İLLER BANKASI ANONİM ŞİRKETİ

BİLİŞİM TEKNOLOJİLERİ KAPSAMINDA İŞ SÜREKLİLİĞİ

Osman DUMRUL

UZMANLIK TEZİ

HAZİRAN 2018


İLBANK
TÜRKİYE'NİN YAPICI GÜCÜ

İLLER BANKASI ANONİM ŞİRKETİ

BİLİŞİM TEKNOLOJİLERİ KAPSAMINDA İŞ SÜREKLİLİĞİ

Osman DUMRUL

UZMANLIK TEZİ

Tez Danışmanı (Kurum)
Namık ÇETİNER

Tez Danışmanı (Ankara Üniversitesi)
Dr. Öğr. Üyesi Mustafa DOĞAN

Osman DUMRUL tarafından hazırlanan “Bilişim Teknolojileri Kapsamında İş Sürekliliği” adlı tez çalışması aşağıdaki Yeterlik Sınav Kurulu tarafından OY BİRLİĞİ / OY ÇOKLUĞU ile UZMANLIK TEZİ olarak kabul edilmiştir.

	Unvanı	Adı ve Soyadı	İmzası
Başkan	Genel Müdür Yardımcısı	Salih YILMAZ	
Üye	Daire Başkanı	Hüseyin TÖREN	
Üye	Daire Başkanı	Hakkı ÇIRAK	
Üye	Daire Başkanı	Orhan IŞIK	
Üye	Daire Başkanı	Doç. Dr. Birol KAYRANLI	

Tez Savunma Tarihi: 19.06.2018

ETİK BEYAN

İLLER BANKASI ANONİM ŞİRKETİ Uzmanlık Tezi Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında; tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi, tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu, tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu, bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Osman DUMRUL
19 Haziran 2018

Bilişim Teknolojileri Kapsamında İş Sürekliliği

(Uzmanlık Tezi)

Osman DUMRUL

İLLER BANKASI ANONİM ŞİRKETİ

Haziran 2018

ÖZET

Günümüzün iş ortamında, verileri içeren bilgi teknolojileri kaynakları bir organizasyonun en önemli varlıkları arasındadır. Depremler, kasırgalar ve sel gibi doğal felaketler bu varlıkları yok edebilmektedir. Ayrıca bilgisayar virüsleri, korsanlar, vandalizm ve terörist saldırılarla kasıtlı olarak yok edilebilmektedirler. Bilgi teknolojileri bugün iş dünyasının omurgasını oluşturmaktadır. Kurtarma zamanı hedefleri küçülmektedir. Bu nedenle, organizasyonların veriyi çabucak kurtarması ve operasyonlarını sürdürecek şekilde hayatta kalması ve itibarını korumak için herhangi bir felakete karşı hazırlanması ve donatılması gerekmektedir. Bu nedenle, etkin ve verimli felaket kurtarma ve iş sürekliliği planları isteğe bağlı değildir ve kuruluşların başarısı için kritiktir. Uzun geçmişe sahip olan süreklilik planları ve felaket kurtarma aksiyonu, bilgi teknolojilerinin kuruluşların ayrılmaz bir parçası olmasıyla birlikte daha da sistemleşerek çeşitli isimlere bürünmüştür. Bu çalışmada iş sürekliliği ve ilişkili olduğu kavramlar ele alınmış, iş sürekliliğinin evrimsel gelişimi ve neticesinde yaşadığı dönüşümler adım adım ayrıntılandırılmıştır. Bilgi teknolojileri ile süreklilik ilişkisi ve bu ilişkinin alt dalları birlikte ele alınmış ve iş sürekliliğinin bilgi teknolojileri ile olan ilişkisi için ayrı bir parantez açılmıştır.

Anahtar Kelimeler	:	BT Sürekliliği, İş Sürekliliği, BT Felaketten Kurtarma, BT Hizmet Sürekliliği
Sayfa Adedi	:	175
Tez Danışmanı	:	Namık ÇETİNER (Kurum)
Tez Danışmanı	:	Dr. Öğr. Üyesi Mustafa DOĞAN (Ankara Üniversitesi)

Business Continuity within Information Technologies

(Expertise Thesis)

Osman DUMRUL

ILLER BANKASI ANONIM SIRKETI

June 2018

ABSTRACT

In today's business environment, information technology resources including data are among the most important assets of an organization. Natural disasters such as earthquakes, hurricanes and floods can destroy these beings. They can also be intentionally destroyed by computer viruses, hackers, vandalism and terrorist attacks. Information technology is today the backbone of the business world. Recovery time objectives are shrinking. For this reason, it is necessary for organizations to prepare and equip themselves against any catastrophes in order to survive and maintain their reputation in a way that can save them quickly and continue their operations. For this reason, effective and efficient disaster recovery and business continuity plans are not voluntary and critical to the success of organizations. The long-standing continuity plans and disaster recovery action have become more and more systematic and varied, with information technology being an inseparable part of the organization. In this study, business continuity and related concepts are discussed, and the evolution of business continuity and the transformations it has undergone are detailed step by step. The continuity relationship with information technologies and the bottom lines of this relationship have been taken together and a separate parenthesis has been opened for the relationship of business continuity with information technology.

Key Words	:	IT Continuity, Business Continuity, IT Disaster Recovery, IT Service Continuity
Page Number	:	175
Supervisor	:	Namık ÇETİNER (Corporate)
Supervisor	:	Asst. Prof. Mustafa DOĞAN (Ankara University)

TEŞEKKÜR

Uzmanlık tezi süreci boyunca yardımlarını esirgemeyen kurum danışmanım Namık ÇETİNER'e, ofis programlarının kullanımındaki yardımlarından dolayı kurum arkadaşlarım Merve ATAR ve Mehmet ÖTEGEN'e, tez yazım kılavuz metriklerinin uygulanmasındaki yardımlarından dolayı kurum arkadaşım Ülkü BOYRAZ'a;

Manevi desteklerinden dolayı değerli eşim Şefika ÖZKAN DUMRUL ve canım kızım Zeynep Derin DUMRUL'a ve bugüne kadar üzerimde sonsuz emeği bulunan yüce Türk milletine teşekkürü bir borç bilirim.

İÇİNDEKİLER

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

KISALTMALAR

Bu çalışmada kullanılmış olan kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
BC	İş sürekliliği
BCI	İş Sürekliliği Enstitüsü
BCM	İş sürekliliği yönetimi
BCP	İş sürekliliği planlaması
BIA	İş etki analizi
BIE	İş etki değerlendirmesi
BS	Bilişim sistemleri
	Bilgi sistemleri
BSI	İngiliz Standartları Enstitüsü
BT	Bilişim (Bilgi) teknolojileri
CEO	İcra kurulu başkanı
CM	Kriz yönetimi
CM	Değişiklik yönetimi
CMT	Kriz yönetim ekibi
COBIT	Bilgi ve ilgili teknolojiler için kontrol hedefleri
CSR	Kurumsal sosyal sorumluluk
DOS	Hizmet reddi
DR	Felaket kurtarma
DRP	Felaket kurtarma planı
EMT	Acil durum yönetim ekibi

EUC	Son kullanıcı hesaplama
EVM	Kurumsal güvenlik açığı haritası
FFIEC	Finansal kurumlar inceleme konseyi
FIPS	Federal bilgi işleme standartları
HRO	Yüksek esnek organizasyon
IMP	Olay yönetimi planı
IMT	Olay yönetim ekibi
IP	İnternet protokolü
ISACA	Bilgi Sistemleri Denetim ve Kontrol Birliği
ISO	Uluslararası Standardizasyon Organizasyonu
ITCM	Bilişim teknolojileri sürekliliği yönetimi
ITIL	Bilişim teknolojileri altyapı kütüphanesi
ITSCM	Bilişim teknolojileri hizmet sürekliliği yönetimi
ITSM	Bilişim teknolojileri servis yönetimi
KOBİ	Küçük ve orta büyüklükteki işletmeler
LAN	Yerel alan ağı
MADs	Maksimum izin verilebilir kesinti
MDT	Maksimum kapatma zamanı
MTBF	Arızalar arasındaki ortalama süre
MTD	Maksimum zaman aşımı
MTO	Maksimum tolere edilebilir kesinti
MTPD	İzin verilen maksimum kesinti süresi
MTTR	Onarıma kadar geçen ortalama süre
NIST	Ulusal Standartlar ve Teknoloji Enstitüsü
NYSE	New York Menkul Kıymetler Borsası

OR	Organizasyonel esneklik
RA	Risk değerlendirmesi
RM	Risk yönetimi
RPO	Kurtarma noktası hedefi
RTO	Kurtarma süresi hedefi
SLA	Hizmet seviye sözleşmesi
SLM	Hizmet seviye yönetimi
SP	Özel yayınlar
SRT	Sistem kurtarma süresi
TQM	Toplam kalite yönetimi
UPS	Kesintisiz güç kaynağı
VB	Ve benzeri
WAN	Geniş alan ağı
WRT	İş kurtarma süresi

GİRİŞ

Günümüz iş dünyasının küreselleşmiş doğası, teknoloji kullanımının her yerde olması, tehditler ve risklerin çeşitliliği, küresel mali konular ve kriz olaylarının çeşitliliği kuruluşların yaşamlarında iş kesintileriyle ne denli birlikte olduğunun tanımını yapmaktadır. Rekabetçi ve başarılı kalmak isteyen kuruluşlar, ciddi bir iş kesintisi durumunda kârlı bir şekilde yaşamlarına devam edebilmeleri için artan esneklik yoluyla korunmalıdır. Hayatta kalabilmek için doğru ürünü, doğru zamanda, müşteriye ve sürekli olarak sağlayabilmek gerekir. Değişen dünyada kuruluşlar, tüm potansiyel tehditler için sahip olduklarından daha büyük ölçüde önlemler hazırlamalı ve planlamalıdır.

İş sürekliliği yönetimi (BCM), bozulma/kriz/felaketin nedeni ne olursa olsun bütüncül yaklaşımla anahtar iş süreçlerinin devam etmesini sağlamaktadır. Etkili bir BCM, kurumların dinamik, global ve müşteri odaklı günümüzün çağdaş pazarında rakiplerine kıyasla avantaj sağlamasına olanak tanımaktadır. BCM, teknolojik açıdan dar kapsamlı olan geleneksel felaket kurtarmadan daha geniş kapsamlı bir bakışa sahiptir; çünkü BCM risk ve tehdit yönetimine, işin tüm görev kritik unsurlarını kapsayan bütünsel bir yaklaşım getirmektedir (Garrett, 2012).

Bilgi teknolojileri (BT), kamu ya da özel fark etmeksizin tüm organizasyonel sektörlerde kritik unsurlara sahip faaliyetlerin çoğunun ayrılmaz bir parçası olmuştur. İnternetin ve diğer elektronik ağ hizmetlerinin çoğalarak artması ve günümüzdeki sistem ve uygulama yeteneklerinin sınırsızlığı, kurumların sürekli ve güvenli BT altyapılarına her zamankinden daha çok ihtiyaç duymasına sebep olmaktadır (ISO/IEC 27031:2011(E), 2011). Kuruluşlar, iş uygulamalarını desteklemek ve müşterilerine mal ve hizmetler sunmak için neredeyse her zaman BT hizmetlerine bağımlı kalmaktadır.

Kuruluş yönetiminin iş süreklilik planlama sürecinin bir parçası olarak kapsamlı bir iş sürekliliği planı (BCP) geliştirmesi gerekmektedir. BCP, kuruluşun büyüklüğüne ve karmaşıklığına dayanmaktadır ve kuruluşun genel işletme stratejisi ile uyumlu olmak durumundadır. BCP'nin amacı, kuruluştaki maddi kayıpları asgari düzeye indirmek, müşterilere ve piyasalara en düşük aksaklıklarla hizmet etmek ve aksamaların işletme faaliyetleri üzerindeki olumsuz etkilerini hafifletmek olması gerekmektedir (FDIC, 2002).

İş sürekliliği yönetimi, iyi kamu sektörü yönetişiminin vazgeçilmez bir bileşenidir. BCM bir kuruluşun etkin risk yönetimine genel yaklaşımının bir parçasıdır ve kuruluşun olay yönetimi, acil müdahale yönetimi ve BT felaket kurtarma konularına yakından bağlı olmak zorundadır. Başarılı bir iş sürekliliği yönetimi, kuruluşun yönetici tarafından farkındalık yaratma ve esneklik oluşturmak için sağlam yaklaşımlar uygulama taahhüdünü gerektirmektedir. Kuruluş olarak esnek bir varlık olmak çağdaş iş sürekliliği uygulamalarının ayrılmaz bir parçasıdır (Australian National Audit Office, 2009).

İş süreçlerindeki ve teknolojideki değişiklikler, terör endişelerini, son zamanlarda yaşanan büyük felaket ve facia tehdidini arttırmaktadır. Bu durum, etkili iş sürekliliği planlamasına olan ihtiyaca daha fazla dikkat çekmektedir. Sonuç olarak, iş sürekliliği planlama sürecinde bu konulara daha fazla ağırlık verilmektedir. Kuruluş yönetimi, tüm bölgeyi etkileyebilecek ve kuruluş için önemli kayıplara yol açabilecek alan çapında olası felaketler için potansiyel dalgalanmaları değerlendirmek zorundadır. İş sürekliliği planlama süreci, kuruluşun ilişkili olduğu sistem katılımcıları ve altyapı hizmet sağlayıcıları arasında hem pazar temelli hem de coğrafi olarak bağımlılıkları ele almaktadır. Çoğu durumda, kurtarma süresi hedefleri (RTO) birkaç yıl önce olduğundan çok daha kısadır ve bazı kuruluşlar için RTO'lar saatler ve hatta dakikalar üzerine kuruludur. Sonuçta tüm kuruluşlar beklenmedik durumları öngörmeli, planlamalı ve iş sürekliliği planlama sürecinin, geçmiş felaketlerden öğrendikleri dersleri uygun bir şekilde ele almalarını sağlamalıdır.

İş sürekliliği alanı, hizmet kalitesine, sistemlerin ve süreçlerin dayanıklılığına büyük ölçüde katkıda bulunduğu için artan bir ilgi görmektedir. Pek çok iyi uygulama, yönetmelik ve tavsiye, iş sürekliliğinin öneminin tüm kuruluşlar için, özellikle BT sistemlerini iş süreçlerini uygulamak için kullananlar için, altını çizmektedir.

İş süreçleri, bilgi ve iletişim teknolojisi yoluyla giderek birbirine bağlanmaktadır. Bu duruma, teknik sistemlerin karmaşıklığındaki artış ve teknolojinin doğru operasyonlarına artan bir bağımlılık eşlik etmektedir (British Standarts Institution, 2005).

İstatistikler, kendilerini yeterince korumak için adım atmayan kuruluşların büyük bir felaketin yaşandığı bir yıl içinde ciddi başarısızlıklar yaşadığını göstermektedir.

Kuruluşlar borsaya kote olduğunda, yatırımcılar felaketin etkisine karşı uygun önlemlerin alınmadığına inandıklarında hisse fiyatlarının olumsuz etkilenmesine neden olmaktadır.

BT'nin anlık değişim ve gelişim sürecinin etkileri, mikro düzeyden makro düzeye doğru hem negatif hem de pozitif anlamda artmaktadır. Pozitif etkilerden maksimum fayda sağlamak ve negatif etkilerden de minimum zararı görmek adına yapılması gerekenlerin temelinde, iş sürekliliği yönetiminin aktif bir şekilde ele alınması ve her düzeyde çalışana idrak ettirilerek uygulamaya konulması vardır. İş sürekliliği yönetiminin BT sistemlerine ve iş akışlarına adaptasyonu bu bakımdan çok büyük önem arz etmektedir. Adaptasyonun hızlı bir geçiş ile sağlanması ve ivedilikle işlerlik kazandırılması adına firma ya da kurumların ayırması gereken finansal paylar, uzun vadede verimlilik, piyasada güven ve benzeri (vb) geri dönüşler ile kendini gösterecektir.

1. İŞ SÜREKLİLİĞİ VE İLİŞKİLERİ

İş sürekliliği; yaşayan, değişen, gelişen ve öğrenen bir kavramdır. Tüm bu nitelikleri itabari ile iş sürekliliği uzun süre dış etkilere ve bileşenlere maruz kalmış ve etkileşime girdiği diğer sistemlerle ilişkiler kurmuştur.

1.1. İş Sürekliliği ve Evrimi

İş sürekliliği kavramı var oluşundan itibaren doğma, emekleme, büyüme ve olgunlaşma gibi süreçlerden geçmiştir. Gelişen bu süreçler çerçevesinde iş sürekliliği katmanlanarak değişmiştir. İş sürekliliğinin yaşamış olduğu bu hayat döngüsü basamakları iş sürekliliğinin evrimini oluşturmaktadır.

1.1.1. İş sürekliliği

İş sürekliliği ISO 22301 standardında: "Bir kuruluşun üzerindeki potansiyel iş kesintilerinin etkilerini önceden tespit eden ve ilgili tarafların çıkarlarını, saygınlığını, markasını ve değer yaratma faaliyetlerini koruyan, etkin yanıt verme becerisiyle kuruluşa tehditlere karşı esneklik kazandırmak için bir altyapı sağlayan bütünsel bir yönetim ve idare sürecidir" şeklinde tanımlanmaktadır (International Organization for Standardization, 2012). İş sürekliliği, bir organizasyonun ciddi olaylar ya da felaketler durumunda çalışmaya devam etmesini ve kısa sürede operasyonel bir duruma gelebilmesini sağlamak için planlama ve hazırlıkları kapsamaktadır (The EU Cyber Security Agency, 2017). İş sürekliliği, bir organizasyonun operasyonlarının ve temel iş fonksiyonlarının, kritik sistemleri çevrim dışı duruma düşüren bir felaket veya planlanmamış olaydan ciddi olarak etkilenmemesini sağlamayı amaçlamaktadır. İş sürekliliği planlaması, genellikle bilgi teknolojisinin öncülük ettiği bölümler arası süreci, normal işi belirli bir süre geri yüklemek için kullanılan taktikleri uygulamayı, iş için kabul edilebilir veri kaybı miktarını tanımlamayı ve olayları takip etmektedir. İş sürekliliği, kritik sistemlerin çalışmasını sürdürme sürecidir. İş sürekliliğinin amacı, kesinti süresini azaltmak veya önlemek ve operasyonları optimize etmektir (ThinkIT by Singlehop, What is business continuity?).

İş sürekliliğinin (BC) tarihçesi ve gelişimi ile kökenlerini kısaca anlatmak öğreticidir. Bunun amacı basitçe bir dizi tarih ve nedensel olayları listelemek değil, aynı

zamanda BC fonksiyonunun ve süreçlerinin gelişimine ilişkin fikir sunmaktır. Tarihçeye bakıldığında uygulayıcının BC unsurlarının, belli algılamalar için başlangıç noktalarını tanıması faydalı olacaktır. BC'nin şu anki statüsüne doğru gelişmesi, organizasyonlarda, düzenlemelerde ve mevzuatta meydana gelen gelişmelere, olaylara ve diğer direnç konularına yansıma, analiz etme, bunlara tepki verme ve bunlara etki eden değişiklikler sonucu ortaya çıkmıştır. Vaka analizlerinden edinilen tecrübe, geliştirilmiş yanıtlar ve gözlemler, BC'nin devam eden evrimine katkıda bulunmuştur.

BC'nin uygulanabilirliği ve gelecekteki şekli açısından son yılların trendlerinin nereye odaklandığını, bu faaliyetlerin ve ilişkili iş akışlarının nerelerde mümkün olan en iyi sonucu alabileceğini düşünmek belki de daha öğretici olacaktır. BC, BT sürekliliğini ve kapasitesini sürdürme ihtiyacından kaynaklanmaktadır ve teknolojinin ve toplumsal bağımsızlığın artmaya devam etmesiyle birlikte, gelecekteki örgütsel kapasitenin geliştirilmesine önemli katkı sağlayacak açık bir temel var etmektedir. Bu nedenle, BC'nin yönetimle uyumlu bir süreç ve tanım olarak gelişmeye devam edeceği varsayımıyla, 21. yüzyıl, iş sürekliliği yönetimini kodlamak ve bunu kalite, bilgi güvenliği ve çevre hizmetleri tarafından halihazırda oluşturulan bir yolu izleyerek yönetim sistemleri standartları ailesinin bir parçası olarak sınıflandırmak için var olan kararlılığı gördü (Business Continuity Institute, 2013) düşüncesi, daha fazla düşünmek için sağlam bir temel sağlamaktadır. Yaklaşımın temeli, BC'nin önemini ve uygulanabilirliğini ve örgütsel işlevsel süreç içindeki yerini daha iyi anlamaktır. Buna paralel olarak nispeten yeni ve genç bir disiplin olarak BC, değişen örgütsel çevreyle kendisini yeniden düzenleyebilecek özellikte olması nedeniyle benzersiz bir şekilde yerleştirilmiştir. Demografik, teknolojik ve düzenleyici gelişmeler karşısında organizasyonel davranışın profili değiştikçe, BC'nin özellikleri ve gerçekleştirilmesi gereken ilgili süreçlerin de değişmesi gerekecektir. Bu normal ve rutin bir yönetim ve organizasyon konseptidir ve BC diğerlerinden farklı olmamaktadır. BC, organizasyon üzerindeki etkileri ve ürün ve hizmetleri üzerinde doğrudan odaklanan bir işlev olarak, etkinliği korumak için dinamik ve tekrarlayan bir yeteneğe bağlı kalmaktadır.

Çizelge 1.1. Disiplinler Karşılaştırması (Arveson, 1998)

	İş Sürekliliği	Güvenlik	Kriz	Acil Durum	Felaket Kurtarma
Tahmin	x	x	x	x	x
Önleme		x			
Koruma	x	x	x	x	x
Yanıtlama	x		x	x	x
Kurtarma	x		x	x	x

Yukarıdaki şekil çeşitli esneklik alt disiplinlerini göz önünde bulundurarak, her birinin uygulanabilirliğini ve odağını değerlendirmek istemektedir. Tüm bunlar; krizler, acil durum yönetimi ve felaket kurtarma ile birlikte tehditlerin gerçekleşmesi potansiyelini öngörmeyi amaçlamaktadır. Güvenlik, riske ve oluşma ihtimaline daha çok odaklanma eğiliminde olmaktadır ve riskin kayba veya hasara yol açmasını önlemeye çalışmaktadır. BC, kriz, acil durum ve felaket kurtarma (DR), önleme, yanıtlama ve kurtarma yönünde daha az odaklanacaktır. Dolayısıyla, güvenlik ile BC arasındaki uyuşma hatalıdır. Her ikisinin de örgütsel esnekliğe katkıda bulunma amacı vardır ancak işlevler tamamlayıcı ve ayrılabilir niteliktedir. Güvenlik, korunma dengesine ve örgüte rahatsızlık vermeyecek şekilde tasarlanabilecek engellerin ve önleyici süreçlerin uygulanmasını gerektirir. BC, engeller ile değil, güvenlik prosedürleri ve risk yönetimi başarısız olsa dahi, organizasyonel olarak gömülü yönetim ve yetenekleri koruyan sistemler ile ilgilidir. Böylece, iş sürekliliği yönetimi (BCM), etkileri önceden tahmin edebilmek ve yönetebilmek için çevikliğe, esnekliğe ve tepki vermeye ihtiyaç duyan bir takım uygulamalar ve ilişkili süreçlere dönüştürülmüştür.

Aynı derecede önemli olan BC uygulayıcısının karşı karşıya olduğu görev, BCM'nin ve ilişkili mesajların yalnızca organizasyonel süreçler ve uygulamalar içinde tamamlayıcı nitelikte olmayıp, aynı zamanda da dâhil edilmesini sağlamaktır. Böylece uygun seviyede standart, kapasite farkındalığı ve kuruluş yeteneği var olmaktadır. Bu değişen geçmişe ve bağlama karşı dinamik ve etkili bir BCM uygulayıcısı olabilmek için, bireylerin ve ekiplerin gelecekte potansiyel tehdit ve etki alanlarını araştırmaya ve esnek ve

verimli BC süreç modelini değişmeden uygulayabilme yeteneğine sahip olmaları gerekmektedir.

İş sürekliliği, kritik iş fonksiyonlarının müşterilere, tedarikçilere, düzenleyicilere ve bu işlevlere erişmesi gereken diğer kişilere sunulmasını sağlamak için bir organizasyon tarafından gerçekleştirilen faaliyettir. Bu faaliyetler, proje yönetimi, sistem yedeklemeleri, değişim kontrolü ve yardım masası gibi pek çok gündelik işleri içerir. İş sürekliliği, felaket anında uygulanan bir şey değildir; iş sürekliliği, hizmet, tutarlılık ve kurtarmayı sürdürmek için günlük olarak gerçekleştirilen etkinlikleri tercih etmektedir (Sinha, 2011).

Gelecekteki BCM hakkındaki herhangi bir düşünce, sadece organizasyona yönelik risklerin ve etkilerin analizini değil aynı zamanda organizasyonun profilini de içerecektir. Pazar ekonomilerindeki mevcut ve gelecekteki insan profili, mümkün olan en kısa zaman diliminde kendi seçtikleri yere ulaştırılan ürün çeşitliliği açısından servis sağlayıcılardan daha fazla hizmet talep etmektedir ve edecektir. Bu durum, örgütsel süreçler ve çıktılar üzerinde artan bir baskı oluşturmaktadır ve bu artan baskı, organizasyonların boşluklarını ve zayıf yönlerini ortaya çıkarabilmektedir. Bu nedenle, aralarında BC ilişkisi olan tüm organizasyon işlevlerinin bu talebi kolaylaştıracak ve karşılayabilecek kapasitede olması gerekmektedir. Bu düşünceler göz önünde bulundurularak, BC'nin etkililiğinin yalnızca kişilerin kabulü, farkındalığı ve kabiliyetine değil, aynı zamanda örgütte bulunan sistemlerle uyuşma kabiliyetine bağlı olduğu görülmektedir. Güvenlik ve kriz yönetiminin, korumayı amaçladıkları örgütsel işlevlerden bir ölçüde ayrı ayrı planlanabileceği görülebilmektedir. BC, kritik işlevleri korumayı amaçlamaktadır ve bu nedenle geliştirilmesi veya geliştirilmesi yerine bu işlevlerin bir parçası olması gerekmektedir ve koruyucu olarak algılanmaktadır. Örgütün, kaynağı olmadan işlev göremeyeceği düşünüldüğünde, organizasyonun organik ve dâhili süreklilik kabiliyeti olmadan çalışamayacağı ortadadır (Woods, 2013).

1.1.2. İş sürekliliği planlamasının kökleri

İş sürekliliği planlamasının (BCP) kökleri, savaş oyunları ve senaryo planlamasından sonra gelişen felaket kurtarma (DR)'da yatmaktadır. Savaş oyunlarının erken dönem oluşumlarında kötü durumları avantaja çevirme olanağı, iyi planlamanın ödülü olarak görülmektedir.

Sun Tzu (M.Ö. 544-496), stratejik düşünce konusunda en eski yazılardan biri olan Savaş Sanatı'nı yazdı ve dünya üzerindeki askeri ve iş dünyası düşünürleri arasında konuyla ilgili en büyük etkileyicilerden biri olarak kabul edildi. Sun Tzu (M.Ö. 544-496), askeri düşünceye senaryo temelli planlama ve hazırlık kavramını getirdi. Askeri odaklı stratejiler; yedeklemeler (silah taşıyıcıları), senaryo planlama ve bilinmeyen için planlama gibi kavramlardır. Bu stratejiler değişen koşullara hızlı, esnek ve uygun bir şekilde karşılık vermeyi kabul etmektedir. Strateji, olası olanı öngörmekte (öngören senaryolar) ve uygun şekilde hazırlanmaktadır (Oriesek ve Schwarz, 2008).

Senaryo planlaması

Senaryo planlaması, II. Dünya Savaşı'ndan sonra askeri planlamanın bir yöntemi olarak savaş oyunundan ortaya çıktı. Senaryo planlama kavramı, sistemler ve oyun teorisi gibi uygulamaları kullanarak 1950'lerde soğuk savaş döneminde Herman Kahn tarafından kullanılmıştır (Oriesek ve Schwarz, 2008).

Senaryo planlamasının temel amaçlarından biri, eğilimleri ve belirsizlikleri belirlemek ve gelecekteki olası olayların sonuçlarına bakmaktır.

Senaryo planlamanın işletme perspektifinden faydası, 1970'lerin başında, Royal Dutch / Shell için bir planlayıcı olarak çalışan Pierre Wack'in eserlerinden anlaşılmaktadır. Shell Group, Wack'in çalışmalarına dayanarak, ana bilgisayarlarındaki hayati verilere erişemeyecekleri bir geleceği planladı ve bunun sonucunda bilgi teknolojisi (BT) yedeklerinin oluşturulmasına yatırım yaptı. Bu erken BCP ve DR girişimlerinin büyük oranda rekabet avantajı kazanma açısından gerçekleştiği dikkate değerdir. Bir organizasyon, tarihi verilere dayanan tahminlere dayanmak yerine yüzleşebileceği sayısız olası geleceğe bakarak ve geleceğin istikrarsız olacağının farkına vararak geleceğin potansiyel sorunlarına ve zorluklarına yönelik farklı stratejiler hazırlayabilmektedir (Wack, 1985).

Senaryonun, senaryoyu ilk başta geliştiren ve dolayısıyla hayal gücünün sınırlı olduğu kişi veya kişilerin görüşleri ile temelde ön yargılı olduğunu belirten sınırlamaları konusunda uyarıda bulunmak gerekmektedir. Benimsenen yaklaşımlara bağlı olarak senaryolar, geçmişin rasyonel ve güvenli uzantılarından başka bir şey değildir ve muhtemel

sonuçları gerçekliğin basit doğrusal görüşleri boyunca sıklıkla sınıflandırırken gerçek dünya karmaşıklığını ve çok boyutları içerir (Oriesek ve Schwarz, 2008).

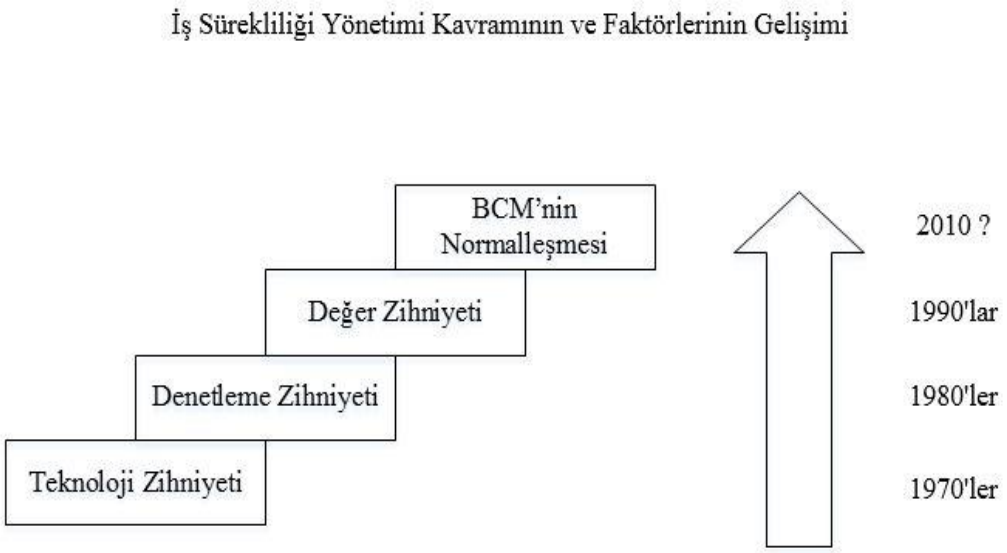
Gelecekteki senaryoların geliştirilmesi, kuruluşların BT sistemlerine ve verilere ne kadar bağımlı olduklarını fark etmesini sağlamıştır. Sistemlerin korunmaya ihtiyaç duyduğunun farkına varılması, erken DR planlama gereksinimlerini ortaya koymuştur.

1.1.3. Felaket kurtarmadan iş sürekliliği planlamasına geçiş

İş sürekliliği planlaması (BCP), 1950 ve 1960'lı yıllarda kuruluşlarda ortaya çıkan DR planlamasına sıkı sıkıya bağlıdır. Felaket sözcüğünün kökeni, Latince kötü yıldız anlamına gelen (dis + astro)'dur. Felaketlerin aslında kötü niyetli astral etkilerden kaynaklandığı şeklinde bir algı vardı. Felaket kurtarmanın amacı, genellikle acil durum planlarının hazırlanmasıyla felaket olaylarını önlemek değil, bunlara cevap vermektir (Swartz, Herbane ve Elliott, 1995).

Herbane, kurumların kritik verilerin kağıt veya elektronik yedek kopyalarını alternatif sitelerde depolamaya başladığı gerçeğine değinmektedir. DR, temelde kuruluşların kurumsal veri merkezlerini daha iyi korumak istemektedir. DR'nin amacı, herhangi bir örgütsel/ticari taraf koruması sağlamak yerine teknik sistemleri korumak olmuştur. DR, senaryo planlamasının bitişi, yedekleme ve kurtarma sitelerine sahip olma fikrinden kaynaklanmıştır. İlk başta, bu yerinde olmayan depolama sadece periyodik olarak gerçekleşti, ancak dosya yedekleme ve dışa aktarma prosedürleri 1970'lerin sonlarına doğru daha sık ve düzenli hâle geldi ve ayrıca bu kez alternatif veya sıcak site hâline gelecek olanları oluşturmak için üçüncü parti bölgesel depolama tesisleri oluşturuldu (Herbane, 2010).

On yıllar boyunca DR, BCP'ye ve ardından iş sürekliliği yönetimine (BCM) dönüşmüştür. Bu evrim Elliott, Swartz ve Herbane (2010) tarafından özetlenen bir dizi düşünce zihniyeti ile en iyi şekilde karakterize edilmektedir.



Şekil 1.1. İş Sürekliliği Yönetimi Kavramının ve Faktörlerinin Gelişimi (Elliott, Swartz ve Herbane, 2010)

Teknoloji zihniyeti

Bu temel DR yaklaşımı, felaketlerden kurtulmanın teknik yönüne odaklanmıştır ve felaketlerin teknoloji başarısızlığıyla tetiklendiğini ve daha geniş ticari nedenlerine bakmak için bunun ötesine geçmediğini düşünmektedir (Elliott, Swartz ve Herbane, 2010).

Felaket kurtarma işleminin iç ve donanım odağı, felaketlerin nedenlerinin yalnızca kısmen incelenmesine izin verir ve bunların etkilerini veya semptomlarını önlemek yerine bunları tedavi etmeye çalışmaktadır (Swartz, Herbane ve Elliott, 1995).

1970'lerin sonu ve 1980'li yıllarda DR, daha geniş bir tabanı kapsayacak şekilde genişletildi ve BCP yaklaşımı, bir organizasyonda kriz olaylarıyla ilgisi olan daha geniş iç faktörlere bakmıştır. Bu genişleme, BT sistemlerinin doğasının bir ana çerçeve merkezli veri işleme yaklaşımından, son kullanıcı hesaplama (EUC) yaklaşımına dönüşümünden kaynaklanmıştır (Panko, 1987). EUC'ye geçiş, kuruluşlar arasında bilgi işlem alanını yaygınlaştırmıştır ve kuruluş verileri artık merkezi olmaktan çıkarılmış olarak DR'de, daha önce ana çerçeve yaklaşımında olduğu gibi, önemli bir etkiye sahiptir. Bu EUC değişikliği, Elliott, Swartz ve Herbane (2010) tarafından BCP'nin başka bir sigorta şekli olduğu gerçeği ile birlikte ortaya konmuştur. 1980'lerde kişisel bilgisayarların ortaya çıkışı,

merkezi bilgi güvenliği departmanları için görevleri düzenleyen bir denetim zihniyetinin geliştirilmesi için temel oluşturmuştur.

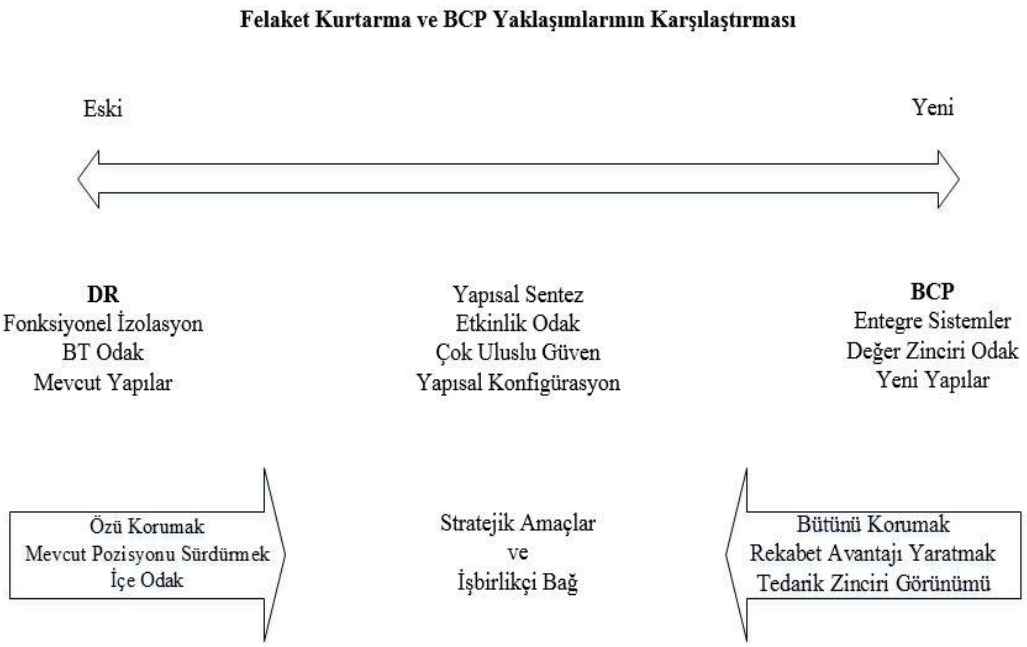
Saf DR yaklaşımından BCP yaklaşımına yapılan bu hareket, denetleme zihniyeti olarak anılmaktadır (Elliott, Swartz ve Herbane, 2010).

Denetleme zihniyeti

Denetim zihniyeti, teknolojiye odaklanırken odağını işletme faaliyetlerinin korunmasını da içerecek şekilde genişletmiştir ve çoğunlukla dış düzenlemeler tarafından yönlendirilmiştir. Herbane (2010), BCM'ye zihin-set yaklaşımı yerine, düzenleme ve mevzuat temelli alternatif bir dört aşamayı özetlemektedir. Bu safhalar birbirinden farklı olmakla birlikte, aralarında bazı çakışmalar vardır.

