T.C.

İSTANBUL SABAHATTİN ZAİM ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

İŞLETME ANABİLİM DALI

ULUSLARARASI FİNANS VE KATILIM BANKACILIĞI BİLİM DALI

İŞ SÜREKLİLİĞİ YÖNETİM SİSTEMİ VE BANKACILIK SEKTÖRÜNE YÖNELİK MODEL

YÜKSEK LİSANS TEZİ

Vedat Aydemir

İstanbul

Şubat 2016

T.C.

İSTANBUL SABAHATTİN ZAİM ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

İŞLETME ANABİLİM DALI

ULUSLARARASI FİNANS VE KATILIM BANKACILIĞI BİLİM DALI

İŞ SÜREKLİLİĞİ YÖNETİM SİSTEMİ VE BANKACILIK SEKTÖRÜNE YÖNELİK MODEL

YÜKSEK LİSANS TEZİ

Vedat Aydemir

Danışman: Yrd. Doç. Dr. Turgay GEÇER

İstanbul

Şubat 2016

Sosyal Bilimler Enstitüsü Müdürlüğüne,

Bu çalışma jürimiz tarafından İşletme Anabilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Başkan Yrd. Doç. Dr. Turgay GEÇER (Danışman) .....

Üye Prof. Dr. Servet BAYINDIR .....

Üye Yrd. Doç. Dr. Ensari YÜCEL .....

Onay

Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım.

.....

Prof. Dr. İbrahim GÜNEY

Enstitü Müdür V.

ÖZET

İŞ SÜREKLİLİĞİ YÖNETİM SİSTEMİ VE BANKACILIK SEKTÖRÜNE YÖNELİK MODEL

Vedat AYDEMİR

Danışman: Yrd. Doç. Dr. Turgay GEÇER

Şubat 2016, x + 58 Sayfa

Bu çalışmada iş sürekliliği yönetim sistemi ve bankacılık sektöründe iş sürekliliğinin nasıl uygulanabileceğine yönelik örnek bir model anlatılmaktadır.

İş sürekliliği yönetim sisteminin amacı, kamu veya özel sektördeki tüm işletmelerde müşterilere yüksek kaliteli hizmeti kesintisiz olarak sunabilmek, işletmenin imajını korumaya, yasal yükümlülükleri yerine getirmeye ve müşterilerin ihtiyaçlarını karşılamaya en olumsuz koşullar altında dahi devam edebilmektir. İş sürekliliği yönetim sistemi, bilgi teknolojileri uygulamaları, çalışan, lokasyon, tedarikçi vb. diğer kaynakların yedeklenmesi ve alternatif çalışma yönteminin belirlenmesi çalışmalarını içermektedir.

İş sürekliliğinin temelini oluşturan tanımlar, dünyada ve ülkemizde bu konudaki standartlar ve kanuni zorunluluklar incelenmiştir.

Olası bir kesinti/afet durumunda mal ve can kaybını önlemek için gereksinim duyulan acil eylem yönetimi çalışmaları, olayın itibar etkisi, kamuoyu ve ilgili yasal otorite bilgilendirmelerinin nasıl yapılabileceğine yönelik çalışmalar kriz yönetimi konuları arasında incelenmiştir.

Kritik faaliyetlerin belirlenmesi, IT sistemlerinin yedeklenmesi ve altyapı tasarımlarına yönelik çalışmalar iş etki analizi konuları arasında incelenmiştir.

ABSTRACT

MASTER THESIS

BUSINESS CONTINUITY MANAGEMENT SYSTEM AND A MODEL FOR THE BANKING SECTOR

Vedat AYDEMİR

Supervisor: Assistant Prof. Dr. Turgay GEÇER

February 2016 – x + 58 pages

This study describes a model that defines business continuity management and how to apply in the banking sector.

The aim of business continuity management system is to be able to provide high quality and sustained services to the customers of all businesses types operating whether in public or in private sector, to protect the company's image, to continue to fulfill their legal obligations and to meet customers' needs even under the most unfavorable conditions. System comprises back–up IT systems, employees, locations, suppliers and other resources and determination of alternative working methods.

Definitions which are creating the basis of business continuity, standards in our country and in the world, legal requirements are examined.

Studies how to create emergency action management studies to prevent loss of property or life in any possible interruption/disaster, reputational effect of event, how to make information to public or legal authority are examined under crisis management.

Identification of critic activities, back–up IT systems and studies for infrastructure designs are examined under business impact analysis.

ÖNSÖZ

Kamu ve özel sektörde yer alan işletmeler için iş/hizmet sürekliliği, teknoloji dünyası ve rekabet piyasasının çok hızlı gelişim göstermesinden dolayı vazgeçilmez en önemli başlıkları arasında yer almaktadır. İş/hizmet sürekliliğini sağlayamayan her kuruluş kısa zamanda faaliyetlerine son vermek durumunda kalacaktır. İş sürekliliği, iş/hizmet kesintisine sebep olacak tüm risklerin belirlenerek bu tür durumlarda finansal, yasal, rekabet ve itibari etkileri açısından kayıpsız ya da en az kayıpla atlatılmasına yönelik faaliyetlerin tamamını kapsayan bir yönetim sistemidir. Bankacılık sektörü açısından ise teknoloji tabanlı işlemlerin çok olması iş/hizmet sürekliliğini daha fazla önemli hale getirmektedir.

İş sürekliliği yönetim sistemi alanında yapılan tez çalışması ile bu alandaki akademik çalışmaların artırılması hedeflenmiştir. Çalışma sırasında iş sürekliliği konusunda tecrübeli kişi ve firmalarla görüşmeler, literatür taramaları, internet araştırmaları, eğitim ve seminerler, iş sürekliliği konusunda yazılan yerli ve yabancı kitap, makale incelemeleri gerçekleştirildi. Literatür çalışması kapsamında daha önce bu konuda yapılmış uygulamalı çalışmalar araştırılmıştır. Konu üzerinde yapılmış araştırmalarda, bu çalışmada kullanabileceğimiz hazır bir model bulunamadığından Z. Serdar Kebapçı'nın doktora tezi, Tübitak–Bilgem'den Ali Dinçkan ve Özgüven Saymaz'ın yaptıkları çalışmalardan yararlanılmıştır.

Tez çalışması esnasında değerli görüşlerini ve desteklerini esirgemeyen tez danışmanı Sayın Yrd. Doç. Dr. Turgay Geçer'e, savunma jürisinde yer alan değerli hocalarım Sayın Prof. Dr. Servet Bayındır'a, Sayın Yrd. Doç. Dr. Ensari Yücel'e ve hayatımın her döneminde desteklerini hiçbir zaman esirgemeyen anneme, babama ve eşime teşekkürlerimi bir borç bilirim.

İÇİNDEKİLER

Sayfa No.

TABLOLAR LİSTESİ

Sayfa No.

GRAFİKLER LİSTESİ

Sayfa No.

ŞEKİLLER LİSTESİ

Sayfa No.

KISALTMALAR ve SİMGELER

ATM	Otomatik Vezne Makinesi
BDDK	Bankacılık Düzenleme ve Denetleme Kurumu
COBIT	Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri
DS4	İş/Hizmet Sürekliliğinin Sağlanması
EFT	Elektronik Fon Transferi
IEC	Uluslararası Elektronik Komisyonu
ISO 22301	Sosyal Güvenlik–İSY Standardı
ISO	Uluslararası Standartlar Örgütü
IT	Bilgi Teknolojileri
ITIL	Bilgi Teknolojileri Altyapı Kütüphanesi
NFPA	ABD Yangından Korunma Kurumu
ODM	Olağanüstü Durum Merkezi
POS	Satış Noktası
RPO	İş Kurtarma Noktalarının belirlenmesi
RTO	İş Kurtarma Zaman Dilimi

GİRİŞ

Günümüz iş dünyasında başarılı olmak ve rekabet yarışında devam edebilmek için iş operasyonlarının sürekliliğinin sağlanması, veri kaybının önlenmesi, beklenmedik olaylara karşı hızlı ve çevik bir şekilde davranabilme imkânı sunan stratejilere sahip olunması büyük önem taşımaktadır. İşletmelerde hizmet kesintilerinin asgari düzeyde olması, olası bir felâket sonrası hizmetlerin en hızlı şekilde tekrar hayata geçirilmesi önem arz etmektedir. Bu ürün/hizmet/süreçlerin hayata geçirilmesi firmalara ve kurumlara faaliyetlerinin devamı açısından önemli düzeyde katkı sağlar.

İş sürekliliği, bir işletmenin her zaman minimum şartlar dâhilinde risklerinin kontrol edilerek operasyonun devamının sağlanmasıdır. Beklenmeyen bir durum, sorun veya felâket anında kritik iş fonksiyonların sürekliliğinin sağlanması hayati bir öneme sahiptir. Tüm finansal sektörlerde olduğu gibi özellikle bankacılık sektöründe 7/24 kesintisiz hizmet sunabilmek çok önemlidir. Bu nedenle bankalar yasal zorunluluk, müşteri memnuniyeti ve finansal etkilerden dolayı iş sürekliliği konusunda maliyeti yüksek yatırımlar yapmaktadır.

İş sürekliliğinde personel, lokasyon, IT sistem kaynakları yedeklenir. Olası bir felâket durumunda veya hizmet kesintisinde yedeklenen bu kaynaklar aracılığıyla işletmelerin kritik süreçlerini devam ettirebilmesi hedeflenir. Sistemin sürekliliği açısından, işletmede bir risk kültürü oluşturulması, acil durumlara karşı hazırlıklı olunması gerekliliğinin üst yönetimce benimsenmesi, planlı ve organize hareket etme bilincinin çalışanlara aktarılabilmesi amacıyla bilinçlendirme çalışmaları yapılır.

Bu çalışma üç bölümden oluşmaktadır. Birinci bölümde iş sürekliliğinin temelini oluşturan tanımlar, standartlar ve kanuni zorunluluklar genel olarak ele alınmıştır.

İkinci bölümde, iş sürekliliğinin teorik çalışmaları hakkında bilgi verilmiştir.

Üçüncü ve son bölümde ise, bankacılık sektöründe iş sürekliliğinin nasıl uygulanabileceğine yönelik örnek bir model anlatılmaktadır.

BÖLÜM I

1. İş Sürekliliği Yönetim Sistemi Nedir?

1.1. İş Sürekliliği Yönetim Stratejisi ve Hedefi

Bir işletmeye yönelik olası iş kesintilerinin etkilerini önceden tespit eden ve ilgili tüm paydaşların çıkarlarını, markasını ve değer oluşturma faaliyetlerini koruyan, olası tehditlere karşı esneklik kazandırmak için bir alt yapı sağlayan bütünsel bir yönetim süreci iş sürekliliği yönetimi olarak ifade edilir (ISO, 2007, s. 3-4). İş sürekliliği yönetimi tüm paydaşların katılımıyla oluşturulan, yönetilen, güncellenen ve kontrol edilen bir süreçler bütünüdür.

İşletmenin hizmet sürekliliğini engelleyen bir felâket veya kesinti sonrasında izlenmesi gereken strateji personeli korumak ve bedensel kayıplarla ilgilenmek, tüm paydaşlarla iletişimi yönetmek, olayın boyutunu değerlendirip tehdidi belirlemek, ortaya çıkan sorunları ve sonuçlarını değerlendirmek, operasyonları/süreçleri olabildiğince hızlı çalışabilir hale getirmek, yazılı–sosyal–görsel medya ilişkilerini yönetmek konularını temel alacaktır (Burgan Pörtföy İş Sürekliliği Planı, 2015, s. 3). Stratejik olarak belirlenen diğer bir hedef ise kritik operasyonları minimum ancak müşterinin kabul edebileceği düzeyde en kısa sürede işlevsel hale getirmektir.

1.2. İş Sürekliliği Nedir?

> *"Türü ve sebebi ne olursa olsun, herhangi bir kesinti veya felâket durumunda, bir organizasyonun kritik iş fonksiyonlarının sürekliliğini sağlayan bir yöntem olarak tanımlanmaktadır* (Kebapcı, 2012, s. 5)*".*

Beklenmeyen bir durum, sorun veya felâket anında kritik iş fonksiyonlarının sürekliliğinin sağlanması hayati bir öneme sahiptir. Kriz anında sorumluluklar acil eylem, kriz yönetimi ve iş kurtarma takımları arasında paylaştırılır, başarılı bir şekilde kriz yönetilir ve işletme faaliyetlerini devam ettirir.

İş süreçlerine ilişkin teknolojik, operasyonel, mali, hukuki riskler belirlenmeli, işe etkileri uygun araç ve metotlarla ölçülmeli ve süreçlerin önem düzeyine göre önceliklendirilir. Gerçekçi ve uygulanabilir stratejiler ile periyodik olarak test edilerek

sürekli gelişim sağlanmalıdır. İş sürekliliği aşağıdaki sorulara daha net cevap verilebilmesini sağlayan sistemler bütünüdür.

- *''İşin 1 saat aksamasının firmaya maliyeti nedir?*
- *İş ve sistemlerin tekrar faal duruma gelmesi için işletme olarak ne kadar süre tahammül edilebilir?*
- *Herhangi bir aksamanın müşteriler, iş ortakları ve tedarikçiler üzerindeki etkisi biliniyor mu?*
- *Kesintiye uğramanın şirketinize getireceği mali kayıplar ne kadar?*
- *Ya imaj kaybı? gibi sorulara bu planlama aşamasında cevaplar verilebilecektir (Rıdvan, 2014, s. 3)''.*

İş sürekliliği kesintisi doğal afetler, planlı çalışmalar ve planlanmayan arızalar benzeri sebeplerden olmaktadır. Doğal afetler, sel, yangın, deprem gibi olağanüstü durumları içermekle birlikte bilgi teknolojileri yazılım, donanım ve siber saldırılardan dolayı oluşabilecek kesintileri de kapsamaktadır.

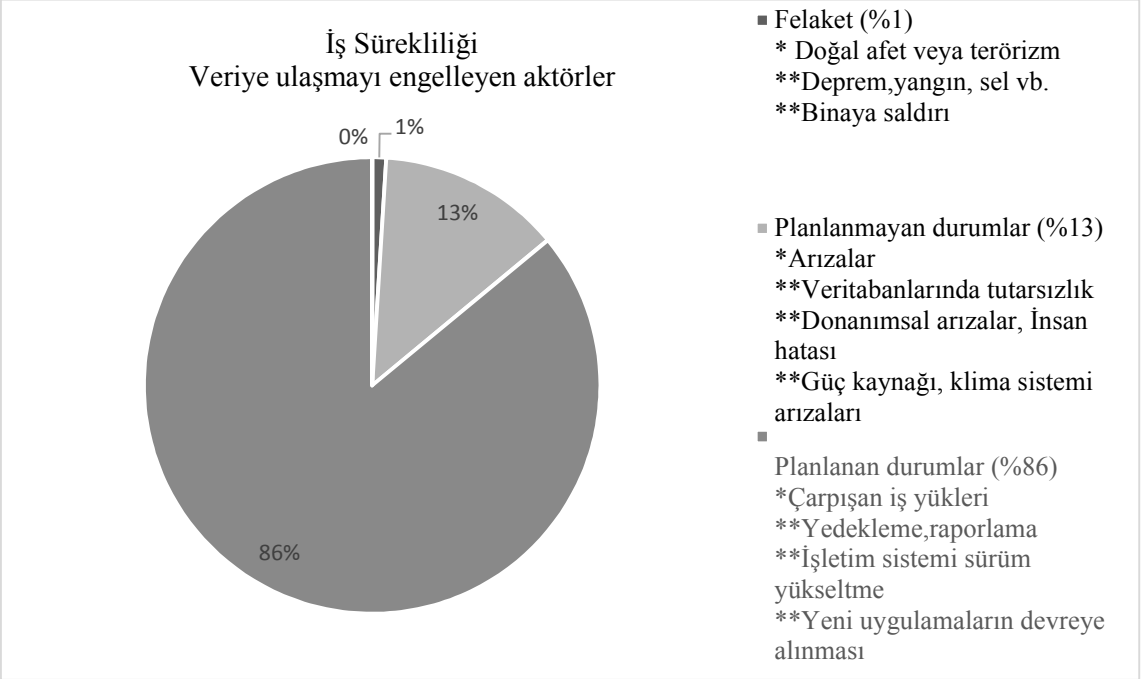
İç kontrol ve fiziksel güvenlik de dâhil olmak üzere tehditler, kurumun kritik iş operasyonları ve hizmetlerinde büyük hasar veya kesintilere neden olabilir, iş sürekliliği yönetim sistemi bu tür durumlarda işin devamlılığını sağlar.

İş sürekliliği altyapısının oluşturulmasında planlanan işlerde yaşanan kesintilerinin oranının yüksek düzeyde olması süreklilik altyapının kurulmasını daha da zorunlu kılmaktadır. Aşağıdaki tabloya göre felaket durumu yaşanması olasılığı, planlanan veya planlanmayan durumların yaşanma olasılığından çok düşük düzeydedir.

Aşağıdaki tabloda iş kesintilerinin % 1'lik kısmı doğal felaketlerden, % 13 planlanmayan durumlardan ve % 87'lik kısım ise planlanan durumlardan kaynaklandığı tespit edilmiştir. Planlanan durumlar işletim sistemi ve veritabanı sürüm artırımları, yeni yazılımların devreye alınması, yedekleme vb. çalışmaları içermektedir. Bu çalışmalarda öngörülemeyen hususlar ortaya çıkar ve genellikle iş kesintisine sebep olur.

İş sürekliliği yönetim sisteminin faydaları; iş sürekliliği yönetim sistemi tüm kuruluş ve işletmelere, altyapı sistemlerine bağımlılık, çalışan ve varlıkların korunması, imaj kaybının engellenmesi gibi konularda farkındalık sağlar.

Grafik 1: Kesinti Kaynakları



Kaynak: Ali Kulaklı ve Serpil Aslan, Beykent Üniversitesi Sosyal Bilimler Dergisi, 4 (1), 2010, s. 3.

Olası bir iş kesintisinde hasarsız veya en az hasar ile kesintinin atlatılmasına olanak sağlar. Aşağıda sistemin faydaları maddeler halinde yer almaktadır.

- *''Afete dayanma, işi sürdürme gereği, artan farkındalık,*
- *Doğal ve insan kaynaklı afet tehditleri,*
- *Altyapı sistemlerine bağımlılık,*
- *Ekonomik çevredeki (örneğin tedarikçiler) riskler,*
- *Çalışanların, varlıkların, bilginin korunması,*
- *Normale dönüş maliyetlerinin azaltılması,*
- *Mevzuat gereklilikleri, iç ve dış denetimler,*
- *Müşteri beklentileri, pazar gereklilikleri,*
- *İmaj kaybının engellenmesi (Yazar, 2009, s. 7)''.*

İş sürekliliği, işletme veya kuruluş ile alakalı müşteriler, tedarikçiler, çalışanlar, üst yönetim ve hissedarlar olmak üzere işletmenin ürün ve hizmetlerini hazırlayan ve kullanan tüm paydaşlara farklı alanlarda katkı sağlar. Aşağıdaki tabloda paydaşlara yönelik faydalar yer almaktadır.

Tablo 1: İş Sürekliliğinin Paydaşlara Fayda Tablosu

Kime	Ne Kazandırır
Müşterilere	İşletmeden Her Durumda Ürün/Hizmet Alacağına Dair Güvence
Hissedarlara	Şirket Değerinin Korunması
Üst Yönetime	Rekabet Avantajı
	Şirket İtibarının Korunması
	Hissedarlara Karşı Yükümlülüklerin Yerine Getirilmesi
	Nakit Akışının Korunması
	Çalışanların Güveninin Kazanılması Ve Pozitif Mesaj Verilmesi
Çalışanlara	Güvenli Bir Çalışma Ortamı
	Olası Bir Afet Sonrası Şirketin Varlığına Devam Etmesi
	Kriz Anında Sorumlulukların Doğru Bir Şekilde Paylaşılması
Tedarikçilere	Güvenilir Bir İş Ortaklığı

Kaynak: Marsh Danışmanlık, İş Sürekliliği Eğitim Notları, 2010, s. 7.

1.3. İş Sürekliliği Standartları

1.3.1. ISO 22301–İş Sürekliliği Standardı

İş sürekliliği ile ilgili standartların 2003 yılında İngiltere Standartları Enstitüsü tarafından yayımlanan Kamuya Açık Şartname kuralları ile başladığı kabul edilir. Bir süre sonra bu konu ile alakalı olarak 2006 yılında resmi bir standart olan 'BS 25999–1:2006–İş Sürekliliği Yönetimi: Uygulama Kuralları' yayımlanmıştır. İş sürekliliği sistemine ilişkin ikinci önemli standart ise Kasım 2007'de yayımlanmıştır. 'BS 25999–2:2007–İş Sürekliliği Yönetimi–Gereksinimler' olarak adlandırılan bu bölümde ise iş sürekliliği için olmazsa olmaz gereksinimler belirtilmektedir. 15 Mayıs 2012 tarihinde yapılan değişikliklerle birlikte uluslararası standart olarak kabul edilmiş ve 'ISO 22301:2012 Social Security–Business Continuity Management Systems–Requirements' ismiyle ISO standardı olarak yayımlanmıştır (Özbilgin, 2014, s. 101). Bu kurallar iş sürekliliğinin çeşitli prosedür, koşul ve politikalarının yönetimini idare etmek için oluşturulmuştur.

ISO 22301 standardı, kurumu kesintiye uğratacak olaylar meydana geldiğinde kurumun hazırlıklı olması, cevap verebilmesi ve geri dönebilmesi için belgelenmiş bir yönetim sitemine ilişkin gereksinimleri belirler. Her tipte ve büyüklükte organizasyon için uyarlanabilir olan bu standart organizasyonun tanınması, yönetimin desteği, planlama, kaynak tahsisi, sürecin işletilmesi, performans değerlendirmesi ve iyileşme başlıklarında ana maddeler içermektedir.

1.3.2. Bankaların İç Sistemleri Hakkında Yönetmelik

28 Haziran 2012 tarih ve 28337 sayılı Resmi Gazetede yayımlanan Bankaların İç Sistemleri Hakkındaki Yönetmelikte iş sürekliliği ve planı hakkında yapılacak çalışmalar belirtilmiştir (BDDK, 2015, s. 12-14).

