsurların fiziksel, operasyonel veya sistemsel olarak diğerlerinden izole edilmesini içerir. *Modülerlik*, sistemin bağımsız bileşenler halinde çalışmasını sağlayarak bir bölümdeki hasarın tüm sisteme yayılmasını önler. *Yedeklilik*, ayrılan bileşenlerin işlevlerinin başka kaynaklarla sürdürülmesini mümkün kılar. Böylece hasar, sınırlı bir alanda tutulur ve operasyon devamlılığı korunur.

g) RS: Kopyalama Stratejisi + DS: Yedeklilik, Modülerlik Stratejileri

Kopyalama stratejisi, kritik süreç, sistem veya varlıkların birebir yedeğini farklı lokasyonlarda veya platformlarda bulundurmaya ifade eder. *Yedeklilik*, aynı işlevi görecekt alternatif kaynakların sürekli hazır tutulmasını sağlar. *Modülerlik*, zarar gören kısmın hızla devre dışı bırakılarak kopyasının devreye alınmasını kolaylaştırır. Bu strateji, ani ve yüksek etkili olaylarda kesinti süresini minimize eder.

h) RS: Çeşitlendirme Stratejisi + DS: Çeşitlilik, Ağ / İşbirliği Stratejileri

Çeşitlendirme stratejisi, olumsuz durumun farklı alanlara dağıtılması yoluyla tekil bir tehditten kaynaklanan olumsuz etkileri sınırlamayı hedefler. *Çeşitlilik*, doğrudan bu stratejinin özünü oluşturarak bağımlılık durumunu azaltır. *Ağ / iş birliği ve ortaklık*, çeşitlendirilen kaynakların verimli kullanımını, yeni pazar ve tedarik kanallarının açılmasını ve destek ağlarının güçlendirilmesini sağlar. Böylece çeşitlendirme yalnızca pasif bir koruma değil, aynı zamanda aktif bir büyüme ve dayanıklılık geliştirme aracına dönüşür.

Jenerik bir eşleştirme, farklı senaryolarda kullanılabilecek standart bir referans çerçevesi sunarken, olumsuz durumun türü çerçevesinde filtrelenerek duruma özgü strateji kombinasyonlarının seçilmesine olanak tanır. Böylece, hem proaktif hazırlık sürecinde hem de kriz yönetimi ve toparlanma aşamalarında hızlı ve etkili müdahale sağlanır.

Diğer taraftan olumsuz durumun türü ve niteliği ile strateji seçiminde değerlendirilmesi gereken kriterler doğrultusunda kuruluşun karşılaştığı her bir olumsuz durum, özgün bir strateji seçimini gerektirir. Bu özgün seçim, anılan jenerik strateji kombinasyonlarını farklılaştırabileceği gibi, söz konusu jenerik stratejiler dışında kuruluşun faaliyet gösterdiği sektör, lokasyon gibi unsurlar ışığında da değişkenlik gösterebilir.

4.4.3. Olay Fazları ve Stratejilerin Devreye Alınması

Bu aşamada, belirlenen sekiz RS'nin her biri için uygulanabilecek destekleyici DS'ler ve bu stratejilerin olayın üç temel fazında – olay öncesi (hazırlık), olay anı (müdahale) ve olay sonrası (toparlanma) – nasıl devreye alınabileceği sistematik bir şekilde ifade edilmektedir. Amaç, yalnızca uygun RS-DS eşleşmelerini belirlemekle kalmayıp, aynı zamanda bu

eşleşmelerin zaman boyutu içerisinde hangi aşamada ve ne şekilde etkinleştirileceğini ortaya koymaktır.

Her bir faz, farklı hedef ve önceliklere sahip olduğundan, destekleyici dayanıklılık stratejilerinin kullanım şekli de değişkenlik göstermektedir. Her olumsuz durum üç temel fazda yönetilir:

1. **Olay öncesi (hazırlık):** Olumsuz durumun gerçekleşme ihtimalini azaltacak veya etkisini sınırlayacak önlemler devreye alınır.
2. **Olay anı (müdahale):** Meydana gelen olayın kontrol altına alınması, yayılımının durdurulması ve kritik süreçlerin korunması hedeflenir. Önceden hazırlanan bir beklenmedik durum planı varsa devreye alınır.
3. **Olay sonrası (toparlanma):** Yönetim, olay sonrasında onarım / restorasyon (mevcut sistemi eski haline döndürme), adaptasyon (yeni koşullara uyum sağlama, sınırlı değişikliklerle devam etme) ya da dönüşüm / transformasyon (yapıyı kökten değiştirerek yeni bir düzen kurma) seçeneklerinden birisinde karar kılar. Karara göre gerekli adımlar uygulanır. Böylece hasarın giderilmesi, operasyonların eski veya daha iyi bir seviyeye getirilmesi, operasyonların dönüştürülmesi ve gelecekte benzer olayların önlenmesi sağlanır.

RS-DS eşleşmesinin her faza uyarlanması, stratejinin zaman boyutunda etkinliğini garanti altına alır. Hazırlık aşamasında yalnızca riskin önlenmesine değil, aynı zamanda olası etkiler için kapasite oluşturmaya; müdahale aşamasında hızlı, koordineli ve esnek aksiyon almaya; toparlanma aşamasında ise sürdürülebilir iyileşme ve dönüşüme odaklanmayı mümkün kılar.

RS - destekleyici DS - olay fazı entegrasyonu Tablo 14'te gösterilmektedir. Tabloda, belirlenen sekiz risk stratejisi (RS) ile bunları destekleyen dayanıklılık stratejilerinin (DS) nasıl entegre bir şekilde uygulanabileceği, olayın üç temel fazı olan olay öncesi (hazırlık), olay anı (müdahale) ve olay sonrası (toparlanma) aşamalarında somut olarak ortaya konulmaktadır.

Bu yöntem, risk yönetimi ile dayanıklılık yönetimi arasındaki boşluğu kapatarak kurumların yalnızca riskleri yönetmesini değil, aynı zamanda diğer olumsuz durumlar karşısında dirençli, esnek ve sürdürülebilir olmasını sağlar.

Tablo 14: Risk ve Dayanıklılık Stratejilerinin Olay Fazlarına Göre Uygulanması

RS	DS	Olay Öncesi (Önleme)	Olay Öncesi (Hazırlık)	Olay Anı (Müdahale)	Olay Sonrası (Toparlanma)
Kaçınma / Sonlandırma	Çeşitlilik	Alternatif kanallar oluşturularak bağımlılık azaltılır.	Alternatif kanallara hızlı geçiş planları hazırlanır.	Gerçekleşme sinyali alındığında alternatif kanallara geçilir.	Yeni süreçler kalıcı hale getirilir.
	Modülerlik	Sistemler bağımsız modüllere ayrılır, riskli modüller kolayca izole edilebilir hale getirilir.	Modüllere izolasyon mekanizmaları eklenir.	Riskli modül devre dışı bırakılır.	İzole edilen modül yenilenir veya güvenli versiyon devreye alınır.
Azaltma	Yedeklilik	Kritik kaynak ve varlıkların yedekleri hazırlanır.	Yedeklerin kullanılabilirliği düzenli test edilir.	Hasar gören kaynak yerine yedek devreye alınır.	Kullanılan yedekler yenilenir.
	Modülerlik	Hasarın yayılımını önleyecek sistem tasarımı yapılır.	Modüller için ayrı koruma ve izleme sistemleri kurulur.	Etkilenen modül devre dışı bırakılır, hasar lokalize edilir.	Modül onarılır veya yenilenir.
	Kapasite Geliştirme	Riskleri sınırlandıracak insan, süreç ve teknoloji kapasiteleri geliştirilir.	Eğitimler, tatbikatlar ve kapasite artırımları yapılır.	Kapasite yetersizliği olduğunda ek kaynaklar devreye alınır.	Kapasite kalıcı şekilde yükseltilir.
Transfer	Ağ / İşbirliği	Güvenilir ortaklarla risk paylaşım sözleşmeleri yapılır.	Ortak operasyon planları hazırlanır.	Olay anında iş ortaklarının devreye girmesiyle yük paylaşılır.	Paydaş ilişkileri gözden geçirilir, gerekirse güçlendirilir.
	Çeşitlilik	Transfer kanalları çeşitlendirilir.	Alternatif transfer anlaşmaları yapılır.	Alternatif transfer yolları kullanılır.	Kullanılan kanalların performansı analiz edilip iyileştirilir.
Kabul	Kapasite Geliştirme	Kabul edilen riskin etkilerini sınırlandıracak kapasite artırılır.	Senaryolara göre kapasite planları hazırlanır.	Kapasite sayesinde olay sırasında operasyon devam ettirilir.	Kapasite eksikleri tamamlanır, öğrenilen dersler uygulanır.
	Yedeklilik	Risk kabul edilirken kayıpları telafi edecek yedek kaynaklar hazırlanır.	Yedeklerin dayanıklılığı test edilir.	Yedekler devreye alınır.	Yedekler yenilenir.

Tablo 14: Risk ve Dayanıklılık Stratejilerinin Olay Fazlarına Göre Uygulanması (Devam)

RS	DS	Olay Öncesi (Önleme)	Olay Öncesi (Hazırlık)	Olay Anı (Müdahale)	Olay Sonrası (Toparlanma)
Paylaşma	Ağ / İşbirliği	Ortak risk paylaşımı anlaşmaları yapılır.	Ortak müdahale planları hazırlanır.	Paydaşlar birlikte müdahale eder.	Ortak toparlanma ve yeniden yapılanma yürütülür.
	Çeşitlilik	Paylaşım farklı alanlara yayılır.	Paylaşım mekanizmaları çeşitlendirilir.	Etkin paylaşım mekanizmaları devreye girer.	Paylaşım sonrası yeni dağılım dengesi oluşturulur.
Ayırma	Modülerlik	Riskli unsurlar fiziksel/sistemsal olarak ayrılır.	Bağımsız modül altyapısı kurulur.	İzole edilen modül devre dışı bırakılır.	Ayrılan kısım onarılır veya yenilenir.
	Yedeklilik	Ayrılan bileşenlerin işlevini yerine getirecek yedekler hazırlanır.	Yedeklerin çalışırılığı kontrol edilir.	Yedekler devreye alınır.	Yedekler yenilenir.
Kopyalama	Yedeklilik	Kritik unsurların birebir kopyaları hazırlanır.	Kopyaların düzenli testleri yapılır.	Orijinal zarar gördüğünde kopya devreye girer.	Kopyalar yenilenir.
	Modülerlik	Kopyalar bağımsız modüller şeklinde tasarlanır.	Kopyaların entegrasyonu sağlanır.	Hasarlı modül yerine kopya devreye girer.	Modüller güncellenir.
Çeşitlendirme	Çeşitlilik	Kaynak, pazar ve süreçler çeşitlendirilir.	Çeşitlilik planları operasyonlara entegre edilir.	En az etkilenen kaynak kullanılmaya devam edilir.	Etkili kaynaklar korunur, zayıf olanlar elenir.
	Ağ / İşbirliği	Çeşitlendirilmiş kaynaklar iş birliği ağına entegre edilir.	Ortaklarla yeni dağıtım planları yapılır.	Ağ içindeki uygun kaynak devreye girer.	Ağ yeniden düzenlenir, yeni iş birlikleri eklenir.

4.4.4. Uygulama Örnekleri

Bu bölümde Tablo 14'teki risk ve dayanıklılık stratejilerinin olay fazlarına göre uygulanmasına yönelik örnekler sunulmaktadır.

1. RS: Kaçınma / Sonlandırma – DS: Çeşitlilik

Olumsuz Durum Sınıfı: **Riskler** – Risk: **Tedarik zinciri kesintisi riski**

Senaryo: Firma, kritik hammaddede tek tedarikçiye bağımlıdır. Tedarikçi ülkesinde yaşanan siyasi kriz nedeniyle sevkiyat durabilir.

- **Olay Öncesi:**

- **Önleme:** Firma tek tedarikçiye bağımlılığı tamamen ortadan kaldırır ve farklı ülkelerden en az üç alternatif tedarikçiyle uzun vadeli anlaşmalar yapar.
- **Hazırlık:** Kritik hammaddeler için hem bölgesel hem de küresel tedarik ağları kurulur. Alternatif lojistik rotaları (deniz, kara, hava taşımacılığı) planlanır.

Olay Anı (Müdahale): Tedarikçi ülkesindeki kriz nedeniyle sevkiyat durdurulduğunda, firma hemen diğer anlaşmalı tedarikçilere yönelir. Mevcut stoklar devreye alınır, alternatif lojistik rotaları hızla aktive edilir.

- **Olay Sonrası (Toparlanma):** Kriz sonrası yeni kaynaklarla sürdürülebilir iş birlikleri geliştirilir. Tek kaynağa bağımlılığı önleyen kalıcı çeşitlendirme politikası uygulanır. Tedarik zinciri risk değerlendirmesi gözden geçirilir ve çeşitlilik stratejisi sürekli güncellenir.

2. RS: Kaçınma / Sonlandırma – DS: Modülerlik

Olumsuz Durum Sınıfı: **Risk** – Risk: **Kimyasal depolama tesisinde yangın riski**

Senaryo: Tesisin kimyasal depolama alanlarında yüksek yanıcılık özelliği taşıyan maddelerin bir arada depolanması ciddi yangın riski oluşturmaktadır.

- **Olay Öncesi:**

- **Önleme:** Yanıcı kimyasallar farklı modüllerde depolanır, ateş kaynakları minimuma indirilir.

- Hazırlık: Modüllere bağımsız yangın söndürme sistemleri kurulur, acil izolasyon vanaları yerleştirilir.
- **Olay Anı** (Müdahale): Herhangi bir depolama modülünde yangın çıkarsa, o modül acil izolasyon sistemiyle derhal devre dışı bırakılır. Yangının diğer modüllere yayılması engellenir ve itfaiye müdahalesi o sınırlı alanda yoğunlaştırılır.
- **Olay Sonrası** (Toparlanma): Güvenli taşınan maddeler alternatif tesislerde kullanılmaya devam edilir. İzole edilen ve hasar gören modül onarılır ya da tamamen değiştirilir. Güvenlik protokolleri güncellenir, yeni modüller eklenerek sistem güçlendirilir.

3. RS: Azaltma – DS: Yedeklilik

Olumsuz Durum Sınıfı: **Genişleyen Tehdit** – Tehdit: **Enerji kesintisinin zincirleme üretim durmasına yol açması**

Senaryo: Bir sanayi tesisinde bölgesel enerji altyapısında yaşanan arıza, yalnızca elektrik akışını kesmekle kalmaz, aynı zamanda bağlı tüm üretim hatlarının zincirleme biçimde durmasına neden olabilir. Bu durum kritik makinelerin çalışamamasına, soğutma sistemlerinin devre dışı kalmasına ve stoklanmış hammaddelerin zarar görmesine yol açar.

- **Olay Öncesi:**
 - Önleme: Enerji altyapısı güçlendirilir, kritik hatlar için bakım protokolleri sıklaştırılır.
 - Hazırlık: Yedek jeneratörler kurulur, alternatif enerji kaynakları (güneş panelleri, taşınabilir enerji üniteleri) hazır bulundurulur.
- **Olay Anı** (Müdahale): Ana enerji hattı çöktüğünde jeneratörler ve alternatif enerji kaynakları devreye alınır, üretim kesintisi sınırlanır.
- **Olay Sonrası** (Toparlanma): Enerji altyapısındaki sorun onarılır, tüketilen yedekler yenilenir ve enerji çeşitliliği artırılır.

4. RS: Azaltma – DS: Modülerlik

Olumsuz Durum Sınıfı: Genişleyen Tehditler – Tehdit: **Siber saldırıların yayılımı**

Senaryo: Şirket ağına sızmaya çalışan kötü amaçlı yazılımın farklı sistemlere bulaşma ihtimali vardır.

- **Olay Öncesi:**

- **Önleme:** Kritik işlevler farklı modüllere ayrılır, her modül ayrı güvenlik duvarı ve erişim kontrol sistemleriyle korunur.
- **Hazırlık:** Yedek ağ segmentleri ve acil izolasyon protokolleri hazırlanır, çalışanlar siber saldırı tatbikatlarıyla eğitilir.

- **Olay Anı (Müdahale):** Zararlı yazılım tespit edildiğinde, etkilenen modül izole edilerek saldırının diğer sistemlere yayılması engellenir. Ağ trafiği yönlendirilerek iş sürekliliği sağlanır.

- **Olay Sonrası (Toparlanma):** İzole edilen modül temizlenir veya yeniden kurulur, saldırı sonrası güvenlik açıkları kapatılır. Yeni güvenlik yamaları uygulanır ve modüler yapı gözden geçirilerek güçlendirilir.

5. RS: Azaltma – DS: Kapasite Geliştirme

Olumsuz Durum Sınıfı: **Beliren Tehditler** – Tehdit: **Pazarda artacak rekabetin fiyat baskısı yaratması**

Senaryo: Sektörde tanınmış, büyük ölçekli bir uluslararası oyuncu bölge pazarına hızla giriş yapar. Şirketin marka gücü, fiyat rekabeti ve geniş dağıtım ağı, mevcut firmaların pazar payı üzerinde doğrudan tehdit oluşturur. Bu durum, mevcut firmaların kâr marjlarını düşürme baskısı yaratır ve fiyat odaklı rekabet artar.

- **Olay Öncesi:**

- **Önleme:** Ürün farklılaştırması, hizmet kalitesinin artırılması ve müşteri sadakati programları geliştirilerek fiyat baskısına karşı kırılganlık azaltılır.
- **Hazırlık:** Üretim kapasitesi artırılır, Ar-Ge yatırımları ve süreç verimliliğiyle maliyet düşürücü önlemler alınır.

- **Olay Anı (Müdahale):** Fiyat baskısı arttığında promosyonlar ve esnek fiyatlandırma stratejileri devreye sokulur, müşteri kayıpları minimize edilmeye çalışılır.
- **Olay Sonrası (Toparlanma):** Pazar dengesi analiz edilerek uzun vadeli kapasite yönetimi, inovasyon yatırımları ve sürdürülebilir maliyet avantajları kalıcı hale getirilir.

6. RS: Transfer – DS: Ağ / İşbirliği

Olumsuz Durum Sınıfı: **Riskler** – Risk: **Uluslararası taşımacılıkta gümrük gecikmeleri**

Senaryo: İhracat yapılan ülkenin gümrük prosedürlerinde ani değişiklik olur ve sevkiyatlar durma noktasına gelir.

- **Olay Öncesi:**
 - Hazırlık: Uluslararası lojistik firmaları, gümrük müşavirleri ve ticaret odalarıyla iş birliği anlaşmaları yapılır. Alternatif taşıma rotaları ve geçiş noktaları belirlenir.
- **Olay Anı (Müdahale):** Ani gümrük değişikliklerinde, iş birliği yapılan lojistik ortakları devreye girer. Alternatif geçiş noktaları veya farklı ülkeler üzerinden taşıma organizasyonu yapılır. Kriz iletişim ağı kullanılarak müşterilere teslimat süreleri hakkında bilgi verilir.
- **Olay Sonrası (Toparlanma):** Süreçte yaşanan aksaklıklar ve darboğazlar analiz edilir. Gümrük prosedürleriyle ilgili bilgi paylaşım mekanizmaları güçlendirilir. Yeni iş birliği protokolleri oluşturularak gelecekte benzer durumlarda daha hızlı aksiyon alınması sağlanır.

7. RS: Transfer – DS: Çeşitlilik

Olumsuz Durum Sınıfı: **Muğlaklık ve Belirsizlikler** – Belirsizlik: **Döviz kurlarında dalgalanma**

Senaryo: İhracat gelirlerinin büyük bölümü tek para birimi üzerinden elde edilmektedir. Dalgalanan döviz kurları nedeniyle gelirlerde öngörülemeyen dalgalanmalar yaşanabilir.

- **Olay Öncesi:**
 - Önleme: Tek para birimine bağımlılık azaltılır; ihracat anlaşmalarında birden fazla döviz cinsi (USD, EUR, GBP vb.) üzerinden sözleşme yapılır.
 - Hazırlık: Finansal riskten korunma (hedging) yöntemleri uygulanır, gelirlerin bir kısmı farklı bankalarda veya farklı yatırım araçlarında çeşitlendirilerek güvence altına alınır.
- **Olay Anı (Müdahale):** Dövizde ani dalgalanma yaşandığında, çeşitlendirilmiş para birimi gelirleri sayesinde kayıplar sınırlandırılır. Hedging sözleşmeleri devreye girer, kritik nakit akışı korunur.
- **Olay Sonrası (Toparlanma):** Dalgalanmanın yarattığı etkiler analiz edilir, çeşitlilik stratejisinin performansı değerlendirilerek gerekirse para birimi dağılımı ve korunma (hedging) politikaları gözden geçirilir.

8. RS: Kabul – DS: Kapasite Geliştirme

Olumsuz Durum Sınıfı: Genel Tehditler – Tehdit: Mevsimsel talep dalgalanmaları

Senaryo: Ürün satışları her yıl kış aylarında önemli ölçüde azalmakta, bu dönemlerde sabit maliyetlerin karşılanması zorlaşmaktadır.

- **Olay Öncesi:**
 - Önleme: Talep dalgalanmaları bir tehdit olarak kabul edilir ve buna uyum sağlamak üzere üretim ve operasyon kapasitesi esnek hale getirilir.
 - Hazırlık: Personel çoklu görev eğitimi alarak farklı dönemlerde farklı birimlerde görev yapabilecek şekilde hazırlanır. Üretim kapasitesi esnek vardiya düzeniyle planlanır.
- **Olay Anı (Müdahale):** Talebin düştüğü dönemde kapasite düşük maliyetli üretime yönlendirilir, enerji ve hammadde tüketimi minimum seviyeye çekilir. Operasyonlar temel talebi karşılayacak şekilde optimize edilir.
- **Olay Sonrası (Toparlanma):** Talep artmaya başladığında kapasite hızla artırılır. Düşük sezonun performans verileri analiz edilerek, üretim planlamasında ve maliyet yönetiminde iyileştirmeler yapılır. Esnek kapasite yönetimi uzun vadeli süreçlere entegre edilir.

9. RS: Kabul – DS: Yedeklilik

Olumsuz Durum Sınıfı: Beliren Tehditler – Tehdit: Yeni düzenleme değişikliği

Senaryo: Üretimde kullanılan bir hammaddenin yasaklanmasına yönelik yasal değişiklik gündeme gelmiştir.

- **Olay Öncesi:**

- Önleme: Düzenleme riskinin farkında olunarak mevcut hammaddenin yerine kullanılabilecek alternatif hammaddeler araştırılır.
- Hazırlık: Kritik üretim hatlarında bu alternatif hammaddelerin test edilmiş küçük stokları yedek olarak bulundurulur.

- **Olay Anı (Müdahale):** Yasak yürürlüğe girdiğinde mevcut hammadde üretimden çıkarılır, yedekte tutulan alternatif hammaddeler üretim süreçlerine hızla entegre edilir.

- **Olay Sonrası (Toparlanma):** Alternatif hammaddeye yönelik üretim süreçleri optimize edilir, uzun vadeli tedarik anlaşmaları yapılarak kalıcı çözüm sağlanır.

10. RS: Paylaşma – DS: Ağ / İşbirliği

Olumsuz Durum Sınıfı: **Genişleyen Tehditler** – Tehdit: **Sel felaketinin lojistik ve ulaşım altyapısını çökertmesi**

Senaryo: Bölgesel bir sel felaketi yalnızca üretici firmaları değil, aynı zamanda karayolu ve demiryolu ulaşımını da işlevsiz hale getirerek tedarik zincirinde çoklu kesinti yaratmaktadır.

- **Olay Öncesi:**

- Önleme: Bölgesel lojistik ortaklarıyla alternatif güzergâhlar ve depolama merkezleri belirlenir.
- Hazırlık: Tedarikçiler ve müşteriler arasında kriz anında kullanılacak iş birliği protokolleri hazırlanır.

- **Olay Anı (Müdahale):** Sel felaketinden etkilenmeyen bölgelerdeki paydaşlar, üretim ve dağıtım üstlenerek tedarik zinciri sürekliliğini sağlar. Ortak lojistik ağ üzerinden mal akışı yeniden yönlendirilir.

- **Olay Sonrası (Toparlanma):** Bölgesel felaket sonrası ortak altyapı yatırımları yapılır, lojistik paylaşım mekanizmaları güçlendirilir ve kalıcı bir bölgesel dayanışma ağı kurulur.

11. RS: Paylaşma – DS: Çeşitlilik

Olumsuz Durum Sınıfı: **Muğlaklık ve Belirsizlikler** – Belirsizlik: **Talep tahminleri**

Senaryo: Yeni ürün lansmanı yapılmak üzeredir ancak talep miktarı hakkında güvenilir bir tahmin bulunmamaktadır. Mevcut veriler yetersiz olduğundan, ürünün hangi pazarda daha hızlı benimsenebileceği net değildir.

- **Olay Öncesi:**
 - **Önleme:** Ürün, farklı coğrafi bölgelerde ve farklı müşteri segmentlerinde eşzamanlı olarak, çeşitlendirilmiş iş ortakları aracılığıyla piyasaya sürülür.
 - **Hazırlık:** Paydaşlarla esnek dağıtım ve stok paylaşımı anlaşmaları yapılır; talebin belirsiz olduğu ortamlarda hızlı yönlendirme için lojistik kapasite esnek tutulur.
- **Olay Anı (Müdahale):** Lansman sonrası talebin yüksek olduğu bölgelerde üretim ve dağıtım hızla artırılır, düşük talep gösteren bölgelerde ise kaynaklar azaltılır. Paydaşlarla yapılan iş birliği sayesinde stoklar bölgesel taleplere göre yeniden yönlendirilir.
- **Olay Sonrası (Toparlanma):** Toplanan talep verileri analiz edilerek pazar dağılımı optimize edilir, gelecekteki belirsizlikler için tahmin modelleri geliştirilir. Ayrıca başarılı olan dağıtım kanalları güçlendirilirken, düşük performanslı kanallar gözden geçirilir.

12. RS: Ayırma – DS: Modülerlik

Olumsuz Durum Sınıfı: **Beliren Tehditler** – Tehdit: **Ani üretim hattı arızası**

Senaryo: Otomotiv fabrikasında üretim hattındaki robotik kol, aniden arıza yaparak tüm hattı durdurma riski oluşturur.

- **Olay Öncesi:**
 - **Önleme:** Üretim hattı birbirinden bağımsız modüller halinde tasarlanır, kritik makineler ayrı devrelerle çalıştırılır.

- Hazırlık: Her modülün bağımsız kontrol sistemleri kurulur, arıza anında hızlı izolasyon sağlayacak acil durdurma mekanizmaları hazırlanır.
- **Olay Anı (Müdahale):** Arızalı robotik kolun bulunduğu modül devre dışı bırakılır, diğer modüller üretime devam eder. Böylece tüm hattın durması engellenir.
- **Olay Sonrası (Toparlanma):** Arızalı modül onarılır veya yenisiyle değiştirilir. Bakım ve izleme protokolleri güçlendirilir, kritik yedek parçalar stokta hazır bulundurulur.

13. RS: Ayırma – DS: Yedeklilik

Olumsuz Durum Sınıfı: **Genel Tehditler** – Tehdit: **Salgın hastalık nedeniyle iş gücü kaybı riski**

Senaryo: Kurumda tüm çalışanların aynı anda etkilenmesi riski vardır. Tek vardiya veya tek bölüm düzeninde çalışıldığında salgın, kritik operasyonların tamamen durmasına yol açabilir.