Dört evre; ortaya çıkan mevzuat ve mevcudiyete gelişi (1970'lerin ortalarından 1990'ların ortalarına kadar), ortaya çıkan standartlar ve daha geniş nüfuz (1990'ların ortalarından 2001'e kadar), 9/11 sonrası manzara-ivme ve odaklanma (2002-05) ve uluslararasılaşma-rakip standartlar ve koparma (2006-10)'dır (Herbane, 2010).

1997'de geleneksel DR'den BCP'ye yapılan önemli kayma fark edilmiştir. BCP yaklaşımı DR'den çok daha geniştir ve bir organizasyonun tüm ticari faaliyetlerini aksatabilecek olaylara hazırlanmayı amaçlamaktadır. BCP, iş kesintilerinin sıklıkla karmaşık nedenlerini belirlemeye ve anlamaya yardımcı olmuştur ve BCP'yi merkezi bir iş süreci olarak gerçekleştirmenin bir sonucu olarak örgütsel rekabet avantajı kazanmak mümkün olmuştur. Ancak denetime dayalı zihniyet yaklaşımı, insan katkısının bozulma olaylarının ve BCP sürecinin üzerindeki etkisini hesaba katmamıştır. Denetim zihniyetinin temel odak noktası, yıkıcı bir olayın nasıl engellenip sürdürüleceği ve uyumu sağlamanın nasıl sağlanacağı olmuştur. DR'den BCP'ye geçiş, kuruluşların nerede olduklarını yargılamalarına izin veren bir sürecin parçası olarak tanımlanmıştır. Böyle bir süreklilik aşağıdaki şekilde gösterilmektedir.



Şekil 1.2. Felaket Kurtarma ve BCP Yaklaşımlarının Karşılaştırması (Elliott, Swartz ve Herbane, 2010)

Denetim zihniyeti BCP'yi 1980'lerin ortalarına kadar kapsarken, kapsam genişletilerek BCM ve değer temelli zihniyet oluşturulmuştur. Bu gelişme denetim zihniyetinin kaybolduğunu ortaya koymamaktadır. Çoğunlukla yönetmeliklere uyularak sürdürülen kuruluşlarda bu zihniyet devam etmektedir.

1.1.4. BCP'den kriz yönetimi ve iş sürekliliği yönetimine geçiş

1980'lerin sonlarına ve 1990'lara doğru ilerlendiğinde BCP'nin alanı, dış faktörleri kriz yönetiminden (CM) daha fazla ipucu almak suretiyle genişletilmiştir. Kriz yönetimi (CM), normal organizasyonel işlemleri engelleyen ya da sekteye uğratan (en önemli hedeflerini tehdit eden) olaylara hazırlıklı ve bunlara tepki veren faaliyetlerin organizasyonu ve koordinasyonudur (Herbane, 2010). BCP'ye CM yaklaşımı, ön, kurtarma ve iç önlem odaklı BCP ve DR yaklaşımlarından farklıdır ve önleme ve kurtarma ile ilgilenmektedir. Mitroff, kriz olaylarının köklerinin tüm organizasyonlara, toplumlara ya da karmaşık bir sisteme yerleştirildiğini ve yaşanan krizlerin durdurulamayacağı bilinmesine rağmen uygulamayla yönetilebileceğini ve krizin seyrek ve öngörülemeyebilirken yönetilebileceğini belirtmiştir (Mitroff, 2001). BCP'ye CM yaklaşımı, tanınması gereken sistem ögelerinin karmaşık bir etkileşiminin olduğunu, DR

yaklaşımlarının tehditleri önlemeye çalışmadığını ve krizin hem iç hem de dış unsurlara sahip olduğunu tespit etmiştir. CM'nin vurgusu, sebepleri iyileştirmek yerine kriz önlemeye yöneliktir. Bir kriz, olay öncesi evre, odak olayı ve kurtarma ve geri dönüşün olay sonrası bir aşamasını içeren en az üç aşamaya sahiptir. Felaket kurtarma yaklaşımları son iki aşamaya odaklanırken kriz yönetimi, olay öncesi aşamada önlemeye özel önem vermektedir.

Elliott, Swartz ve Herbane (2010) tarafından ortaya konan kriz yönetimi yaklaşımı, BCP'yi bir bütün olarak örgüte daha fazla değer katmak ve tüm organizasyonel paydaşları kapsayacak şekilde genişletmek için genişleme potansiyeli üzerinde yoğunlaşan değer tabanlı zihniyete dâhil etmektedir. Bu yeni genişletilmiş odak, BCM yaklaşımını yaratmıştır. Kapsamlı organizasyonu olan geniş ve dış faktörlerle BCM yaklaşımı, organizasyonun önündeki felaket olaylarından daha iyi tahmin ve koruma sağlamaktadır.

Belirtilen yaklaşımlardan hiçbiri, bir olay meydana geldiğinde yüzde yüz başarılı bir şekilde iyileşmeyi veya kurtarmayı garanti etmemektedir. Kabul edilen yaklaşım dikkate alınmaksızın, herhangi bir felaket senaryosu ile sonuçlanacak bir dizi olay meydana gelme ihtimali hâlâ yüksektir. Ancak bir BCM yaklaşımı benimsenerek, bir organizasyonun esnek olması, felaket sonrası kurtarma ve devam etme kabiliyeti kazanması sağlanmaktadır.

Değer tabanlı zihniyet

Değer tabanlı zihniyet, BCP'yi BCM'ye doğru taşımış ve şu şekilde tanımlanmıştır: Çoğu organizasyon uyum, yönetmelikler veya teknolojik başarısızlıkları işin kendisinden daha çok önemsemektedir. En önemlisi bu zihniyette BCM, yalnızca gelirleri tüketmekle kalmaz, organizasyona değer katma potansiyeli olarak kabul edilmektedir (Elliott, Swartz ve Herbane, 2010).

Bu zihniyet setinde BCP'nin kapsamı, Elliott, Swartz ve Herbane (2010) tarafından BCM sürecinin uygulanması ve yönetilmesindeki en büyük zorluk olarak kabul edilen çalışanlar da dâhil olmak üzere tüm organizasyonu kapsayacak şekilde genişletilmiştir. Organizasyonel paydaşlar, değişim ve dolayısıyla BCM'nin tanıtılması ile geliştirilmesi için önemli bir itici güç olarak kabul edilmiştir. BCM, etkili BCM için birlikte çalışan

sosyal ve teknik sistemlerin bir kombinasyonudur ve bir kuruluşun yaptığı her şeye nüfuz etmek durumundadır. Bu durum daha iyi yanıt verme, güvenilirlik, güvenlikle daha verimli sistemler ve daha iyi müşteri değerini sağlaması nedeniyle katma değerli bir süreç olarak görülmektedir.

BCM'yi çok dar teknik alana odaklama tehlikesi akademik literatürde halen ön plana çıkmaktadır. Myers (2006) daha bütünsel bir yaklaşımın benimsenmesi yerine sistemleri korumanın BCM'nin hedefi olma tehlikesine işaret etmektedir. Kuruluşlar bugüne kadar teknolojiye daha fazla bağımlı hale geldikçe, teknik ve işletme odağı arasındaki dengeler hâlen geçerlidir.

1.2. İş Sürekliliği Planlaması (BCP)

İş sürekliliği planlaması, afetler ve yıkıcı olaylar öncesi, sırası ve sonrasında sürekli iş operasyonlarının sürdürülmesi için bir plan oluşturmak ve onaylamak için kullanılan bir yöntemdir. İş sürekliliği 1990'ların sonunda, kuruluşlar 1 Ocak 2000'de ve sonrasında iş sistemleri hatası olasılığını değerlendirmeye çalışırken ön plana çıkmıştır. İş sürekliliği, bir işletmenin gelir elde etmek için normal bir şekilde çalışmasına izin veren operasyonel ögeleri yönetmekle ilgilidir. Genellikle çeşitli teknoloji stratejilerini değerlendirirken kullanılan bir kavramdır (Snedaker, 2007).

İş sürekliliği planlaması, kuruluşun yıkıcı bir olaydan sonra kritik bir iş fonksiyonu sunmak için kullanacağı cevapları belirtmektedir. Bu işlevlerin kesinti veya aksamadan sonra mümkün olan en kısa sürede eski hâline getirilmesi, iş sürekliliği planlamasının ana hedefidir.

İş sürekliliği planlaması, organizasyonu olumsuz etkileyen risklerden etkili bir değerlendirme, hazırlık, tepki ve kurtarma sağlamak için çeşitli kaynakları bir araya getirirken, aynı zamanda kuruluşun çeşitli risklere maruz kalma durumunu tanımlar. İş sürekliliği planlaması, kuruluşun nasıl yürütüldüğü konusunda devamlılık arz eden bir stratejik uygulamadır (Hayes ve Kotwica, 2013).

İş sürekliliği planlaması, kuruluş faaliyetlerini kabul edilebilir ve önceden tanımlanmış bir seviyede devam ettirmek için organizasyonun olayları ve iş kesintilerini

planlaması ve bunlara tepki vermesi için stratejik ve taktik yeteneği olarak tanımlanmaktadır (British Standards Institution, 2006). İş sürekliliği planlaması aynı zamanda, bir iş sürekliliği planı el kitabının uygulanması yoluyla bir felaket sırasında iş devamlılığını sağlamak için organizasyonu hazırlayan bir disiplin olarak tanımlanmaktadır (Syed ve Syed, 2004). İş sürekliliği planlaması, iç kontrol ve fiziksel güvenlik de dâhil olmak üzere tehditlerin, organizasyonun kritik işletme operasyonlarında ve hizmetlerinde önemli hasarlara veya aksamalara neden olabileceği durumlarda iş devamlılığını sağlamaktadır (Barnes, 2001). Bunlara ek olarak, Federal Finansal Kurumlar İnceleme Konseyi (FFIEC) tarafından doğal afetler, teknolojik arızalar, insan hataları veya terörizm gibi olumsuz olaylarla karşı karşıya kalındığında, müşterilere sunulan hizmetler de dahil olmak üzere organizasyonların operasyonların sürdürülmesi veya kurtarılmasını sağlama süreci olarak tanımlanmaktadır (Federal Financial Institutions Examination Council, 2008). Diğer tanımıyla, kuruluşların aksamadan sonra önceden tanımlanmış bir operasyon seviyesine yanıt vermelerine, kurtarmalarına, devam ettirmelerine ve geri yüklemelerine rehberlik eden dokümante edilmiş prosedürlerdir (ISO/IEC 27031:2011(E), 2011).

İş sürekliliği planlaması, kuruluşların risklerini yönetmenin unsurlarından biridir ve günümüzde kuruluşların doğal felaketlere, terörizme ve çalışmasını engelleyebilecek birçok yıkıcı olaya karşı daha esnek hâle getirilmesinde önemli bir bileşen hâline gelmiştir. Devletler, iş sürekliliğinin toplumun ve kuruluşların esnekliğine nasıl katkıda bulunduğunu giderek daha fazla fark etmeye başlamıştır. Bu durum, kilit iş alanlarında daha fazla istikrar sağlamak için iş sürekliliğinin teşvik edilmesini sağlamaktadır (Austin, 2011).

BCP, kuruluşların temel işlevlerini belirtmekte, hangi sistemlerin ve süreçlerin sürdürüleceğini tanımlamakta ve bunları nasıl sürdüreceğini ayrıntılandırmaktadır. Bunlara ek olarak olası herhangi bir iş kesintisini hesaba katmaktadır. BCP; üretim süreçleri, müşteri ilişkileri ve etkileşimleri, araştırma tesisleri, bilgi teknolojisi altyapısı gibi temel iş fonksiyonlarına odaklanmaktadır (Jones, 2011).

BCP, kuruluşun büyüklüğüne ve karmaşıklığına dayanmakta ve kuruluşun genel işletme stratejisi ile uyumlu olmaktadır. BCP'nin amacı, kuruluşlardaki maddi kayıpları asgari düzeye indirmek, en düşük aksaklıklarla hizmet etmek ve aksamaların işletme faaliyetleri üzerindeki olumsuz etkilerini hafifletmektir. İş sürekliliği planlaması, kritik hizmetlerin kesilmesini önlemeyi ve mümkün olan en kısa sürede ve sorunsuz bir şekilde

organizasyona tam işlev kazandırmayı amaçlayan risk yönetimi süreçlerini ve prosedürlerini belirler (http://searchdatacenter.techtarget.com/guide/Building-a-disaster-recovery-architecture-with-cloud-and-colocation).

Bilgi teknolojileri, iş sürekliliğinin ayrılmaz parçasıdır ve kuruluşlar kritik iş süreçlerinin devamlılığını sağlayabilmek için ilgili bilgi teknolojileri altyapısının da sürekliliğini sağlamaktadır. Bu sebeple de BT sistemleri faaliyetlerinin sürekliliği için planlar oluşturulmaktadır.

İş sürekliliği planı, organizasyonun felaket ya da etki anından normal düzenine erişmesine yakın bir olaya tepkisini oluşturmak üzere bütünleştirilen belgeler setidir. Kurtarma ve iyileştirme eylemlerinden sorumlu olan herkes, kendi kurtarma planına göre çalışmaktadır. Bir kuruluşun iş sürekliliği planlama süreci aşağıdaki hedefleri yansıtmaktadır:

- İş sürekliliği planlama süreci yalnızca teknoloji bileşenlerini kurtarmak değil, işletmenin tüm yönlerinin iyileştirilmesini, sürdürülmesini ve bakımını içermektedir,
- İş sürekliliği planlaması, kurum çapında bir BCP'nin geliştirilmesini ve iyileştirme için gerekli olan iş hedeflerinin ve kritik operasyonların önceliklendirilmesini içermektedir,
- İş sürekliliği planlaması, kuruluşun piyasalardaki rolünün entegrasyonunu sağlamaktadır,
- İş sürekliliği planlaması, iş süreçlerindeki değişiklikler, denetim tavsiyeleri ve testlerden alınan derslere dayanılarak BCP'ye yönelik düzenli güncellemeleri içermektedir,
- İş sürekliliği planlaması, bir iş etki analizi (BIA), bir risk değerlendirmesi, risk yönetimi ve risk izleme ve testini içeren döngüsel, sürece odaklı bir yaklaşımı temsil etmektedir.

İş sürekliliği planlama süreci tüm işletmenin kurtarılması, yeniden başlatılması ve sürdürülmesini içermektedir. BT sistemlerinin ve elektronik verilerin restorasyonu önemlidir, ancak bu sistemlerin ve verilerin kurtarılması, işletme işlemlerini geri yüklemek için her zaman yeterli olmayabilmektedir.

İş sürekliliği planlaması, kurum çapında bir BCP'nin geliştirilmesini ve iyileştirme için gerekli olan işletme hedeflerinin ve kritik operasyonların önceliklendirilmesini içermektedir. Bu kurumsal çapta çerçeve, kritik süreçlerin, işletme biriminin, departmanın ve sistemin kesintilere nasıl cevap vereceğini ve hangi iyileştirme çözümlerinin uygulanması gerektiğini düşünmektedir. Bu çerçeve, kısa ve uzun vadeli kurtarma işlemleri için bir plan içermektedir. Kuruluşun tüm kritik unsurlarını göz önüne alan kurumsal çapta bir BCP olmadan bir kuruluş, müşteri hizmetlerini kabul edilebilir bir seviyede devam ettiremeyebilmektedir. Yönetim; maliyet, lojistik ve diğer öngörülemeyen koşullar nedeniyle tüm iş birimlerinin restorasyonu mümkün olmayabileceğinden, kuruluşun hayatta kalması için şart olan işletme hedeflerine ve kritik operasyonlara öncelik vermek durumundadır.

İş sürekliliği planlaması, kuruluşun piyasalardaki rolünün entegrasyonunu içermektedir. Kritik ve önemli piyasalardaki işlemlerin önemli bir kısmını işleyen kuruluşlar için takas ve uzlaştırma faaliyetleri yürüten sektör katılımcılarının, işleyişinin devam etmesini sağlamak için tasarlanan kurumlar arası yönergeleri izlemesi gerekmektedir. Bu yönergelere dayanarak kilit sektör katılımcılarının, bu kritik piyasaları destekleyen faaliyetleri tanımlamaları, kritik işlemleri zamanında geri kazanma ile sürdürme yeteneklerini sürekli olarak sürdürmeleri ve iyileştirme ile yeniden başlatma düzenlemelerini düzenli olarak kullanmaları veya test etmeleri beklenmektedir. Bu kuruluşlar, bir veya daha fazla kritik finans piyasasına katılır ve bunların iş gününün sonuna kadar kritik faaliyetleri yerine getirememesi finansal sistemler için sistemik bir risk oluşturabilir ve finansal piyasalardaki rolü iş sürekliliği planlama sürecinin bir parçası olarak ele alınmaktadır (U.S. Securities and Exchange Commission, Interagency paper on sound practices to strengthen the resilience of the U.S. financial system).

İş sürekliliği planlama süreci, BCP'ye yönelik düzenli güncellemeleri içermektedir. BCP, iş süreçlerindeki değişiklikler, denetim tavsiyeleri ve testten alınan derslere dayanarak güncellenmektedir. İş süreçlerinde meydana gelen değişiklikler, kabul edilebilir iş süreci kurtarma sürelerini azaltarak daha hızlı ve daha verimli bir işleme olanak tanıyan teknolojik gelişmeleri içermektedir. Rekabetçi pazar ve müşteri taleplerine yanıt olarak, birçok kuruluşu daha kısa kurtarma sürelerine doğru zorlamakta ve iş süreçlerine teknoloji kurtarma çözümleri tasarlamaktadır. Bu teknolojik gelişmeler kurumsal çapta bir BCP'nin korunmasının önemini vurgulamaktadır.

Mevcut bir BCP'yi korumak için yaygın olarak kullanılan ek endüstri uygulamaları ise şunları içermektedir:

- İş sürekliliği planlamasını her iş kararına entegre etmek,
- BCP sürdürme sorumluluklarını geçerli çalışanların görev tanımlarına ve personel değerlendirmelerine dahil etmek,
- BCP'nin periyodik gözden geçirme sorumluluğunu bir planlama koordinatörüne, departmanına, grubuna veya komitesine atamak,
- BCP'nin düzenli denetimi ve yıllık veya daha sık yapılan testlerin yapılmasıdır.

1.3. İş Sürekliliği Planlamasının Önemi

Genel olarak bir kuruluş için BCP'nin amacı, risk açığını tanımlamak, azaltmak ve olasılığı proaktif olarak yönetmektir. Diğer amaçlar ise hem bozulmanın kapsamı ve süresi hem de belirlenen olumsuz paydaş etkilerini azaltmaktır. İş sürekliliği planlaması, gevşek bilgi yönetimi kontrolleriyle ilişkili operasyonel riski azaltmaya yardımcı olan bir organizasyonel öğrenme çabasının bir parçasıdır. Bu süreç, bilgi güvenliği ve kurumsal risk yönetimi uygulamalarının geliştirilmesiyle bütünleştirilebilmektedir.

İş sürekliliği, iş gerçekleştirme biçiminin bir parçası hâline gelmektedir. İş devamlılığı olan organizasyonlar, önemli bir olayın etkisinden kurtulamayanlara oranla çok daha fazladır. Bir sorun oluştuğunda başa çıkmak zorunda kalmak yerine, her zamanki gibi faaliyetleri etkileyebilecek olayları planlamak daha kolaydır.

İş sürekliliği yönetimi (BCM), kuruluşun hayatta kalma ihtimalini tehdit eden büyük aksaklıklara yanıt vermesini sağlamaktadır. BCM, bir kuruluşun operasyonel kabiliyetinin bir bölümünü veya tamamını kaybetmesine neden olarak kilit paydaşların ve müşterilerin çıkarlarını, itibarını, markasını ve değer yaratan etkinliklerini zedeleyen olayları etkili bir şekilde yanıtlayan organizasyon çapında esneklik geliştirmektedir. Bir kuruluşun BCM direnci, yönetim ve operasyonel personelin yanı sıra teknolojik ve coğrafi çeşitliliğe bağlı olduğu için, bu esneklik tüm sitelerdeki ve tedarik zincirindeki üst düzey yöneticilerin organizasyonu boyunca geliştirilmektedir.

İşletme faaliyetlerini ve hizmetlerini kapsayan tüm kuruluş birimleri, ciddi bir planlanmamış olay meydana gelmesi durumunda kritik iş süreçlerinin devam etmesini sağlamak için BC planlarını geliştirmekte, sürdürmekte ve test etmektedir. İşlevler, bilgi varlıkları veya işleme yeteneği, bir organizasyonun süreçlerinin normal yürütülmesine zarar verebilecek bir kayıp veya arıza keşfinden sonra kurtarılmaktadır (University of Wollongong, 2005).

İş sürekliliği organizasyonlar için gelir devamlılığı sağlamaktadır. Herhangi bir iş sürecinin yüzde yüz kullanılabilirliği bugünün iş dünyasındaki standarttır. BCP, organizasyonun operasyonel olmasını engelleyecek en kötü duruma hazır olduğunu garanti etmektedir. İyi düşünülmüş bir BCP, kuruluş için herhangi bir olaya ya da krize uymaktadır. En kötü senaryo için hazırlanmak önemlidir. Planın karmaşık olması gerekmemekte ve her olasılığı veya her iş sürecini değil, en kritik olanları kapsaması yeterli gelmektedir (Mellish, 2008).

BCP çoğu sektörde kök salmaktadır. Tartışmasız olarak her organizasyonun kuruluş ömrünü garantilemek için bir tane BCP el kitabı olması gerekmektedir. Felaketten sonra hayatta kalma istatistiklerinde kuruluşların BCP hazırlıklarına yeterli zaman ve kaynak sağlamadığı açıktır. 1993 Dünya Ticaret Merkezi'nin bombalanmasında, 350 etkilenen kuruluştan 150'si olaydan sağ kurtulamamıştır. Katı bir BCP'yi yerine getirmeyen ve büyük veri kaybı yaşayan kuruluşlar üzerinde yapılan bir çalışmada, kuruluşların yüzde 43'ü hiçbir zaman yeniden açılamamıştır, yüzde 51'i iki yıl içinde kapatılmıştır ve uzun vadede sadece yüzde 6'lık kısmı hayatta kalabilmiştir. Diğer bir deyişle, kuruluşların sadece yüzde 6'sının uzun vadede hayatta kalması beklenmektedir. Bu büyük veri kaybı yaşayan şirketler için yüzde 94'lük bir ölüm oranı anlamına gelmektedir. 11 Eylül saldırılarından etkilenen, iyi hazırlanmış ve test edilmiş BCP el kitapları olan kuruluşlar birkaç gün içinde işlerine geri dönmüştür (Haag, Cummings ve Mccubbrey, 2005).

BCP, kuruluşların güvenlik açıklarının temel alanlarını koruyarak yıkıcı olayların üstesinden gelmelerine yardımcı olur ki bunlar:

- Personelin kaybolması veya yaralanması,
- Kuralların ve düzenlemelerin önemsenmemesi,
- Gelir kaybı,

- Kritik kaynaklarda hasar,
- Müşteri kaybı,
- Sivil ve cezai yükümlülükler,
- Şöhretin zarar görmesidir (Syed ve Syed, 2004).

İş sürekliliği (BC), iş için esneklik inşa etmek ve geliştirmektir; temel ürün ve hizmetleri tanımlamak, bunları destekleyen en acil etkinlikleri belirlemek ve daha sonra analiz tamamlandıktan sonra işletme faaliyetlerine devam edilmesini ve hızlı bir şekilde iyileşmesini sağlayacak planlar ve stratejiler tasarlamaktır. BCP, kriz dönemlerinde yaslanmak için sağlam bir çerçeve sunmakta, istikrar ve güvenlik sağlamaktadır (Business continuity institute, What is BC?).

Çizelge 1.2. İş Sürekliliğinin Paydaşlara Fayda Tablosu (Marsh Danışmanlık, 2010)

Kime	**Ne Kazandırır**
Müşterilere	İşletmeden her durumda ürün/hizmet alınacağına dair güvence
Hissedarlara	Şirket değerinin korunması
Üst Yönetime	Rekabet avantajı
	Şirket itibarının 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 kuruluşun varlığına devam etmesi
	Kriz anında sorumlulukların doğru şekilde paylaşılması
Tedarikçilere	Güvenilir iş ortaklığı

Etkili bir BCP, sadece finansal felaketlere karşı işletmelerin güvenliğini sağlamakla kalmaz, aynı zamanda operasyonlar beklenmedik şekilde kesildiğinde iş süreçlerini korumak ve iyileştirmek için işletmelerin temelini oluşturur. Bu durum, müşteri memnuniyetini ve gelişmiş kurumsal imajı garanti eder ve pazar payında herhangi bir düşüş yaşanma ihtimalini ortadan kaldırır. BCP, bir organizasyonun risk maruziyetlerini belirleme ve azaltma, kontrolü yönetme ve operasyonların kesintisiz ve sürekli çalışmasına hazırlamak için kritik önem taşıyan tüm iş süreçlerini içeren iyi belgelenmiş ve

doğrulanmış proaktif risk yönetimi planı oluşturmak için kullanılan bir yöntemdir. Afetler ve yıkıcı olaylar öncesi, sırası ve sonrasında, iç kontrolde ve fiziksel güvenlikte herhangi bir kusura bakılmaksızın zamanında ve düzgün bir şekilde yeniden başlatma prosedürlerinin uygulanmasıyla birlikte, tehditlere karşı sürdürme faaliyetleri, tüm personelin sağlık ve güvenliğini sağlamak BCP'nin hedefleridir.

İş sürekliliği planlaması (BCP), bir organizasyonun beklenmedik felaketler, aksamalar ya da değişiklikler yaparak hayatta kalmaya hazırlanıp kritik iş süreçlerinin olumsuz koşullarda kabul edilebilir sınırlamalarla işlev görmeye devam edeceğini güvence altına almaktadır. BCP, ayrıca bilgi güvenliği yönetiminin alanlarından biridir. Standartlar tarafından bir organizasyonun belirsizlik dünyasındaki yükümlülüklerini yerine getirmek için bir iş sürekliliği (BC) programı olması gerektiğini vurgulamıştır. Temel hedefler; olağandışı durumlarda işletmeyi hayatta tutmak, mevzuata uygunlukları sürdürmek, ürün ve hizmetlerini çalışanlarına, müşterilerine, satıcılarına ve genel olarak topluma minimum kayıp ile sunmaktır (Dey, 2011).

İş sürekliliği planlaması, kesintiler sırasında kritik hizmetlerin veya ürünlerin teslim edilmesini sağlayan proaktif bir planlama sürecidir (Office of Critical Infrastructure Protection, 2003). Siber saldırılardan doğal afetlere ve insan hatasına kadar değişen risklerle, kuruluşların sağlık ve itibarını korumak için bir iş sürekliliği planına sahip olması hayati önem taşımaktadır. Uygun bir BCP, maliyetli bir kesinti olasılığını azaltmaktadır.

Her kuruluş aşağıdakileri içeren olası felaketlerden dolayı risk altındadır:

- Kasırga, sel, kar fırtınaları, depremler ve yangın gibi doğal felaketler,
- Kazalar,
- Sabotaj,
- Güç ve enerji kesintileri,
- İletişim, ulaşım, güvenlik ve hizmet sektörü arızası,
- Kirlenme ve tehlikeli maddeler gibi çevresel felaketler veya
- Siber saldırılar ve bilgisayar korsanlığı etkinliği.

BCP oluşturmak ve devam ettirmek, bir kuruluşun bu acil durumlarla başa çıkması için gerekli kaynaklara ve bilgilere sahip olmasını sağlamaya yardımcı olmaktadır. BCP'ye

sahip olmak, bir organizasyonun imajını çalışanlar, hissedarlar ve müşterilerle proaktif bir tutum sergileyerek geliştirmektedir. BCP ek olarak, genel organizasyonel etkinliğin iyileştirilmesini ve varlıkların, insanların ve finansal kaynakların kritik hizmetlere ve çıktılara olan ilişkisini tanımlamayı içermektedir (Office of Critical Infrastructure Protection, 2003).

İyi geliştirilmiş bir BCP paketi, süreç boyunca BC planlayıcılarına rehberlik ederek, planların üretilmesi ve sürdürülmesini önemli ölçüde daha verimli hâle getirmektedir. BCP, herhangi bir boyutta organizasyon için paha biçilemez bir araçtır; çünkü bir felaket durumunda kurumun mevcut hazır olma durumunun bir anlık görüntüsünü sağlamaktadır (Hanwacker, 2010).

1.3.1. Planlama maliyeti ve başarısızlık maliyeti karşılaştırması

Kuruluşlar genel olarak üst çizgi ve alt çizgisine (kârlılık) bakmaktadır. Birçok kuruluş, üst düzey büyüme ve satır geliri kovalamaktadır, bu durum da agresif olarak gelirleri arttırma isteğini tetiklemektedir. Bu istek de şirketlerin, sıklıkla pazarın daha büyük bir bölümünü kaptıkları veya piyasayı genişletmek için zorladığı anlamına gelmektedir.

Planlama maliyeti; personel zamanı, kaynak ve benzerleri bakımından önemli olabilmektedir ve şirketlerin alt çizgisini, birçok faktöre bağlı olarak etkileyebilmektedir. Kuruluşlar yalnızca üst düzey büyüme ile ilgili olduklarında, BC/DR proje planının maliyetiyle aşırı derecede ilgilenmeyebilmektedir. Fakat kilit müşteriler, şirketlerin böyle bir plana sahip olmasını arzulayabilmekte veya talep edebilmektedir. Bu yüzden bu planın yaratılmasının üst düzey bir büyümeye katkıda bulunabileceği savunulabilmektedir. Şirketlerin bir BC/DR planı olduğu için yeni bir müşteri yakalayabilmektedir. BCP'ye kuruluşlarda operasyonel verimlilik artacaktır veya çalışanlar tarafından yeni bir müşteri arayışı başlayacaktır. Bunun ötesinde, bir BC/DR planı olmadan bir felaket yaşandığı durumda, alt çizgiye gelebilecek potansiyel hasarlar belirlenmek durumundadır. Bununla birlikte, felaketin etkisini hafifletmede yaşanacak başarısızlığın, kuruluşların hem üst hem de alt satırlarını etkileyeceği ve kuruluşların varlığını tehlikeye atacağı bir gerçektir. Planlama maliyeti başarısızlık maliyetiyle karşılaştırıldığında, işi mantıklı kılan tek bir

yaklaşım vardır ve bunu gerçekleştirmek için mali açıdan mantıklı bir ölçüt planlanması gerekmektedir.

Felaketler büyük mali kayıplara, yatırımcıların güvenine ve kurumsal imajın düşüşüne neden olabilmektedir. Ayrıca, özellikle kamuya açık internette daha fazla özel veri yakalanmakta, depolanmakta ve iletilmekteyken ciddi hukuki sorunlar ortaya çıkabilmektedir. Bu kayıplar ve yasal zorunluluklar, küçük ancak kısa vadeli bir etkiye sahip olabilmektedir; fakat bazı durumlarda önemli, uzun vadeli bir etkiye sahiptir ve şirketin varlığını tehlikeye atmaktadır.

Bir çeşit felaket planı olan kuruluşlar büyük olasılıkla BT departmanı merkezli çalışmakta ya da BT yapısını önemsemektedir. BT personeli, bir sunucunun bile kesintiye uğramasının ticari anlamlarını çok iyi anlamışlardır. Bununla birlikte açıktır ki, BT ekipmanı-yönlendiriciler, sunucular, anahtarlar, merkezler, güvenlik duvarları ve daha fazlası sadece genel ticari denklemin bir parçasıdır. Elbette bu teknoloji bileşenleri olmadan her zamanki gibi kuruluşlar eninde sonunda sınırlı olacaktır. Ek olarak, kuruluşların gelir kazanma ve işini yürütme şekli dikkate alınmaksızın, bir felaket söz konusuysa, dünyadaki hiçbir BT planı bir kuruluşu korumamaktadır. Herhangi bir iş sürekliliği ve felaket kurtarma planlamasının gerçekçi ve etkili olabilmesi için işe bütünsel bir yaklaşım gereklidir. Bu, kuruluşların her önemli alanını ve bu iş birimlerini temsil eden çeşitli paydaşları içermektedir. Depo operasyonları kesintiye uğradığında, web sitenin e-ticaret işlevlerini yerine getirebilmesi kuruluşlara yardımcı olamaz.

Çoğu BT departmanı bazı küçük felaket kurtarma prosedürlerine sahiptir. Basit olarak, kuruluşlar kritik verilerin yedeklerini sunucularda gerçekleştiriyorsa ve bu yedeklemelerin yerinden alınması veya uzaktan saklanması (veya gerçekleştirilmesi) varsayılarak temel felaket kurtarma yeteneklerine sahip olabilmektedir. Bunun çok basit olduğu düşünülse de birçok kuruluşun (ve BT uzmanlarının kendisi) ya yedekleme yapmakta başarısız oldukları ya da güvenli bir yerde depolamayı başaramadıkları bilinmektedir. Bununla birlikte çoğu küçük, orta ve büyük şirketlerin en azından makul bir veri yedekleme çözümü bulunmaktadır. Bu, kendi içinde iyi bir başlangıçtır ancak BC/DR planını teşkil etmemektedir.

Felaket planlaması bir olaydan sonra kurtarmadır, ancak iş sürekliliği planlaması sadece anahtar teknik bileşenlerin kesintilerinden kurtulmakla kalmaz ve ek olarak işe bakmak ve yönetmek için bir yöntemdir. BCP, ileriye bakmak, kuruluşların operasyonlarını potansiyel olarak aksatacak durumları görmek ve daha sonra bu olayları hafifletmek veya önlemek için yollar bulmaktır. Gerçekten de BCP, tüm kuruluşu ve operasyonları kapsayan koordine edilmiş ve entegre bir yaklaşımdır. Yaşamın herhangi bir alanında olduğu gibi, bir veya iki zayıf karar genellikle düzeltilebilmekte veya bu kararın üstesinden gelinebilmekte, ancak işler stresli hâle geldiğinde bir dizi zayıf kararlar kelimenin tam anlamıyla kuruluşlar için felakete yol açabilmektedir. BC/DR planlamanın amacı: Kaçınılması gereken tuzaklardan kaçınmaya ve bir olay meydana geldiğinde felaketi yönetmeye, rasyonel ve iyi düşünülmüş bir yaklaşım sağlamaya yardımcı olmaktır. Sorunların çözümünü sağlayabilmek ve daha hızlı ve nispeten iyi bir şekilde kuruluşların hayatına devam edebilmesi, zayıf kararların sayısının en düşük seviyede tutulabilmesine bağlıdır (Laye, 2002).

Çalışmalar, bir plan yaratmanın zaman ve masraflarının herhangi bir ters yüz dönüşünden çok daha fazla olacağı yönünde yaygın olarak yapılan yanlış kavramları işaret etmektedir. Birçok BC/DR planlama faaliyetleri nispeten hızlı bir şekilde ve çok az veya hiç fonlamadan başarılabilmektedir. Acil durum planlamaya ihtiyaç duymadığını düşünen kuruluşların yüzde 12'si, acil bir durumla karşılaştıklarında kuruluşun işin içinden çıkma olasılığının olmadığını düşünmektedir.

Acil durumların ve felaketlerin uzun vadeli etkilerinden en çok etkilenen kuruluşların, iş sürekliliği ve felaket kurtarma planlamasını önleme, geciktirme veya kısaltma olasılıkları daha yüksektir. Kuruluşlar boyutundan bağımsız olarak, doğal veya insan yapımı herhangi bir felaket ile karşı karşıya kaldığı durumlarda, yüzde 40 ila yüzde 50 arasında işlerini terk etmek zorunda kalmaktadır. Kuruluşların, sektörlerin ve diğer faktörlerin gücü, felaketlerle vurulan kuruluşların uzun vadeli sağ kalımlarına bakmaktan gelmektedir. Fakat kuruluşların bir iş sürekliliği ve felaket kurtarma planı yoksa başarısızlık ihtimalleri yüzde 50 artmaktadır. İyi tasarlanmış bir iş sürekliliği ve felaket kurtarma planı olmadan, bu çok büyük bir kumar olacaktır. Bu olasılıklar sadece kuruluşların kendisini değil, aynı zamanda tüm çalışanların ve tedarikçilerin hayatlarını da etkilemektedir. Dalgalanma etkisi büyük olabilmekte ve toplumun geri kalanını ve ailelerini de etkilemektedir.

Planlama maliyeti, hiçbir şey yapmamanın bedeli ve işten çıkma riski ile dengelenmek durumundadır. Sonuçta bir plan olmadan felaketle yüzleşmekten ziyade, planı oluşturmak ve sürdürmek için uygun ve orantılı miktarda zaman ve kaynak harcamak daha az pahalıdır. Diğer taraftan kötü ya da tamamlanmamış plan, genelde hiçbir plan yapmamaktan daha kötüdür. Yanlış bir güvenlik duygusu, felaket olayının kendisinden daha büyük sorunlara yol açabilmektedir. Çalışanların yanlışlıkla kuruluşların felakete hazır olduğuna inanması pek çok probleme yol açabilmektedir. Kötü tasarlanmış bir plan önemli mali cezalara ve yasal yükümlülüklere neden olabilmektedir (Snedaker, 2007).

İnsanlar

Acil durum yanıtlarını planlamak için zaman ve kaynakları bir organizasyon açısından harcamak birçok nedenden ötürü mükemmel bir yatırımdır. Etkisi hemen ortaya çıkmayan faydalardan biri, çalışanların kuruluşun ihtiyati olma planları olduğunu anladıklarında, şirketin örgütlendiğini, başarı için konumlandıklarını ve güvenliklerinden endişe duymadıklarını ortaya koymaktır. Kuruluşların, çalışanlarının esenliği konusundaki taahhüdünü göstermesi, kilit çalışanları korumaya yardımcı olabilecek bir fırsat sunmaktadır. Sürekli geçici personelle çalışan kuruluşlar aynı nedenden ötürü kilit çalışanları kaybetme riskiyle karşı karşıya kalmaktadırlar. Katı bir BC/DR planı çalışanları mutlu tutmak amacını gütmemektedir. Fakat bu sistematik, çalışanların refahı için saygı artırmayı ve endişeyi azaltmayı teşvik eden genel bir ortama katkıda bulunur. Buna ek olarak kuruluşlar tarafından iyi yönetilen bir krizin, kilit çalışanların başka istihdam olanaklarını görmezden gelmelerini sağladığı ortadadır. İyi yönetilen bir etkinlik aynı zamanda kuruluşların itibarını artırmakta, kuruluşları olay öncesi durumdan daha güçlü duruma getirmekte, çalışanların sakin ve odaklı olmasını sağlamaktadır.