- *Madde 9–İç kontrol sisteminin amacı ve kapsamı (2) İç kontrol sisteminden beklenen amacın sağlanabilmesi için; c) Acil ve beklenmedik durum planı hazırlanması,*
- *Madde 13–Acil ve beklenmedik durum planı; 14 Eylül 2007 tarihli Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğde ise bilgi sistemlerine ilişkin iş sürekliliği ve kurtarma planına yönelik çalışmalar belirtilmiştir,*
- *Madde 18–Bilgi sistemlerine ilişkin iş sürekliliği ve kurtarma planı; yönetim kurulu tarafından onaylanmış bilgi sistemlerine ilişkin bir iş süreklilik ve kurtarma planı hazırlanır,*
- *Madde 31–Servis sürekliliği ve kurtarma planı.*

1.3.3. COBIT 4.1

COBIT olarak isimlendirilen standart 'ISACA–Information Systems Audit and Control Association' ve 'ITGI–IT Governance Institute' tarafından 1996 yılında geliştirilmiştir. Bilgi teknolojileri yönetiminin oluşturulmasına altyapı sağlayan en iyi uygulamalar standardıdır. COBIT 4 temel alan ve 34 üst seviye kontrol hedefiyle, IT kaynaklarının etkin ve verimli yönetimini hedefleyen bir çerçeve dokümanıdır. IT yönetiminin işletme unsurları içerisinde sağlanması ve iş ihtiyaçlarını karşılayacak şekilde tasarlanması ana hedefleri arasında yer almaktadır (Bayoğlu, 2015, s. 2). COBIT; kullanıcılar, denetçiler, yönetim ve iş süreçleri sahiplerine hitap etmektedir. Sağlıklı bir iş sürekliliği için mutlaka gerekli olan IT yönetişimi ve diğer destekleyici süreçler haricinde, COBIT çerçevesinin iş sürekliliği konusuna değinen DS4–kesintisiz hizmetin garanti edilmesi kontrol hedefi bulunmaktadır. DS4 süreci, kritik iş süreçlerine hizmet veren IT hizmetlerindeki kesintilerin olasılığını ve iş süreçlerine etkisini en aza indirgemeyi amaçlar. Bu amaçla IT süreklilik planlarının hazırlanması, testlerinin yapılması, eğitimlerinin verilmesi, süreklilik planlarının ve bilgilerin dış lokasyonlarda

saklanmasını tavsiye etmektedir. DS4 süreci içerisinde verilen on adet detaylı kontrol hedefi aşağıda özetlenmiştir.

- *''DS4.1 IT Continuity Framework/IT Süreklilik Çerçevesi,*
- *DS4.2 IT Continuity Plans/IT Süreklilik Planları,*
- *DS4.3 Critical IT Resources/Kritik IT Kaynakları,*
- *DS4.4 Maintenance of the IT Continuity Plan/IT Süreklilik Planının Devamlılığı,*
- *DS4.5 Testing of the IT Continuity Plan/IT Süreklilik Planının Test Edilmesi,*
- *DS4.6 IT Continuity Plan Training/IT Süreklilik Planı Eğitimi,*
- *DS4.7 Distribution of the IT Continuity Plan/IT Süreklilik Planının Dağıtımı,*
- *DS4.8 IT Services Recovery and Resumption/IT Hizmetleri Kurtarma ve Devam Ettirme,*
- *DS4.9 Offsite Backup Storage/Dış Lokasyonda Yedekleme,*
- *DS4.10 Post–resumption Review/Kurtarma Sonrası Gözden Geçirme (Türkiye Bilişim Derneği, 2012, s. 31-33)''.*

1.3.4. ISO/IEC 27001/27002

ISO/IEC 27002 standardına göre bilgi güvenliği, hizmet sürekliliğinin sağlanması, iş ve süreç risklerinin en düşük seviyeye indirilmesi, yatırım geri dönüşünün ve yeni iş fırsatlarının artırılması amacıyla bilginin her türlü tehdide karşı korunması olarak tanımlamıştır. İş sürekliliği çalışmaları, bilgi güvenliği yönetim sistemi kurulumunun temel amaçları arasında yer almaktadır. ISO/IEC 27001 standardında yer alan 11 ana başlık arasında yer alan başlıklardan biri de iş sürekliliği yönetimidir.

ISO/IEC 27001 standardının 'A.14.1 İş sürekliliğinin bilgi güvenliği hususları' başlığında iş ve hizmet faaliyetlerindeki kesintileri önlemek, iş süreçlerini bilgi sistemleri felâketlerden korumak ve faaliyetlerin aksamadan zamanında devam etmesini sağlamak amacıyla, A.14.1 kontrol hedefi altında beş adet kontrol tanımlanmıştır. Bu kontroller aşağıda listelenmiştir.

- *''A.14.1.1 Bilgi güvenliğini iş sürekliliği prosesine dâhil etme,*
- *A.14.1.2 İş sürekliliği ve risk değerlendirme,*
- *A.14.1.3 Bilgi güvenliğini içeren süreklilik planlarını geliştirme ve gerçekleştirme,*
- *A.14.1.4 İş sürekliliği planlama çerçevesi,*

- *A.14.1.5 İş sürekliliği planlarını test etme, sürdürme ve yeniden değerlendirme, (Bayoğlu, 2015, s. 2)".*

1.3.5. ITIL v.3

ITIL v3 içerisinde iş sürekliliği yönetimi ayrı bir başlık olarak belirtilmemiştir. Hizmet tasarımı, hizmet geçişi, hizmet işletme ve sürekli hizmet iyileştirmesi adımlarından oluşan bir yaşam döngüsü olarak IT iş sürekliliği süreci tanımlanmıştır.

ITIL v3 IT İş Sürekliliği 'nin amacı aşağıdaki gibi özetlenebilir:

- *''IT hizmet süreklilik planlarıyla, ilgili IT kaynaklarını ve hizmetlerini gerekli durumlarda iş ihtiyacını karşılayabilecek şekilde çalışır hale getirerek kurumun genel iş sürekliliği sürecini desteklemek,*
- *IT kaynaklarının iş süreçlerine olan etkisi ya da iş ihtiyaçlarındaki değişikliklerin planlara yansıtıldığından emin olmak üzere düzenli iş etki analizi yapılması,*
- *Düzenli (IT iş sürekliliği) risk analizlerinin yapılması,*
- *IT iş sürekliliği ve kurtarma çalışmaları konusunda diğer departmanlara tavsiyeler verilmesi, rehberlik edilmesi. (Bayoğlu, 2015, s. 3)".*

1.3.6. Ülkemizde İş Sürekliliği ile Alakalı Mevcut Standartlar

Türkiye'de iş sürekliliği konusunda yasal düzenlemeye tabi üç sektör bulunmaktadır. Bu sektörler içerisinde yer alan enerji sektöründe iş sürekliliği konusunda henüz somut çalışmalar bulunmamaktadır. Somut çalışmalar içeren diğer sektörler aşağıda yer almaktadır.

Elektronik haberleşme sektörü; sektörün yasal düzenleyicisi Bilgi Teknolojileri ve İletişim Kurumudur. Bu alanda temel kanun, 5809 Sayılı Elektronik ve Haberleşme Kanunudur. Yasa, elektronik ve haberleşme sektörüne zorunlu kurallar getirmiştir. Milli güvenlik ve kamu düzeni ile olağanüstü hal, sıkı–yönetim, seferberlik, savaş halleri, yangın, deprem, sel, vb. doğal afet durumlarında haberleşme hizmetlerinin sağlanmasına ilişkin özel kanun hükümleri saklı tutulmuştur (Komut, 2013, s. 103).

Bankacılık sektörü yasal otorite BDDK'dır ve sektörün temel yasası 5411 Sayılı Bankacılık Kanunu ile kurulmuştur. Yasada 'İş Sürekliliği' dolaylı olarak düzenlenmiş ve konuyla ilgili bir de yönetmelik çıkartılmıştır. Yasa tebliğlerinde; Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere yer verilmiştir (Komut, 2013, s. 104). Bu

düzenlemede ‘Bankanın iş sürekliliğinin önemli oranda bilgi sistemlerinin işlerliğine bağlı duruma gelmesi’ ve ‘Bilgi sistemlerine ilişkin iş sürekliliği ve kurtarma planı’ geliştirilmiştir. Bu plan aynı zamanda yönetmelik ile ayrıntılı bir şekilde düzenlenmiştir. Yönetmelikle birlikte tüm bankalar için yurt içinde en az bir tane olağanüstü durum merkezinin kurulması da zorunlu hale getirilmiştir.

İş sürekliliği alanında SS 540, ABD Yangından Korunma Kurumu 1600, HB292, ISO/IEC 20000, NIST SP 800–34 gibi uluslararası farklı standartlar da bulunmaktadır.

1.4. İş Sürekliliği ‘nin Yoğun Kullanıldığı Sektörler

İş sürekliliği günümüzde ticari kazanç hedefleyen her sektöre ve kuruluşa hitap etmektedir. En yaygın kullanılan sektörleri ise aşağıdaki şekilde detaylı inceleyebiliriz.

- *‘’Bankacılık; Müşteri güveni, uyumluluk, paydaş ve ortakların haklarının korunması ve banka operasyonlarının sürekliliğinin sağlanması,*
- *Telekom; Kesintisiz iletişim sürekliliğinin sağlanması,*
- *Perakende; Tedarik zinciri, ürün planlaması ve mağaza operasyonlarının sürekliliğinin sağlanması,*
- *Sağlık; Medikal hataların azaltılması, itibari yönetmeliklerle uyum, hastane operasyonlarının sürekliliğinin sağlanması, maliyetlerin kontrolü ve hastaların ilgisinin çekilmesi,*
- *Sigorta; İş operasyonlarının merkezde, bölgesel ve binlerce acente ofislerinde sürekliliğinin sağlanması,*
- *Otomotiv Endüstrisi; Üretim ve hizmet operasyonlarının sürekliliğinin sağlanması (Akdağ, 2009, s. 18-19)”.*

2008 yılında ABD’de yapılan bir çalışmaya göre çeşitli sektörlerdeki 1 saatlik kesintinin finansal maliyetine yönelik değerler aşağıdaki tabloda yer almaktadır. Bankacılık, kredi kartları, sigorta ve güvenlik sektörü iş kesintilerden en yüksek düzeyde etkilenen sektörler olduğu görülmektedir. Finansal etki dışında itibari ve yasal etkileri de oluşmaktadır.

Tablo 2: Sektörel Bazda Saatlik Kesinti Maliyeti

Sektör	İş Tipi	Bir Saatlik Kesintinin Maliyeti ($)
Telekom	Mobil Telekom	1.500.000
Finans	Sigorta–Güvenlik	6.500.000
Finans	Kredi Kartları, Bankacılık	2.600.000
Medya	İzle–Öde TV	150.000
Perakende	Evden Alışveriş	113.000
Perakende	Katalog Satışları	90.000
Ulaşım	Uçuş Rezervasyonları	89.500
Medya	Tele–Bilet Satışları	69.000

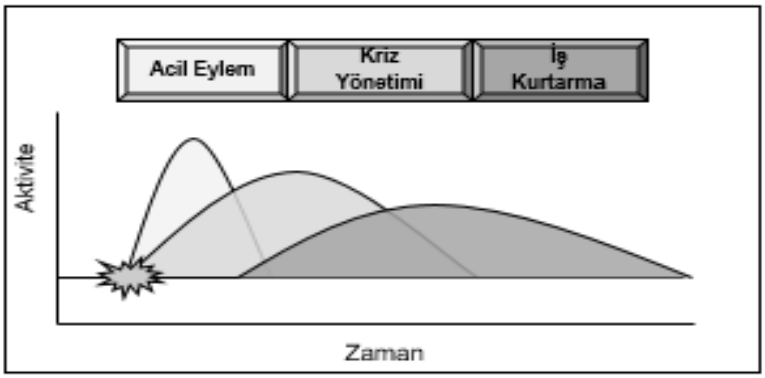
Kaynak: Ali Kulaklı ve Serpil Aslan, Beykent Üniversitesi Sosyal Bilimler Dergisi, 4 (1), 2010, s. 5.

BÖLÜM II

2. İŞ SÜREKLİLİĞİ YÖNETİM SİSTEMİ KURULUMU

2.1. Başlangıç

İş sürekliliği temel olarak üç fazdan oluşmaktadır. Herhangi bir olağanüstü durum veya kesinti meydana geldiğinde öncelikle birinci aşamada acil eylem yönetimi devreye girer. Bu aşamada meydana gelen olayın fiziksel olarak sonlanması sağlanır. ikinci aşamada kriz yönetimi aşamasına geçilir. Olayın büyüklüğü, firma açısından itibari risk oluşturması, kamuoyuna bilgi verilmesi gerekliliğini oluşturabilecek durumları içerir. Firmanın/çalışanların krizden en az düzeyde etkilenmesine yönelik faaliyetler gerçekleştirilir. Üçüncü aşamada ise iş kurtarma planı devreye alınır ile kritik süreçlerin devam ettirilmesine yönelik faaliyetler gerçekleştirilir.



Şekil 1:İş Sürekliliği Yönetim Aşamaları

Kaynak: Marsh Danışmanlık, İş Sürekliliği Yönetimi Eğitim Notları, 2010

İş sürekliliği sistemi aşağıdaki adımlardan oluşmaktadır.

- Acil Eylem Yönetimi
- Risk Analizi
- Kriz Yönetimi
- İş Kurtarma
- İş Etki Analizi
- Eğitim–Test

2.2. Acil Eylem Yönetimi

Toplumun, işletmenin veya bir organizasyonun tamamı veya belli bölümünün normal işleyiş ve faaliyetlerini durduran, kesintiye uğratan ve acil müdahale gerektiren olayları ve bu olayların oluşturduğu kriz halinin tamamı acil durum olarak tanımlanmaktadır (Çakır, 2007, s. 8). Acil durumlar doğal afetler (deprem, yangın, sel vb.), yolların kapanması, haberleşme kayıpları, tesis içi kazalar, yanlış işletme, düzensiz bakım, personel dalgınlığı, terörizm, savaş, siber saldırı vb. diğer olaylar sonucunda oluşabilir. Acil durum ifadesi daha çok tıp alanında kullanılmasına rağmen, yönetim literatürüne Dünya Bankası'nın önerisi üzerine 17 Ağustos 1999 İzmit depreminden sonra girmiştir (Beyatlı, 2010, s. 4).

Ülkemizde 6331 Sayılı İş Sağlığı ve Güvenliği Kanunu hükümlerince tüm işletmelerin acil eylem planlarını hazırlaması gerekir. Plan içeriğinde aşağıdaki detaylandırılan başlıklar yer alabilir.

Acil durum planı genel esasları; acil durum planının hangi şartlarda ve kimler tarafından devreye alınacağı belirtilir. Planın amacı ve genel akışı hakkında bilgilendirmeler yer alır. Doğal afet veya felâket durumunda nasıl hareket edilmesi gerektiği ve can–mal kaybı yaşanmamasına yönelik alınacak aksiyonları içerir.

Acil durum organizasyonu ve acil durum ekiplerinin görevi; acil durumda nasıl hareket edileceği, hiyerarşik düzenin ne şekilde işletileceği belirlenir. Bu kapsamda acil durum organizasyonu net olarak belirlenir ve rol–sorumluluklar ilgili kişilere atanır. Olası bir acil durum esnasında görev alacak ekipler önceden belirlenir. Genel olarak her işletmede ilk yardım ekibi, can–mal kurtarma ekibi, söndürme ekibi, tahliye ekibi, haberleşme–teknik ekip ve güvenlik ekibi olmak üzere acil durum ekipleri oluşturulur. Her ekibin sorumlulukları ve görev yapacağı lokasyon belirlenir.

Haberleşme/iletişim sistemi ve planı; işletmelerin acil durumlardaki olumsuzlukları kayıpsız veya en az kayıpla atlatabilmeleri için bir organizasyon yapısı kurulur. Oluşturulan bu organizasyonda ise haberleşme ve iletişim sisteminin etkin bir şekilde kullanılacak şekilde çalışmalar yapılır. Can kaybı yaşanması durumunda haberleşme konusunda daha hızlı ve etkin çözümler sağlanır. Tüm organizasyonlarda işlerin yürütülmesi adına hiyerarşik bir yapılanma bulunmaktadır. Olası bir acil durum

meydana geldiğinde ilgili ekiplerin kim ile–nasıl–nerede–ne zaman iletişim kuracağı belirlenir.

Acil durum prosedürleri; meydana gelebilecek acil durumlara göre farklı aksiyon planlaması yapılır. Yaşanan olaylar sonucunda elde edilen tecrübeler doğrultusunda acil durum tiplerine göre en uygun aksiyonların neler olacağı konusunda prosedürler oluşturulur. Bu prosedürlerde ilgili olay meydana geldiğinde ekiplerin rol ve sorumlulukları, nasıl hareket edecekleri ve iletişim konusunda alınması gereken aksiyonlar hakkında bilgiler yer almalıdır. Genel olarak yangın, deprem, sel, soygun, tahliye vb. konularda prosedürler oluşturulur.

Gerekli araç, gereç ve malzeme planlaması; acil durum ekiplerinin olası bir durum da kullanması için çeşitli yetkinliklerde araç gereç ve malzeme ihtiyacı ortaya çıkmaktadır. Bu araçların belirlenmesi, önceden tedarik edilmesi ve belirli periyotlarla test edilerek varsa kullanım ömrü sona eren veya kullanılamaz duruma gelen araç–gereçler değiştirilir.

Acil durum kuruluşları ile koordinasyon ve işbirliği; ülkemizde 2009 yılında kabul edilen 5902 no.lu afet ve acil durum yönetimi başkanlığının teşkilat ve görevleri hakkında kanun ile ülke çapındaki tüm afet ve acil durumlarda koordinasyon için bir afet ve acil durum yönetimi başkanlığı adıyla yeni bir yapı kurulmuştur. Afet ve acil durum yönetimi başkanlığı, afet ve acil durumlar ile sivil savunmaya ilişkin hizmetlerin ülke düzeyinde etkin bir şekilde gerçekleştirilmesi için gerekli önlemlerin alınması ve olayların meydana gelmesinden önce hazırlık, olay sırasında yapılacak müdahale ve olay sonrasında gerçekleştirilecek iyileştirme çalışmalarını yürüten kurum ve kuruluşlar arasında koordinasyonun sağlanması ve bu konularda politikaların üretilmesi ve uygulanması hususlarını içerecek çalışmalar yapmakla sorumludur (Resmi Gazete, 2009, s. 15). Bu yapının yanı sıra özellikle 112 Acil, 155 Polis İmdat, 110 İtfaiye gibi ülke çapında ve yerel olarak acil durumlarda destek veren devlet birimlerinin bu haberleşme sistemi içerisinde yer alması önem arz etmektedir. İşletmelerde meydana gelebilecek acil durumlarda bu birimlerle iletişim kurulur.

Acil durum senaryoları ve tatbikat planlaması; acil durum planları ve ekipleri belirlendikten sonra yıl içerisinde periyodik olarak belirli dönemlerde tatbikat yapılır.

Testin içeriği, amacı, türü, katılımcılar ve katılımcıların görev ve sorumlulukları, test ile ilgili kabullenmeler ve kısıtlar önceden belirlenmelidir. Yapılan bu tatbikatlarda varsa eksiklerin belirlenmesi ve planların yeniden revize edilmesi gerekmektedir. Tatbikat öncesinde hangi kapsamda test edileceğinin belirlenmesi için titiz bir çalışma yapılması gerekir. Gerekli hazırlık ve planlama faaliyetleri yapılmadığında test sırasında yaşanması öngörülmeyen ciddi kesintilerin oluşması söz konusu olabilir. Bu sebeplerden dolayı tatbikatlar için bir model belirlemek gereklidir (Dinçkan, İş Sürekliliği Kritik Başarı Faktörleri, 2010, s. 4). Tatbikat sonrasında ise hedeflerin ne kadar gerçekleştirildiğine yönelik sonuçların elde edilerek varsa eksik hususlarda aksiyon alınır. Tatbikatlar öngörülen birçok riske karşı hazırlık seviyesinin ölçümlenebildiği faaliyetlerdir. Bu nedenle acil durum tatbikatları yapısı gereği gerçekleştirilmesi zor olan testlerdir. Gerçekçi senaryolar üzerinden test yapabilmek olası acil durumlara hazırlık için son derece önemlidir.

Medya ile ilişkiler; herhangi bir işletme veya kuruluşta meydana gelebilecek olası bir acil durumda kamuoyunu doğru bilgilendirme için medya ile ilişkiler önemlidir. Yazılı ve görsel medya, sosyal medya ile nasıl ve kimler tarafından iletişim kurulacağı konuları çalışmada kriz yönetimi başlığında detaylı olarak yer almaktadır.