- **Olay Öncesi:**
 - Önleme: İnsan kaynağı vardiya ve bölümlere ayrılarak aynı anda etkilenme riski azaltılır.
 - Hazırlık: Kritik görevler için alternatif personel görevlendirilir ve yedek ekipler hazır tutulur.
- **Olay Anı (Müdahale):** Bir bölümde salgın kaynaklı iş gücü kaybı yaşandığında, diğer vardiyalar veya bölümler üretime devam eder. Yedek ekipler devreye girer.
- **Olay Sonrası (Toparlanma):** Etkilenen ekiplerin sağlık ve iş gücü durumu düzeltilir, işe dönüş süreçleri planlanır. Bu süreçten öğrenilen derslerle vardiya planları ve personel rotasyon sistemleri güçlendirilir.

14. RS: Kopyalama – DS: Yedeklilik

Olumsuz Durum Sınıfı: **Genel Tehditler** – Tehdit: **Kritik müşteri verilerinin kaybolması**

Senaryo: Şirketin müşteri veri tabanı, sunucu odasında yaşanan su baskını nedeniyle kullanılamaz hale gelir.

- **Olay Öncesi:**

- **Önleme:** Veri tabanının düzenli yedekleri farklı fiziksel lokasyonlarda ve bulut tabanlı platformlarda kopyalanır.
- **Hazırlık:** Yedekleme sistemleri periyodik olarak test edilir, kurtarma protokolleri ve erişim yetkilendirmeleri tanımlanır.

- **Olay Anı (Müdahale):** Sunucu odasındaki sistem devre dışı kaldığında, yedek veri tabanları anında devreye alınır ve müşteri bilgilerine erişim kesintisiz olarak sürdürülür.

- **Olay Sonrası (Toparlanma):** Hasar gören sunucu onarılabilir veya değiştirilerek yeniden sisteme entegre edilir. Yedekleme altyapısı ve felaket kurtarma planı gözden geçirilir, gerekli iyileştirmeler yapılır.

15. RS: Kopyalama – DS: Modülerlik

Olumsuz Durum Sınıfı: **Genişleyen Tehditler** – Tehdit: **Siber saldırı yayılımı**

Senaryo: Zararlı yazılım bir sunucuya sızar ve diğer sistemlere yayılma potansiyeli taşır.

- **Olay Öncesi:**

- **Önleme:** Ağ yapısı modüler şekilde tasarlanır; kritik sunucular bağımsız segmentlere ayrılır.
- **Hazırlık:** Sunucuların kopyaları güvenli ağ segmentlerinde hazır bulundurulur.

- **Olay Anı (Müdahale):** Enfekte olan sunucu modülü ağdan izole edilir, temiz kopya modül devreye alınır.

- **Olay Sonrası (Toparlanma):** Saldırı analizi yapılır, güvenlik açıkları kapatılır, kopya sistemler yeniden güncellenir.

16. RS: Çeşitlendirme – DS: Çeşitlilik

Olumsuz Durum Sınıfı: **Genişleyen Tehditler** – Tehdit: **Yerel salgının tedarik bölgelerine yayılması**

Senaryo: Tedarik zincirinin kritik parçası olan hammaddenin sağlandığı bölgelerden birinde salgın başlar. İlk etapta tek bölge etkilenirken, kısa süre içinde diğer tedarik bölgelerine de yayılma riski ortaya çıkar.

- **Olay Öncesi:**

- Önleme: Tedarik kaynakları farklı coğrafyalara dağıtılır, aynı kaynağa aşırı bağımlılık engellenir.
- Hazırlık: Alternatif tedarikçilerle sözleşmeler yapılır, lojistik rotalar çeşitlendirilir.

- **Olay Anı (Müdahale):** Salgından daha az etkilenen bölgelerden tedarik artırılır, riskli bölgeler geçici olarak izole edilir.

- **Olay Sonrası (Toparlanma):** Etkilenen bölgelerdeki tedarikçiler kademeli olarak yeniden devreye alınır, kalıcı çeşitlilik stratejisiyle daha dengeli bir tedarik ağı oluşturulur.

17. RS: Çeşitlendirme – DS: Ağ / İşbirliği

Olumsuz Durum Sınıfı: **Muğlaklık ve Belirsizlikler** – Belirsizlik: **Küresel ticaret politikalarındaki ani değişiklikler**

Senaryo: Uluslararası ticaret politikalarında belirsizlik artmaktadır. Bazı ülkelerin ithâlât vergilerini yükseltmesi veya beklenmedik kısıtlamalar getirmesi, şirketin dış ticaret faaliyetlerini tehdit etmektedir. Hangi ülkede ne tür bir uygulamanın olacağı öngörülemediği için belirsizlik yüksektir.

- **Olay Öncesi:**

- Önleme: Şirket, farklı bölgelerde çoklu ticaret ortaklıkları kurarak tek bir ülke veya pazarın düzenlemelerine bağımlılığını azaltır.
- Hazırlık: Bölgesel ticaret birlikleriyle anlaşmalar yapılır, stratejik iş birlikleri geliştirilir.

- **Olay Anı (Müdahale):** Beklenmedik kısıtlama veya tarife uygulandığında, iş birliği yapılan diğer bölgeler ve ortaklar üzerinden alternatif pazar girişleri sağlanır.

- **Olay Sonrası** (Toparlanma): Belirsizlikten etkilenen bölgelerle ilişkiler yeniden değerlendirilir, başarılı iş birliği ağları kalıcı hale getirilerek ticaret ağı daha dirençli kılınır.



BEŞİNCİ BÖLÜM

DAYANIKLILIK ODAKLI

KURUMSAL RİSK YÖNETİMİ MODELİ ÖNERİSİ

Bu bölümde, KRY ve kurumsal dayanıklılığın birlikte etkin bir şekilde yönetilebilmesi amacıyla dayanıklılık odaklı bir kurumsal risk yönetimi modeli önerilmektedir. Önerilen model, KRY çerçevesi ile kurumsal dayanıklılığın sağlanmasına yönelik unsurları yapısal olarak sentezleyerek özgün ve kapsamlı bir mekanizma sunmaktadır. Modelin işletilmesi, kuruluşların ani ve hızlı değişim ve dönüşümler ile belirsizliklerden kaynaklanan olumsuz etkileri, süreklilik arz eden bir korunma kalkanı oluşturularak bütüncül ve dinamik bir yaklaşımla yönetebilmelerine imkân sağlamaktadır.

Kuruluşlar, etkin bir şekilde faaliyet göstermeleri ve kurumsal sürekliliğin sağlanmasını teminen paydaşlarına karşı sorumludur. Model, kuruluşların karşılaşılabilecekleri durum ve olayları yönetebilmesi için dayanıklılık kapasitelerini geliştirmelerine ve sürekliliği güvence altına almalarını sağlayan bir kılavuz niteliği taşımaktadır.

Önerilen *Dayanıklılık Odaklı Kurumsal Risk Yönetimi Modeli* (Model) özel, kâr amacı gütmeyen, sivil toplum ve kamu sektörlerinde uygulanabilir olacak şekilde jenerik niteliğe sahiptir. Model, kuruluşlarda aksaklık ve kesintiye neden olabilecek her türlü olumsuz duruma (risk, tehdit ve belirsizlikler) yönelik öngörü ve hazırlık, önleme ve durumun gerçekleşmesi sonrasında müdahale etmek üzere bir karar ve eylem çerçevesi ortaya koymaktadır.

Önerilen model, “Dayanıklılık Odaklı KRY Modelinde yer alması gereken ana bileşenler, modelin işleyişi, kullanılabilecek araç ve yöntemler nelerdir?” şeklindeki araştırma sorusuna yanıt vermektedir.

5.1. Modelin Amacı

Model, kuruluşların karşı karşıya kaldıkları riskler, belirsizlikler, tehditler ve krizlerin etki temelli yönetimine ilave olarak, bu durumların gerçekleşmesi halinde onarım, uyum ve dönüşüm süreçlerini de kapsayan uygulamaya dönük bütüncül yaklaşım ortaya koymak üzere tasarlanmıştır.

Bu bağlamda Modelin amacı:

- kuruluşların karşılaştığı riskler, tehdit türleri ile muğlaklık ve belirsizlikler gibi her türlü olumsuz durum ile
- bu durumların gerçekleşmesini takiben ilgili olayı yönetebilmesini sağlamak üzere,
- öncüllük-ardıllık, tamamlayıcılık ve kapsayıcılık ilişkilerini dikkate alan,
- durum ve zaman fazlı müdahaleyi esas alan,
- strateji – olay fazı – eylem zincirinin kurulmasına imkân veren,
- bütüncül, sistematik ve yapılandırılmış

bir uygulama çerçevesi sunmaktadır.

5.2. Modelin Kapsamı

Model, kuruluşların içinde bulunduğu iç ve dış ortama ilişkin olumsuz durumların geniş bir perspektiften ele alınarak tanımlanması, analiz edilmesi, uygun stratejiler aracılığıyla önleyici, koruyucu ve toparlayıcı eylemlerin belirlenmesi, söz konusu kontrol ve eylemlerin uygulanması ile bu sürecin sürekli izleme ve gözden geçirme yoluyla takip edilmesi ve geri bildirimler ile beslenmesi aşamalarından oluşmaktadır.

Model, bu aşamalardan oluşan süreci ilerletirken aşağıda ifade edilen unsurları kapsamına almaktadır.

- **Olumsuz Durumların Çeşitliliği**

Model, yalnızca risklerle sınırlı kalmayıp, belirsizlikler, tehditler, krizler ve öngörülemeyen olayları da kapsamına almaktadır. Bu çerçevede aleatorik, epistemik ve ontolojik belirsizlik türleri ile karmaşık tehdit zincirlerinden, basit risklere kadar geniş bir olumsuz durum türü yelpazesi modele dâhil edilmektedir.

- **Olumsuz Durumların Önceliklendirilmesi**

Olumsuz durumlar, karar alma süreçlerinin etkinliğini artırmak amacıyla, önceden tanımlanmış kriterler üzerinden önceliklendirilmekte; bu sayede sınırlı kaynaklar ve stratejiler en kritik alanlara yönlendirilebilmektedir.

- **Yönetim Stratejilerinin Kombinasyonu**

Model, olumsuz durumun mahiyetine ve kuruluşun kapasitesine bağlı olarak risk stratejilerinin (RS) uygun dayanıklılık stratejileri (DS) ile desteklenmesini sağlamaktadır. Böylece risk kontrolü ve dayanıklılık inşası birbirini tamamlayan bir mekanizma haline gelmektedir.

- **Faz Odaklı Yaklaşım**

Model, olayların yalnızca öncesini değil; gerçekleşme anı ve sonrasını da kapsayan dinamik bir yönetim anlayışını benimsemektedir. Olay öncesi hazırlık, olay anında hızlı müdahale ve olay sonrasında onarım–adaptasyon–dönüşüm aşamaları bir bütün olarak ele alınmaktadır.

- **Eylem Planlarının Oluşturulması**

Stratejilere uygun eylemler, belirlenerek eylem planı oluşturulur. Böylece henüz gerçekleşmemiş bir olumsuz durumdan başlayarak durumun gerçekleşmesi ve yönetilmesi süreçlerinin tamamını kapsayacak şekilde durum / olay - strateji - eylem zinciri kurulmuş olur.

- **Gerçekleşme Sonrasında Toparlanma Kararı**

Olumsuz bir olayın ardından kuruluş, toparlanma biçimine ilişkin stratejik bir karar alır. Onarım, uyum ve dönüşüm seçenekleri arasında yapılacak tercih, kurumun uzun vadeli sürdürülebilirliğini ve rekabet gücünü belirleyici hale gelmektedir. Model, bu seçeneklere yönelik ön hazırlıkların gerçekleştirilmesini öngörür.

5.3. Modelin Teorik Temeli

Modelin teorik altyapısı, KRY, DY ve kriz yönetimi literatürüne ilave olarak uluslararası genel kabul gören standart ve çerçevelere dayanmaktadır. Modelin oluşturulmasında KRY'ye ilişkin COSO KRY (2018) ve ISO 31000 Risk Yönetimi (2018) standartlarından yararlanılmıştır.

Diğer taraftan Model, DY'ye yönelik ANSI/ASIS (2009) tarafından yayımlanan Organizasyonel Dayanıklılık, ISO (2017) tarafından yayımlanan 22316 - Organizasyonel Dayanıklılık, ISO (2019) tarafından yayımlanan ISO 22301 Güvenlik ve Dayanıklılık - İş

Sürekliliği Yönetim Sistemleri - Gereklilikler ve BSI (2022) tarafından yayımlanan BS 65000 Organizasyonel Dayanıklılık - Uygulama Kodu standartlarında yer verilen husus ve öğelerle güçlendirilmiştir.

5.4. Modelin Öne Çıkan Özellikleri

Model, bütüncül ve çok boyutlu bir yaklaşım sergiler. Öncelikle, odaklanma ve kaynak optimizasyonu açısından modelin stratejik, taktik ya da operasyonel seviyelerden hangisi esas alınarak uygulanacağı belirlenir. Sadece klasik risk yönetimi mantığıyla ölçülebilir riskleri değil, belirsizlik, tehdit ve kriz gibi öngörülemez durumları da kapsayarak daha geniş bir evreni yönetim sürecine dâhil eder.

Zaman boyutunu esas alarak olay öncesi, olay anı ve olay sonrası olmak üzere üç temel faz üzerinden ilerler. Bu, statik risk yönetimi modellerinden farklı olarak döngüsel ve dinamik bir yapı sunar.

Modelin merkezinde tampon ve emilim kapasitesi bulunur. Bu özellik, olumsuz durumların tamamen engellenemediği hallerde bile etkilerin sınırlandırılmasını ve sistemin işlevselliğini korumasını sağlar.

Süreçte geri bildirim mekanizması kritik rol oynar. Her bir olaydan sonra öğrenilen dersler ve yapılan gözden geçirmeler yeniden sisteme entegre edilerek sürekli iyileştirme sağlanır. Böylece model, sadece olaylara tepki veren değil, aynı zamanda öğrenen ve adaptif bir yapı ortaya koyar.

Paydaş entegrasyonu da önemli bir özelliktir. Hem iç hem de dış paydaşların süreçte konumlandırılması, iletişim ve koordinasyonun yönetim döngüsüne dâhil edilmesi, modelin kapsayıcılığını artırır.

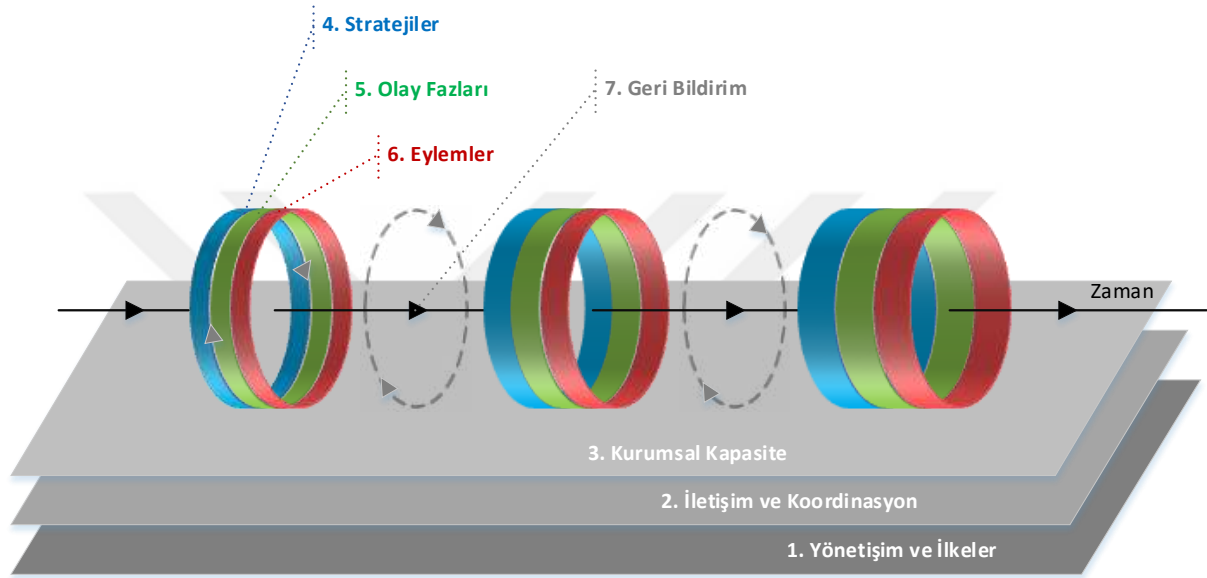
Strateji seçiminden kontrol uygulamasına kadar olan akış, kurumsal kapasiteyle doğrudan bağlantılıdır. Kapasitenin güçlendirilmesi modelin sürdürülebilirliğini desteklerken, strateji–kontrol–eylem zincirinin uygulanabilirliğini de güvence altına alır.

Son olarak, model dinamik revizyon mekanizması içerir. Başarısız strateji ve kontrollerin hızla yeniden gözden geçirilip revize edilmesi, modelin esnekliğini ve çevikliğini artırır.

5.5. Modelin Bileşenleri

Dayanıklılık Odaklı Kurumsal Risk Yönetimi Modeli, birbirini tamamlayan ve döngüsel yapısıyla sürekli gelişime imkân tanıyan yedi temel bileşenden oluşmaktadır. Şekil 18’de modelin bileşenleri işlevsel ilişkileri gösterecek şekilde katmanlı ve döngüsel bir yapı olarak sunulmaktadır.

Şekil 18: Modelin Bileşenleri ve İşleyişi



Diyagram, zaman eksenini boyunca tekrarlanan döngüsel halkalar aracılığıyla ilerleyen bir yapıyı göstermekte ve bu durum, olumsuzlukların dinamik ve öngörülemez doğasına karşı modelin sürekliliğini ve kendini yenileyebilme kapasitesini vurgulamaktadır. Döngüsel düzen, yalnızca yinelenen bir süreç akışını değil; aynı zamanda kurumun strateji–faz–eylem üçlüsü üzerinden hem kaynaklarını hem de uygulama kapasitesini sürekli geliştirdiği bir öğrenme mekanizmasını temsil etmektedir.

İlk döngüde kurum, mevcut kapasitesine dayanarak uygun stratejileri seçmekte, olay fazlarına göre hareket etmekte ve gerekli eylemleri uygulamaktadır. Bu aşamada elde edilen deneyimler ve ortaya çıkan eksiklikler, sonraki süreçlerin temelini oluşturmaktadır. Yedinci adımı oluşturan geri bildirim mekanizması, olay sonrasında gerçekleştirilen değerlendirme ve öğrenme faaliyetleriyle hangi stratejilerin etkili olduğunu, hangi eylemlerin ise yetersiz kaldığını ortaya koymaktadır.

Bu öğrenme sürecinin sonucunda izleyen döngülerde kurum, önceki aşamalara kıyasla daha donanımlı hâle gelmekte; hem kaynak kullanımı (finansal, teknik ve insan kaynağı) hem

de kurumsal kapasite (öngörü, uyum, toparlanma ve dönüşüm) bakımından güç kazanmaktadır. Her tekrar, kurumsal gelişimin yeni bir olgunluk basamağını temsil etmekte; stratejiler daha rafine, faz yönetimi (öncesi–anı–sonrası) daha belirgin, eylemler ise daha hızlı ve etkin hâle gelmektedir. Böylelikle süreç, yalnızca risk ve tehditlere tepki verme işlevi görmekten öteye geçerek, kurumun dayanıklılık kapasitesini sürekli olarak geliştiren öğrenme temelli bir mekanizma niteliği kazanmaktadır.

5.5.1. Yönetişim ve İlkeler

Yönetişim boyutu, risk ve dayanıklılık süreçlerinin üst yönetimden operasyonel birimlere kadar bütün kademelerde sahiplenilmesini ve koordineli bir şekilde yürütülmesini esas alır. Bu çerçevede, rol tanımlarının netleştirilmesi, hesap verebilirliğin sağlanması ve karar süreçlerinde paydaş katılımının artırılması kritik öneme sahiptir. Ayrıca, yönetim yapısının esnek ve uyarlanabilir olması, hızlı değişen koşullar karşısında karar alma süreçlerinin etkinliğini artırır.

Model, kurumsal yönetim yapısı ile dayanıklılığın rehber ilkelerini bütünleştirmektedir. İlkeler, modelin zeminini ve yönlendirici çerçevesini ortaya koymaktadır. İlkeler, strateji ve eylemlerin seçimini ve uygulanmasını yönlendirir. Kuruluşlar, modelin etkin bir şekilde hayata geçirilmesini teminen temel ilkeleri benimsemelidir.

1. **Dayanıklılık Odaklı Liderlik ve Yönetişim:** Kuruluşun rutin işleyişi ile kriz anlarında yön gösterici, güven artırıcı ve dayanıklılık kültürünü destekleyici liderlik pratiklerinin benimsenmesi.
2. **Kaynakların Etkin Yönetimi ve Dağıtım İlkesi:** Kaynakların esnek yönetimi ile optimal tahsisi, kritik süreçlerin sürekliliğini güvence altına alacak şekilde kaynak planlamasının yapılması.
3. **Açıklık İlkesi:** İç ve dış paydaşlarla şeffaf, doğru ve zamanında bilgi paylaşımının yapılması, dış sistemlerle açık etkileşim sağlanması ve güven ortamının geliştirilmesi.
4. **İşbirliği İlkesi:** Kurum içi ve dışı aktörlerle ortak hedefler doğrultusunda koordinasyon kurulması, dayanışmanın ve kolektif kapasitenin geliştirilmesi, gerektiğinde iş birlikleri ve ortaklıkların tesis edilmesi.
5. **Kapsayıcılık İlkesi:** Karar alma ve uygulama süreçlerinde farklı paydaşların görüşlerinin dikkate alınması, süreçlere etkin katılımlarının sağlanması.

6. **Sistemsal Sadelik ve Bağımsızlık İlkesi:** Aşırı karmaşıklıktan kaçınılması, süreçlerin yalınlaştırılması ve kritik bağımlılıkların azaltılması.
7. **Sürekli İyileştirme İlkesi:** Her olay ve deneyimden öğrenilerek süreçlerin yeniden değerlendirilmesi ve sürekli geliştirilmesi.
8. **Hazırlıklılık İlkesi:** Olası tehditlere karşı senaryoların geliştirilmesi, tatbikatların yapılması ve acil durum planlarının güncel tutulması. Kaynaklarda yedeklilik ile çeşitliliğin sağlanması.

Bu ilkeler, yalnızca uygulamalara değil; aynı zamanda kurum kültürüne, etik değerlere ve stratejik yönetime de yön vermektedir. Bu bileşen, modelin normatif ve kurumsal temelini oluşturarak hem yönetsel hem de kültürel boyutta kararların tutarlılığını, şeffaflığını ve etkinliğini güçlendirmektedir.

5.5.2. Kurumsal Kapasite

Modelin uygulanabilirliğini ve etkinliğini sağlayan unsur kapasite boyutudur. Bu bağlamda aşağıdaki alanlarda gerçekleştirilen iyileştirmeler bileşenin kapsamındadır.

- İnsan kaynakları, bilgi ve iletişim sistemleri, fiziksel ve teknolojik altyapı ile tedarik ve lojistik kapasitesinin geliştirilmesi,
- Kurumsal yapının iyileştirilmesi, yatay ve dikey iletişim kanallarının güçlendirilmesi,
- İSY, iç kontrol gibi yönetim araçlarının kullanılması, süreç geliştirme ve süreçlerde standardizasyonun sağlanması,
- Performans ve izleme sistemlerinin kurulması,
- Kaynak ve rezerv yönetiminde kapasite ve etkinliğin artırılması,
- İşbirlikleri ve dış paydaş katılımının sağlanması,
- Kurumsal kültür ve değerler ile mevzuat ve düzenlemelere uyumun güçlendirilmesi.

Bu bileşen, dayanıklılığın kurumsal kapasite üzerinden somut uygulamalar aracılığıyla hayata geçirilmesini sağlamaktadır.

5.5.3. İletişim ve Koordinasyon

Model, iç ve dış paydaşlara düzenli bilgi akışı aracılığıyla ortak anlayış ve koordinasyonun sağlanmasını hedefler. Bu bileşen, modelin tümünü bir arada tutmakta, modelin canlılığını sağlamaktadır.

Bu bağlamda, kurum içi birimler arasında yatay ve dikey bilgi akışının sağlanması amacıyla yöntem ve araçlar belirlenir. Bu amaçla, düzenli izleme ve değerlendirme toplantıları ile raporlar kullanılır. İhtiyaca göre dış paydaşlarla görüşülebilir, değerlendirmeleri alınabilir. İlave olarak ilgili stratejiler çerçevesinde iş birliği ve ortaklıklar kurulabilir, kurumsal ağlara katılım yoluyla destek alınabilir.

Özellikle kriz yönetimini ve kuruluş dışında diğer aktörlerin dâhil olmasını gerektiren olumsuz durumlara yönelik hızlı karar almayı ve eşgüdümlü hareket etmeyi mümkün kılmak üzere koordinasyon çalışmaları gerçekleştirilebilir.

İletişim ve koordinasyonun nasıl ve hangi araçlar (görüşme ve toplantılar, durum ve izleme raporları vb.) kullanılarak sağlanacağı hususları netleştirilir.

5.5.4. Yanıt Stratejileri

Yanıt stratejileri, kuruluşların tanımlanan olumsuz duruma yönelik tutumlarının formüle edilmiş halidir. Yönetimin yanıt konusundaki tutumları, kurum genelinde farklı türdeki olumsuz durumlara karşı stratejilerini şekillendirmektedir.

Modeldeki stratejiler, KRY’de kullanılan risk stratejileri (kaçınma, azaltma, paylaşma, kabul) ile literatür analizi aracılığıyla derlenen ve bu stratejileri destekleyen dayanıklılık stratejilerinden (yedeklilik, modülerlik, çeşitlilik, ağ iş birliği, kapasite geliştirme) oluşmaktadır. Bu bileşen, modelin operasyonel kapasitesini zenginleştirerek kurumların stratejik seçeneklerini çeşitlendirmektedir.

5.5.5. Olay Fazları

Model, olumsuz durum ve olayların yönetimini olay öncesi, olay anı ve olay sonrası olmak üzere üç temel faz üzerinden ele almaktadır. Olay öncesi aşama hazırlık ve risk azaltmaya, olay anı hızlı müdahale ve koordinasyona, olay sonrası ise onarım, adaptasyon ve

dönüşüm süreçlerine odaklanmaktadır. Böylece risk yönetimi, tek seferlik bir faaliyet değil, dinamik ve döngüsel bir süreç olarak kurgulanmaktadır. Bu bileşen, modelin zaman boyutunu tanımlamakta ve modele sistematik bir süreklilik kazandırmaktadır.

Her bir olay fazı, farklı hedef ve önceliklere sahip olduğundan, eylem türleri farklı fazlara yönelik belirlenir. Her olumsuz durum üç temel fazda yönetilir:

1. **Olay öncesi (hazırlık):** Olumsuz durumun gerçekleşme ihtimalini azaltacak veya etkisini sınırlayacak önleyici ve yönlendirici eylemler devreye alınır. Müdahale ve toparlanma fazlarına yönelik planlar ve eylemler tanımlanır.
2. **Olay anı (müdahale):** Önceden hazırlanan planlar ve eylemler varsa devreye alınır.
3. **Olay sonrası (toparlanma):** Bu aşamada tespit edici ve düzeltici kontroller uygulamaya konulur.

5.5.6. Eylemler

Stratejilerin uygulamaya aktarılması bu bileşenin kapsamına dâhildir. Seçilen stratejiler doğrultusunda yanıt eylemleri belirlenir ve uygulanır. Eylemler, olay fazlarına göre farklılaşarak esnek bir yönetim imkânı sunar. Bu sayede hem önleyici hem de müdahale edici faaliyetler sistematik olarak devreye alınabilmektedir.