Acil durumlarda stresin insanlar üzerindeki etkisi yeterince önemsenmemektedir. İyi düşünülmüş ve iyi provalı bir BC/DR planına sahip olmak, bu stresi önemli ölçüde azaltmaktadır. Böylece insanlar tekrar işlev görebilmekte ve işlerine daha çabuk dönebilmektedirler. Bu nedenle, acil durumlarda kuruluşlardaki insanlara nasıl davranılacağını planlama eylemi, kuruluşların normal operasyonlara dönme kabiliyetini hızlı bir şekilde etkileyebilmekte ve gelir yaratılmasına katkı sağlayabilmektedir. Böylece BC/DR planlama, doğrudan üst ve alt satırı etkilemekte ve planlama maliyeti, yönetilmeyen bir etkinliğin maliyetini hızla dengelemektedir (Snedaker, 2007).

Süreç

BC/DR planlama, kuruluşların iş süreçlerini değerlendirip iyileştirmesi için fırsatlar sağlayabilmektedir. Proje ekipleri iş süreçlerini BC/DR ile ilişkili olarak değerlendirmekte, işlemleri düzene sokmanın yeni yollarını keşfedebilmektedir. Doğal veya insani bir felaketten ötürü büyük bir aksaklığın planlanmasında proje ekipleri en düşük gereksinimleri belirlerken yeni yöntemler ortaya çıkarabilmektedir. Bir süreç deneyimlendiğinde bir sonraki benzer senaryo için düşünülmesi gereken planlama adımları kısalacaktır. Her şeye (bir felaketle uğraşırken yaşananlara) bakmak zorunda kalındığında, bütün tepki sistemlerine ihtiyaç olmadığı fark edilecektir. Bu deneyim, bazen basitleştirilmiş süreçlere tercüme edilebilmekte ve günlük işlemlere dahil edilebilmektedir. Buna ek olarak, kritik iş süreçlerini belgelemek, gerçek anlamda kuruluşların varlığı için yaşam ve ölüm arasındaki fark anlamına gelebilmektedir. Bir felaketten sonra makul bir zaman diliminde bir takım işlemler tekrar başlatılamadığında, kuruluşların hayatta kalması muhtemel değildir. Bu durumda maliyet nihai kurumsal başarısızlık olabilmektedir. Bu sadece kurumsal pay sahipleri için değil, aynı zamanda şirketin çalışanlarının ve ailelerinin hayatları için de talihsizliktir ve dalgalanma etkisi düşünülenden çok daha fazla olmaktadır (Snedaker, 2007).

Teknoloji

Felaket olduktan sonra teknoloji konularıyla uğraşmaya çabalamak, sağlam bir plana sahip olunmasından daha maliyetli bir uğraştır. Örneğin geçici bilgi işlem tesislerine ihtiyacınız varsa, önceden hazırlanmış bir acil durum sözleşmesi yapmak, çeşitli imkanları umutsuzca aramaktan daha az maliyetlidir. Buna ek olarak felaket diğer kuruluşları da etkilediğinde, aynı zamanda teknoloji bileşenlerini fiyatlandıran rekabetçi bir durum oluşturabilmektedir. Yine; acilen acil servisler için sözleşme görüşmelerini sakin bir şekilde yapmak ve temin etmek, acil bir durum söz konusu olduğunda bu sözleşmelerin etkinleştirilmesi durumundan hemen hemen daha düşük maliyetler üretmektedir (Snedaker, 2007). Kuruluşlar bilgi teknolojisi (BT) altyapısına daha fazla bağımlı hale geldikçe iş kesintileri riskleri ve maliyetleri artmaktadır. İş sürekliliği planlaması için kapsamlı bir

yaklaşım, iş sistemlerinin tüm önemli iş kesintilerine karşı hafifletmeyi amaçlamaktadır (Cerullo ve Cerullo, 2004).

1.3.2. İş kesintilerinin finansal etkileri

Bir iş kesintisinin maddi etkisi önemli ve uzun süreli olabilmektedir. Geçtiğimiz birkaç yılda veri güvenliği ihlallerinden kaynaklanan aksamalar, kurtarma maliyetleri ve yasal ücretlerde milyonlarca dolara mal olmuştur. Tam rakamlar mevcut değildir, ancak anekdot kanıtları birçok kuruluşun yaşadığı veri kayıplarının ardından acil hizmetler, kurtarma hizmetleri ve altyapı eksikliğinin bir sonucu olarak dibe girdiğini açıkça göstermektedir.

Nakit akışı çoğu birey için olduğu gibi kuruluşların da can damarıdır. Nakit akışı hesaplarında kısa vadeli çözümler sürdürülebilir değildir. Bu mali modeli kullanmanın sonu gerilemektir ve bu durum şahıslar ve kuruluşlar için de geçerlidir. Her gün, hafta veya ayda şirketler gelir elde etmektedir. Aynı zaman aralıklarında, çalışanların bordrosu, sağlık sigortası, işletme sigortası, kira, kamu hizmetleri, seyahat masrafları, sarf malzemeleri ve daha fazlasını içeren giderleri bulunmaktadır. Kuruluşların giderleri gelirlerini aştığında ek bir kaynak bulmaları gerekmektedir. Kuruluşlar için bu, bankada duran ve gelirlerin masrafları aştığı zamanlarda biriktirdikleri nakit yastığı olabilmektedir. Diğer durumlarda kuruluşlar, bir bankadan faizle geri ödemesi gereken bir krediyi kullanabilmektedir. 30, 60 veya 90 gün için faturaları ödemeyi geciktirmek için kilit satıcılarla olan kredi şartlarına güvenilebilmektedir. Eğer kuruluşlar yeni ülkelere açılma veya yeni tesisler kurma gibi olağandışı giderlere sahip olacağını önceden bilebilirse, bankalardan, finansal kuruluşlardan veya yatırımcılardan kredi alabilecek, hisse senedi veya tahvil satabilecektir (şirket tipine bağlı olarak). Bunların çoğu, kuruluşların mevcut nakit akışları yoluyla önemli bir büyümeyi finanse edememesi nedeniyle, büyüme için sermaye artırmasına izin veren uzun vadeli finansal stratejilerdir. Bununla birlikte, bu borca dayanarak yeni veya daha büyük gelir akışları üretebilecek ve böylece karlı kalacak ya da hatta daha kârlı hale gelecektir. Kuruluşların genellikle bir dereceye kadar tahmin edebilecekleri gelirleri bulunmaktadır. Beklenen gelir akışlarına dayalı olarak giderleri yönetmektedirler. Bir felaket, veri güvenliği ihlali, bir kasırga veya bir kimyasal saçıntı olsun isabet ettiğinde, kuruluş gelirlerinde bir düşüş yaşanmakta ve giderlerde artış olmaktadır (Snedaker, 2007).

1.4. İş Sürekliliği Planlaması (BCP) ve İş Sürekliliği Yönetimi (BCM) İlişkisi

İş sürekliliği, yıkıcı bir olayı takiben, organizasyonun ürün veya hizmetlerinin kabul edilebilir önceden tanımlanmış seviyelerde verilmesine devam etme kabiliyeti olarak nitelendirilmektedir. İş sürekliliği planlaması (BCP), kesintileri takiben kuruluşlara önceden tanımlanmış bir operasyon seviyesine yanıt vermeye, iyileştirmeye, devam ettirmesine ve geri yüklemesine rehberlik eden belgelendirilmiş prosedürleri ifade etmektedir. Tipik olarak bu, kritik iş fonksiyonlarının sürekliliğini sağlamak için gereken kaynakları, hizmetleri ve faaliyetleri kapsamaktadır. İş sürekliliği yönetimi (BCM), başlıca paydaşlarının itibarlarını, menfaatlerini koruyan ve etkili bir cevap verme olanağı sağlayan örgüt çapında bir disiplindir ve bir organizasyonu tehdit eden potansiyel etkileri tanımlayan eksiksiz bir süreçler grubudur (International Organization for Standardization, 2012).

Literatürde, bir organizasyonun genel BCM sistemi içerisinde iş sürekliliği planlamasının önemli bir kurucu süreç olarak önemi veya gerekliliği hakkında bazı tartışmalar bulunmaktadır. Çoğunluk, hazırlık ve ön planlamanın bir organizasyon krizden kurtulduğunda kritik iş süreçlerinin devam ettirilmesinde kilit önem taşıdığına ilişkin görüş bildirmektir (Botha ve Solms, 2004). Krizde olumlu veya olumsuz bir sonuç çıkma ihtimali yarı yarıyadır ve iş sürekliliği planlamasının olumlu olasılıkları artıracağını ileri süren görüşler de bulunmaktadır (Fink, 1986).

BCM süreci boyunca iş sürekliliği planlamasının hazırlanması ve sürekli geliştirilmesinin önemi ile merkeziyetçilik bakımından önemi vurgulanmaktadır. İş sürekliliği planlaması ile ilgili olarak aşağıdaki adımlar önerilmektedir:

- Bir plan geliştirmek,
- Kişilerin ve ekiplerin gerekli uzmanlığa ve kaynaklara sahip olmasına dikkat etmek,
- Performansı incelemek ve plan için gerekli düzenlemeleri yapmak (Lindell, Prater ve Perry, 2007).

Kuruluşların itibarını, markasını ve değer yaratan faaliyetlerini korumak açısından BCM ve BCP savunulmaktadır. Etkin BCM'nin önemli ödüller sunduğunu ve iş

bakımından zenginlik yarattığı söylenmektedir. Copenhaver ve Lindstedt (2010) ve Gosling ve Hiles (2008), BCP'nin faydalarının geleneksel varsayımlarına ve iddialarına karşı olduğunu belirtmiştir ve çok fazla vaka incelemesinin olduğunu ve değeri için yeterli delil olmadığını söylemiştir. Copenhaver ve Lindstedt (2010) daha ileri araştırmaların BCP etkililiğini belirlemede garanti edildiğini söylemektedir. BCP ve BCM'nin önemi konusundaki görüş farklılıkları, göreceli olarak yeni bir iş disiplini olması nedeniyle olabilmektedir.

1.5. İş Sürekliliği Yönetimi (BCM)

İş sürekliliği yönetimi potansiyel teknoloji kayıplarının etkisini belirlemek, acil durum veya felaket durumunda iş hizmetlerinin sürekliliğini garanti eden iyileştirme planlarını geliştirmek ve test etmek ile kapsamlı bir eğitim, test ve sürdürme gerçekleştirmek için gerekli olan önceden planlama ve hazırlıklar programı olarak tanımlanabilmektedir (IT Governance CEN 667, 2012).

BCM ve BC işlemleri, kuruluşun birlikte bir iş sürekliliği planı geliştirmesini, bunu sürekli olarak hazır durumda tutmasını ve bir bozulma durumunda onu yürütmesini sağlamaktadır. BCP yönetimi, BCP'nin yönetim ve organizasyon bileşenlerine odaklanmaktadır. BCP yönetiminin kilit faaliyetlerinden bazıları aşağıda listelenmiştir:

- Yönetimi yönlendiren, organizasyon çapında iş sürekliliği politikası çıkarmak ve kritik sürekliliğin sağlanmasından sorumlu olmak için her bir iş biriminin personeli, iş fonksiyonları ve süreçleri hakkında bilgi vermek,
- Üst yönetimin üyelerini tanımlamak için bir yönlendirme komitesi oluşturmak,
- BCP kapsamı, devam eden BCP destek ve yönünü sağlamak, BCP durumunu izlemek ve ilerleme kaydetmek ve BCP finansmanını tahsis etmek,
- Tüm organizasyonu kapsayan bir iş sürekliliği planı geliştirmek için resmi bir proje başlatmak,
- İş sürekliliği planının geliştirilmesi ve uygulanmasına katılan personelin yeterince eğitildiğinden emin olmak ve tüm kuruluş için bir BCP bilinirliği ve eğitim programı geliştirmek ve uygulamak,
- BCP'nin ilgili hükümet yasalarına, yönetmeliklerine ve endüstri standartlarına uygun olmasını sağlamak,

- BCP faaliyetlerini ilgili felaket kurtarma ve iş sürekliliği ajansları ile yerel yetkililerle koordine etmek,
- İş sürekliliği planının her zaman hazır bulunmaya devam ettiğinden emin olmak,
- Felaket anında iş sürekliliği planını yürütmek (Syed ve Syed, 2004).

Herbane (2010), BCM'nin bir örgütün kriz yönetim değerlerinin ve uygulamalarının 2000'lerin başında geliştirilen standartlarla ifade edilmesiyle resmi bir yapı olarak kurulduğunu belirtmektedir. BCM sürekli iş süreçlerini sağlamaya odaklanmaktadır ve kuruluşların aksamadan sonra kurtarma yeteneğinde belirgin bir rol oynamaktadır. BCM devam eden bir süreçtir ve bunun için planlama DR, işyeri kurtarma, iş yeniden başlatma ve acil durum planlamasını içermektedir. Bu nedenle BCM'nin kapsamlı ve devam eden doğası, herhangi bir BCM tanımının parçası olarak dahil edilmek durumundadır.

Elliott, Swartz ve Herbane (2010) tarafından yürütülen araştırmalar, BCM'ye bir kriz yönetimi yaklaşımı benimsemesini önermektedir. BCM sürecini, sıklıkla yıkıcı bir olayın parçası olan ve toplumsal öğeleri içerecek şekilde genişletmeyi ve kuruluşların çoğu zaman başarısızlıklarına engel olan bir rol oynamasını sağlamayı önermektedirler. Ayrıca bir organizasyonun yöneticilerinin BCM'de oynadığı rolün önemine, aksamaların bir organizasyonda birçok paydaş üzerinde etkili oluşuna ve düzgün yönetildiği takdirde olayların kaçınılmaz olarak bir krize neden olmadığı gerçeğine dikkat çekmektedirler. Bu, daha geniş tedarik zincirinin ve tüm organizasyon paydaşlarının hem içerde hem de dışta bir BCM tanımında olması gerektiği anlamına gelmektedir.

Bilgi teknolojileri altyapı kütüphanesi (ITIL) ve BT hizmet yönetimi çerçevesi, BCM'nin işle ilgili riskleri yönetmenin sorumlu olduğu ve önemli paydaşların, kurumsal itibarın, markanın ve kuruluşların menfaatlerini, değer yaratma faaliyetlerini koruduğunu söyleyen alternatif bir risk yönetimi görüşü sunmaktadır. ITIL tanımında, BCM'nin riskleri kabul edilebilir seviyeye düşürmeye yardımcı olduğuna da dikkat çekmektedir. ITIL temelde teknoloji odaklı bir süreç olduğu için ITIL tanımının iş odaklılığına dikkat çekmek ilgi çekici olmaktadır. ITIL tanımı, BCM'nin odağını teknoloji ve iş dünyasına ve paydaşlarına kaydırmaktadır.

Basel bankacılık gözetim komitesi, finansal ve iş odaklı bir yaklaşımla BCM'yi, kesintili bir durumda, belirli operasyonların zamanında muhafaza edilebilmesi veya düzeltilebilmesi için politikalar, standartlar ve prosedürleri içeren bir bütünsel işletme yaklaşımı olarak tanımlamaktadır (Basel Committee on Banking Supervision, 2006).

İş sürekliliği yönetimi, bir işletmenin bir iş kesintisini yönetmesine yardımcı olmak ve varlıkların esnekliğini oluşturmak için politikaların, çerçevelerin ve programların geliştirilmesi, uygulanması ve sürdürülmesidir. Bu, yıkıcı bir olayın önlenmesinde, hazırlanmasında, yanıt alınmasında, yönetilmesinde ve iyileştirilmesinde yardımcı olabilme kabiliyetidir. İş sürekliliği yönetimi, bir olayın olumsuz sonuçlarını değerlendirmekte ve fayda ve kazanç için fırsatlar yaratabilmektedir. Kararsız bir olayın olumlu bir şekilde tepki verdiği kuruluşlar, kendilerini hızlı bir şekilde iyileştirmek ve uzun vadeli işletme performansını iyileştirmek için kendilerini konumlandırabilmektedir. İş sürekliliği yönetimi, varlığın normale dönmesi ve iyileşmesi için atacağı adımları hazırlamaktadır. BCM; tek başarısızlık noktalarını sınırlamak, destek alanı ve iş birimi acil durum planlarını ve iş yeniden başlatma planlarını geliştirmek için iş süreçlerini ve bilgi mimarisini tasarlamayı içermektedir. Ayrıca, tırmanış prosedürlerini tanımlamak, kilit personel ve önemli bir bağımlılığın bulunduğu diğer kuruluşlar için irtibat bilgilerini elde etmek de buna dahil edilmektedir.

İş devamlılığı, önemli bir iş kesintisi sonucu olan bir risk oluştuğunda başlatılmaktadır. Bu yıkıcı olaylar düşük frekanslı olabilir, ancak varlık için ciddi sonuçlar doğurmaktadır. İş kesintisi olayları, sistem bağlantısının durması veya kısa bir iletişim hatası kaybı gibi normal işlemlerin bir parçası olarak oluşabilecek arızalardan kaynaklanan diğer kesintilerden ayırt edilmek durumundadır. Bir iş kesintisi, normal operasyonel yönetimin askıya alındığı bir olaydır (Australian National Audit Office, 2009).

BCM'nin temel amacı, kuruluşların olumsuz koşullar altında faaliyetlerini, esnek risk stratejileri, kurtarma hedefleri, BCM ve kriz yönetimi planlarını entegre bir risk yönetim girişimi ile işbirliği içinde veya önemli bir bileşen olarak uygulayarak yönetmelerine izin vermektir.

BCM'nin önceki tanımlarının kapsadığı çoklu unsurları içeren en kapsamlı tanımın İngiliz Standartları Enstitüsü (BSI) tarafından öne sürüldüğü belirtilmektedir: Bir

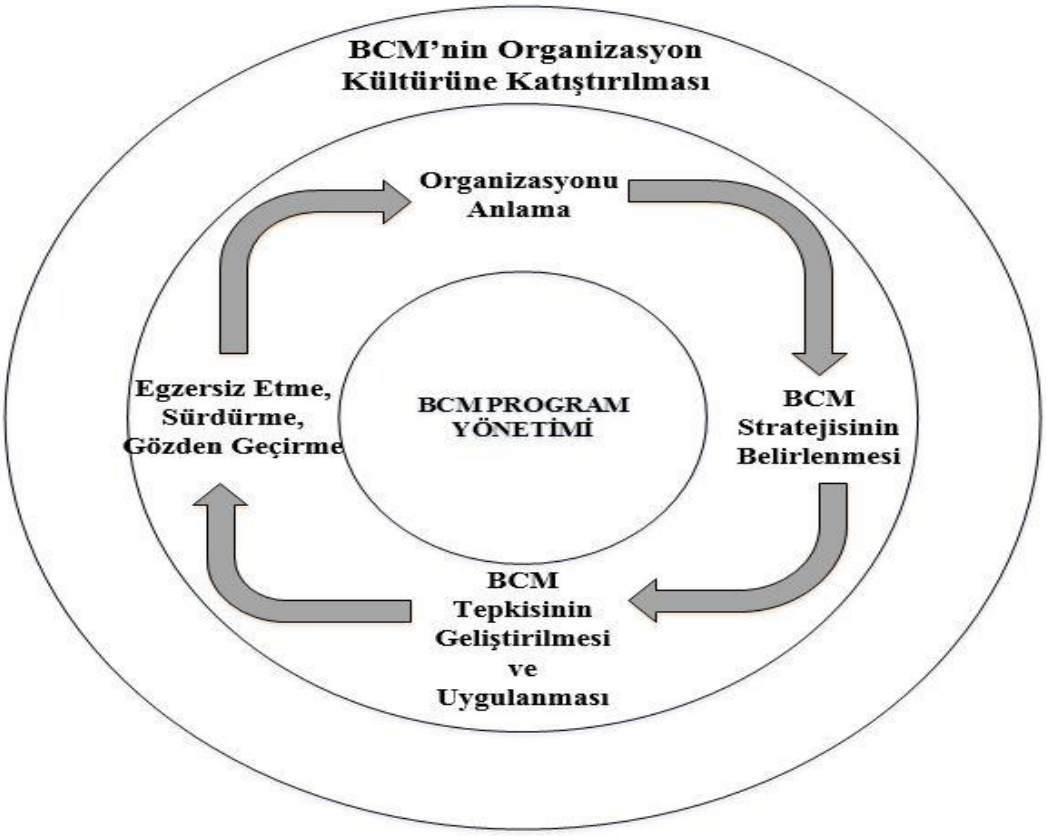
organizasyona olası tehditleri tanımlayan bütüncül yönetim süreci ve gerçekleştiğinde söz konusu tehditlerin sebep olabileceği işletme faaliyetlerine olan etkileri, kilit paydaşların, itibarın, markanın ve değer yaratma faaliyetlerinin menfaatlerini koruyan etkin bir tepki verme kabiliyeti ile örgütsel esneklik oluşturmak için bir çerçeve oluşturabilmektir (British Standards Institution, 2006). Bu tanım, BCM'nin yıkıcı olaylara genel olarak organizasyonel esneklik temelli bir yaklaşım inşa etmenin bir parçası olduğunun farkındadır ve yıkıcı bir olaydan sonra işe yeniden başlama, işin kritik unsurlarının hayatta kalması, işin yeniden başlatılması gibi daha önceki tanımların ana unsurlarını kapsamaktadır.

Herbane (2010) tarafından belirtildiği gibi, İngiltere merkezli ve bilgi teknolojisine odaklı bir faaliyet olarak başlayan BCM artık lüks değil beklenti haline gelen bir süreçtir.

İş sürekliliği yönetimi, yıkıcı bir olayın olumsuz sonuçlarını hafifletmek için faaliyet göstermektedir ve ayrıca iş geliştirmeleri sağlayabilmektedir. Etkin bir iş sürekliliği yönetimi programının bir kuruluşa sağladığı faydalar şunları içerebilmektedir:

- Bir iş durgunluğu durumunda müşterilere hizmetlerin verilmesine devam edilmesi,
- Bir iş kesintisinin sonuçlarını proaktif olarak tanımlama yeteneği,
- Kuruluşun zarar görmesini en aza indirgeyen bir iş kesintisine etkili bir yanıt verebilme yeteneği,
- Kuruluşun ekonomik olarak bozulması sırasında işletme masraflarının azaltılması ve daha maliyet etkin kurtarma sağlaması,
- Dayanılmaz risklerin yönetimi ve sigorta poliçelerine uyum,
- Mevzuat gerekliliklerine (varsa) uyulması,
- Paydaşlara inanılır bir yanıt göstererek kuruluşun itibarını arttırmak,
- Disiplinlerarası ve kurumlar arası takım çalışmasının artması,
- Operasyonların etkinliğini ve etkililiğini arttırması,
- Olumsuz olayları iş süreçlerini iyileştirmek için fırsat olarak kullanma becerisi,
- Aksi açıkça görülemeyen önemli bağdaşıklıkları tanımlamak,
- Bir iş kesintisinden kurtulma ve yönetimi kolaylaştıran esneklik.

İşletmenin iş sürekliliği stratejisini belirlerken maliyetleri ve potansiyel süreklilik tedavilerinin faydalarını göz önüne almak önemlidir. Bir maliyet fayda analizi, sağlanan fayda ve masrafları karşılaştırmaktadır. Literatür etrafında gözden geçirilen çerçeve, iş sürekliliği için ingiliz standardının merkezindeki BCM yaşam döngüsünden alınır ve akademik literatüre yansıyan temel temaları yakalamaktadır.



Şekil 1.3. BCM'nin Örgüt Kültürüne Katıştırılması (British Standards Institution, 2008)

Standartlar bir organizasyonda iş sürekliliğini anlamak, geliştirmek ve uygulamak için bir temel oluşturmaktadır. Geniş bir yelpazede uzman ve endüstri profesyonelleri tarafından geliştirilen standartlar, herhangi bir sektördeki büyük veya küçük herhangi bir organizasyona uyacak şekilde tasarlanmıştır. BCM yaşam döngüsünün altı unsurunun her biri, konunun özüne rehberlik etmek için kullanılmaktadır.

- BCM program yönetimi,
- Örgütü anlamak,
- İş sürekliliği stratejisinin belirlenmesi,
- BCM tepkisinin geliştirilmesi ve uygulanması,

- BCM egzersizleri, BCM düzenlemelerinin gözden geçirilmesi ve sürdürülmesi,
- BCM'nin örgüt kültürüne katıştırması.

1.5.1. BCM program yönetimi

Program yönetimi, BCM sürecinin merkezinde yer almakta ve aşağıdakileri içermektedir:

- Üst düzey yöneticilerin katılımının sağlanması,
- Sorumlulukları atama (yönetişim),
- Örgüt içinde iş sürekliliğinin uygulanması,
- Devamlı iş sürekliliği yönetimi.

Üst yönetimin katılımı

Üst yönetimin katılımının BCM'nin başarısı için çok önemli olduğu açıktır. Seow (2009), üst düzey yönetim istihdam etmemenin bir kuruluştaki BCM programını başlatma ve sürdürme taahhüdünün başarısında bir engel olabileceğine işaret etmektedir. Üst yönetimsiz BCM programı neredeyse kesinlikle başarısız olacaktır. Koch'a (2001) göre yönetim süreci programını yıllık olarak gözden geçirmek yönetim kurulunun sorumluluğunda bulunmaktadır. Yöneticiler, kurumsal varlıkları korumak ve kuruluşun uzun vadeli hayatta kalmasını sağlamak için yeteneklere sahiptirler. Yönetim kurulu BCM'de etkin rol oynamıyorsa, bir programın sürdürülmesi çok zor olacaktır.

Literatürde BCM'nin üst düzey yöneticilere stratejik olarak ortak edilmesi ve organizasyona önemini göstermek suretiyle bağlamsallaştırma gereksinimi tanımlanmaktadır. Seow (2009) tarafından belirtildiği gibi, BCM'yi üst düzey yöneticilere ortak etmek önemlidir. Seow (2009), bir felaket olayından sonra başarısız olan ve geçmiş olaylara ilişkin vaka incelemeleri sunarak, iş sürekliliği planları olmayan şirket sayısına ilişkin istatistikleri öne çıkararak ve sadece iş modellerini kullanarak değil hissedar değerindeki getirileri göstermekle elde edildiğini savunmaktadır, çünkü diğerleri genel ve yüzeysel olma eğilimindedir. Bu tür yaklaşımlar genellikle üst düzey yöneticileri BCM ile etkileşime sokmaya motive etmekte başarısız olmaktadır. Üst düzey yöneticilerin dikkatini çekmek için Seow (2009), mümkün olduğunda, BCM lideri tarafından şahsen BCM'nin

durumunun üst düzey yöneticilere doğrudan yönetim bağlamında sunulmasının ve olayı değerlendirmesinin önemini vurgulamaktadır.

Lindstedt (2007), BCM'nin önemi hakkında üst düzey yönetim bilincinin artırılmasına yönelik olarak, yöneticilerin yalnızca risk yönetimi gibi işin bir başka işlevinin bir parçası olarak görülmesi durumunda BC programını desteklemesinin beklenemeyeceğinden bahsetmektedir. Bu nedenle BCM uygulayıcısının, üst düzey yönetimin önceliklerinin neler olduğunu, BCM'yi desteklemek veya desteklememek konusunda sahip oldukları tutumun ne olduğunu, onları motive eden şeyin ne olduğunu iyi analiz etmesi gerekmektedir.

De Waal'a (2006) göre ahlaki imgelemde yankılanan felaketler tepkiler üretmektedir. De Waal (2006) afetlerin önlenmesinde dört siyasi unsur olduğuna dikkat çekmektedir; felaketin görünürlüğü, felaketin siyasi anlamdaki önemi, seçmenlerin etkilenmesi ve tepkiye dahil olması ile etkin tepki için teknolojilerin varlığı. Herhangi bir BCM girişimi ile ilgili olumlu yönetimsel yanıtı almaya çalışırken bunların akılda tutulması gerekmektedir.

BCM mesajının güvenilir bir iletişim kurucu tarafından iletilmesi gerekmektedir. Myers (2006) ayrıca, BCM sorumluluğundaki kişinin BC'nin doğru konumlandırılmasının gerekliliğini savunmaktadır. Bu da, üst düzey yönetimin kurumsal bir acil durum planlaması politikası ve stratejisi üzerinde konumlandırılması, ortak edilmesi ve bu politikayı ve stratejiyi başka faaliyetlerin yapılmasından önce program sürecini içerecek şekilde yazılı olarak belgelendirmesi anlamına gelmektedir.

Yönetim kurulu taahhütü edinmek, Gallagher'a (2003) göre bir BCM programını başlatmanın ilk adımıdır ve ayrıca BCM sorumluluğunun birine mevcut rollerine ek olarak ya da sadece bir şey yapması için verilmemesi gerektiğini de söylemektedir. Bu süreçten, bir BCM sponsoru ortaya çıkmak durumundadır.

Genel yönetim çerçevesi, iletişimin etkililiğini artırmak adına BCM'yi savunanlar için, üst yönetimin iletişimde aşağıdaki üç değişkeni tanıması açısından önemlidir:

- İletişimin kaynağı (bunu söyleyen),

- İletişimin niteliği (nasıl söyledikleri),
- Seyircilerin özellikleri (kime söyledikleri) (Aronson, 1999).

Herhangi bir BCM programında baştan başa, başta yönetim başlama toplantılarında olmak üzere, icra kurulu başkanı (CEO) tarafından bilgi ve taahhüt almak hayati önem taşımaktadır. Barnes (2001) bu konuyla ilgili olarak, yazılması planlanan planın CEO'nun büyük bir felaket sonrası yeniden operasyonel hale getirme planı olduğunu söylemektedir. CEO'dan BCM'ye destek de devam etmek durumundadır. Elliott, Swartz ve Herbane'in (2010) belirttiği gibi, BCM sürecinin normalde üst yönetim desteğine ihtiyacı vardır ve ilerleme düzenli olarak üst düzey yönetim ekibine bildirilmek durumundadır. Üst düzey yönetim, BCM'de iş sürekliliği sağlama odaklılığının nerede olacağına karar vererek ve aynı zamanda iş sürekliliği yönetimini stratejik bir perspektiften yönlendiren zihniyet belirlemede karar vererek hayati bir rol oynamaktadır.

Kurumsal yönetişim ve düzenleyici konuların üst yönetim üzerindeki etkisi, üst yönetim katılımının ve herhangi bir BCM programının desteklenmesinin önemini daha da vurgulamaktadır. Hiles (2010) tarafından da belirtildiği gibi kurumsal yönetim, riski dengelemek, yönetmek ve iç kontrol prosedürlerini uygulamak için yürürlüktedir. Hiles (2010), yöneticilerin ve üst düzey yönetimin hem düzenleyicilere hem de paydaşlara kurumsal yönetim konusunda güvence vermek zorunda olduklarını ve organizasyonel riskler ve yükümlülükleri hakkında kendilerini bilgilendirmesi gerektiğini özetlemektedir. Elliott, Swartz ve Herbane (2010) tarafından belirtildiği gibi, düzenleme dışındaki organizasyonların denetimlerinin, uygulanan otoritenin uyumu zorunlu kılmak için muhtemelen yasal yetkilere sahip olacağı için uyguladığı denetimlerin uygulanması gerekmektedir. Bu nedenle, bir organizasyonun BCM meselelerinin dış regülatörler tarafından zorla tutulmalarından ziyade ele alınması daha iyidir. Dolayısıyla, üst yönetimin BCM programlarına sürekli olarak katılımının operasyonel risk yönetiminin normal bir parçası olması gerekir. Üst düzey yönetime ilişkin öncelikler ve konular hakkında bilgi sahibi olunması, BCM uygulayıcısının BCM programının sağlam bir temel üzerine kurulması için gerekli desteğini almasını sağlayacaktır.

Yönetim onayını ve desteğini kazandıktan sonra BCM programının bir sonraki önemli adımı, program sorumluluklarının ilgili gruplara ve kişilere doğru bir şekilde verilmesini sağlamaktır.

Sorumlulukları atama (yönetişim)

BCM programı sorumluluklarını belirlerken, literatürde, sorumluluğun programın başarıyla tamamlanması için gerekli olan yetki ve kıdem düzeyine sahip olması gerektiği açıkça belirtilmektedir. Sorumluluk BT ekibinin bir üyesine verilmemelidir, çünkü BCM'nin kuruluşun geri kalan kısmı tarafından bir BT girişimi olarak görülecek olması büyük bir tehlikedir. Kuruluşun her seviyesi BCM'nin uygulanmasına dahil olmak durumundadır.

Standartlar, BCM programının uygulanması ve sürdürülmesi için sorumlu olmak adına uygun kıdem, yetki ve becerilere sahip bir birey, ekip veya grup ataması gerektiğini vurgulamaktadır. Dikkat çeken nokta, vurgunun uygun kıdem ve otoriteye sahip bir birey üzerinde olması ve planı uygulamak ve sürdürmekten tek bir kişiden ziyade bir takımın sorumlu olmasıdır. Aronson (1999) ayrıca bir BCM programına sorumluluk yüklenmesinin en önemli adımlardan birinin, programa başkanlık etmek için gerekli yetki düzeyine sahip olan kişinin seçilmiş olması olduğunu vurgulamaktadır.

BCM programlarının başarıya ulaşmasını sağlamak için, sorumlulukların pek çok grup veya bölüme ayrılmaması, ancak uygun alanlarda yoğunlaşılması önemlidir. Kuruluşlar hala BCM sorumluluklarını operasyonlar, güvenlik, BT, yönetim ve diğer departmanlar arasında bölüştürme eğilimi göstermektedir ve bu durum bir şeylerin çatlaklara yayılması riskini arttırmaktadır (Adkins, Thornton ve Blake, 2009). Elliott, Swartz ve Herbane (2010), BCM proje yönetimi rolünün BT uzmanına verilmemesi gerektiğini, çünkü bunun BCM'yi bir BT meselesi haline getirdiğini ve yönetim kurulunun bir iş sürekliliği yönlendirme grubu atamasını ve süreci yerel veya bölüm düzeyinde yürütmek için BCM proje yöneticisini desteklemesini tavsiye etmektedir. Yönlendirme grubu, farklı iş birimlerinden veya departmanlarından kıdemli ve etkili personeli içermektedir ve operatif düzeydeki çalışanlar ile herhangi bir merkezi BCM ekibi arasında bir yol gibi davranmaktadır. Çalışanların BCM programına standartların altını çizdiği gibi katılımı, BCM programını uygulamaya yardımcı olmak için kuruluştan temsilcileri seçmenin uygun olabileceğini belirtmektedir ve BCM rollerinin ve sorumluluklarının yetkililerin iş tanımlarına ve beceri setlerine entegre edilmesini savunmaktadır. Bu sorumlulukları güçlendirmek için kuruluşun değerleme ve ödüllendirme sistemine dahil

edilmeleri gerekmektedir. BCM için doğru sorumluluklar tanımlandıktan sonra programın uygulanması bir sonraki mantıklı adımdır.

Örgütte iş sürekliliğinin uygulanması

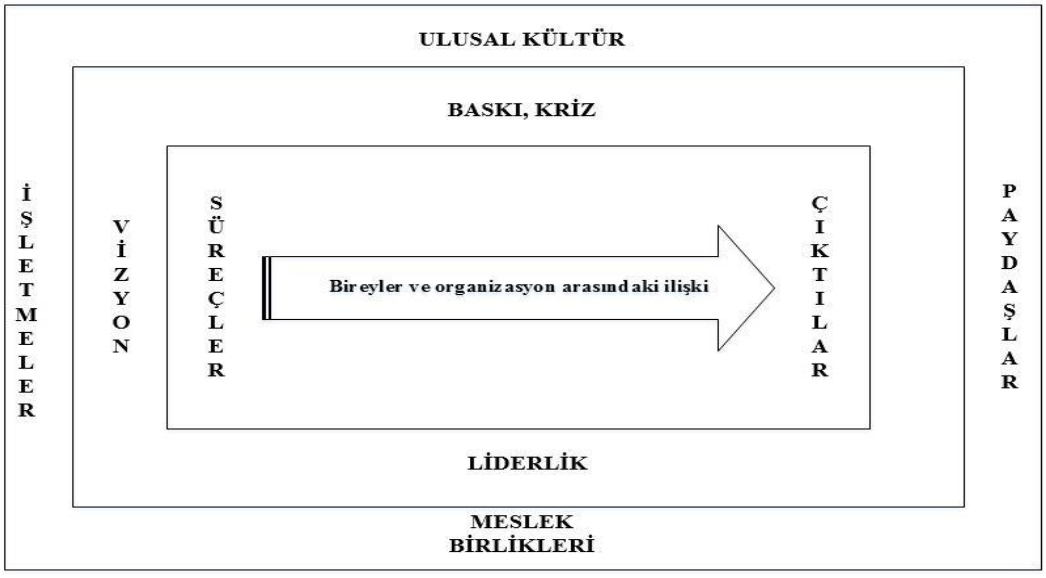
BCM programını uygularken veya gerçekten bir organizasyonda herhangi bir programı uygularken yapılması gereken faaliyetler, programın tasarımı, oluşturulması ve uygulanmasını içermektedir. Literatür, programın etkili olmasını sağlamak için uygun bir proje yönetim çerçevesinin kullanılması gerektiğini belirtmektedir. BCP'yi tasarlamak ve oluşturmak ve bunları büyük bir organizasyonda güncel tutmak, Hiles'a (2010) göre çok zor bir görev olabilmektedir. Uygun proje raporlama ilişkileri ilk BCM projesi boyunca ve sürecin şirket süreçlerine entegre olmasını sağlamak için sürekli olarak kullanılması gerektiği savunulmaktadır.

Standartlar, organizasyonun uygulamanın en etkili biçimde tamamlandığından emin olması için standart bir proje yönetimi metodolojisini kullanarak BCM'yi uygulamasını önermektedir. Bir BCM projesinin aşamalarını değerlendirirken, hepsinin benzer proje yönetimi aşamalarına sahip çeşitli yaklaşımlar savunulmaktadır (ISO/IEC 27031:2011(E), 2011).

Barnes (2001) ana aşamaları varlık, proje temeli, işletme değerlendirmesi, strateji seçimi, plan geliştirme, test ve sürdürme olarak tanımlamaktadır. Elliott, Swartz ve Herbane (2010), başlatma, iş sürekliliğinin planlanması, uygulanması ve operasyonel yönetimi olmak üzere dört farklı aşamaya sahip olduğu süreklilik yönetimi sürecine atıfta bulunmaktadır. Howe (2007) bir BCM projesinin bilgi toplama, plan geliştirme ve BCP projesinin devam eden kurumsal çapta bir süreç haline geldiği dönüşüm safhası olmak üzere üç aşamaya ayrılabilir olduğunu savunmaktadır. BCP oluşturulma sürecinden bağımsız olarak Ginn (1992), sonuçta ortaya çıkan BCP'nin modüler bir tasarıma sahip olması gerektiğini ve böylece tüm felaketlerin büyük felaket olabilmesi için kolaylıkla güncellenebilir ve okunabilir bölümlere ayrılabileceğini kaydetmektedir. BCP planı yürürlüğe girdikten sonra, devam eden yönetim konusunun ele alınması gerekmektedir.