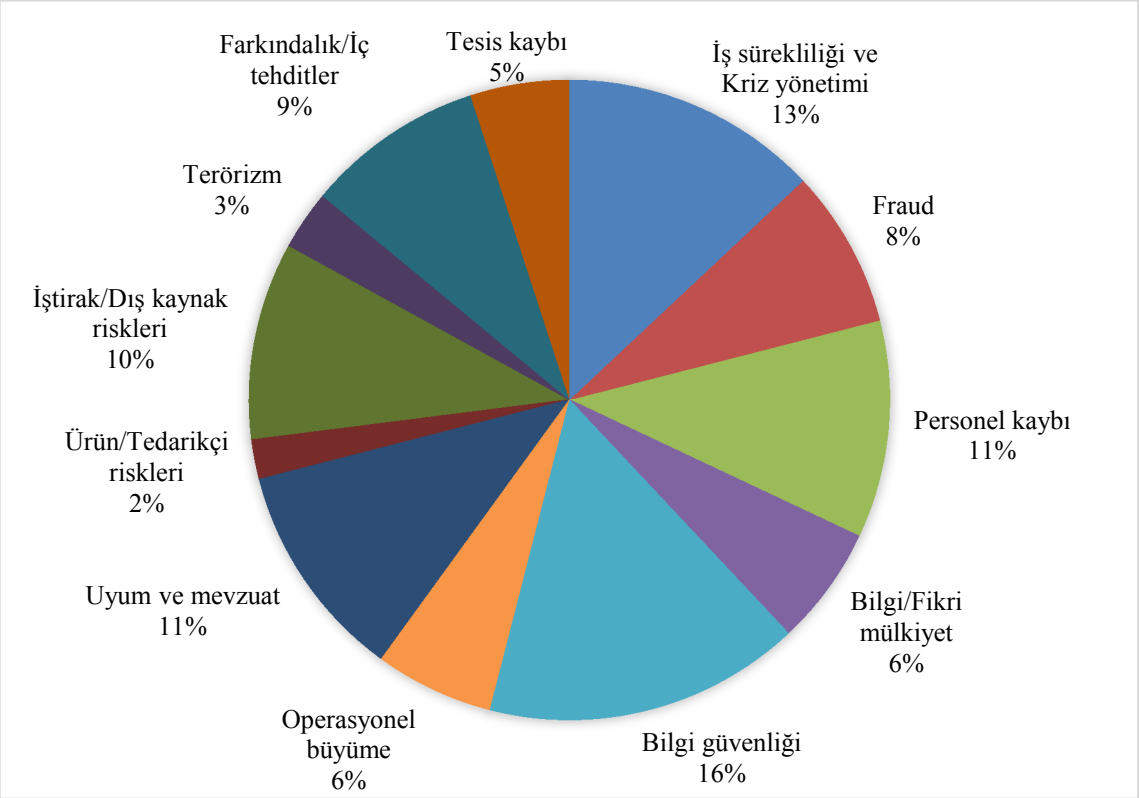
2.3. Risk Analizi

2.3.1. Risk Nedir?

> *"Risk, kelime anlamı ile zarara uğrama tehlikesini ifade eder. Risk potansiyel sorun, tehlike veya kaybı gösteren bir kavramdır. Belirli bir zaman aralığında belirli bir hedefe ulaşamama ve dolayısıyla zarara uğrama olasılığı olarak da tanımlanabilir. Dolayısıyla risk gelecekte oluşabilecek sorunlara ve tehlikelere işaret etmektedir. Riskin en belirgin özellikleri ise tam ve net olarak belirlenememesi, zamanla değişkenlik göstermesi, olumsuz sonuçlar doğurabilir olması ve yönetilebilir nitelikte bulunmasıdır* (Şahin, 2008, s. 3)*"*.

İş sürekliliği; likidite riski, kur riski veya kredi riski gibi risklere yönelik direkt bir çözüm sağlamamaktadır.

Aşağıdaki grafikte kurumsal ölçekte risk dağılımlarının hangi başlıklarda olduğu yer alır. Bilgi sistemleri güvenliği % 16 ile İş sürekliliği ve krizi yönetimi % 13 ile en yüksek riskin oluştuğu alanlar olduğu görülmektedir.



Grafik 2: Kurumsal Ölçekte Risk Dağılımı

Kaynak: Mustafa Komut, İ.Ü. Siyasal Bilgiler Fakültesi Dergisi, No:49, 2013 s. 110.

2.3.2. Risk Yönetim Süreci

Risk yönetim süreci; kapsamın belirlenmesi, risklerin tespit edilmesi, risklerin analiz edilmesi, risklerin önceliklendirilmesi, strateji ve aksiyon belirlenmesi, aksiyonların uygulanması ve izlenmesi, güncelleme yapılması faaliyetlerini içeren bütüncül bir süreçtir.

2.3.2.1. Kapsamın Belirlenmesi

Risk analiz çalışmasının ilk adımı kapsam belirlenmesidir. Risk analizi sonucunda ortaya çıkacak sonuç veya hedeflenen çıktıların net olması kapsamın belirlenmesinde önemli girdi sağlar. İçeriğin ilk aşamada doğru ve kurum hedeflerine uygun olarak

belirlenmesi sonraki aşamalarda risk analizinin kalitesini arttırır (Ulusal Elektronik Ve Kriptoloji Araştırma Enstitüsü, 2007, s. 11).

2.3.2.2. Risklerin Tespit Edilmesi

Risklerin tespit edilmesi, birimin hedeflerine ulaşmasını engelleyen veya zorlaştıran risklerin, önceden tanımlanmış yöntemlerle belirlenmesi, gruplandırılması ve güncellenmesi sürecidir. Tespit edilen riskler iç risk veya dış risk olabilir. Risklerin kimin sorumluluğunda olduğu belirlenir.

Riskleri belirlemede kullanılabilecek yöntemler aşağıda verilmiştir:

> *"Kontrol Listeleri: Önceki faaliyetlerden edinilen tecrübelere ve diğer kaynaklardan edinilen bilgilere dayanılarak risk tanımlama kontrol listeleri hazırlanabilir.*
>
> *Beyin Fırtınası: Amacı herhangi bir kısıtlama ya da önem sırası olmadan oluşabilecek bütün risklerin belirlenmesidir. Kontrol listeleri ve anketlere nazaran katılımcıların daha etkin olduğu bir tekniktir, ayrıca daha verimli yol alınmasını sağlar,*
>
> *Sebep–Sonuç Diyagramı: Problemin temel nedenini bulabilmek, mevcut nedenleri gruplamak, problem çözme sürecini daha düzenli hale getirmek ve tartışmanın amacından sapmasını önlemek amacıyla kullanılır* (Çalışma ve Sosyal Güvenlik Bakanlığı Strateji Geliştirme Başkanlığı, 2014, s. 9)*"*.

2.3.2.3. Risklerin Analiz Edilmesi

Risklerin tespit edilmesi aşaması ile birlikte doğru bir şekilde analiz edilmesi de önemlidir. Değerlendirmede nicel yöntemler kullanılabileceği gibi nitel yöntemler de kullanılabilir.

Risklerin analiz edilmesi sürecinde ağırlık oranları hesaplanarak derecelendirme yapılır ve risklerin önlem alınmasının gerekli olup olmadığına karar verilir. Öncelikle hangi konularda analiz yapılacağı belirlenir. Risk değerlendirme ve acil durum planında bu analiz çalışması sonucunda ne tür aksiyonlar alınması gerektiği detaylı şekilde açıklanır. Aşağıdaki tabloda yer alan tehdit başlıklarına göre risk analizi yapılır. Her tehdit tipine maruz kalma olasılığı ve etkisi işletme bazında değişir.

Tablo 3: Tehdit Başlıkları Listesi

Deprem	Medikal Acil Durum	Rehin Alma
Volkanik Aktivite	Radyoaktif Kirlenme	HVAC Arızası
Toprak Kayması	Yangın: İç–Katastrofik	Güç Kesintisi: İç
Mevsimsel/Lokal Seller	Yangın: İç–Büyük	Yedek Ekipman Arızası
Gelgitlerle İlgili Seller	Yangın: İç–Küçük	İletişim Arızası (Veri)
Tsunami	Uçak Kazası	Ses İletişim Ekipmanı Arızası
Hortum	Toksik Kirlenme	Medya Arızası
Kasırga/Tayfun	Su Tesisat Arızası	Satın Alınmış Yazılım Sorunu
Tropikal Fırtına	Su Sızıntısı	Regülasyonlar
Kar/Buz Fırtınası	Yangın: Dış	İnsan Hatası: Kullanıcılar
Kuvvetli Rüzgârlar	Patlama: Kurum Dışı	İnsan Hatası: Bakım
Kum Fırtınası	Patlama: Kurum İçi	Kaynakların Kaybı
Meteor Etkisi	Güç Kesintisi: Dış	Hırsızlık: Veri
Savaş Durumu: Geleneksel	Merkezi Bilgisayar Ekipmanı Arızası	Hırsızlık: Fiziksel Varlıklar ($250+)
Savaş Durumu: Nükleer	Güç Dalgalanmaları	Yolsuzluk
Sabotaj: İç Fiziksel	Vandalizm	İnsan Güvenlik Ölçümleri
Salgın Hastalık	Grev	Bio–Terorizm
Sabotaj: Dış Fiziksel	İsyan/Sivil Kargaşa	Kapasite Planlaması
Market	Kundakçılık	Operasyonel
Sabotaj: İç & Dış Veri Yazılımı	Bomba Tehdidi & Bombalama	İnsan Hatası: Operasyonlar & Programcılar

Kaynak: Sibel Akdağ, 2009, Risk Yönetiminde Başarı Faktörü 'İş Sürekliliği Yönetimi' Sunumu, s. 20.

2.3.2.4. Risklerin Önceliklendirilmesi

Risk ölçülmesi, tespit edilmiş risklere karşılık verilip verilmeyeceğine ve karşılık verilecekse fayda/maliyet dengesi açısından en uygun olan karşılığın seçilmesine yardımcı olur (Maliye Bakanlığı Strateji Geliştirme Başkanlığı, 2015, s. 12). Önceliklendirme ise risklerin öncelik sırasına göre listelenmesidir. Risk puanları büyükten küçüğe sıralanarak riskler önceliklendirilir.

Risk analizleri sonucunda belirlenen risklerden hangilerinin öncelikli olarak iyileştirilmesi gerektiğine karar verilir. Belirlenen risk önem derecesinin, risk kriterleri ve risk alma iştahları ile karşılaştırılması ve önem sırasına koyulması gerekir.

Organizasyonun hedefleri alternatif fırsatların potansiyel sonuçları ve şirketin risk alma isteği de göz önünde bulundurulur.

2.3.2.5. Strateji ve Aksiyon Belirlenmesi

Risklerin belirlenmesi sonrasında hedeflenen stratejiler belirlenmedir. Risk yönetim aksiyonlarına yönelik alternatiflerin belirlenmesi, bu alternatiflerden en uygun olanına karar verilmesi, alternatif uygulama planlarının hazırlanması ve uygulanmasını, özetle risk yönetim stratejilerinin belirlenmesini gerekir (Kalyoncu, 2013, s. 89). Belirlenen genel yaklaşım çerçevesinde bağlı olunan mevzuat ve işyeri koşulları dikkate alınır, alınması gerekli önlemlere karar verilerek strateji ve aksiyon belirlenmiş olur.

2.3.2.6. Aksiyonların Uygulanması ve İzlenmesi

İşletmede gerçekleştirilen risk yönetiminin tüm aşamaları ve uygulanması düzenli olarak izlenir, denetlenir ve aksayan yönler yeniden gözden geçirilir. Risk yönetiminin tüm fonksiyonları uygun şekilde işlese de, üretilen çıktıya göre uygun aksiyonlar alınmalıdır. Etkin bir risk yönetiminde, risklerin hedeflenen seviyede kalmasını sağlamak üzere ilgili aksiyonların alınması sağlanmalıdır (PwC, 2007, s. 12). Tespit edilen riskler ve risklerin önem derecesine göre belirlenen sıklıkta gözden geçirilmesi gerekir.

2.3.2.7. Güncelleme Yapılması

Güncelleme faaliyeti genellikle ihmal edilen konulardan biri olduğundan birçok şirkette yıllar önce tanımlanmış risklerin değişmeden takip edildiğini görmek mümkündür. Yılda en az bir defa olmak üzere; yeni eklenen riskler, durumu değişmiş riskler tespit edilerek güncelleme mutlaka yapılmalıdır.

2.4. Kriz Yönetimi

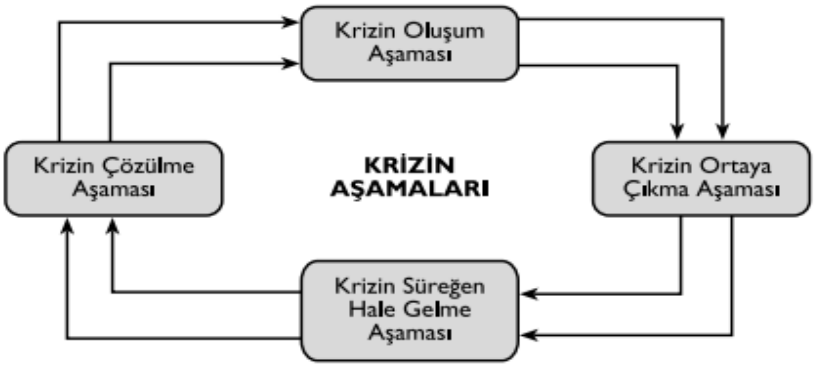
Kriz bir işletmenin mevcut konumunu ve geleceğini etkileyen beklenen veya beklenmeyen bir zaman diliminde ortaya çıkan ve genelde önlem alınmakta geç kalınan olumsuz bir durumu ifade eder. Risk gerçekleşmesi muhtemel olayları ifade ederken kriz ise gerçekleşmiş olayları kapsamaktadır (Balıkçı, 2009, s. 13). Kriz yönetimi ise ortaya çıkan krizlerin yönetilmesi konusundaki aksiyonları içerir.

İş sürekliliğinin 2.aşamasında kriz yönetim çalışmaları yapılmaktadır. Kriz yönetim takımı krize dönüşme potansiyeli bulunan olaylara müdahaleyi yönetmekle

görevlidir. Takım krizle alakalı tüm kararları alır ve başta kamuoyu ve diğer paydaşlar olmak üzere dış dünya ile olan her türlü iletişimi sağlamaktan sorumludur. Kriz yönetim planı, meydana gelen olayın olumsuz etkilerini mümkün olan en düşük seviyeye indirmek ve olay gerçekleşmeden önceki duruma en kısa zamanda ve en verimli şekilde dönülmesini temin etmek amacıyla hazırlanır.

2.4.1. Kriz Yönetim Planının Amacı ve Kapsamı

Kriz yönetimi; krizin oluşması, krizin ortaya çıkması, sürekli hale gelmesi, çözülme aşamalarından oluşmaktadır. Kriz yönetim planında amaç ve kriz ile alakalı genel akışı hakkında bilgilendirmeler yer alır. Planın hangi şartlarda ve kimler tarafından devreye alınacağı da planda içeriğinde bulundurulur.



Şekil 2: Kriz Yönetimi Aşamaları

Kaynak: Melek Tüz, Gürkan Haşit, İsa İpçipoğlu ve İdil K. Suher, (2013). Kriz İletişimi ve Yönetimi. T.C. Anadolu Üniversitesi Açık Öğretim Fakültesi Yayını No: 1776, s. 7.

2.4.2. Senaryo ve Stratejiler

Çevresel etkenler, doğal sebepler, ekonomik nedenler, teknolojik yenilikler, sosyal kültürel etkenler, uluslararası ilişkiler, yönetimin niteliği, bilgi toplama ve değerlendirmede yetersizlik, örgüt kültürü gibi sebeplerden dolayı krizler ortaya çıkabilmektedir.

Kriz yönetimi aşaması sadece içinde bulunulan durum gerektirdiği takdirde devreye alınır. Kriz yönetimi planını hayata geçirme kararı organizasyondaki kesilme veya aksamanın büyüklüğü, organizasyonun isminin ve itibarının korunması ihtiyacı, can

kaybı veya ağır yaralanma vb. durumları içerecek zamanlarda devreye alınabilir. Her işletme ve kuruluşa göre farklı değerlendirmeler olabilir. Senaryo ve stratejiler belirlenir, hangi durum ve senaryolarda ilgili planın devreye gireceği belirtilir.

2.4.3. Organizasyon Yapısı–Rol ve Sorumluluklar

Kriz yönetim takımı, kriz olasılığına göre gerekli hazırlıkların yapılması, kriz olduğunda işletmenin karşılaşabileceği riskin en kısa sürede azaltılması, işletmenin imajını korumakla görevlidir. Krize dönüşme potansiyeli bulunan ve şirketin normal operasyonuna devamını engelleyen olaylara müdahaleyi yönetmeli, krize yönelik stratejik yönlendirme sağlamalıdır. Bu takımın üyeleri, krizi sezebilme, bunların gerektirdiği işlemleri geliştirebilme, kriz anında işlerin yürütülmesini sağlayabilme ve danışmanlık görevi yapabilecek nitelikte olmalıdırlar (Sucu, 2009, s. 57).

İşletmelerde genel olarak üst yönetim kademesi kriz yönetim takımını oluşturmaktadır. Kriz yönetim takımı, işletmenin farklı kurumlarından, farklı alanlarında uzmanlaşmış yönetim kademesindeki kişilerin bir araya getirilmeleri ile oluşmuş farklı bir yapıya sahip olmalıdır. İdari işler, lojistik, satın alma, haberleşme, hukuk danışmanı, insan kaynakları, güvenlik, kurumsal iletişim, halkla ilişkiler, muhasebe birimleri de kriz yönetim takımına destek sağlayan birimler olarak organizasyon şemasında yer alır.

2.4.4. İletişim

Günümüzdeki serbest piyasa ekonomisi tüketici hakları ve müşteri mutluluğunu ön plana getirmiştir. ‘İmaj’ kavramı da bir kurum veya kuruluşun rekabet alanındaki en güçlü silahıdır. Bir kuruluşun kamuoyunda hangi özellikleri ile bilindiği, hangi sıfatlar ile tanımlandığını açıklayan ‘imaj’ tanımı uzun sürede ve büyük çabalarla oluşturulan bir kavramdır, fakat bunca güçlüklerle dönüşerek belleklere yerleşebilen bir olgudur (Canpolat, 2012, s. 122). Bugün bir kuruluş kamuoyunda olumlu bir imaj yaratmadıkça rakipleriyle rekabet edemeyeceğinin farkındadır. Kriz anında kurum ya da kuruluş doğrudan ilk haber kaynağı olarak görev yapmalıdır. Eğer bunu gerçekleştiremezse kontrolü elinde tutamaz ve kriz istenmeyen yönde yani kurum ya da kuruluşun imajını sarsacak doğrultuda ilerler.

> *“Kriz zamanlarında hedeflenen kamuoyu kitlesine mesajı iletecek kişi kurum sözcüsü olmalıdır. Sözcünün krizle ilgili olarak basına yapılan açıklamalarda*

söylenen sözlere dikkat etmesi gereklidir. İletişim kurulması gereken birden fazla paydaş olacaktır. Başta kamuoyu, resmi kurumlar, ortaklar, hissedarlar, çalışanlar ve aileleri, tedarikçiler, müşteriler gibi birçok paydaş olası bir krizde iletişim kurulması gereken paydaşlar arasında yer almaktadır (Suher, 2013, s. 116)*"*.

İletişim kanallarında yazılı ve görsel medyanın yanı sıra sosyal medya (Facebook, Twitter, Linkedin vb.) aracılığıyla da paydaşlar ile bilgi paylaşımı yapılır. Resmi kurumlar ile iletişim aşamasında işletmenin ilişkide olduğu tüm resmi kurumlar ve ilgilileri belirlenip bir listesi hazır hale getirilmelidir.

2.5. İş Etki Analizi

İş etki analizi aşaması iş sürekliliğinin temelini oluşturan aşamadır. İş etki analizi, işletmenin iş ve organizasyon yapısının tanınması ve tanımlanması için gerekli olan temel bilgilerin sağlanması, kritik ürün/hizmetlerin ve bunların sürekliliğini sağlamak için gerekli olan süreçlerin ve bu süreçlerin kurtarma önceliklerinin belirlenmesi, kritik süreçleri destekleyen, iç ve dış kaynakların belirlenmesine yönelik detaylı ve kapsamlı bilgilerin toplanması çalışmalarını içeren bir analiz çalışmasıdır (Saymaz, 2012, s. 84). İş etki analizi, işletmelerin mevcut durumdaki iş süreçlerinin incelenerek olası kesintilerin ve bu süreçlerin yasal, finansal, itibari vb. her türlü etkilerinin analiz edilmesi olarak tanımlanır. Kritik iş süreçlerinin belirlenmesi sonrasında bu süreçleri etkileyebilecek tehditler ile süreçlerde oluşacak ürün ve hizmet kesintilerinin yol açacağı zararların belirlenmesini hedeflemektedir (Türkiye Bilişim Derneği, 2012, s. 43).

İş etki analizi; iş süreçlerindeki kesintilerin etkilerini belirleyerek, ne kadar süre ile bu kesintilere tolerans gösterilebileceğini belirlemeye çalışmalarını kapsar. Bu çalışmadan elde edilen veriler, iş sürekliliği stratejilerinin tespit edilmesi için gerekli girdileri sağlamaktadır. İş etki analiz süreci aşağıdaki başlıklardan oluşmaktadır.

- Süreçlerin belirlenmesi,
- İş etki analizi çalışmalarının oluşturulması,
- Süreçlerin önceliklendirilmesi,
- Bağımlılık ve kaynakların belirlenmesi,

- Alternatif çalışma stratejilerinin oluşturulması ve olağanüstü durum merkezi tasarımı,
- İş sürekliliği planlarının hazırlanması.

2.5.1. Süreçlerin Belirlenmesi

İş etki analizi çalışmasının en önemli aşamalarından biridir. Bu aşamada işletmede gerçekleştirilen süreçler veya ürünler ele alınır. Süreç, proses kelimesinin karşılığı olarak dilimize girmiştir. Bir girdi ile başlayan, iç ve dış müşteriden gelen talep, bilgi veya hammadde ile bu girdiye katma değer katarak belirli bir çıktı üreten birbiriyle bağlantılı adımlar ve işlemler akışı şeklinde tanımlanmaktadır. İşletmelerde bir ürün elde edebilmek için yapılan çalışmaların tamamı da süreç olarak ifade edilmektedir (Sönmez, 2013, s. 13). İşletme içerisinde yer alan ana faaliyet konusu ile alakalı tüm süreçler ve departmanlar belirlenir.

2.5.2. İş Etki Analizi Çalışmaları

İş etki analizinde amaç işletme için süreçleri önem düzeyine göre gruplandırmaktır. Bu şekilde kritik süreçler ortaya çıkarılır.

2.5.2.1. Kritik Süreçlerin Belirlenmesi ve Önceliklendirilmesi

Etki kriterleri ve derecelerinin belirlenmesi; işletmelerde yer alan ürün ve hizmetlerin kritikliğini, önem düzeyini ve önceliğini belirlemeye yardımcı olacak değerlendirme kriterleri belirlenir. Sebebi ne olursa olsun meydana gelen iş kesintileri, işletme için finansal zararların yanında itibar kaybı, müşteri memnuniyeti gibi direkt finansal olmayan zararlara da yol açabilmektedir (Saymaz, 2012, s. 65). Etki türlerine göre belirli bir puan aralığında bir puanlama cetveli oluşturulur. Genel olarak tüm risklerin gerçekleşmesi durumunda gelir kaybı, gider artışı, personel değişimi, kötü reklam, hizmet tesliminin dengesizleşmesi, ceza ve yükümlülükler, hisse senedi değeri düşüşü, rekabet avantajı kaybı, pazar payı kaybı, verimlilik kaybı, şirket imajının ve itibarının kaybı vb. etkiler oluşabilir.