Kontrol eylemlerinin temel amacı öncelikle olumsuz durumun gerçekleşmesinin önlenmesidir. Bunun başılamaması halinde olayın etkisini en aza indirmek ikincil amaçtır. Bu amaç doğrultusunda önleyici, yönlendirici, tespit edici ve düzeltici olmak üzere farklı eylem türleri uygulanır. Bu eylemler, maliyet ve fayda dengesi gözetilerek seçilen stratejiye ve müdahale fazına uyumlu olacak şekilde tasarlanır.

5.5.7. Geri Bildirim

Son bileşen, modelin döngüsel karakterini ortaya koymaktadır. İzleme ve değerlendirme süreçlerinden elde edilen bilgiler, başarısız ya da eksik kalan strateji ve kontrollerin revize edilmesini sağlar. Olay sonrası edinilen tecrübeler, kurumsal hafızaya aktarılır ve gelecekteki olumsuz durumların yönetiminde kullanılır. Bu bileşen, dayanıklılık kapasitesinin güçlendirilmesinde sürekliliği sağlamaktadır.

5.6. Rol ve Sorumluluklar

Modelin uygulanmasına yönelik üst yönetim, birim yöneticileri ve alt birimler nezdinde rol ve sorumlulukların atanacağı yapılar belirlenir. Bu amaçla doğrudan pozisyonlara atama yapılabileceği gibi çeşitli seviyelerde kurul, komite ve ekipler teşkil edilebilir. Bu yapılanma, organizasyonel bağlamda olabileceği gibi fonksiyonel ya da süreç bağlamında da bir yapılanma tercih edilebilir.

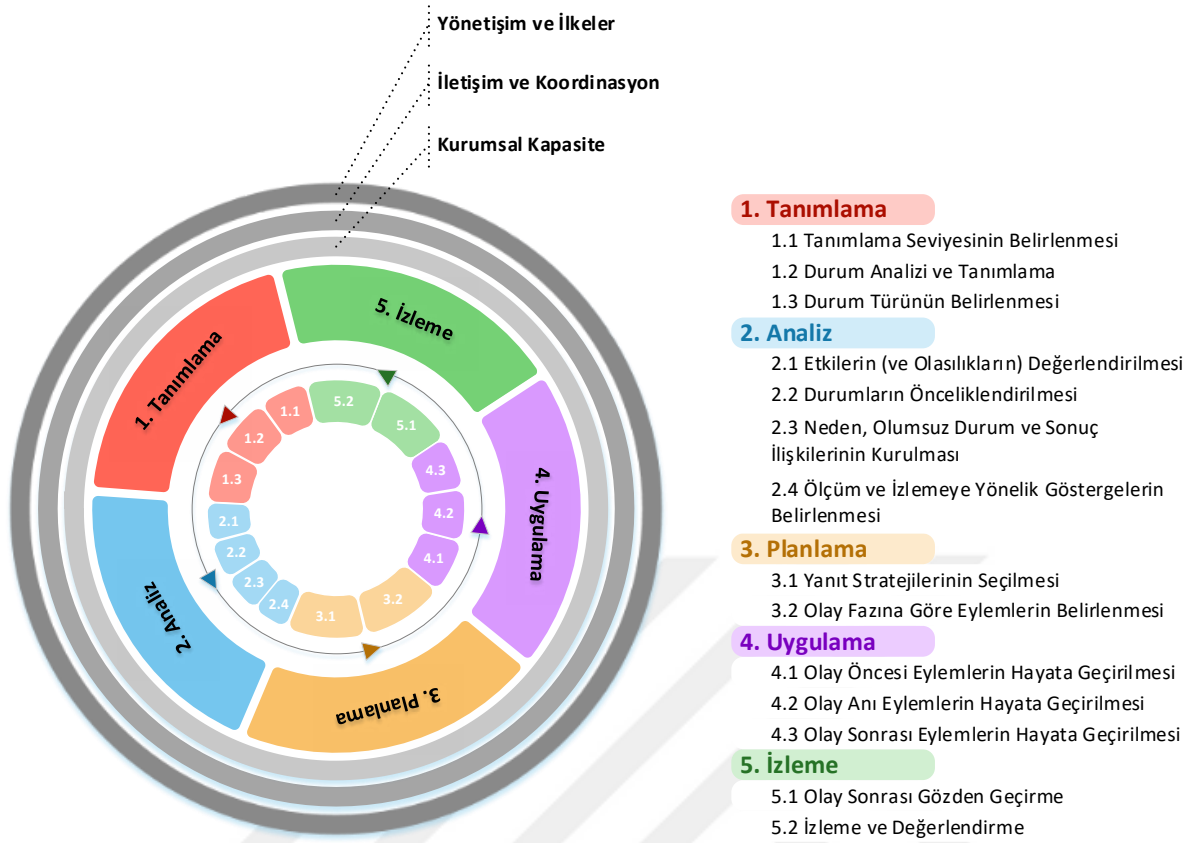
Yapıda yer alan aktörler ile kurul, komite gibi yapıların rol, sorumluluk ve yetkileri ile hangi durumlarda, aşamalarda devreye girecekleri belirlenir. Aktörler arasındaki bilgi akışı ile raporlamanın nasıl ve hangi yönde olacağına karar verilir.

5.7. Modelin İşleyişi ve Uygulama Süreci

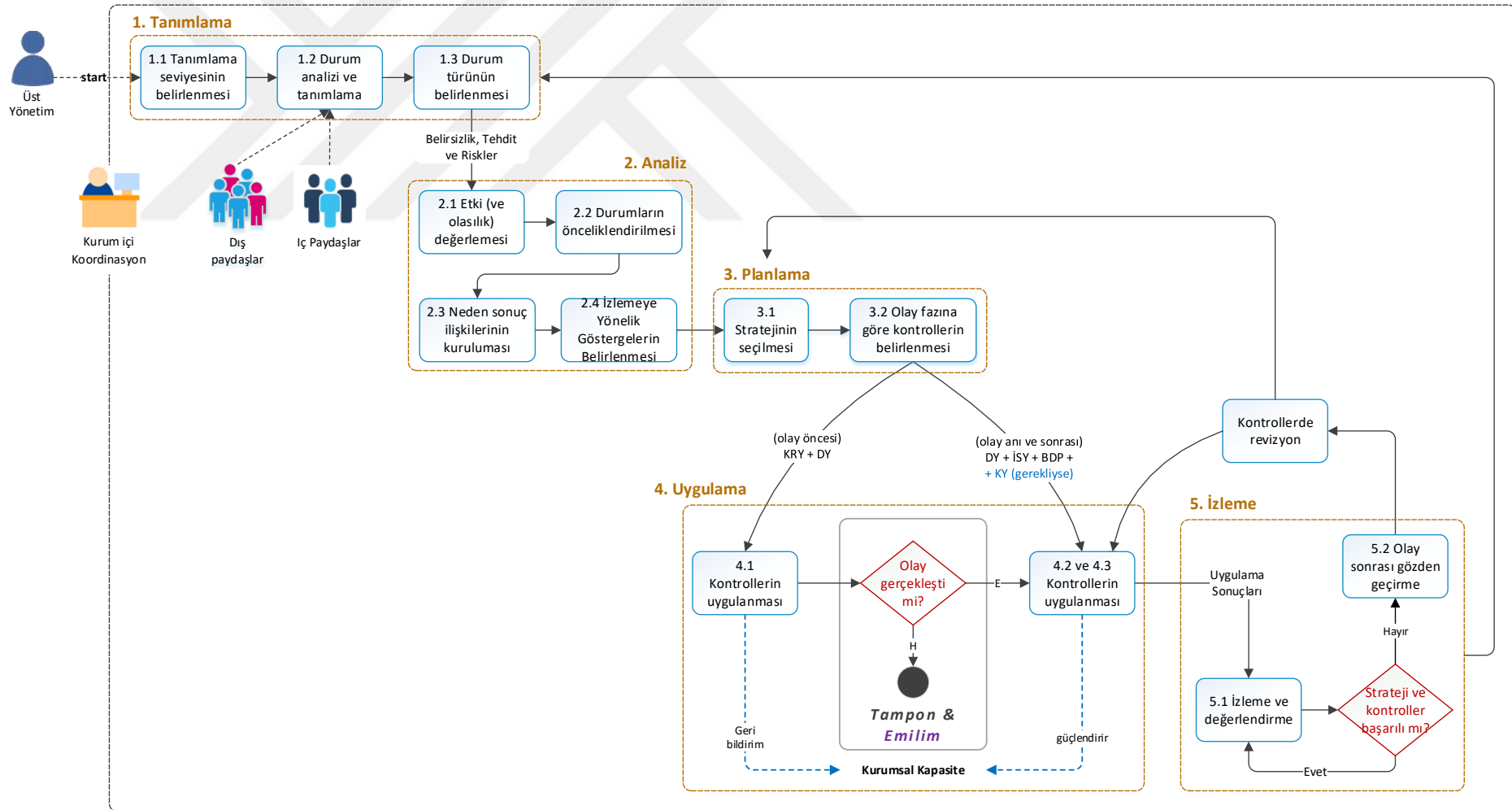
Model, tanımlama, analiz, planlama, uygulama ve izleme olmak üzere birbirini izleyen beş temel aşamadan oluşmaktadır. Her bir aşama, sürecin detaylandırılmasını teminen alt adımlardan oluşmaktadır.

Önerilen modelin girdisi ve tetikleyicisi, kuruluşların karşılaştığı riskler, tehditler, belirsizlikler ve krizler gibi geniş bir yelpazede ele alınan olumsuz durumlardır. Bu bütüncül yaklaşım, modelin kapsayıcılığını ve gerçek dünyadaki tehdit çeşitliliğine uyumunu güçlendirmektedir.

Şekil 19: Modelin Aşamaları ve Alt Adımları



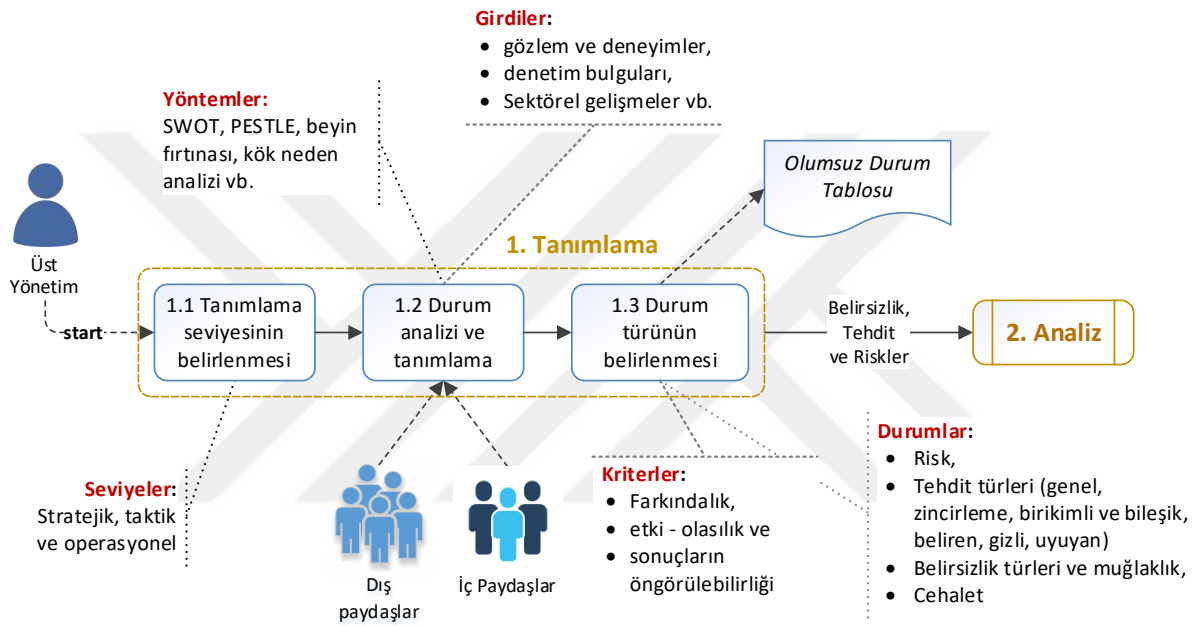
Modelin uygulama sürecine yönelik iş akış diyagramı Şekil 20’de sunulmaktadır. Her bir aşamaya yönelik alt adımlarda akış diyagramı detaylandırılacaktır.



5.7.1. Tanımlama

İlk aşama, kuruluşların içinde bulunduğu ortamda yer alan ve kuruluşun işleyişine, sürekliliğine ve faaliyetlerine etkisi olabilecek olumsuz durumların mahiyetleriyle birlikte kayıt altına alınması ve niteliğinin belirlenmesi üzerine kuruludur. Bu aşama, tanımlama seviyesine karar verilmesi, durumun tanımlaması ve türünün belirlenmesine yönelik üç alt adımdan oluşmaktadır.

Şekil 21: Tanımlama Aşaması



Olumsuz durumların belirlenmesinde süreç odaklı, amaç ve hedef odaklı ya da fonksiyon/bölüm odaklı yaklaşımlar izlenebilir. Modelin uygulama aşamalarına geçmeden üst yönetim tarafından bu yaklaşımlardan birisi belirlenir. Seçilen yaklaşım, çalışılacak alan üzerinde doğrudan etkili olacaktır.

1. **Süreç Odaklı Yaklaşım:** Kuruluşun iş süreçleri adım adım incelenerek her aşamada karşılaşılabilecek potansiyel olumsuz durumlar belirlenir. Bu yöntem, operasyonel işleyişin akışından doğan olumsuz durumları ortaya çıkarır.
2. **Hedef Odaklı Yaklaşım:** Kuruluşun stratejik amaç ve hedeflerine ulaşmayı engelleyebilecek unsurlar, olumsuz durumlar olarak tanımlanır. Böylece olumsuz durumlar doğrudan kuruluşun amaçlarıyla ilişkilendirilir.

3. **Fonksiyon/Bölüm Odaklı Yaklaşım:** Organizasyonun farklı fonksiyonları (finans, üretim, pazarlama vb.) veya bölümleri (örneğin tedarik, lojistik, bilgi teknolojileri) ayrı ayrı ele alınarak her birine yönelik olumsuz durumlar tespit edilir.

5.7.1.1. Tanımlama Seviyesinin Belirlenmesi

Olumsuz durumların tanımlanmasında etkileri bakımından stratejik, taktik ya da operasyonel seviyelerden hangisinin esas alınacağı belirlenir. Bu seviyelerden yalnızca biri (örneğin sadece etkileri stratejik seviyedeki olumsuz durumlar ya da sadece etkileri operasyonel seviyedeki olumsuz durumlar) doğrultusunda tanımlamalar yapılabileceği gibi, tüm seviyeleri kapsayan bütüncül bir yaklaşım da benimsenebilir. Bunun kararı üst yönetimce verilir.

- *Stratejik seviye*, kuruluşun uzun vadeli hedeflerini, vizyonunu ve sürdürülebilirliğini tehdit eden olumsuz durumların ele alındığı seviyedir; tüm organizasyonu etkiler. Genellikle üst yönetim ve yönetim kurulu düzeyinde karar alınmasını gerektirir.
- *Taktik seviye*, orta vadeli plan ve projelerin başarıya ulaşmasını tehdit eden olumsuz durumların ele alındığı seviyedir; birim, alt birim veya fonksiyon düzeyinde ortaya çıkar. Genellikle orta kademe yöneticilerin sorumluluğundadır.
- *Operasyonel seviye*, günlük iş süreçlerinde ortaya çıkan, kısa vadeli faaliyetleri aksatabilecek olumsuz durumların ele alındığı seviyedir; operasyonel seviyede çalışanlar ve süreç yöneticileri tarafından yönetilir.

Tanımlama seviyesinin belirlenmesi, hedefe yönelik odaklanmanın sağlanması ile kaynak kullanımının optimize edilmesi bakımından önem arz etmektedir. Tercih edilen seviye, çalışmanın kapsamını belirleyecektir. Tanımlama, analiz ve planlama aşamaları bu seviye üzerinden ilerleyecektir.

5.7.1.2. Durum Analizi ve Tanımlama

Durum analizi, karşı karşıya kalınan olumsuz durumların (risk, tehdit, belirsizlik, kriz veya olaylar) tanımlanması, anlaşılması ve kayıt altına alınması sürecidir. Paydaşların katılımlarıyla, kuruluşun faaliyetlerini gerçekleştirdiği iş ortamı geniş bir perspektiften analiz edilir. Kuruluşu etkileyen, etkileme potansiyeli bulunan içsel ya da dışsal kaynaklı her türlü olumsuz durum taranarak analiz için veri toplanır. Amaç, olumsuz durumlara yönelik evrenin

oluşturulmasıdır. Bu evren içerisinde teknoloji, operasyon, finans, strateji, uyum ve itibar açılarından riskten belirsizliğe kadar her seviyede olumsuz durum türü yer alabilir.

Olumsuz durumların belirlenmesinde yönetim ve çalışanlar tarafından gerçekleştirilen gözlem ve deneyimler, ihbarlar, denetim bulguları, sektörel gelişmeler, ekonomik, politik, hukuki ve çevresel değişimler gibi kaynaklar girdiler olarak kullanılabilir.

Bu adımda, olumsuz durumların belirlenmesi amacıyla çalıştay, beyin fırtınası, yapılandırılmış görüşmeler ve mülakatlar, Delphi tekniği, nominal grup tekniği, SWOT (güçlü yönler, zayıf yönler, fırsatlar ve tehditler) analizi ile PESTLE (siyasi, ekonomik, sosyolojik, teknolojik, mevzuat ve çevre) analizi gibi kolaylaştırıcı yöntemler kullanılabilir.

Örtük tehditler, başlangıçta sezilmesi ve tespit edilmesi kolay olmayan durumlardır. Bu sınıftaki durumların kendilerini açıkça göstermesi zaman alabileceği gibi farkına varılması da mümkün olmayabilir. Durum, ancak gerçekleşikten sonra bilinebilir.

5.7.1.3. Durum Türünün Belirlenmesi

Tanımlanan olumsuz durumlar; etki ve olasılık ile sonuçların öngörülebilirliği kriterleri doğrultusunda değerlendirilir ve durumların mahiyetlerine göre türleri belirlenir. Olumsuz durum türlerinin sınıflandırılmasına yönelik Şekil 9'daki karar diyagramı kullanılarak her bir olumsuz durum; risk, tehdit türleri ya da muğlaklık ve belirsizlik şeklinde etiketlenir ve ait olduğu olumsuz durum sınıfı netleştirilir. Tablo 15'te olumsuz durum türleri ve bu türlerin ait olduğu sınıflar gösterilmektedir.

Tablo 15: Olumsuz Durum Türleri ve Ait Oldukları Sınıflar

Olumsuz Durum Türleri	Olumsuz Durum Sınıfları
Riskler	1. Riskler
Genel Tehditler	2. Genel Tehditler
Zincirleme, Birikimli ve Bileşik Tehditler	3. Genişleyen Tehditler
Beliren Tehditler	4. Beliren Tehditler
Muğlaklık ve Belirsizlik (Ontolojik)	5. Muğlaklık ve Belirsizlikler
Uyuyan ve Gizli Tehditler	6. Örtük Tehditler
Cehalet	7. Cehalet

Sınıflandırma, belirsizlik, risk, tehdit ve olayların doğasının netleştirilmesini sağlayarak kuruluşların daha bilinçli, hedefe yönelik ve stratejik hareket etmesine imkân tanır. Bu yaklaşım, duruma özgü müdahale geliştirilmesini, hazırlıkların ve kapasite kullanımının doğru yönlendirilmesini sağlayarak önceliklendirme ve karar alma süreçlerini kolaylaştırır.

Tanımlama aşamasında elde edilen bilgiler, Olumsuz Durum Tablosuna (ODT) işlenir.

5.7.2. Analiz

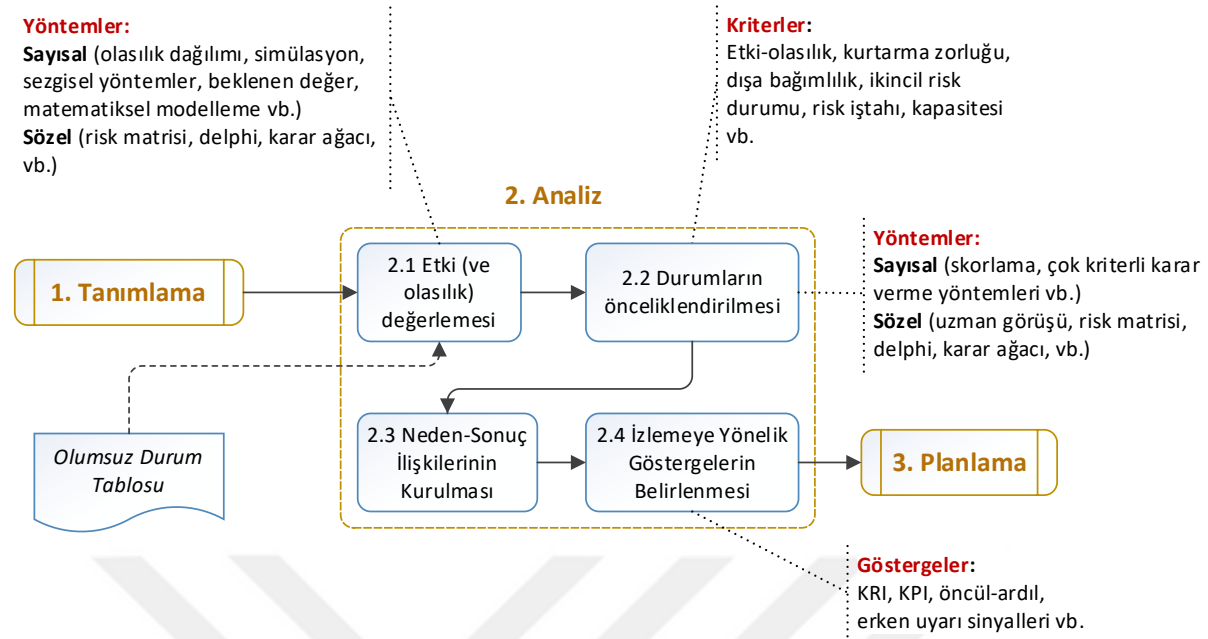
Analiz aşaması, tanımlama aşamasında oluşturulan ODT'yi esas alarak, durumların nedenlerini, etki (ve olasılıklarını) ile sonuçlarını sistematik biçimde inceleyerek kuruluş üzerindeki toplam etkilerini anlamayı ve önceliklendirmeyi amaçlayan analitik bir aşamadır. Bu aşamada, ODT'deki her bir duruma ilişkin hâlihazırda kullanılan kontrol eylemleri ortaya konularak etkinlikleri değerlendirilir. Söz konusu duruma yönelik analizler gerçekleştirilir.

Değerlendirmesi yapılan olumsuz durumlar çeşitli kriterler çerçevesinde önceliklendirilir. Önceliklendirmeyi müteakiben henüz gerçekleşmeden (olay öncesi) ya da gerçekleşikten sonra (olay sonrası) yanıt verilmesi gereken nihai olumsuz durum setine ulaşılır. Bu aşama, etkilerin (varsa olasılıkların) değerlendirilmesi, olumsuz durumların önceliklendirilmesi, olumsuz durumu ortaya çıkaran nedenler ile gerçekleşmesi halindeki sonuçların tespit edilerek aralarındaki ilişkilerin kurulması ve olumsuz durumun izlenmesine yönelik göstergelerin belirlenmesi olmak üzere Şekil 22'de gösterildiği üzere dört alt adımdan oluşmaktadır.

5.7.2.1. Etki (ve Olasılık) Değerlendirmesi

Tanımlanan olumsuz durumlar, bu adımda türleri dikkate alınarak kuruluş üzerindeki muhtemel etkileri (ve olasılıkları) bakımından sistematik olarak incelenirler. Risklerde, kavramsal tanım gereği, etki ve olasılık değerlendirilmesi birlikte yapılırken diğer durum türleri yalnızca etki bakımından değerlendirilirler. Amaç, her bir olumsuz duruma ilişkin önem düzeyini belirlemek ve sonraki aşamalarda strateji ve kontrol eylemi seçimlerine temel oluşturmaktır.

Şekil 22: Analiz Aşaması



Değerlendirme sürecinde nitel, nicel ve hibrit yöntemler kullanılabilir. Bu kapsamda:

- Etki boyutu, finansal kayıplar, operasyonel kesinti, itibar zedelenmesi, yasal yaptırımlar ve paydaş güveni gibi unsurlar üzerindeki sonuçlar dikkate alınarak değerlendirilir.
- Olasılık boyutu, olumsuz durumun gerçekleşme ihtimaline ilişkin tarihsel veriler, sektör trendleri, dış çevresel faktörler ve uzman öngörüler vb. üzerinden belirlenir.

Elde edilen veriler, etki-olasılık matrisleri veya derecelendirme tabloları aracılığıyla görselleştirilir. Bu sayede her bir olumsuz durumun kuruluş ve hedefler üzerindeki görece önemi ortaya konulur.

Risk dışındaki diğer olumsuz durum türlerinde olasılık bilgisinin söz konusu olmadığı dikkate alınmalıdır. Bu durum türlerinde olası etkileri aynı düzlemde buluşturma amacıyla hazırlanan etki ölçeği tabloları kullanılabilir. Bu tablolarda finansal, operasyonel, hukuki ve itibari vb. açılardan etkilerin büyüklüğü tanımlanır ve bu büyüklüğü göstermek üzere “1-10 puan arası” ya da “çok düşük, düşük... çok yüksek” gibi bir skala aracılığıyla yapılan değerlendirmeler yer alır.

Diğer taraftan, süreç bazlı yaklaşım tercih edildiği ve olumsuz durum tanımlamalarının bu yaklaşım üzerine inşa edildiği çalışmalarda etkilerin boyutunu ölçmek üzere iş etki analizleri

de kullanılabilir. Muğlaklık ve belirsizlik durumları için herhangi bir etki – olasılık değerlendirmesi söz konusu değildir.

5.7.2.2. Durumların Önceliklendirilmesi

Bu adımın çıktısı, önceliklendirilmiş olumsuz durum listesidir. Böylece hangi durumların daha acil müdahale gerektirdiği belirlenir ve planlama aşamasında uygun stratejiler ile destekleyici dayanıklılık kapasitelerinin seçilmesine zemin hazırlanır.

Durumlar, çeşitli kriterler bakımından değerlendirilerek önceliklendirilirler. Dayanıklılık kapsamına alınması gereken olumsuz durumlar için kriter olarak (1) süreç, işlem vs. üzerindeki etkisi, (2) yayılma etkisi, (3) kurtarma zorluğu, (4) kurumsal zayıf noktaları etkileme durumu, (5) itibar üzerindeki etkisi, (6) olayın gerçekleşmesini müteakip hızlı bir şekilde karşılık verilmesi gerekliliği, (7) düzenlemelere yönelik uyum üzerindeki etkisi, (8) dışa bağımlılık üzerindeki etkisi, (9) ikincil ya da zincirleme yeni durum veya olay yaratma potansiyeli ve (10) stratejik etki yaratma potansiyeli gibi kriterler kullanılabilir. Olumsuz durumlar, kriter seti içerisinde durumun mahiyetine uygun olanlar aracılığıyla ele alınmalıdır.

Olumsuz durumların sıralanması ve önceliklendirilmesinde bahse konu kriterler de dikkate alınarak, nitel ve nicel yöntemler ile bunların birlikte kullanıldığı hibrit yöntemler kullanılabilir.

- Veri eksikliğinin olduğu, belirsizliğin yüksek olduğu, zamana duyarlı ve hızlı kararların gerektiği acil durumlarda basit ve pratik bir araç olarak uzman görüşü, beyin fırtınası, senaryo analizi ve Delphi tekniği ile iki boyutlu matrisler (etki-olasılık, maliyet-kurtarma zorluğu vb.) gibi nitel yöntemler tercih edilebilir.
- Yeterli ve güvenilir verinin bulunduğu, olumsuz durumların farklı boyutlarda sayısal olarak ölçülebildiği ortamlarda objektif yöntemler olarak skorlama ve çok kriterli karar verme gibi nicel yöntemler de kullanılabilir.
- Nicel verilerin bulunduğu ancak, belirsizliğin ve öznel faktörlerin etkili olduğu, uzman görüşünün ve sayısal analizlerin sentezlenmesi gerektiğinde hibrit yöntemler de kullanılabilir.