Devamlı iş sürekliliği yönetimi

Literatürde düzenli olarak kanıtlandığı üzere üst yönetim, BCM programının önemini, tüm organizasyona ve uygun paydaşlara odaklanabilmek için iletmek durumundadır. Tüm personel için uygun BCM eğitimi yapılmalı ve üst yönetim BCP'nin canlı bir doküman olarak tutulmasını sağlamak durumundadır. BCM kuruluşun ortamında, personelinde, süreçlerinde veya teknolojisinde önemli bir değişiklik olduğunda sistemlerin ve planların güncellendiğinden emin olmak zorundadır. Bir egzersiz veya olay eksiklikleri vurguladığında BC planlarının da güncellenmesi gerekmektedir. Brazeau'ya (2008) göre bir organizasyon içindeki herkes, BCM'nin etkin olması için BCM'yi benimsemek durumundadır. Elliott, Swartz ve Herbane (2010) tarafından da belirtildiği gibi etkin BCM, süreç üzerinde bir civata değil sağlam yönetim uygulamasının bir parçasıdır. BCM'nin güncel kalmasını sağlamak için, kuruluşun başından başlayarak kuruluşun kültürü içine gömülmesi ve sürekli iletişim yoluyla yol boyunca ilerlemesinin sağlanması önemlidir; böylelikle organizasyon yönetilmektedir. BCM sürecinin her aşamasında bunu sağlamak, bir kuruluşun BCM kültürünü tanıtmayı ve geliştirmek için fırsatlar yaratmayı sağlamaktadır.



Şekil 1.4. Örgüt Kültürünü Anlamak İçin Kavramsal Bir Model (De Witte ve Van Muijen, 1999)

De Witte ve Van Muijen (1999), örgüt kültürüyle uğraşırken dikkate alınması gereken farklı öğelerin kavramsal bir modelini sunmaktadır. Bir örgütün kültürü üzerindeki etkiler geniş kapsamlı ve çeşitlidir; genel ulusal kültür, iş ortamı, paydaş etkileri,

organizasyonun iç vizyonu, kendi süreçleri ve hedefleri, çalışanları ile kuruluş ilişkilerini içermektedir.

Örgütsel kültürü anlamak

BCM'yi kuruluş kültürü içine yerleştirirken, örgüt kültürü ile neyin kastedildiği hakkında genel yönetim perspektifinden bir bakışa sahip olunması gerekmektedir. Kello (2009), kültür tanımlarının çoğunun, kültürün üst düzey bir tutum, inanç, norm ve davranış toplamını temsil ettiğini vurgulamaktadır. Bu bağlamda kültür, işlerin kuruluşlarda nasıl işlediğini belirtmektedir. Kello (2009), kültür ve onun ölçümü ile ilgili her zaman bir miktar tavuk ve yumurta sorunu olduğunu tespit etmektedir ve bu noktada ilk önce ortaya çıkan davranışlar ve tutumlar mı yoksa kültür mü ikilemi karşımıza çıkmaktadır.

Luthans'a (2002) göre tüm organizasyon kültürleri, davranışsal düzensizlikler, normlar, belgelenmiş değerler, felsefe, kurallar ve örgüt iklimi gibi bir takım özelliklere sahiptir. Luthans (2002), örgütlerin sürekli olarak tek biçimli kültürlerine sahip olmadıklarını, ancak bir kültür yönetimi perspektifinden tutarlı bir kültüre sahip oldukları varsayılması gerektiğini söylemektedir. Kültür, örgüt üyelerine örgütsel bir kimliğe sahip olma imkanı sağlamaktadır ve kendilerinden daha büyük olan inanç ve değerlere bağlılık taahhüdü getirmektedir. Törenler, hikayeler, semboller ve organizasyonda kullanılan dille yorumlanabilmektedir. Daft'a (2001) göre kültürün örgütlerde iki kritik göreve hizmet ettiğini belirtmek gerekir; üyeleri birbirleriyle nasıl ilişkilendireceğini bilmektedir ve organizasyonun dış çevreye uyum sağlamasına yardımcı olmaktadır.

Kello'nun (2009) belirttiği gibi, hem açık (kurumun söylediklerini ifade eder) hem de örtük (çalışanların kuruluştaki tecrübelerinden çektiği çoğu kez yazılmayan çıkarımlar) kültürlerin belirgin olduğunu ve kuruluşlarda faaliyet gösterdiğini kabul etmek gerekmektedir. Herbane (2010), bir organizasyon kültürünün kuruluş içinde ve dışında kabul edilebilir davranışları yönetecek yazılı olmayan kurallar kümesi olduğunu ileri sürmektedir. Tüm bunları önemsemek, bir BCM programı üzerindeki kültürel etkiler göz önüne alındığında önemli olmaktadır.

BCM ve kültür

Kültürü bir BCM perspektifinden izlerken Von Rossing (2007), kültürün sürecin her aşamasında olduğunu belirtmektedir. Bir kuruluşun BCM sürecini denetlerken / gözden geçirirken zaman içinde gelişen kültür dikkate alınmak durumundadır. Güçlü bir BCM kültürü, muhtemelen BCM programının güçlü üst yönetim desteğine ve bu nedenle yüksek esneklik düzeylerini korumada görünür yatırımlara sahip olduğunu yansıtmaktadır. Zayıf bir BCM kültürüyle bu unsurlar kaybolacaktır. Esneklik kültürü oluşturulurken, hesap verebilirlik otoriteyle birlikte bulunmaktadır ve BCM bileşenleri günlük işlemlere entegre edilmektedir (Alesi, 2008). Her çalışanı bir planın parçası haline getirmek ve planı çalışanlara erişilebilir yapmak önemli bir noktadır. Aynı zamanda kuruluşlar doğaçlama yapmaya hazırlıklı olmak durumundadır. Çalışanların ihtiyaç duyulan esnekliğe uygun bir model oluşturdukları, tanıdık araçları kullanarak olaylara hızlı bir şekilde tepki verdikleri bir organizasyon içinde esneklik kültürü oluştururken, başarılı olmak için paylaşılan bir tutku düşüncesi esnek girişim yaratmada çok önemli bir bileşendir (Sheffi, 2007).

Özellikle güvenlik kültürü kavramına değinen Kello (2009), genel bir organizasyon kültürünün unsuru olan emniyet kültürü kavramının, işyerinde emniyet araştırması ve uygulamasının belirgin bir parçası haline geldiğini belirtmektedir. Spigener'e (2009) göre, organizasyonlar güvenlik performansının odağını yaralanmalardan uzaklaştırmaktadır ve maruz kalmaları yönetmek ve en aza indirme yönüne kaydırmaktadır. Güvenlik konularında maruz kalmaları en aza indirgeme konusundaki itici güç, bu sürecin bir parçası olarak risklerin değerlendirilmesi ve ele alınması gerektiğinden, BCM kültürünün tamamına da yardımcı olacaktır.

BCM kültürünün kuruluş içinde oluşturulması, tanıtılması ve yerleştirilmesi, kurumun temel değerlerinin ve etkili yönetiminin bir parçası haline gelmesini sağlamak için gereklidir. Cummings'in (2003) belirttiği gibi, bazı şirketler için bu kültüre yönelik teşvik genellikle düzenleyici gereklilikler şeklinde örgüt dışından gelmektedir. Youngblood (2000), 21. yüzyılda başarılı olmak için organizasyonların çevik, yenilikçi ve canlılığı olan bir kültüre ihtiyacı olduğunu söylemektedir. Bu ihtiyaç, organizasyonların yeni iş kurallarına başarılı şekilde adapte olmalarını ve başarabilmelerini sağlamaktadır. Çevik ve yenilikçi bir organizasyon kültürünün olması, BCM programının güncel tutulmasını ve organizasyona gömülmesini sağlayacaktır.

Standartlarda belirtilen olumlu bir kurumsal BCM kültürünün sağladığı faydalar, BCM sürecini daha verimli hale getirmek, paydaş güvenini kazanmak, zamanla esnekliği artırmak ve aksama şansını en aza indirmektir. Örgüt kültürü bu nedenle BCM'nin veya herhangi bir değişikliğin nasıl ele alındığını belirlemektedir. Luthans (2002) tarafından da belirtildiği gibi, örgütlerin değişimi öğrenen ve öngören bir kültüre sahip olması gerekmektedir. Kuruluşların egemen kültürü proaktif olmaktan ziyade reaktiftir ve değişimi öğrenme ve öngörebilme yeteneğine sahip değildir, o zaman BCM'yi sürdürmek zor bir süreç olacaktır.

Hiles (2010), BCM uygulayıcılarının BCM konusunda farkındalık yaratırken büyük sopa yaklaşımını kullanmamalarını savunmaktadır; çünkü bu yaklaşım geri tepebilmektedir. Aronson'un (1999) belirttiği gibi, insanların uyuşmasının iki olası nedeni vardır. Bunlar, başkalarının davranışlarının insanları uymaya ikna etmesi ya da sopa cezalandırılmasını istememek istediklerinden uymak zorunda kalmalarıdır. İnsanlar, tehdit altında olmaktan ziyade ikna olmak noktasında daha iyi yanıt vermektedir. Aronson (1999) bireylerin neden daha uygun olduklarını göz önünde bulundurarak, bireyden gerekli cevabı elde edebilmek için değer veya inancın içselleştirilmesi gerektiğini ve en derin cevabı elde etmenin en kalıcı yolu olduğunu söylemektedir. Bu, başarılı olmak için herkes tarafından içselleştirilmesi gereken BCM programı için geçerlidir. Uyum, Aronson'a (1999) göre iç içe geçirmeden daha az kalıcıdır ve birey üzerinde daha az etkiye sahiptir. Hiles (2010), BCM programının etkili bir şekilde uygulanmasını sağlamak için, CEO veya yönetim kurulu tarafından BCM programının önemi konusunda bir açıklama yapılmasını önermektedir.

Bir organizasyonda BCM sürecinin başarılı olması için mevcut olması gereken iki temel unsur; birincisi, örgüt yapısının açık bir iletişim otoritesi, kontrol ve iletişim hatları sağlamak için yerinde olması gerekmektedir ve ikincisi, BCM'nin etkili bir şekilde uygulanması için örgütsel koşulların doğru olması gerekmektedir (Elliott, Swartz ve Herbane, 2010).

Kotnour (2009) tarafından işlevsiz bir örgüt kültürü ve bilişsel uyumsuzluğun etkileri ile ilgili bir uyarı yapılmaktadır: Değerler kitaplarda, herkese verilen kartlarda, duvardaki plakalarda anlatılabilir, ancak bu değerler kalplerde ve davranışlarda yoksa, işlevsiz bir kültüre sahip olunur. Özünde, bu ahenksizliktir. Bilişsel uyumsuzluk,

düşüncelerimizin (bilişler) ve eylemlerimizin birbirine karşı geldiğinde ortaya çıkmaktadır. Mühendislik terimleriyle, dengesizlik hali oluşmaktadır. Pragmatik açıdan, bir şey vermek zorundadır. Genellikle bahsi geçen verir olgusu, küçük bir grup birey arasında işlevsiz kültürün eşleşmesi için değişen değerlerdir.

BCM'yi örgüt kültürüne dahil etmek, bu nedenle daha geniş kurumsal organizasyon kültürünün farkında olmayı gerektirmektedir ve gelecek için çalışanlar tarafından içselleştirilebilmesi için dikkatli yapılmak durumundadır. Yukarıdaki tüm BCM program öğelerine yer verilmesi, kuruluşların BCM programının kurulduğu andan kuruluşun ömrü boyunca kapsamlı ve işlevsel olmasını sağlamaktadır.

BCM ve değişiklik yönetimi

Gallagher (2003), BCP'nin devamlı olarak sürdürülmesinin yaşamsal önem taşıdığını, ancak BCP'nin örgütsel değişiklikleri takiben güncel tutulmaması durumunda bunun önemsiz olacağı uyarısında bulunmaktadır. Elliott, Swartz ve Herbane (2010) BCM sürecinin planlama boyutuna, hem pratikte hem de çeşitli yayınlarda daha çok dikkatin yönlendirildiği gerçeğine atıfta bulunmaktadır. Kjærgaard (2009) örgütsel değişim ve sürdürülebilir BCP'ler söz konusu olduğunda, süreklilik ve değişim arasındaki sabit gerilimi dengelemek zorunda oldukları için, strateji oluştururken örgütler bir ikilemle karşı karşıyadır yorumunda bulunmaktadır. Kuruluşlar günümüz iş ortamının bir sonucu olarak sürekli bir değişim geçirirken, BCM yönetim stratejisi bu meydan okumaya ayak uydurabilmek için yeterince esnek olmak durumundadır.

Herhangi bir BCM sürecinde, organizasyonun bir değişiklik yönetimi (CM) süreci boyunca zamanla geliştikçe planlarının güncellenmesi önem arz etmektedir. Bu nedenle BCM programı güncel tutulması için örgütsel değişiklik yönetimi programının bir parçası olmak durumundadır. Hiles (2010), planların ilgili tarihteki iş gereksinimlerini yansıttığını belirtmektedir. Gereklilikler ve kurtarma süreleri sabit değildir ve BCM, değişiklik yönetimi süreci ile korunmak durumundadır. Elliott, Swartz ve Herbane (2010), BC programının değişiklik yönetimini yorumlayarak, etkili BCM uygulamasını sağlamak için genel değişim yönetimi stratejilerinin kullanılması gerektiğini belirtmektedir.

Örgütsel değişim üzerine detaylı olarak bakmak adına Johnson, Scholes ve Whittington (2002), dört tür stratejik değişim tanımlamaktadır: Uyum, yeniden yapılandırma, evrim ve artımlılık.

Johnson, Scholes ve Whittington'a (2002) göre BCM süreci, hangi değişim yönetimi stili seçilmiş olursa olsun, eğitim ve iletişim, işbirliği, müdahale, yönlendirme, zorlama olmak üzere beş yöntemden biri ile yönetilebilmektedir. İş sürekliliği değişiklik yönetimi süreci yerine getirildiğinde, örgüt içinde kullanılan daha geniş örgütsel değişiklik yönetimi sürecinin bir parçası olmak durumundadır.

BCM programının uygulanmasına ilişkin olarak standartlar, organizasyonun programı paydaşlara iletmesi, personel için uygun eğitim düzenlemesi veya sunması ve iş sürekliliği kabiliyeti ile çalışması gerektiğini savunmaktadır. BCM programı organizasyona dahil edildiğinde, değişiklik yönetimi süreci diğer proseslerin sürdürülmesiyle uyumlu hale gelecektir. Gallagher (2003), BCP'yi oluşturmak için kullanılan grupların birlikte olmasını savunmaktadır. Bu düşünce ile daha az sıklıkla toplanabilirler, ancak operasyonel bir seviyede çalışmalara odaklanmaları sağlanmaktadır ve farklı birim veya birimler arasında iş sürekliliği sorunlarının etkin iletişimini sağlamaya yardımcı olunmaktadır. Bir BCM programının başarılı olabilmesi için ön şart, organizasyonun birden fazla düzeyde anlaşılmış olmasıdır.

1.5.2. Örgütü anlamak / Analiz

Etkin BCM'yi destekleyen kuruluşlar, organizasyonun, dış varlıkların ve içinde faaliyet gösterdiği ortamların da dahil olduğu tüm bileşen kısımlarını derin bir şekilde anlamayı içermektedir. Standartlarda değinildiği gibi, BCM programının bu öğesinin ana amacı, ana ürün ve hizmetlerini, bunları destekleyen kaynakları ve faaliyetleri belirleyerek organizasyonu anlamaya yardımcı olmaktır. Bu süreç, BCM programını kuruluş hedefleriyle uyumlu hale getirmektedir.

Bir organizasyonu anlamak, BC uzmanı için yıldırıcı bir girişim olabilmektedir ve işin birden fazla alanı hakkında bilgi gerektirmektedir. Anlama, BCM bakımından, Von Rossing (2007) tarafından kritik faaliyetlerin ve kuruluşla ilişkinin devamını sağlamanın kapsamlı bir bilgiye sahip olduğu şeklinde tanımlanmaktadır.

Sandesh, McHugh ve Jones (2008), örgütlerin sık sık tabi oldukları çok sayıda dış bağlantıları ve bir kuruluşun faaliyet gösterdiği çevreyi oluşturan çok sayıda ve farklı organları, kişileri ve organizasyonları diyagram olarak göstermektedir.

BCM literatürü, tedarik zincirlerinin sürekliliğine ve bunların örgütlere etkisine odaklanmaktadır. Modern tedarik zincirleri yüksek müşteri hizmetleri seviyesi ve düşük maliyetler sunarken, aynı zamanda yüksek etkili/düşük ihtimal olaylarına karşı savunmasız olduğunu kabul ederek daha geniş kurumsal tedarik zincirinin korunmasının önemini ortaya koymaktadır (Sheffi, 2007). Dünya ekonomik forumu, tedarik zincirlerinin yalnızca organizasyonlara değil, aynı zamanda hükümetlere de önem verdiğini belirterek, dış tedarikçilere bağımlı olan tüm şirketlerin ve hükümetlerin, tedarik zincirinde bozulma riskine maruz kaldıklarını tespit etmektedir. Mevcut küresel tedarik zincirlerinin kapsamı ve karmaşıklığı, tedarik zinciri yönetimi probleminin tek bir işletme veya endüstri ile sınırlı olmadığı anlamına gelmektedir. Küresel bir risk olayının neden olduğu nispeten küçük bir tedarik zinciri bozulması bile sonuç olarak küresel ekonomik sistemde sonuçlar doğurabilmektedir.

Örgütler, Smith'in (2005) belirttiği gibi bir ikilemle karşı karşıya kaldıklarını belirtmektedir. Sistematik, iyi tanımlanmış ve test edilmiş eylem kuralları ile çalışmaktadır ve karar verme süreçlerinde açık ve şeffaf olan rasyonel varlıklar gibi davranmak durumundadır. Öte yandan, daha geniş bir dünyayla etkileşime girmeleri gerekir ve bu durum kontrol ve sınırlama için sorunlar yaratmaktadır. Dolayısıyla örgütler, açıklık ve kontrol arasında ve rasyonel davranış ile kazanılmış kendi çıkarları arasında sürekli bir akış halinde bulunmaktadır. Bu gerginlikler, hüküm süren koşulları anlamanın ve gelecekteki sonuçlarını tahmin etmenin zorluklarıyla birlikte, krizin potansiyelinin hasır altı edildiğini garanti etmektedir.

Bilinmeyen olaylarla başa çıkma

Bilinmeyen olaylarla uğraşmak ya da bilinmeyen için bir şekilde hazırlanmak BCM literatüründe vurgulanmaktadır. Bilinmeyen olaylar, doğaları gereği, bir BCM programını uygularken karşılaşılan en büyük zorluklardan biridir. Elliott, Swartz ve Herbane (2010) iş sürekliliği uygulayıcıları ve yöneticilerinin potansiyel kesinti senaryoları ve bunların faaliyetler ve paydaşlar üzerindeki muhtemel etkileri konusunda yaratıcı düşünmeleri

gerektiğini söylemektedir ve yaratıcı, çoklu perspektifi olan, tekrarlayan ve sorgulayan bir zihniyet önermektedir. Lagadec (2009) kriz olaylarıyla (bilinmeyen olaylar) ilgili olarak, sorunun artık neyi bilmediğimizi belirlemek için değil, ancak mevcut bilgimizin hangi paketinin modern krizlerin ortaya çıkardığı her iki taraftan sorgu dalgalanmalarına cevap verecek kadar güçlü olduğunu ayırt etmeye çalışmak olduğunu söylemektedir.

Taleb (2007) bilinmeyen olayları daha da ileri götürerek, bin yıl boyunca geçerli olan genel bir fikri geçersiz kılan tek bir gözlemi (Black Swan) ifade etmektedir. Kara kuğu (Black Swan) olaylarının Taleb'e (2007) göre üç özelliği vardır; düzenli olarak kökleri beklenenlerin dışında yatmaktadır, aşırı bir etki göstermektedirler ve nihayet insan doğası, olayın mantıksal bir şekilde açıklanmasına izin vererek, olaydan sonra gerçekleşen olaylara dair açıklamalar düzenlenmesine izin vermektedirler. Kara kuğu olayları, Taleb (2007) tarafından nadirlik, aşırı etki ve geriye dönük (öngörülen olmasa da) öngörülebilirlik olarak özetlenmektedir ve beklenmedik durumların oluşabileceğinin kabul edilmesi gerektiği vurgulanmaktadır. Bu beklenmedik olaylar genelde tarihin yönünü değiştiren olaylardır. Ve bu tür olaylar genellikle büyük bir şok olarak karşımıza çıkmaktadır.

Youngblood (2000), Taleb'e benzer bir şekilde, evrim örneklerini kullanarak, sismik kuantum kaymalarının veya bilim adamlarının noktalamalı dengeler dediği gibi olduğunu belirtmektedir. Kararlı ortamlar, çevre içinde herkesi etkileyen periyodik muazzam bozulmaya tabidir ve bu durum kuruluşlar için de geçerli olmaktadır.

Alesi (2008), ender/aşırı olaylara değinen iş sürekliliği planlamasının sürekli bir değişim ve gelişme halinde olduğunu söylemektedir. Değişiklikler yavaş ve hemen hemen fark edilmeyecek düzeyde olabilmektedir, ancak geniş kapsamlı ve hızlı sonuçlara sahip olabilmektedir. Değişiklik aniden gerçekleştiğinde genellikle öngörülemeyen, dışsal bir olay değişikliğe eşlik etmektedir ve bu durum kuruluş üzerinde birden fazla etki yaratabilmektedir.

Nadir olayların ortaya çıkışı konusunda anlayış sahibi olma, bir organizasyon üzerindeki etkilerini tahmin etme ve esnek ve modüler bir BCP'ye sahip olma özelliği, nadir ve aşırı etki olayıyla etkili bir şekilde başa çıkabilecek daha kapsamlı ve daha iyi çalışan BCM sürecini sağlayabilmektedir. Bilinmeyen olaylarla baş edebilme yeteneğinin

bir parçası, organizasyonu ve krizin organizasyon üzerindeki etkisini tam olarak anlamak için bir iş etki analizi yapmak olacaktır.

İş değerlendirme aşaması

Etkili bir BCP, desteklenmesi gereken iş işlevleri ve bu desteğin hangi kapsamda olacağı net bir şekilde anlaşılmadan başlamamaktadır (Forbes ve Buchanan, 2006). Bu nedenle iş değerlendirmesi aşaması, gerekli risk ve etki analizlerinin yapıldığı aşamadır. İş değerlendirmesi aşaması, risk değerlendirmesi ve iş etki analizi (BIA) olmak üzere iki bileşene ayrılmıştır. Risk değerlendirmesi ve iş etki analizi bir felaketin neden olabileceği olası zararı değerlendirirken organizasyonun mevcut maruziyetlerini de değerlendirmek için tasarlanmıştır. Risk değerlendirmesi, işletmedeki hem iç hem de dış tehditleri tanımlamaya yardımcı olmaktadır. Bu aşamada üretilen bilgiler stratejilerin ve nihai BCP'nin oluşturulması için temel oluşturmaktadır (Barnes, 2001).

Risk yönetimi

İş devamlılığı ve risk yönetimi yakından ilişkilidir. İngiliz Standartları Enstitüsü (BSI) tarafından yayımlanan ve en yaygın kabul gören BCM standardında açıklandığı üzere risk yönetimi, bir kuruluşun sunduğu önemli ürün ve hizmetlerin etrafındaki riskleri yönetmeye çalışmaktır. Tabii ki ürünlerin ve hizmetlerin teslim edilmesi çok çeşitli olaylardan etkilenebilmektedir. Bu tür olayların tahmin edilmesi ve analiz edilmesi aynı derecede zor olmaktadır. Risk yönetimi, iş sürekliliğiyle ilgili riskleri değerlendirmek ve risklerin oluşmasını önlemek ya da etkilerini kabul edilebilir düzeylere düşürmek için kontrol geliştirmek içindir. Yedi aşamaya bölünebilmektedir ki bunlar:

Aşama 1: Değerlendirme
Aşama 2: Kontrol seçenekleri değerlendirmesi
Aşama 3: Kontrolün maliyet ve etkinlik değerlendirmesi
Aşama 4: Raporlama
Aşama 5: Kontrol opsiyonu kararı
Aşama 6: Kontrol opsiyonu uygulaması
Aşama 7: İzleme ve Kontrol (Syed ve Syed, 2004)

Aşama 1: Değerlendirme

Risk değerlendirmesi, potansiyel güvenlik açıklarını ve tehditlerini tespit etme ve analiz etme egzersizidir ve ardından kuruluşun iç ve dış ortamındaki maruz kalmaların değerlendirilmesi ile devam etmektedir (International Organization for Standardization, 2009). Kuruluşun sel, kasırga, ısıtma ve havalandırma arızası, sabotaj vb. olaylara duyarlı olup olmadığını tespit etmektedir. Daha sonra, bu tehditleri gidermek için hangi hafifletici adımların atıldığını belgelemektedir (Barnes, 2001). Risk kaynakları şunlar olabilmektedir:

- Topluluk çapında tehlikeli olaylar,
- Acil felakete neden olan kazalar veya sabotaj,
- Güvenlik tehditleri, ağ ve iletişim hataları,
- Felaket uygulama hataları veya daha fazlası.

Bu risk alanlarının her biri, etkileyebileceği iş birimleri ile birlikte ve olası kaynakları da eklenerek düşünülmek durumundadır. Tanımlanan her kaynak için, riskin maruz kalma derecesini değerlendirmek adına, hem riskin büyüklüğü hem de oluşma ihtimali değerlendirilmek durumundadır. Risk maruziyeti, bir risk kaynağına ne kadar dikkat edilmesi gerektiğini bilmek için en kolay yolu göstermektedir.

Risk değerlendirmesinin nihai sonucu, tam tehditleri ve tahmin edilen maruz kalma ile birlikte gerekli olan ihtimal ve hafifletici önlemleri ve aynı zamanda riski kapsayan menfaatleri veren bir risk-fayda analizi tablosudur. Bu tablo, var olan varsayımları veya kısıtlamaları da tasvir etmek durumundadır (Barnes, 2001).

Aşama 2: Kontrol seçenekleri değerlendirmesi

Kontrol seçenekleri değerlendirmesi, değerlendirilen tehditlerin kontrolünde kullanılabilir seçenekleri tanımlamaktadır. Riskin kabulü, riskten kaçınma, riski azaltma ve risk transferini içeren dört ana risk kontrol seçeneği bulunmaktadır.

Adından da anlaşılacağı gibi riskin kabulü, riski kabul etmek ve hiçbir şey yapmamak demektir. Riskin kabul edilmesinin bir nedeni, tehdidin kendisiyle ilgili ihmal edilebilir bir riski taşımasıdır. Riskten kaçınma en çok tercih edilen kontrol seçeneğidir, ancak çoğu durumda pratik veya maliyet açısından yasak olabilmektedir. Riski azaltma

kontrol seçeneği, riskten kaçınma kontrol seçeneğinin yanında tercih edilen seçenektir. Riski azaltmanın ilk adımı belirli bir tehdit için kabul edilebilir bir risk seviyesinin belirlenmesidir. İkinci adım, mevcut risk seviyesini kabul edilebilir seviyeye indiren kontrol seçeneklerini keşfetmektir. Risk transfer kontrol seçeneği, yıkıcı bir olaydan kaynaklanan kayıp veya etkiyi telafi edebilen bir başka kuruluşa riski aktarmak için kullanılmaktadır. Örneğin risk, yıkıcı bir olaydan kaynaklanan kayıpları kapsayan bir sigorta poliçesi aracılığıyla bir sigorta şirketine devredilebilmektedir. Risk, servis sağlayıcının kuruluşu herhangi bir hizmet aksamasından telafi etmesini gerektiren bir anlaşmayla bir hizmet sağlayıcısına da aktarılabilmektedir. Risk transferi, risk azaltma ile birlikte kullanılabilmektedir. Risk azaltılarak belirli bir düzeye indirilmekte ve geriye kalan risk, risk transferiyle ele alınmaktadır (Barnes, 2001).

Aşama 3: Kontrolün maliyet ve etkinlik değerlendirmesi

Kontrol maliyetleri ve etkinlik değerlendirmesinin amacı, halihazırda tanımlanmış olan kontrol seçeneklerinin maliyet ve etkinliğini değerlendirmektir. Risk kontrolünün maliyet ve etkinliğinin değerlendirilmesi üç aşamada yapılabilmektedir. İlk adım risk kontrol seçeneğinin uygulanmasının toplam maliyetini tahmin etmektedir. İkinci adım kontrol riskinin azaltılmasında kontrol seçeneklerinin etkinliğini değerlendirmektedir ve üçüncü adım maliyeti kontrol seçeneklerinin etkinliği ile karşılaştırmaktadır. Kontrol opsiyonlarının maliyeti, bir opsiyonun parasal değeri üzerinden ölçülen toplam maliyeti ifade etmektedir ve aşağıdakiler ile ilgilidir:

- Ekipman / malzeme,
- Nakliye,
- Hizmet ve emek,
- Vergiler,
- Sigorta,
- Kira,
- Bakım.

Diğer yandan, risk kontrol seçeneklerinin maliyet etkinliği karşılaştırması, maliyet ve risk azaltma etkinlik değerlerinin karşılaştırılması yoluyla en iyi risk kontrol seçeneklerinin seçimini kolaylaştırmayı amaçlamaktadır (Barnes, 2001).

Aşama 4: Raporlama

Risk raporlama aşaması, bir risk değerlendirme raporunda önceki aşamalarda toplanan sonuçları belgelemektedir. Risk değerlendirme raporu yönetime sunulmakta ve aşağıdakileri içermektedir:

- Tehdit ve tehlikenin belirlenmesi,
- Tehditlere maruz kalan kritik varlıklar,
- Her tehdit olayı için risk kontrol seçeneklerinin ve kategorilerinin bir listesi
- Her bir risk kontrol seçeneği için,
    - Her bir risk seçeneğinin uygulanmasının maliyeti,
    - Risk azaltma etkinliği,
    - Risk azaltma birimi başına maliyet,
    - Maliyet odaklı en iyi risk kontrol seçenekleri (Barnes, 2001).

Aşama 5: Kontrol opsiyonu kararı

Üst yönetim, hazırlanan risk değerlendirme raporunu gözden geçirmekte ve bazı adımlarla en iyi risk kontrol seçeneğini seçmektedir. Kabul edilebilir bir dizi risk değeri oluşturmak mümkündür. Kabul edilebilir risk değerleri aralığı, risk yönetiminin herhangi bir tehdide tahammül etmeye istekli olduğunu göstermektedir.

Mevcut risk değerlerini kabul edilebilir risk değerlerinin aralığı ile karşılaştırarak kabul edilebilir bir risk seviyesine sahip tehditleri seçmek başka bir seçenektir. Mevcut risk değerleri, kabul edilebilir risk değerleri aralığı içerisindeyse seçilen tehditler için risk kabul kontrolü opsiyonu kabul edilmiştir. Diğer bir deyişle üst yönetim, seçilen tehditle bağlantılı olan riski kabul etmeye ve riskin ortadan kaldırılması veya azaltılması için raporda belirtilen herhangi bir seçeneği ihmal etmeye hazır bulunmaktadır.

Mevcut risk değerlerine sahip tehditler, kabul edilebilir risk değerleri aralığının dışında olabilmektedir. Bu tehditlerin her biri için, riski kabul edilebilir seviyeye düşürecek veya tamamen ortadan kaldırabilecek risk kontrol seçenekleri, uygulama adayı olarak seçilmektedir.

Her tehdit için tek bir en uygun risk kontrol seçeneği de belirlenebilmektedir. Bu karar, bir tehdit için risk kontrol seçeneğinin sağlanması gibi yönetimin hedeflerine dayanabilmektedir;

- Risk azaltma birimi başına maliyeti en aza indirir,
- Risk kontrol opsiyonunun uygulanması sonucunda organizasyonda aksamayı en aza indirir,
- Pay sahipleri üzerindeki etkisini en aza indirgemek,
- Kontrol gerçekleştirildikten sonra ek işletme masraflarından kaçınır,
- Uygulamayı tamamlamak için gereken süreyi ve çabayı en aza indirir,
- Bu aşamadaki sonuç, kabul edilebilir risk değerleri aralığı ve risk değerlendirme raporunda tanımlanan her tehdit için (yönetimin risk kontrol kararlarını temsil eden) risk kontrol seçenekleri listesini oluşturmaktadır (Barnes, 2001).

Aşama 6: Kontrol opsiyonu uygulaması

Yönetimin risk kontrollerini uygulamayı amaçlayan kontrol uygulaması, organizasyon tarafından belirlenen proje uygulama talimatlarına ve usullerine göre düzenlenmek durumundadır. Genel olarak, bu aşama her bir risk kontrol seçeneği için bazı ana adımlara bölünebilmektedir. Başlangıçta, risk kontrol opsiyonunun uygulanması için bir fizibilite çalışması yapılmaktadır. Fizibilite çalışması, kontrol seçeneğinin operasyonel, teknik, ekonomik açıdan uygulanabilir olup olmadığını belirlemektedir. Proje fizibilite çalışmasının bulguları, yönetim tarafından sunulacak bir proje fizibilite raporunda belgelenmiştir. Fizibilite raporu oluşturulduktan ve proje finansmanı talebi yayınlandıktan sonra yönetim, proje finansman talebini onaylayıp onaylamayacağına karar vermek için raporu incelemektedir. Risk kontrol projesi uygulama adımı takip edilmektedir. Ancak yönetim risk kontrol projesini ve finansman gereksinimlerini onaylarsa uygulanabilmektedir. Bu aşamada eksiksiz bir proje uygulama planı geliştirilmiş ve uygulanmıştır (Barnes, 2001).

Aşama 7: İzleme ve kontrol

Bu aşama, var olan tehditteki değişikliklerin denetlenmesi ve kuruluşa yeni tehditler eklenmesini temsil etmektedir. Gerekli veya beklenen performans seviyesinden

değişikliği tanımlamak için durumun sürekli denetlenmesi, kritik olarak gözlemlenmesi veya belirlenmesi gibi bir eylem listesinden oluşmaktadır (International Organization for Standardization, 2009). Risk izleme ve kontrol aşaması, organizasyona yönelik tehdit ve risk değişikliklerini değerlendirmek için periyodik risk değerlendirmesi ve risk denetimleri yapmaktadır ve uygun risk kontrol seçeneklerini uygulamaktadır. Risk yönetimi sürecinin bir parçası olarak, izleme ve kontrol faaliyetlerini doğrulama şunları sağlamaktadır:

- Risklerle ilgili varsayımlar geçerli kalmaktadır,
- Dış ve iç içerik dâhil, risk değerlendirmesinin dayandığı varsayımlar geçerli kalmaktadır,
- Beklenen sonuçlara ulaşılmaktadır,
- Risk değerlendirmesi sonuçları gerçek deneyimlerle uyumlandırılmaktadır,
- Risk değerlendirme teknikleri doğru uygulanmaktadır,
- Risk tedavileri etkilidir (International Organization for Standardization ve International Electrotechnical Commission, 2009).

İş etki analizi (BIA)

Bir organizasyonun ve işleyişinin daha iyi anlaşılabilmesi için kullanılan temel teknik iş etki analizi (BIA)'dir. Elliott, Swartz ve Herbane (2010) BIA'nın, tüm BCM sürecinin omurgasını oluşturduğunu ve bir krizin muhtemel finansal ve operasyonel sonuçlarını değerlendirmek zorunda kalması anlamına geldiğini belirtmektedir. BIA, Smith ve Shields'a (2007) göre, iç ve dış temel bağımlılıkların yanı sıra bir organizasyonda var olabilecek doğal riskleri ve zayıf noktaları içeren kritik süreçleri, öncelikleri ve tek başarısızlık noktalarını belirlemeye yardımcı olmaktadır.

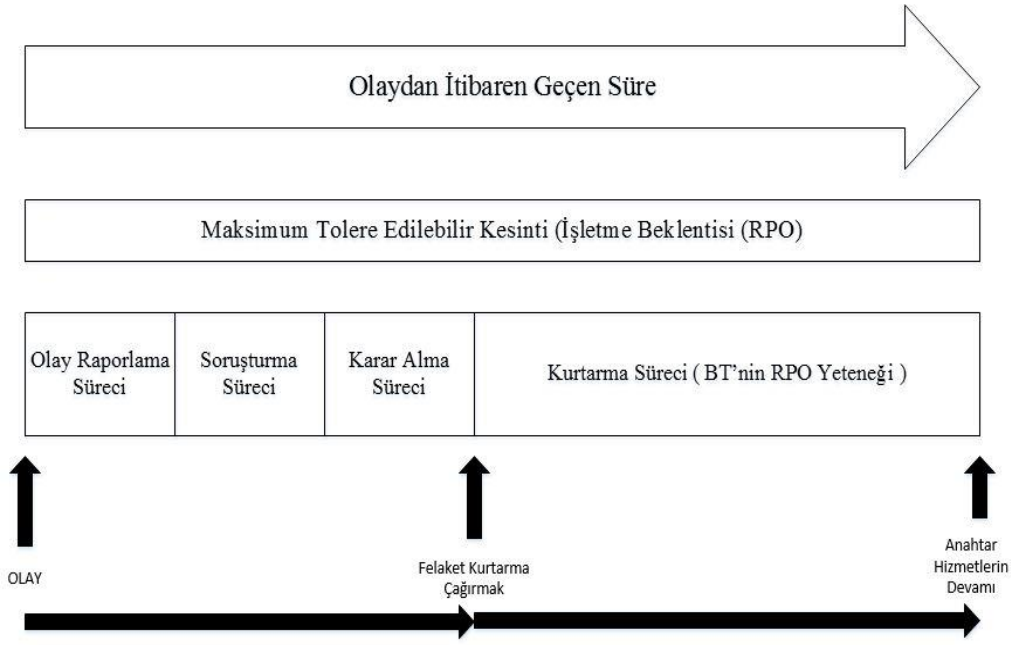
Standartlar, kritik ürünlerin ve hizmetlerin sunulmasını destekleyen her işletme faaliyeti için, organizasyonun zamanla faaliyetler üzerindeki aksamanın etkilerini değerlendirmesini, her faaliyetin maksimum tolere edilebilir bozulma süresini belirlemesini ve birbirine bağlı faaliyetleri tanımlamasını önermektedir.