Zaman kriterleri belirlenmesi; kritik hizmetlerde oluşacak kesintinin süresi, ne kadar itibar kaybı oluştuğunu, işletmeye ne kadar para kaybı oluşturduğu ve sektördeki konumuna etkisinin boyutunu gösterecektir. Süreçlerin etki değerlendirmesinde hangi zaman dilimlerine göre yapılacağının belirlenmesi gerekmektedir. Süreçlerin 1 saat

yapılmamasında oluşacak etki ile 4 saat yapılmamasında oluşacak etkisi farklılaşmaktadır. Zaman dilimleri her sektöre, işletmeye göre farklılık gösterebilir. Genel olarak kabul edilen zaman dilimleri 1 saat, 4 saat, 1 gün, 1 hafta ve 1 ay olarak kullanılmaktadır.

Kritik iş süreçlerinin önceliklendirilmesi çalışması; iş sürekliliği kapsamında ürün ve süreçlerini belirleyen işletmeler, süreçlerini veya faaliyetlerini kesinti etkisi açısından önceliklendirir. Belirli bir zaman dilimi içinde hizmet kesintisi en yüksek düzeyde zarara yol açan ve kısa süre içerisinde kesintiden kurtulması istenen süreçler kritik süreç olarak belirlenir. Yüksek öncelik verilen kritik süreçler işletmenin ana başlık olarak odaklanacağı, planlama yapacağı, daha yüksek bütçe ayıracağı ana iş faaliyetlerini kapsamaktadır (Türkiye Bilişim Derneği, 2012, s. 43).

İlk aşamada yer alan en önemli çalışmalar süreçlerin önceliklendirilmesi kısmında yer almaktadır. Bu aşama sonucunda kritik süreçler belirlenerek ve zaman dilimlerine göre önceliklendirilmesi tamamlanır. Bu çalışmalar aynı zamanda iş etki analizinin ana taslağının oluşmasında en büyük paya sahiptir. Yapılacak bu önceliklendirmeye göre yatırım kararları, maliyetler vb. konular tamamen netlik kazanacaktır. Finans sektöründeki bir firma 1 gün ve öncesi için yatırım yapabileceğini belirtirken, otomotiv sektöründeki bir firma 1 hafta ve öncesi diye karar alabilir. Burada yatırım yapılabilecek zaman diliminin eşik seviyesi belirlenmesi gerekir.

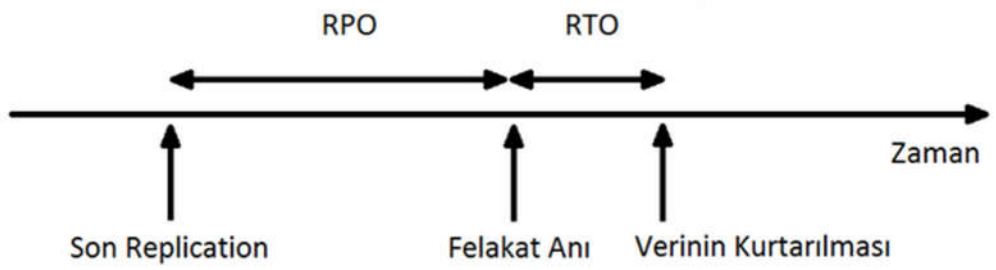
İşletmede yer alan her bölüm kendi süreçleri için zaman dilimlerine göre etki puanlaması yapar, elde edilen tüm sonuçlar bir değerlendirmeye tabi tutulur. Bu analiz sonucunda kritiklik dereceleri belirlenir. Kritiklik puanına göre önceliklendirme tablosuna yerleştirilir. İşletmenin belirleyeceği eşik zaman dilimi öncesinde yer alan süreçler kritik süreçler olarak ortaya çıkacaktır.

2.5.2.2. Kritik Süreçlerin Bağımlılıklarının Belirlenmesi

İş etki analizinin ikinci aşama çalışmalarında önceki aşamada kritik olarak belirlenen süreçlerin birbiriyle bağımlılıkları, dış kaynak bağımlılığı, bilgi teknolojileri bağımlılığı, personel ve diğer kaynak bağımlılıkları belirlenmesi konusundaki çalışmaları içermektedir.

RTO; kesintiye uğrayan iş veya hizmet sürecinin ne kadar zaman sonra tekrar faal duruma gelebileceğine dair belirlenen hedef süredir. RTO değerinin 30 dakika olması uygulamanın veya sürecin herhangi bir sebepten dolayı çalışamaz duruma gelmesi sonucunda 30 dakika içerisinde tekrar çalışır duruma getirilmesini ifade etmektedir.

RPO; bir iş veya hizmet süreci için işletmenin kabul edebileceği en yüksek düzeyde veri kaybını süre olarak belirtir. Bir süreç için RPO değerinin 4 saat olması sürecin en fazla 4 saatlik veri kaybına tahammülü olduğunu ifade eder. Herhangi bir sebepten dolayı veri kaybı yaşandığında 4 saat önceki veri geri yüklenir.



Şekil 3:RTO ve RPO Şekilsel Gösterimi

Kaynak: http://www.1stbasis. com/rto–rpo–for–business–continuity–disaster–recovery/, 2015.

Maksimum kabul edilebilir kesinti süresi değerlerinin belirlenmesi; maksimum kabul edilebilir kesinti süresi, bir iş süreci veya bilgi teknolojileri uygulaması için işletmenin kabul edebileceği en yüksek kesinti süresini belirtir. Bir iş süreci için Maksimum Kabul Edilebilir Kesinti Süresi değerinin 1 gün olması, sürecin herhangi bir sebeple çalışamaz hale gelmesi durumunda işletmenin bu kesintiye en fazla 1 günlük tahammülü olduğunu ifade etmektedir (Dinçkan, İş Sürekliliği Kritik Başarı Faktörleri, 2010, s. 3). Bu sürenin aşılması durumunda işletmenin ciddi boyutta zarara uğrayacağı ve pazardan silineceği ön görülmüştür. İşletme açısından oluşacak zarar finansal, yasal, müşteri memnuniyetsizliği olabileceği gibi kurum imajına yönelikte olabilir.

Kritik personel listesi; işletmede kritik süreç olarak belirlenen süreçleri gerçekleştiren kişiler kritik personel olarak belirlenir. Olası bir kesinti veya felâkette bu kişilere gerçekleştirdiği sürecin zaman dilimi içerisinde ulaşılmalı ve sistemsel yetkileri

vb. ayarlamaları yapılmalıdır. Kritik personel listesi oluşturulurken yedekler de belirlenmeli ve birden fazla iletişim numarası listede yer almalıdır.

Kaynaklar; bir süreci gerçekleştirmek için değişik kaynak ve donanımlara ihtiyaç duyulmaktadır. Kritik olarak belirlenen bir sürecin hangi kaynakları kullanarak gerçekleştirildiği belirlenir. Kritik süreçlerin gerçekleştirilmesi aşamasında ise IT kaynakları, personel, dokümantasyon, tedarikçi gibi değişik kaynaklara göre planlama yapılır. Bu kaynakların en önemlisi olarak bilgi teknolojileri kaynaklarıdır. IT kaynaklarının, kritik iş süreçleri için belirlenen öncelik seviyelerine uygun olarak kurtarılması planlanır (Bayoğlu, 2015, s. 5). Bir sürecin gerçekleştirilmesi için herhangi bir yazılım programı veya donanım programı gerekmektedir. Günümüzde işletmelerde gerçekleştirilen tüm süreçlerin en alt aşamalarına kadar yapılan işlemlerde IT uygulamaları yer almış bulunmaktadır. Tüm firma ve kuruluşlar için bilgi teknolojileri olmazsa olmaz konumdadır. Kritik olarak ortaya çıkan IT uygulamalarının olağanüstü durum merkezinde teknik altyapı olarak hazır hale getirilmesi gerekir. İş sürekliliği çalışmasının en önemli ve en pahalı çıktısı olağanüstü durum merkezidir.

Dokümantasyon; bu aşamada ise kritik süreçler gerçekleştirirken kullanılan fiziki ve dijital dokümantasyon ortamları hakkında değerlendirmeler yapılır. Kritik olarak belirlenen süreçlerin gerçekleştirilmesi için gerekli dokümantasyonlar belirlenir.

Dokumanın biçimi basılı veya dijital olarak belirtilerek buna göre alınacak aksiyonların belirlenmesinde faydalı olur. Dijital ortamda tutulduğu belirtilen dosyalar için ortak bir dosya belirlenir, belirli süreler de periyodik olarak yedeklenir.

İç bağımlılıklar; işletmede gerçekleştirilen tüm süreçlerin en az bir girdi ve bir çıktı süreci bulunmaktadır. Burada girdi başka bir sürecin sonucunda oluşan çıktıdır. Bu süreçlerin birbiriyle bağlantısı iç bağımlılık olarak belirtilmektedir. Bu sebepten daha önce oluşturulan kritik süreçlerin kesin sonuç olmadığı, nihai olarak oluşacak kritik süreçler bağımlılıklar tablosundaki değerlendirmelerden sonra ortaya çıkacaktır. Önceki aşamalarda kritik zaman dilimine giremeyen birçok süreç bağımlılıklardan dolayı kritik olarak değerlendirebilecektir.

Tüm kritik süreçler için iç bağımlılık değerlendirmesi yapılır. Elde edilen veriler tekrar analiz edilerek zaman dilimlerine göre süreçler yeniden güncellenir. Bu çalışma sonucunda nihai olarak kritik süreçler tespit edilir.

Kritik tedarikçilerin listesi; işletmede faaliyet gösterilen tüm süreçlerin bir kısmında ise dış tedarikçi firmalara bağımlılık bulunabilir. Tedarikçilerden, IT, danışmanlık, süreç ve yasal konuları içerecek konularda destek alınabilir. Bir süreci gerçekleştirirken birden fazla tedarikçiye bağımlılık olabilir, Bu durumda her tedarikçiyi ayrıca belirtmek gerekir. Her tedarikçiye bağımlılık düzeyi farklı olabilir. Tedarikçiler ile alakalı yapılması gereken konularından biri ise kritik olarak belirlenen tedarikçilerin iş sürekliliği ve olağanüstü durum merkezlerinin var olup olmadığının tespit edilmesidir. Tedarikçinin sağladığı hizmet veya ürünün olası bir felaket durumda aksamaması için ne tür çalışmalar yapıldığının bilinmesi işletmenin hizmet sürekliliği açısından önem arz etmektedir.

Ayrıca hizmet veya ürün seçiminde de bu kriteri göz önünde bulundurmak iş sürekliliği açısından gereklidir. Yapılacak olan sözleşmeler için bu tür bir madde eklenmesi firmanın olası kayıplarını en aza indirgerken sigorta maliyetlerinin düşürülmesine imkân tanıyacaktır.

Periyodik iş süreçleri tablosu; kritik süreçlerin günlük aylık, yıllık bazda yoğun olduğu dönemler belirlenir. Bu bilgi, eğer olağanüstü bir durum yoğun döneme denk gelirse nasıl bir planlama yapılması gerektiği konusunda veri sağlayacaktır (Saymaz, 2012, s. 88). Özellikle her ay veya haftanın belirli bir gününde yapılması gerekli olan zorunlu işlerin tespiti yapılmalıdır. Buradaki zorunluluk borsaya açık olan bir şirketin örneğin her üç aylık dönem sonunda gelir tablosu, bilanço vb. raporlarını sunması veya sosyal sigortalar kurumu, maliye bakanlığı gibi resmi kurumlara verilmesi gereken raporlar gibi sabit ve tarihi belirli olan işleri içerir.

Bölümler seviyesinde iletişim yapısı; olası bir kriz veya felâket durumda kimlerin aranacağı neler yapılacağı konusunda genellikle bir karmaşa oluşur. Bu konuda genel olarak bir çözüm bulunmasa da hazırlıklı olmak amacıyla bir arama zinciri oluşturulması gerekir. Bu arama zincirinde yer alan kişiler kimleri arayacağını bilmeli ve periyodik

testlerle bu konudaki süreklilik sağlanmalıdır. Arama zincirinde yer alan kişi iletişim bilgilerinde telefon bilgisinin en az iki farklı numara olması gerekir.

2.5.3. Alternatif Stratejilerinin Oluşturulması ve Olağanüstü Durum Merkezi Tasarımı

2.5.3.1. Alternatif Stratejilerinin Oluşturulması

Bu aşamada senaryolar belirlenerek bu senaryoların oluşması durumunda kritik süreçlerin sürekliliğinin sağlanabilmesine yönelik ne tür aksiyonlar alınacağı belirlenir. Senaryo sayısının fazla olması firmanın iş sürekliliğini sağlaması açısından daha verimli sonuçlar ortaya koyar. Strateji ne kadar kapsamlı ve iyi olursa olsun insanlar onu doğru biçimde uygulamayı başaramazlarsa işletme için hiçbir değeri olmayacaktır (Sarıkaya, 2008, s. 11).

2.5.3.2. Senaryo Bazlı Alternatif İş Kurtarma Planları

Belirlenen her bir sürecin olası felâket durumlarında nasıl sürekliliğinin sağlanacağına yönelik çalışmalar yapılması gerekir. Bu konuda yapılacak en kolay ve pratik çalışma senaryo oluşturup bu senaryolara göre alternatif çalışma yöntemlerini belirlemektir. Varsa diğer senaryolara göre de çözümler belirtildikten sonra diğer kritik süreçler içinde aynı çalışma yapılır. Tüm kritik süreçlere yönelik alternatif çalışma yöntemlerini belirledikten ve sonuçları derlendikten sonra iş kurtarma planının ana bilgileri tamamlanmış olur.

2.5.3.3. Bilgi Teknolojilerine Yönelik Kurtarma Planı ve Çalışmaları

Tüm işletme ve kuruluşlarda hizmet sürekliliği müşteri memnuniyeti, pazar payı, rekabet, itibar ve finansal etkileri açısından kritik düzeyde öneme sahiptir. Bilgi güvenliği, yazılım, donanım, network ve işletim sistemi, doğal afet veya fiziksel hatalardan kaynaklanan hizmet kesintilerini en düşük seviyeye indirmek, mümkün olduğunca ortadan kaldırması maksadıyla kullanılan yöntemlerden birisi olağanüstü durum merkezinin oluşturulmasıdır. Olağanüstü durum merkezi tasarımı yapılırken iş etki analizi çalışması sonucunda ortaya çıkan kritik IT sistemleri referans alınarak tasarım yapılır. Tespit edilen süre tip ve önceliklendirmelerine göre veri aktarımı planlanır.

2.5.3.4. Olağanüstü Durum Merkezi Nedir?

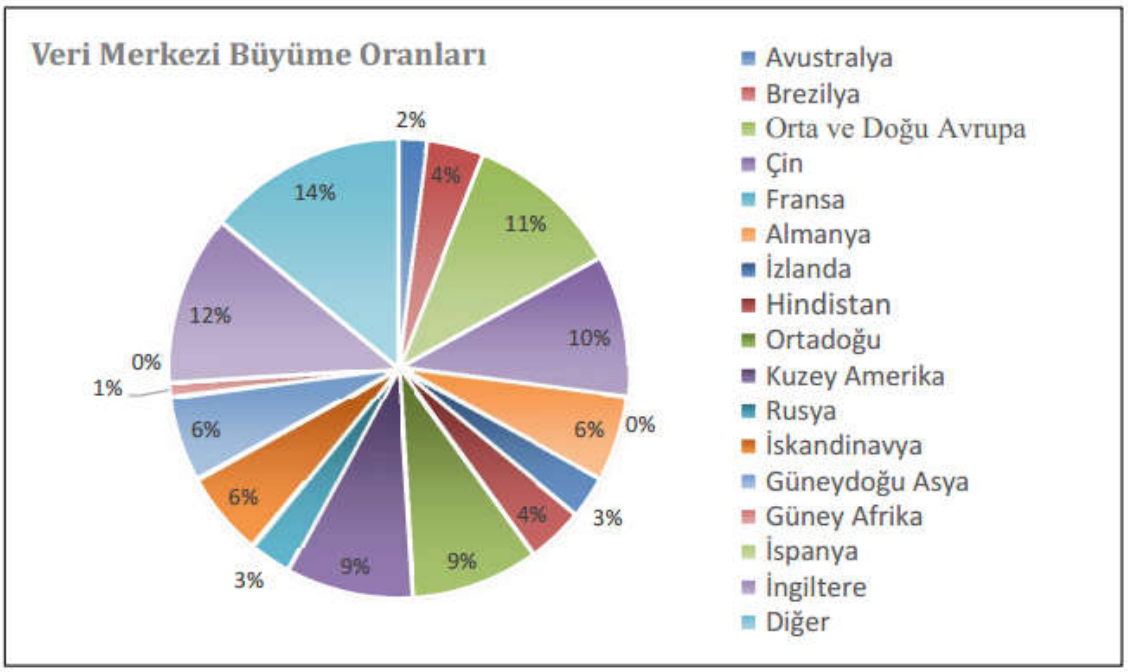
Olağanüstü durum merkezi, önceden tasarımı yapılan ve işletmenin kritik uygulamalarının sürekliliğini hedefleyen merkezi işlem birimi ve çevre birimlerinden oluşan bir veri merkezidir. Veri merkezi ana bankacılık sistemleri, işletmede yer alan diğer bilgisayar sistemleri ile veri ambarı sistemleri gibi birçok sistemi içerisinde barındıran bir tesistir. Sunucu odası veya sistem odası olarak da adlandırılan bu tesisler işletmelere ait storage, sunucu ve veri tabanlarının bulunduğu alanlardır.

Veri Merkezleri, koridorlarca uzanan, raf kabinleri dolusu yığılmış birçok sunucu barındırdığı için sunucu çiftlikleri olarak da adlandırılır. Veri merkezlerinde genel olarak veri depolama, yedekleme, kurtarma, veri ve ağ yönetimi, sunucu barındırma uygulamaları, ofis hizmetleri gibi hizmetler sağlanmaktadır. Bu merkezler işletmelere ait kurumsal web sitelerinin yayında olması, mobil ve ATM uygulamaların hizmet vermesi, e–posta ve anlık ileti gönderimi, bulut depolama hizmetleri, e–ticaret işlemleri, çevrimiçi oyun gruplarının ihtiyaç duyduğu bir çatı altında toplanma gibi konularda hizmet sunmaktadırlar. (Telkoder Serbest Telokomünikasyon İşletmecileri Derneği, 2015, s. 11). Bütün özel şirketler ve devlet kurumları, kendi verilerine erişilebilmesi için veri merkezlerine ihtiyaç duymaktadır. Kimi kurum ve kuruluşlar kendi veri merkezlerini kurmayı tercih ederken, kimileri sunucu barındırma ve kiralama hizmetlerinden yararlanır, bir kısmı ise umuma açık bulut bilişim hizmetlerinden yararlanmaktadır.

İş etki analizi çalışması sonucunda ortaya çıkan kritik süreçler ve bu süreçleri destekleyen IT altyapısının (yazılım, donanım, network, güvenlik, sunucu vb.) tasarlanarak felâket durumlarında kullanılması planlanan veri merkezine genel olarak olağanüstü durum merkezi olarak adlandırılmaktadır. Olağanüstü durumda faaliyetlerin yeniden başlatılması ve önceden yapılan planlamalar sonucunda hedeflenen sürede çalışmaların başlatılması amacıyla tasarlanan ve konumlandırılan veri merkezidir.

Veri merkezlerinin mevcut durumu; teknolojik gelişmeler bu alandaki yatırımlarında hızla büyümesine sebep oluşturmaktadır. Teknolojik büyümeler, veri büyümelerini, verilerin artması da sunucu ve storage vb. depolama teknoloji altyapısının büyümesini sağlamaktadır. Bu durum ise veri merkezlerinin artışına girdi sağlar.

Emerson firması tarafından 2011 yılında yapılan bir araştırmaya göre, dünya üzerinde toplam 509.149 veri merkezi bulunmaktadır. Bu veri merkezlerinin sahip olduğu toplam alan 26.555.619 metrekaredir. Bu araştırmaya göre dünyada ayrıca barındırma hizmeti sunan 3.441 tane veri merkezi bulunmaktadır (Telkoder Serbest Telokomünikasyon İşletmecileri Derneği, 2015, s. 18). Teknolojik alandaki büyümeler birbirleri bütünleşmiş tüm altyapılarında aynı hızla genişlemesine olanak sağlar. Aşağıdaki tabloda veri merkezi büyüme oranları ülke bazlı karşılaştırması yer almaktadır. İngiltere, ABD ve Çin bu alanda en hızlı büyüme oranlarına sahip ülkeler olarak öne çıkmaktadır.



Grafik 3: Dünya'da Veri Merkezi Büyüme Oranları

Kaynak: Telkoder Serbest Telekomünikasyon İşletmecileri Derneği, Veri Merkezi İşletmeciliği Raporu, 2015, s.18.

Türkiye'deki mevcut durum ise dünyada bu alandaki mevcut büyümeden daha yüksek bir eğilimle artış göstermektedir. Özellikle BDDK tarafından bankalara yönelik birincil ve ikincil sistemlerin yurtiçinde tutulmasına yönelik oluşturulan tebliğ sonrasında bu alandaki yatırımlar ivme kazanmıştır. 2013 yılında yapılan bir araştırmaya göre veri merkezi yatırımlarının % 26.7, kapasitelerinin % 31, enerji ihtiyaçlarının % 29.6, operasyonel giderlerinin % 32.1, personel istihdamın % 13.5 ve toplam % 26.58 oranında

bir büyüme gerçekleştirilmiştir (Telkoder Serbest Telokomünikasyon İşletmecileri Derneği, 2015, s. 19). Hızla büyüyen teknolojik sektörlere paralel olarak veri merkezi sektörünün de hızlı bir büyüme göstermesi beklenmektedir.

Türkiye'de veri merkezi hizmeti Türk Telekom, IBM vb. önde gelen teknoloji firmaları tarafından verilmektedir. Türk Telekom firması veri merkezi hizmetini Ankara lokasyonunda, IBM firması ise İzmir lokasyonunda vermektedir.