Diğer taraftan, olasılık ve etkilerin bilindiği risk durumlarında iştah ve tolerans seviyeleri somut olarak belirlenebilir ve önceliklendirme için kullanılabilir. Buna karşılık, yalnızca etkilerin öngörülebilir olduğu genel tehditlerde iştah ve tolerans seviyeleri ancak yaklaşık düzeyde tanımlanabilir. Diğer olumsuz durum türlerinde (genişleyen tehditler, örtük tehditler,

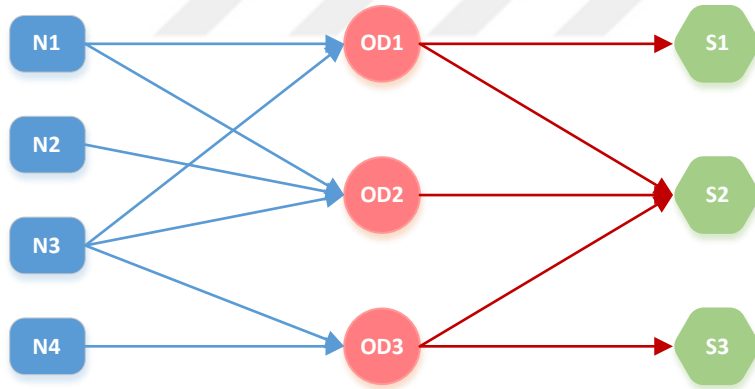
beliren tehditler, muğlaklık, belirsizlik ve cehalet) ise olasılık ve etkilerin ölçülemez veya öngörülemez olması nedeniyle iştah ve tolerans kavramları geçerli değildir.

Bu aşamada, aynı olumsuz durum sınıfında yer alan durumlar kendi içlerinde sıralanarak önceliklendirilebileceği gibi, sınıf farkı gözetilmeksizin durumlar arasında da önceliklendirme yapılabilir. Belirsizlik ve muğlaklık durumlarında olasılık ve etki bilgileri ile yayılma ve zincirleme etkiler gibi bilgiler söz konusu olmadığı için önceliklendirme yapılamaz. Dolayısıyla, muğlaklık ve belirsizlikler sınıfındaki durumlar planlama aşamasında değerlendirilmek üzere ODT’de korunur.

5.7.2.3. Neden, Olumsuz Durum ve Sonuç İlişkilerinin Kurulması

Öncelikli durum listesinde yer alan olumsuz durumların nedenleri ile gerçekleşmeleri halinde olası sonuçları belirlenir. Neden ve sonuçlar, durum özelinde tespit edilir. Ancak, bir neden, birden fazla durumu da etkileyebilir. Benzer şekilde birden fazla durum aynı sonuçları yaratabilir.

Şekil 23: Neden (N), Olumsuz Durum (OD) ve Sonuç (S) İlişkilerinin Kurulması



5.7.2.4. Ölçüm ve İzlemeye Yönelik Göstergelerin Belirlenmesi

Bu aşamada risk, tehdit ve belirsizliklere yönelik uygulanacak yanıt strateji ve eylemlerinin etkinliği ile başarısını ölçmek ve düzenli takip ederek iyileştirmeyi sürekli kılmak adına risk göstergeleri ile performans göstergeleri tanımlanır.

Risk göstergeleri, kuruluşun maruz kaldığı risklerin olasılık veya etki açısından değişimlerini gösteren erken uyarı sinyalleridir. Olay öncesine dair tanımlanan risk göstergeleri, risklerin erken tespit edilmesi ve yönetilmesi bakımından önem arz eder.

Performans göstergeleri, bir kurumun veya sürecin belirlenen hedeflere ulaşım ulaşmadığını ölçen göstergelerdir. Verimlilik, etkinlik ve kalitenin ölçülmesi amacıyla kullanılırlar. Öncül performans göstergeleri, girdilere ilişkin olup gelecekteki performansı öngörmeye yardımcı olur. Ardıl performans göstergeleri, elde edilen çıktılar, amaç ve hedeflerin gerçekleştirilmesinde nasıl ve ne ölçüde başarılı olduklarını gösterirler. Hedeflenen sonuçlara ulaşmadaki başarı seviyesi etkililik ile ifade edilmektedir.

Tehditler, genellikle erken uyarı sinyalleri ve durum farkındalığı göstergeleri ile izlenir. Altyapı arızaları, çevresel sinyaller, piyasadaki beklenmedik dalgalanmalar, siber saldırı girişimleri, sistem açıklıkları, güvenlik denetimlerinde bulunan açık sayısı gibi göstergeler kullanılabilir.

Yönelim, etki ve/veya olasılık gibi hususlar hakkında bilgi sahibi olunamadığı için belirsizliklere yönelik doğrudan gösterge tanımlanması mümkün olmayabilir. Belirsizliklerin azaltılması amacıyla bilgi edinme çalışmalarına devam edilir.

Her bir olumsuz duruma yönelik performans ve/veya risk göstergesi tanımlanması esastır. Bunun başarılamadığı durumlarda uzman görüşleri, düzenli aralıklarla gerçekleştirilen değerlendirme toplantıları, senaryo çalışmaları gibi yollarla etki değerlendirmeleri gerçekleştirilir ve izlemeye alınır.

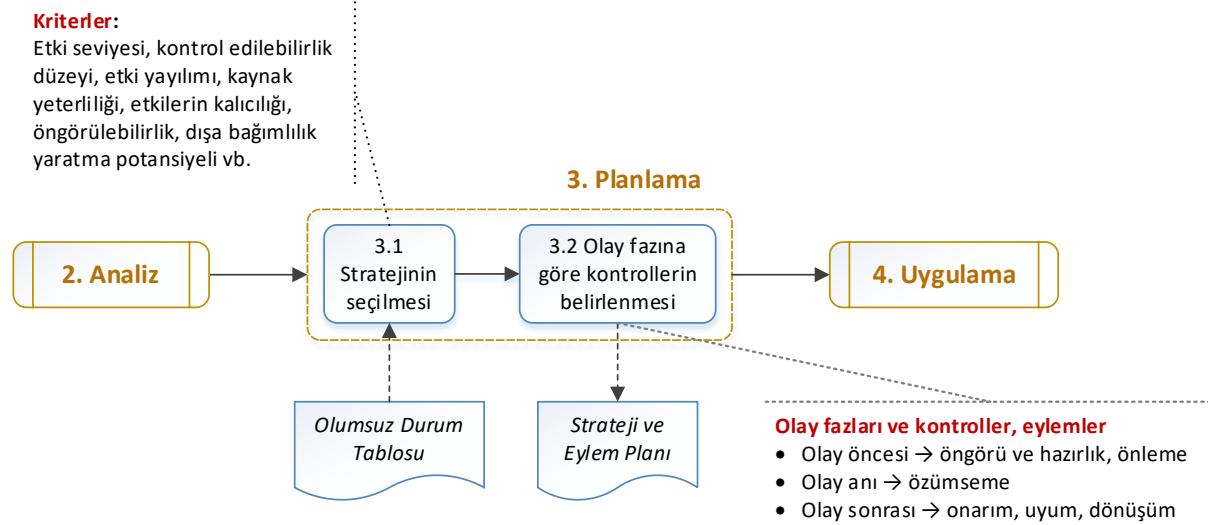
5.7.3. Planlama

Planlama aşaması, önceliklendirilmiş ve önleme, koruma ya da toparlanma amacıyla kendisine karşı kontrol eylemi uygulanmasına karar verilmiş olumsuz durumlara ilişkin stratejilerin seçilmesi ve bu stratejilerin uygulanmasına ilişkin eylemlerin belirlenmesi aşamasıdır.

Eylemler, olumsuz duruma yönelik olay öncesi, anı ve sonrası dikkate alınmak suretiyle belirlenir. Bu adımın sonunda, olumsuz durumlara karşı uygulanacak strateji ve kontrol eylemleri, müdahale fazları doğrultusunda belirlenmiş olur.

Bu aşama, stratejilerin seçilmesi ve olay fazına göre kontrollerin belirlenmesi olmak üzere iki alt adımdan (Şekil 24) oluşmaktadır.

Şekil 24: Planlama Aşaması



5.7.3.1. Yanıt Stratejilerinin Seçilmesi

Kuruluşlarda olumsuz durumlara karşı geliştirilen yaklaşımların seçiminde kuruluşun tutumu belirleyicidir. Kuruluşun durumu yönetmek üzere sahip olduğu insan kaynağı ve yetkinliği ile finansal, teknolojik ve yapısal kapasitesi dikkate alınmalıdır. İlave olarak, tercih edilen stratejinin uygulanabilirliği, maliyet etkinliği ve sürdürülebilirliği ile yasal düzenlemeler ve sektörel standartlarla uyumluluğu gözetilmelidir.

Anılan hususlarla birlikte, olumsuz durumlara yönelik stratejiler, mahiyetleri ile yer aldıkları sınıflar dikkate alınarak belirlenir. Yanıt stratejileri, öncelikle ilgili duruma yönelik risk stratejisinin seçilmesi, ardından bu stratejiyi destekleyecek dayanıklılık stratejilerinin belirlenmesi şeklinde iki adımdan oluşmaktadır. Aşağıda yer verilen Tablo 16 ve

Tablo 17, durum sınıflarına yönelik risk stratejileri ile bu stratejiler doğrultusunda tercih edilebilecek destekleyici dayanıklılık stratejilerini göstermektedir.

Tablo 16 ve

Tablo 17’de sunulan olumsuz durum sınıfına göre risk stratejileri ve bu stratejiler doğrultusunda belirlenen destekleyici dayanıklılık stratejilerine yönelik eşleştirmeler, olumsuz durumun mahiyeti ile strateji seçiminde değerlendirilmesi gereken maliyet, uygulanabilirlik, kuruluşun tutumu ve kapasitesi gibi kriterler çerçevesinde değişkenlik gösterebilir. Tablolardaki jenerik eşleştirmeler, karar vericilerde fikir oluşmasını teminen öneri olarak sunulmaktadır.

Tablo 16: Olumsuz Durum Sınıflarına Göre Uygulanabilir Risk Stratejileri

Olumsuz Durum Sınıfları	Uygulanabilir Risk Stratejileri
1. Risk ve 2. Genel Tehditler	Kaçınma / Sonlandırma, Azaltma, Transfer, Kabul, Paylaşma, Ayırma, Kopyalama, Çeşitlendirme
3. Genişleyen Tehditler	Azaltma, Transfer, Paylaşma, Çeşitlendirme, Ayırma
4. Beliren Tehditler	Azaltma, Paylaşma, Çeşitlendirme
5. Muğlaklık ve Belirsizlikler	Azaltma, Paylaşma, Ayırma, Kopyalama, Çeşitlendirme
6. Örtük Tehditler	Kaçınma / Sonlandırma, Azaltma, Kabul
7. Cehalet	Azaltma, Paylaşma, Kabul

Tablo 17: Risk Stratejilerini Destekleyen Dayanıklılık Stratejileri

Risk Stratejileri	Destekleyici Dayanıklılık Stratejileri
Kaçınma / Sonlandırma	Çeşitlilik, Modülerlik
Transfer	Ağ / İşbirliği ve Ortaklık, Çeşitlilik
Azaltma	Yedeklilik, Modülerlik, Kapasite Geliştirme
Paylaşma	Ağ / İşbirliği ve Ortaklık, Çeşitlilik
Ayırma	Modülerlik, Yedeklilik
Kopyalama	Yedeklilik, Modülerlik
Çeşitlendirme	Ağ / İşbirliği ve Ortaklık, Çeşitlilik
Kabul	Kapasite Geliştirme, Yedeklilik

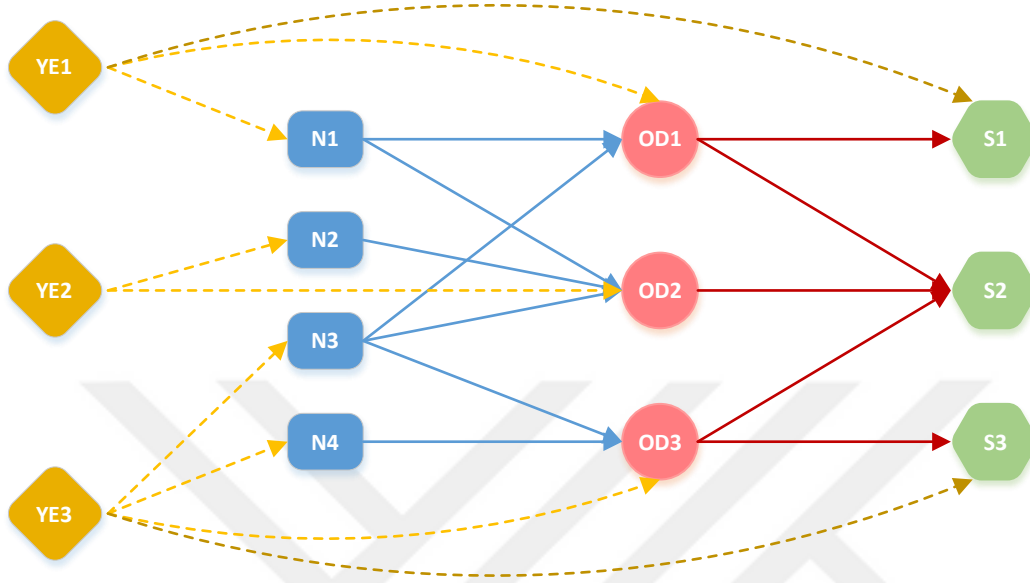
5.7.3.2. Olay Fazına Göre Kontrol Eylemlerinin Belirlenmesi

Stratejilerin uygulamaya geçirilmesini sağlayan eylemler, kuruluşların risk, tehdit ve belirsizliklere yönelik hazırlık, müdahale ve uyum kapasitelerini somut adımlarla hayata geçirir. Kontrol eylemleri, olumsuz durumların önlenmesi, etkilerinin (ve varsa olasılıklarını) azaltılması, bu durumlardan kaçınılması, transfer ya da kabul edilmesi ile olumsuz duruma kaynaklık eden ya da bu durumdan etkilenen ilgili alt birim, süreç ve operasyonların paylaşılması, ayrılması, kopyalanması ya da çeşitlendirilmesi kapsamında yürütülen planlı uygulamalardır.

Eylemlerin belirlenmesinde, neden - olumsuz durum - sonuç ilişkileri dikkate alınmalıdır. Söz konusu ilişkiler dikkate alınarak seçilecek bir yanıt eylemi birden fazla

nedeni ve/veya durumu ortadan kaldırabilir, etkisini azaltabilir. Bahse konu ilişkilendirme Şekil 25’te gösterilmektedir.

Şekil 25: Yanıt Eylemlerinin Neden, Olumsuz Durum ve Sonuçlar ile İlişkilendirilmesi



Şekilde, yanıt eylemi - neden - olumsuz durum - sonuç ilişkileri bütüncül olarak gösterilmektedir. Model, önleyici (nedenlere müdahale) ve düzeltici (sonuçlara müdahale) eylemleri içermektedir. İlave olarak tek bir nedenin birden çok olumsuz duruma, tek bir olumsuz durumun da birden çok sonuca yol açabileceği görülmektedir. Bu çerçevede çok yönlü etkilene gücüne sahip yanıt eylemlerinin seçilmesi maliyet etkinliğinin sağlanması ve modelin sadelik ilkesinin gereklerinin karşılanması bakımından önem arz etmektedir.

Bu adımda, her bir olumsuz duruma yönelik seçilen yanıt stratejisi doğrultusunda aşağıdaki soruların yanıtları aranır.

- Olumsuz durum henüz gerçekleşmeden, bu durumun önlenmesi ya da gerçekleşmesi durumundaki etkisinin azaltılması, sınırlandırılması amacıyla hangi tedbirler alınabilir?
- Durumların gerçekleştiği olay anında, kısa süre içinde devreye alınması gereken planlar ve eylem neler olabilir?
- Olayın gerçekleşmesiyle birlikte, uzun vadede toparlanma (onarım, adaptasyon ve dönüşüm) amaçlı neler yapılabilir?

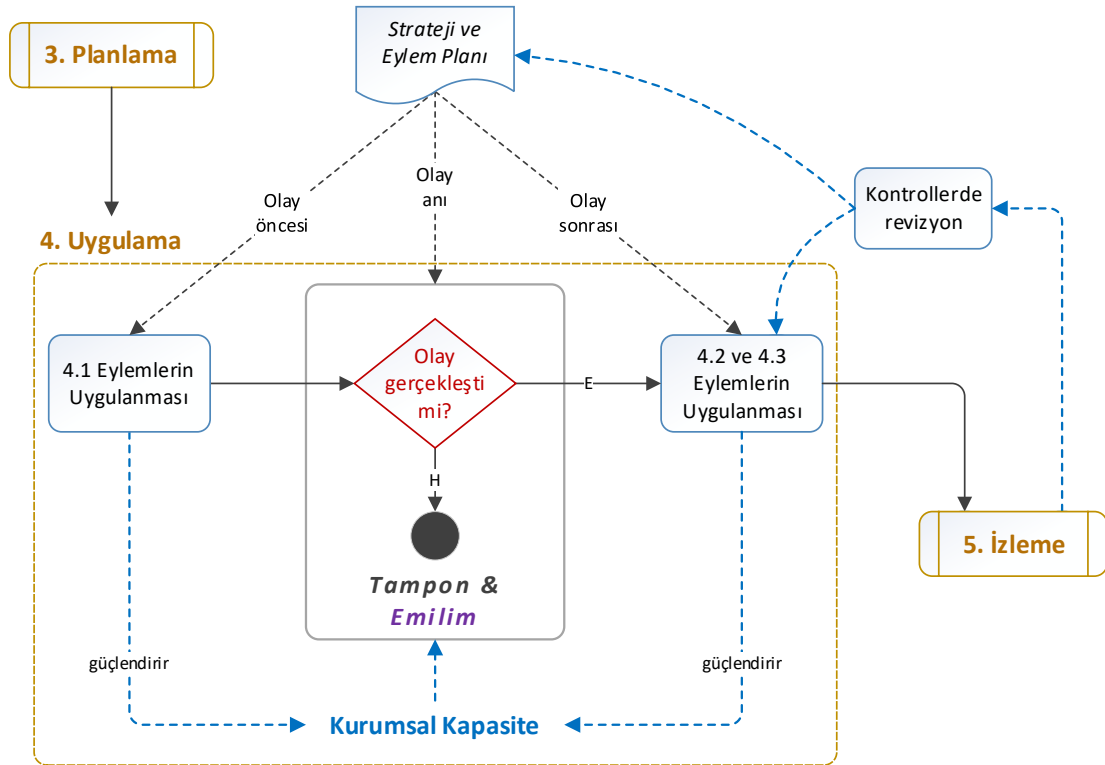
Sorulara verilen yanıtlar, müdahale fazlarına göre kontrol eylemlerinin belirlenmesinde yönlendirici rol oynar. Bu doğrultuda seçilen eylemlerin etkinliği göz önünde bulundurulmalıdır. Öncelikle, yanıt eylemi olumsuz durumun büyüklüğü ile orantılı ve duruma uygun olması gerekir. Eylemin sağlayacağı fayda maliyet dengesi gözetilmeli, eylem maliyetinin olası kaybı geçmemesine dikkat edilmelidir. Eylem, kurumun kapasitesi ve yetkinliği açısından uygulanabilir ve gerçekçi olmalıdır. Durumun ya da olayın büyüklüğü çerçevesinde paydaşların da görüşleri dikkate alınmalıdır.

5.7.4. Uygulama

Uygulama aşamasında, kurgulanan stratejilerin gerçek koşullar altında işlerlik kazanması sağlanır. Bu aşamada, olumsuz durumlara yönelik olarak planlama safhasında olay fazları dikkate alınarak geliştirilen stratejiler ve bu stratejilerden türetilmiş kontrol eylemlerinin fiilen hayata geçirilmesini sağlar.

Olay öncesi ve sonrası gerçekleştirilen uygulamalar kurumsal kapasiteyi güçlendiren geri beslemeler sağlar.

Şekil 26: Uygulama Aşaması



5.7.4.1. Olay Öncesine Yönelik Eylemlerin Hayata Geçirilmesi

Olay öncesinde, eylemlerin uygulanması daha çok önleyici ve hazırlık odaklıdır. Bu aşamada strateji ve eylem planındaki olumsuz durumlara yönelik olay öncesi faz için tasarlanan eylemler devreye alınır. Hazırlıklara yönelik planlanan sistem ve mekanizmaların tesis edilmesi, erken uyarı sistemlerinin devreye alınması, çeşitli eğitim ve tatbikatların yapılması ve kurumsal kapasitenin artırılması gibi eylemler gerçekleştirilir. Bu dönemde temel amaç, olumsuz durumun gerçekleşmesini engellemek ya da etkilerini en aza indirmektir.

Bu adımdaki eylemler aracılığıyla dayanıklılık kapasitesi artırılarak tampon ve emilim mekanizmaları güçlendirilir. Söz konusu mekanizmalar, olay öncesi, anı ve sonrasında her daim aktif olarak işlemeye devam eder. Tampon ve emilim mekanizmaları durum ve olayların etkilerini absorbe ederek işlevlerin tamamen çökmesini engellemeye çalışır. Bu sayede kesintilerin kapsamı daraltılır ve toparlanma için gerekli zeminin korunması sağlanır.

5.7.4.2. Olay Anına Yönelik Eylemlerin Hayata Geçirilmesi

Olayın gerçekleşmesiyle birlikte, olay anı ve sonrasındaki adımlara geçilir. Olay anındaki uygulamalar daha çok kriz yönetimi ve acil müdahale faaliyetlerini kapsar. Kriz yönetim planları doğrultusunda beklenmedik durum, acil durum, felaket kurtarma ve iş sürekliliği planları hızla devreye alınır. Amaç, olayın etkilerini sınırlamak, kritik işlevlerin devamlılığını sağlamak ve daha büyük kayıpların önüne geçmektir. Kaynakların etkin seferber edilmesi, kritik işlevlerin sürdürülebilmesi ve zincirleme etkilerin kontrol altına alınması bu aşamanın temel faaliyetleridir.

5.7.4.3. Olay Sonrasına Yönelik Eylemlerin Hayata Geçirilmesi

Olay sonrası aşama, olumsuz durumun etkilerinin giderilmesi, işlevselliğin yeniden kazanılması ve geleceğe yönelik dayanıklılığın artırılması açısından kritik bir süreci ifade eder. Bu aşamada temel amaç, kuruluşun yaşanan olaydan en az kayıpla çıkmasını, mümkün olan en kısa sürede operasyonel işlevlerini yeniden kazanmasını ve daha güçlü bir yapıya dönüşmesini sağlamaktır.

Kuruluş, olay sonrasında onarım (bounce back), adaptasyon (bounce forward) ve dönüşüm (build it better) yaklaşımlarından birini seçerek, toparlama çalışmalarını seçtiği yönde yoğunlaştırır. Planlama aşamasında tasarlanan eylemler hayata geçirilir.

Olay sonrası eylemler genel olarak öncelikle onarım faaliyetlerini kapsar. Fiziksel hasarların giderilmesi, sistemlerin yeniden işler hale getirilmesi, etkilenen süreçlerin devreye alınması ve normal işleyişin tesis edilmesi bu çerçevede yürütülen ilk adımlardır. Bunun yanı sıra, olayın kurumsal süreçlerde yarattığı kesintilerin kalıcı etkiler bırakmaması amacıyla restorasyon odaklı gerekli düzeltici ve iyileştirici faaliyetler hayata geçirilir.

Bu aşamanın ikinci boyutu, adaptasyon ve öğrenme süreçleridir. Kuruluşlar, yaşanan olaydan elde edilen deneyimleri kurumsal hafızaya aktararak benzer durumlara karşı daha hazırlıklı hale gelir. Olay sonrası yapılan incelemeler, risklerin yeniden değerlendirilmesi, eksik kalan noktaların tespiti ve yeni önlemlerin geliştirilmesi yoluyla gelecekteki dayanıklılık kapasitesi güçlendirilir.

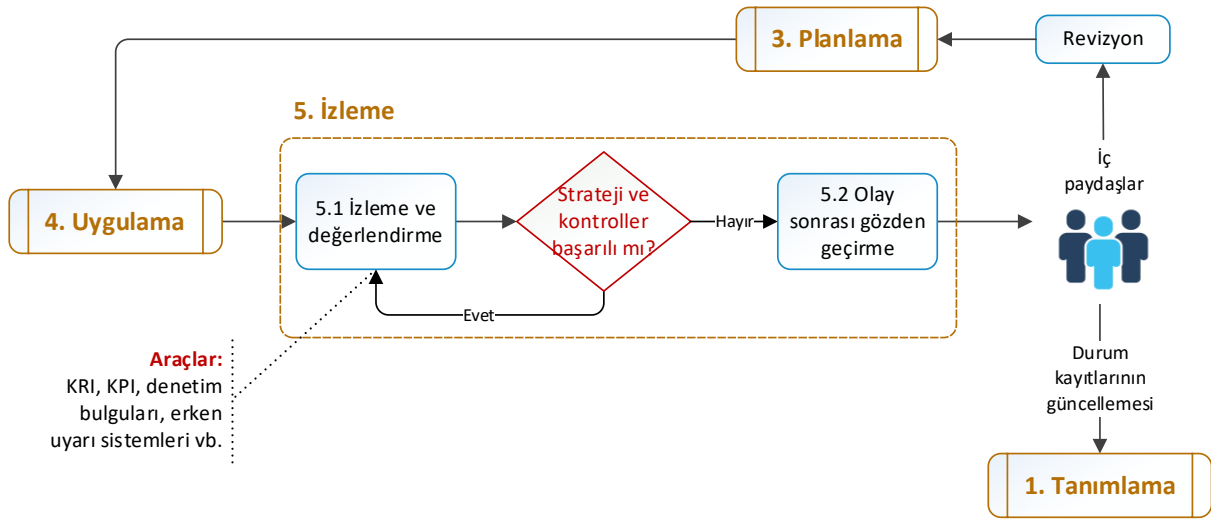
Diğer taraftan, olay sonrası süreçler dönüşüm kapasitesini harekete geçirme potansiyeli taşır. Özellikle büyük ölçekli krizler, yalnızca mevcut işleyişin onarılmasıyla sınırlı kalmamakta; aynı zamanda yapısal değişimlere ve stratejik yeniliklere de zemin hazırlamaktadır. Bu çerçevede, kuruluşlar değişen çevresel koşullara uyum sağlayacak yeni iş modelleri, organizasyonel düzenlemeler veya dijitalleşme temelli dönüşüm programları geliştirebilir.

Olay sonrası eylemler, sadece bir toparlanma süreci değil, aynı zamanda kurumsal öğrenme, kapasite geliştirme ve stratejik yenilenme için kritik bir fırsat alanıdır. Bu aşama, dayanıklılık döngüsünün sürekliliğini sağlayarak kuruluşların uzun vadeli sürdürülebilirliğini ve rekabet gücünü desteklemektedir.

5.7.5. İzleme

Süreç boyunca eylemlerin etkinliği sürekli değerlendirilir ve gerekiyorsa strateji ve kontrollerde revizyon yapılarak uygulamaya konulur. Revize edilen kontrollere ilişkin uygulamalar ve sonuçlar, tekrar 5. İzleme bölümüne bağlanır.