BIA'nın bir sonucu olarak, BCM uygulayıcıları her iş fonksiyonunun iyileşme zamanı hedeflerini (RTO) belirleyebilmektedir. RTO, bir iş fonksiyonunun iyileştirilmesi

için izin verilen süre olarak Barnes (2001) tarafından tanımlanmıştır. RTO aşılırsa, organizasyona ciddi zarar verilmektedir.

BIA süreci ayrıca, kurtarma noktası hedefi (RPO) hakkında bir fikir vermektedir. Bradbury'ye (2008) göre RPO, işleme döngüsündeki hangi noktadan veri toplanacağını belirlemektedir. Diğer bir deyişle, örgüt ne kadar çok veriyi kaybetmeye hazırdır veya veriyi yeniden girmek zorunda kalmaktadır. Bu noktada BIA, izin verilen maksimum kesinti süresinin (MTPD) değerlendirilmesini sağlamaktadır. Bradbury (2008) tarafından açıklanan MTPD, bir işletmenin ilk hizmet kesintisinde hayatta kalacağı maksimum süre olarak tanımlanmaktadır.

Önlemlerin tümü, BCM uygulayıcılarına daha geniş işletme ve kurtarma gereksinimlerini daha net bir şekilde göstermektedir. İş gereksinimlerinin genel kurtarma hedeflerini belirlediğini unutmamak önemlidir. Bradbury (2008) tarafından özetlendiği gibi, herhangi bir iyileştirme hedefi BIA süreci tarafından belirlenen katı iş gereksinimlerine dayanmak durumundadır. BIA süreci ve olay başlangıç zamanı, olay raporlama süreci, olay soruşturma süreci, karar verme süreci ve RTO'nun geri kazanım süreci arasındaki korelasyonu şematik olarak göstermektedir.



Şekil 1.5. İş Etki Analizi Süreci (Bradbury, 2008)

Bu zaman tahminlerine ve aynı zamanda bozulma nedeniyle ortaya çıkan maliyetlere sahip olmak, yönetimin kıt iyileşme fonlarının ve kaynaklarının nerede tahsis edildiğine karar vermesine olanak tanımaktadır. BIA'ya daha maliyet bilinçli bir yaklaşım benimseyen Myers (2006), bir BIA uygularken BCM'nin maliyetlerini kabul edilebilir seviyelerde tutmak için, başkalarına BCM sorularının sorulduğu bağlamın bildirilmesinin önemini vurgulamaktadır. Myers'a (2006) göre BIA'nın amacı muhtemel kayıpları belgelemek değil, yönetimin acil durum planlamasını yüksek bir öncelik hâline getirmesi veya maliyet yaratan gereksiz işleme kapasitesini aktive etmektir. Myers (2006) tarafından belirtildiği üzere BIA, yöneticileri BCM sürecine katılmada rahat ettirmekte, yöneticileri çeşitli çözümlerle ilişkili maliyetlerde eğitmekte ve tüm seçenekleri değerlendirmeye yardımcı olmaktadır.

Elliott, Swartz ve Herbane (2010), BIA'nın kuruluşların kaynak, sistem ve operasyonlarının bazı belirsizliklerinin bir analizini sunduğuna dikkat çekmektedir. Tam, kapsamlı ve düşük maliyetli bir BCM prosesinin sağlanması için, genel organizasyonun ve iyileştirme ihtiyaçlarının anlaşılması için kapsamlı BIA yapılmasının önemi vurgulanmaktadır.

BCP, bir organizasyonun görev kritik işlevlerini ve süreçlerini etkileyebilecek olası olayların tanımlanmasını talep etmektedir. Varsayımlar bir örgütün tamamen bağlı olduğu alanlar hakkında sıklıkla yapılmaktadır; ancak bu alanlara misyon kritikliği testi uygulanırsa, göz ardı edilen diğer alanlardan daha az önemde olduğu tespit edilebilmektedir. Kritik alanlar tanımlanıncaya kadar iş, bu alanlar kaybolduğunda veya bozulduğunda bir örgüt üzerindeki etki derecesini belirlemeye başlayamamaktadır. Etki seviyesi ciddi olursa, kritik görev veya alanın kaybolmasına neden olacak bir olayla ilgili bir değerlendirme yapılmak durumundadır (Rittinghouse, Ransome ve CISSP CISM, 2011). İş etki analizi, yıkıcı olayların işletme ve iş alanlarındaki finansal ve operasyonel etkisini incelemektedir. Mali etki; kayıp satış, kayıp fonlama ve sözleşmeye bağlı cezalar gibi parasal kayıpları ifade etmektedir. Operasyonel etki, ticari faaliyetlerle ilgili parasal olmayan kayıpları temsil etmektedir ve rekabet avantajı kaybı, yatırımcı güvenini kaybetme, kötü müşteri hizmetleri, düşük personel morali ve iş itibarına zarar verebilmektedir (Syed ve Syed, 2004). İş etki analizi, risk yönetimi aşaması ve iş süreklilik planı geliştirme aşaması arasında önemli bir bağlantıdır (Gallagher, 2003). İş etki analizi,

iş sürekliliği planının ana odağı haline gelen işin kritik alanlarını ve süreklilik gereksinimlerini tanımlamaktadır ve derecelendirmektedir (Barnes, 2001).

İş etki analizi, kritik görev alanlarının ve kuruluş süreçlerinin iyileştirilmesi için gereksinimleri belirtmektedir. İş etki analizi bulguları ile birlikte, risk değerlendirmeden çıkarımlar, başlangıç BCM çabasının yoğunlaştırılması gereken alanları belirleyen bir sıralama sistemi oluşturmak için birleştirilmek durumundadır. Üst düzey yönetim ekibi, üretilen sıralamaları kabul etmektedir. Bu kurtarma gereksinimleri, uygun bir iş sürekliliği stratejisi ve etkili bir iş sürekliliği planı geliştirmenin temelini oluşturmaktadır. Üstelik iş etki analizi, mevcut iş sürekliliği stratejisinin kurtarma gereksinimlerini karşılayıp karşılamadığının belirlenmesine yardımcı olabilmektedir. İş etki analizi yardımıyla işletme fonksiyonlarını sınıflandırmak mümkündür.

- Kritik fonksiyonlar: Bu iş işlevleri bir süre yarıda kesilir veya kullanılamaz durumdaysa, işi tamamen tehlikeye atabilmekte ve işletmenin ağır hasar görmesine neden olabilmektedir.
- Temel fonksiyonlar: Zararları, organizasyonun uzun süre çalışabilme kabiliyetini ciddi şekilde etkileyen işlevlerdir.
- Gerekli fonksiyonlar: Organizasyon işleyişine devam edebilmektedir; bununla birlikte, bu işlevlerin yokluğu etkinliklerini büyük ölçüde sınırlamaktadır.
- İstenilen fonksiyonlar: Bu işlevler faydalı olacaktır; bununla birlikte, yokluğunun örgütün kabiliyetini etkilemeyeceği düşünülmektedir (Snedaker, 2007).

1. Kurtarma zamanı çerçeveleri

Kuruluşlar, iyileşme ihtiyaçlarına göre yukarıdaki sınıflandırmalar için standart iyileştirme süresi çerçeveleri oluşturabilmektedir. Örneğin, bir şirket kritik işlevlerin 1 günden daha kısa bir sürede iyileştirilmesi gerektiğini, aksine 2-4 gün arasında temel işlevleri ve 5-7 gün içinde gerekli işlevleri yerine getirmesi gerektiğini kararlaştırabilir. Aynı şirket, istenilen işlevlerin 10 gün sonra bile geri kazanılabileceğini beyan edebilmektedir (Snedaker, 2007).

2. Kurtarma öncelikleri

İş etki analizi, kuruluşların işletme fonksiyonlarını sıralamasına ve yetiştirilecekleri bir emri çıkarmalarına yardımcı olmaktadır. Başka bir deyişle, iyileştirme önceliklerini tanımlamaktadır (Rittinghouse, Ransome ve CISSP CISM, 2011). İş gereksinimleri listelendikten ve risk değerlendirmesi yapıldıktan sonra, kurtarma için öncelikleri belirlemek daha kolay hâle gelmektedir. Bu öncelikler, birden çok sistemi kurtarmak adına dizinin geliştirilmesi için kullanılmaktadır (Snedaker, 2007).

3. Kurtarma hedefleri

İş etki analizi, her bir süreç için kurtarma süresi hedefi (RTO) ve süreçleri desteklemek için gereken kritik uygulama sistemleri sağlamaktadır. Kurtarma zamanı hedefleri, iyileşme hedefleri olarak görülmemelidir. Aslında kurtarma zamanı hedefleri, tüm planlama sürecine öncelik vermede kullanılabilmektedir (Kavanagh, 2004).

4. Kaynak gereksinimleri

Bir felaket veya kesintiden sonra bir iş fonksiyonunu işlevsel hâle getirmek için kaynak gereksinimlerini ayrıntılı olarak tanımlamak da mümkün olacaktır. Bu altyapı, işgücü, belgeler, kayıtlar, makineler, telefonlar, faks makineleri vb. ne gerekiyorsa tam spesifikasyonları içerecektir. Yeterli ayrıntıya sahip olmak önemlidir, zira afetler durumunda bir miktar panik yaşanması zorunludur ve bu gibi ayrıntılara gelmek mümkün olmayabilmektedir (Snedaker, 2007).

5. Kurtarma süresi gereklilikleri

Kurtarma süresi gereksinimleri çeşitli bileşenlerden oluşmaktadır. Bu bileşenler bir kesintiden kurtulmak için mevcut süreyi ifade etmektedir.

İş etki analizi sonuçlarının bir sonucu, her iş fonksiyonunun kurtarma süresi hedeflerini belirlemektir. Kurtarma süresi hedefleri, bir iş fonksiyonunun kurtarılması için izin verilen süre miktarıdır. Bir sistemin veya fonksiyonun restorasyonunun teknik noktasıdır. Bu, başarısızlıktan sonra işlemlerin yeniden başlatılabileceği başlangıç noktasıdır (Wilder, 2008).

Kurtarma süresi hedefi aşılırsa, organizasyona ciddi zarar verilmektedir. Bu tahminler ve işletme biriminin maliyeti, yönetimin kurtarma fonlarının nasıl tahsis edileceği konusunda bilinçli bir karar vermesine izin vermektedir. Ayrıca iş etki analizi süreci, bilgi servislerinin kritik iş birimlerini destekleyen uygulamalar için belirlenen bir kurtarma süresi hedefi olmasını sağlamaktadır. RPO, bir sistem üzerinde sistem veya işlev bazında geçerli verilerin bilinen en son noktasıdır. Bu, verilerin geri yüklenmesinin başlangıç noktasıdır ve BT tarafı mülkiyetindedir. Maksimum zaman aşımı (MTD) (veya maksimum kapatma zamanı - MDT), günümüzdeki normal günlük etkinlikleri işlerken tüm kurtarma işlemlerinin tamamlandığı noktadır. Bu nokta normal durumdaki işe gerçek dönüştür. İş kurtarma süresi (WRT), krizden kurtulmak için gereken zaman ve çaba miktarını belirtmektedir. Bu nokta, gelen verilerin yeniden girilmesini içermektedir;

- Krizin toparlanma noktasına geri dönme hedefi,
- Kriz noktasından kurtarma zamanı hedefine kadar toplanan elle ilgili veriler,
- Ticari hizmet beklentisiyle güncel kalmak zorunda olan günlük veriler. (Wilder, 2008).

6. Dayanışma

Çeşitli işlevler (iç ve dış) arasındaki karşılıklı bağımlılık, analizin bir parçası olarak elde edilen önemli bilgilerdir. Anketlerden/tartışmalardan toplanan bilgileri bir araya getirirken ve iyileştirme önceliğini tayin edecek işlevleri derecelendirirken, kendileri düşük önceliğe sahip olan ancak bunlara bağlı bazı kritik işlevlere sahip olan işlevleri gözden kaçırmamak gerekmektedir. Bu bağımlılık önem kazanmaktadır (Snedaker, 2007).

7. Maliyetle ilgili hususlar

Maliyetle ilgili düşünceler bu süreç esnasında göz ardı edilmemek durumundadır. Akılda tutulması gereken şeyler şunlardır:

- Gelir zararları ve fırsat kaybı, kurtarma için alınan zaman ile doğru orantılı olacaktır.
- Bir kurtarma stratejisinin maliyeti, bir kurtarma stratejisi için izin verilen süre ile ters orantılı olacaktır.

- Olası kurtarma stratejisinin maliyeti, stratejiyi kabul etmeden önce kesilen gerçek zarar ile karşılaştırılmak durumundadır. Önerilen çözüm öngörülen kayıplardan çok daha pahalıya mal oluyorsa, yatırımın yönetim tarafından gerekçelendirilmesi mümkün olmayacaktır (Snedaker, 2007).

Kritik faaliyetlerin belirlenmesi

BIA tamamlandıktan sonra bu, hangilerinin çok önemli olduğunu ve onları iyileştirmek için yapılması gerekenleri belirlemek için organizasyon faaliyetlerinin analizini sağlamaktadır. Elliott, Swartz ve Herbane (2010) tarafından önerilen bir sonraki süreç, kuruluşun çalışma ortamının sistematik bir analizi ve çıktıları, faaliyetleri ve bağımlılıklarının detaylı incelenmesi yoluyla BIA üzerine kurulmasıdır. Neyin kritik olduğunu belirlemek için Myers (2006), 'kritik olan nedir?' sorusu sorulduğunda, bir felaket sonrasında hangi teknolojiye restorasyon önceliği verilmesi gerektiğini keşfetmektir cevabını vermektedir. Bu analiz aynı zamanda kuruluşun tüm alanlarına da yayılmak durumundadır. Standartlar, bir organizasyonun planlama faaliyetlerini kritik faaliyetlere odaklamak isteyebileceğini, ancak diğer faaliyetlerin de MTPD içinde geri kazanılması gerektiğini belirtmektedir.

BIA ve BCM programının diğer unsurlarının güncellenmiş olmasının önemi üzerinde fazla durulmamaktadır. Koch (2001), tekrar eden bir BIA, kurtarma planı ve teknik gözden geçirme süreci olmaksızın, sonuçta BC programının başarısız ve geçersiz sayılacağını vurgulamaktadır.

Süreklilik gereksinimlerinin belirlenmesi

BIA'nın tamamlanmasının ardından ana kurumsal devamlılığın gerekleri belirlenmiş olacaktır ve literatüre göre bir sonraki gereklilik, her faaliyetin devam etmesi için ihtiyaç duyacağı kaynakları tahmin etmektir. Gerekli kaynaklar şunların hepsi olmasa bile bir kısmını içerebilmektedir: İnsanlar, tecrübe, beceriler, tesisler, destekleyen teknoloji, fabrika, ekipman, bilgi (elektronik veya kağıt bazlı) ve 3. şahıslar veya şebeke sağlayıcıları gibi harici kaynaklar. Daha geniş dış paydaş topluluğunun ihtiyaçları da göz önüne alınmak durumundadır. Elliott, Swartz ve Herbane (2010), BCM'ye atfedilen kriz

yönetimi yaklaşımının bir parçası olarak dış paydaşların etkisini kabul etmenin önemini kabul etmektedir.

BCM sürecinin bu aşamasındaki konulardan biri, kritik iş fonksiyonlarının çalışmasını sağlamak için ihtiyaç duyulan ihtiyaçları tahmin etmenin altında/başarısız olmaktır. Barnes (2001), şartları değerlendirenlerin iş sürekliliğinin her zamanki gibi iş devam etmesi için bir ortam yaratılması anlamına geldiğini varsayan bir eğilim olduğunu kabul etmektedir. Gerçekten de durum küçük bir azınlığın niyeti olabilir, ancak aranan şeyin çoğunluğunda en azından başlangıçta kuruluşun kritik olanı minimalist bir yaklaşımla sürdürmesi mümkündür. Barnes'a (2001) göre sonuçta, BCM sürecinin neyi içerip içermediğine karar vermek CEO'ya (icra kurulu başkanı) ya da üst yönetime kalmıştır.

Kritik faaliyetlere yönelik tehditlerin değerlendirilmesi

Herhangi bir BCM sürecinin literatüre göre önemli bir unsuru, risk değerlendirmesi yapılmasının gerekliliğidir. BCM ile risk yönetimi (RM) veya risk değerlendirmesi (RA) arasındaki çizginin, aslında aynı tehditlere baktıkları için bulanıklaştığı gözlemlenebilmektedir. Vaid'in (2008) belirttiği gibi, operasyonel riske atıf yapılmaksızın BCM hakkında hiçbir konu açığa kavuşturulamamaktadır. RA, bir takım olayların sonuçlarını ve sonuçlarının sonuçlarını ölçme sürecini tanımlamak için kullanılan bir terim olarak Elliott, Swartz ve Herbane (2010) tarafından tanımlanmıştır. Whittet (2008), operasyonel riskin Basel II'de yetersiz veya başarısız iç süreçler, insanlar ve sistemler veya dışsal olaylardan kaynaklanan kayıp riski olarak tanımlandığını belirtmektedir. O'Hehir (2007) RM/RA'yı oluşturan kilit unsurlara değinirken, üst yönetimin/kurulun risk iştahının, iç ve dış risklerin analizinin, riskleri hafifletmek için yapılan kontrollerin ve RM sisteminin bu unsurlarla çalışmasından bahsetmektedir.

Bir kuruluşun risklerini değerlendirmede yardımcı olmak için Charters (2007), kuruluşun faaliyet gösterdiği yerde spesifik tehditler olasılığını değerlendirmek için sigortacılardan, yerel ticaret derneklerinden veya iş sürekliliği kullanıcı forumlarından tavsiye istemektedir. Ve dört ana aşamadan oluşan risk değerlendirmesinden bahsetmektedir ki bunlar: Varlık ve tehdit tanımlama, potansiyel kayıpların miktarının tespiti, kırılganlıkların değerlendirilmesi ve çözümlerin değerlendirilmesidir.

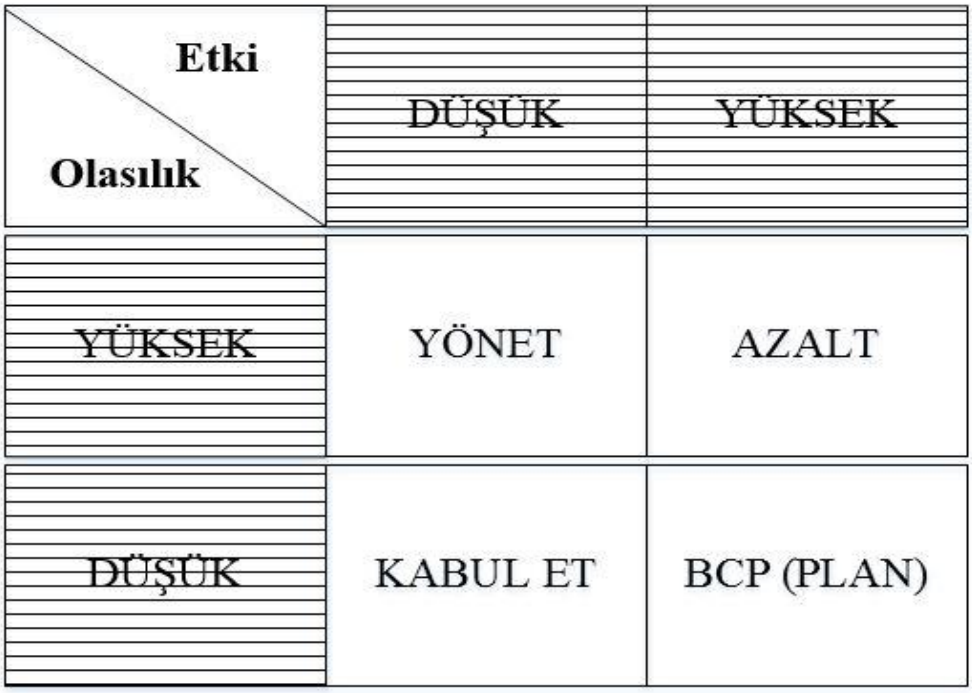
Sheffi'ye (2007) göre bir organizasyonun yıkıcı bir olaya karşı açık olması, bozulma ihtimali ve potansiyel şiddetinin bir kombinasyonundan oluşmaktadır. Bazı risk seviyelerinin tüm faaliyetlerde olduğu gibi bir işletmenin tüm riskleri tamamen kaldırabileceği ihtimali düşüktür, ancak Charters (2007) tarafından da belirtildiği üzere sadece temel iş üzerinde yoğunlaşarak bu durum bir organizasyonun diğer riskleri kaçırmasına neden olabilmektedir. Temel işletme riskleri organizasyon tarafından bir öncelik olarak ele alınmakta ve Gallagher'ın (2003) belirttiği gibi, riskler gerçekçi bir değerlendirme ve yönetime tabi olmaktadır, ancak bu, temel olmayan risklerin ele alınmaması gerektiği anlamına gelmemektedir. Bir organizasyon üzerinde etkiye sahip görünmeyebilecek küçük riskleri göz önünde bulundururken BCM uygulayıcısı, kuruluşlar arasındaki ara bağlantı nedeniyle küçük çaplı bozuklukların hızla yayılabildiğinin farkında olmak durumundadır.

Tehditleri değerlendirirken dikkat edilmesi gereken önemli bir nokta, örgütlerin karşılaştıkları olayların çoğunun küçümsenmesi ya da olayların tam olarak afet olmamasıdır. Ginn (1992), BCP'nin toplam felaketle ve en kötü durumla başa çıkmak için tasarlanmış olmasına rağmen, birçok durumda ortaya çıkan felaketlerin doğada az veya orta derecede olacağını özetlemektedir. Operasyonel risklerle ilgili olarak Whittet (2008), risklerin dâhili dolandırıcılık, dış dolandırıcılık, istihdam uygulamaları ve iş yeri güvenliği, müşteriler, ürünler ve ticaret uygulamaları, fiziksel varlıklara zarar verme, iş kesintisi ve genel olarak kategorilere ayrılabileceğini belirtmektedir. Karmaşık sistemler söz konusu olduğunda en muhtemel olay sonuçlarının ve sonuçlarının belirlenmesinin sorunlu veya son derece zor olabileceği akılda tutulmak durumundadır. Elliott, Swartz ve Herbane (2010) riskin ölçülmesine yönelik herhangi bir girişimin başarısız olacağına dikkat çekmektedir, çünkü matematik ne kadar karmaşık olursa olsun, tüm risk değerlendirmesi doğal olarak değerler yüklüdür.

Risk değerlendirme yöntemleri

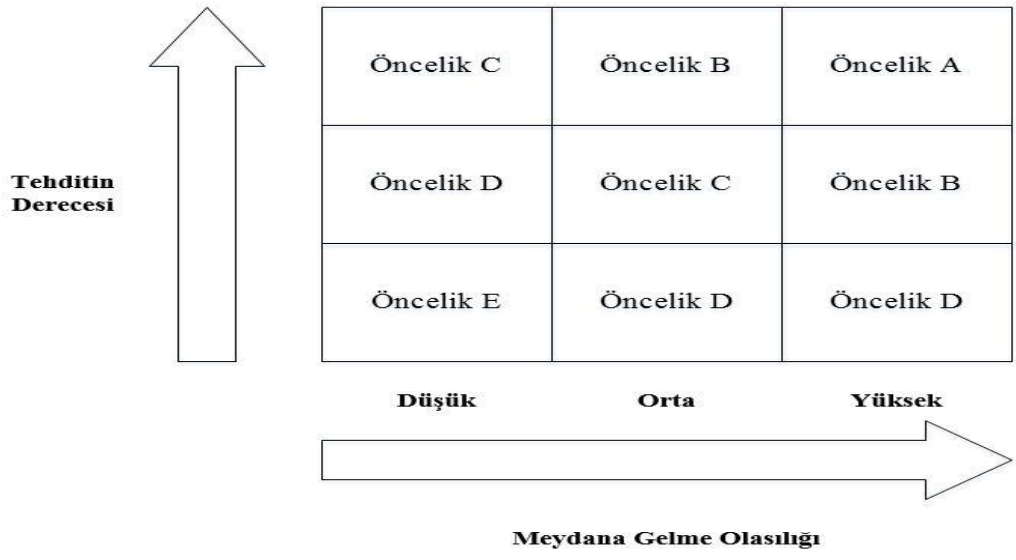
BCM operasyonel risk yönetimi gibi diğer yönetim süreçleriyle yakından alakalıdır. Hiles (2010) tarafından özetlenen operasyonel risk yönetiminin hedefleri, işletmenin hedeflerine ulaşmasını sağlamak için riskleri belirlemek, değerlendirmek ve kontrol etmektir. Riskleri değerlendirmek, bir organizasyonun BIA'sında tanımlanan risklerin

etkisini değerlendirmesine yardımcı olmak ve iyileştirici öncelikleri belirlemek için gözden geçirilen literatürde çeşitli risk matrisleri önerilmektedir.



Şekil 1.6. Risk ve Etki Matrisi (Charters, 2007)

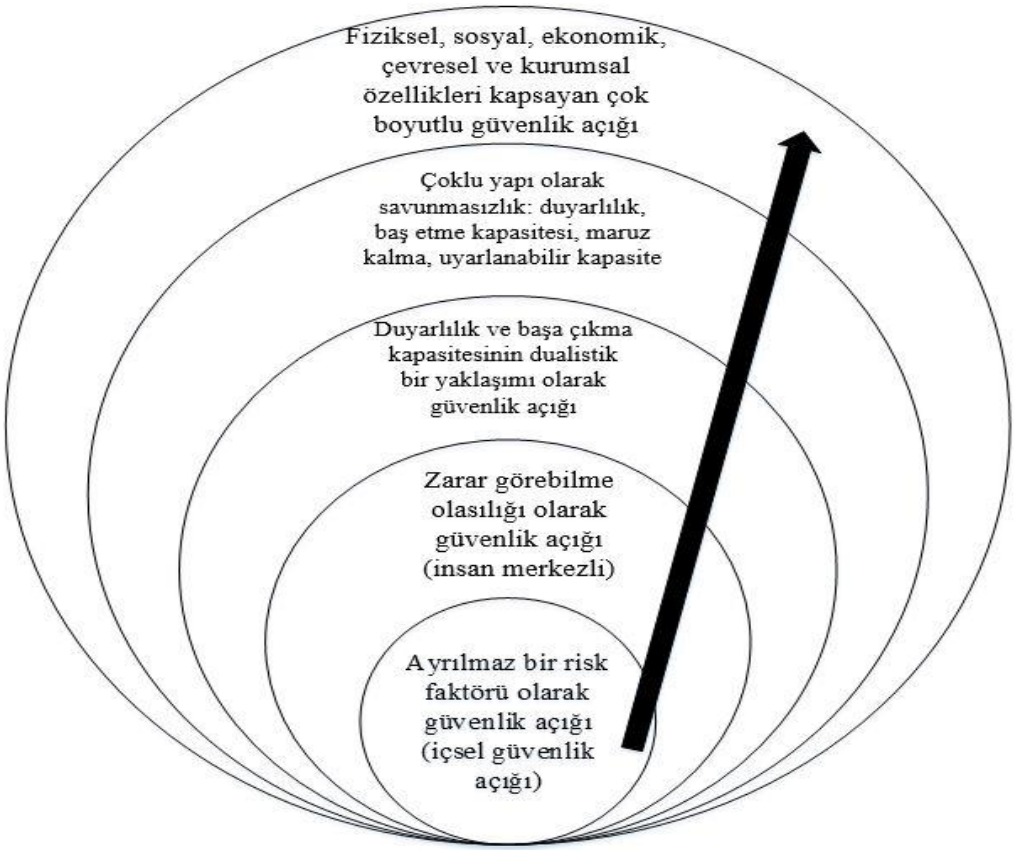
Charters (2007) matrisini kullanırken risk olasılığı düşükse ve etki düşükse risk kabul edilebilmektedir, olasılık yüksekse ve etki düşükse o zaman risk yönetilmektedir.



Şekil 1.7. Risk Değerlendirme Matrisi (Elliott, Swartz ve Herbane, 2010)

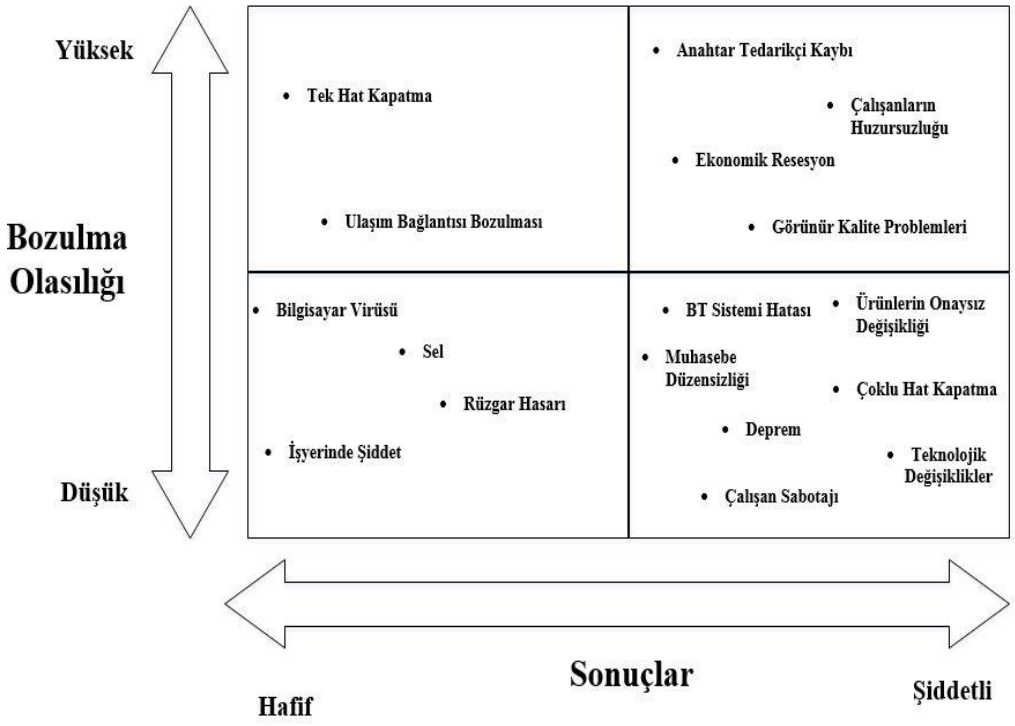
Tabloda özetlenen risk değerlendirme matrisi, risk oluşma ihtimaline ve riskin oluşturduğu tehdidin derecesine bağlı olarak bir risk öncelik yöntemi kullanmaktadır. Risk oluşma şansının düşük, orta veya yüksek olup olmadığına bağlı olarak, o zaman bir öncelik belirlenmektedir. Öncelik A riskleri, ortaya çıkma ihtimali yüksek ve en yüksek olasılıklı olma ihtimali olan riskleri temsil etmektedir. Bu risk matrisleri, soruna biraz farklı perspektiflerden yaklaşmaktadır; örneğin tehdit derecesine karşı etkiler, ancak tümü organizasyonların risk değerlendirilmesi ile sonuçlanmaktadır.

Birkmann'a (2005) göre, yüksek olasılık/düşük etkili olaylar gündelik operasyonların bir parçası olmakla birlikte düşük olasılık/yüksek etkili olaylar planlamayı gerektirmektedir ve günlük operasyonların alanı dışında bulunmaktadır. Birkmann (2005), güvenlik açığı kavramının anahtar alanlarına bir örnek sağlamaktadır ki bu, kuruluşun yüz yüze görülebilecek aksaklıklarını sınıflandırmaya yardımcı olan ve kuruluşların benimseyebileceği yararlı bir araç olabilmektedir.



Şekil 1.8. Güvenlik Açığı Kavramının Anahtar Küreleri (Birkmann, 2005)

Güvenlik açığı haritasının merkezine doğru listelenen güvenlik açıkları kuruluş içinden gelme eğilimindedir, çevrede listelenenler dışardan gelme eğilimindedir. Olası organizasyon güvenlik açıklarının ön plana çıkarılması için kullanılabilecek bir diğer araç ise kurumsal güvenlik açığı haritası (EVM)'dır. Sheffi (2007), yöneticilerin kuruluşlarının güvenlik açıklarını görselleştirmesine yardım etmek ve bunlardan nasıl etkileneceklerini anlamaları adına bir grafik sunum yapmak için EVM kullanılmasını önermektedir.



Şekil 1.9. Kurumsal Güvenlik Açığı Haritası (Sheffi, 2007)

EVM (önceden açıklanan risk matrislerine benzemektedir), riskin olası sonuçlarına ve bozulmanın olasılığına karşı kuruluş için riskleri ölçmektedir. Bilinen riskler değerlendirildikten sonra nadir bulunan olayların ele alınması mümkün olmaktadır. İnsan doğası (belirsizlikle uğraşan), bu göreve kolayca kavuşmadığı için bu kolay bir uygulama değildir.

Nadir olayların öngörülebilirliği

İncelenen BCM literatürü boyunca, ender olaylarla uğraşma teması oluşmaktadır. Taleb (2007) tarafından da belirtildiği gibi, nadir olayların tahmin edilmesi kolay bir alıştırma değildir, çünkü doğaları gereği, sonuçta ortaya çıkan sonuçların tümünü hayal

etmek ya da tahmin etmek genellikle mümkün değildir. Ayrıca insan durumunun, büyük miktarda belirsizlik içeren seyrek olayları görmezden gelmek pahasına normal olana daha kolay odaklanılmasına neden olduğu belirtilmektedir.

Charters (2007), nadir olayların tahmininde yaşanan zorlukların ötesinde, belli tehditlerin belirli yerlerde daha yaygın olması nedeniyle belirli tehditleri değerlendirmede karşılaşılan zorlukların bazılarını vurgulamaktadır: Depremler menşei noktalarına çok uzakta hasara neden olabilmektedir, çoğu BT başarısızlığı kullanıcı tarafından üretilmektedir, dâhili tehditler dışardan olanlardan daha olasıdır, alt katlarda mutlaka sel meydana gelmemektedir (örneğin su depoları çatıya monte edilmişse). Bununla birlikte önceki endişelere rağmen, Elliott, Swartz ve Herbane (2010), risk değerlendirmesi için yapılandırılmış bir yaklaşım kullanmanın, hiç değerlendirme yapmamaktan daha iyi olduğunu savunmaktadır.

ISO/IEC 27001 gibi standart risk değerlendirme çerçeveleri, nadir bulunan olayların veya herhangi bir riskin değerlendirilmesine yardımcı olmak için kabul edilebilmektedir. Böyle bir çerçevenin tipik unsurları, risk kabul kriterlerinin belirlenmesi, organizasyon için kabul edilebilir risk düzeylerinin belirlenmesi ve risk analizinin gerçekleştirilmesidir. Çoğu kuruluşun faaliyet gösterdiği değişen çevre nedeniyle riskler gelip gittiği için devam eden bir risk değerlendirme ve yönetim programı da hayati öneme sahiptir.

Seçeneklerin belirlenmesi

Literatüre göre, risk değerlendirme süreci başladıktan ve BIA ile bağlantılı olarak tespit edilen, kategorize edilen ve öncelik verilen risklerden sonra dikkatin, sunulan çeşitli riskleri hafifletme, kabul etme veya görmezden gelme sürecine kayması söz konusudur.

Standartlar, bu risk azaltma önlemlerinin bazen 4T modeli olarak adlandırıldığına işaret etmektedir. Bunlar; etkisini azaltmak için riski tedavi etmek (treat), tolere (tolerate) etmek yani riski kabul etmek, riski aktarmak (transfer) veya sona erdirmek (terminate) yani riski ortadan kaldırmaktır. Charters (2007), çözümler odaklı bakıldığında risk kontrol önlemlerinin beş kategoriye girdiğini belirtmektedir: Riskin kabul edilmesi, riskin

yönetilmesi, riskin aktarılması, riskin askıya alınması veya feshedilmesi ve riskin planlanması.

Standartlar, her bir risk için bir bozulma olasılığını azaltmak, aksama süresini azaltmak ve önemli kurumsal ürün ve hizmetler üzerinde bir aksamanın etkisini azaltmak için alınan önlemlerin uygulanmasını öngörmektedir. Bu görevleri yerine getirmek için alınacak tedbirlere genellikle kayıp hafifletme, risk tedavisi veya risk kontrolü denmektedir. Elliott, Swartz ve Herbane (2010), BIA'nın ilk BCP hedeflerini yeniden değerlendirip bu hedeflere yönelik riskleri değerlendirdiğini belirtmektedir. BIA, her bir işletme birimi ve fonksiyonunun uygun bir zamanda yeniden başlatılmasını gerektirdiği kaynakları değerlendirmek durumundadır. Böyle bir analiz, birden fazla alternatif yeniden başlatma senaryosu sağlayabilmektedir. Elliott, Swartz ve Herbane (2010), iş etki değerlendirmesi (BIE) olarak BCM sürecinin bu aşamasına değinmektedir ve BIE'nin aşağıdaki faydalardan oluştuğunu açıklamaktadır:

- İş sürekliliği hedefleri rafine edilmektedir.
- Riskler değerlendirilmektedir.
- İş yeri kurtarma öncelikleri belirlenmektedir.
- İş kesintileri senaryoları geliştirilmektedir.

Sonlandırılması

Üst düzey yönetim, diğer BCM evrelerinde olduğu gibi, işin uygun olduğunu ve kuruluşun gerçek bir yansımasını sağlamak için şimdiye kadar BCM sürecinin bir parçası olarak oluşturulan çeşitli belgeleri imzalamak durumundadır. Belge seti, önemli ürünlerin ve hizmetlerin dokümante edilmiş listesini, BIA ve BIE'yi ve risk değerlendirme belgelerini içermektedir.

1.5.3. İş sürekliliği stratejisini belirleme / Dizayn

BIA ve sonraki analizin bir sonucu olarak, bir organizasyon stratejik hedeflerini yerine getirmesini sağlamak adına uygun bir süreklilik stratejisi seçmek için daha iyi bir konuma gelecektir. BCM bağlamında strateji, bir organizasyondaki kilit ürün ve hizmetleri korumak veya yenilemek ve bir olayın ardından kritik faaliyetleri desteklemek adına kabul

edilebilir minimum seviyeye indirmek için kullanılacak alternatif işletim yöntemlerinin belirlenmesi ve seçilmesiyle ilgilidir. Johnson, Scholes ve Whittington (2002) tarafından belirtildiği üzere stratejik kararlar, rakiplere karşı bir avantaj elde etmeye çalışmak ve bir organizasyonun faaliyet gösterdiği kaynakları ve faaliyetleri içinde bulunduğu ortamla eşleştirmek olarak görülebilmektedir. Bir organizasyonun seçtiği BCM stratejisi, rakiplerine kıyasla rekabet avantajı kazanmasına yardımcı olabilmektedir.