Olağanüstü durum merkezi gereksinimi; günümüz dünyasında IT uygulaması kullanmayan bazı şirketler olmasına rağmen birçok işletme tüm iş ve süreçlerini tamamen IT uygulamaları ile devam ettirmektedir. Herhangi bir işletme ürettiği veya kullandığı her türden veri için bir veri merkezine ihtiyaç duyar. IT uygulamalarının çalışması, sonrasında üretilen verilerin saklanması, yedeklenmesi vb. birçok süreç için sunucuların yer aldığı veri merkezleri oluşturulur.

Bankacılık ve finans kurumları, eğitim işletmeleri, enerji şirketleri, telekomünikasyon şirketleri, devlet kurumları, sağlık kurumları, toptan ve perakende sektörü, Linkedin, Google, Twitter ve Facebook gibi bilgi ve sosyal ağ hizmetleri sunan firmalar da dâhil olmak üzere tüm işletmelerin veri merkezi ihtiyaçları bulunmaktadır. Verilere hızlı, güvenilir ve sağlık bir şekilde ulaşarak müşterilere kesintisiz hizmet verilmesi her işletme açısından öncelikli amaçtır. Verilere, yavaş ve güvenilir olmayan bir erişim, hayati önem taşıyan bazı süreçlerin durmasına sebebiyet verebilir. Bu durumda, yasal cezaların oluşması, müşteri memnuniyetinin düşmesi ve gelir kaybının yaşanması durumu ortaya çıkabilir (Telkoder Serbest Telokomünikasyon İşletmecileri Derneği, 2015, s. 11). En küçük işletmelerde bile kullanılan bir internet tanıtım sayfası firma için çok kritik bir işleve sahip olabilir. Olağanüstü durum merkezi kurulmasının faydaları genel olarak aşağıdaki başlıklarda ele alınmaktadır.

- IT sistemlerinin yedeklenmesi,
- Olası bir felâket sırasında ana veri merkezinin hizmet verememesi durumda hizmet sürekliliğinin sağlanacağı bir yapının bulunması,
- Tüm paydaşlara (müşteri, çalışan, tedarikçi, ortaklar, yasal otorite vb.) güven verilmesi.

Olağanüstü durum merkezi kurulmasına yönelik zorluklar IT yatırımının çok pahalı olması, 7/24 çalışan sistemlerin operasyon işlemlerinin zorluğu, veri merkezinin taşınma zorluğu, lisansların pahalı olması, sürüm yükseltme sorunları, veri depolama sürecinde oluşabilecek sorunlar, telekom bağlantılı bant genişliği (bakır ve fiber karışımı) yeterli olmaması, bakım maliyetlerinin yüksekliği, bu konuda yeterli düzeyde yetkin tedarikçi olmaması vb. başlıklarda ele alınabilir (Öztürk, 2013, s. 65-66).

Olağanüstü durum merkezi seçimi; olağanüstü durum merkezi konumlandırılmasında ne tür yetkinlikte bir ihtiyaç olduğu belirlenmelidir. İşletmenin ihtiyaçları, yasal gereksinimler ve diğer başlıklara göre değerlendirme yapılır. Yasal otoriteler tarafından düzenleme yapılan sektörlerde tam donanımlı bir olağanüstü durum merkezi yapılanması bulundurulması istenmektedir. Firmanın büyüklüğüne, iş sürekliliği riskleri konusundaki farkındalığına göre yapılacak yatırımlar ve alınacak kararlar farklılık gösterecektir.

Yedek sunucu kiralama bu alandaki en kolay ve basit yöntem olarak öne çıkmaktadır. Genel olarak çok küçük şirketlere hitap etmekte olup günümüzde bulut teknolojisi ile birlikte yaygın kullanılmaya başlayan bir yöntemdir. Olağanüstü durum merkezi kurulum ve işletim maliyetleri çok yüksek olduğundan dolayı genellikle bu hizmeti veren firmalardan kiralama yapılır.

Kiralama yapılan firmaların bu konuda bilinen ve sektörde kabul görmüş olmaları olası felaketlerde hızlı ve etkin bir hizmet alınabilmesine dikkat edilmesi gereken hususların başında gelir. Tam donanımlı olağanüstü durum merkezi oluşturma yöntemi ise hem kurulum hem de sonraki işletme maliyetleri açısından firmalar açısından çok tercih edilmeyebilir. Olağanüstü durum merkezi yapılanması seçiminde yer alan dört farklı yapılanma hakkında aşağıdaki tabloda bilgiler sunulmaktadır.

Olağanüstü durum merkezi kurulumuna karar oluştuktan sonra nereye kurulması gerektiğine karar verilir. Ana veri merkezi ile aynı riskleri içermeyecek bir lokasyonda konumlandırma yapılır. Genel olarak sistemsel altyapı, coğrafi riskler, kalifiye işgücü vb. başlıklara göre değerlendirme yapılır.

Tablo 4: Olağanüstü Durum Merkezi Türleri ve Fayda Maliyet Analizi

	Olası Durumlar	Artılar	Eksiler
Yedek Sunucu Kiralama	Merkezi Tüm Operasyonu Aksatmayacak, Sadece IT Sistemlerine Geçici Zarar Verecek Felaketler için Çözüm Sunar	Maliyeti Düşüktür	Veri Yedeklemesi ile Sınırlıdır
		Yeni Bir Merkez İnşaatı Gerektirmez	Felaket Durumunda Personele Yedek Bir Çalışma Ortamı Sunmaz
		IT Sistemleri Operasyon Riskine Karşı İyi Bir Çözümdür	Sunucunun Büyük Çapta Bir Felaket Durumunda Yüksek Kalitede Hizmet Vermesi Garanti Değildir
Olağanüstü Durum Merkezi Kiralama	Tüm Operasyonu Aksatmayacak, Sadece IT Sistemlerine Geçici Zarar Verecek Felaketler için Çözüm Sunar	Maliyeti Düşüktür	Veri Yedeklemesi ile Sınırlıdır
		Yeni Bir Merkez İnşaatı Gerektirmez	Felaket Durumunda Sınırlı Sayıda Personele Yedek Bir Çalışma Ortamı Sunar
		IT Sistemleri Operasyon Riskine Karşı İyi Bir Çözümdür	Sunucunun Büyük Çapta Bir Felaket Durumunda Yüksek Kalitede Hizmet Vermesi Garanti Değildir
			Şubelerde Aynı Depremden Etkilenirse Yedek Çalışma Ortamı İmkânı Olmayabilir
Tam Donanımlı Olağanüstü Durum Merkezi Oluşturma	Çok Sayıda Müşterisi ve Çalışanı Bulunan, 24 Saat Operasyonun Devamlılığını Gerektiren Büyük Kurumlar Tarafından Tercih Edilir	Büyük Bir Felakette Faaliyetlerinin Devamını Sağlar	Maliyeti Yüksektir
		Sunucu Kiralamadan Kaynaklı Operasyonel Riskleri İçermez	Felaket Merkezinden Sorumlu Ek Personel, Gerektirir
		Personel Yedek Lokasyondan Çalışmaya Devam Edebilir.	Ulaşım Sorunu
Çift Olağanüstü Durum Merkezi Oluşturulması	Çok Sayıda Müşterisi ve Çalışanı Bulunan, 24 Saat Operasyonun Devamlılığını Gerektiren Büyük Kurumlar Tarafından Tercih Edilir	Bir Felakette Faaliyetlerinin Devamını Sağlar	Maliyeti En Yüksektir.
		Lokasyona Erişimin Olmadığı Durumlarda Çalışanların Yakın Olağanüstü Durum Merkezi Gönderilebilir.	Felaket Merkezinden Sorumlu Ek Personel, Bazı Durumlarda Departman Gerektirir
		Çalışanlar Olağanüstü Durum Merkezine Sevk Edilebilir.	

Kaynak: TÜBİTAK–BİLGEM, https://www.bilgiguvenligi.gov.tr/kurumsal–guvenlik/olaganustu–durum–merkezi–karar–verme–ve–lokasyon–firma–secim–kriterleri.html, 2013

Tablo 5: Olağanüstü Durum Merkezi Seçim Kriterleri

Altyapı	Sağlam ve Yeterli Kapasitede Geniş Banda Sahip Dayanıklı Bir Telekomünikasyon Altyapısı Gereklidir
	Elektrik, Doğalgaz, vb. Hizmetler Ucuz ve Kaliteli, Kesintisiz Olarak Sağlanabiliyor Olmalıdır
Risk	Deprem, Sel, Fırtına Gibi Doğal Afet Riski Düşük Olmalıdır
	Olası Hedeflerden Uzak Güvenli Bir Bölge Seçilmelidir
Demografik Faktörler ve Kalifiye İş Gücü	Çalışabilir Nüfusun Yeterli Olduğu Bir Bölge Seçilmelidir
	Nüfusa Paralel Olarak Bölge De Yeterince Gelişmiş Olmalıdır
	Afet Durumunda Karşılaşılabilecek Ana Merkezdeki İş Gücü Kaybında, Hızlı Bir Şekilde İşe Alınabilecek, Eğitim Düzeyi Yüksek Kalifiye İş Gücüne Sahip Bir Bölge Olmalıdır
Gelişmiş Olanaklar	Personelin İhtiyacını Karşılayacak Yeterli Sayıda Otel, Restoran, Alışveriş Merkezleri İçermelidir.
	Acil Durumda Personelin Hızlı Bir Şekilde Ulaşımını Sağlayacak Gelişmiş Olanaklar Bulunmalıdır
Emlak ve Kira Fiyatları	Sadece Olağanüstü Durumlarda Kullanılacak Bir Olağanüstü Durum Merkezinin Kirası Veya Emlak Değeri Düşük Tercih Edilmelidir

Kaynak: Marsh Danışmanlık, İş Sürekliliği Eğitim Notları, 2010, s. 47.

Olağanüstü durum merkezi kurulumu; olağanüstü durum merkezi kurulum ve tasarımında ana veri merkezi ile aynı riskleri taşımaması, veri ve iletişim network hat yapısı, elektrik tesisat yapısı, soğutma sistemleri alt yapısı, donanımlar, güvenlik yönetimi, çalışma alanı konularında değerlendirme yapılır.

Veri merkezi türleri; veri merkezlerinin iletişim altyapısı ve sunucu odaları için asgari gereksinimleri uluslararası standartlar ile belirlemiştir. Veri merkezi konusunda uluslararası boyutta üç farklı kuruluş tarafından standartlar belirlenmekte ve sertifikasyon süreci gerçekleştirilmektedir. Bu standartlardan en yaygın olan TIA kuruluşu tarafından belirlenen standartlardır. Standartta veri merkezleri için dört farklı sınıflandırma belirlenmiş olup detay bilgiye aşağıda yer verilmiştir.

"Tier 1 Seviyesi: Küçük işletmelere hizmet veren veri merkezleridir. Bilgisayar sistemleri, elektrik, mekanik tesisat yedeksizdir. Genel olarak 10 dakikadan daha

fazla bir enerji kesintisine bir önlemi yoktur. Tahmini % 99,676 kullanılabilirlik sunmaktadır.

Tier 2 Seviyesi: Enerji ve soğutma sistemlerinde kısmen yedeklik içerir. Jeneratör kullanarak 24 saatlik bir enerji kesintisine dayanabilmektedir. Tahmini % 99,741 kullanılabilirlik sunmaktadır.

Tier 3 Seviyesi: Yedek elektrik şebekesi içerir. Yedek enerji ve soğutma sistemleri içerir. Yedek hizmet sağlayıcıları içerir. 72 saatlik bir kesintiye karşı dayanabilir. Tahmini % 99,982 kullanılabilirlik sunmaktadır.

Tier 4 seviyesi: Bütün Tier 3 kriterleri sağlanır. Ek olarak 96 saatlik kesintiye dayanabilir. 7/24 çalışan bir personel ekibi mevcuttur. Yer seçiminde çok sıkı davranılır, yüksek güvenlik önlemleri alınmıştır (Telecommunications Industry Association , 2014, s. 12)

2.5.3.5. Olağanüstü Durum Merkezi Sistem Altyapı Teknolojileri

Sistem altyapı çalışmaları, fiziksel altyapı ve IT sistem altyapısı olarak iki başlıkta ele alınır.

Fiziksel altyapı; olağanüstü durum merkezinin fiziksel altyapısı olağanüstü durumlarda ilgili lokasyonun hem IT bileşenleri hem de personelin çalışması için kullanışlı olacak bir şekilde tasarlanmalıdır. Fiziksel altyapı konusunda dikkat edilmesi gereken bazı özellikler aşağıda listelenmiştir.

- *''Yükseltilmiş Taban: Su baskını ve sel felâketine karşı donanım ve tesisatı korumak için yükseltilmiş tabana sahip olması tercih edilmelidir.*
- *Klima: Sistem odalarını uygun ve sabit sıcaklıkta tutacak klimalar yer almalıdır.*
- *Yangın Ekipmanı: Yangın riskine karşı koruyacak donanımlar bulundurulmalıdır.*
- *Kamera Sistemi (CCTV): Gerek ana merkezden gerekse yedek veri yönetim merkezinden sunucuları sürekli olarak izleyebilecek görüntü izleme altyapısı kurulmalıdır.*
- *Kartlı Erişim Sistemi: Olağanüstü durum merkezine ve sunucu odalarına sadece yetkili personelin girişine izin verecek biyometrik veya kartlı erişim sistemi kurulmalıdır.*

- *Kesintisiz Güç Kaynakları ve Jeneratörler: Veri merkezinde bulunan tüm sunucular ile diğer donanımların olası bir elektrik kesintisine karşı sürekliliği sağlayacak kapasitede kesintisiz güç kaynakları ve jeneratörler kurulmalıdır.*
- *İletişim Ağı: Güvenilir ve yeterli bant genişliğinde iletişim altyapısı kurulmalıdır. Ucuz ve esnek olması nedeniyle, güvenlik önlemleri alınmış kablosuz iletişim ortamı etkin bir çözüm sağlayabilmektedir* (Karabük Üniversitesi Bilgi İşlem Daire Başkanlığı, 2015, s. 3)*''.*

IT sistemsel altyapı; olağanüstü durum merkezinin bilgi teknolojileri altyapısı olağanüstü durumlarda ilgili lokasyonun hem IT bileşenleri hem de personelin çalışması için kullanışlı olacak bir şekilde tasarlanır.

> *"Olağan üstü durumdan kurtarma ve depolama politikalarının ve planlarının gerçekleşmesi için çeşitli sistemsel altyapılara ihtiyaç duyulmaktadır. Veri merkezi mimarisi; uygulama sunucuları, erişim sunucuları, müşterilerin sunucuları, depolama birimleri, yönlendiriciler, güvenlik sistemleri ve yönetim araçlarını kapsar. Bunlara ek olarak, sistemlerin sürekli ve güvenli çalışmasına destek olan enerji birimleri (güç kaynağı bağlantı ve dağıtım elemanları, kesintisiz güç kaynağı, jeneratör), klima, yangın uyarı ve söndürme sistemleri, güvenli giriş sistemleri, telekomünikasyon ağına bağlantı birimleri gibi altyapı elemanları da internet veri merkezini oluşturan temel unsurlardır* (Teknik Altyapı ve Bilgi Güvenliği Çalışma Grubu, 2005, s. 9)*''.*

Aktif–pasif sistemi; ana veri merkezinin aktif, felâket durumu haricindeki zaman dilimlerinde ise pasif olduğu tasarımdır. Herhangi bir felaket meydana geldiğinde yedek veri merkezi aktif hale geçer ve sistemler bu şekilde çalışmaya devam eder.

Aktif–yarı aktif; ana veri merkezi aktif olarak çalışırken, verilerin belirli periyotlarla yedeklendiği veri merkezi üzerinden, anlık veri değişikliklerin çok önemli olmadığı raporlar alınabildiği veya test ortamı olarak kullanılabildiği tasarımdır. Genel itibariyle bu şekilde bir tasarım mimarisi ülkemizde tercih edilmemektedir.

Aktif–aktif sistemi; ana veri merkezi ve yedek veri merkezinin gelen istekleri yoğunluğa göre karşıladığı ve her iki veri merkezinde de anlık olarak verilerin eşit olduğu mimaridir. Bu tasarımda felâket anında devreye girecek bir olağanüstü durum merkezi yerine eşit ağırlıklı iki sistem merkezine sahip olunur. Her iki veri merkezi de bir birinin yedeği konumda yer alır. Veri merkezlerden herhangi bir tanesi hizmet veremez duruma

gelmesi durumunda bile son kullanıcılar bu kesintiden etkilenmez ve hizmet kesintiye uğramadan diğer veri merkezinden verilmeye devam eder. Ancak her iki veri merkezini de etkileyebilecek bir felaket durumunda işletme hizmet veremez duruma gelir. Bu sebepten bu tür yapılanmalarda iki veri merkezinin de aynı riskleri içeren coğrafi konumlarda olmaması önem arz etmektedir. Bu mimaride cihaz arızası gibi küçük hatalarda bile sistem kısa da olsa kesintiye uğramaz. Maliyeti en yüksek olan tasarımdır (Türkiye Bilişim Derneği, 2012, s. 63-64). Bu tasarım yöntemlerine göre gerekli donanım ve bağlantı teknolojisi belirlenir. İş kurtarma planında kullanılan farklı teknolojiler vardır. Bu planlama, işletmenin var olan teknik altyapısına göre değişir. Kullanılan sunucu işletim sistemleri, uygulamalara göre farklı çözümler kullanabilir. Aşağıda aktif–aktif mimari yapısı işleyişi gösterilmiştir

Olağanüstü durum merkezi teknoloji altyapılarında temel olarak kullanılan sanallaştırma, kümeleme, yedekleme vb. bazı teknolojiler hakkında detay bilgiler aşağıda verilmiştir.

Sanallaştırma; işletim sistemleri, depolama aygıtları ya da ağ kaynaklarından herhangi birinin aslını kurmak yerine ilgili teknolojiyi sanal olarak kurmaktır. Sunucuların donanım–bağımsız olmasını sağlanır. Mevcut bulunan fiziksel donanımın sanal makineler yardımıyla çok daha verimli kullanılabilmesini sağlayan, çeşitli yazılım ve donanım bağımlılıklarını ortadan kaldıran, bu sayede de yeni ürün ve servis geliştirme maliyetlerinde büyük tasarruflar sağlayan bir yazılım çözümüdür. Sanallaştırma; işletim sistemleri, depolama aygıtları ya da ağ kaynaklarından herhangi birinin aslını kurmak yerine onları sanal olarak kurmaktır. Özellikle 2005 yılında bu teknoloji ilgili kullanıcıları tarafından çok hızlı kabullenilerek sektördeki yerini almıştır. Uygulamalar ve bunların altında bulunan donanım bileşenlerini destekleyen ve bu kaynakların uzak veya sanal bir görünüm sunmak için tercih edilen mantıksal bir yoldur (Kusnetzky, 2011, s. 3). Sanallaştırmanın genel amacı ise ölçülebilir iş yükünü geliştirirken yönetimsel görevleri merkezi bir yapıya getirilmesidir. Sanallaştırma ile özellikle fiziksel makinelerdeki operasyon (iş gücü, elektrik ve soğutma giderleri vb.) ve bakım maliyetleri daha düşük seviyelere çekilir. Ayrıca hem yazılım hem de donanım testlerini daha hızlı yapılması ve sonuçlarında eskiye nazaran daha verimli olması bu teknolojinin sağlayacağı artılar arasında yer almaktadır. Ağ sanallaştırılması, yedekleme sanallaştırılması ve sunucu

sanallaştırılması en yaygın olarak gerçekleştirilen sanallaştırma süreçleridir. Bu alanda Hyper–V, VMware öne çıkan teknolojilerdir.

Kümeleme çözümleri; bir sistemin aynı yapıdaki bir benzerinin de farklı bir sistemde çalışmasını sağlayan sistemler bütünüdür. Kümeleme işleminin üç temel amacı vardır. Bunlar süreklilik, yük dengeleme ve yüksek düzeyde performans sağlanmasıdır.

Storage replikasyon; depolama üniteleri arasında verilerin birebir kopyalanmasını sağlayan çözümlerdir. İki veya daha fazla veri merkezi arasındaki otomatik kopyalama işlemi olaraktan ifade edilmektedir. Veri merkezi ile yedek veri merkezi arasında asenkron replikasyon veya senkron replikasyon yapılabilir (Pulton, 2014, s. 4). Ana veri merkezinde yer alan ve iş sürekliliği kapsamında kritik süreç veya veri olarak belirlenen kaynakların belirli zaman dilimlerine göre olağanüstü durum merkezindeki sunuculara replike edilmesi olayının tamamıdır. Bu teknolojide yapılan işlem verilerin diğer veri merkezindeki sunucu ve veritabanı üzerine kopyalanmasıdır.

Yedekleme çözümleri; verilerin bir yedeğinin saklanıp gerektiğinde tekrardan alınmasını sağlayan çözümleri içermektedir. İşletmelerde belirli periyotlarla veriler yedeklenir ve olası bir durumda veri kaybı yaşanırsa öncelikli olarak son alınan yedek verilere dönüş yapılır. İşletme faaliyetleri bu yedek veri üzerinden devam ettirilir. Yedekleme işlemleri işletmenin tabi olduğu sektör düzenleyici kurum tarafından belirlenen zaman periyotlarına göre yapılır. Saat, gün, hafta, ay ve yıl bazlı olarak yedekleme faaliyetleri gerçekleştirilebilir. Yedeklerin saklanması ve belirli bir zaman diliminden sonra imha edilmesi de belirli standartlar çerçevesine göre yapılır. Özellikle imha işleminde verinin tekrar geri döndürülemeyecek şekilde imha edilmesi bilgi güvenliği açısından elzemdir.

Bağlantı çözümleri; verilerin olağanüstü durum merkezine sağlıklı bir şekilde aktarılabilmesi için uzak lokasyon bağlantı teknolojileri kullanılır. Bunun için olağanüstü durum merkezinin yerine göre fiber, noktadan–noktaya metro ethernet, noktadan–noktaya G.SHDLS, VPN ve GSM üzerinden APN vb. teknolojiler kullanılabilir. Burada kullanılacak teknoloji verinin büyüklüğü, yedeklenme sıklığına göre değişiklik gösterecektir. Özellikle telekom altyapı kalitesinin yüksek olduğu bölge ya da teknolojiler tercih edilmesi operasyon ve güvenlik açısından getiri sağlayacaktır.