Şekil 27: İzleme Aşaması



5.7.5.1. Olay Sonrası Gözden Geçirme

Olay sonrası gözden geçirme, yaşanan olumsuz durumun etkilerinin değerlendirilmesi ve uygulanan strateji ile eylemlerin etkinliğinin analiz edilmesi sürecidir. Bu adım, aynı zamanda kuruluşun dayanıklılık kapasitesinin ne ölçüde başarılı olduğunu ortaya koyar. Temel amaç, dayanıklılık kapsamında hayata geçirilen uygulamaların güçlü ve zayıf yönlerini belirleyerek gelecekteki benzer durumlara karşı daha hazırlıklı bir yapı oluşturmaktır.

Bu süreçte öncelikle olayın gerçekleşme biçimi, etkileri ve müdahale sonuçları ayrıntılı şekilde incelenir. Uygulanan stratejilerin ve kontrollerin amaca uygunluğu, kaynak kullanımının etkinliği ve karar süreçlerinin başarısı gözden geçirilir. Elde edilen veriler, kayıtlara işlenerek kurumsal hafızanın güçlendirilmesi sağlanır.

Söz konusu strateji ve eylemlerin başarısız olması durumunda, eylemlerde revizyon yapılmak üzere planlama aşamasına dönüş yapılır. Revize edilen ya da yeni tanımlanan eylemler uygulamaya alınarak sonuçlar izlenir.

Olay sonrası gözden geçirme aynı zamanda öğrenme ve iyileştirme mekanizması olarak işlev görür. Olayın ortaya çıkışında etkili olan zayıflıkların, kapasite eksikliklerinin veya iletişim ve koordinasyon sorunlarının tespit edilmesi, gelecek planlamalarının geliştirilmesine katkı sunar. Bu çerçevede, yeni prosedürlerin tasarlanması, mevcut stratejilerin güncellenmesi veya ek kontrollerin geliştirilmesi gündeme gelebilir.

5.7.5.2. İzleme ve Değerlendirme

İzleme ve değerlendirme, modelin etkinliğinin sürekliliğini sağlamak amacıyla uygulanan strateji ve eylemlerin düzenli olarak gözden geçirilmesi sürecidir. Bu aşama, yalnızca gerçekleşen olaylardan sonra değil, olay öncesi ve olay sırasında alınan tedbirlerin de etkinliğini değerlendirmek için kritik öneme sahiptir. Temel amaç, kullanılan yöntemlerin hedeflere ne ölçüde ulaştığını ölçmek ve gerektiğinde düzeltici veya geliştirici aksiyonların alınmasını sağlamaktır.

İzleme sürecinde, performans göstergeleri, risk göstergeleri ve kapasite ölçütleri üzerinden veriler toplanır ve analiz edilir. Bu sayede, uygulanan kontrollerin öngörülen sonuçları verip vermediği, kaynakların ne kadar etkin kullanıldığı ve risklerin veya tehditlerin yönetiminde ne tür boşlukların bulunduğu belirlenir.

Öte yandan, olumsuz durumlar zaman içerisinde bu vasıflarını kaybedebilirler, başka bir olumsuz duruma ya da durum türüne dönüşebilirler. Bununla birlikte yeni olumsuz durumlar ortaya çıkabilir. Olumsuz durumlara yönelik izlenen stratejilerde değişime gitmek gerekebilir. Bu nedenle ODT belirli periyotlar halinde düzenli olarak güncellenmelidir.

Değerlendirme ise, toplanan verilerin sistematik bir şekilde analiz edilmesini ve karar vericilere geri bildirim olarak sunulmasını içerir. Bu aşamada, stratejilerin başarısı, olumsuz durumların yönetilme düzeyi, koordinasyon ve iletişim süreçlerinin işlevselliği gibi unsurlar göz önünde bulundurulur. Ayrıca, mevcut uygulamalardan elde edilen bulgular yeni bir risk önceliklendirme çalışmasına temel teşkil ederek sürecin döngüsel yapısını destekler.

Değerlendirmeler, düzenli raporlar şeklinde üst yönetime ve karar vericilere sunulur. Bu raporlarda ODT içerisinde izlenen olumsuz durumlara yönelik gösterge değerleri ile değişen, geçerliliğini yitiren, azaltılan, kabul edilen ve gerçekleşen durumlara ilişkin bilgiler yer alır.

5.8. Beklenen Değer ve Katkıları

Bu kısımda “Kuruluşlarda KRY ve DY’nin birlikte yönetilebilmesi amacıyla yeni bir ‘Dayanıklılık Odaklı KRY Modeli’nin geliştirilmesi, olumsuz durumların etkin bir şekilde yönetilmesi açısından nasıl bir katma değer yaratabilir?” şeklindeki araştırma sorusunun yanıtı aranacaktır.

Dayanıklılık Odaklı Kurumsal Risk Yönetimi modeli, KRY ve DY'nin birbirlerini tamamlayıcı yönlerini bütünleştirerek her iki yaklaşımın eksikliklerini tematik düzeyde kapatma kapasitesine sahiptir.

Model, KRY'nin sadece ölçülebilir ve hesaplanabilir risklere odaklanmasından kaynaklanan kapsam sınırlılığını aşarak ölçülemeyen durumları da yönetim kapsamına almakta, belirsizlik ve tehditleri ayrı kategoriler olarak ele almakta ve çeşitli risk ve performans göstergeleri aracılığıyla izlenebilir hale getirmektedir.

Ayrıca, tehdit ve ani şoklara karşı hazırlıklılık, yedeklilik, modülerlik ve çeşitlilik gibi dayanıklılık stratejilerini devreye sokarak KRY'nin kapsama alanını genişletmekte; karmaşık olay zincirlerini ise olay öncesi, olay anı ve olay sonrası olmak üzere çok katmanlı bir çerçevede ele alarak yönetilebilir kılmaktadır. Böylelikle model, ölçülebilir risklerle sınırlı kalan KRY yaklaşımına karşı bütüncül, esnek ve uyarlanabilir bir çözüm sunmaktadır.

Diğer taraftan önerilen model, KRY'deki kaynak (finansal, operasyonel ve teknolojik kaynaklar ile insan kaynağı) yetersizliği algısını aşmak üzere kaynak kullanımını optimize eden, ihtiyaç halinde esnek ve uyarlanabilir bir kaynak yönetimini öngörmektedir. Kaynaklar, diğer alanlarda kullanılmak üzere modüler tasarım ve yönlendirme bakış açısıyla yönetilmektedir.

Model olumsuz durumları risk, tehdit ve belirsizlikler şeklinde kategorilere ayrıştırarak itibar gibi maddi olmayan, karmaşık veya ölçülmesi zor durumların doğasının daha net anlaşılmasını ve bu yolla soyut olanın yönetilebilir hale getirilmesini sağlar.

Ölçülmesi zor durumlar için yalnızca “etkiyi tam hesaplamaya” çalışmak yerine, uygun dayanıklılık stratejileri (çeşitlilik, modülerlik, yedeklilik) ve kontroller devreye alınır. Böylece ölçümdeki belirsizlik, pratik tamponlama ve esneklikle telafi edilir. Modelin döngüsel yapısı, her olaydan sonra geri bildirim alınmasını zorunlu kılar. Bu sayede “başta ölçülemeyen” karmaşık risklerin etkileri zamanla veri birikimiyle daha iyi anlaşılır, ölçüm yetkinliği artar.

Bir başka husus, KRY'nin rolünün çoğunlukla olay öncesinde risklerin önlenmesi ve azaltılması ile sınırlı kalması, risklerin gerçekleşme durumlarına yönelik olay öncesinde bir hazırlığın (beklenmedik durum planları) yapılmamasıdır. Dayanıklılık odaklı KRY modeli, olay öncesindeki hazırlığa ilave olarak, olay anı ve sonrası için de planlama yapılmasını öngörmekte, bu amaçla onarım, uyum ve dönüşüm için ihtiyaç duyulan toparlanma kapasitesinin geliştirilmesini sağlamaktadır. Böylece model, kurumlara bütüncül bir hazırlık ve toparlanma çerçevesi sunmaktadır.

Model olumsuz durumları yalnızca tekil ve izole değil, aynı zamanda birbirini tetikleyen ve karmaşık olay zincirleri yaratan unsurlar olarak değerlendirmekte; bu sayede sistemsel kırılmalıkların görünür kılınmasını ve yönetim kapsamına alınmasını sağlamaktadır.

KRY genellikle statik çerçevelere dayanmakta ve bu nedenle hızlı değişen koşullara karşı yavaş tepki vermektedir. Dayanıklılık odaklı KRY modeli, dinamik ve uyarlanabilir yapısıyla değişen çevresel, teknolojik ve toplumsal koşullara hızlı tepki verilmesini sağlamaktadır. Model, esneklik, öğrenme ve sürekli güncelleme mekanizmalarını içeren yaklaşımıyla KRY'nin statik yapısını aşarak kurumlara çevik bir risk ve dayanıklılık yönetimi imkânı sunmaktadır.

Dayanıklılık odaklı KRY modeli, risk yönetimini sadece koruyucu bir uyum ve kontrol mekanizması şeklinde değil, aynı zamanda proaktif ve fırsat odaklı bir süreç olarak ele almakta, kurumların değişime uyum sağlama, yenilik geliştirme ve dönüşüm kapasitesi üzerinden değer yaratmasını mümkün kılmaktadır. Böylece model, KRY'yi uyum odaklı bir yük olmaktan çıkararak stratejik bir rekabet aracı haline getirmektedir.

Diğer taraftan, aşağıda değinildiği üzere DY'nin de teori ve uygulamada çeşitli sınırlılıkları ve yetersizlikleri söz konusudur.

Dayanıklılık, farklı şekillerde tanımlandığı için ortak bir uygulama standardı oluşturmak güçtür ve bu durum ölçüm ve yönetim konularında belirsizlik yaratmaktadır. Dayanıklılık odaklı KRY modeli ise dayanıklılık ilkelerini KRY süreci ile bütünleştirerek kurumsal düzeyde ortak bir çerçeve sunmakta, ölçüm için performans ve risk göstergelerini, yönetim içinse olay öncesi–anı–sonrası fazlarını temel alan standartlaştırılmış bir yaklaşım geliştirmektedir. Böylece model, disiplinler arası dağınıklığı azaltarak dayanıklılığın kurum içinde daha net tanımlanmasını, ölçülmesini ve yönetilmesini mümkün kılmaktadır.

Dayanıklılık kavramı soyut ve çok boyutlu yapısı nedeniyle KRY'de olduğu gibi sistematik bir metodoloji sunmamakta, bu da uygulamada farklı yorumlara ve dağınık, parçalı yaklaşımlara yol açmaktadır. Dayanıklılık odaklı KRY modeli ise KRY'nin metodolojik yapısını dayanıklılık ilkeleriyle bütünleştirerek soyut kavramı somut süreçlere, göstergelere, strateji ve eylemlere dönüştürmektedir. Böylece model, birimler, fonksiyonlar özelindeki parçalı uygulamalar yerine bütüncül, sistematik ve operasyonel olarak uygulanabilir bir çerçeve ortaya koymaktadır.

Model, risk yönetiminin operasyonel boyutuna ilave olarak stratejik boyutunu dayanıklılıkla bütünleştirerek belirsizlik, tehdit ve risklerin sadece olumsuz etkilerini değil,

bunların kabul edilmesinden doğabilecek fırsat ve maliyetleri de değerlendirmektedir. Böylece model, “kesintiden kurtulma” odaklı operasyonel yaklaşımı aşarak risk–getiri dengesi (örneğin, belirli bir belirsizliği, tehdidi ya da riski kabul etmenin yaratacağı fırsat ya da maliyeti) üzerinden stratejik düzeyde değer yaratma kapasitesini geliştirmektedir.

Dayanıklılık odaklı KRY modeli, sayısallaştırılması genelde mümkün olmayan soyut boyutları yönetilebilir hale getirmek için performans ve risk göstergeleri ile niteliksel değerlendirme yöntemlerini bir arada kullanarak dayanıklılığı izlenebilir ve karar süreçlerine entegre edilebilir hale getirmektedir. Böylece model, soyut kapasite unsurlarını somut karar mekanizmalarıyla buluşturan uygulanabilir bir çerçeve sunmaktadır.

Dayanıklılık çoğu zaman uzun vadeli sürdürülebilirlik çerçevesinde konumlanmakta, ancak kurumların kısa vadeli öncelikleri ve kaynak kısıtları nedeniyle uygulamada geri planda kalmaktadır. Dayanıklılık odaklı KRY modeli ise dayanıklılığı yalnızca uzun vadeli bir hedef olarak değil, kısa vadeli karar ve kaynak tahsis süreçlerine entegre edilen bir unsur olarak ele almakta, böylece stratejik sürdürülebilirlik ile operasyonel gereklilikler arasında köprü kurarak dayanıklılığın pratikte uygulanabilirliğini artırmaktadır.

Dayanıklılık çoğunlukla operasyonel krizlerden sonra gündeme gelmekte ve yalnızca “toparlanma” ile sınırlandırılmakta, risk yönetimi süreçleriyle bütünleşmediğinde ise proaktif bir değer yaratamamaktadır. Model, dayanıklılığı risk yönetimi sürecinin ayrılmaz bir parçası haline getirerek kriz sonrası toparlanmanın ötesine geçmekte, olay öncesi hazırlık, olay anı yönetimi ve olay sonrası onarım, uyum ve dönüşümü kapsayan bütüncül bir çerçeve sunmaktadır. Böylece model, proaktif değer yaratma kapasitesini güçlendirerek dayanıklılığı kurumsal yönetimin stratejik bir unsuru haline getirmektedir.

Bu bütünleşik yaklaşım sayesinde model, KRY ve DY’nin tek başlarına ulaşamayacağı bir sinerji yaratarak, kuruluşlara belirsizlik ve tehditler karşısında esnek, sistematik ve stratejik bir yönetim çerçevesi sunmaktadır.

SONUÇ VE ÖNERİLER

Son yıllarda iş dünyası, her geçen gün belirsizliklerin arttığı, karmaşıklığın derinleştiği, değişkenliğin hız kazandığı ve öngörülemez gelişmelerin sıkça yaşandığı dinamik bir ortama dönüşmektedir. Ani şoklar ve karmaşık olay zincirleri, yalnızca yerel ölçekte değil, küresel düzeyde de kuruluşların işleyişini kesintiye uğratmaktadır.

Örneğin, COVID-19 pandemisi küresel ölçekte üretim ve tedarik ağlarını durma noktasına getirirken; Rusya–Ukrayna savaşı enerji arz güvenliğini derinden sarsmış, yarı iletken kıtlığı otomotivden teknolojiye kadar birçok sektörde üretim krizine yol açmıştır. Benzer şekilde, Süveyş Kanalı’nın kapanması gibi lojistik şoklar milyarlarca dolarlık kayıplara neden olmuş, büyük ölçekli siber saldırılar ve toplumsal olaylar ise şirketlerin operasyonel sürekliliğini tehdit etmiştir. Türkiye’de yaşanan büyük deprem felaketi ise, beklenmedik afetlerin hem ekonomik hem de sosyal düzeyde ne denli yıkıcı sonuçlar doğurabileceğini bir kez daha ortaya koymuştur.

Böylesine dalgalı bir ortamda kuruluşlar, olumsuz durumlarla baş edebilmek için farklı yönetim araçlarına başvurmaktadır. Bir yandan ölçülebilir riskleri tanımlamaya, değerlendirmeye ve kontrol etmeye odaklanan kurumsal risk yönetimi (KRY) sistemleri kullanılmakta; diğer yandan belirsizliklere, ani şoklara ve uzun vadeli tehditlere karşı daha esnek ve uyumlu çözümler geliştirmeyi amaçlayan kurumsal dayanıklılık yönetimi (DY) kapsamındaki uygulamalar devreye sokulmaktadır.

KRY ve DY’nin ayrı ayrı uygulanması, kuruluşlara yalnızca sınırlı bir koruma sağlamakta ve bütüncül bir güvence oluşturmamaktadır. KRY daha çok risklerin önceden analiz edilmesine ve önlenmesine odaklanırken, DY ağırlıklı olarak kriz sonrası toparlanmayı hedeflemektedir. Bu parçalı yapı, kurumların bütünsel değer yaratma kapasitesini zayıflatmaktadır. Oysa günümüzün belirsiz, değişken ve öngörülemez koşulları, risk ve belirsizliklerin hem koruyucu hem de uyarlanabilir ve stratejik bir bakış açısıyla bütünleşik olarak yönetilmesini gerekli kılmaktadır.

Bu doğrultuda, söz konusu araçların anılan olumsuz durumların yönetilmesindeki etkinliğine yönelik gerçekleştirilen literatür analizinde her iki aracın da müstakil kullanımlarında bir takım sınırlılık ile yetersizliklere sahip olduğuna yönelik bulgulara ulaşılmıştır.

Özellikle araçların kapsamı, devreye alındıkları zamanlama boyutu, sağladıkları stratejik katkı ve bütünsellik düzeyinde ortaya çıkan söz konusu sınırlılıklar, her iki yaklaşımın güçlü yönlerinin yanında zayıf yönlerini de açık biçimde görünür kılmıştır.

KRY, ölçülebilir ve hesaplanabilir risklere odaklanması nedeniyle belirsizlikler ve ani şoklar karşısında yetersiz kalmakta; maliyetli, bürokratik ve sürdürülemez bir araç olarak algılanabilmektedir. Ayrıca riskleri genellikle tekil biçimde ele alması zincirleme etkilerin ve sistemsal kırılganlıkların göz ardı edilmesine yol açmakta; statik çerçevelere dayanması nedeniyle hızlı değişen koşullara yavaş tepki vermektedir. Uyum ve kontrol odaklı yönü ise KRY'nin stratejik değer yaratma işlevini zayıflatmaktadır.

Dayanıklılık Yönetimi (DY) açısından da çeşitli sınırlılıklar dikkat çekmektedir. Farklı disiplinlerde farklı tanımlanması, ortak standartların ve ölçüm yöntemlerinin oluşmasını engellemekte; soyut ve çok boyutlu yapısı sistematik bir metodoloji geliştirilmesini zorlaştırmaktadır. DY çoğunlukla operasyonel kriz yönetimi ve toparlanmaya indirgenmekte, risk–getiri dengesi gibi stratejik boyutları dikkate almamaktadır. Kurumsal kapasite, ağlar ve adaptasyon gibi soyut boyutların ölçülmesindeki zorluklar, uygulamaların etkinliğini sınırlamakta; uzun vadeli sürdürülebilirliğe odaklanması ise kısa vadeli önceliklerin geride kalmasına yol açmaktadır.

Araştırmanın ortaya koyduğu bir diğer önemli bulgu, KRY ve DY'nin aslında birbirini tamamlayan yapılar olduğudur. KRY metodoloji, süreç ve yapı sağlarken, DY esneklik, uyarlanabilirlik, yenilikçilik ve bütüncül bakış açısı kazandırmaktadır.

Bulgular, KRY'nin çoğunlukla ölçülebilir risklere ve hesaplanabilir parametrelere odaklanması nedeniyle belirsizlikler ve öngörülemeyen olaylar karşısında sınırlı kaldığını göstermektedir. DY ise operasyonel düzeyde krizlerden sonra gündeme gelmekte, stratejik karar alma süreçlerinde yeterince kullanılmamakta ve çoğu zaman soyut bir kavram olarak görülmektedir. Bu eksiklikler, kurumların uzun vadeli sürdürülebilirliğini ve rekabet avantajını tehlikeye atmaktadır. Her iki aracın yetkinliklerinin birlikte değerlendirilmesi ve bağımsız kullanımlarından doğan sınırlılıkların aşılması önem taşımaktadır.

Bu doğrultuda, tez çalışmasında, ortaya konulan bulgularda bahsedilen sınırlılık ve yetersizliklerin aşılması amacıyla KRY ile DY'yi bünyesinde sentezleyen bütünleşik bir yaklaşım önerisi geliştirilmiştir.

Önerilen Dayanıklılık Odaklı KRY Modeli, KRY'nin metodolojik yapısı ile DY'nin esnek ve kapsayıcı bakış açısını bütünleştirerek, kurumlara hem olay öncesi hazırlık hem de

olay anı ve sonrası için uygulanabilir bir çerçeve sunmaktadır. Böylece kurumların sadece riskleri azaltma değil, aynı zamanda belirsizlikleri yönetme, tehditlere yanıt verme, beklenmedik olaylardan öğrenme ve uzun vadeli değer yaratma kapasiteleri güçlenmektedir.

Modelin teori ve pratik bağlamında sunduğu katkılar çok boyutlu durum ve olay yönetimi, olay fazlı müdahale yapısı, dayanıklılık stratejilerinin entegrasyonu, gösterge ve ölçüm sistematigi, geri bildirim ve öğrenme döngüsü, bütünleşik ve stratejik yönetim çerçevesi, paydaş katılımı ve ortak değer, ölçeklenebilirlik ve uygulanabilirlik olmak üzere 8 temel başlıkta toplanabilir.

Model, kuruluşlara çok boyutlu olay yönetimi perspektifi sunmaktadır. Geleneksel risk yönetimi ölçülebilir risklere odaklanırken, önerilen model risklerin yanı sıra belirsizlik, tehdit ve krizleri de yönetim sürecine dâhil etmektedir. Böylelikle yalnızca olasılık-etki temelli yaklaşımlarla sınırlı kalmamakta, farklı belirsizlik türlerine (örneğin aleatorik, epistemik ve ontolojik) özgü stratejilerle çok katmanlı bir yönetim çerçevesi geliştirmektedir.

Bir diğer katkı, olay fazlı müdahale yaklaşımıdır. Model, olumsuz durumları yalnızca öncesi veya sonrası ile sınırlı tutmayıp, olay öncesi hazırlık, olay anındaki müdahale ve olay sonrası izleme-öğrenme-dönüşüm aşamalarını bütünleşik bir yapıda ele almaktadır. Bu fazların kesintisizliği sayesinde önleme, mücadele ve toparlama süreklilik arz eden bir mekanizma haline gelmekte ve döngüsel ve dinamik işleyiş, statik risk yönetimi modellerinden önemli ölçüde farklılaşmaktadır.

Model aynı zamanda dayanıklılık stratejilerinin entegrasyonunu da sağlamaktadır. Risk yanıt planları yedeklilik, çeşitlilik, modülerlik, hazırlıklılık, iş birliği ve kapasite geliştirme gibi stratejilerle desteklenmektedir. Bu sayede olumsuz durumların tamamen engellenemediği hallerde dahi tampon ve emilim kapasitesi devreye girerek etkiler sınırlandırılmakta ve sistemin işlevselliği korunmaktadır. Ayrıca strateji-faz-eylem zincirinin kurumsal kapasiteyle doğrudan bağlantılı olması, modelin sürdürülebilirliğini güvence altına almaktadır.

Ölçüm ve değerlendirme boyutunda model, anahtar risk göstergeleri (KRI) ile anahtar performans göstergelerinin (KPI) birlikte kullanımını öngörmektedir. Olay öncesinde erken uyarı sağlamak için KRI'lar, olay sonrasında etkinliği ölçmek için KPI'lar kullanılmakta; böylece ölçüm yalnızca risk kontrolüne değil, aynı zamanda performans değerlendirmesi ve iyileştirmeye dayalı bütünsel bir sistematige dönüşmektedir.

Modelin önemli bir katkısı da geri bildirim ve öğrenme döngüsüdür. Olaylardan elde edilen derslerin kurumsal hafızaya entegre edilmesi ve başarısız strateji ya da kontrollerin hızla

revize edilmesi, modelin sürekli gncellenmesini saęlamaktadır. Bylece model, sadece tepki veren deęil, aynı zamanda ğrenen adaptif bir yapıya dnşmektedir.

Btnleşik ve stratejik ynetim çerçevesi de modelin katkıları arasındadır. KRY'nin metodolojik ve sreç odaklı yapısı, DY'nin esneklik, adaptasyon ve yenilikçi ynleriyle bir araya getirilerek parçalı yaklaşımların tesinde btncl bir anlayış geliştirilmiştir. Bu sayede kurumlara yalnızca koruyucu deęil, aynı zamanda proaktif ve stratejik deęer yaratıcı bir işlev kazandırılmakta; risklerin azaltılmasıyla birlikte belirsizliklerden doęan stratejik fırsatların deęerlendirilmesi de mmkn hale gelmektedir.

Modelin kurumsal yansımaları çok boyutlu bir çerçevede deęerlendirilebilir. Model, kurumlarda yalnızca teknik sreçleri deęil, aynı zamanda kltrel yapıyı da dnştrr. Psikolojik gvenlik, kolektif ğrenme ve çalışan katılımını teşvik ederek “ğrenen organizasyon” kltrnn yerleşmesine katkı saęlar. Bu da kurumsal dayanıklılıęın sadece kriz anına ynelik bir kapasite deęil, gnlk işleyişe yerleşmiş bir davranış biçimi olmasını mmkn kılar.

Model, risk ve dayanıklılık sreçlerini stratejik hedeflerle ilişkilendirerek st ynetim dzeyinde daha gçl bir hesap verebilirlik saęlar. Stratejik planlama sreçlerine entegre edilen risk ve dayanıklılık analizleri, olası engellerin belirlenmesine ve bunlara ynelik uygun stratejilerin geliştirilmesine imkân tanır. Bu yaklaşım, KRI ve KPI gstergeleri arasındaki baęlantıyı gçlendirerek risk takibi ile stratejik başarı lçmn aynı sistemde btnleştirir. Bylece stratejik hedeflere ulaşma yolları esnekleştirilir ve kriz dnemlerinde stratejiler gncellenebilir hale gelir.

Olay fazlı yaklaşım, karar sreçlerini yalnızca kriz anına odaklı olmaktan çıkarır. Hazırlık, olay anı ve sonrası aşamalarıyla desteklenen btncl yapı, kurumlarda daha proaktif, uzun vadeli ve esnek karar alma alışkanlıęı oluşturur. Bu da kuruluşların belirsizlikleri ynetme becerisini gçlendirir.

Model, yedeklilik ve esnek kaynak tahsisini n plana çıkararak kurumların btçeleme ve planlama sreçlerini etkiler. Kaynak ynetiminde yalnızca mali verimlilik deęil, dayanıklılık yatırımları da stratejik ncelik haline gelir. Bylece organizasyonlar hem krizlere direnç kazanır hem de srdrlebilirliklerini gvence altına alır.

Model, krizleri yalnızca tehdit olarak deęil, aynı zamanda inovasyon iin bir fırsat olarak grr. Olaylardan ğrenme ve dnşm sreçlerinin entegre edilmesi, yenilikçi uygulamaların

hızla hayata geçirilmesine olanak tanır. Bu da modelin yalnızca savunma mekanizması değil, aynı zamanda kuruma değer yaratıcı bir işlev kazandırmasını sağlar.

Ayrıca model, risk ve dayanıklılık kavramları arasında köprü kurarak yalnızca risklerin azaltılmasını değil, aynı zamanda şokların absorbe edilmesi, uyum sağlanması ve dönüşüm kapasitesinin güçlendirilmesini sağlayarak uzun vadeli kurumsal sürdürülebilirliğe katkıda bulunmaktadır.

Model aynı zamanda paydaş katılımı ve ortak değer yaratma boyutunu öne çıkarmaktadır. İç paydaşların yanı sıra tedarikçiler, kamu otoriteleri ve toplum gibi dış paydaşların katılımı sağlanmakta; iletişim, koordinasyon ve iş birliği süreçleri yönetim döngüsüne dâhil edilmektedir. Böylece kurumsal dayanıklılık yalnızca içsel süreçlerle sınırlı kalmayıp, ekosistem düzeyinde güçlendirilmektedir.

Son olarak, modelin ölçeklenebilirlik ve uygulanabilirlik özelliği, farklı sektörlerde ve farklı büyüklükteki kurumlarda kullanılabilmesini mümkün kılmaktadır. Strateji, faz ve eylem zincirinin kurumsal kapasiteyle ilişkilendirilmesi, uygulanabilirliği güvence altına almakta; bu esneklik, modelin hem akademik alanda hem de pratik düzeyde geniş bir kullanım alanı bulmasını sağlamaktadır.