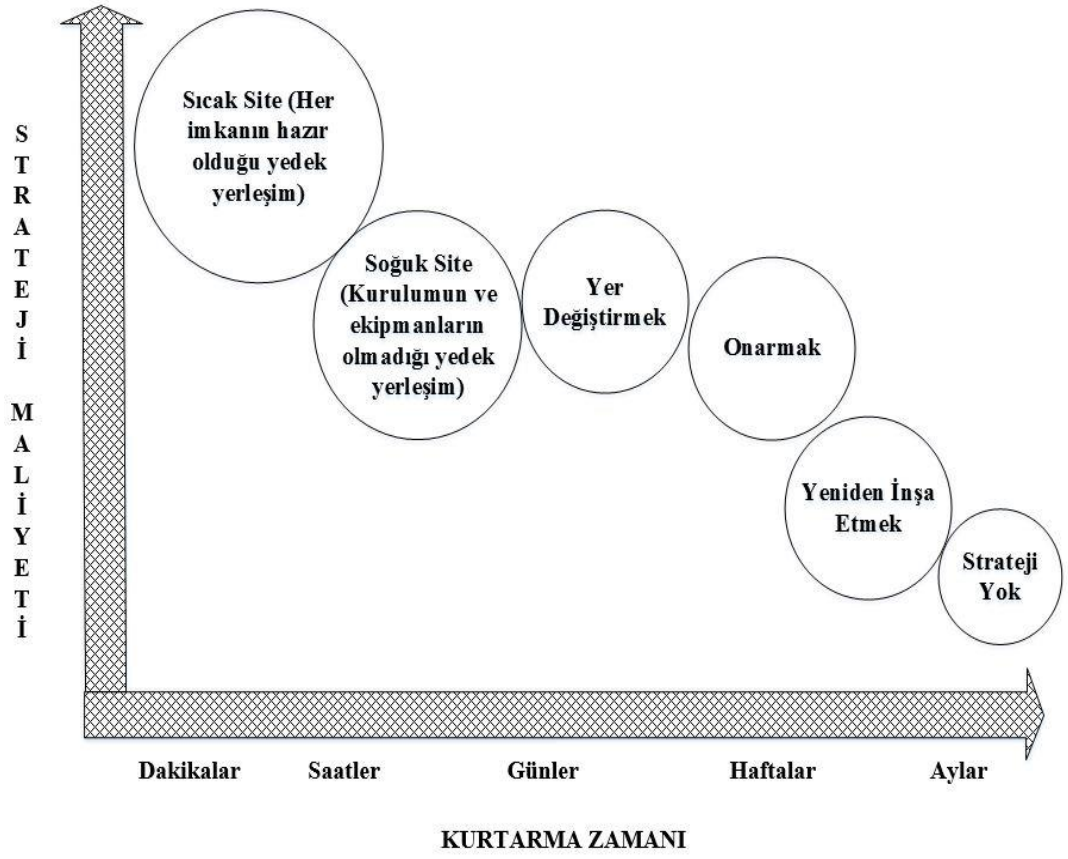
Johnson, Scholes ve Whittington'a (2002) göre strateji seçiminde kültür ve siyaset önemli bir rol oynamaktadır ve strateji karar verme aşamalarını ana hatlarıyla belirtmektedirler; farkındalık vermek, formül hazırlamak, çözüm geliştirmek ve çözüm seçimi yapmak. Bir ürün ya da hizmet için uygun bir BCM stratejisi seçerken, BCM sürecinin bir parçası olarak halihazırda yaratılan dokümantasyonun özellikle BIA'yı kullanması ve organizasyonların temel hizmet/faaliyetlerinin RTO, RPO ve MTPD'lerinin farkında olması tavsiye edilmektedir.

Strateji opsiyonları

Tüm organizasyonlar, kritik faaliyetleri için mevcut stratejik seçenekleri ve bu faaliyetleri sürdürmek için gereken kaynakları düşünmek durumundadır. Hiles (2010), seçilen strateji ne olursa olsun, tamamlanması ve herhangi bir boşluk ya da zayıflık olmaksızın tüm iyileştirme gereksinimlerini karşılaması gerektiğine dikkat çekmektedir. Uygun bir iyileştirme stratejisi seçilirken dikkate alınması gereken diğer faktörler, uygulama veya stratejinin maliyetleri ve hiçbir şey yapmamanın etkilerine dayanmaktadır (British Standards Institution, 2006). Barnes (2001), BCM'den sorumlu olanların, çözümün maliyetine karşı zamanın çeşitli noktalarında (hizmet kesintisi süresi) hizmet dışı olma maliyetini tartması gerektiğini söylemektedir. Burada amaç, etki ve çözüm maliyetinin en aza indirgenmesidir.

Mümkün olduğunca çeşitli alternatif stratejiler düşünülmek durumundadır. Hiles (2010) bu alternatif stratejilerin (en az üç alternatif strateji seçilmesini önerdiğini belirtmektedir) farklı maliyet seviyelerinde kurtarma süreleri ve kesin iyileşme aralığı sağlaması gerektiğini söylemektedir. Her bir stratejinin bir risk analizi, üst düzey yönetime farklı strateji seçenekleri sunulmadan önce yapılmak durumundadır. Standartlar; insanlar, tesisler, teknoloji, bilgi, malzeme, paydaşlar ve sivil acil durumlar için ayrı bir stratejinin

gerekli olabileceğini önermektedir. Barnes (2001) çeşitli kurtarma seçeneklerinin gerektirdiği iyileşme sürelerini grafik olarak göstermektedir. Bu grafik, bir kuruluş kurtarma stratejisinin ne kadar gerçek zamanlı olursa o stratejinin maliyetinin o kadar yüksek olacağını gösterdiği için ilgi çekici niteliktedir.



Şekil 1.10. Geçerli ve RTO'yu Karşılayan BT Stratejileri (Barnes, 2001)

Kuruluş bir iş sürekliliği stratejisi seçerken, kuruluşun kurumsal politikaları içinde kalan ve iyileştirme gereksinimlerini yansıtan bir strateji seçmek durumundadır. Hiles (2010) en uygun maliyetli çözümü seçmeyi savunmaktadır. Seçilen herhangi bir strateji muhtemelen maliyet ile huzur arasındaki dengeyi göstermektedir.

İnsanlar

İnsanlara yönelik BCM stratejileri ile ilgili olarak, kuruluşun temel becerileri ve işletme bilgilerini korumak için uygun stratejileri belirlemesi önerilmektedir. Analizin yalnızca çalışanları içermesi gerekmemekle birlikte, organizasyonun gerektirdiği uzman bilgi ve beceriye sahip yükleniciler ve diğer menfaat sahiplerini de içermek durumundadır.

Standartlar, bir organizasyonun tüm kritik faaliyetlerinin iyi belgelendirilmesi ve organizasyonun daha esnek olması için birden çok beceriye sahip personel sayısının artmasının sağlanması da dâhil olmak üzere, bu becerileri korumak veya sağlamak için kullanılabilecek bir takım stratejileri tanımlamaktadır. Beceri ayrımı ve birden çok personel kaynağı veya üçüncü taraflar kullanımını kapsayan stratejiler, bir kriz olayından kurtulmaya da yardımcı olacaktır.

Perman (2009), özellikle ardıl planlamaya bakıldığında, örgütlerin kilit bir çalışanın ayrılmasına hazırlıklı olmadığında büyük mali kayıplar yaşayabileceğini belirtmektedir. Bir karşılık bulmada yaşanan gecikme ise sıklıkla görülmektedir. Perman (2009) ayrıca, uzatılmış boşluk dönemlerinde projelerin ertelenebileceğini, gelirlerin gerçekleştirilemeyeceğini, müşterilerin kaybedildiğini, inovasyonun genellikle durabileceğini veya yavaşlatılabileceğini, fazla mesai maliyetlerinin artabileceğini ve çalışanların moralinin düştüğünü ileri sürmektedir. Perman'a (2009) göre başarılı bir halef planlama sürecinin başlıca faydaları, düzgün iş geçişleri; adayları yeni görevlerine düzgün bir şekilde hazırlayan görev atamalarının yapılması, anlamlı değerlendirmeler ve geri bildirim sağlaması, önemli kriterlere uygun seçme kriterlerini ve sonuçlarını sağlamasıdır. Devralma planlaması çeşitli biçimlerde olabilmektedir; departmanlar ve bölümler içinde ve dışındaki iş rotasyonu, işe gölge düşürme ve iş paylaşımı da iki kişinin birbirinin rolleri için uyum sağladığı ve bu nedenle çok yetenekli hâle geldiği ve bu nedenle tüm önemli bilgiye sahip olan bir çalışanın risklerini sınırladığı durumlarda kullanılabilmektedir.

Bir BCM programı sırasında insan stratejilerine bakarken yukarıdaki olası etkilerin tümünün dikkate alınması gerekmektedir. Ayrıca kriz zamanlarında en sağlam çalışanlara bile travmatik olaylar nedeniyle aciz verilebileceği akılda tutulmak durumundadır. Gallagher (2003) son zamanlara kadar, bir felaketin insan üzerindeki ve psikolojik etkileriyle ilişkili olarak önemli bir hayat kaybına neden olabileceği yönündeki pek çok planın hemen hemen yok olduğunu belirtmiştir. Bu nedenle, insan kaynaklarının organizasyonun mümkün olan en iyi BC personel stratejilerine sahip olmasını sağlamaları önerilmektedir.

Tesisler

Literatür, organizasyonun normal çalışma alanlarının kullanılmamasının etkisini azaltmak için bir strateji geliştirilmesi gerektiğini not etmektedir. Standartlar, bunun aşağıdaki seçeneklerden birini veya birkaçını içerebileceğini söylemektedir: Kuruluş içindeki alternatif tesisler, diğer kuruluşlar tarafından sağlanan alternatif binalar, üçüncü taraf uzmanlarınca sağlanan alternatif binalar, evden veya uzak yerlerden çalışma, diğer uygun ortam ve kullanım yerleri kurulu bir yerde alternatif bir iş gücünün kullanılmasıdır.

Teknoloji

Literatüre uygun bir teknoloji stratejisi seçmek, kullanılan teknolojinin doğasına ve kritik faaliyetlerle olan ilişkisine bağlı olacaktır. Herbane'in (2010) belirttiği gibi, zamanla ve hızla değişen sistemler ve aletlerle teknoloji alanında hızlı bir gelişme vardır ve organizasyonlar bu gelişmelere ayak uydurmak için süreçlerini uyarlamak durumundadır. Bazen bu sorunlara hazır olmayan kişiler kendilerini, güçsüzlük ve başarısızlık ihtimali olan alanlar yaratan teknolojilerin bir sürümü ile bulmaktadır. Literatüre göre kullanılabilen bazı teknoloji stratejileri; birden fazla BT konumunu korumak, eski ekipmanı acil durum yedeği veya yedek olarak kullanmak, özel veya uzun süre öncülük etmiş ekipman için ek riskleri azaltmak ve bekleme cihazını hazır bulundurmak veya başkasıyla karşılıklı anlaşma yapmaktır. BT hizmetleri sıklıkla karmaşık süreklilik stratejileri gerektirmektedir. Bu stratejileri seçerken, kritik BIA faaliyetlerini destekleyen sistemler ve uygulamalar, teknoloji sitelerinin yeri, sayısı ve uzaklığı, uzaktan erişim seçenekleri, yedek telekomünikasyon yönlendirmesi, yerine getirilen 3. taraf bağlantılarının niteliği, harici bağlantılar ve teknolojisiz sitelerin kullanımı gibi RTO'ya da dikkat edilmek durumundadır. Bu listeye eklenebilecek diğer ögeler, arıza durumunda güç sağlamak için yedek jeneratörlerin sağlanması ve jeneratörler çevrimiçi durumdayken de güç yükünü almak için kesintisiz güç kaynaklarının (UPS'ler) tedarik edilmesidir.

Bütün bu stratejiler maliyet ve karmaşıklıkla birlikte gelmektedir. Üst yönetime sunmak üzere bir veya daha fazla stratejiyi seçmeden önce her stratejinin esasını değerlendirmek BCM koordinatörüne kalmaktadır. BT kurtarma stratejilerinin karmaşıklığı, bugün organizasyonların kullandığı veri miktarındaki artışa bağlı olarak daha da karmaşık hâle gelmektedir. Preimesberger (2009) ve Chen (2007) tarafından

belirlendiği üzere şirketler, hükümetler ve diğer kullanıcıların depoladığı verilerin artması, başka bir BCM meydan okuması sunmaktadır. Chen (2007), bu zorluğa dijital koruma demektedir. Bu fazladan verilerin, maliyet ve komplikasyon eklenerek BCM sistemleri tarafından saklanması ve korunması gerekmekte ve kuruluşlara ciddi bir sorun teşkil etmektedir. Preimesberger'e (2009) göre hızlı veri büyümesi ve daha sonra gelen depolama gereksinimi, bugün yüksek çözünürlüklü video, gözetim videosu, üst seviye video oyunları ve yüksek çözünürlüklü fotoğraf ve grafik verilerinin kuruluşlar tarafından kullanılmasından ve ayrıca iş sürekliliği teknolojilerinin her gün iyileşmesinden dolayı ortaya çıkmaktadır. Chen'e (2007) göre, donanım ve yazılımların sıklıkla yükseltilmeye tabi olması, eski depolama teknolojilerinin tarih dışı kalması nedeniyle veri alım sorunlarına yol açabilmektedir.

BT organizasyonlarının genellikle devam eden BT operasyonlarını desteklemek için yeterli fonları olmasına rağmen, Vizard'a (2008) göre, sağlam bir iş sürekliliği yanıtı dağıtmak için gereken ikincil altyapıyı satın alma noktasında çoğu zaman fon yetersiz gelmektedir. Vizard (2008) bunun nedenini, öncelikle satıcı topluluğunun iş sürekliliğini ek ürünler satma fırsatı olarak görmesine ve altta yatan BT altyapısının dâhili bir iş sürekliliği kabiliyeti sağlayacak kadar akıllı olması gerekliliğine dayandırmaktadır. Vizard (2008) bu sorunun en iyi cevabının, her ürünün ve her cihazın otomatik olarak diğer sistemi desteklediği bir sistemle ilişkili olması olduğunu söylemektedir.

Birçok BT departmanı ve BT sağlayıcısı Vizard'ın vizyonundan uzak olsa da, BT altyapısının satın alma, bakım ve kurulum maliyetleri açısından çaba harcamaya değer bir süreç olduğunun farkına varamamaktadırlar. BT altyapısının iyi gözetilmesi, çok daha net ve daha az karmaşık BT kurtarma stratejileri sağlayacaktır. Bu, belki de mevcut bulut bilişim girişimlerinin kendi BT altyapısını korumak adına kuruluşlara olan ihtiyacını ortadan kaldırarak BCM'ye fayda sağlayabileceği ve bunun yerine, uzman tedarikçi tarafından yönetilen bulut tabanlı bir amaca yönelik altyapıyı kullandığı bir alan oluşturmaktadır.

Bilgi

Bilgi kurtarma stratejileri, kuruluşun operasyonu için hayati önem taşıyan bilgilerin, BIA'da tanımlanan zaman dilimlerine göre korunması ve geri kazanılabilir

olmasını sağlamak için gereklilik arz etmektedir. Kuruluşun kritik faaliyetlerinin yerine getirilmesi için gerekli tüm bilgiler uygun gizliliğe, bütünlüğe, erişilebilirliğe ve değerliliğe sahip olmak durumundadır.

Gallagher (2003), BT sistemlerine, veri tabanlarına ve e-posta tesislerine yapılan örgütsel bağımlılığa rağmen, kağıt dosyaların çoğu kuruluş için hayati kayıtlar oluşturduğunu söylemektedir. İş sürekliliği stratejileri geliştirilirken çoğunlukla gözden kaçırabileceği için bu kağıt temelli kaynağın önemi göz önüne alınmak durumundadır. En belirgin alanlar, imzalanan belgelerin elektronik kopyalarının mevcut olmadığı veya kabul edilemeyeceği yasal belgeler ve sözleşmeler tarafından oluşturulmaktadır. Finans ve insan kaynakları gibi diğer alanlarda da dikkate alınması gereken önemli kağıt kayıtları olabilmektedir.

Bilgi için yedekleme stratejilerinin sağlam olması, düzenli olarak test edilmesi ve bir krizin ortaya çıkması durumunda bunların yeterli olmasını ve organizasyona gerekli olasılık düzeylerini sağlamasını temin etmek büyük önem arz etmektedir. Yedekleme stratejileri, hem teknolojik (teyp ve disk yedeklemeleri) olarak hem de uzman sağlayıcılarla veya alternatif kurumsal yedekleme tesislerinde hayati belgelerin dışında belgelerin depolanmasını içermektedir. Ayrıca, henüz kopyalanmayan veya güvenli bir yere yedeklenen bilgilerin kurtarılması için bilgi stratejileri belgelendirilmek durumundadır (Snedaker, 2007).

Gereçler

BCM literatürü, örgütlerin kritik faaliyetlerini destekleyen temel malzemelerin bir envanterini tanımlamaları ve muhafaza etmeleri gerektiğini özetlemektedir. Standartlara göre devam eden sarf malzemeleri temin etme stratejileri arasında; başka yerlere ilave sarf malzemelerinin depolanması, kısa sürede stoktan teslim eden üçüncü şahısların bulunması, tam zamanında teslimatların başka yerlere bölünmesi, malzemelerin ambarlarda veya nakliye sitelerinde tutulması, alternatif/yedek malzemeleri belirleme bulunmaktadır. Kritik faaliyetlerin uzman tedariklerine bağlı olduğu durumlarda organizasyon, kilit tedarikçileri ve tek bir hata noktasını temsil edebilecek tek tedarik kaynaklarını tanımlamak durumundadır. Arzın sürekliliğini yönetmek için burada kullanılan stratejiler; belirli bileşenlerin birden fazla tedarikçisine sahip olma, tedarikçileri temin etme veya talep etme,

doğrulanmış bir iş sürekliliği kabiliyetine sahip olma, hizmet seviye sözleşmesi (SLA) ile kilit tedarikçilerin veya temel tedarikçilerin belirlenmesine sahip olma gibi süreçler olabilmektedir.

Gallagher'a (2003) göre arz zorlukları genellikle, teslimat sürelerinin artması, tedarik kalitesindeki farklılıklar, müşterilerle olan ilişkilerin gerginleşmesi, müşterilerin normal marka ürünlerini diğer markalarla değiştirmesi ve rakip organizasyonların satışlarını arttırmasıyla sonuçlanmaktadır.

Paydaşlar

Bir organizasyonun kriz zamanlarında tüm paydaşlarına karşı sorumluluğa sahip olduğu açıktır ve buna hem iç hem de dış paydaşlar dâhildir. Turner (1976), belli bir yıla kadar iş sürekliliğinin kısa sürdüğünü, daha sonra kriz olaylarının hem sosyal hem de teknik unsurları içerdiğini dikkate alarak genişletildiğini kabul etmiştir. Bu nedenle BCM, yalnızca teknik tarafı değil, aynı zamanda organizasyon ortamının insan, organizasyonel ve sosyal yönlerini de dikkate almaktadır ve birleşik bir süreç olarak görülmektedir.

Standartlar, uygun BCM stratejileri tasarlarken organizasyonun kilit paydaşlarının çıkarlarını göz önünde bulundurması, yönetmesi ve koruması gerektiğini belirtmektedir. Temel paydaşların çıkarlarını korumak için uygulanacak stratejiler; engellilik, hastalık veya gebelik nedeniyle belirli şartları taşıyan çalışanlar gibi belirli ihtiyaçları olan paydaşlar için özel düzenlemeler içerebilmektedir. Herhangi bir stratejiyi seçerken olduğu gibi, tedarik zincirinin üyeleri de zincirin yukarı ve aşağı taraflarındaki paydaşlar olduğundan, BCM sürecinde daha geniş tedarik zinciri düşünülmek durumundadır. (Oldfield, 2008), geniş tedarik zinciri, sektör ve toplulukta kritik paydaşlarla birlikte destekleyici ortaklıkların geliştirilmesi ve sürdürülmesi tavsiyesinde bulunmaktadır ve aynı zamanda, hangi önemli paydaşların sıkıntılar altında kuruluşu destekleyeceği ve örgütün altını oymaya çaba gösterebileceği konularına dikkat çekmektedir.

Kurumsal sosyal sorumluluk (CSR) alanı da göz önüne alınmak durumundadır. Tencati, Perrini ve Russo (2007) CSR'yi, firmaların sosyal ve çevresel sorumluluk ilkelerini operasyonlarında olduğu kadar paydaşları ile etkileşimde bulunduğu bir kavram olarak tanımlamaktadır.

Tencati, Perrini ve Russo'ya (2007) göre bu tanım, CSR'nin kuruluş ile başlıca dış paydaşlar arasındaki etkileşiminden ve bir diğeri de CSR ilkelerini örgüte entegre eden bir iç değişim sürecinden gelen iki farklı şekilde izlenebileceğini göstermektedir. Collicutt (2009) tarafından belirtildiği gibi, CSR ilkelerini örgüte entegre eden birçok organizasyon şimdi kurumsal sorumluluğu bir iş türevi ve olası rekabet avantajı kaynağı olarak görmektedir; bu nedenle CSR'nin BCM stratejilerine dâhil edilmesi çok büyük önem arz etmektedir.

BCM programlarında çoğunlukla göz ardı edilen paydaşlardan biri gerçek çalışanlardır. Gallagher (2003), çoğu planın varlıkların kaybına dayandığını ve insanların çoğunlukla ikinci derecede önem taşıdığını söylemektedir. Bunun nedeni BCM'nin kökeni ve temel olarak teknik odaklı bir disiplin olan felaket kurtarma (DR) içindedir. Organizasyon, bir olayı takiben refah sorunlarının sorumluluğunu yerine getiren bir kişiyi (normalde insan kaynakları departmanı dâhilinde) tanımlamak durumundadır.

Medya

Kurumların literatürde tanımlanan kriz sırasında medyayla uğraşmak için net bir strateji geliştirmeleri gerekmektedir. Barnes (2001), yalnızca uygun medya eğitimine sahip CEO veya atanmış personelin medyayla ilgilenmesine izin verilmesini tavsiye etmektedir. Gallagher (2003), felaket durumunda medyayı yönetmek için her organizasyonun açık, iyi anlaşılmış ve iyi provası yapılmış bir medya politikası, medya planı ve medya eğitimli sözcüsü olmasının kuruluş için hayati önem taşıdığını söylemektedir. Medyayla uğraşırken, BC olaylarını duyururken kirli çamaşırlarınızı halkla yıkama olarak bir unsur bulunmaktadır. Bu nedenle, organizasyon açısından medyaya özlü ve tutarlı bir mesaj verilmesi hayati önem taşımaktadır.

Sivil acil durumlar

Sivil acil durumlar, örgütün durumunun artık kontrolü altında olmaması, sivil yetkililerin ve acil servislerin emrinde olması nedeniyle, daha geniş topluluk üzerinde etkili olan ve organizasyonlar için belirli bir zorlayıcı olan acil durumlardır. Sivil acil durumlar polis ve yerel yetkililerden oluştuğundan, dolayısıyla sivil acil durumlar için BCM stratejileri oluştururken, organizasyonun bu dış ajanslarla birlikte çalışıp dâhil edilmesini

ve daha geniş planların farkında olmasını sağlamak için bu ajanslarla yakın çalışması gerekmektedir. Herhangi bir BCM stratejisi tasarlarken, Gallagher (2003), birçok BCP'nin fabrika kapısında bittiği gibi herhangi bir planın acil servisleri içermesi gerektiğini de not etmiştir. Acil hizmetler söz konusu olduğunda genellikle BCM organizasyonunda bir boşluk vardır ve bu boşluklar göz ardı edilemez; bu durum acil durumlarda rol konusunda karışıklık doğuracaktır. Sivil acil durumların erken evrelerine baktığımızda yerel yetkililerin, acil servislerin ve diğer müdahalecilerin hayat kurtarmak, hasarın yayılmasını sınırlandırmak ve işletmelere yardımcı olmaktan çok temel araçlardan kurtulmak üzerine odaklandıkları belirtilmektedir (Collicutt, 2009).

Sivil acil durumlarla mücadele stratejileri hakkında kuruluşlara pek az tavsiyede bulunulmaktadır veya hiç tavsiye verilmemektedir. Bununla birlikte, kamu sektörünün bir sivil acil durumla nasıl başa çıkacağı ve öncelik listesindeki kuruluşların sivil yetkililer için ne kadar düşük seviyede görüneceği konusunda özel sektör için bir görüş ortaya konmaktadır. Özel sektör kuruluşları büyük bir acil duruma iki şekilde dâhil olabilmektedir. Örneğin, acil durumun meydana geldiği alanın (sitenin) mülkiyeti veya acil durumla ilgili bazı unsurların sahipliği yoluyla dâhil olabilirler; bir uçak, otobüs, fabrika vb. gibi alanlarda kullanılabilmektedir. Ayrıca temel müdahale ajanslarında normalde tutulmayan ya da bulunmayan uzman servis ve teçhizatları sağlayarak büyük bir acil duruma müdahale etmeye yardımcı olması için çağrılabilmektedir (M.E.M. Project Team, 2011). Bu nedenle, sivil acil durumlarla mücadele stratejisinin örgütsel BCM sürecinin bir parçası olması önemlidir. Bu da, acil durum esnasında her birinin oynadığı rolü anlamak için yerel yetkililerle temas kurmayı ve aynı zamanda kuruluşların BCM stratejisinde yer alanlarla ilgili olarak onlarla bilgi paylaşmayı içermektedir. Gallagher (2003), herhangi bir BCM stratejisine yerel acil durum hizmetleri dahil edilmesinin önemini vurgulamaktadır ve bir felaket gerçekte gerçekleşmeden önce iş süreklilik planlarının hazırlanmasında acil servislerle yakın bir çalışma gereksiniminin olduğunu belirtmektedir. (Gallagher, 2003)'e göre, bir felaketle baş etmede ekipler rollerini, prosedürlerini ve uygulamalarını anlamak ve örgütsel BCP'yi daha etkili hâle getirmek için hangi girdiyi sağlayabileceklerini bilmeleri gerekmektedir. Ayrıca örgütsel BCP oluştururken daha geniş toplumu da göz önünde bulundurmak önemlidir. Kuruluşlar, Snedaker'a (2007) göre, işletmeler için toplumda esneklik geliştirmeye başlamak durumundadır. Toplulukların esnekliği, işletmelerin büyük bir bölgesel veya ulusal acil durumun etkilerine dayanmasına yardımcı olacaktır.

Collicutt (2009), üç temel topluluk gruplandırması olduğunu söylemektedir: Yerel topluluklar, işlevsel toplumlar ve bilgi temelli topluluklar. Somers ve James (2009), yerel yönetimlerin sivil acil durumlarda özel sektörü kapsaması gerektiğinin ve acil durumların etkili bir şekilde yönetilmesinin, kurumların ve devletin farklı kademelerinde ve özel sektörde geleneksel olmayan bağlantılarının yapılmasını gerektirdiğinin altını çizmektedir.

Yerel düzeyde acil durumları daha geniş bir Avrupa düzeyinde değerlendiren Rhinard (2009), ulus devletler arasında daha geniş bir uluslararası iş birliğini savunmaktadır ve hükümetlerin ve kamu kurumlarının kökenleri sınırlarının dışına çıktıklarını, ancak içinde etkileri olan krizle baş etmede güçlük çekeceklerini belirtmektedir. Rhinard (2009), Avrupa ülkelerinin teknolojik yenilik, ekonomik entegrasyon ve siyasi ortaklık yoluyla yakından örülmüş olduğunu savunmaktadır. Tek piyasa, birbirine bağlı altyapılar ve insanların, malların ve hizmetlerin serbest dolaşımı için sistemler bulunan ortak çözümler üretilmiştir. Bu çözümler genellikle refah ve barış getirmesine rağmen, yeni sorunları da hızlandırmıştır. Birden fazla eyalet arası bağlantı, karşılıklı bağımlılık oluşturmaktadır ve bu bağımlılıklar tehditlerin büyük ölçüde sınırsız bir Avrupa alanında hareket etmesine ve tırmanmasına izin vermektedir. Literatür ve özellikle Fritzon, Ljungkvist, Boin ve Rhinard (2007), kritik altyapıların korunmasının tam olarak sağlanmasının, günümüzün hayati sistemlerinin çok karmaşık ve geniş bir tehdit dizilimine karşı çok savunmasız olmasından dolayı imkansız olduğunu savunmaktadır. Bununla birlikte örgütsel acil durum stratejilerine bakıldığında, kuruluşlar üzerinde etkili olabilecek devletler arası bağlantıların olası etkilerine dikkat edildiğinde onlarla başa çıkmak için uygun düzenlemeler yapılması hayati önem taşımaktadır.

1.5.4. BCM tepkisinin geliştirilmesi ve uygulanması / Uygulama

BCM yaşam döngüsünün bu bölümü, organizasyonel iş devamlılığını ve bir olayın etkili bir şekilde yönetilmesini sağlamak için uygun plan ve düzenlemelerin geliştirilmesi ve uygulanması üzerine yoğunlaşmaktadır.

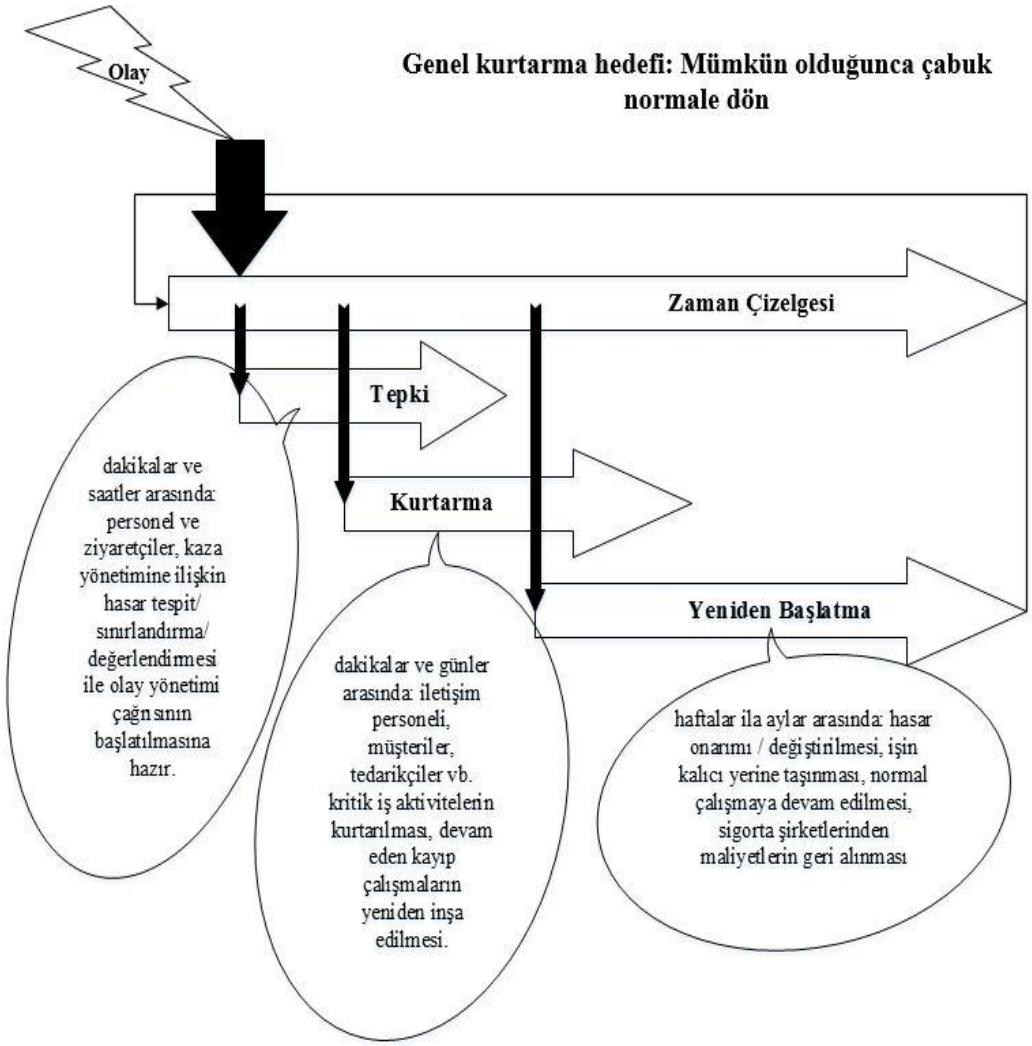
Olay tepki yapısı

Örgütler, standartlara göre, etkili bir yanıt vermeyi ve kesintilerden kurtulmayı sağlayan bir olay tepki yapısı kurmak durumundadır. Bu yapı, organizasyonun olayın

doğasını ve boyutunu doğrulamasını, kontrolü ele geçirmesini, olayı içermesini ve kilit paydaşlarla iletişim kurmasını sağlayacak kapsamda, basit ve hızlı bir şekilde oluşturulmak durumundadır. Çoğunlukla olay yönetim ekibi (IMT) veya kriz yönetim ekibi (CMT) olarak da adlandırılan bu yapı, herhangi bir iş sürekliliği yanıtı için tetikleyici olmaktadır. IMT veya CMT, olayı yönetmeye yardımcı olacak plan ve prosedürlere sahip olmaktadır ve kritik faaliyetlerin devamlılığını veya iyileştirilmesini sağlamak için iş sürekliliği araçları tarafından desteklenmektedir. Olay tepkisinin harekete geçirilmesi, işletilmesi, eşgüdümü ve iletilmesi için planlar da olmak durumundadır.

Ekiplerin bu bağlamda önemi, Elliott, Swartz ve Herbane (2010) tarafından vurgulanmıştır. Elliott, Swartz ve Herbane (2010), ekipler acil durumlar bağlamında genellikle bireylerden daha iyi oldukları için ekiplere önem verildiğini belirtmektedir. Literatürde ilk tepki ekibi için çeşitli isimler önerilmiştir ve Barnes (2001) ana olay tepki ekibini acil durum yönetim ekibi (EMT) olarak adlandırmıştır. Organizasyonların çizelge rehberinde ekip yapısının tasarımına izin vermesi gerektiğini savunmaktadır. EMT, herhangi bir acil durum sırasında personelin güvenliğini sağlamak, bir felaket bildirmek, kurtarma ekiplerini etkinleştirmek ve kurtarma çabalarını yönetmekten sorumludur. (Barnes, 2001), EMT'nin genel müdür olarak CEO gibi en üst düzey yöneticiden oluşmasını tavsiye etmektedir.

Elliott, Swartz ve Herbane (2010), önemli olayları yönetmek için alternatif bir komut ve kontrol yapısı sunmaktadır ve bir organizasyonun olaya tepkisinin iyi yönetilebilmesini sağlamak için İngiliz polis teşkilatının kullandığı bronz (operasyonel), gümüş (taktik) ve altın (stratejik) olmak üzere üç kademeli bir yapı kullanıldığını öne sürmektedir. Bu yapı, acil durumlara daha önceden hazırlanacağı gibi tepki vermeyi de kolaylaştıracaktır. Elliott, Swartz ve Herbane (2010), ikinci komuta ve kontrol yapısını önermekle birlikte, her organizasyonun kendine özel yapıları gerektirdiğini de kabul etmektedir. Aşağıdaki şekil, bir olayın zaman içindeki üç ana safhasını (olay tepkisi, BC ve kurtarma/yeniden başlatma) ve olay yönetimi ile iş devamlılığı arasındaki ilişkiyi göstermektedir.



Şekil 1.11. Olay Zaman Çizelgesi (British Standards Institution, 2006)

Quarantelli ve Dynes (1977), BCM sürecini başlatma kararını verirken dikkate alınması gereken birkaç ayırt edici özellik bulunduğuna, kuruluşun düzeylerine göre karar verme oranının arttığına ve kararların sayısının azaldığına dikkat çekmektedir. Quarantelli ve Dynes (1977), örgüt üyeleri arasında daha az istişarenin var olduğunu belirtmektedirler ve bu bireysel özerklik, örgütsel personelin ve kaynakların, genellikle yeterlik alanındaki önceki organizasyonların dışında hızlı bir şekilde işlendiği anlamına gelmektedir. Onların görüşüne göre, örgütler yeni koordinasyon düzenlemelerinin kontrolü altına girdiğinde genellikle özerkliklerini kaybetmektedirler. Organizasyonların içinde krizle alakalı bölümler, yangın hizmetleri gibi, karar alma özerkliği kazanmaktadır. Quarantelli ve Dynes (1977) ayrıca örgütsel iletişimin karar verme sürecinin bir parçası olarak görülmesi gerektiğini ve içerik, kanal ve bağlamda farklılaşmayı içerdiğini belirtmektedir. Genel olarak stres koşulları altında, öncelikle teknolojik faktörlerden ziyade sosyal iletişimin

bozulmasından sorumludur. Krizler sırasında bulaşmanın teknolojik formlarındaki artış, yalnızca bilginin hacmini arttırır, doğruluğu arttırmaz ve bu nedenle harmanlama ve entegrasyon gereksinimini artırır. Son nokta BCM için önemli bir noktadır. Bir kriz olayında önemli olmayan iletişimlerin filtrelenmesi, doğru hizmetlerin doğru sırada ve doğru zaman çizelgelerinde geri getirilmesini sağlamak, kurtarma işlemlerine katılanlar için hayati öneme sahiptir. Gereksiz iletişim sadece kurtarma işlemini engellemektedir. Organizasyonun tüm unsurları bir dereceye kadar olay yönetim sürecine dahil edilmektedir. Burası, BCM'nin sıklıkla risk yönetimi ve kriz yönetimi gibi diğer disiplinleri kapsayan birleşik bir süreç olarak görüldüğü yerdir.

Hiles'ın (2010) belirttiği gibi, bir organizasyon BCM'nin iyileştirme sürecini ne kadar çok uygularsa, bir kriz meydana geldiğinde bu süreci çağırmak o kadar kolay olur ki hazırlık aşaması olaylara tepki verirken anahtar noktadır. Acil durumun tek bir tür olay olmadığı ve genellikle çok geniş kapsamlı ve çok sayıda unsurdan oluştuğu literatürde belirtilmektedir. Bir kurtarma programının özellikleri, genellikle bir felaket meydana geldiğinde belirlenebilmektedir. Myers (2006) ve Fink (1986) felaketin doğasına, afetin meydana geldiği noktaya ve kesintiye uğrama dönemine bağlı oldukları etkili bir kriz yönetimi planının önemli kararları önceden belirlediği gerçeğine değinmektedirler.