RAID teknolojisi; veri saklama ortamlarından kaynaklanabilecek hatalar ve dolayısıyla felâket durumlarının en aza indirilmesine yönelik bir artık veri saklama ve erişim teknolojidir. Bu teknolojide birden fazla fiziksel diski birleştirilir, daha sonra bir gruba dönüştürülür ve bu grubunda bir ya da daha fazla mantıksal disk olarak tanımlanmasına olanak veren bir teknolojidir (Örencik, 2007, s. 5). Bu teknolojide diskler eş zamanlı çalıştırılarak; daha yüksek performans, dayanıklılık, güvenilirlik ve daha büyük veri depolama alanları elde edilir.

Veri ve iletişim network hat yapısı; bir veri merkezinin altyapı mimarisi tasarlanırken veri ve iletişim ağının tasarımı en önemli bölümlerden birini oluşturur. Ağ yapısının etkin ve verimli bir şekilde tasarlanması sunulacak hizmetlerin hızlı ve kesintisiz bir şekilde gerçekleşmesine olanak sağlayacaktır. Veri merkezi veri ve iletişim hat yapısında aşağıdaki maddelerin kontrolü yapılarak tasarlanmalıdır.

- İletişim altyapısının alternatifli olup olmadığı (Alternatiften kasıt, Telekom operatörünün farklı santral, güzergâh, NODE, cihaz da sonlanıyor olması vb.),
- Metro ethernet, DWDM, dark fiber imkânı, Radyo–Link, FSO–Free Space Optic, SDH, chanelized E1, PRI, ATM vb. şebeke tiplerinin varlığı, vb. teknolojik alt yapı hizmetleri,
- Network hat kapasitesi (gigabit metro, TDM, PCM, LL, XDSL vb. şebeke tiplerinin ve hızlarının varlığı),
- Alternatif Telekom telekom operatörlerinin fiber tesis edebilmesine olanak tanınması, farklı telekom omurgalarından erişim imkânının sağlanabilirliği,
- Data hatlarında noktadan noktaya kriptolama,
- Dinamik routing protokolleri ile Network seviyesinde lokasyonların olağanüstü durum merkezine ye otomatik yönlenme kabiliyeti,
- Üçüncü kişi kurumlarla veya kamu kurumları ile iletişim/şebeke uyumluluğu,
- Olağanüstü durum merkezine internetten SSL VPN/Client–to–Site VPN vb. yöntemlerle erişim,
- Olağanüstü durum merkezinde (Olağanüstü durum merkezinde olağanüstü durum sırasında çalışacak yeterli client alanı var ise) kablosuz erişim imkânı,

- Önerilen kablolama çözümleri, bakır sistemler için Cat6A, Cat6 ve Cat5e ile fiberoptik multimode OM3 veya 50 mikron/62.5 mikron ile single mode ürünlerdir. Veri merkezleri klasik ofis kablolama sistemlerine oranla kablolamanın çok yoğun olarak kullanılmasına ihtiyaç olan yerlerdir.

Olağanüstü durum merkezi test çalışmaları; planların geçerliliğini, işletme olağanüstü durum karşısındaki tepkilerini test etmek, işletme personelinin iş sürekliliği konusunda bilgisini, görevli personelin tecrübesini arttırmak amacıyla planlı ve programlı testler yapılır. Test ve tatbikatlarda en önemli aşama hedef konulması ve tatbikat sonucunda hedefin ne kadar gerçekleştirildiğinin tespit edilmesidir. Periyodik olarak yapılan bu testlerde hedefler sürekli iyileştirilir ve en ideal sonuca ulaşmak için güncellemeler yapılır. Test çalışmasında alternatif lokasyonda tüm kritik süreçler ve ilgili personelin katılımıyla yılda bir kez gerçekleştirilebilir veya daha az sayıda katılımcı ile daha az sayıda süreç testi ile yılın değişik zaman dilimlerinde sürekli olarak yapılabilir.

2.5.3.6. Sonuç Raporlarının Hazırlanması ve Sunumu

Bu aşamaya kadar elde edilen tüm bilgiler doğrultusunda iş sürekliliği planı hazırlanır ve gerekli onaylardan sonra işletme de uygulamaya konulmuş olur. Oluşturulan planların ISO 22301 iş sürekliliği standardına uygun olması hedeflenmelidir. Bu şekilde hazırlanan plan resmi bir sertifika alınması sürecinde işletmeye kolaylık sağlayacaktır.

İş sürekliliği planı ve ilişikte olduğu planlar aşağıdaki tabloda yer almaktadır. İnternet temelli ihlallere yönelik plan siber saldırılara yönelik detaylı çalışmaları içerirken, işe yeniden başlama planı ise olası bir felaket durumu sonrası olağanüstü durum merkezinde çalışmaların nasıl başlayacağına dair detayları içerir.

İş sürekliliği konusuyla ilgili olan diğer planların kapsamı ve amaçları hakkındaki genel bilgiler aşağıdaki tabloda yer almaktadır. Tabloda sekiz plan yer almaktadır. Bu planlar işletme veya kuruluşun seçimine göre tek tek oluşturularak kullanılabilir veya tamamını içerecek bilgilerin yer aldığı şekliyle tek bir plan kapsamında da ele alınabilir.

Tablo 6: İş Sürekliliği Planı ile İlişkili Plan Listesi

Plan Adı	Amacı	Kapsamı
İş Sürekliliği Planı	Temel İş Operasyonlarının Sürdürülmesi için Prosedürler	İş Süreçleri IT Esaslı İş Süreçleri
İşe Yeniden Başlama Planı	Felaketten Hemen Sonra Kurtarma Prosedürleri	İş Süreçleri IT Esaslı Süreçler
Süreklilik Operasyonları Planı	30 Güne Kadar İşlerin Sürdürülebilirliği için İş Gerekleri, Stratejik Fonksiyonlar için Prosedürler	IT Odaklı Değil Kurumsal Misyon için Kritik
Destek Sürekliliği/IT Sürekliliği Planı	Genel Destek Veya Majör Uygulamaları Kurtarmak için Prosedürler	IT Odaklı IT Sürekliliği Planı IT Sistem Kesintileri
Kriz İletişim Planı	Kullanıcılar ve Halk için İlgili Raporları Yayınlama ve Bilgilendirme Prosedürler	IT Odaklı Değil Personel ve Halk için İletişim Araçları
İnternet Temelli İhlallere Yönelik Plan	Kötü Niyetli Saldırılara Karşı Önlemler, Taramalar, Limit Sınırlamaları.	Bilgi Güvenliği Esaslı Sistemlere Veya Ağlara Yönelik İhlallerin Etkileri
Felaket Kurtarma Planı	Alternatif Sistemler, İmkânlar, Varlıklar için Ayrıntılı Kapasite ve Prosedürler	IT Bazlı Büyük Kesintiler Uzun Süreli Etkiler
Acil Durum Planı	Fiziksel Tehditler için Minimum Kayıplar, Hasarlar için Koordinasyon Prosedürleri	Personel Odaklı IT Esaslı Özel Durumlar

Kaynak: Türkiye Bilişim Derneği (2012), İş Sürekliliği Yönetimi Çalışma Grubu Raporu, s. 85

2.6. Eğitim ve Test Çalışmaları

İş sürekliliği yönetim sisteminin hayata geçirilmesindeki en önemli aşama eğitim ve test çalışmalarıdır. Eğitim ve test süreci birbiriyle iç içe bir yapıdadır. İş sürekliliği konusunda işletme veya kuruluşta sorumluluğu olan tüm personele bilinçlendirme ve farkındalık eğitimleri verilmesi sistemin hayata geçirilmesi için ilk aşamalardan biridir. Görevli personel, iş sürekliliğinin ne olduğu, ne tür faaliyetleri kapsadığını, işletme için ne ifade ettiği konularında genel kapsamda bilgi sahibi olması gerekir. İşletmedeki diğer personeller için de bilinçlendirme eğitimleri yapılması olası bir felaket veya sistemsel kesintinin en az hasarla atlatılması ve müşteri memnuniyetsizliğinin azaltılması açısından gereklidir.

Oluşturulan tüm sistemin test edilmesi varsa eksiklerinin giderilmesi önemli bir gereksinimdir. Test ve tatbikat işlemleri öngörülen birçok riske karşı hazırlık seviyesinin ölçülmeye çalışıldığı faaliyetleri kapsamaktadır. Bu yüzden iş sürekliliği testleri yapılaması zor olan testler arasında yer alır. Kapsamda belirlenen senaryolar üzerinden test yapılması olası acil durumlara hazırlık için önem arz eder.

Test çalışması planlaması testin başarılı olması açısından gereklidir. Testin hangi içerikte yapılacağı, hangi iş süreç/hizmetlerinin ve teknolojik sistemlerin test edileceği belirlenmesi kapsamlı bir planlama aşamasında belirlenir. Test öncesinde titiz bir hazırlık ve planlama yapılmaması durumunda test sırasında öngörülmeyen ciddi kesintilerin yaşanması söz konusudur. Bu nedenle iş sürekliliği testleri için bir model oluşturulmalıdır. İş sürekliliği testleri her yıl en az bir kere yapılır. İş sürekliliği test planında hangi aşamalardan oluştuğu belirlenmelidir.

İş sürekliliği yönetim sistemindeki eksikleri tespit edebilmenin en etkili yolu ilgili planın testinin yapılmasıdır. İş sürekliliği testlerinin amaçları arasında işletme veya kuruluşun iş sürekliliği konusundaki kapasitesini ölçümlemek ve değerlendirmek, planın eksik kalan bölümlerini ve bilgilerini tespit etmek, geliştirilmesi gereken yönleri belirlemek, IT sistem altyapısının performansını ve kapasiteye yeterliliğini gözlemlemek, acil durum takımları, iş kurtarma takımları ve diğer sorumlu personelin çalışma performansını gözlemlemek ve iyileştirmek, iş sürekliliği bilincini artırmak, plan içerisinde yer alan tüm süreç ve faaliyetlerinin etkinliğini ölçmek, önceden hedef olarak belirlenen kurtarma hedeflerinin gerçekçiliğini kontrol etmek, tedarikçi firma, yasal otorite ve diğer iletişim kurulması gereken kurumlarla iletişim noktasındaki yetkinliğin ölçümlemek, kamuoyuna güven vermek yer almaktadır (Dinçkan, İş Sürekliliği Tatbikatları İçin Örnek Bir Model, 2016, s. 4).

İş sürekliliği yönetim sistemi kapsamındaki çalışmalarının tamamını tek seferde test edebilmek oldukça zordur. Planın her yönden kontrolü için düzenli periyotlarda ve planın farklı bölümlerini test eden bir takvim hazırlanmalıdır. İş sürekliliğinde acil eylem yönetimi aşaması için farklı bir test yöntemi, kriz yönetim aşaması için farklı ve iş kurtarma aşaması içinde farklı bir test yöntemi uygulanır. Acil eylem testleri çoğunlukla bina tahliye, yangın, sel vb. senaryo durumlarını içerir. Bu teste tüm personel katılımı gerekir. Kriz yönetim aşamasındaki test ise çoğunlukla kriz yönetim takımı üyeleri ile

gerçekleştirilir. Bu testte genel olarak benzetim yöntemi ile firmanın maruz kalabileceği bir kriz durumu ele alınarak rol ve sorumluluklara göre çözüm sağlanır. İş kurtarma aşamasına yönelik test çalışması ise en geniş kapsamlı ele alınan testlerdir. İş etki analizi kapsamında belirlenen kritik süreçler ve bu süreçleri destekleyen IT sistemleri, tedarikçi, personel vb. kaynakların test edilmesi sürecini kapsamaktadır.

Tablo 7: Tatbikat Türleri

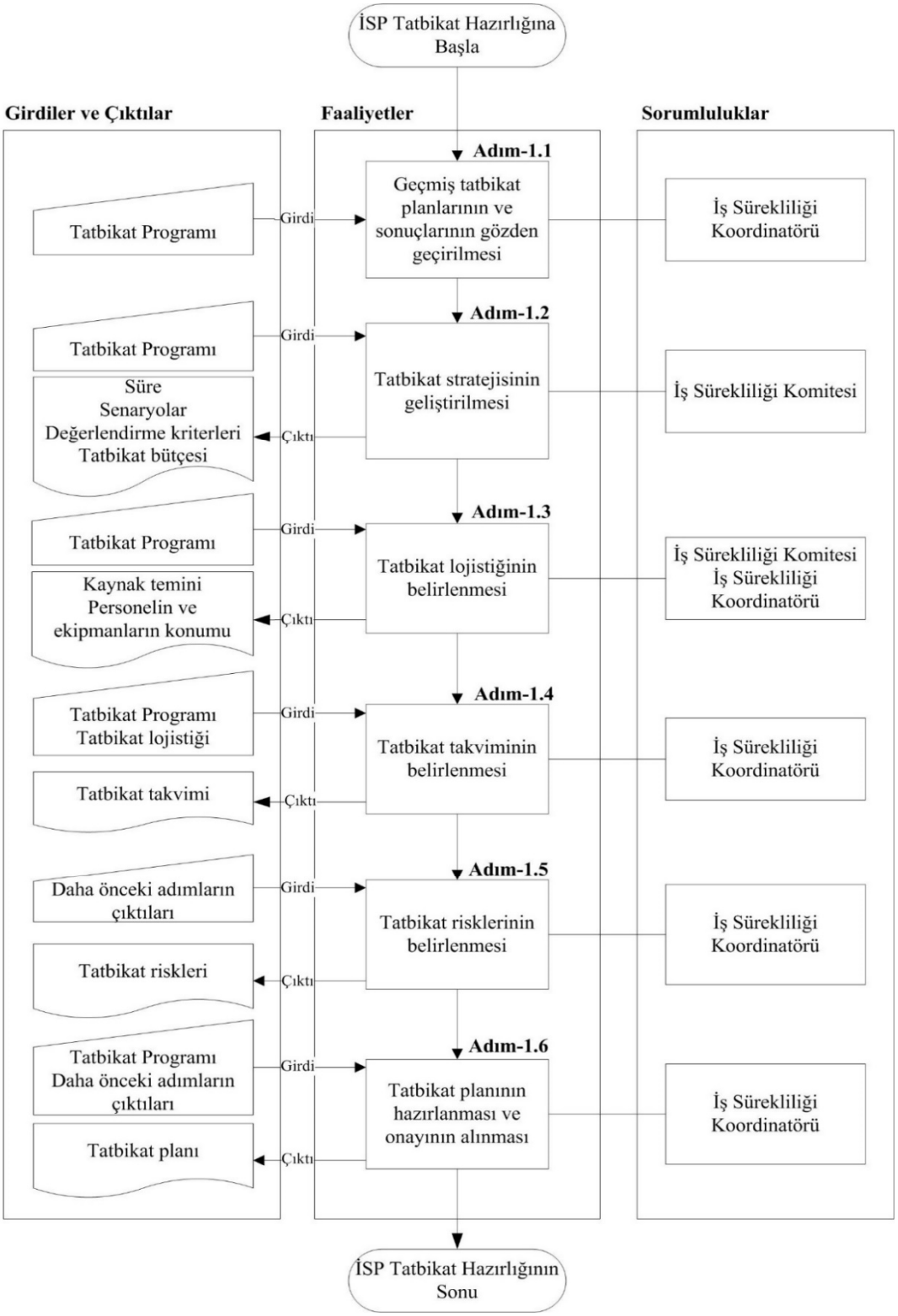
Tatbikat Türü	Tanım
Kavramsal Tatbikat	İş Sürekliliği Planı ve İlgili Dokümantasyonun Gözden Geçirilmesidir.
Detaylı Kavramsal Tatbikat	Kavramsal tatbikatın daha detaylı olarak yerine getirilmesidir. Bu tatbikat türünde planda yer alan her adımın üzerinden geçilerek eksiklikler tespit edilmeye çalışılır.
Simülasyon	Bu tatbikat türünde örnek bir olay üzerinden iş sürekliliği planı çalıştırılır. Tatbikat sırasında süreç veya sistemlerde herhangi bir kesinti gerçekleştirilmez. İş sürekliliği planı kesinti gerçekleşmiş gibi düşünülerek çalıştırılarak tatbikatı yapılır.
Bileşen Veya Servis Tatbikatı	İş süreçlerinin bir kısmı için gerçekleştirilir. İş süreçlerinde kesintiye neden olabilecek bir olay gerçekleştirilir ve süreç tekrar çalışır hale getirilir. Bu tatbikat çalışan bir sistem üzerinde gerçekleştirildiğinden, kurumun acil durum tatbikatı kapsamında olmayan operasyonunu aksatmayacak biçimde planlanması gereklidir.
Tam Tatbikat	İş sürekliliği planının tamamının test edilmesidir. Tam tatbikat kurum süreçlerinin felaketten kurtarma merkezinde tekrar çalıştırılmasını da kapsayan detaylı bir tatbikattır.

Kaynak: http://www.btyon.com.tr/is_surekliligi_tatbikat.pdf sayfasından alınmıştır. 2016

Test çeşitleri maliyet, zaman, karmaşıklık ve iş süreçlerinde oluşabilecek kesintiler açısından ayrı özelliklere sahiptir. Kavramsal test, detaylı kavramsal tatbikat, simülasyon test, bileşen veya servis tatbikatı, tam tatbikat olmak üzere beş farklı kategoride test türü bulunur. Kavramsal test en basit test türüdür. Testin karmaşıklık düzeyi, maliyeti ve zaman değeri kavramsal testten tam teste doğru ilerledikçe artmaktadır. İşletmeye uygun olabilecek test türü ve sıklığı belirlenerek test programı hazırlanır. Test programında kullanılabilecek tatbikat türleri aşağıdaki tabloda gösterilmiştir.

2.6.1. İş Sürekliliği Test Çalışması İş Akışı

İş sürekliliği test hazırlık çalışmaları strateji oluşturulması ile başlar. Test stratejisine göre nelerin amaçlandığını net olarak ortaya konulur. Test çalışması ilk kez yapılıyorsa stratejik hedeflerin belirlenmesi zor olabilir. Süregelen test çalışmaları yapılmakta ise stratejik hedefler konusunda daha başarılı sonuçlar ortaya konabilir. Strateji belirlendikten sonra önceki dönemlerde yapılan test çalışmaları, yaşanan sorunlar, mevcut kısıtlamalar ve diğer öne çıkan başlıklar incelenir. Bu inceleme sonucunda planlama çalışmaları stratejik hedefler doğrultusunda başlatılır. Tatbikatın zamanı, yeri, kapsamı, katılımcıları, bilgilendirme yapılacak kurumlar vb. başlıklar planlama aşamasında ortaya konması gereken önemli ayrıntılardır. Planlama çalışmalarında özellikle testin başarısını ölçümlemek için mümkünse sayısal hedefler belirlenmelidir. Test sonuçlarını değerlendirirken sayısal olarak hedefe ne kadar yaklaşıldığı bu şekilde tespit edilecektir. Test çalışmasının bütçesi, bütçeye uygun kaynak ve donanımların sağlanması, lojistik gereksinimlerinin belirlenmesi test ile alakalı olası risklerin ortaya konması planlama aşamasında ele alınacak diğer konular arasında yer almaktadır. Test kapsamı planlanırken işletmenin ihtiyaç duyduğu kapsamda bir seçim yapılması testin başarısı, işletmeye katkısı ve olası riskleri en aza indirgemesi açısından önem arz etmektedir. Gereğinden büyük kapsamda yapılan test çalışmaları çoğu zaman işletme ve kuruluşlara katkı sağlamak yerine sorun oluşturabilmektedir. Aşağıdaki iş akışında bankacılık sektöründe iş kurtarma testi veya olağanüstü durum merkezi testi olarak adlandırılan sürecin örnek bir akışı gösterilmiştir. Başarılı bir test çalışması faaliyeti için iş akışına uygun şekilde hazırlık yapılması gerekir.



Şekil 4: Test ve Tatbikat Süreç İş Akışı

Kaynak: http://www.1stbasis. com/rto–rpo–for–business–continuity–disaster–recovery/, 2015.

BÖLÜM III

3. Bankacılık Sektörü Model Vaka Analizi

3.1. Örnek Uygulamanın Amacı ve Önemi

Bir yanda tüm hızıyla gelişen bankacılık, iletişim ve altyapı imkânları ile hayallerimizin sınırlarını zorlarken, diğer yanda onları her an yerle bir edecek doğal afetler yangın, terör, siber saldırı, altyapı ve insan kaynaklı sorunlar çevremizi kuşatmış durumdadır. Dünya'da ve Türkiye'de sürekli gelişmekte olan bankacılık sektöründe iş sürekliliği daha büyük önem kazanmaktadır. Olası bir kesintide bankalar büyük miktarda finansal kayıp, itibar ve müşteri kaybı ve doğal olarak pazar kaybı yaşamak durumunda kalmaktadır.

Başta hazine işlemleri olmak üzere birçok alanda saniyelerin dakikaların bile çok önemli hale geldiği günümüz bankacılık sektöründe en az kesinti ile iş sürekliliği hedeflenmektedir. Bankacılık sektörü için önerilen model bu alanda uzman bir ekip tarafından kurulumu yapılan ve sonrasında bir bankada uygulanan iş sürekliliği sistemini içermektedir. Bu sistemin eksik yönleri belirlenerek etkin ve verimli bir model oluşturulmaya çalışılmıştır. Önerilen modelde bankacılık sektöründe iş sürekliliği çalışmaları nasıl yapılır, elde edilen sonuçlar nasıl değerlendirilir ve olağanüstü durum merkezinde konumlandırılması nasıl yapılabilir konularına yönelik çalışmalar yer almaktadır.