Bu araştırma, kavramsal ve teorik bir model geliştirmeyi hedeflediğinden, modelin ampirik olarak test edilmesi çalışmanın kapsamı dışında kalmaktadır. Önerilen Dayanıklılık Odaklı Kurumsal Risk Yönetimi Modeli, literatür taraması ve mevcut standartların analizi üzerinden geliştirilmiş olup, jenerik bir yapı ortaya konulmaktadır.

Modelin hâlihazırda teorik olması ve henüz sahada test edilmemiş olmasına istinaden uygulanabilirliği bağlamında bazı hususların değerlendirilmesi gerekmektedir. Özellikle farklı sektörlerin kapasite düzeyleri, kaynak yapıları ve kültürel dinamikleri modelin ölçeklenebilirliğini sınırlayabilir. Ayrıca belirsizlik türlerinin pratikte ayrıştırılması ve her birine özgü stratejilerin uygulanması, kurumların metodolojik olgunluk seviyesine bağlı olarak değişkenlik gösterebilir. Bu nedenle, modelin etkinliğinin farklı bağlamlarda test edilmesi, akademik literatüre olduğu kadar uygulamaya da katkılar sağlayacaktır.

İlave olarak, KRY ve DY entegrasyonunu ölçmeye yönelik metodolojilerin geliştirilmesi, alandaki teorik tartışmaları zenginleştirecektir. Yönetim bilimi, örgütsel davranış, stratejik yönetim, sistem mühendisliği ve kriz yönetimi gibi alanlardan beslenen disiplinler arası araştırmalar, modelin teorik zenginliğini artıracaktır.

Bu tez, KRY ve DY'nin sınırlılıklarını ortaya koymuş, bunların birbirini tamamlayıcı niteliklerini vurgulamış ve eksiklikleri gidermeye yönelik özgün bir Dayanıklılık Odaklı KRY Modeli önermiştir. Model, olay öncesi hazırlık, olay anı müdahale ve olay sonrası izleme-öğrenme süreçlerini bütünleştiren döngüsel yapısıyla hem teorik hem de pratik düzeyde önemli katkılar sunmaktadır.

Sonuç olarak, önerilen model, artan belirsizlikler, karmaşık tehditler ve ani şokların hâkim olduğu günümüz iş dünyasında kurumların yalnızca risklere karşı korunmasını değil, aynı zamanda değişime uyum sağlayarak değer yaratmasını mümkün kılmaktadır. Bu yönüyle, sürdürülebilirlik ve rekabet avantajı elde etmek isteyen tüm kurumlar için uygulanabilir, bütüncül ve yenilikçi bir yönetim yaklaşımı olarak değerlendirilmektedir.



KAYNAKLAR

- Abimbola, M., & Khan, F. (2019). Resilience modeling of engineering systems using dynamic object-oriented Bayesian network approach. *Computers & Industrial Engineering*, 130, 108-118. <https://doi.org/10.1016/j.cie.2019.02.022>
- Adebiyi, O., Adeoti, M., & Mupa, M. N. (2025). The use of employee ownership structures as strategies for the resilience of smaller entities in the US. *International Journal of Science and Research Archive*, 14(1), 1002-1018. <https://doi.org/10.30574/ijrsra.2025.14.1.0039>
- Adger, W. N. (2000). Social and ecological resilience: Are they related? *Progress in Human Geography*, 24(3), 347-364. <https://doi.org/10.1191/030913200701540465>
- Afifa, Y. N., & Santoso, I. (2022). Proactive risk mitigation strategies and building strategic resilience in the foodsupply chain: A review. *Food Research*, 6(2), 9-17. [https://doi.org/10.26656/fr.2017.6\(2\).257](https://doi.org/10.26656/fr.2017.6(2).257)
- AICPA. (2018). *Practice Aid: Enterprise Risk Management: Guidance for Practical Implementation and Assessment*. Association of International Certified Professional Accountants.
- AIRMIC. (2018). *Explained: Risk and Managing Risk A Short Guide*. AIRMIC and Marsh.
- Akçakanat, Ö. (2012). Kurumsal Risk Yönetimi Ve Kurumsal Risk Yönetim Süreci. *Süleyman Demirel Üniversitesi Vizyoner Dergisi*, 4(7), 30-46.
- Aksay, K., & Şendoğdu, A. (2022). Improving Organizational Resilience in Businesses: A Qualitative Study on the Effect of COVID-19. *Journal of Economy Culture and Society*, 0(0), 0-0. <https://doi.org/10.26650/JECS2021-1040786>
- Alawattagama, K. K. (2022). Enterprise risk management: Challenges and the strategies for success. *International Journal of Research in Business and Social Science* (2147- 4478), 11(6), 110-115. <https://doi.org/10.20525/ijrbs.v11i6.1931>
- Aldea, A., Vaicekauskaitė, E., Daneva, M., & Sebastian Piest, J. P. (2020). Assessing Resilience in Enterprise Architecture: A Systematic Review. *2020 IEEE 24th International Enterprise Distributed Object Computing Conference (EDOC)*, 1-10. <https://doi.org/10.1109/EDOC49727.2020.00011>

- Aldianto, L., Anggadwita, G., Permatasari, A., Mirzanti, I. R., & Williamson, I. O. (2021). Toward a Business Resilience Framework for Startups. *Sustainability*, 13(6), 3132. <https://doi.org/10.3390/su13063132>
- Alexander, D. E. (2013). Resilience and disaster risk reduction: An etymological journey. *Natural Hazards and Earth System Sciences*, 13(11), 2707-2716. <https://doi.org/10.5194/nhess-13-2707-2013>
- Aliekperov, A. (2021). *Creating Business and Corporate Strategy: An Integrated Strategic System* (1. bs). Routledge. <https://doi.org/10.4324/9781003172567>
- Alleman, G. B., & Quigley, J. M. (2024). *Risk Management* (1. bs). Auerbach Publications. <https://www.taylorfrancis.com/books/9781003425465>
- Alspach, J. G. (2017). The Checklist: Recognize Limits, but Harness Its Power. *Critical Care Nurse*, 37(5), 12-18. <https://doi.org/10.4037/ccn2017603>
- Amoroso, S., Moncada-Paternò-Castello, P., & Vezzani, A. (2017). R&D profitability: The role of risk and Knightian uncertainty. *Small Business Economics*, 48(2), 331-343. <https://doi.org/10.1007/s11187-016-9776-z>
- Amuah, J. (2023). *Leveraging the Proactive Power of Enterprise Risk Management*. <https://ssrn.com/abstract=4624088> or <http://dx.doi.org/10.2139/ssrn.4624088>
- Andrés, B., & Poler, R. (2013). Enhancing Enterprise Resilience through Enterprise Collaboration. *IFAC Proceedings Volumes*, 46(9), 688-693. <https://doi.org/10.3182/20130619-3-RU-3018.00283>
- Annarelli, A., & Nonino, F. (2016). Strategic and operational management of organizational resilience: Current state of research and future directions. *Omega*, 62, 1-18. <https://doi.org/10.1016/j.omega.2015.08.004>
- ANSI. (2009). *ASIS SPC.1 Organizational Resilience: Security, Preparedness, and Continuity Management Systems—Requirements with Guidance for Use*. American National Standards Institute, Inc.
- Arizzi, S., Egger, M., Rittenhouse, D., & Williams, P. (2014). Corporations and Resilience 9. İçinde R. Kupers (Ed.), *Turbulence A Corporate Perspective on Collaborating for Resilience*. Amsterdam University Press, Project Muse.

- Assibi, A. T. (2022). The Role of Enterprise Risk Management in Business Continuity and Resiliency in the Post-COVID-19 Period. *OALib*, 09(06), 1-19. <https://doi.org/10.4236/oalib.1108642>
- Assibi, A. T. (2022). The Role of Enterprise Risk Management in Business Continuity and Resiliency in the Post-COVID-19 Period. *OALib*, 09(06), 1-19. <https://doi.org/10.4236/oalib.1108642>
- Aven, T. (2017). How some types of risk assessments can support resilience analysis and management. *Reliability Engineering & System Safety*, 167, 536-543. <https://doi.org/10.1016/j.ress.2017.07.005>
- Aven, T., & Renn, O. (2010). *Risk Management and Governance*. Springer Berlin Heidelberg. <https://doi.org/10.1007/978-3-642-13926-0>
- Aven, T., & Steen, R. (2010). The concept of ignorance in a risk assessment and risk management context. *Reliability Engineering & System Safety*, 95(11), 1117-1122. <https://doi.org/10.1016/j.ress.2010.05.006>
- Azadeh, A., Salehi, V., & Mirzayi, M. (2016). The Impact of Redundancy and Teamwork on Resilience Engineering Factors by Fuzzy Mathematical Programming and Analysis of Variance in a Large Petrochemical Plant. *Safety and Health at Work*, 7(4), 307-316. <https://doi.org/10.1016/j.shaw.2016.04.009>
- Bachtiar, N. K., Setiawan, A., Prastyana, G. A., & Kijkasiwat, P. (2023). Business resilience and growth strategy transformation post crisis. *Journal of Innovation and Entrepreneurship*, 12(1), 77. <https://doi.org/10.1186/s13731-023-00345-5>
- Baghersad, M., & Zobel, C. W. (2022). Organizational Resilience to Disruption Risks: Developing Metrics and Testing Effectiveness of Operational Strategies. *Risk Analysis*, 42(3), 561-579. <https://doi.org/10.1111/risa.13769>
- Banahene, K. O., Anvuur, A., & Dainty, A. (2014). *Conceptualising Organisational Resilience: An Investigation into Project Organising* (A. B. Raiden & E. Aboagye-Nimo, Ed.; ss. 795-804). Association of Researchers in Construction Management.
- Banks, E. (2012). *Risk Culture*. Palgrave Macmillan UK. <https://doi.org/10.1057/9781137263728>
- Barad, M. (2018). *Strategies and Techniques for Quality and Flexibility*. Springer International Publishing. <https://doi.org/10.1007/978-3-319-68400-0>

- Barton, T. L., Shenkir, W. G., & Walker, P. L. (2002). *Making enterprise risk management pay off*. Financial Times/Prentice Hall PTR.
- Béné, C. (2013). Towards a Quantifiable Measure of Resilience. *IDS Working Papers*, 2013(434), 1-27. <https://doi.org/10.1111/j.2040-0209.2013.00434.x>
- Berkes, F., & Folke, C. (1998). Linking social and ecological systems for resilience and sustainability. İçinde J. Colding (Ed.), *Linking Social And Ecological Systems Management Practices And Social Mechanisms For Building Resilience*. Cambridge University Press.
- Bevan, L. D. (2022). The ambiguities of uncertainty: A review of uncertainty frameworks relevant to the assessment of environmental change. *Futures*, 137, 102919. <https://doi.org/10.1016/j.futures.2022.102919>
- Biggs, R., Schlüter, M., & Schoon, M. L. (Ed.). (2015). *Principles for Building Resilience: Sustaining Ecosystem Services in Social-Ecological Systems* (1. bs). Cambridge University Press. <https://doi.org/10.1017/CBO9781316014240>
- Biringer, B. E. (with Vugrin, E. D., & Warren, D. E.). (2013). *Critical infrastructure system security and resiliency*. Taylor & Francis. <https://doi.org/10.1201/b14566>
- Biyela, N. Y., & Utete, R. (2024). Agenda for future business resilience and survival avenues in crisis times: A systematic literature review of the effects of COVID-19 on SMEs' productivity in South Africa. *Social Sciences & Humanities Open*, 10, 100982. <https://doi.org/10.1016/j.ssaho.2024.100982>
- Blanco-Mesa, F., Rivera-Rubiano, J., Patiño-Hernandez, X., & Martinez-Montaña, M. (2019). The Importance of Enterprise Risk Management in Large Companies in Colombia. *Technological and Economic Development of Economy*, 0(0), 1-34. <https://doi.org/10.3846/tede.2019.9380>
- Bohnert, A., Gatzert, N., Hoyt, R. E., & Lechner, P. (2019). The drivers and value of enterprise risk management: Evidence from ERM ratings. *The European Journal of Finance*, 25(3), 234-255. <https://doi.org/10.1080/1351847X.2018.1514314>
- Bonime-Blanc, A. (2020). *Gloom to boom: How leaders transform risk into resilience and value*. Routledge, Taylor & Francis Group.
- Borghesi, A., & Gaudenzi, B. (2013). *Risk Management: How to Assess, Transfer and Communicate Critical Risks*. Springer Milan. <https://doi.org/10.1007/978-88-470-2531-8>

- Bosetti, L., Ivanovic, A., & Munshey, M. (2016). *Fragility, Risk, and Resilience: A Review of Existing Frameworks*.
- Bouyssou, D., Dubois, D., Prade, H., & Pirlot, M. (2010). *Decision Making Process: Concepts and Methods*. John Wiley & Sons, Inc.
- Bresch, D. N., Berghuijs, J., Egloff, R., & Kupers, R. (2014). A resilience lens for enterprise risk management 3. İçinde R. Kupers (Ed.), *Turbulence A Corporate Perspective on Collaborating for Resilience*. Amsterdam University Press, Project Muse.
- Bronk, R. (2011). *Uncertainty, Modelling Monocultures and the Financial Crisis*. 42(2).
- Brouwer, R., & De Blois, C. (2008). Integrated modelling of risk and uncertainty underlying the cost and effectiveness of water quality measures. *Environmental Modelling & Software*, 23(7), 922-937. <https://doi.org/10.1016/j.envsoft.2007.10.006>
- BSI. (2011). *BS 31100:2011 Risk Management: Code of Practice and Guidance for the Implementation of Bs Iso 31000*. British Standards Institution.
- BSI. (2022). *BS 65000 Organizational Resilience—Code of Practice* (No. 65000). British Standards Institution.
- Burnard, K., & Bhamra, R. (2011). Organisational resilience: Development of a conceptual framework for organisational responses. *International Journal of Production Research*, 49(18), 5581-5599. <https://doi.org/10.1080/00207543.2011.563827>
- Camarinha-Matos, L. M., & Afsarmanesh, H. (2005). Collaborative networks: A new scientific discipline. *Journal of Intelligent Manufacturing*, 16(4-5), 439-452. <https://doi.org/10.1007/s10845-005-1656-3>
- Cambridge. (2025). Resilience. İçinde *Cambridge Online Dictionary*. <https://dictionary.cambridge.org/dictionary/english/resilience>
- Cambridge. (t.y.). Situation. İçinde *Cambridge Online Dictionary*. Geliş tarihi 20 Nisan 2025, gönderen <https://dictionary.cambridge.org/dictionary/english-turkish/situation>
- Caralli, R. A., Allen, J. H., & White, D. W. (2011). *CERT resilience management model: A maturity model for managing operational resilience*. Addison-Wesley.
- Carpenter, S., Arrow, K., Barrett, S., Biggs, R., Brock, W., Crépin, A.-S., Engström, G., Folke, C., Hughes, T., Kautsky, N., Li, C.-Z., McCarney, G., Meng, K., Mäler, K.-G., Polasky, S., Scheffer, M., Shogren, J., Sterner, T., Vincent, J., ... Zeeuw, A. (2012). General

- Resilience to Cope with Extreme Events. *Sustainability*, 4(12), 3248-3259. <https://doi.org/10.3390/su4123248>
- Carrel, P. (2010). *The handbook of risk management: Implementing a post-crisis corporate culture*. Wiley. <https://doi.org/10.1002/9781119208655>
- Cato, C. R., Blue, S. N., & Boyle, B. (2018). Conceptualizing Risk and Unit Resilience in a Military Context. İçinde B. Trump, M.-V. Florin, & I. Linkov (Ed.), *IRGC Resource Guide on Resilience (Volume 2)*. EPFL International Risk Governance Center. <http://infoscience.epfl.ch/record/262527>
- Caza, B. B., Barton, M. A., Christianson, M. K., & Sutcliffe, K. M. (2020). Conceptualizing the who, what, when, where, why and how of resilience in organizations 22. İçinde E. H. Powley, B. Barker Caza, & A. Caza (Ed.), *Research Handbook on Organizational Resilience*. Edward Elgar Publishing. <https://doi.org/10.4337/9781788112215>
- Cedergren, A., & Hassel, H. (2024). Building organizational adaptive capacity in the face of crisis: Lessons from a public sector case study. *International Journal of Disaster Risk Reduction*, 100, 104235. <https://doi.org/10.1016/j.ijdr.2023.104235>
- Chang, S. E., Brown, C., Handmer, J., Helgeson, J., Kajitani, Y., Keating, A., Noy, I., Watson, M., Derakhshan, S., Kim, J., & Roa-Henriquez, A. (2022). Business recovery from disasters: Lessons from natural hazards and the COVID-19 pandemic. *International Journal of Disaster Risk Reduction*, 80, 103191. <https://doi.org/10.1016/j.ijdr.2022.103191>
- Chapelle, A. (2019). *Operational Risk Management Best Practices in the Financial Services Industry*. John Wiley & Sons, Ltd.
- Chapman, R. J. (2012). *Simple Tools and Techniques for Enterprise Risk Management* (1. bs). Wiley. <https://doi.org/10.1002/9781118467206>
- Chen, R., Liu, Y., & Zhou, F. (2021). Turning Danger into Safety: The Origin, Research Context and Theoretical Framework of Organizational Resilience. *IEEE Access*, 9, 48899-48913. <https://doi.org/10.1109/ACCESS.2021.3069301>
- Chen, S. (2016). Construction of an Early Risk Warning Model of Organizational Resilience: An Empirical Study Based on Samples of R&D Teams. *Discrete Dynamics in Nature and Society*, 2016, 1-9. <https://doi.org/10.1155/2016/4602870>

- Cimellaro, G. P., Reinhorn, A. M., & Bruneau, M. (2010). Framework for analytical quantification of disaster resilience. *Engineering Structures*, 32(11), 3639-3649. <https://doi.org/10.1016/j.engstruct.2010.08.008>
- Clement, A., Wioland, L., Govaere, V., Gourc, D., Cegarra, J., Marmier, F., & Kamissoko, D. (2021). Robustness, resilience: Typology of definitions through a multidisciplinary structured analysis of the literature. *European J. of Industrial Engineering*, 15(4), 487. <https://doi.org/10.1504/EJIE.2021.116128>
- Conz, E., & Magnani, G. (2020). A Dynamic Perspective on the Resilience of Firms: A Systematic Literature Review and a Framework for Future Research. *European Management Journal*, 38(3), 400-412. <https://doi.org/10.1016/j.emj.2019.12.004>
- Conz, E., Denicolai, S., & Zucchella, A. (2017). The resilience strategies of SMEs in mature clusters. *Journal of Enterprising Communities: People and Places in the Global Economy*, 11(1), 186-210. <https://doi.org/10.1108/JEC-02-2015-0015>
- Cooper, D. F., Grey, S., Raymond, G., & Walker, P. (2005). *Project Risk Management Guidelines: Managing Risk in Large Projects and Complex Procurements*. John Wiley & Sons, Ltd.
- COSO. (2004). *COSO Enterprise Risk Management—Integrated Framework Executive Summary Framework*. The Committee of Sponsoring Organizations of the Treadway Commission.
- COSO. (2018). *COSO Enterprise Risk Management—Integrating with Strategy and Performance*. Committee of Sponsoring Organizations of the Treadway Commission.
- Crichton, M. T., Ramsay, C. G., & Kelly, T. (2009). Enhancing Organizational Resilience Through Emergency Planning: Learnings from Cross-Sectoral Lessons. *Journal of Contingencies and Crisis Management*, 17(1), 24-37. <https://doi.org/10.1111/j.1468-5973.2009.00556.x>
- Crickette, G., Demian, R., Fox, C., Hach, J., Makomaski, J., Mazumdar, R., McGuire, R., O'Rourke, M., & Arbasetti, K. (2012). *Exploring Risk Appetite and Risk Tolerance*. Risk and Insurance Management Society. [https://web.actuaries.ie/sites/default/files/erm-resources/RIMS Exploring Risk Appetite Risk Tolerance 0412.pdf](https://web.actuaries.ie/sites/default/files/erm-resources/RIMS_Exploring_Risk_Appetite_Risk_Tolerance_0412.pdf)

- Cuadra, L., Salcedo-Sanz, S., Del Ser, J., Jiménez-Fernández, S., & Geem, Z. (2015). A Critical Review of Robustness in Power Grids Using Complex Networks Concepts. *Energies*, 8(9), 9211-9265. <https://doi.org/10.3390/en8099211>
- Cutter, S. L., Barnes, L., Berry, M., Burton, C., Evans, E., Tate, E., & Webb, J. (2008). A place-based model for understanding community resilience to natural disasters. *Global Environmental Change*, 18(4), 598-606. <https://doi.org/10.1016/j.gloenvcha.2008.07.013>
- Çera, G., Khan, K. A., Olah, J., & Metzker, Z. (2023). Business Recovery and Institutional Constraints: Evidence from Visegrad Countries and Serbia. *Journal of Business Economics and Management*, 24(5), 877-900. <https://doi.org/10.3846/jbem.2023.20238>
- Dahmen, P. (2023). Organizational resilience as a key property of enterprise risk management in response to novel and severe crisis events. *Risk Management and Insurance Review*, 26(2), 203-245. <https://doi.org/10.1111/rmir.12245>
- Dalziell, E. P., & McManus, S. T. (2004). Resilience, Vulnerability, and Adaptive Capacity: Implications for System Performance. *International Forum for Engineering Decision Making (IFED)*.
- Davidson, J. L., Jacobson, C., Lyth, A., Dedekorkut-Howes, A., Baldwin, C. L., Ellison, J. C., Holbrook, N. J., Howes, M. J., Serrao-Neumann, S., Singh-Peterson, L., & Smith, T. F. (2016). Interrogating resilience: Toward a typology to improve its operationalization. *Ecology and Society*, 21(2), art27. <https://doi.org/10.5751/ES-08450-210227>
- De Waal, G. A., Kenworthy, A. L., Opatska, S., Trevoho, O., Boychuk, Y., & Kozlova, V. (2025). Exposing Pathways to Organisational Resilience: Revenue Recovery Patterns Among Ukrainian Firms in a War Economy. *Journal of Contingencies and Crisis Management*, 33(2). <https://doi.org/10.1111/1468-5973.70058>
- Dehghani Sadrabadi, M. H., Makui, A., Ghousi, R., & Jabbarzadeh, A. (2024). An integrated optimization model for planning supply chains' resilience and business continuity under interrelated disruptions: A case study. *Kybernetes*, 53(12), 5801-5842. <https://doi.org/10.1108/k-04-2023-0547>
- Deloitte. (2021). *The resilient organization—How to thrive in the face of uncertainty* (s. 14). Deloitte.
- Devinney, T., & Dowling, G. (2020). *The Strategies of Australia's Universities: Revise & Resubmit*. Springer Nature Singapore. <https://doi.org/10.1007/978-981-15-3397-6>

- Dinapoli, T. P. (2016). *Standards for Internal Control in New York State Government*. Office of the New York State Comptroller.
- DKKV. (2023, Şubat). *Resilience at the International Level*. <https://dkkv.org/en/topics/resilience/>
- Douglas, S. (2021). Building organizational resilience through human capital management strategy. *Development and Learning in Organizations: An International Journal*, 35(5), 19-21. <https://doi.org/10.1108/DLO-08-2020-0180>
- Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. *Business Research*, 13(1), 215-246. <https://doi.org/10.1007/s40685-019-0085-7>
- Duong, A. T. B., Pham, T., Truong Quang, H., Hoang, T. G., McDonald, S., Hoang, T.-H., & Pham, H. T. (2024). Ripple effect of disruptions on performance in supply chains: An empirical study. *Engineering, Construction and Architectural Management*, 31(13), 1-22. <https://doi.org/10.1108/ECAM-10-2022-0924>
- Durst, S., Hinteregger, C., & Zieba, M. (2024). The effect of environmental turbulence on cyber security risk management and organizational resilience. *Computers & Security*, 137, 103591. <https://doi.org/10.1016/j.cose.2023.103591>
- Ecsite. (2015). *Risks and Contingency Plan*. Ecsite.
- Eisinger, P. (2002). Organizational Capacity and Organizational Effectiveness among Street-Level Food Assistance Programs. *Nonprofit and Voluntary Sector Quarterly*, 31(1), 115-130. <https://doi.org/10.1177/0899764002311005>
- Engemann, K. J., & Henderson, D. M. (2012). *Business continuity and risk management: Essentials of organizational resilience*. Rothstein Associates Inc., Publisher.
- Enserink, B., Kwakkel, J. H., & Veenman, S. (2013). Coping with uncertainty in climate policy making: (Mis)understanding scenario studies. *Futures*, 53, 1-12. <https://doi.org/10.1016/j.futures.2013.09.006>
- Enwereji, P. C., Van Rooyen, A. A., & Joshi, M. (2024). Entrepreneurial resilience strategies for startups: A view from the VUCA paradigm. *Corporate and Business Strategy Review*, 5(4), 140-151. <https://doi.org/10.22495/cbsrv5i4art13>

- Erkip, F., Kızılgün, Ö., & Akinci, G. M. (2014). Retailers' resilience strategies and their impacts on urban spaces in Turkey. *Cities*, 36, 112-120. <https://doi.org/10.1016/j.cities.2012.12.003>
- Faber, M., & Proops, J. L. R. (1993). *Evolution, Time, Production and the Environment*. Springer Berlin Heidelberg. <https://doi.org/10.1007/978-3-662-03624-2>
- Fadun, O. S. (2013). Promoting 'Enterprise Risk Management' Adoption in Business. *Enterprise Risk Management*, 2(1), 69-78.
- Fewtrell, L., & Bartram, J. (2014). *Water Quality: Guidelines, Standards and Health Assessment of Risk and Risk Management for Water-Related Infectious Disease*. IWA Publishing.
- Florin, M.-V. (2016). Resilience in IRGC's Recommendations for Risk Governance. İçinde M.-V. Florin & I. Linkov (Ed.), *IRGC Resource Guide on Resilience (Volume 1)*. EPFL International Risk Governance Center.
- Florin, M.-V., & Linkov, I. (Ed.). (2016). *IRGC Resource Guide on Resilience (Volume 1)*. EPFL International Risk Governance Center.
- Florio, C., Wieczorek-Kosmala, M., Linsley, P. M., & Shrives, P. (Ed.). (2022). *Risk Management: Insights from Different Settings* (C. 20). Springer International Publishing. <https://doi.org/10.1007/978-3-030-88374-4>
- Folake, A. (2021). Organizational Resilience in the Face of Disruptions. *Journal of Management and Administration Provision*, 1(3), 45-52. <https://doi.org/10.55885/jmap.v1i3.228>
- Folke, C. (2006). Resilience: The emergence of a perspective for social–ecological systems analyses. *Global Environmental Change*, 16(3), 253-267. <https://doi.org/10.1016/j.gloenvcha.2006.04.002>
- Fox, C. R., & Ulkumen, G. (2011). Distinguishing Two Dimensions of Uncertainty. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3695311>
- Förster, C., Füreder, N., & Hertelendy, A. (2023). Why time matters when it comes to resilience: How the duration of crisis affects resilience of healthcare and public health leaders. *Public Health*, 215, 39-41. <https://doi.org/10.1016/j.puhe.2022.11.024>