Her kriz olayı olaydan etkilenen organizasyon adına farklı süreçler sergileyeceği için, kriz olayı ve tam normal faaliyete dönme anı arasında geçen ve önceden ayarlanmış belirli bir zaman yoktur. Standartlar, örgütsel iyileşme planlarının (işlemleri normal duruma geri döndürme planları) derhâl uygulanamayacağını belirttiğinden, belirli olaylardan sonra bir süre için normalin ne olduğunu tanımlamak mümkün olmayabilmektedir. Bu nedenle kuruluşların, kurtarma planlarının yürürlüğe konması için genişletilmiş operasyonlara izin veren BCP'ye sahip olmaları istenmektedir.

Planların içeriği

Literatür, planların (olay yönetim planları, iş sürekliliği planları, iş kurtarma planları), sorumlulukları planlarda belirtilenler için özlü ve erişilebilir olması gerektiğini belirtmektedir. Her plan, amacı ve kapsamı (üst yönetim tarafından kararlaştırıldığı gibi), rollerin ve sorumlulukların ayrıntıları, planın nasıl çağrılabileceğine ilişkin bilgi, ilgili irtibat bilgileri, görev ve eylem listeleri, kaynak gereksinimleri ve ilgili formların kopyaları

hakkında ayrıntı içermek durumundadır. Herhangi bir planda, ele alınacak kritik faaliyetler için öncelikli hedefler, kritik faaliyetler için iyileştirme seviyeleri, zaman çizelgeleri ve her planın kullanılabileceği durumun net bir açıklaması da bulunmak durumundadır. Bu planların herhangi birinin çağrılma yönteminin mümkün olduğunca çabuk çağrılabilmesi için açıkça belgelenmesi ve anlaşılması önemlidir. Uygulama ve BCM egzersizleri ile kuruluş, çeşitli BCM planlarının başlatılması konusunda daha bilgili ve rahat konuma gelecektir (Snedaker, 2007).

Olay yönetim planı (IMP)

IMP dokümantasyonunda organizasyon IMT, CMT veya EMT aracılığıyla bir olayın başlangıç aşamasını standartlaraa göre yönetebilmektedir. British Standards Institution'a (2006) göre IMP, ilk olaydan daha fazla kayıpların önlenmesini, kuruluşun paydaşları ile nasıl iletişim kuracağına ilişkin bilgileri, BIA'nın sorumlularının listelerindeki bilgilerin listelenmesi gibi BIA'ya dayanan görev ve eylem listelerini, ilk yardım, çalışan iletişimi vb. gibi ayrıntıları içermek durumundadır. İçeriği ne olursa olsun, IMP'nin modüler olması ve olayla ilgili tüm bilgilerin bir olay durumunda ele alınması için kullanımının kolay olması önem arz etmektedir.

IMP'nin bir parçası olan önceden belirlenmiş olay yönetimi konumlarıyla ilişkili olarak Gallagher (2003), önceden belirlenmiş bir yerde afet grevleri yaşamanın hayati önem taşıdığında bir mekan arayışı meselesi olmaması gerektiğini söylemektedir. Elliott, Swartz ve Herbane (2010), CMT'nin etkili olabilmesi için, kararları ve bilgileri sürekli olarak soracak olan insanlardan oluşması gerektiğini düşünmektedir. Hızlı ve etkili uygulamalara izin vermek için ilgili süreçlerin, kişilerin ve iletişim kanallarının yerinde olması gerekmektedir. Kararları ve bilgileri sürekli soranların CMT'ye dâhil edilmesi, bir krize tüm açılarından bakılmasını ve ilgili soruların uygun zamanda sorulmasını sağladığından önemlidir.

Acil durum operasyonlarından kurtarma operasyonlarına geçiş, organizasyonun acil durumun yerini ve hasarın başlangıç tahminlerini veya algılamalarını bilmesi durumunda başlamaktadır. Hiles'in (2010) belirttiği gibi, acil durum prosedürleri mantıksal olarak iyileşmeye, iş sürekliliği prosedürlerine ve faaliyetlere yol açmak durumundadır.

İş sürekliliği planlaması (BCP)

Bir iş sürekliliği planının temel amacı, bir kuruluşun normal iş operasyonlarının aksaması halinde faaliyetlerini iyileştirmesini veya sürdürmesini ve bu faaliyetlerin hepsi ya da bir kısmının bir olayın cevabının herhangi bir aşamasında çağrılabilmesini sağlamaktır (British Standards Institution, 2006).

BCP'nin birçok biçimi gözden geçirilmiş literatürde mevcuttur, ancak Gallagher (2003), birçok formatın ve yazılımın bir BCP kurmada yardım sağlamak için mevcut olmasına rağmen, tüm organizasyonlara uyan tek bir format bulunmadığını söylemektedir. Bir BCP'nin önerilen içeriğini özetleyen çok çeşitli listeler mevcut bulunmaktadır ancak, standartların bir BCP eylem planına dâhil edilmesi gereken daha önemli ögelerden bazılarını vurgulaması dikkat çekicidir. Öncelikli eylem ve görevlerin kontrol listeleri; planın nasıl çağrıldığı ve kimin tarafından çağrılma kararının alındığı, planın başlatılması için karar alınırken kimlerin bilgilendirileceği/bilgilendirilmesi gerektiği, kişilerin nasıl tahsis edildiği, kuruluşun harici olarak harekete geçirdiği durumu veya üçüncü parti kaynaklarından ve nerede olduklarından, bilgilerin nasıl iletildiğinden ve manuel geçici çözümler veya sistem kurtarma hakkında bilgilerden oluşmaktadır.

BCP ayrıca, işyeri kurtarımı için farklı zamanlarda gereken farklı kaynakları (insanlar, tesisler, teknoloji, sarf malzemeleri, paydaşların yönetimi ve bilgi) tanımlamak durumundadır. Ayrıca BCP'de, bir olay sırasında alınan kararlar hakkında bilgi kaydetmek için destek ve olay günlükleri için gerekli olabilecek hem iç hem de dış kişiler için BCP güncel iletişim bilgilerini yöneten sorumlu kişi(ler) de olmak durumundadır.

Bir organizasyon için uygun olan şeyler bir dizi faktöre bağlıdır ve bazı durumlarda BCP, Gallagher'a (2003) göre önemli kişilerin listesinden biraz daha fazla olabilmektedir. Gallagher (2003), kuruluşlara çok karmaşık bir plana sahip olmalarına karşı uyarıda bulunmaktadır; bu plan hiçbir plana sahip olmamaktan daha kötü olabilmektedir ve muhtemelen zamanla tüm planları başarısızlığa götürecektir.

Gallagher (2003) tarafından kısaca özetlendiği gibi iyi bir planın özellikleri; basit, stratejik, pratik, olasılık (planın etkinleştirilme ihtimalini hesaba katan), esnek ve kolay

sürdürülebilir olmasıdır. Bundan dolayı, aşırı ayrıntılı BCP kullanmanın ve ayrıntıya ışık tutmak zorunda kalmanın zorluğu arasında bir denge kurulması gerekmektedir.

1.5.5. BCM egzersizi, gözden geçirme ve devam ettirme / Doğrulama

Literatür boyunca BCM düzenlemelerinin egzersiz, sürdürme ve sürekli gözden geçirilmesinin önemi vurgulanmaktadır. Sağlam bir BCM programı, bir kuruluşun BCM düzenlemelerinin egzersizle doğrulanmasını, düzenli olarak gözden geçirilmesini ve güvenilir olduğundan emin olmak için güncel tutulmasını sağlamak durumundadır. Gallagher (2003), değişim oranı ve iş ortamının giderek artan teknolojik gelişmişliğinin BCM alanında önemli zorluklar doğurduğunu belirtmektedir. Bir planın güncellenmiş ve alakalı tutulması iş sürekliliği koordinatörünün karşı karşıya bulunduğu en zor görevlerden biridir. Gallagher (2003) tarafından özetlenen örgütlerin karşılaştığı zorluklardan bazıları; düzenli yeniden yapılanmalar ve yeniden şekillendirme, dönüşüm, değişim ve rasyonalizasyon süreçleri, birleşme ve devralmalar, hızlı teknolojik değişim oranları, tam zamanında yapılan düzenlemelere olan bağımlılığın artması, daha fazla dış kaynak kullanımı, daha esnek çalışma uygulamaları, bilgi kaybına yol açan personel devri ve erken emeklilik düzenlemeleri ve sanal ofis düzenlemeleridir. Bunların hepsi, bir BCM koordinatörünün planı güncel tutma kabiliyetini etkilemektedir ve bu nedenle kuruluş değişikliği gerçekleştiğinde güncel tutulması ve düzenli güncellemelere tabi tutulmasını sağlamak için BCM sürecinin kuruluşta yer alması önem arz etmektedir.

Egzersiz programı

Herhangi bir BCM programının parçası olarak, zamanla BCP'nin öngörüldüğü gibi çalışmasını sağlayacak bir egzersiz programının hayata geçirilmesi esastır. Gallagher'a (2003) göre BCP'nin test edilmesi/uygulanmasının önemi vurgulanmak durumundadır. Tatbik edilmemiş bir planın uygulanabilir olduğu söylenemez ve gerçekte bir plan kullanıldığında ve ortaya çıktığı zaman konular belirginleşeceğinden yanlış bir güvenlik duygusu sağlayacaktır. Bir BCP'yi egzersiz yapmak standartlara göre kuruluş için birçok avantaj getirmektedir. Egzersiz, bir organizasyonun olayı iyileştirme, BCP'nin tüm kritik faaliyetleri içerdiğini doğrulama, ele alınması gereken herhangi bir varsayımın altını çizme, BCP'nin çalışmalarını güvence altına alma, BCM'nin farkındalığını arttırma, etkinliği doğrulama becerisini uygulama olanağı tanımaktadır ve kritik faaliyetlerin

restorasyonunun zamanında yapılmasını ve birincil müdahale ekiplerinin ve alternatiflerinin yeterliliğini göstermektedir. Bradbury (2008), test yapıldığında planları, süreci, insanları ve altyapıyı test etmenin öneminden bahsetmektedir. Ana test hedefleri; iyileştirme süreçlerini ve prosedürlerini uygulamak, personeli proses ve ilgili dokümanlarla tanıştırmak, dokümantasyonun çalıştığını doğrulamak, iyileştirme hedeflerine ulaşılabilir olup olmadığını belirlemek ve strateji ve süreçler için gerekli iyileştirmeleri belirlemektir.

Egzersiz planları, literatürde önerilen çeşitli şekillerde yapılabilmektedir. Egzersiz seçenekleri arasında şunlar bulunmaktadır: Simülasyon egzersizleri, bileşen fonksiyonel veya dönme testi ve tam canlı BCP testi. Hiles'a (2010) göre kullanılabilen bazı diğer test türleri ise şunlardır: Bileşen testi, BT testleri, kaskad testleri, çağrı testleri, çağırma testleri, ortam testleri, kurul seviyesi testleri. Egzersiz programı planın tüm teknik, lojistik, idari, usul ve operasyonel sistem unsurlarının zaman içinde uygulanmasını sağlamak durumundadır. Aynı zamanda bu program, BCM düzenlemelerini ve ilgili altyapıyı kullanmak ve personel taşınması da dâhil olmak üzere BT iyileşme planlarını doğrulamak durumundadır. Bir egzersiz senaryosuna yaklaşırken Gallagher (2003), egzersizin amacına, katılan taraflar ve kaynaklara, beklenen egzersiz sonuçlarına ve çeşitli egzersiz kilometre taşlarına ulaşılma zamanlarına ilişkin net bir fikir veren dokümante edilmiş bir egzersiz planının kullanılmasını önermektedir. Standartlar, testler sırasında bozulma riskini ortadan kaldırmak için alıştırmaların gerçekçi, özenle planlanmış ve paydaşlarla mutabık kalması gerektiğini not etmektedir. Tüm egzersizlerin net amaç ve hedefleri olmakta ve egzersizden sonra ders almak adına bir tartışma toplantısı yapılmaktadır. Tamamlanmayı sağlamak için BCP'ler ve IMP'ler uygulanmaktadır. BCM egzersizlerinden ve testlerden öğrenmek, BCM programının önemli bir parçasıdır. Olaylardan öğrenmek, daha iyi genel kurumsal esnekliği sağlar ve olaylar meydana geldiğinde BCM süreci bu öğrenmeyi yakalamaktadır (Crichton, Ramsay ve Kelly, 2009). BCP'nin test edilmesi ve uygulanması, planın her yönüyle sürekli olarak hazır olmasını sağlamaktadır. Elliott, Swartz ve Herbane'e (2010) göre testin dört temel yararı vardır:

- Kuruluşun çalışmaya başlamadan önce yürüyebileceğinden emin olunması,
- Gururun azaltılması (bir planımız var, bu yüzden güvendeyiz vb. tavırların),
- Sürdürülebilirliği ve denetimi iyileştirme,
- Farkındalığın korunması.

Testleri düzenli olarak yapmaya duyulan ihtiyaç literatürde açıkça görülmektedir. Alexander (2005), planların tekrarlanan bir döngüyle periyodik olarak test edilmesini ve güncellenmesini tavsiye etmektedir. Genellikle, yılda en az bir kez planı test etmek için masa üstü veya saha çalışması ve en az altı ayda bir kez kapsamlı bir revizyon yapılmak durumundadır. Cari detaylar ve veriler doğruluk açısından kontrol edilmeli ve plan Alexander'a (2005) göre optimum işlevselliğini sağlamak için ayarlanmış olmak zorundadır. Yapılan her test, çeşitli BCP'nin içeriğini doğrulamakta ve organizasyonda bir olay meydana gelmesi durumunda, planların gerektiği gibi işlev görmesini sağlamak için belli bir düzeyde güvence vermektedir.

BCM düzenlemelerinin sürdürülmesi

Literatür, BCM düzenlemelerini güncel tutmak için, kuruluşu etkileyen dahili veya harici değişikliklerin BCM ile ilgili olarak gözden geçirilmesini sağlamak adına açıkça tanımlanmış ve belgelendirilmiş bir BCM sürdürme programının mevcut olması gerektiğini belirtmektedir. Tanımlanan yeni ürünler veya hizmetler, BCM sürdürme programına dâhil edilip edilmeyeceklerini görmek için BIA ve RM yoluyla değerlendirilmektedir. BCM sürdürme programının sonuçları, organizasyonun BCM'de yapılan tüm varsayımları gözden geçirmesine ve meydan okumasına olanak tanımaktadır ve resmi bir değişim kontrol süreci altında güncellenmiş veya değiştirilmiş BCM politikası, stratejilere, çözümlere, süreçlere ve planlara yayılacaktır.

Elliott, Swartz ve Herbane'e (2010) göre sürdürme, planın güncel ve alakalı olup olmadığını görmek için gerekli olan faaliyetleri kapsayan genel bir terimdir. BCP'nin test veya inceleme yoluyla düzenli olarak tutulması gerektiğini savunmaktadırlar. Standartlara göre BCM sürdürme süreci, BCP kuruluşlarının yönetimi ve yönetişiminin kanıtını belgelemek, gerekli temel kişilerin eğitildiğini doğrulamak, kuruluşun karşılaştığı risklerin izlendiğini ve kontrol edildiğini kanıtlamak ve örgütsel değişikliklerin BCP ve IMP'ye dâhil edildiğini kanıtlamak durumundadır.

BCM düzenlemelerinin gözden geçirilmesi

Gallagher (2003) ve British Standards Institution (2006) tarafından belirtildiği üzere, başlatılacak çok miktarda başlangıç çalışması, risk azaltma önlemleri getirilmesi,

iyileştirme stratejilerine karar verilmesi ve başlangıç planlarının oluşturulması gibi çalışmalar, daha az yoğun bir tempoda da olsa, gelecekte de devam edecektir.

Üst düzey yönetimden devam eden taahhüt, BCM sürecinin devam eden uygunluğunu, yeterliliğini ve etkinliğini sağlamak adına gözden geçirilmesi için üst yönetimin devam etmesi gerektiğini bildirmesi yönüyle önemlidir. Belgelenmiş inceleme, BCM politikasının ilgili kanunlara, standartlara ve düzenleyici gerekliliklere uymasını sağlamak durumundadır. Bir BCM egzersizinin sonucu, politika veya stratejik kayma veya değişikliklerle bağlantılı olarak, gereken değişiklikleri belirtmeyi önemsemektedir. İncelemeler periyodik olarak yapılmak durumundadır ve bunlar dahili veya harici denetim veya öz değerlendirme şeklinde olabilmektedir. Bu incelemeler, BCM sürecinin güncel tutulmasını ve paydaşlar tarafından unutulmamasını sağlamaktadır. Başlangıçtaki BCM eğitimi tamamlandıktan sonra, BCM eğitiminin organizasyon içinde canlı olması ve BCM eğitiminin devam eden bir programı ortaya koyması da önemlidir. Gallagher'a (2003) göre, iş ve planlar değiştikçe ve personel gelip gittikçe, BCM eğitim ve bilinçlendirme programının devam ettirilmesi ve üst yönetimin taahhütünü sağlamak için bilinçlendirme programları şeklinde eğitim verilmesi gerekmektedir.

1.5.6. BCM'nin örgüt kültürüne katıştırılması

BCM'yi direnç açısından büyümeye devam etmek ve kriz zamanlarında temel işlevleri ve çıktıları sürdürmek adına bir organizasyonun kültürüne sağlam bir şekilde bağlı kılmak için güçlü bir liderlik gerekmektedir (Snedaker, 2007). BCM'ye girmek, organizasyonda işin yapılma şeklini değiştirmeyi içerebilmektedir (Deal ve Kennedy, 1982). BCM'nin yerleştirilmesi ve kaynak kullanımı yoğun kurumsal iş ortamında birçok rekabet önceliği olan yönetim için bir sorun olabilmektedir. BCM, kuruluşun ve yönetiminin aksamalara karşı baş edebilmesi için müşterilerin, tedarikçilerin, personelin ve fon sağlayıcıların paydaşlarına güven duyarak kuruluşun temel değerlerinin bir parçası hâline gelmek durumundadır.

Uluslararası standardizasyon teşkilatı (ISO) standartları, BCM'nin bir organizasyona tam olarak nasıl gömüleceğini belirtmemektedir. Bebeklik döneminde bir işletme uygulaması olarak, kuruluşlarda BCM'yi yerleştirmeye yönelik literatürde eksikliğin bulunduğunu belirtmekte fayda bulunmaktadır. Bu çalışmalar; vizyon, vizyonun

strateji ve plana dönüştürülmesi, vizyonun iletişimi, üst yönetim taahhütü, örgütsel değişim için destek, değişim sürecinde sürekli iyileştirme gibi noktalara katkısı bulunacaktır. Kültür, BCM yaşam döngüsünün her aşamasına nüfuz etmektedir ve sertifikasyon amaçlarıyla bir kuruluşun BCM sistemi değerlendirilirken BCM denetmenleri tarafından önceliklendirilmektedir. Hiles'a (2010) göre olgun organizasyonlar, iş sürekliliğini kurumsal bir değer olarak birleştiren güçlü bir kültüre sahiptirler. Etkin BCM'nin öncüsü, bir organizasyonun kültürü içindeki tam gömülülük başarısıdır.

1.6. İş Sürekliliği ve Risk Yönetimi Arasındaki İlişki

İş sürekliliği yönetimi, risk yönetimi ile ayrılmaz bir ilişkiye sahiptir. Geleneksel düşünce, risk yönetimini iş sürekliliğinde kullanılmak için bir araç olarak konumlandırırken daha çağdaş düşünce, risk yönetimini belirsizliği, bilinçli karar vermeyi ve hedeflere ulaşmada sürprizliği anlamak için geniş bakış açısına sahip bir felsefe olarak görmektedir. Bu düşünce aynı zamanda, BCM'yi organizasyonun bozulmasına neden olan risklerin yönetimini (olay öncesi ve sonrası) dikkate alan geniş bir risk yönetimi alanının ayrılmaz bir parçası olarak görmektedir (Gibson ve Love, 2006).

Gibson ve Love (2006) risk ve iş sürekliliği konusundaki bu çağdaş yaklaşımın faydaları arasında aşağıdakileri sunmaktadır:

- BCM süreci boyunca daha kapsamlı bir risk hesabı,
- BCM ve risk yönetimi faaliyetleri arasındaki entegrasyonun geliştirilmesi:
    - Riskle ilgili bilgi akışının geliştirilmesi,
    - Her iki faaliyetin gereksinimlerini daha iyi anlamak,
    - Aynı bilgi seti için tekrarlanan taleplerin azaltılması,
    - İş sürekliliği ile ilgili olanlar da dâ"hil olmak üzere öncelikli riskler üzerine örgütsel bir odaklanma,
    - Kaynakların daha maliyet etkin bir şekilde kullanılması,
    - Yalnızca reaktif planlamadan ziyade iş geliştirme konusundaki BCM etkinliğinin iyileştirilmiş bir odağı.

Risk yönetim süreci ile iş sürekliliği süreci arasındaki örtüşme gösterilmektedir; burada iş sürekliliği yönetimi için çerçeve tanımı, risk yönetimi çerçevesinin tanımının bir

parçası olarak yapılabilmektedir. Bir iş etki analizi yapmak riski değerlendirmenin bir uzantısıdır ve iki görev aynı anda organizasyonun karşılaştığı riskleri, bunların oluşma ihtimalini ve kuruluşun devam etme kabiliyeti üzerindeki etkisini tam olarak öğrenmenin bir yolu olarak kullanılabilmektedir. Bununla birlikte, kritik süreçlerin gerektirdiği kaynakları ve normal çalışmayı engelleyen bir olay olması durumunda iyileşme için zaman çizelgelerini belirlemek için iş sürekliliği aşamasında daha fazla çalışma yapılması gerekmektedir.

Kurtarma stratejisini belirlerken, operasyonun sürekliliği ile ilgili daha fazla risk vurgulanacak gibi görünmektedir. Bunlar daha sonra risk yönetimi sürecine geri beslenmektedir. Riskleri kabul etmek veya riski tedavi etmek için bir eylem planı geliştirecek kararlar alınmaktadır. Bu da daha sonra iş sürekliliği sürecine dönüşebilmektedir. Risk yönetimi sürecinde risk tedavisinin aşamaları; riski önlemek, paylaşmak, korumak veya değiştirmek için yapılacak işlemi belirlemektedir. Riski değiştirmek için bir yöntem, süreklilik için bir plan uygulayarak etkisini azaltmaktır: Bu durum süreklilik kontrolleri olarak literatürde yer bulmaktadır. İş sürekliliğinin yalnızca kalıcı (devamlılık) riski kapsamanın bir yolu olarak görülmesi ve dolayısıyla bir önleyici kontrol olarak görülmeyen iş sürekliliği konusundaki klasik yaklaşımı temsil etmektedir. Standartlar, önleyici kontrollerin iş sürekliliği yönetiminin bir parçası olduğu risk yönetimi ve iş sürekliliği için daha entegre bir yaklaşım sunmaktadır (European Union Agency for Network and Information, 2008).

1.7. BCM ve Organizasyonel Esneklik (OR)

Standartlarda belirtildiği gibi BCM, kilit paydaşların, itibarın, markanın ve değer yaratan faaliyetlerin çıkarlarını koruyan etkili bir yanıt verme becerisine sahip örgütsel esneklik oluşturmak için bir çerçeve sunmaktadır. BCM'nin organizasyonel esneklik (OR) üzerindeki etkisinin analizi, BCM perspektifini genişletmek ve BCM'yi OR'ye götüren daha kapsamlı bir yaklaşım oluşturmak için risk, kriz ve acil durum yönetimi gibi diğer disiplinlerle birleştirmeye çalışmaktadır. Esneklik kelimesi, ilk önce 1626'da kaydedilen ve direnmek anlamına gelen 'resiliens' ve 'resiliour' latince sözcüklerinden türetilmiştir. Oldfield (2008) tarafından belirtildiği üzere esneklik sözcüğünün konusu şirket, işletme, duygusal, bireysel, örgütsel, sektörel ya da toplumsal olabilmektedir. Her iki durumda da

amaç farklı olabilmektedir. Ancak her biri değişimi zarif bir şekilde emme ve çalkantılı bir ortamda istikrarlı kalma gibi ortak temel unsurlara sahiptir.

Organizasyonel esnekliği (OR) sağlamak için OR'nin bir unsuru olan BCM'nin kuruluş ortamının insan, örgütsel ve sosyal yönlerini dikkate alması gerektiği kabul edilmektedir. BCM'nin bu genişletilmiş görünümü onu OR alanına taşımaktadır. BCM'nin önemi sadece organizasyon içinde değil, tedarik zincirinin hem yukarı hem de aşağı akışının olduğu gibi organizasyonun harici işletim ortamı üzerinde vurgulanamamaktadır. Coles ve Buckle (2004) esnekliğin boyutlarını tanımlamaktadır ve etkilenen toplulukların kurtarma sürecine katılımlarının önemini vurgulamaktadır. Birleşik Krallık hükümeti 2004 sivil muhakemeler yasasında yer alan yerel yönetimlere, işyerlerine ve gönüllü kuruluşlara BCM konusunda tavsiyeler vermekle yükümlüdür. Bu görev, yerel işletmelerin aksamadan daha çabuk kurtulabilmelerini ve bir kategorideki tüm katılımcıların bir iş sürekliliği yönetim planına sahip olmalarını sağlamayı amaçlamaktadır. Bu yasanın arkasındaki fikir esnek bir iş dünyasının dirençli bir ülke yaratılmasına yardımcı olmasıdır.

BCM'nin tüm organizasyon süreçlerinin her aşamasında yer alan örgütsel geniş bir süreç olması gerektiği kabul edilmekle birlikte, mevcut düşünce BCM'yi, risk, güvenlik, acil durum ve BC yönetimi de dahil olmak üzere kapsamlı bir yaklaşım olan OR şemsiyesi altına taşımaktadır. OR elde etmek için kuruluşların BCM veya risk yönetimi ötesine geçmesi ve esneklik kavramı geliştirmesi gerekmektedir. Cummings (2003), bir organizasyonun hazırlanabilmesi için süreklilik kültürünün gerekli olduğunu belirtmektedir. Örgütsel esneklik bir organizasyonu Elwood'a (2009) göre, karşı karşıya kalabileceği zorluklara cevap verebilmek için uyarlanabilen bir canlı organizma kavramına benzer şekilde görmektedir. Esneklik ile ne denmek istediğini daha iyi anlamak için, Orr ve Horne'un (1998) tanımına bakmak gerekmektedir. Esneklik, bireylerin, grupların, organizasyonların ve sistemlerin kapsamlı bir kalitesidir ve uzunca bir gerileyen davranışa maruz kalmadan beklenen olayların bozulmasına neden olan önemli değişikliklere üretken cevap vermektir (Orr ve Horne, 1998). OR kavramı yeni bir şey değildir ve 1990'ların sonunda BCM alanında düşünme ufku olarak kabul edilmiştir. OR bir sistemin, sistem parçalarının bileşimi/kompozisyonu, yapısal bağlantıları ve çevresel değişikliğin iletildiği ve sistemin her tarafına yayılımına dayanan çevresel yüklerin streslerine dayanması kabiliyetidir. Ayrıca değişen derecelerde esneklik, bireylerde, gruplarda, organizasyonlarda ve sistemlerde bir bütün olarak bulunan temel bir niteliktir. Bu durum, gerileyen/üretken

olmayan davranışa neden olmaksızın beklenen olayları bozan önemli değişikliğe olumlu bir yanıt vermektedir. Paylaşılmış misyon ve planlama duygusu, OR'yi gerçekleştirmede hayati faktörlerdir. Literatürde bilişim teknolojilerinin hayati bir rol oynadığı da belirtilerek, kuruluşların kendi yetkinliklerinin ve karşılaştığı zorlukların farkında olması gerektiği belirtilmiştir. Organizasyonların krizlerden ve yıkıcı ekonomik kaymalardan kurtulmalarına yardımcı olmak için bir süreç olarak OR kavramları Riolli ve Savicki (2003) tarafından daha da genişletilmiştir.

Esnek organizasyon kavramı, örgütlerin zor ya da yıkıcı ekonomik zamanlarda hayatta kalmalarını ve gelişmelerine yardımcı olabilecek bir kavram olarak popülarite kazanmıştır. Örgütsel düzeyde OR, çevik tepkiler ve yıkıcı, talepkar ve kasvetli çalışma koşulları altında sağkalımın devamı ile ilgilidir. Riolli ve Savicki (2003) ayrıca uyarlanabilirliğin geride kalan sıkıntıda önemli bir bileşen olduğuna da işaret etmektedir. Orr ve Horne'a (1998) göre OR, yedi kurumsal davranışsal akıştan (topluluk, yetkinlik, bağlantılar, taahhüt, iletişim, koordinasyon ve düşünme) oluşmaktadır. Ayrıca örgütlerin bugün karşılaştıkları tek değişimin değişim olduğunu iddia etmektedirler. Bu durum, değişime uyarlanabilir esnek bir organizasyon kültürü uygulanmasını gerektirmektedir. Elwood (2009), maddi ve maddi olmayan unsurları ele alan kuruluşlara dayandığını göz önüne alarak, bina inşasında doğru yönlendirmeyi seçmeyi ve başarının temelini oluşturmayı ve iş sürekliliği yönetimi standardını rehber olarak kullanmayı savunmaktadır.

DR'den BCP'ye ve BCM'ye ve daha sonra BCM'ye OR'nin bir parçası olma yolundaki gelişimi, son 40 artı yıl içinde yavaş yavaş meydana gelmiştir. Daha önce de belirtildiği gibi, BCM sadece bir olaya tepki vermek ve sadece DR, CM, RM veya teknoloji kurtarma hakkında değildir. BCM, bir organizasyona ürün ve hizmet sunma şeklini gözden geçirmek ve bozulma, kesinti veya kayıplara karşı direncini artırmak için bir çerçeve verebilen bir ticari faaliyettir.

1.7.1. Organizasyonel esnekliğin tanımlanması

Horne (1997) OR'yi, sistem parçalarının birleşimi ya da kompozisyonu, yapısal bağlantıları ve çevresel değişimin tüm sisteme yayılması ile iletilme şekli üzerine bir sistemin çevresel yüklemenin streslerine dayanması yeteneği olarak tanımlamaktadır. Horne (1997) çeşitli derecelerde direncin kişilerin, grupların, kuruluşların ve sistemlerin

genelinde bulunan temel bir nitelik olduğunu belirtmektedir. Bu, gerileyen/üretken olmayan davranışa neden olmaksızın beklenen olayları bozan önemli değişikliğe olumlu bir yanıt vermektedir. OR temel olarak, organizasyonun faaliyet gösterdiği ortamdaki önemli değişiklikler karşısında ne kadar esnek olduğuyla ilgilidir.

1.7.2. Esneklik karakteristikleri

Coutu'ya (2002) göre üç temel özellik dirençli insanları ve şirketleri diğerlerinden ayırmaktadır. Bu özelliklerden bir veya ikisine sahip olmak sıkıntıdan sıyrılmayı mümkün kılmaktadır, ancak gerçek esneklik her üçünü de gerektirmektedir. Coutu (2002) tarafından özetlenen ilk özellik, gerçekliği kabul etme ve karşı karşıya yükleme kapasitesidir. Bunu yapmak, zorluklara katlanmak ve hayatta kalabilmek için kendinizi eğitmenize yardımcı olmaktadır. İkinci olarak, esnek insanlar ve kuruluşlar yaşamın bazı yönlerinde anlam bulma yeteneğine sahiptirler ve değerler anlam kadar önemlidir. Esnek şirketlerde değer sistemleri zamanla çok az değişmekte ve sorun yaşandığı zaman kullanılmaktadır. Esnekliğin üçüncü özelliği doğaçlama becerisidir. Her zamanki ya da belirgin araçlara gerek duymadan problemleri çözme becerisi büyük bir güç olarak kabul edilmektedir.

OR'a BCM perspektifinden bakıldığında özünde esnekliğe sahip kuruluşlara, yani yüksek esnek organizasyonlara (HRO) bakmak mantıklı olacaktır. Güç sağlama, petrol endüstrisi ve nakliye ile ilgili organizasyonların, bu tür sanayilerdeki başarısızlıkların etkileri büyük sonuçlar doğuracağından, HRO'lar olması muhtemeldir. Burke, Wilson ve Salas (2005), bir HRO'nun temel özelliklerini operasyonlara duyarlı, basitleştirmek için isteksiz, başarısızlıktan kaygı duyan, esnekliğe bağlı ve uzmanlığa saygı olarak tanımlamaktadır.

1.7.3. Organizasyonel esnekliğin kurulması

Brouggy'ye (2009) göre OR, bir organizasyonun pek çok unsuruna nüfuz etmektedir ve performans yönetimi, iş mükemmellik çerçeveleri, kurumsal sürdürülebilirlik, BCM, DR ve toplam kalite yönetimi (TQM) gibi birçok örgüt disiplini ve işleminde bulunmaktadır. Lengnick-Hall ve Beck (2009) bir örgütün dayanıklılık kapasitesini, kuruluşun uzun vadeli sağ kalımını tehlikeye atma potansiyeline sahip

beklenmedik ve güçlü olaylarla karşı karşıya kaldığında duruma özel, sağlam ve dönüştürücü eylemleri alma becerisinin belirlediğinden bahsetmektedir.

Hiles (2010) BCM ve OR'a özel olarak bakıldığında, OR'u oluşturmak için bölümler arası ekiplerin kullanılmasını savunmaktadır ve organizasyonların iş sürekliliğine yaklaşımının genel kurumsal planlamanın bir parçası olduğunu, kavramın sahibi olmak için çapraz bir departman ekibi kullandığını, kendi teknolojilerini ve süreçlerini halihazırda inşa edilmiş bir süreklilik unsuru ile birlikte sunduklarını not etmektedir. Bu yaklaşım başlangıçtan itibaren sürece esneklik kazandıracağından, örgütsel esneklik düzeyinin yükselmesini sağlayacaktır. OR'a sahip olmak, bir organizasyonda değişimin (hem iyi hem de kötü) daha verimli bir şekilde yerleştirilebileceği anlamına gelmektedir. Lengnick-Hall ve Beck'e (2009) göre, stratejik çeviklik yanında, esneklik kapasitesi kuruluşların değişen koşullara etkili bir şekilde cevap vermesine yardımcı olmakta, ciddi bir sarsıntı sonrasında restorasyonun temelini sağlamakta ve ayrıca organizasyonun bir sonucu olarak ve son derece zor bir tecrübenin üstesinden gelerek olumlu bir dönüşüme fırsat verebilmektedir.

Esnek bir organizasyon oluşturmak, emniyet ve OR hedefleri genellikle diğer organizasyonel etkilerle çakıştığından, birçok zorluk getirmektedir. Vogus ve Sutcliffe (2007) tarafından belirtildiği üzere, emniyet hedefleri sıklıkla diğer örgütsel hedeflerle karışır ve emniyet üstünlük için devamlı ve yavaş bir şekilde azaltılır. Vogus ve Sutcliffe (2007) OR'a gelindğinde, örgüt iş kültürü tarafından önemli bir rol oynanmaktadır; çünkü endüstri düzenleyicileri, siyasi kararlar ve özellikle emniyet, medya çıkarları ve dikkat çeken popüler görüş söz konusu olduğunda harici etkilerden etkilenen hedefler ve sınırlar içinde çalışılmaktadır diye görüş belirtmiştir. Vogus ve Sutcliffe (2007) tarafından özetlendiği gibi bir organizasyona OR kurma zorluklarından bazıları şunları içermektedir: Güç üretme stratejileri, uyumsuz hedefler, yetkinlik, sansür, iş dünyası kültürü, yönetim tuhaflıkları, akademik tartışmalar, öğrenmede başarısızlık ve kısa vadeli hedeflerle uzun vadeli hedef uyuşmazlığı.

Yukarıdaki zorluklar listesinden bina edilen OR'un yukarıdan aşağıya doğru genel bir organizasyonel taahhütte bulunması gerektiği açıktır. Arif (2007) tarafından önerildiği üzere, esneklik tüm kuruluşa nüfuz etmek durumundadır. Dye ve Langsett (2008) organizasyonların BT güvenlik, fiziksel güvenlik, gizlilik, kurumsal risk yönetimi,

sözleşme uyumu, tedarikçi yönetimi, etik ve kurumsal yönetişim gibi riskle ilgili işlevlerle ilgili diğer kurumsal fonksiyonlarla entegre olmaları ve işbirliği yapmalarının BCM'ye olan ihtiyacı doğurduğunu kabul etmektedir.

Bugün kuruluşların çoğunun önemli bir şartı esnek bir tedarik zincirine sahip olmaktır. Sheffi (2007) OR hakkında, tedarik zinciri yalnızca en zayıf halkası kadar güçlü olduğu için ticaret ortaklarıyla işbirliğine dayalı ilişkilere sahip olmaya bağımlıdır düşüncesini ortaya atmıştır.

Esneklik yeteneği, ortaya çıkan tehditleri öngören ve anlayan, tehdit etkisini anlayan, tedarik zincirinde, sektörde ve topluluktaki kritik paydaşlarla ortaklıklar geliştiren ve sürdüren bir kurumda en güçlüdür. Esneklik yeteneği, birleşik bir organizasyon takımı olarak aksamalara yanıt vermektedir ve aksamalardan kurtulduğunda bozulmalara uyum sağlar ve olaylara esnek bir şekilde tepki vermektedir. Esneklik kabiliyeti, personelin sıkıntı yaşandığı zaman organizasyonu desteklemeye istekli olmasını sağlar ve net kurumsal amaçlar ifade eder. Esneklik yeteneği, bir bozulmaya tepki olarak ve bu bozulmalardan kurtulmada güçlü bir amaç duygusu oluşturmaktadır, açık bir yön verir ve çözülmüş problemi çözmeyi sağlamaktadır.

1.7.4. Organizasyonel esneklik kabiliyetini belirleme

Sheffi ve Rice'a (2005) göre, bir kuruluşun dayanıklılığını, kuruluşun rekabet edebilirliğini ve tedarik zincirinin tepkisini belirlerken oyunda iki önemli değişken vardır. Düşük maliyetli rekabetçi durumlarda organizasyon hızlı bir şekilde tepki vermelidir ya da pazar payını kaybedecektir, ancak çok tepki veren bir organizasyon rekabet ortamında pazar payını kazanabilecek ya da egemen olursa hakim konumunu sağlamlaştırabilecektir.