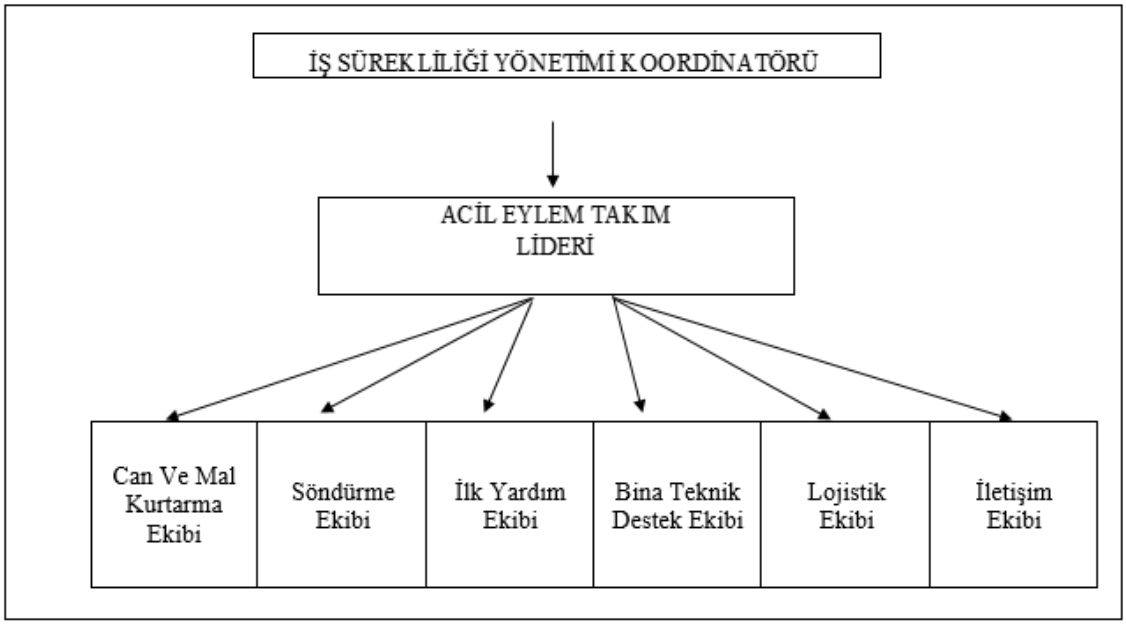
3.2. Örnek Uygulama ve Model Önerisi

Bankacılık sektöründe iş sürekliliği sistemi en yoğun kullanıldığı alanlardan biridir. Bu sektörde iş/hizmet kesintisi bankaya finansal, yasal ve itibari etki açısından yüksek düzeyde sorun oluşturur. Bu yüzden her etkin, verimli ve sürekli güncellenebilecek bir yapıda iş sürekliliği sisteminin kurulması gerekir. Bankacılık sektörüne yönelik yapılan çalışmanın aşamaları aşağıda detaylı olarak anlatılmıştır. Acil eylem yönetimi, kriz yönetimi ve iş kurtarma olmak üzere ana hatları ile üç fazda ele alınmalıdır. Banka bünyesine uygun bir organizasyon yapısı oluşturulmalıdır. Kriz yönetim takımı, acil eylem takımı, iş kurtarma takımı, iş sürekliliği koordinatörü IT

sorumlusu, güvenlik, haberleşme, muhasebe, hukuk, kurumsal iletişim vb. fonksiyonların içinde yer aldığı bir organizasyon yapısı oluşturulur.

3.2.1. Acil Eylem Yönetimi

Bu aşamada bir taraftan risk analiz değerlendirilmesi yapılırken diğer yandan acil durum organizasyonu ve müdahale ekipleri oluşturulur. Bu ekiplere yönelik rol ve sorumluluklarda belirlenir. Bu ekiplerin hem olaydan haberdar olmaları hem de kendi aralarında sağlıklı iletişim kurabilmesi adına iletişim sistemi önem arz etmektedir. Aşağıda örnek bir organizasyon yapısı ve kurulması gereken acil durum ekipleri yer almaktadır.



Şekil 5: Acil Durum Yönetimi Organizasyon Yapısı

Kaynak: Marsh Danışmanlık, Acil Eylem Yönetimi Eğitim Notları, 2010, S. 4.

Acil durumlarda aksiyon alacak ekipler ve organizasyon yapısı belirlendikten sonra acil durum prosedürleri (yangın, sel, soygun vb.) oluşturulur. Bu aşamada bankacılık sektörüne öneri olarak 7/24 çalışan çağrı merkezi birimleri olduğu için olası acil durumlardan anında haberdar olabilmek için Çağrı merkezi acil durum hattı kurulmalı ve 911, 155, 112 vb. çok bilinen bir numara kısa yol olarak atanmalıdır. Banka içi aramalarda bu numaralarla acil durum hattına ulaşılabilirken banka dışından ise önce çağrı merkezi numarası sonrasında ise bu numarayı tuşlayarak ilgili hatta en kısa sürede

ulaşılma imkânı sağlanmalıdır. Acil durumlar 7/24 meydana gelebileceği için bu tür bir haberleşme mekanizması oluşturulur.

3.2.2. Kriz Yönetimi

Kriz yönetim takımı olası bir kriz durumunda banka ile alakalı kararların alınması ve uygulanmasını sağlar. Genel olarak banka üst yönetim kadrosundan oluşur. Çoğunlukla acil durum olayı sonlandıktan sonra olayın büyüklüğüne göre kriz yönetim ekibi devreye girerken bazen de görsel veya sosyal medya da çıkan banka itibarını etkileyen olumsuz bir haber olması durumunda direkt olarak devreye girebilir. Bankacılık sektörüne öneri olarak olası kriz durumlarında özellikle ilk basın açıklamalarını bankanın en üst düzey yetkilisi yerine daha alt düzeyde bir yetkilinin yapması şeklinde bir akış olmasıdır. Olası yanlış beyanları veya varsa gelişen sonraki durumları düzeltmek ve değerlendirmek adına daha sonra en üst düzey yetkili açıklama yapabilir.

3.2.3. İş Kurtarma ve İş Etki Analiz Çalışması

Bankanın gerçekleştirdiği tüm süreçler ve ilgili departmanlar belirlenir. Buradaki süreçlere idari işler, satın alma, denetim, teftiş vb. bankanın ana faaliyeti haricindeki süreçleri gerçekleştiren birimler dâhil edilmez. Bankacılık süreçlerini içeren aktiviteler çalışmada yer almalıdır.

Tablo 8: Örnek Süreç Listesi

No	Departman Adı	Süreç Adı
1	Alternatif Dağıtım Kanalları	ATM İşletilmesi ve Arıza Bildirimleri
2	Alternatif Dağıtım Kanalları	Fatura Borç ve Tahsilât Bildirimleri
3	Bankacılık	E–Haciz İşlemleri
4	Kurumsal Krediler	İnşaat Projeleri Taleplerinin Sonuçlandırılması
5	Ödeme Sistemleri Müdürlüğü	ATM Kartı, POS, Kredi Kartı, Switch İşlemleri
6	Güvenlik ve Harcama İtirazları	Fraud Monitoring–İnternet Bankacılığı
7	Risk Takip Müdürlüğü	Ekspertiz İşlemlerinin Yerine Getirilmesi
8	Bireysel Krediler	Bireysel/Kurumsal Fon Kullandırım Projeleri
10	Şube	Çek, Senet ve Takas İşlemleri
11	Dış Ticaret ve Hazine Operasyonları	EFT İşlemlerinin Yerine Getirilmesi
12	Bankacılık	Hesap Açılışları

Kaynak: Kuveyt Türk, Banka İş Sürekliliği Çalışma Notları, 2014, s. 8.

Zaman kriterleri belirlenir. Genel olarak 1 saat, 4 saat, 1 gün vb. değerler zaman kriteri olarak belirlenir. Her bankaya göre değişiklik gösterebilir fakat bu değerler bankacılık sektörü açısından uygun olacaktır.

Etki kriterleri tablosu dikkate alınarak ilgili sürecin belirtilen zaman aralıklarında gerçekleştirilememesi halinde oluşacak negatif etkileri finansal, yasal yükümlülük, müşteri memnuniyeti, şirket itibarı ve rekabet olarak 0–5 arasında önem dereceleriyle derecelendirilmesi gerekmektedir.

Tablo 9: Etki Kriterleri ve Derece Tablosu

Risk Etki Kriterleri ve Dereceleri						
No	Etki	Finansal	Yasal Yükümlülükler	Müşteri Memnuniyeti	Şirket İtibarı	Rekabet
0	Etki Yok	0 ile 1,000 $ Arası Kayıp	Etki Yok	Etki Yok	Etki Yok	Etki Yok
1	Önemsiz	1,000 ile 10,000 $ Arası Kayıp	Sözleşme Kapsamında Hafif Cezai Şartların Uygulanması	Müşteri Memnuniyetsizliği	Medyanın Olumsuz Yaklaşımı Yok	Minimal Oranda Etki
2	İhmal Edilebilir	10,000 ile 50,000 $ Arası Kayıp	Sözleşme Kapsamında Önemli Cezai Şartların Uygulanması	Cezai Şart Kapsamına Girmeyen Müşteri Şikâyetleri	Sektörde Veya Yerel Medyada Olumsuz Haber	Bir Miktar Negatif Etki Söz Konusudur.
3	Orta	50,000 ile 250,000 $ Arası Kayıp	Maddi Yaptırımla Sonuçlanan Cezalar	Hafif Cezai Şartlar	Sektörde Veya Yerel Medyada Olumsuz Haber	Orta Dereceli Negatif Etki
4	Önemli	250,000 ile 1.000.000 $ Arası Kayıp	Olayın Mahkemeye İntikal Etmesi	Önemli Cezai Şartların Uygulanması	Ulusal Medyada Olumsuz Haber	Önemli Oranda Negatif Etki
5	Çok Önemli	1.000.000 $ Üzeri Kayıp	Lisans/Yetki İptali	Sözleşmenin İptali	Medyada Aleyhte Kampanya	Yüksek Düzeyde Negatif Etki.

Kaynak: Marsh Danışmanlık, İş Sürekliliği Eğitim Notları, 2010, s. 14

Süreçler, etki ve zaman parametreleri de belirlendikten sonra her müdürlük kendi süreçlerinin puanlamasını gerçekleştirir. Elde edilen tüm sonuçlar bir uygulama aracılığıyla analize tabi tutulur. Girdi değerleri aşağıdaki tabloda gösterilmiştir.

Tablo 10: İş Etki Analizi Süreç Puanlama Tablosu

Bölüm /Birim	İş Süreci	Zaman Dilimleri	Finansal	Yasal Yükümlülük	Müşteri Memnuniyeti	İmaj	Rekabet
Alternatif Dağıtım Kanalları	ATM İşletilmesi Ve Arıza Bildirimleri	1 Saat	1	0	1	1	1
		4 Saat	2	1	1	1	2
		1 Gün	3	1	2	1	2
		1 Hafta	4	1	3	4	4
		1 Ay	5	3	4	5	4
Bireysel Krediler	Devam Eden İnşaat Projeleri Taleplerinin Sonuçlandırılması	1 Saat	0	0	0	0	0
		4 Saat	0	0	0	0	0
		1 Gün	0	0	1	1	1
		1 Hafta	4	0	2	2	3
		1 Ay	4	0	2	3	4
Çağrı Merkezi	Telefon Bankacılığı Hizmetleri	1 Saat	0	0	3	4	4
		4 Saat	0	0	4	5	4
		1 Gün	0	0	5	5	4
		1 Hafta	0	0	5	5	4
		1 Ay	0	0	5	5	4
Şube	Nakit Yatırma	1 Saat	0	0	0	0	0
		4 Saat	2	0	1	1	1
		1 Gün	3	0	2	1	2
		1 Hafta	4	1	3	2	3
		1 Ay	5	1	4	3	4

Kaynak: Kuveyt Türk, Etki Analizi Çalışma Notları, 2014, s. 13.

Yapılan bu etki analiz değerlendirmesi sonrasında her bir sürecin önceliklendirme matrisindeki yeri belirlenmiş olur. Aşağıda yer alan önceliklendirme matrisinde bazı süreçler 1 saat içinde yapılması gereken kritik süreçler olarak ortaya çıkarken, bazı süreçler 4 saat, bazıları ise 1 aydan fazla bir zaman dilimi içerisinde yer almaktadır. Çağrı Merkezi Müdürlüğü'ne ait telefon bankacılığı süreci 1 saat içinde yer almaktadır.

Bu durumda olağanüstü bir durum yaşandığında öncelikli olarak 1 saat zaman dilimi içerisindeki süreçlerin gerçekleştirilmesi gerekir. Telefon bankacılığı süreci ilk önce ayağa kaldırılması gereken süreçlerden biri olması gerekir. Kritik süreç olarak adlandırılan süreçler banka üst yönetimi tarafından yatırım yapılacak zaman dilimi

içerisinde yer alan süreçlerdir. 1 hafta ve öncesinde yer alan tüm süreçler iş sürekliliği kapsamında yedeklenir.

Tablo 11: Süreç Önceliklendirme Tablosu

Bölüm	4 Saat İçinde	1 Gün İçinde	1 Hafta İçinde	1 Ay İçinde
Alternatif Dağıtım Kanalları Ürün Geliştirme Müdürlüğü		XTM Login Süreci	Mobil Şube Süreci	Ticari Kartlar Başvuru, Tahsis Süreci
			İnternet Şube Süreci	İhtiyaç Kart Başvuru ve Değerlendirme Süreci
Aktif–Pasif Yönetimi Müdürlüğü	Swap (Inter Bank) Süreci	Kira Sertifikası Alım Yurtdışı İhaleye Katılım Portföye Alım Süreci	Fiziksel Altın Transferi Süreci	Elektronik Altın Transferi Süreci
Bankacılık Operasyonları Müdürlüğü	Çekin Portföye Alınması Süreci	Bloke Çek Düzenleme Süreci	Çek İade Süreci	Senetlerin Teslim Alınması Süreci
	Bankamız Türk Lirası Çekleri Tahsil Süreci	Çek Karne Basım ve Teslimi Süreci	Karşılıksız Çek Kayıtlarının Risk Merkezine Bildirimi	Muhabir Senet Tahsilâtı Süreci
Bireysel Krediler Müdürlüğü		Bireysel Kredi Kartı Başvuru ve Değerlendirme Süreci	Kredi Kartları Limit Artırım Süreci	DIP Komite Süreci
		Fon Başvuru ve Limit Tahsis Süreci Bireysel		

Kaynak: Kuveyt Türk, Banka İş Sürekliliği Çalışma Notları, 2014, s. 13.

Kritik süreçler belirlendikten sonra bu süreçleri gerçekleştirmek için gerekli olan insan, IT sistem, lokasyon, doküman vb. her tür kaynak tespit edilerek bu kaynaklarında kritikliği belirlenir.

Öncelikle kritik süreçler hangi personel tarafından yapılıyor ise isimler ve yedekleri oluşturulur. Belirli periyotlarda yapılan test çalışmasına bu kişilerin dâhil edilmesi farkındalık açısından gereklidir.

Tablo 12: Kritik Personel Listesi

Kritik Personel Tablosu			
Birim	İş Süreci	Kritik Personel	1. Alternatif Kritik Personel
Alternatif Dağıtım Kanalları Ürün Geliştirme Müdürlüğü	Hesap Açılış Süreci–XTM	A	X
	İnternet Şube Süreci	B	Y
Bankacılık Operasyonları Müdürlüğü	Bloke Çek Düzenleme Süreci	C	Z
Bireysel Krediler Müdürlüğü	Bireysel Kredi Kartı Başvuru ve Değerlendirme Süreci	D	T
	Fon Başvuru ve Limit Tahsis Süreci Bireysel	E	S
Bireysel Pazarlama Müdürlüğü	Fatura Anlaşmaları Süreci	G	N

Kaynak: Kuveyt Türk, Banka İş Sürekliliği Çalışma Notları, 2014, s. 46.

Kritik süreçlerin gerçekleştirilmesinde hangi IT sistemleri kullanıldığı ve varsa bağımlı olunan tedarikçi firma, bağımlılık düzeyi, kabul edilebilir kesinti süresi, kabul edilebilir veri kaybı değerleri belirlenir. Bu tabloda elde edilen bilgiler, IT sistemlerinin veri merkezi tasarımında referans olarak kullanılır.

Ödeme sistemleri yazılımı, ana bankacılık yazılımı, krediler yazılımı, çağrı merkezi yazılımı gibi uygulamalar kritik olarak belirlenmiş olup bu uygulamaların çalıştırabilmesi için gerekli sunucu network, database vb. altyapının veri merkezi tarafında hazır hale getirilmesi gerekmektedir.

Ayrıca verilerin iletilmesi ve yedeklenmesi içinde RTO ve RPO bilgileri kullanılır. Örneğin; telefon bankacılığı süreci için gereksinim duyulan ana bankacılık yazılımındaki verilerinin, RPO değeri 1 saat olduğu belirlenmiş olup bu durumda 1 saat önceki verilerin sağlanması durumunda çalışmalara devam edeceği belirlenmiş olur.

Tabloda yer alan dış bağımlılık önem düzeyi alanındaki veriler ise tedarikçi firmanın süreç içerisindeki rolünün önemi hakkında bilgi sağlar. Bir süreç tedarikçi firma olmadan gerçekleştirilemiyorsa bu durumda bağımlılık düzeyi yüksek olacaktır.

Tablo 13: Kritik Süreçler IT Uygulama ve Dış Tedarikçi Bağımlılık Tablosu

Birim	İş Süreci	Uygulama	RPO	Uygulama Önem Düzeyi	Dış Bağımlılık	Dış Bağımlılık Önem Derecesi	RTO
Çağrı Merkezi	Müşteri Memnuniyeti	A	1 Gün	Yüksek	M	Orta	1 Gün
Alternatif Dağıtım Kanalı Ürün Müdürlük	İnternet Şube İşlemleri	Banka İçi Uygulama	4 Saat	Yüksek	Banka İçi Uygulama	Orta	4 Saat
Çağrı Merkezi	Telefon Bankacılığı	Çağrı Merkezi	1 Saat	Yüksek	Çağrı Merkezi	Orta	4 Saat
Kurumsal Krediler	Limit Tahsis Süreci	Fon tahsis	4 Saat	Yüksek	C	Orta	4 Saat
Ödeme Sistemleri	Mutabakat Süreci	B	1 Gün	Yüksek	B	Yüksek	1 Gün

Kaynak: Kuveyt Türk, Banka İş Sürekliliği Çalışma Notları, 2014, s. 79.

Kritik süreçlere yönelik son olarak iç bağımlılığı olduğu süreçleri ve süreci gerçekleştirilirken varsa kullanılan basılı ve dijital dokümanlar belirlenmelidir. Bu dokümanlardan hangi personelin sorumlu olduğu bilgisine olağanüstü durumlarda gereksinim duyulur. İç bağımlılık, bir sürecin gerçekleştirilebilmesi için öncesinde yapılması gereken süreci ifade etmektedir. Her sürecin bir girdi ve bir çıktı süreci bulunmaktadır. Süreçlerinin birbirinden bağımsız olması mümkün olmadığı gibi sistemlerde birbirinden tamamen bağımsız değildir. Kritik süreçlere iç bağımlılığı olan süreçlerinde kritik olması gerekir. İç bağımlılık çalışmasına yönelik çıktı değerleri aşağıda gösterilmiştir.

Tablo 14: Kritik Süreç İç Bağımlılık ve Dokümantasyon Listesi

İş Süreci	Kritik Dokümanlar	Biçim	Dokümanların Tutulduğu Yer	Sorumlu Kişi
ATM İşletilmesi	Uygulama Esasları	Dijital Doküman	Bilgi Portalı/ATM Bankacılığı	A
Tüketici Kredi Talepleri	Kredi Dosyaları	Her İkisi de	Genel Müdürlük Binası 5B Katı	B
Küçük İşletme Kredi Talepleri	Kredi Dosyaları	Her İkisi de	Genel Müdürlük Binası 5B Katı.	C

Kaynak: Kuveyt Türk, İş Kurtarma Uygulama Notları, 2014, s. 56.

Son aşamada ise belirli senaryolar kapsamında kritik süreçlerin gerçekleştirilmesi için alternatif çalışma yöntemleri oluşturulur. 5 farklı senaryo kapsamında kritik olarak belirlenen süreçlerin alternatif çalışma yöntemlerine yönelik çalışmanın çıktı değerleri aşağıda yer alan tabloda gösterilmiştir. Bu senaryolarda herhangi biri gerçekleştiğinde ilgili sürecin sürekliliğinin nasıl sağlanacağı açık ve net olarak oluşturulur.

Son yıllarda siber saldırılardan dolayı hizmet kesintileri yaşanabilmekte olup iş sürekliliği senaryolarına bu konuda eklenmektedir. Özellikle internet şube, mobil şube ve ödeme sistemleri uygulamalarına yönelik olarak yüksek düzeyde iş kesintileri yaşanabilir. Müşterilerin direkt olarak etkilendiği sistemlerdeki kesinti süresinin en az olması finansal kayıplar yaşanmaması için önem arz etmektedir.

Tablo 15: Senaryolara Göre Alternatif Çalışma Yöntemleri

	Senaryo 1	Senaryo 2	Senaryo 3	Senaryo 4
Açıklama	Lokasyona Fiziksel Erişim Yok Ancak IT Sistemleri Devrede	Lokasyona Fiziksel Erişim Var Ancak IT Sistemleri Devre Dışı	Lokasyona Fiziksel Erişim Yok ve IT Sistemleri Devre Dışı	Olası Marmara Depremi
Devam Eden İnşaat Projeleri Taleplerinin Sonuçlandırılması	İlgili Lokasyonda Kritik Personel Normal DİP Süreçlerini Devam Ettirir.	Dip Analiz Raporu Excel'de Manuel Olarak Hazırlanmaya Başlanır	Olağanüstü Durum Merkezi Devreye Girer, Kritik Personel İşlemlere Devam Eder.	Farklı Lokasyonda DİP Analiz Raporunu Hazırlanır
Küçük İşletme Kredi Taleplerinin Sonuçlandırılması	İlgili Lokasyonda Kritik Personel Normal Kredi Süreçlerini Devam Ettirir.	Olağanüstü Durum Merkezinin Devreye Girmesi Beklenir.	Olağanüstü Durum Merkezi Devreye Girer, Kritik Personel Belirlenen Lokasyonda Üzerinden İşlemlere Devam Eder.	Müşterinin İstihbaratını Yaparak Kredi Taleplerine Cevap Verecek Şekilde Komiteye Sunması.

Kaynak: Kuveyt Türk, Banka İş Sürekliliği Çalışma Notları, 2014, s. 67.