- Francis, R., & Bekera, B. (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering & System Safety*, 121, 90-103. <https://doi.org/10.1016/j.ress.2013.07.004>
- Fraser, J. R. S., & Simkins, B. J. (2016). The challenges of and solutions for implementing enterprise risk management. *Business Horizons*, 59(6), 689-698. <https://doi.org/10.1016/j.bushor.2016.06.007>
- Fraser, J., & Simkins, B. J. (2010). *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*. Wiley.
- Fraser, J., Quail, R., & Simkins, B. (2024). What's Wrong with Enterprise Risk Management? *Journal of Risk and Financial Management*, 17(7), 274. <https://doi.org/10.3390/jrfm17070274>
- Freud, S., & Burlingham, D. T. (1944). Infants Without Families: The Case For and Against Residential Nurseries. *Journal of the American Medical Association*, 126(6), 400. <https://doi.org/10.1001/jama.1944.02850410070036>
- Friedman, H., & Lewis, B. J. (2021). The Importance of Organizational Resilience in the Digital Age. *Academia Letters*. <https://doi.org/10.20935/AL1643>
- Gafoor. (2012). *Considerations in measurement of awareness*. <https://doi.org/10.13140/2.1.2109.2643>
- Galloway, D., & Funston, R. (2000). The challenges of enterprise risk management. *Balance Sheet*, 8(6), 22-25. <https://doi.org/10.1108/EUM0000000005390>
- Gansch, R., & Adee, A. (2020). System Theoretic View on Uncertainties. *2020 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 1345-1350. <https://doi.org/10.23919/DATE48585.2020.9116472>
- Gay, L. F., & Sinha, S. K. (2013). Resilience of civil infrastructure systems: Literature review for improved asset management. *International Journal of Critical Infrastructures*, 9(4), 330. <https://doi.org/10.1504/ijcis.2013.058172>
- Gibson, C. A., & Tarrant, M. (2010). A 'conceptual models' approach to organisational resilience. *The Australian Journal of Emergency Management*, 25(02). <https://knowledge.aidr.org.au/media/2909/ajem-25-02-03.pdf>

- Goffin, K., Hopkin, P., Szwejcowski, M., & Kauf, E. K. D. (2014). *Roads to Resilience*. Airmic.
- Gotsi, M., & Wilson, A. M. (2001). Corporate reputation: Seeking a definition. *Corporate Communications: An International Journal*, 6(1), 24-30. <https://doi.org/10.1108/13563280110381189>
- Gover, L., & Duxbury, L. (2018). Inside the Onion: Understanding What Enhances and Inhibits Organizational Resilience. *The Journal of Applied Behavioral Science*, 54(4), 477-501. <https://doi.org/10.1177/0021886318797597>
- Granig, P., & Hilgarter, K. (2020). Organisational resilience: A qualitative study about how organisations handle trends and their effects on business models from experts' views. *International Journal of Innovation Science*, 12(5), 525-544. <https://doi.org/10.1108/IJIS-06-2020-0086>
- Graveline, M.-H., & Germain, D. (2022). Disaster Risk Resilience: Conceptual Evolution, Key Issues, and Opportunities. *International Journal of Disaster Risk Science*, 13, 330-341.
- Green, P. E. J. (2016). Introduction to Risk Management Principles. İçinde P. E. J. Green, *Enterprise Risk Management: A Common Framework for the Entire Organization* (ss. 1-13). Butterworth-Heinemann.
- Gregory, C. A. (2003). *Minimizing Enterprise Risk A practical guide to risk and continuity*. Pearson Education Limited.
- Greiman, V. (2013). *Megaproject management: Lessons on risk and project management from the Big Dig*. Wiley Project Management Institute.
- Grote, G. (2004). Uncertainty management at the core of system design. *Annual Reviews in Control*, 28(2), 267-274. <https://doi.org/10.1016/j.arcontrol.2004.03.001>
- Haddow, G. D., Bullock, J. A., & Coppola, D. P. (2021). *Introduction to Emergency Management* (Seventh edition). Butterworth-Heinemann is an imprint of Elsevier.
- Haimes, Y. Y., Crowther, K., & Horowitz, B. M. (2008). Homeland security preparedness: Balancing protection with resilience in emergent systems. *Systems Engineering*, 11(4), 287-308. <https://doi.org/10.1002/sys.20101>

- Hallowell, M. R., Molenaar, K. R., & Fortunato, B. R. (2013). Enterprise Risk Management Strategies for State Departments of Transportation. *Journal of Management in Engineering*, 29(2), 114-121. [https://doi.org/10.1061/\(ASCE\)ME.1943-5479.0000136](https://doi.org/10.1061/(ASCE)ME.1943-5479.0000136)
- Hamel, G. (2007). *The future of management*. Harvard Business School Press.
- Hamel, G., & Välikangas, L. (2021). The Quest for Resilience 2. İçinde *HBR's 10 must reads on organizational resilience*. Harvard Business Review Press.
- Handmer, J. W., & Dovers, S. R. (1996). A Typology of Resilience: Rethinking Institutions for Sustainable Development. *Industrial & Environmental Crisis Quarterly*, 9(4), 482-511. <https://doi.org/10.1177/108602669600900403>
- Handmer, J., & Williams, J. (2001). Managing the Residual Risk. *Australasian Journal of Environmental Management*, 8(4), 239-244. <https://doi.org/10.1080/14486563.2001.10648535>
- Hardy, K. (2015). *Enterprise risk management: A guide for government professionals* (1. ed). Jossey-Bass.
- Häring, I. (2015). *Risk Analysis and Management: Engineering Resilience*. Springer Singapore. <https://doi.org/10.1007/978-981-10-0015-7>
- Harrison, D. A., & Klein, K. J. (2007). What's the difference? Diversity constructs as separation, variety, or disparity in organizations. *Academy of Management Review*, 32(4), 1199-1228. <https://doi.org/10.5465/amr.2007.26586096>
- Harrison, D. A., Price, K. H., Gavin, J. H., & Florey, A. T. (2002). Time, Teams, and Task Performance: Changing Effects of Surface- and Deep-Level Diversity on Group Functioning. *Academy of Management Journal*, 45(5), 1029-1045.
- Hatton, T., Brown, C., Kipp, R., Seville, E., Brouggy, P., & Loveday, M. (2018). Developing a model and instrument to measure the resilience of critical infrastructure sector organisations. *International Journal of Critical Infrastructures*, 14(1). <https://doi.org/10.1504/IJCIS.2018.090653>
- Helaakoski, H., Iskanius, P., & Peltomaa, I. (2007). Agent-Based Architecture for Virtual Enterprises to Support Agility. İçinde L. M. Camarinha-Matos, H. Afsarmanesh, P. Novais, & C. Analide (Ed.), *Establishing the Foundation of Collaborative Networks* (ss. 299-306). Springer US. https://doi.org/10.1007/978-0-387-73798-0_31

- Herbane, B. (2013). Exploring Crisis Management in UK Small- and Medium-Sized Enterprises. *Journal of Contingencies and Crisis Management*, 21(2), 82-95. <https://doi.org/10.1111/1468-5973.12006>
- Hillmann, J., & Guenther, E. (2021). Organizational Resilience: A Valuable Construct for Management Research? *International Journal of Management Reviews*, 23(1), 7-44. <https://doi.org/10.1111/ijmr.12239>
- Hillson, D. (2003). *Effective Opportunity Management for Projects: Exploiting Positive Risk*. CRC Press LLC.
- Hillson, D. (2019). *Capturing Upside Risk: Finding and Managing Opportunities in Projects* (1. bs). Auerbach Publications. <https://doi.org/10.1201/9780367360450>
- Hillson, D. (with Dalcher, P. D.). (2009). *Managing Risk in Projects* (1st ed). Routledge.
- Hohenstein, N.-O., Feisel, E., Hartmann, E., & Giunipero, L. (2015). Research on the phenomenon of supply chain resilience: A systematic review and paths for further investigation. *International Journal of Physical Distribution & Logistics Management*, 45(1/2), 90-117. <https://doi.org/10.1108/IJPDLM-05-2013-0128>
- Hollands, L., Haensse, L., & Lin-Hi, N. (2024). The How and Why of Organizational Resilience: A Mixed-Methods Study on Facilitators and Consequences of Organizational Resilience Throughout a Crisis. *The Journal of Applied Behavioral Science*, 60(3), 449-493. <https://doi.org/10.1177/00218863231165785>
- Holling, C. S. (1973). Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics*, 4(1), 1-23.
- Holling, C. S. (1996). Engineering Resilience versus Ecological Resilience. İçinde P. C. Schulze (Ed.), *Engineering Within Ecological Constraints* (ss. 31-43). National Academy Press.
- Home, J. F., & Orr, J. E. (1997). Assessing behaviors that create resilient organizations. *Employment Relations Today*, 24(4), 29-39. <https://doi.org/10.1002/ert.3910240405>
- Hopkin, P. (2015). Achieving enhanced organisational resilience by improved management of risk: Summary of research into the principles of resilience and the practices of resilient organisations. *Journal of Business Continuity & Emergency Planning*, 8(3), 252. <https://doi.org/10.69554/NMXP6813>

- Hopkin, P., & Thompson, C. (2022). *Fundamentals of risk management: Understanding, evaluating and implementing effective enterprise risk management* (Sixth Edition). Kogan Page.
- Hosseini, S., & Barker, K. (2016). Modeling infrastructure resilience using Bayesian networks: A case study of inland waterway ports. *Computers & Industrial Engineering*, 93, 252-266. <https://doi.org/10.1016/j.cie.2016.01.007>
- Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience. *Reliability Engineering & System Safety*, 145, 47-61. <https://doi.org/10.1016/j.ress.2015.08.006>
- Howell, W. (2016). *Economics, Law, Social Sciences and International Affairs to obtain the title of Doctor of Philosophy in Law*. <https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5a4b5674e&appId=PPGMS>
- Huber, G. P. (1991). Organizational Learning: The Contributing Processes and the Literatures. *Organization Science*, 2(1), 88-115. <https://doi.org/10.1287/orsc.2.1.88>
- Hunziker, S. (2019). *Enterprise Risk Management: Modern Approaches to Balancing Risk and Reward*. Springer Fachmedien Wiesbaden. <https://doi.org/10.1007/978-3-658-25357-8>
- Ibrahim, F. S., & Esa, M. (2017). A Study on Enterprise Risk Management and Organizational Performance: Developer's Perspective. *International Journal of Civil Engineering and Technology*, 8(10), 184-196.
- IIA. (2004). *The Role of Internal Auditing in Enterprise-wide*. Institute of Internal Auditors. <https://www.iiajapan.com/pdf/data/erm/ERM.pdf>
- IMA. (2011). *Enterprise Risk Management: Frameworks, Elements, and Integration*. Institute of Management Accountants. https://www.stjohns.edu/sites/default/files/uploads/enterprise_risk_management_frameworks.pdf
- IPCC. (1990). *Climate Change The IPCC Scientific Assessment. The First Assessment Report of the Intergovernmental Panel on Climate Change 1990* (s. 414). Intergovernmental Panel on Climate Change. https://archive.ipcc.ch/ipccreports/far/wg_I/ipcc_far_wg_I_full_report.pdf

- IPCC. (2012). *Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation: Special Report of the Intergovernmental Panel on Climate Change* (C. B. Field, V. Barros, T. F. Stocker, & Q. Dahe, Ed.; 1. bs). Cambridge University Press. <https://www.cambridge.org/core/product/identifier/9781139177245/type/book>
- IPCC. (2014). Annex II - Glossary. İçinde V. R. Barros, C. B. Fiel, D. J. Dokken, & M. D. Mastrandrea (Ed.), *Climate change 2014: Impacts, adaptation, and vulnerability. Part B: Regional aspects. Contribution of Working Group II to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change*. (ss. 1757-1776). Cambridge University Press.
- IRM. (2012). *Risk Culture. Resources for Practitioners*. Institute of Risk Management (IRM). <https://www.theirm.org/media/7230/risk-culture-resources-for-practitioners.pdf>
- ISO. (2009). *ISO 31000:2009 Risk management—Principles and guidelines* (Versiyon ISO 31000-2009) [Standard]. International Standards Organization.
- ISO. (2017). *ISO 22316 Security and Resilience Organizational Resilience Principles and Attributes* (No. 22316). International Organization for Standardization.
- ISO. (2018). *ISO 31000:2018 Risk management—Guidelines* [Standard]. International Standards Organization.
- ISO. (2019). *BS EN ISO 22301 Security and resilience Business continuity management systems. Requirements* (No. 22301). British Standards Institution. <https://doi.org/10.3403/30382483>
- Jackson, S. (2016). Principles for Resilient Design—A Guide for Understanding and Implementation. İçinde M.-V. Florin & I. Linkov (Ed.), *IRGC Resource Guide on Resilience (Volume 1)* (C. 1). EPFL International Risk Governance Center.
- Jackson, S. E., Joshi, A., & Erhardt, N. L. (2003). Recent Research on Team and Organizational Diversity: SWOT Analysis and Implications. *Journal of Management*, 29(6), 801-830. [https://doi.org/10.1016/S0149-2063\(03\)00080-1](https://doi.org/10.1016/S0149-2063(03)00080-1)
- Jackson, S., & Ferris, T. L. J. (2013). Resilience principles for engineered systems. *Systems Engineering*, 16(2), 152-164. <https://doi.org/10.1002/sys.21228>
- Jeans, H., Thomas, S., & Castillo, G. (2016). *The Future is a Choice: The Oxfam Framework and Guidance for Resilient Development*. Oxfam.

- Jiang, Y., Prayag, G., Chowdhury, M., Hossain, M. I., & Akter, N. (2025). A community capitals perspective of multi-level retrospective and prospective resilience in hospitality firms. *International Journal of Hospitality Management*, 129, 104193. <https://doi.org/10.1016/j.ijhm.2025.104193>
- Jnitova, V., Efatmaneshnik, M., Joiner, K., & Chang, E. (2021). Enhancing Enterprise Architecture with Resilience Perspective. *INCOSE International Symposium*, 31(1), 1176-1192. <https://doi.org/10.1002/j.2334-5837.2021.00894.x>
- Johnsen, S. (2010). Resilience in Risk Analysis and Risk Assessment. İçinde T. Moore & S. Shenoï (Ed.), *Critical Infrastructure Protection IV* (C. 342, ss. 215-227). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-16806-2_15
- Jovanović, A., Klimek, P., Renn, O., Schneider, R., Øien, K., Brown, J., DiGennaro, M., Liu, Y., Pfau, V., Jelić, M., Rosen, T., Caillard, B., Chakravarty, S., & Chhantyal, P. (2020). Assessing resilience of healthcare infrastructure exposed to COVID-19: Emerging risks, resilience indicators, interdependencies and international standards. *Environment Systems and Decisions*, 40(2), 252-286. <https://doi.org/10.1007/s10669-020-09779-8>
- Jum'a, L., Qamardin, S., & Ikram, M. (2024). Developing resilience strategies amid supply chain risks in the automotive industry: A stakeholder theory perspective. *Business Strategy and the Environment*, 33(8), 9197-9213. <https://doi.org/10.1002/bse.3977>
- Jung, K., & Song, M. (2015). Linking emergency management networks to disaster resilience: Bonding and bridging strategy in hierarchical or horizontal collaboration networks. *Quality & Quantity*, 49(4), 1465-1483. <https://doi.org/10.1007/s11135-014-0092-x>
- Jüttner, U., & Maklan, S. (2011). Supply chain resilience in the global financial crisis: An empirical study. *Supply Chain Management: An International Journal*, 16(4), 246-259. <https://doi.org/10.1108/13598541111139062>
- Kahan, J. H., Allen, A. C., & George, J. K. (2009). An Operational Framework for Resilience. *Journal of Homeland Security and Emergency Management*, 6(1). <https://doi.org/10.2202/1547-7355.1675>
- Kantabutra, S., & Ketprapakorn, N. (2021). Toward an Organizational Theory of Resilience: An Interim Struggle. *Sustainability*, 13(23), 13137. <https://doi.org/10.3390/su132313137>
- Karaçolak, M. B. (2024). Beyond Fight or Flight: Alternative Risk Response Strategies. İçinde H. Kırak (Ed.), *Rethinking Enterprise Risk Management* (ss. 101-129). Springer Singapore.

- Karunaratne, D. R. (2022). Organizational Resilience: A Paradox-Based Conceptualization. *Vidyodaya Journal of Management*, 8(1). <https://doi.org/10.31357/vjm.v8i1.5606>
- Keeble, B. R. (1988). The Brundtland report: 'Our common future'. *Medicine and War*, 4(1), 17-25. <https://doi.org/10.1080/07488008808408783>
- Kemp, M. (2022). *Good Practice Guide: Business Resilience* (1. bs). RIBA Publishing. <https://doi.org/10.4324/9781003297253>
- Kerstin, D., Simone, O., Nicole, Z., & Lehner, O. M. (2014). *Challenges in Implementing Enterprise Risk Management*. 3(3).
- Keshavarz, M., Hosseini-Nasab, H., Fakhrzad, M. B., & Zare, H. K. (2024). Impact of resource reconfiguration on the dairy supply chain resilience. *RAIRO - Operations Research*, 58(6), 5341-5368. <https://doi.org/10.1051/ro/2024186>
- Ketcham, C., & Louisot, J.-P. (Ed.). (2014). *ERM, enterprise risk management: Issues and cases*. Wiley. <https://doi.org/10.1002/9781118892015>
- Khan, M. J., Hussain, D., & Mehmood, W. (2016). Why do firms adopt enterprise risk management (ERM)? Empirical evidence from France. *Management Decision*, 54(8), 1886-1907. <https://doi.org/10.1108/MD-09-2015-0400>
- Khan, T. Z. A., Farooq, W., & Rasheed, H. (2019). Organizational Resilience: A Dynamic Capability of Complex Systems. *Journal of Management and Research*, 6(1).
- Khin Khin Oo, N. C., & Rakthin, S. (2022). Integrative Review of Absorptive Capacity's Role in Fostering Organizational Resilience and Research Agenda. *Sustainability*, 14(19), 12570. <https://doi.org/10.3390/su141912570>
- Khuan, H. (2024). Building Organizational Resilience in the Era of Uncertainty: Strategies and Best Practices. *Management Studies and Business Journal (PRODUCTIVITY)*, 1(2), 238-249. <https://doi.org/10.62207/xdej2b78>
- Kiureghian, A. D., & Ditlevsen, O. (2009). Aleatory or epistemic? Does it matter? *Structural Safety*, 31(2), 105-112. <https://doi.org/10.1016/j.strusafe.2008.06.020>
- Knight, F. H. (1921). *Risk, Uncertainty, and Profit*.
- Kokkranikal, J., Prayag, G., Meera, S., Vinodan, A., & Shyju, P. J. (2024). Organisational resilience and recovery of tour operators: Towards a challenge-metamorphosis model. *Tourism Recreation Research*, 1-17. <https://doi.org/10.1080/02508281.2024.2413833>

- Koronis, E., & Ponis, S. (2018). Better than before: The resilient organization in crisis mode. *Journal of Business Strategy*, 39(1), 32-42. <https://doi.org/10.1108/JBS-10-2016-0124>
- Kozine, I., & Andersen, H. B. (2015). Integration of Resilience Capabilities for Critical Infrastructures into the Emergency Management Set-Up. İçinde L. Podofillini, B. Sudret, B. Stojadinovic, E. Zio, & W. Kröger (Ed.), *Safety and Reliability of Complex Engineered Systems: ESREL 2015*. CRC Press. <https://doi.org/10.1201/b19094>
- Lai, C., & Hsu, Y. (2018). Understanding activated network resilience: A comparative analysis of co-located and co-cluster disaster response networks. *Journal of Contingencies and Crisis Management*, 27(1), 14-27. <https://doi.org/10.1111/1468-5973.12224>
- Lake, P. S. (2013). Resistance, Resilience and Restoration. *Ecological Management & Restoration*, 14(1), 20-24. <https://doi.org/10.1111/emr.12016>
- Lam, J. (2014). *Enterprise risk management: From incentives to controls* (2nd ed). J. Wiley & Sons.
- Lam, J. (2017). *Implementing enterprise risk management: From methods to applications*. John Wiley & Sons.
- Lang, S., Fewtrell, L., & Bartram, J. (2001). Risk communication. İçinde *Water Quality: Guidelines, standards and health*. IWA.
- Lark, J. (with Nikonov, V.). (2015). *ISO31000: Risk management : a practical guide for SMEs*. International Organization for Standardization : International Trade Centre : UNIDO.
- Lee, A. V., Vargo, J., & Seville, E. (2013). Developing a Tool to Measure and Compare Organizations' Resilience. *Natural Hazards Review*, 14(1), 29-41. [https://doi.org/10.1061/\(ASCE\)NH.1527-6996.0000075](https://doi.org/10.1061/(ASCE)NH.1527-6996.0000075)
- Leflar, J. J., & Siegel, M. H. (2013). *Organizational Resilience: Managing the Risks of Disruptive Events—A Practitioner's Guide*.
- Lengnick-Hall, C. A., & Beck, T. E. (2005). Adaptive Fit Versus Robust Transformation: How Organizations Respond to Environmental Change. *Journal of Management*, 31(5), 738-757. <https://doi.org/10.1177/0149206305279367>
- Lengnick-Hall, C. A., & Beck, T. E. (2009). Resilience Capacity and Strategic Agility: Prerequisites for Thriving in a Dynamic Environment. İçinde C. P. Nemeth, E. Hollnagel,

- & S. Decker (Ed.), *Resilience Engineering Perspectives, Volume 2 Preparation and Restoration* (C. 2). CRC Press.
- Lengnick-Hall, C. A., Beck, T. E., & Lengnick-Hall, M. L. (2011). Developing a capacity for organizational resilience through strategic human resource management. *Human Resource Management Review*, 21(3), 243-255. <https://doi.org/10.1016/j.hrmr.2010.07.001>
- Liddle, D. (2022). Achieving Resilience through Structural and Systems Change. İçinde PMI (Ed.), *Building Resilient Organizations Best Practices, Tools, and Insights to Thrive in Ever-Changing Contexts*. Project Management Institute.
- Lindhout, P., Kingston-Howlett, J., Hansen, F. T., & Reniers, G. (2020). Reducing unknown risk: The safety engineers' new horizon. *Journal of Loss Prevention in the Process Industries*, 68, 104330. <https://doi.org/10.1016/j.jlp.2020.104330>
- Linkov, I., Trump, B. D., & Fox-Lent, C. (2016). Resilience: Approaches to Risk Analysis and Governance. İçinde M.-V. Florin & I. Linkov (Ed.), *IRGC Resource Guide on Resilience (Volume 1)*. EPFL International Risk Governance Center.
- Linnenluecke, M., & Griffiths, A. (2010). Beyond Adaptation: Resilience for Business in Light of Climate Change and Weather Extremes. *Business & Society*, 49(3), 477-511. <https://doi.org/10.1177/0007650310368814>
- Logan, T. M., Aven, T., Guikema, S. D., & Flage, R. (2022). Risk science offers an integrated approach to resilience. *Nature Sustainability*, 5(9), 741-748. <https://doi.org/10.1038/s41893-022-00893-w>
- Longman. (2025). Resilience. İçinde *Cambridge Online Dictionary*. <https://www.ldoceonline.com/dictionary/resilience>
- Longstaff, P. H., Koslowski, T. G., & Geoghegan, W. (2014). Translating Resilience: A Framework to Enhance Communication and Implementation. *Proceedings 5th Symposium on Resilience Engineering: Managing Trade-Offs*, 1-10.
- Louisot, J.-P. (2015). Risk and/or resilience management. *Risk Governance and Control: Financial Markets and Institutions*, 5(2), 84-91. <https://doi.org/10.22495/rgcv5i2c1art2>
- Lovell, E., Bahadur, A., Tanner, T., & Morsi, H. (2016). *Resilience The Big Picture Top themes and trends*. ODI.

- Lu, S., & Chan, W. K. (2024). Understanding Organizational Resilience of Care Homes for Older People During COVID-19 in China: A Qualitative Study with Post-Pandemic Policy Implications. *Journal of Aging & Social Policy*, 36(6), 1432-1451. <https://doi.org/10.1080/08959420.2024.2403828>
- Lucarelli, C. (Ed.). (2011). *Risk tolerance in financial decision making*. Palgrave Macmillan.
- MacLeman, H., Miller, A. M., & Marty, L. (2016). *Resilience Systems Analysis Learning & Recommendations Report*.
- Macmillan. (2004). Resilience. İçinde *Macmillan English Dictionary*. Macmillan Education.
- Mahaboob, H., Ramamurthy, P., & Huligeshwari Devi. (2022). Achieving Resilience Through Structural and Systems Change. İçinde PMI (Ed.), *Building Resilient Organizations Best Practices, Tools, and Insights to Thrive in Ever-Changing Contexts* (ss. 124-134). Project Management Institute.
- Mallak, L. A. (1999). Toward a theory of organizational resilience. *PICMET '99: Portland International Conference on Management of Engineering and Technology. Proceedings Vol-1: Book of Summaries (IEEE Cat. No.99CH36310)*, 223. <https://doi.org/10.1109/PICMET.1999.808142>
- Manyena, B., Machingura, F., & O'Keefe, P. (2019). Disaster Resilience Integrated Framework for Transformation (DRIFT): A new approach to theorising and operationalising resilience. *World Development*, 123, 104587. <https://doi.org/10.1016/j.worlddev.2019.06.011>
- Marchetti, A. M. (2012). *Enterprise risk management best practices: From assessment to ongoing compliance*. Wiley.
- Masood, O., Javaria, K., & Majeed, E. (2020). Enterprise Risk Management Program Effectiveness, Determinants, Execution and effect on Financial Performance: Evidence from Global Takaful Industry. *Journal of Islamic Financial Studies*, 6(2), 77-87. <https://doi.org/10.12785/jifs/060202>
- McManus, S., Seville, E., Vargo, J., & Brunsdon, D. (2008). Facilitated Process for Improving Organizational Resilience. *Natural Hazards Review*, 9(2), 81-90. [https://doi.org/10.1061/\(ASCE\)1527-6988\(2008\)9:2\(81\)](https://doi.org/10.1061/(ASCE)1527-6988(2008)9:2(81))
- Meerow, S., Newell, J. P., & Stults, M. (2016). Defining urban resilience: A review. *Landscape and Urban Planning*, 147, 38-49. <https://doi.org/10.1016/j.landurbplan.2015.11.011>

- Melián-Alzola, L., Fernández-Monroy, M., & Hidalgo-Peñate, M. (2020). Hotels in contexts of uncertainty: Measuring organisational resilience. *Tourism Management Perspectives*, 36, 100747. <https://doi.org/10.1016/j.tmp.2020.100747>
- Mentges, A., Halekotte, L., Schneider, M., Demmer, T., & Lichte, D. (2023). A resilience glossary shaped by context: Reviewing resilience-related terms for critical infrastructures. *International Journal of Disaster Risk Reduction*, 96, 103893. <https://doi.org/10.1016/j.ijdr.2023.103893>
- Meredith, C., Moolenaar, N. M., Struyve, C., Vandecandelaere, M., Gielen, S., & Kyndt, E. (2017). The measurement of collaborative culture in secondary schools: An informal subgroup approach. *Front Learning Research*, 5(2), 24-35. <https://doi.org/10.14786/flr.v5i2.283>
- Mızrak, F. (2024). Resilience and Innovation Strategies: How Businesses Adapt to Supply Chain Disruptions in the Post-Pandemic Era. *Politik Ekonomik Kuram*, 8(3), 581-600. <https://doi.org/10.30586/pek.1497718>
- Michaela, O.-O. E. (2023). Managerial Capacity Skills and Corporate Resilience of Private Security Firms in South-South Nigeria. *International Journal of Research Publication and Reviews*, 4(6), 3225-3233.
- Mochizuki, J., Keating, A., Liu, W., Hochrainer-Stigler, S., & Mechler, R. (2018). An overdue alignment of risk and resilience? A conceptual contribution to community resilience. *Disasters*, 42(2), 361-391. <https://doi.org/10.1111/disa.12239>
- Moeller, R. R. (2007). *COSO Enterprise Risk Management: Understanding the New Integrated ERM Framework*. John Wiley & Sons, Inc. <https://doi.org/10.1002/9781118269145>
- Mokline, B., & Ben Abdallah, M. A. (2021). Organizational resilience as response to a crisis: Case of COVID-19 crisis. *Continuity & Resilience Review*, 3(3), 232-247. <https://doi.org/10.1108/CRR-03-2021-0008>
- Molak, V. (Ed.). (1997). *Fundamentals of risk analysis and risk management*. Lewis Publishers.
- Monazzam, A., & Crawford, J. (2024). The role of enterprise risk management in enabling organisational resilience: A case study of the Swedish mining industry. *Journal of Management Control*, 35(1), 59-108. <https://doi.org/10.1007/s00187-024-00370-9>

- Mondragón, I. J. G., Rendón Trejo, A., & Morales Alquicira, A. (2022). Is Organizational Resilience a Competitive Advantage? *Mercados y Negocios*, 46, 57-82. <https://doi.org/10.32870/myn.vi46.7670.g6738>
- Moshesh, R., Niemann, W., & Kotzé, T. (2018). Enterprise Risk Management Implementation Challenges: A Case Study in a Petrochemical Supply Chain. *South African Journal of Industrial Engineering*, 29(4), 230-244.
- Mousavi, S., & Gigerenzer, G. (2014). Risk, uncertainty, and heuristics. *Journal of Business Research*, 67(8), 1671-1678. <https://doi.org/10.1016/j.jbusres.2014.02.013>
- Murray-Webster, R., & Williams, G. (2010). *Management of risk: Guidance for practitioners*. The Stationery Office.
- Namdar, J., Torabi, S. A., Sahebjamnia, N., & Nilkanth Pradhan, N. (2021). Business continuity-inspired resilient supply chain network design. *International Journal of Production Research*, 59(5), 1331-1367. <https://doi.org/10.1080/00207543.2020.1798033>
- Nan, C., Sansavini, G., Kröger, W., & Heinimann, H. R. (2014). *A Quantitative Method for Assessing the Resilience of Infrastructure Systems*.
- Nasab, Y. H., Amiri, M., Keyghobadi, A., & Hafshejani, K. F. (2023). *Identifying Effective Factors of Organizational Resilience: A Meta-Synthesis Study*.
- Nipa, T. J., Kermanshachi, S., & Pamidimukkala, A. (2023). Identification of Resilience Dimensions in Critical Transportation Infrastructure Networks. *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction*, 15(2), 03122001. <https://doi.org/10.1061/JLADAH.LADR-870>
- Nocco, B. W., & Stulz, R. M. (2006). Enterprise Risk Management: Theory and Practice. *Journal of Applied Corporate Finance*, 18(4), 8-20. <https://doi.org/10.1111/j.1745-6622.2006.00106.x>
- Nosike, C. J., Ojobor, O. S. N., & Nosike, C. U. (2024). Enhancing business resilience: Innovation and adaptation during and after the global pandemic. *International Journal of Financial, Accounting, and Management*, 6(2), 217-229. <https://doi.org/10.35912/ijfam.v6i2.1891>
- O'Brien, P. W., & Mileti, D. S. (1980). Citizen participation in emergency response following the 1971 San Fernando earthquake. *Disasters*, 4(3), 431-445.