Olağanüstü durum merkezi tasarımını aktif–aktif çalışacak şekilde tasarlamak bankacılık sektörü açısından gittikçe zorunlu hale gelmektedir. Sistemlerin büyük ve karmaşık hale gelmesi sonucunda kesinti sayı ve süreleri her geçen gün artmaktadır. Finansal ve itibari risk açısından kayıpların yaşanmaması veya en az düzeyde yaşanması

adına sistem sürekliliğini uygun değer şekilde sağlamak gerekmektedir. Bankacılık sektörü için bu model çalışması sonucunda yedek veri merkezi tasarımında sistemlerin aktif–aktif çalışacak şekilde bir altyapı kurulması öneri olarak ortaya çıkmaktadır.

Ana veri merkezi ve olağanüstü durum merkezi bir birinin yedeği konumundadır. Veri merkezlerden herhangi biri hizmet veremez duruma gelmesi durumunda müşteriler kesintiden etkilenmez ve hizmetler kesintiye uğramadan diğer veri merkezi üzerinden verilmeye devam edecektir. Bu sistem kurulum ve yönetim açısından diğerlerine göre biraz daha fazla maliyetli fakat orta ve uzun vadede sağlayacağı katkılarla daha avantajlı bir hale gelecektir.

3.2.4. Eğitim ve Test Çalışmaları

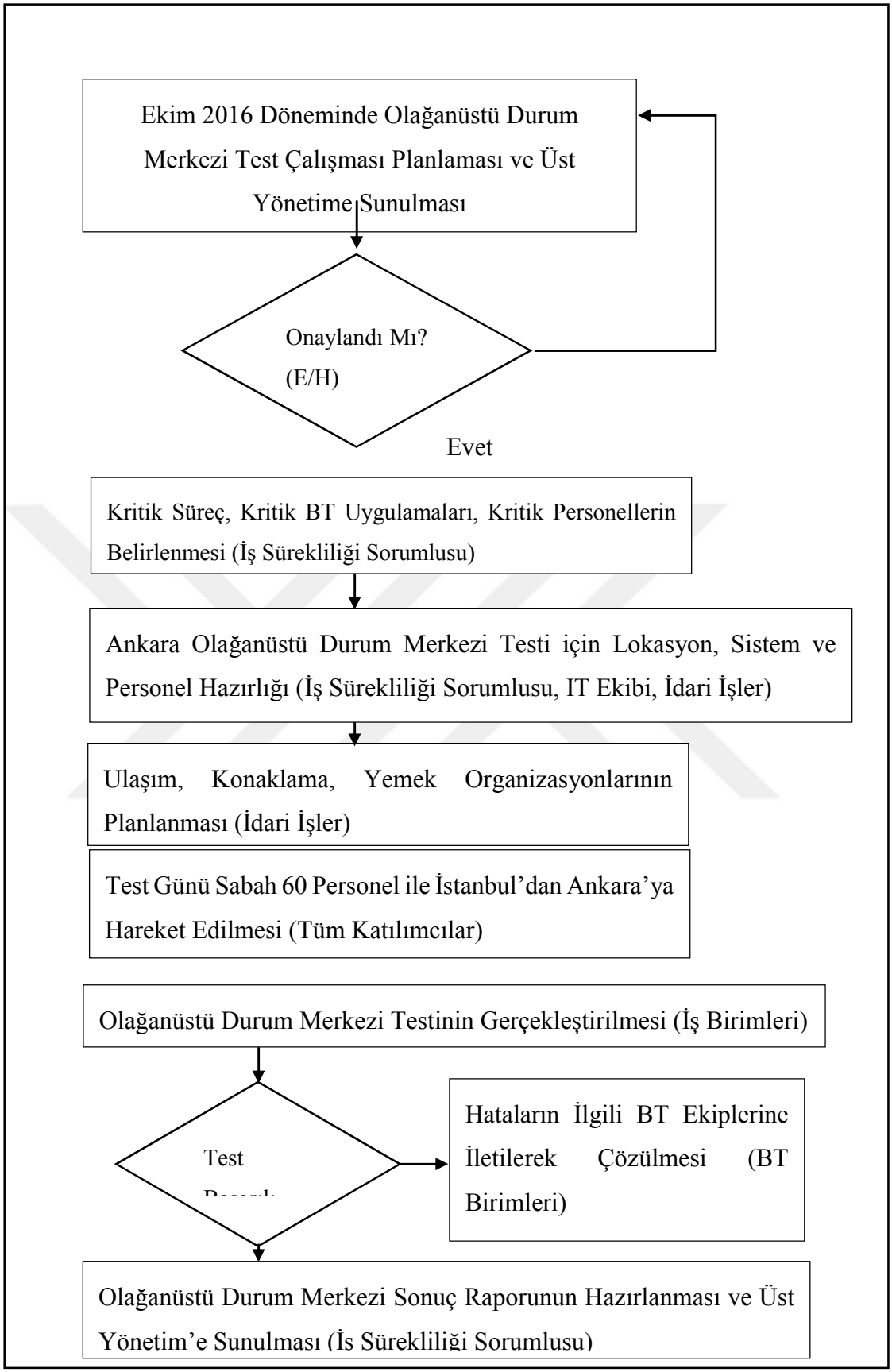
Bankacılık sektörüne yönelik olarak oluşturulan iş sürekliliği yönetim sisteminde eğitim ve test çalışmaları önemli bir yere sahiptir. Bankacılık sektöründe çalışan kesimin büyük çoğunluğunun beyaz yakalı olmasından dolayı bilinçlendirme ve farkındalık eğitimleri ile iş sürekliliği alanında ilerleme kaydedilebilir. İş sürekliliği eğitimlerinin her yıl düzenli olarak yapılması, işe yeni başlayan personellere bu eğitimlerin zorunlu olarak verilmesi konu ile alakalı farkındalığın oluşmasında en önemli çalışmalardır. İş sürekliliği testleri bankalarda üç farklı test ile yapılabilir. Bu testler acil eylem tatbikatı, kriz yönetim testi ve iş kurtarma testi olarak tanımlanmaktadır.

Acil eylem testleri çoğunlukla her çalışanın kendi bulunduğu lokasyonda meydana gelecek bir afet senaryosuna göre yapılır. Çoğunlukla yangın senaryosuna göre yapılan bu test çalışmasında çalışanların binadan sağlıklı bir şekilde tahliyesi hedeflenir. Acil eylem takımların rol ve sorumlulukları, ilkyardım ekibi üyelerinin alacağı aksiyonlar, acil toplanma noktalarının oluşturulması ve binada kalan/kalabilecek personelin belirlenmesi aşamaları acil eylem test sürecindeki en önemli faaliyetler arasında yer alır. Her lokasyon için farklı bir takım lideri belirlenerek olası tatbikat ve durumlarda bu takım liderinin direktifleri doğrultusunda hareket edilmelidir. Olay ilk meydana geldiğinde varsa acil durum hattına telefon ile bilgi verilmeli ve takım liderine konu hakkında veriler aktarılmalıdır. Bina tahliye süresi bu test için en önemli hedef göstergeleri arasındadır. Her yıl süreyi biraz daha iyileştirerek tatbikat yapılması sürecin verimliliği açısından önemlidir.

Kriz yönetim aşamasındaki test çalışmaları genel olarak benzetim testleri olarak gerçekleştirilmektedir. Test planlama aşamasında senaryo kapsamı belirlenir. Kriz yönetim takımı bir odada toplanır. Önceden belirlenen senaryo kapsamında her zaman diliminde farklı bir olay meydana gelir ve bu olaylar sırasıyla kriz yönetim takımına iletilir. Kriz yönetim takımı gelen veriler doğrultusunda nasıl aksiyonlar alacağını beyin fırtınası yaparak belirler. Olaylarda can–mal kaybı olması, yazılı/görsel/sosyal medyadaki olumsuz haberler oluşturulan senaryolar içerisine eklenir. Buradaki bilgilere göre takımın faaliyetleri gözlemlenir. Varsa olumlu–olumsuz durumlar tespit edilerek test sonrası katılımcılar ile paylaşılır.

İş kurtarma aşamasındaki testler çoğunlukla bilgi teknolojileri altyapısının test edilmesine yönelik süreçleri kapsamaktadır. İş etki analizinde ortaya çıkan süreçler ve bu süreçleri destekleyen tüm kaynakların test edilmesinin hedeflendiği bu test çalışmasında kapsamlı bir planlama gerekir. Bankacılık sektörü için yasal otorite olan BDDK tarafından açıklanan tebliğe göre bu test çalışmasının yılda bir kere yapılması zorunludur. Planlama aşamasında banka için belirlenmiş kritik süreçler, kritik IT uygulamaları, kritik tedarikçiler, kritik personel, kritik dokümanlar vb. tüm kaynaklar tespit edilir. Belirlenen test tarihi için ilgili üst yönetim komitesinin onayı alınır. Test bütçesi, lojistik ve ulaşım, varsa konaklama, yemek, test lokasyonundaki sistemsel altyapı, kullanıcılar için bilgisayar veya laptop, katılımcı listesi, tedarikçi desteği, yasal izinler plan içerisinde öncelikli ele alınacak başlıklar arasındadır. Test sırasında mevcuttaki bankacılık hizmetlerinin aksamaması için gerekli aksiyonlar, hangi veriler üzerinden ne tür işlemlerin test edileceği, test sonrası canlı sistemlere nasıl dönüş yapılacağı konuları detaylı olarak belirlenir. Test öncesi katılımcılara testin kapsamı, nasıl yapılacağı ve olası sorunlarda hangi IT birimleri iletişim kurulacağı hakkında bilgiler aktarılır.

Aşağıdaki iş akışında bankacılık sektöründe iş kurtarma testi veya olağanüstü durum merkezi testi olarak adlandırılan sürecin örnek bir akışı gösterilmiştir. Akışta yer alan faaliyetlere göre planlama yapılması testin verimli olmasına katkı sağlar.



Şekil 6: Olağanüstü Durum Merkezi Testi İş Akışı

Kaynak: Kuveyt Türk Banka Çalışma Notlarından Uyarlanmıştır, 2015.

SONUÇ

Teknoloji dünyasındaki gelişmeler hızlı bir şekilde devam etmektedir. Gelişen teknoloji sonrasında tüm sektörlerde rekabet çok yoğun bir şekilde gerçekleşmektedir. Bu rekabet ortamında kamu veya özel sektördeki tüm işletmeler faaliyetlerini en hızlı, doğru ve kaliteli bir şekilde gerçekleştirmek ve son müşterilerine kesintisiz hizmet vermek durumundadır. Olası felâket veya kesintilerden dolayı müşterilerine hizmet veremeyen kuruluşlar bir süre sonra müşteri memnuniyetsizliğinden dolayı pazar kaybı yaşayacak ve hizmet verememe süresine göre pazardan bile silinebilecektir. Bu olaylar herhangi bir doğal afetten, yazılı/görsel/sosyal medyadaki olumsuz haberlerden, siber saldırılardan veya IT sistemlerindeki herhangi bir sebepten kaynaklanabilir. Tüm bu durumlarda kesintiden en az düzeyde etkilenmek için iş sürekliliği tasarlanmalı ve buna uygun planlamalar yapılmalıdır.

Bankacılık sektörü dünyada ve Türkiye'de teknolojiyi en yoğun kullanan sektörlerin başında gelmektedir. Ödeme sistemleri, internet şube, mobil şube, EFT, Swift vb. onlarca banka uygulamasında yaşanabilecek kesintilerde yüksek düzeyde parasal kayıplarla birlikte itibar kayıpları ve yasal yaptırımlar oluşacaktır. Bu tür sistemlerde zaman çok yüksek düzeyde önem arz etmektedir.

Yaşanacak kesintilerin etkisini en az düzeye indirgemek için öncelikli ne tür senaryolar yaşanacağı belirlenerek aksiyon planları oluşturulmalıdır. Özellikle doğal afetlerde can–mal kaybı olmaması adına acil eylem planlaması çok detaylı yapılmalı, acil durum takımları oluşturulmalı ve belirli periyotlarda tatbikatlar yapılarak felâketlere hazırlık ve bilinçlendirme sağlanmalıdır.

Yazılı, görsel veya sosyal medyadaki işletme itibarini etkileyecek haberler veya afetlerde can–mal kaybı oluşan durumları yönetebilmek için kriz yönetim planları oluşturulmalı, kurumsal iletişim birimleri kurulmalı ve bu birimlerin görev alanlarına sosyal medya da eklenmelidir. Banka itibarını etkileyecek bir olay kısa zamanda yüksek düzeyde bir mevduat çıkışına sebebiyet verebileceği için bankalar için en önemli konulardan biri olarak ele alınmalıdır.

Bankacılık sektöründeki kritik süreçler zaman dilimlerine göre önceliklendirilmeli, kritik süreç olarak belirlenen süreçlerin olası bir kesintide en az

kayıpla tekrar faaliyete geçmesi için gerekli kaynak planlamaları yapılmalıdır. Bu kapsamda en önemli aşama IT sistemlerinin yedeklenmesi amacıyla yedek veri merkezinin kurulmasıdır. Türkiye'de yasal otorite tarafından her bankanın en az bir tane yedek veri merkezi kurulması zorunluluğu bulunmaktadır. Bu merkezin tasarımı, konumlandırılması ve yönetilmesi çok maliyetli bir iş olup etkin ve verimli bir planlama yapılması önem arz etmektedir. Ayrıca kritik süreçlerin gerçekleştirilmesi için gerekli personel, tedarikçi vb. diğer tüm kaynaklar net olarak belirlenmeli ve belirli periyotlarla tatbikatlar yapılarak sistemin verimliliği ölçümlenmelidir.

Bankacılık sektörü çok hızlı değişimlerin yaşandığı bir alan olduğu için her yeni eklenen süreç veya ürünle alakalı değerlendirmeler yapılarak bu plan güncellenmeli ve her daim kesinti ve felâketlere hazırlıklı olunmalıdır.

Bu çalışmada bankacılık sektörüne yönelik olarak uygulamalı bir model önerisi yer almaktadır. Her banka bu model ile iş sürekliliğini altyapısını oluşturabilir ve olası felâketlerde en az kesinti ile müşterilerine hizmet vermeye devam edebilir. Özellikle farklı lokasyonlarda çalışabilme ve lokasyon bağımsız çalışma şekilleriyle bankacılıkta yeni eğilimler ile kesintilerden en az düzeyde etkilenmek mümkün olmaktadır.

KAYNAKÇA

Akdağ, S. (2009). *Risk Yönetiminde Başarı Faktörü: İş Sürekliliği Yönetimi.* http://aymed.org/images/files/3a-IBM%20IS%20ESNEKLIGI-Sunusu-190909.pdf

Balıkçı, Y. (2009). *İşletmelerde Risk Yönetimi* . İstanbul: Cinius Yayınları.

Bayoğlu, B. (2015). *İş Sürekliliği Standartları*. http://www.bilgiguvenligi.gov.tr/is-surekliligi/is-surekliligi-konusunda-cobit-iso-iec-27001-27002-ve-itil-ne-der.html

BDDK. (2015). *Bankaların İç Sistemleri Hakkında Yönetmelik.* Bankacılık Düzenleme ve Denetleme Kurumu: http://www.bddk.org.tr/websitesi/turkce/mevzuat/bankacilik_kanununa_iliskin_duzenlemeler/11013bankalarin_ic_sistemleri_hakkinda_yonetmelik_24_02_2011.pdf

Beyatlı, C. (2010). *'Acil Durum Barınakları ve Bir Barınak Olarak Acil Durum Konteynır Öneri Modeli' Yüksek Lisans Tezi. T.C.* Trakya Üniversitesi Fen Bilimleri Enstitüsü. Trakya Üniversitesi - Fen Bilimleri Enstitüsü.

Burgan Pörtföy (2015). *Burgan Pörtföy İş Sürekliliği Planı.* http://www.burganportfoy.com/docs/default-source/finansal-bilgiler/acil-durum-esasi.pdf

Canpolat, N. (2012). *Risk Toplumunda Halkla İlişkiler Şirketlerinin Kriz ve Kriz İletişimine Yönelik Bakış Açılarının Değerlendirilmesine Yönelik Bir Araştırma.* Gümüşhane Üniversitesi – İletişim Fakültesi Elektronik Dergisi, s. 122.

Çakır, B. (2007). *Afet Ve Acil Durum Yönetimi: Bolu Belediyesi Örneği Yüksek Lisans Tezi.* Abant İzzet Baysal Üniversitesi Sosyal Bilimler Enstitüsü.

Çalışma ve Sosyal Güvenlik Bakanlığı Strateji Geliştirme Başkanlığı. (2014). *İç Kontrol Kurumsal Risk Yönetim Rehberi.* İstanbul.

Dinçkan, A. (2010). *İş Sürekliliği Kritik Başarı Faktörleri.* https://www.bilgiguvenligi.gov.tr/is-surekliligi/is-surekliligi-yonetim-sistemi-icin-kritik-basari-faktorleri-2.html

Dinçkan, A. (2016). *İş Sürekliliği Tatbikatları İçin Örnek Bir Model.* Tübitak: http://www.bilgiguvenligi.gov.tr/is-surekliligi/is-surekliligi-tatbikatlari-icin-ornek-bir-model.html

ISO. (2007). ISO 22301: Social Security. s.3-4.

Kalyoncu, D. (2013). Risksiz Risk Yönetiminin Alternatif Yolları. *Okan Üniversitesi - Sosyal Bilimler Enstitüsü*, s. 89. http://www.tusiad.org.tr/__rsc/ shared/file/ 17MartTUSIADSunum.pdf

Karabük Üniversitesi Bilgi İşlem Daire Başkanlığı. (2015). *Sistem Odasının Önemi*. http://sistemnetwork.karabuk.edu.tr/sistem_odasi/sistem_odasi.html

Kebapcı, Z. S. (2012). '*Perceived Effectiveness of Business Continuity Planning' Doktora Tezi.* Yeditepe Üniversitesi.

Komut, M. (2013). *İş Sürekliliği Organizasyonu.* İ.Ü.Siyasal Bilgiler Fakültesi, s.101-116.

Kusnetzky, D. (2011). *Virtualization: A Manager's Guide.* Kaliforniya: O'Reilly Media.

Maliye Bakanlığı Strateji Geliştirme Başkanlığı. (2015). *Defterdarlık İç Kontrol Eğitimi.* https://www.google.com.tr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwisnvKCtMfKAhUBjSwKHQOzAVMQFggbMAA&url=http%3A%2F%2Fwww.antalyadefterdarligi.gov.tr%2Fickontrol%2Frisklerin.tespiti.ppt&usg=AFQjCNGoq93A-cmlbUU1bf-MxOUcsbNOLA

Örencik, B. (2007). *Yüksek Başarımlı Bir Girdi/Çıktı Sistemi : RAID.* T.C. İstanbul Teknik Üniversitesi - Bilişim Enstitüsü, s. 5.

Özbilgin, İ. G. (2014). *Yeni bir standart: ISO 22301 İş Sürekliliği Yönetimi Sistemi ve Gereksinimler.* Bilişim Dergisi: http://www.bilisimdergisi.org/s144/pages/ s144_ web.pdf

Öztürk, A. (2013). *Bilgi Teknolojileri Altyapılarının Yönetiminde Yeni Nesil Yaklaşımlar.* Bilgi Teknolojileri Kurumu.

Pulton, N. (2014). *Network Storage & Data Replication.* İndianapolis: Sybex.

PwC. (2007). *Kurumsal Risk Yönetimi Temel Kavramlar ve Uygulamalar.* İstanbul.

Resmi Gazete. (2009). Afet ve Acil Durum Yönetimi Balkanlığının Teşkilat ve Görevleri Hakkında Kanun. Resmi Gazete 5902 nolu Kanun: http://www.dicle.edu.tr/Contents/67d90dd8-dc4c-4690-9c74-9b3cd00fb7b9.pdf

Rıdvan, A. (2014). *Bilgi Sistemleri ve İş Sürekliliği*. http://ridvan-ahmet.blogspot.com.tr/2008_03_01_archive.html

Sarıkaya, Ö. (2008). *Kriz Yönetimi.* İstanbul: Türkiye İş Bankası Kültür Yayınları.

Saymaz, Ö. (2012). *İş Sürekliliği Yönetim Sistemi.* İstanbul: Cinius Yayınları.

Sönmez, Z. (2013). *Altı Sigma Metodolojisi ile Süreç İyileştirme ve Hizmet Sektöründe Bir Uygulama Yüksek Lisans Tezi*. İstanbul Kültür Üniversitesi – Sosyal Bilimler Enstitüsü.

Sucu, Y. (2009). *Kriz Yönetimi.* Ankara: Elit Yayıncılık.

Suher, İ. K. (2013). *Kriz İletişimi Ve Yönetimi*. Anadolu Üniversitesi Yayını No: 2818 s.116.

Şahin, S. (2008). *'Bankacılıkta Risk Yönetimi ve Türk Bankacılık Sisteminin Risk Yönetimi Açısından Değerlendirilmesi' Yüksek Lisans Tezi*. İstanbul: Marmara Üniversitesi – Sosyal Bilimler Enstitüsü – İktisat Bölümü.

Teknik Altyapı ve Bilgi Güvenliği Çalışma Grubu. (2005). *E-Dönüşüm Türkiye Kdep-2004 7 Numaralı Eylem Planı.*

Telecommunications Industry Association . (2014). *TIA–942 Telecommunications Infrastructure Standard for Data Centers.*

Telkoder Serbest Telokomünikasyon İşletmecileri Derneği. (2015). *Veri Merkezi İşletmeciliği Raporu.* İstanbul.

Türkiye Bilişim Derneği. (2012). *İş Sürekliliği Yönetimi Çalışma Grubu Raporu.* Kamu Bilgi İşlem Merkezleri Yöneticileri Birliği: http://www.tbd.org.tr/usr_img/kamu_bib/RP2-2012.pdf

Ulusal Elektronik Ve Kriptoloji Araştırma Enstitüsü. (2007). *BGYS - Risk Yönetim Süreci Kılavuzu.* Ankara: TÜBİTAK.

Yazar, Z. (2009). *İş Sürekliliği Yönetimi ve İşe Etki Analizi için Uygulama Örneği; İş sürekliliği Uygulama Örneği: Siemens.* Almanya Yüksekokulları Mezunlar Derneği: http://aymed.org/images/files/5b-BCMsunum_ZekiYazar_102009.pdf