- OECD. (2014). *Guidelines for Resilience Systems Analysis: How to Analyse Risk and Build a Roadmap to Resilience* [Best Practices in Development Co-operation]. OECD. https://www.oecd-ilibrary.org/development/guidelines-for-resilience-systems-analysis-how-to-analyse-risk-and-build-a-roadmap-to-resilience_3b1d3efe-en
- Oehmen, J., Locatelli, G., Wied, M., & Willumsen, P. (2020). Risk, uncertainty, ignorance and myopia: Their managerial implications for B2B firms. *Industrial Marketing Management*, 88, 330-338. <https://doi.org/10.1016/j.indmarman.2020.05.018>
- Okolita, K. (with Safari, an O'Reilly Media Company). (2016). *Building an Enterprise-Wide Business Continuity Program* (1st edition). Auerbach Publications.
- Olson, D. L., & Wu, D. (2020). *Enterprise Risk Management Models*. Springer Berlin Heidelberg. <https://doi.org/10.1007/978-3-662-60608-7>
- Orderud, G. I., & Naustdalslid, J. (2018). The understanding and role of uncertainty and risk in climate change adaptation: Local and central authorities in Norway. *International Journal of Sustainable Development & World Ecology*, 25(7), 579-591. <https://doi.org/10.1080/13504509.2018.1443524>
- Ortiz-de-Mandojana, N., & Bansal, P. (2016). The long-term benefits of organizational resilience through sustainable business practices. *Strategic Management Journal*, 37(8), 1615-1631. <https://doi.org/10.1002/smj.2410>
- Otun, T. O., Muritala, T. A., Ibrahim, U. A., & Gambo, N. (2023). *Impact of Enterprise Risk Management on Organizational Resilience: A Qualitative Approach*. 13(4).
- Oxford. (2025). Resilience. İçinde *Oxford Learner's Dictionary Online*. <https://www.oxfordlearnersdictionaries.com/definition/english/resilience?q=resilience>
- Pacelli, V. (Ed.). (2025). *Systemic Risk and Complex Networks in Modern Financial Systems*. Springer Nature Switzerland. <https://doi.org/10.1007/978-3-031-64916-5>
- Palin, P. J. (2016). Supply Chain Resilience Diversity + SelfOrganisation = Adaptation 8. İçinde R. Bhamra (Ed.), *Organisational Resilience: Concepts, Integration, and Practice* (0 bs). CRC Press. <https://doi.org/10.1201/b19305>
- Park, J.-H., & Seo, R. (2024). A contingent value of bricolage strategy on SMEs' organizational resilience: Lessons from the COVID-19 pandemic. *Humanities and Social Sciences Communications*, 11(1), 263. <https://doi.org/10.1057/s41599-024-02771-6>

- Passenheim, D. O. (2013). *Enterprise Risk Management*.
- PECB. (2025). *The Importance of Organizational Resilience*. <https://pecb.com/article/the-importance-of-organizational-resilience>
- Pertheban, T. R., Thurasamy, R., Marimuthu, A., Venkatachââm, K. R., Annamalah, S., Paraman, P., & Hoo, W. C. (2023). The Impact of Proactive Resilience Strategies on Organizational Performance: Role of Ambidextrous and Dynamic Capabilities of SMEs in Manufacturing Sector. *Sustainability*, 15(16), 12665. <https://doi.org/10.3390/su151612665>
- Pescaroli, G., & Alexander, D. (2018). Understanding Compound, Interconnected, Interacting, and Cascading Risks: A Holistic Framework. *Risk Analysis*, 38(11), 2245-2257. <https://doi.org/10.1111/risa.13128>
- Pescaroli, G., Guida, K., Reynolds, J., Pulwarty, R. S., Linkov, I., & Alexander, D. E. (2023). Managing systemic risk in emergency management, organizational resilience and climate change adaptation. *Disaster Prevention and Management: An International Journal*, 32(1), 234-251. <https://doi.org/10.1108/dpm-08-2022-0179>
- Pessina, I. (2021). Risk and Resilience Management as a Response to COVID-19 Pandemic Outbreak. Towards a New and Refreshing Approach. *Economia Aziendale Online* -, Vol 12, 27-37 Pages. <https://doi.org/10.13132/2038-5498/12.1.27-37>
- Pimm, S. L. (1984). The complexity and stability of ecosystems. *Nature*, 307(5949), 321-326. <https://doi.org/10.1038/307321a0>
- Pinkwart, A., Schingen, G., Pannes, A.-T., & Schlotb  ller, D. (2022). Improving Resilience in Times of Multiple Crisis: Commentary from a German Economic Policy Point of View. *Schmalenbach Journal of Business Research*, 74(4), 763-786. <https://doi.org/10.1007/s41471-022-00150-y>
- Pla  ek, M., Daniel, G., Valentinov, V., Ochrana, F., & Kov  cs, R. (2025). Resilience strategies of public organizations and social enterprises: Evidence from Slovakia and the Czech Republic. *International Journal of Public Sector Management*, ahead-of-print(ahead-of-print). <https://doi.org/10.1108/IJPSM-06-2024-0200>
- PMI (Ed.). (2018). *A Guide to the Project Management Body of Knowledge (PMBOK Guide) 6th* (6. bs). Project Management Institute, Inc.

- Pont, A., & Simon, A. (2024). Nurturing family business resilience through strategic supply chain management. *Journal of Family Business Management*, 15(1), 68-101. <https://doi.org/10.1108/JFBM-11-2023-0272>
- Posch, E., Eckert, E., & Thiebes, B. (2024). Towards a future conceptualization of destination resilience: Exploring the role of actors, agency and resilience narratives. *Journal of Tourism Futures*. <https://doi.org/10.1108/JTF-10-2022-0270>
- Prahâlâd, C. K., & Hamel, G. (2006). The Core Competence of the Corporation. İçinde D. Hahn & B. Taylor, *Strategische Unternehmensplanung—Strategische Unternehmensführung: Stand und Entwicklungstendenzen*. Springer-Verlag Berlin Heidelberg. <https://doi.org/10.1007/3-540-30763-X>
- Proag, V. (2014). The Concept of Vulnerability and Resilience. *Procedia Economics and Finance*, 18, 369-376. [https://doi.org/10.1016/S2212-5671\(14\)00952-6](https://doi.org/10.1016/S2212-5671(14)00952-6)
- Protiviti. (2006). *Protiviti Guide to Enterprise Risk Management Frequently Asked Questions Guide Book* (s. 153).
- PWC. (2021). *Operational Risk and Operational Resilience*.
- Quendler, E. (2017). Organisational resilience: Building business value in a changing world. *J. for International Business and Entrepreneurship Development*, 10(2), 101. <https://doi.org/10.1504/JIBED.2017.084301>
- Rabbani, M., Farrokhi-Asl, H., Karimi, M., & Ghavamifar, A. (2020). Reliable Supply Chain Network Design Considering Resilience Strategies Under Risk of Disruption. *Journal of Quality Engineering and Production Optimization*, 5(2).
- Ramezani, J., & Camarinha-Matos, L. M. (2020). Approaches for resilience and antifragility in collaborative business ecosystems. *Technological Forecasting and Social Change*, 151, 119846. <https://doi.org/10.1016/j.techfore.2019.119846>
- Rankine, W. J. M. (1862). *A Manual of Applied Mechanics* (17. bs).
- Rausand, M. (2011). *Risk assessment: Theory, methods, and applications* (Online-Ausg). Wiley.
- Renault, B. Y., Agumba, J. N., & Balogun, O. A. (2016). Drivers for and Obstacles to Enterprise Risk Management in Construction Firms: A Literature Review. *Procedia Engineering*, 164, 402-408. <https://doi.org/10.1016/j.proeng.2016.11.637>

- Richardson, G. (2023). Business Resilience Strategies for Navigating Economic Uncertainty in 2023. *Journal of Business & Financial Affairs*, 12(4).
- Richman, L. L. (2012). *Improving your project management skills* (2nd ed). American Management Association.
- Roberts, A. (2023). Risk, Reward, and Resilience Framework: Integrative Policy Making in a Complex World. *Journal of International Economic Law*, 26(2), 233-265. <https://doi.org/10.1093/jiel/jgad009>
- Roberts, D., Choudhury, I., Kovala, S., Roberts, S., & Tanvir, J. (2022). *Business resilience: A practical guide to sustained progress delivered at pace*. KoganPage.
- Rose, A. (2004). Defining and measuring economic resilience to disasters. *Disaster Prevention and Management: An International Journal*, 13(4), 307-314. <https://doi.org/10.1108/09653560410556528>
- Roy, D., & Zeckhauser, R. (2015). The anatomy of ignorance. İçinde M. Gross & L. McGoey (Ed.), *Routledge International Handbook of Ignorance Studies* (1. bs, ss. 61-73). Routledge. https://www.taylorfrancis.com/books/9781317964674/chapters/10.4324/9781315867762_-8
- Rubim, I. C., & Borges, M. R. S. (2017). *The Resilience and Its Dimensions*.
- Sadeqi-Arani, Z., & Ghahfarokhi, E. A. (2022). Sports Business Resilience in the COVID-19 Crisis: The Delphi Qualitative Approach. *Iranian Journal of Management Studies (IJMS)*, 15(1).
- Sadiq, S., & Governatori, G. (2010). Managing Regulatory Compliance in Business Processes. İçinde J. Vom Brocke & M. Rosemann (Ed.), *Handbook on Business Process Management* 2 (ss. 159-175). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-01982-1_8
- Salim, A., Pepperil, A., Mitchell, C., & Candy, C. (2021). *An Introduction to Emerging Risks and How to Identify Them*. Institute of Risk Management. <https://www.theirm.org/media/9230/charities-sig-an-introduction-to-emerging-risks-and-how-to-identify-them.pdf>
- Sanchis, R., Canetta, L., & Poler, R. (2020). A Conceptual Reference Framework for Enterprise Resilience Enhancement. *Sustainability*, 12(4), 1464. <https://doi.org/10.3390/su12041464>

- Scholtz, S. (2000). Threat: Concept Analysis. *Nursing Forum*, 35(4), 23-29. <https://doi.org/10.1111/j.1744-6198.2000.tb01227.x>
- Sharma, P., Leung, T. Y., Kingshott, R. P. J., Davcik, N. S., & Cardinali, S. (2020). Managing uncertainty during a global pandemic: An international business perspective. *Journal of Business Research*, 116, 188-192. <https://doi.org/10.1016/j.jbusres.2020.05.026>
- Sheffi, Y. (2005). *The resilient enterprise: Overcoming vulnerability for competitive advantage*. MIT Press.
- Sheffi, Y. (2015). *The power of resilience: How the best companies manage the unexpected*. MIT Press.
- Sheffi, Y., & Rice, J. B. (2005). A Supply Chain View of the Resilient Enterprise. *MIT Sloan Management Review*, 47.
- Shi, Z., Watanabe, S., Ogawa, K., & Kubo, H. (2018). Reviews of resilience theories and mathematical generalization. İçinde *Structural Resilience in Sewer Reconstruction* (ss. 17-78). Elsevier. <https://doi.org/10.1016/B978-0-12-811552-7.00002-X>
- Siddiqui, S. T. (2017). Can Employee Training and Development Increase Organizational Resilience Against Economic Crises? *International Journal of Managerial Studies and Research*, 5(4). <https://doi.org/10.20431/2349-0349.0504011>
- Sincorá, L. A., Oliveira, M. P. V. D., Zanquetto-Filho, H., & Ladeira, M. B. (2018). Business analytics leveraging resilience in organizational processes. *RAUSP Management Journal*, 53(3), 385-403. <https://doi.org/10.1108/RAUSP-04-2018-002>
- Singh, J., Abdul Hamid, A. B., & Garza-Reyes, J. A. (2023). Supply Chain Resilience Strategies and Their Impact on Sustainability: An Investigation from the Automobile Sector. *Supply Chain Management: An International Journal*, 28. <https://doi.org/10.1108/SCM-06-2022-0225>
- Singh, L. (2024). Enhancing resilience of human resource practices in the tourism and hospitality business of India during the COVID-19 pandemic. *Journal of Organizational Effectiveness: People and Performance*. <https://doi.org/10.1108/joepp-07-2023-0292>
- Singh, N. (2022). Developing Business Risk Resilience through Risk Management Infrastructure: The Moderating Role of Big Data Analytics. *Information Systems Management*, 39(1), 34-52. <https://doi.org/10.1080/10580530.2020.1833386>

- Singh, P., Ghadei, K., & Roy, P. (2024). Capacity Building in Organizational Management. İçinde *Emerging Trends in Agricultural Extension Education* (C. 2).
- Sinniah, S., Soomro, M. A., Rawshdeh, M., Rahman, M. R. C. A., Kadir, K. B. A., & Jamil, A. H. (2022). Post-COVID-19 Organizational Resilience in the Manufacturing and Service Industries. *Jurnal Pengurusan*, 66. <https://doi.org/10.17576/pengurusan-2022-66-02>
- Skinner, D. J. C., Rocks, S. A., & Pollard, S. J. T. (2014). A review of uncertainty in environmental risk: Characterising potential natures, locations and levels. *Journal of Risk Research*, 17(2), 195-219. <https://doi.org/10.1080/13669877.2013.794150>
- Soosay, C. A., Hyland, P. W., & Ferrer, M. (2008). Supply chain collaboration: Capabilities for continuous innovation. *Supply Chain Management: An International Journal*, 13(2), 160-169. <https://doi.org/10.1108/13598540810860994>
- Sprčić, D. M., Kožul, A., & Pecina, E. (2015). State and Perspectives of Enterprise Risk Management System Development—The Case of Croatian Companies. *Procedia Economics and Finance*, 30, 768-779. [https://doi.org/10.1016/S2212-5671\(15\)01326-X](https://doi.org/10.1016/S2212-5671(15)01326-X)
- Su, W., & Junge, S. (2023). Unlocking the recipe for organizational resilience: A review and future research directions. *European Management Journal*, 41(6), 1086-1105. <https://doi.org/10.1016/j.emj.2023.03.002>
- Sundstrom, S. M., Angeler, D. G., Barichievy, C., Eason, T., Garmestani, A., Gunderson, L., Knutson, M., Nash, K. L., Spanbauer, T., Stow, C., & Allen, C. R. (2018). The distribution and role of functional abundance in cross-scale resilience. *Ecology*, 99(11), 2421-2432. <https://doi.org/10.1002/ecy.2508>
- Sutcliffe, K. M., & Vogus, T. J. (2003). Organizing for Resilience 7. İçinde K. S. Cameron, J. E. Dutton, & R. E. Quinn (Ed.), *Positive Organizational Scholarship: Foundations of a New Discipline* (1st ed). Berrett-Koehler.
- Taleb, N. N. (2007). *The black swan: The impact of the highly improbable* (C. 45). Random House (U.S.) Allen Lane (U.K.).
- Tanner, T., Bahadur, A., & Moench, M. (2017). *Challenges for resilience policy and practice*. <https://doi.org/10.13140/RG.2.2.30130.30402>
- Tasic, J., Amir, S., Tan, J., & Khader, M. (2020). A multilevel framework to enhance organizational resilience. *Journal of Risk Research*, 23(6), 713-738. <https://doi.org/10.1080/13669877.2019.1617340>

- Tatar, Ü., & Karabacak, B. (2012). An Hierarchical Asset Valuation Method for Information Security Risk Analysis. *i-Society 2012 Proceedings*. International Conference on Information Society, London, United Kingdom.
- Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal*, 28(13), 1319-1350. <https://doi.org/10.1002/smj.640>
- Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(7), 509-533. [https://doi.org/10.1002/\(SICI\)1097-0266\(199708\)18:7<509::AID-SMJ882>3.0.CO;2-Z](https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z)
- Tekletsion, B. F., Gomes, J. F. D. S., & Tefera, B. (2024). Organizational resilience as paradox management: A systematic review of the literature. *Journal of Contingencies and Crisis Management*, 32(1), e12495. <https://doi.org/10.1111/1468-5973.12495>
- Thekdi, S., & Aven, T. (2024). Understanding the implications of low knowledge and high uncertainty in risk studies. *Risk Analysis*, 44(7), 1651-1665. <https://doi.org/10.1111/risa.14262>
- Theocharidou, M., Melkunaite, L., Eriksson, K., Winberg, D., & Honfi, D. (2016). *D1.3 Final lexicon of definitions* (No. D1.3). DHS Risk Steering Committee.
- Thoms, M. C., Piégay, H., & Parsons, M. (2018). What do you mean, ‘resilient geomorphic systems’? *Geomorphology*, 305, 8-19. <https://doi.org/10.1016/j.geomorph.2017.09.003>
- Tierney, K. J. (2014). *The social roots of risk: Producing disasters, promoting resilience*. Stanford Business Books, an imprint of Stanford University Press.
- Timmerman, P. (1981). *Vulnerability, resilience and the collapse of society: A review of models and possible climatic applications*. Institute for Environmental Studies, University of Toronto.
- Timoshenko, S., & Goodier, J. N. (1951). *Theory of Elasticity* (2. bs). McGraw-Hill.
- Tjahyono, B., Prabowo, H., Alamsjah, F., & Hamsal, M. (2024). The Influence of Digital Adoption, Absorptive Capacity and Risk Management Implementation on Organizational Resilience: An Empirical Study in The Indonesian Banking Industry. *2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI)*, 1-6. <https://doi.org/10.1109/IATMSI60426.2024.10502857>

- Togok, S. H., & Zainuddin, S. (2014). *Review of Enterprise Risk Management (ERM) Literature*.
- Trump, B., Florin, M.-V., & Linkov, I. (Ed.). (2018). *IRGC Resource Guide on Resilience (Volume 2)*. EPFL International Risk Governance Center. <http://infoscience.epfl.ch/record/262527>
- UNISDR & WMO. (2012). *Disaster Risk And Resilience: Thematic Think Piece* (UN System Task Force on the Post-2015 UN development agenda) [Technical Report]. United Nations.
- Unit4. (2023). Organizational Resilience: Why it Matters and How to improve it. *ORGANIZATIONAL RESILIENCE*.
- Valbuena, P. N., Montenegro, Y. A. M., González, M. H., & Cendales, B. (2023). Organizational resilience factors in Bogotá-based businesses during the COVID-19 pandemic. *Cuadernos de Administración*, 39(77), e2712965. <https://doi.org/10.25100/cdea.v39i77.12965>
- Vhanda, D., Chinowaita, F., Chinowaita, K., Vhanda, R., Nherera, B., Dzinamarira, T., & Chitungo, I. J. B. (2023). *Enterprise risk management implementation challenges in the Zimbabwean medical laboratory industry*. In Review. <https://doi.org/10.21203/rs.3.rs-2864979/v1>
- Vogus, T. J., & Sutcliffe, K. M. (2007). Organizational resilience: Towards a theory and research agenda. *2007 IEEE International Conference on Systems, Man and Cybernetics*, 3418-3422. <https://doi.org/10.1109/ICSMC.2007.4414160>
- Vugrin, E. D. (2010). A framework for assessing the resilience of infrastructure and economic systems. İçinde K. Gopalakrishnan & S. Peeta (Ed.), *Sustainable and Resilient Critical Infrastructure Systems*. Springer Berlin Heidelberg. <https://doi.org/10.1007/978-3-642-11405-2>
- Walker, B., Holling, C. S., Carpenter, S. R., & Kinzig, A. P. (2004). Resilience, Adaptability and Transformability in Social-ecological Systems. *Ecology and Society*, 9(2), art5. <https://doi.org/10.5751/ES-00650-090205>
- Walker, W. E., Harremoës, P., Rotmans, J., Van Der Sluijs, J. P., Van Asselt, M. B. A., Janssen, P., & Krayen Von Krauss, M. P. (2003). Defining Uncertainty: A Conceptual Basis for

- Uncertainty Management in Model-Based Decision Support. *Integrated Assessment*, 4(1), 5-17. <https://doi.org/10.1076/iaij.4.1.5.16466>
- Wang, Y. (2024). Possible Challenges and Recommendations for Risk Managers in Financial Institutions. *Academic Journal of Science and Technology*, 10(3), 192-194. <https://doi.org/10.54097/c36vhq88>
- Weick, K. E., & Sutcliffe, K. M. (2007). *Managing the unexpected: Resilient performance in an age of uncertainty* (C. 45). John Wiley & Sons, Inc. <http://choicereviews.org/review/10.5860/CHOICE.45-3293>
- Werner, E. E., & Smith, R. S. (1982). *Vulnerable, but invincible: A longitudinal study of resilient children and youth*.
- Werner, E., Bierman, J., & French, F. (1971). *The Children of Kauai: A Longitudinal Study from the Prenatal Period to Age Ten* (C. 35). University of Hawaii Press. <https://www.jstor.org/stable/350669?origin=crossref>
- Wied, M., Oehmen, J., & Welo, T. (2020). Conceptualizing resilience in engineering systems: An analysis of the literature. *Systems Engineering*, 23(1), 3-13. <https://doi.org/10.1002/sys.21491>
- Wieland, A., & Wallenburg, C. M. (2013). The influence of relational competencies on supply chain resilience: A relational view. *International Journal of Physical Distribution & Logistics Management*, 43(4), 300-320. <https://doi.org/10.1108/IJPDLM-08-2012-0243>
- Williams, T. A., Gruber, D. A., Sutcliffe, K. M., Shepherd, D. A., & Zhao, E. Y. (2017). Organizational Response to Adversity: Fusing Crisis Management and Resilience Research Streams. *Academy of Management Annals*, 11(2), 733-769. <https://doi.org/10.5465/annals.2015.0134>
- Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering & System Safety*, 141, 5-9. <https://doi.org/10.1016/j.ress.2015.03.018>
- Wu, D., & Olson, D. L. (2008). *New Frontiers in Enterprise Risk Management* (D. L. Olson & D. Wu, Ed.). Springer Berlin Heidelberg. <http://link.springer.com/10.1007/978-3-540-78642-9>

- Xue, X., Wang, L., & Yang, R. J. (2018). Exploring the science of resilience: Critical review and bibliometric analysis. *Natural Hazards*, 90(1), 477-510. <https://doi.org/10.1007/s11069-017-3040-y>
- Yoe, C. E. (2019). *Principles of risk analysis: Decision making under uncertainty* (Second edition). CRC Press, Taylor and Francis Group.
- Yu, D. J., Schoon, M. L., Hawes, J. K., Lee, S., Park, J., Rao, P. S. C., Siebeneck, L. K., & Ukkusuri, S. V. (2020). Toward General Principles for Resilience Engineering. *Risk Analysis*, 40(8), 1509-1537. <https://doi.org/10.1111/risa.13494>
- Zahra, S. A., & George, G. (2002). Absorptive Capacity: A Review, Reconceptualization, and Extension. *The Academy of Management Review*, 27(2), 185. <https://doi.org/10.2307/4134351>
- Zhao, X., Hwang, B.-G., & Low, S. P. (2015). Enterprise risk management in international construction firms: Drivers and hindrances. *Engineering, Construction and Architectural Management*, 22(3), 347-366. <https://doi.org/10.1108/ECAM-09-2014-0117>
- Zhou, Q., Edafioghor, T. E., Wu, C., & Doherty, B. (2023). Building organisational resilience capability in small and medium-sized enterprises: The role of high-performance work systems. *Human Resource Management Journal*, 33(4), 806-827. <https://doi.org/10.1111/1748-8583.12479>

EKLER

EK: Kavram Sözlüğü (Türkçe - İngilizce)

Türkçe	İngilizce
Ayırma Stratejisi	: Separation Strategy
Azaltma Stratejisi	: Mitigation Strategy
Beklenmedik Durum Planı	: Contingency Plan
Çeşitlendirme Stratejisi	: Diversification Strategy
Çeşitlilik	: Diversity
Daha iyi yeniden inşa etme	: Build back better
Ekolojik Dayanıklılık	: Ecological Resilience
Geri sıçrama	: Bounce back
İleri sıçrama	: Bounce forward
İşbirliği ve Ortaklık	: Collaboration and Partnership
Kabul Etme Stratejisi	: Acceptance Strategy
Kaçınma / Sonlandırma Stratejisi	: Avoidance / Termination Strategy
Kapasite Geliştirme	: Capacity Building / Improving
Kopyalama Stratejisi	: Duplication Strategy
Kurumsal Ağlar	: Networking
Modülerlik	: Modularity
Mühendislik Dayanıklılığı	: Engineering Resilience
Paylaşma Stratejisi	: Sharing Strategy
Risk Algısı	: Risk Perception
Risk İletişimi	: Risk Communication
Risk İştahı	: Risk Appetite
Risk Kapasitesi	: Risk Capacity
Risk Kültürü	: Risk Culture
Risk Toleransı	: Risk Tolerance
Risk Tutumu	: Risk Attitude
Transfer Etme Stratejisi	: Transfer Strategy
Yayılma (Dalgalanma) Etkisi	: Ripple Effect
Yedeklilik	: Redundancy