Günümüzde Sheffi'ye (2007) göre, zorlu rekabet ve müşterilere açık seçeneklerin seçimi nedeniyle firmalar, daha önce çalışanlara kıyasla daha fazla çalışmak zorundadırlar. Çünkü bir olay yüzünden başarısız olduklarında yerlerini almak için diğerleri sırada beklemektedirler.

OR'yi düşünürken Sheffi (2007), bozulmanın altında yatan sebepler hakkında çok fazla düşünmenin verimli olmayabileceğini belirtmektedir ve bunun yerine ağa (tedarik

zinciri) zarar gelmesine ve bu zararın nasıl hızlı bir şekilde toparlanabileceğine odaklanılması gerektiğini belirtmektedir. Bu konuda Sheffi (2007), yüksek teknoloji ya da moda endüstrisi gibi sık sık aksayan endüstrilerdeki esnek tedarik zincirlerine bakılmasını önermektedir.

1.7.5. Esnek organizasyon

OR'yi amaçlarken çoğu kuruluş, Burke, Wilson ve Salas'ın (2005) savunduğu gibi, bölgede muazzam tecrübeye sahip nükleer güç sağlayıcıları ve hava trafik kontrol operatörleri gibi yüksek esnek kuruluşlara (HRO) bakmaktadır. HRO'lar La Porte (1996) tarafından özellikle güvenlik ve performans arayışında esneklik ve fazlalık karakteristiği olarak tanımlanmıştır. Bu noktada artık birincil ünite başarısız olursa, görevin yürütülmesini sağlamak için artıklık La Porte ve Consolini (1991) tarafından tanımlanmaktadır. Roberts'a (1990) göre HRO'lar, bölümlerin çoğaltıldığı teknik yedekliğe (örneğin yedek bilgisayarlar) ve personel işlevlerinin çoğaltılmasına (örneğin belirli bir güvenlik kontrolünü gerçekleştirmek üzere birden fazla kişinin görevlendirilmesi) sahip personel artıklılığı kullanmaktadır. Bu tür HRO'lar güçlü bir emniyet kültürü kurmaktadır ve başarısızlığa karşı daha dirençli ve esnek olabilmektedir. Daha geleneksel kuruluşlar başarılarına odaklanırken, HRO'lar başarısızlığı önlemeyi önceden deneyimlemektedir. Sonuncusu felaketin yokluğunu kendi yetkinliklerinin ve yöneticilerinin becerilerinin kanıtı olarak yorumlamaktadır. Crichton, Ramsay ve Kelly'ye (2009) göre başarıların yeterlilik sergilediği varsayımlar altında, insanlar gönülsüzlük, dikkatsizlik ve alışkanlık rutinlerine sürüklenebilmektedir.

Burke, Wilson ve Salas (2005), BCM programı ya da herhangi bir kuruluş çapında girişim programı gibi OR'yi teşvik etmenin, özellikle karmaşık bir ortamda çalışırken hayati önem taşıdığına dikkat çekmektedir. Organizasyonlarda proaktif olmak yetmemektedir, buna ek olarak çok çeşitli durumlara uyum sağlamak için esneklik sağlanmak durumundadır. Burke, Wilson ve Salas (2005), karmaşık ortamlarda faaliyet gösteren örgütlerin, beklenmedik şeyleri beklemek konusunda çok etkili ve uyarlanabilir olmalarına duyulan gereksinimin arttığını belirtmektedir. Buna ek olarak Burke, Wilson ve Salas (2005) aynı zamanda beklenmeyen olayların hala meydana gelebileceğinin unutulmamasının öneminden bahsetmektedir.

Normal bir organizasyonun HRO statüsüne dönüştürülmesiyle ilgili öncüllerin, süreçlerin ve sonuçların bir çerçevesi Burke, Wilson ve Salas (2005) tarafından özetlenmiştir. Sunmuş oldukları teorik çerçeve, örgütlerin bir takım temel strateji yoluyla HRO statüsüne nasıl dönüşebileceği konusundaki argümanı tasvir etmektedir. Bu çerçevenin temel kuramsal temeli;

- Örgütsel değişim,
- Kurumsal teori,
- HRO teorisidir.

Teorik çerçevenin odak noktası, gerçek değişim süreci üzerinedir. Bir HRO olma yolunda geçiş yaparken, beklenmedik durumları yakalamak için gereken değerleri, inançları ve davranışları artırmak adına varolan örgütsel varsayımların değiştirilmesi gerekmektedir. Sürecin her aşamasında çalışanlardan katılım, başarıyı daha iyi garanti etmektedir.

Burke, Wilson ve Salas (2005) tarafından açıklandığı üzere kuruluşu bir HRO'ya dönüştürme adımları, herhangi bir değişim süreci sırasında gerçekleşen adımlara benzemektedir. Bir HRO tabanına geçilmesi, bir organizasyonun BCM bilgi aktarma yeteneklerini geliştirmesini sağlayacaktır. Elliott'ın (2009) belirttiği gibi bilgi transferi ile ilgili konular, yeni anlayışların (felaketlerden ve krizlerden öğrenme durumunda) örgütler içindeki değişen normlara ve davranışlara dönüştürülme olasılığını sınırlamada önemli etkilere sahiptir. Bu, HRO'ların örgütsel öğrenme ile mücadele etmeye çalıştıkları bir durumdur.

Bir BCM programı gibi, bir HRO oluştururken liderlikten gelen girdi hayati olarak görülmektedir. Johar, Birk ve Einwiller (2010), CEO'nun katılımının temel form ve örgütlerin emniyet tutumlarını, davranışlarını ve performansını teşvik etmekte görünür bir liderlik aldığını ve sonuçlarının sektör genelinde hissedilebilecek, endüstri odaklı girişimlere ve faaliyetlere katılımı olduğunu söylemektedir. La Porte ve Consolini (1991), HRO'larda liderlerin performans ve güvenliği örgütsel amaçlar olarak ön planda tuttuğunu, ancak bu hedefler üzerinde fikir birliğine varılamadığını belirtmektedir.

OR'ye bakıldığında Vogus ve Sutcliffe (2007) esnek ve daha az esnek kuruluşlar arasındaki farkın, esnek bir kuruluşun proaktif güvenlik yönetimine odaklandığı durumlarda toplamda güvenliği nasıl yönettiği olduğunu söylemektedir. Daha az esnek kuruluşlar kazaların önlenmesinden elde edilen tasarrufların kaza masraflarıyla nadiren dengelenmesi durumunda reaktif emniyet yönetimini uygulamaktadır. Aslında esnek bir organizasyon oluşturmak, emniyet yönetimi prensiplerinin sistematik bir şekilde uygulanması sorunudur ve bu da gerçekte her zaman maliyet, önceliklendirme ve kültür aracılığı ile sağlanmaktadır.

1.8. İş Sürekliliği Yönetimi ve BT Yönetişimi

BT yönetişimi, yönetim kurullarının ve üst düzey yöneticilerin BT uygulamaları ile ilgilidir. Odak nokta, BT yapıları, süreçleri, mekanizmaları ve BT kararları, hissedarlar ve diğer paydaşların çıkarları için mi yoksa öncelikle yöneticilerin menfaatleri için mi getirildiğinin kararıdır. BT yönetimi, kurumsal yönetişime, BT organizasyonunun yapısına ve iş hedeflerine uyum konusunda yakından ilgili olmak durumundadır. BT yönetiminin temel odak noktası BT stratejisinin formülasyonunu ve uygulanmasını kontrol etmek, BT ile iş dünyasının uyumlaştırılmasını sağlamak, BT'nin işletme değerini ölçmek için metrikleri belirlemek ve yönetim kurulu ve üst yönetimin sorumluluğunda BT risklerini yönetmek için etkili bir yol seçmektir (Spremić, 2009). BT yönetişimi, bilgi ve iletişim sistemleri ve teknolojisi de dahil olmak üzere bir kuruluşun BT kaynaklarını kontrol etme sürecidir (Hunton, Wright ve Wright, 2004). Kurumsal yönetişimin ayrılmaz bir parçasıdır ve organizasyonun BT'sinin kuruluşun stratejilerini ve hedeflerini sürdürmesini ve genişletmesini sağlayan liderlik ve organizasyon yapıları ve süreçlerinden oluşmaktadır (Van Grembergen, De Haes ve Moons, 2005). BT yönetişimi, BT stratejisinin formülasyonu ve uygulanmasını denetlemek adına, yürütme ve BT yönetimi tarafından uygulanan organizasyonel kapasite olarak tanımlanmıştır ve bu şekilde iş ve BT'nin kaynaşması sağlanmıştır.

BT risklerini yönetmek için iyi veya kesinlikle kaçınılmaz bir yaklaşım, donanım, yazılım, veri, ağlar, organizasyon ve anahtar iş süreçleri de dahil olmak üzere, BT ve BT'nin tüm yönlerinin kapsamlı denetimi ve kalite değerlendirmesi içermektedir. Bilgi sistemi (BS) denetiminin ana hedefi, BT'ye bağlı olan temel iş süreçlerini belirlemek, BT kontrol verimliliğini sistemli ve dikkatli bir şekilde incelemek, temel risk alanlarını

belirlemek ve risk düzeyini sürekli ölçmek, olası arızalar hakkında uyarıda bulunmak ve mevcut BT risk yönetim uygulamalarını nasıl geliştirebileceklerini yöneterek yönetime öneride bulunmaktır (Spremic, Bajgoric ve Turujla, 2012).

1.8.1. BC risk tepkileri için olası stratejiler

Kuruluşlar, BT risklerini belirledikten ve sınıflandırıp değerlendirdikten sonra, risk sahipleri ve etkilenen süreç sahipleri belirlenecek, uygun yanıtlar geliştirilecek ve bu riskler üzerinde belirli maliyet etkin kontrolleri tasarlanacaktır. BC riskine verilen yanıtlar aşağıdaki stratejileri içerebilmektedir:

- Kabul - organizasyon riski ile yaşamayı ve seviyesini sürekli olarak izlemeyi seçer,
- Azaltma - organizasyon, etkinin veya risk oluşma olasılığının azaltılması için adımlar atmayı seçer,
- Kaçınma - organizasyon riskten tamamen veya kısmen kaçınmayı seçer,
- Paylaşım - organizasyon, riskini (örneğin iş sürekliliği ve felaket kurtarma planlarında) tamamen veya kısmen karşılamak üzere risk yönetimi süreci ile ilgili olarak, sigorta satın alımı, risk yönetimi hizmetleri dış kaynak kullanımı veya ortaklıklara katılması yoluyla riski aktarmayı seçer.

BT riskleri karşısında verilen stratejiler, genellikle, belirli BT kontrollerinin uygulanması ve verimliliği sürekli izlenmesi anlamına gelmektedir. Kontrol faaliyetleri, iş hedeflerine ulaşılması ve risk azaltma stratejileri uygulanması için uygulanan politika, prosedür ve uygulamalardır. Kontrol faaliyetleri, belirlenen riskleri azaltmak için her bir kontrol hedefine özel olarak hitap etmek için geliştirilmiştir. Bir BT kontrol hedefi, belirli bir BT faaliyetinde kontrol prosedürlerini uygulayarak elde edilecek istenilen sonuç veya amaca yönelik bir açıklamadır. BS denetim faaliyetleri genellikle BT kontrol verimliliğinin incelenmesini içermektedir. Bunu yaparken BS denetçileri, BT denetimlerinin genelde belirli metriklerini (örneğin iş süreklilik süreci için RTO, RPO) ve olgunluk modellerini kullanarak test yapmaktadır. İş sürekliliği planının etkinliğini test etmek için ortak ölçümler şunlar olabilmektedir:

- MTBF (arızalar arasındaki ortalama süre), bir sistemin potansiyel bir uygulama için uygunluğunu nicelleştirmeye yardımcı olan önemli bir sistem karakteristiğini temsil etmektedir. MTBF, sistemlerin işlevselliğinin ve hizmet seviyesinin ölçüsüdür. MTBF genellikle onarıma kadar geçen ortalama süre (MTTR) ile bağlantılıdır.
- Kullanılabilirlik, sistemin çalıştığı zaman yüzdesini temsil etmektedir (örneğin, yüzde 99 kullanılabilirlik sistem kesintilerinin yılda 3,65 gün olduğu anlamına gelirken, yüzde 99,99 kullanılabilirlik oranı kesintilerin yılda 52 dakika olduğu anlamına gelmektedir).
- İlk düzeltme oranı, ilk saldırı teşebbüsünde başarıyla geri kazanılan olayların yüzdesini ölçmektedir. Sistem kullanılabilirliğinin ve MTTR'nin göstergesidir.
- RTO (kurtarma süresi hedefi), sistemin, hizmetlerin, uygulamaların veya işlevlerin bir kesintiden sonra kurtarılacağı süre hedefidir. Bir arıza veya felaket gerçekleştikten sonra BT altyapısının kapalı kalabileceği maksimum dayanılabilir süredir.
- RPO (kurtarma noktası hedefi), bir organizasyonun bir olay sırasında dayanabileceği maksimum veri kaybı miktarıdır. Aynı zamanda, sistemlerin ve verilerin geri yüklenmesi gereken zamanı da belirtir (Spremic, Bajgoric ve Turujla, 2012).

1.8.2. BCM'yi destekleyen BT yönetişim yöntemleri ve çerçeveleri

Bilgi teknolojileri ve bunlara potansiyel tehditlerle ilgili her türlü risk, örgütsel düzeyde entegre bir risk yönetiminin bir parçası olmak durumundadır. Risk yönetimi, olumsuz bir olay meydana gelme olasılığını değerlendirmek, böyle bir olayın meydana gelme riskini azaltmak için önlemleri uygulamak ve organizasyonun olayın sonuçlarını en aza indirecek şekilde yanıt verebilmesini sağlamak için tasarlanmış bir süreçtir.

Bugünün iş dünyası sadece müşterilerin, tedarikçilerin ve rakiplerin değil, aynı zamanda düzenleyici gerekliliklerin de baskısı altında bulunmaktadır. BT yönetişimi ve BT denetim çerçevelerinin uygulanması, kuruluşların BT risk düzeyini, özellikle de BC risklerini yönetmesine yardımcı olabilmektedir. Çeşitli gruplar, bir kuruluşun BT işlevlerini yönetmek için en iyi yöntemleri belirleyen, dünya çapında bilinen BT yönetişim yönergeleri, standartları ve yönetmelikleri geliştirmişlerdir. Uluslararası standardizasyon

kuruluşlarının öngördüğü standartlara ek olarak, çeşitli ulusal standartlar ve tavsiyeler ile çeşitli şirketlerin en iyi uygulamaları kullanılmaktadır. Bu standartlar ve çerçeveler şunlardır:

- BT süreçleri ve iş gereksinimleri arasındaki ilişkinin kontrolünü kurmak için bir çerçeve olarak oluşturulmuş ve temel BT yönetişim çerçevesini temsil eden ISACA (Bilgi Sistemleri Denetim ve Kontrol Birliği) tarafından COBIT (bilgi ve ilgili teknoloji için kontrol hedefleri) yayınlanmıştır.
- ITIL (Bilgi Teknolojisi Altyapı Kütüphanesi), İngiliz Ticaret Ofisi Bürosu tarafından verilen BT hizmetlerinin yönetiminde uygulanan en iyi uygulama çözümlerinin bir toplamıdır.
- NFPA 1600, acil durum yönetimi ve İş Sürekliliği Teknik Komitesi tarafından hazırlanan afet acil durum yönetimi ve iş sürekliliği programlarında standarttır.
- ISO/IEC 27000 (Bilgi Güvenliği Yönetiminde Uygulama Kuralları), bilgi güvenliği yönetimiyle ilişkili uluslararası standartlar dizisidir. (ISO 27000 - ISO 27008)
- ISO/IEC TR 1335 (Bilişim Güvenliği Yönetim Rehberi), BT güvenlik konusundaki bilgi ve talimatları içeren, hem yönetim hem de uygulama açısından, teknik bir belgedir.
- BT ürün ve hizmetlerinin gözden geçirilmesi ve belgelenmesi için referans olarak ISO/IEC 15408 (Güvenlik Teknikleri-Bilgi Güvenliği Değerlendirme Kriterleri) kullanılır.

Endüstrideki en iyi uygulamaları (örneğin ITIL, COBIT) benimseyerek BT altyapısını güncelleyen şirketler yıllık kesintilerini yüzde 85'e kadar düşürebilmekte ve günlük veri işleme ve erişimindeki kesintileri büyük ölçüde azaltıp operasyonel maliyetleri de içeren iş devamlılığını destekleyebilmektedir.

BT'nin bankacılığa getirebileceği en büyük risklerden biri, bu alanda yaşanan sürekli iyileştirme sürecinin sunduğu yeteneklerin yetersiz kullanılması ve dolayısıyla bankanın rekabet gücünü azaltmasıdır. Bu nedenle, risk yönetimi bakış açısından BT operasyonlarını bir bütün olarak görmek ve bilgi güvenliği yönetimini bütünün bir parçası olarak görmek gerekmektedir. Bielski (2008) bazılarının iş sürekliliğini, insanları çeşitli olay kurtarma aşamaları yoluyla olay tepkisinden alacak bir gölge organizasyonu

oluşturmak için gerekli olduğunu düşünenlerin olduğunu söylemektedir. Winniford, Conger ve Erickson-Harris (2009), ITSM (BT servis yönetimi), ITIL, SLM (hizmet seviye yönetimi) ve COBIT gibi bazı kavramların kesin kapsamı ve çakışması konusunda halen devam eden tartışmaların bulunduğunu belirtmektedir. Pollard ve Cater-Steel (2009), başarılı ITIL uygulamaları için üç kritik başarı faktörü belirlemiştir: ITIL dostu kültür oluşturma, öncelikli süreç ve müşteri odaklı ölçümler. McNaughton, Ray ve Lewis (2010), ITIL'in en iyi uygulamalarının iş süreçlerini destekleme konusunda ne ölçüde başarılı olduğunu değerlendiren bütüncül bir değerlendirme çerçevesi önermektedir. Simonsson, Johnson ve Ekstedt (2010), BT yönetişim olgunluğu ve BT yönetişim performansı arasındaki korelasyon üzerinde durmaktadır. Tüm bu çerçeve ve yöntemler hakkında daha detaylı bilgi çerçeve, standartlar ve kılavuzlar başlığında incelenmektedir.

1.8.3. BT yönetişimi

Şirket yöneticilerinin bilgi güvenliği konularıyla doğrudan ve kişisel olarak ilgilenmesini beklemek gerçekçi değildir ve BT yönetiminin bunu orta vadeli bir sürece adapte etmesi şimdi yaygın şekilde ifade edilmektedir. ISACA, BT yönetişim süreçleri kurma gereksinimini belirleyen ilk gruplar arasında yer almıştır. Bu sayede, özellikle bir kuruluşun denetim komitesi, yönetim kurulunun kullanımı için BT üzerinde yetkili değerlendirmeler yapabilecektir. Bu, güçlü bir denetim duruşuna sahip COBIT metodolojisinde açıklanmıştır (ISACA, 2003). Jordan ve Silcock (2005) diğer taraftan proaktif olan ve ileride BT projelerinin yerini almasına olanak tanıyan bir BT yönetişim yaklaşımı önermektedir. BT yönetimine yönelik bu yaklaşım, Peppard ve Ward'ın (2004) yetenek olarak ifade ettikleri yaklaşımla benzeşmektedir.

Jordan ve Silcock (2005) modeli, Baskerville, Stage ve DeGross'un (2000) yalnızca, güvenlik veya süreklilikle ilgili olanlar değil tüm BT risklerinin entegre bir yaklaşımla bir araya getirilmesi gerektiği argümanını benimsemektedir. BT riskleri, yönetim kurulunun güvendiği süreçler aracılığıyla izlenmesi gereken bir risk portföyü içinde toplanmaktadır (Jordan ve Silcock, 2005). Ayrıca BT yönetiminin eksiksiz olmasını sağlayan tamamlayıcı boyutların, BT faydaları ve BT stratejisi ile ilgilenen boyutlarını önermektedir. Kurul, BT risklerinin, BT avantajlarının ve BT stratejisinin doğru bir şekilde ele alındığından emin olabiliyorsa, organizasyonun BT yönetişimi düzdür (Jordan ve Silcock, 2005). Bu yaklaşımın bir avantajı bilgi güvenliğinin statik ve dinamik yönlerinin

birbirinden ayrılmasıdır. Bilgi varlık riskleri, bilginin korunması ile ilgiliyken, BT hizmet sürekliliği riski yalnızca işletmeyi destekleyen BT sistemlerinin sürekli çalışması ile ilgilidir. BT hizmet devamlılığı tartışmalarına devam edilmektedir ve ardından bir organizasyon tarafından kullanılabilecek bir performans modeli geliştirilmektedir.

1.8.4. BT hizmet sürekliliği

BT hizmet sürekliliği başarısızlığına ilişkin örnekler iş dünyasında genel olarak yaygındır, ancak bireysel organizasyonlar için de genellikle nadirdir. Durum iki örnekle açıklanabilmektedir. Birincisi, gevşek bir şekilde bilgisayar korsanlığı yoluyla verilen siyasi aktivizm olarak tanımlanabilen, hacktivizm tarafından yönlendirilen hizmet reddi (DoS) saldırısıdır: Şubat 2004'te SCO Grup, tarihteki en hızlı yayılmış e-posta solucanlarından biri olan Mydoom ile bağlantılı bir hizmet reddi saldırısının hedefi olmuştur. SCO web sitesine erişilememiş ve site kaldırılmıştır. Şirket alan adını değiştirmiş ve yeni bir internet protokolü (IP) adresine taşınmıştır (Lebihan, 2004). İkinci örnek ise, teknolojinin basit başarısızlığı olan daha sıradan bir şeyi ifade etmektedir: Londra Menkul Kıymetler Borsası'ndaki işlemler, yılın en yoğun günleri olması gerekenler üzerine bilgisayar sorunları ile yaklaşık sekiz saat kesilmiştir. Vergi yılı o gün sona ermiştir ve binlerce perakende yatırımcı, sermaye kazançları vergisi amacıyla hisse alıp sattığından, dövizin en ağır günlerinden biri yaşanmıştır. Ancak hazine, döviz sorununun telafi edilmesi için vergi yılını bir gün uzatmayacağını söylemiştir. Arıza, borsanın Frankfurt finansal piyasalarının operatörü Deutsche Börse ile muhtemel birleşmesi yönündeki görüşmelerini yeniden başlattığı haberi ile çakışmıştır (Financial Times, 2000).

Teknolojinin bu başarısızlığı, kurulun potansiyel ortağı ile müzakere pozisyonunu zayıflatma gücüne sahiptir. Yönetim kurulu üyelerinin endişeleri hayal edilebilmektedir. Her iki durumda da kritik konu işletme üzerindeki etkinin önemli olduğunu ve BT hizmet sürekliliği yönetiminin sürüş mekanizması olarak kullanılan iş etkisi olduğudur.

BT hizmet sürekliliğine standart bir yaklaşım, bir kesintinin neden olacağı ticari etkiyi belirlemek için kuruluşun temel iş süreçlerini gözden geçirmeyi içermektedir. Açıktır ki zamanaşımı arttıkça bozulma artmaktadır. Her süreç için, bir felaketin ilan edilmesi adına bir sürecin çalışmamasının ne kadar süreceğini gösteren, maksimum tolere edilebilir kesinti (MTO) olarak adlandırılan süre belirlenmektedir. Uygulamada,

düzeltilmesi gereken tahmini sürenin MTO'yu aştığı bir kesinti olursa da bir felaket beyan edilmektedir. Bu, saniyeler ve aylar arasında değişebilmektedir.

MTO'nun uygulanabilirliğini belirleyen her süreç için afet önleme ve/veya felaket kurtarma stratejisinin eklemlenmesi gerekmektedir. Birçok organizasyonda bu, simülasyon çalışmaları ile test edilecek bir planda sunulmaktadır.

Afet kurtarma planlamasına yönelik birçok araştırma yapılmıştır ve sonuçlar planlama faaliyetlerinin benimsenmesi için, bankacılık gibi kritik endüstriler hariç, tutarlı bir düşük seviyede olduğunu göstermektedir (Marlin, 2004). New York Menkul Kıymetler Borsası (NYSE) için listeleme kurallarında ve başka yerlerde de benzer düzenlemelerde yer alan BCP şartları ile gelecekte alım yapılması beklenmektedir. Bununla birlikte, BT hizmet sürekliliği faaliyetlerinin performansı pek araştırılmamıştır (Jordan E. , 2005). BT hizmet sürekliliği ve bileşenleri hakkında daha ayrıntılı bilgi BT hizmet sürekliliği yönetimi konusunda verilecektir.

1.8.5. İş sürekliliği ve BT sürekliliği

Çoğu kuruluşta, ürün ve hizmetler sunma süreçleri bilgi teknolojilerine bağlıdır. BT'in aksaması, stratejik bir risk oluşturabilmektedir ve bu da örgütün işletme kabiliyetine zarar vermekte ve itibarını zayıflatmaktadır. Parçalanabilir bir olayın sonuçları değişebilmekte ve çok geniş kapsamlı olabilmekte ve o sırada sonuçları hemen belli olmayabilmektedir.

BT sürekliliği yönetimi bir kuruluşun genel iş süreklilik yönetimi (BCM) sürecini desteklemektedir. BCM, organizasyonun süreçlerinin aksamadan korunmasını ve bozulma olduğunda organizasyonun olumlu ve etkili bir şekilde yanıt alabilmesini sağlamayı amaçlamaktadır. Kuruluş, BCM önceliklerine karar verir ve bu bağlamda BT sürekliliği yönetim faaliyetleri gerçekleştirilir. BT sürekliliği yönetimi, gerekli bilgi ve iletişim teknolojisinin ve hizmetlerinin sağlam olduğunu ve üst yönetim tarafından istenen ve üst yönetimle mutabık kalınan zaman ölçeği içerisinde önceden belirlenmiş seviyelere getirilebilmesini sağlamaktadır. Dolayısıyla etkin BCM, organizasyonun özellikle bozulma dönemlerinde hedeflerini her zaman karşılayabilmesini sağlamak için BT süreklilik

yönetimine bağlıdır. Başarılı olabilmek için hem BCM hem de BT sürekliliği yönetimi örgütün kültürüne dahil edilmek durumundadır (Snedaker, 2007).

BCM ve BT süreklilik yönetimi etkili yönetim, sağlam yönetişim ve örgütsel ihtiyatın önemli bir unsurunu oluşturmaktadır. Üst yönetim, organizasyonun bozulma karşısında çalışmaya devam etme yeteneğini korumaktan sorumludur. Birçok organizasyonun, BCM de dahil olmak üzere etkin riske dayalı kontrolleri sürdürmek için kanuni veya düzenleyici bir görevi vardır. BT sürekliliği yönetimi, hem kurumsal strateji ile uyumlu hem de BT stratejisi ve BT hizmet yönetiminin ayrılmaz bir parçasıdır. Olumsuz şartlar oluştuğunda bir organizasyonun hedeflerine ulaşmaya ve ürünlerini ve hizmetlerini sunmaya devam etmesini sağlayan, BT stratejisi ve hizmet yönetimi unsurudur (European Union Agency for Network and Information, 2008).

Bazı endüstriler bilgi yoğunluğuna sahiptir ve BT'ye bağımlılıkları, yüksek koruma seviyelerini gerektirecek şekildedir. Yinelenen veri merkezleri, çift telekomünikasyon sağlayıcıları ve güç kaynakları, verilerin ve işlemlerin senkronize çoğaltılması, otomatik yük devretme sistemleri ve sık yapılan testler gibi gelişmeler ticaret stoklarının bir parçasıdır. Bu durum, bazı sektörlerde düzenleyiciler tarafından talep edilmektedir. Bir bankacılık sistemini korumak için, bankalar müşterilerine fonlarına çok yüksek seviyede erişim imkanı sağlamak durumundadır. Artık düzenlenmemiş elektrik piyasalarında faaliyet gösteren şirketler gibi bilgisayar borsaları, elektrik enerjisi alımlarının yapılabilmesi için her zaman çalışmak durumundadır. Havayolları ve çevrimiçi perakendecilerin müşterileri dünyanın her yerinde bulunduklarından iş saatleri yoktur ve bu nedenle işleri her zaman açık olmak durumundadır. Buna ek olarak telekomünikasyon şirketleri, elektrik tedarikçileri ve müşterilere bu işlerin yanı sıra hastane ve polis hizmetleri gibi kritik toplum altyapısını içeren diğer araçlar da bulunmaktadır. Bu kuruluşlar için iş sürekliliği BT sürekliliğini yakından ilgilendirmektedir (Porter ve Millar, 1985).

Birçok organizasyonda süreklilik konusundaki uzmanlık, beceri, bilgi ve ilgi BT personeli ile olmaktadır. İlk ana bilgisayar teknolojileri o kadar savunmasız ve günümüzün güvenilirlik standartlarının çok gerisinde kalmıştır ki; yedekleme, kayıt işlemleri ve geri yükleme işlemleri 1960'larda bile rutin bir işlem olmuştu. Günümüzdeki sistemler çok daha karmaşıktır ve bağımlılık ağları daha fazladır, ancak BT personelinin beceri seti

onlara uyum sağlamak için büyümüştür. Bu karmaşıklıktaki artış tedarik zincirinin bazı yönlerine de yansıyabilmektedir, ancak organizasyonun büyük bir kısmı paralel olarak değişmemiştir. Dolayısıyla bir çok organizasyon iş sürekliliği alanında BT uzmanlığına, çoğunlukla bunu açıkça tanımaksızın, ve işlevine ihtiyaç duymaktadır (Jordan E. , 2005).

2. BT SÜREKLİLİĞİ VE İLİŞKİLERİ

Kuruluşların önemli parçalarından biri olan iş sürekliliğinin tüm süreçlerle ilgisi bulunmaktadır. Günümüz iş dünyasında kuruluşların hayatlarına devam edebilmeleri için BT sistemlerinin ayakta kalması gerekmektedir. Bu noktada BT'nin iş sürekliliği ile olan ilişkisi, hizmet sürekliliğin ve ekonomik faaliyetlerin devam edebilmesi açısından önem arz etmektedir.

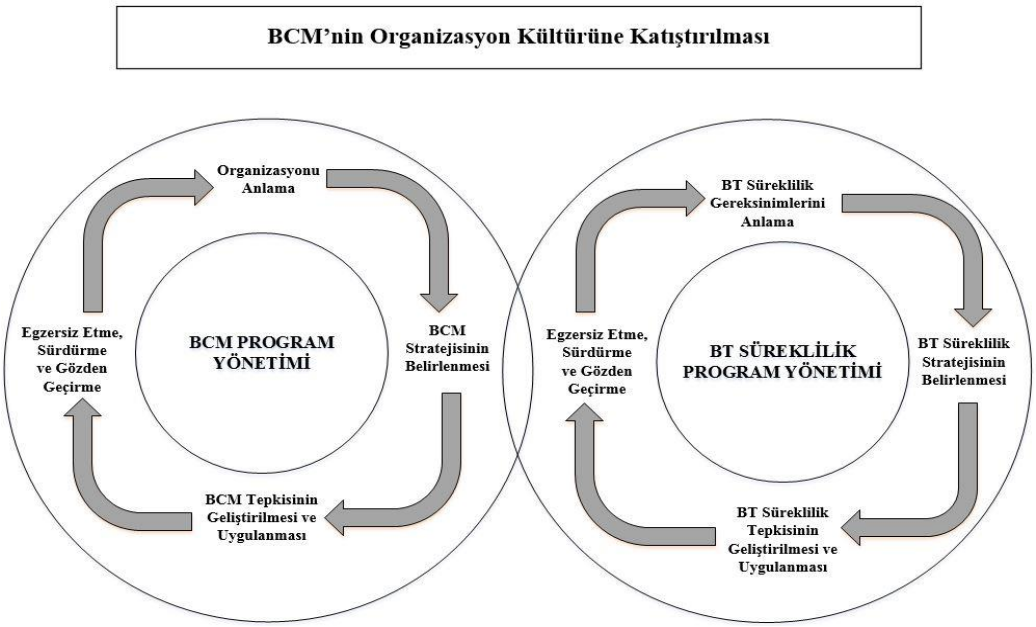
2.1. BT Süreklilik Yönetimi

Tarihsel olarak iş sürekliliği planlaması (BCP) çoğu kuruluşun BT departmanında yerleşikti. Bu nedenle, çoğu şirketin BT sistemleri için bazı felaket kurtarma alternatifleri vardır. En sık kullanılan felaket kurtarma alternatifi, verilerin düzenli olarak kaset veya diske yedeklendiği ve uzak bir yerde tutulduğu yerinde olmayan veri depolama alanı olarak göze çarpmaktadır. Özellikle sıcak ve soğuk alanlar, elektronik tonlama, gölgelendirme, yansıtma ve diskten diske uzaktan kopyalama gibi büyük kuruluşlar için BT kurtarma adına birkaç teknolojik alternatif mevcut olsa da, bu seçenekler birçok şirket tarafından kullanılmamaktadır. Bu zorlu ekonomik ortamda, BCP kaynaklarını kesmek çok cazip gelebilmektedir. Birçok işletme yanlışlıkla BCP'yi hiçbir zaman dava açmak zorunda kalmayacakları bir sigorta poliçesi olarak görmektedir (Rittinghouse, Ransome ve CISSP CISM, 2011).

BT süreklilik planlaması, kaynakları işlemek, politikalar, prosedürler ve araçlar geliştirmek ve kritik iş süreçlerini korumak için BT altyapısını ayarlama sürecidir. İş sürekliliği planlamasının (BCP) bir alt kümesi olan BT süreklilik planları, bir kuruluşun iş kesintisi sırasında, elektrik kesintisinden doğal bir felakete kadar bir süre boyunca operasyonları sürdürme kabiliyeti için kritik öneme sahiptir.

BT sürekliliği bir kuruluşun genel BCM sürecini desteklemektedir. BCM, organizasyonun süreçlerinin aksamadan korunmasını ve bozulma olduğunda organizasyonun olumlu ve etkili bir şekilde yanıt verebilmesini sağlamayı amaçlamaktadır. Kuruluş BCM önceliklerine karar verir ve bu bağlamda BT faaliyetleri gerçekleştirilir. BT sürekliliği, gerekli BT hizmetlerinin esnek olmasını ve üst yönetim tarafından istenen ve kabul edilen zaman ölçeği dahilindeki önceden belirlenmiş seviyelere ulaşılmasını

sağlamaktadır. Bu noktada etkin BCM'nin örgütün amaçlarını her zaman, özellikle bozulma zamanlarında, karşılayabilmesini sağlamak için BT sürekliliğine bağımlıdır (British Standards Institution, 2008).



Şekil 2.1. BCM'nin Örgüt Kültürüne Katıştırılması (British Standards Institution, 2008)

BT sürekliliği yalnızca yıkıcı olayların olasılığı ve etkileri üzerine değil, aynı zamanda örgütün bu tür olayların ortaya çıkmasını tespit etme ve bunlara tepki verme becerisine de odaklanmaktadır. Bu durum, organizasyonların BT hizmetlerini takip etmesini sağlamak için izlemesini gerektirmektedir. BT sürekliliği altı ana ilkeye dayanmaktadır:

1. Korumak - BT çevresini çevresel ve donanımsal arızalardan, operasyon hatalarından, kötü niyetli saldırılardan ve doğal felaketlerden korumak, bir kuruluş için istenen düzeyde sistem kullanılabilirliğini sağlamak için kritik öneme sahiptir.
2. Algılama - En kısa sürede olayları saptamak, hizmetlere olan etkiyi en aza indirir, kurtarma çabalarını azaltır ve hizmet kalitesini korur.
3. Reaksiyon - Bir olaya en uygun şekilde tepki verilmesi daha verimli bir iyileşmeye yol açarak herhangi bir kesintiyi en aza indirir. Kötü müdahale, küçük bir kazanın daha ciddi bir noktaya yükselmesine neden olabilmektedir.

4. Kurtarma - Uygun kurtarma stratejisinin belirlenmesi ve uygulanması, hizmetlerin zamanında yeniden başlatılmasını ve verilerin bütünlüğünün korunmasını sağlayacaktır. Kurtarma önceliklerinin anlaşılması, en kritik hizmetlerin ilk önce eski haline getirilmesini sağlar. Daha az kritik olan nitelikteki hizmetler daha sonraki bir zamanda kurtarılmakta ya da bazı durumlarda tamamen kaldırılabilmektedir.
5. Çalıştırma - Normal duruma dönene kadar felaket kurtarma modunda çalışma olasılığı, zamanla hizmet edilmesi gereken artan işletme hacimlerini desteklemek için zaman kazandırabilmekte ve felaket kurtarma işlemlerini ölçeklendirmeyi gerekli kılabilmektedir.
6. İade - Her BT sürekliliği planı için bir strateji geliştirilmesi, bir organizasyonun felaket kurtarma modundan normal işi destekleyebileceği bir konuma geri döndürülmesini sağlar (British Standards Institution, 2008).

Bir kesinti durumunda kritik programların sürekliliğini sağlamaya yardımcı olması için bir BT sürekliliği yönetimi (ITCM) programı bulunmak durumundadır. Buna bir yönetişim yapısı, BT bağımlılıklarını tanımlayan bir iş etki analizi, maksimum izin verilebilir kesinti (MADs) ve düzenli olarak test edilen ve güncellenen BT süreklilik planlarının geliştirilmesi de dahil edilmektedir. Bir ITCM programı, kritik programlar ve hizmetler için bir BT kesintisi durumunda BT gereksinimlerini, BT bağımlılıklarını ve bir iş yeniden başlatma stratejisini içermektedir (Järveläinen, 2013).

2.1.1. Kritik faaliyetlere yönelik tehditlerin değerlendirilmesi

BCM bağlamında risk düzeyi, özellikle örgütün kritik faaliyetleri ve bunlara zarar gelme riski açısından anlaşılmak durumundadır. Kritik faaliyetler; insanlar, binalar, teknoloji, bilgi, malzeme ve paydaşlar gibi kaynaklar tarafından desteklenmektedir. Kuruluşlar bu kaynaklara yönelik tehditleri, her bir kaynağın güvenlik açığını ve olay olduğunda ve iş kesintisine neden olursa bir tehdidin etkisini anlamak durumundadır. Risk değerlendirme yaklaşımının seçimi tamamen organizasyonun kararıdır, ancak bu yaklaşımın kurumun tüm gereksinimlerini karşılamak için uygun olması önemlidir.

İş etki analizi (BIA) ve risk değerlendirmesi sonucunda kuruluşlar aşağıdaki önlemleri tanımlamak durumundadır:

- Kesinti olasılığının azaltılması,
- Kesinti süresini kısaltılması,
- Bir bozulmanın organizasyonun ana ürün ve hizmetleri üzerindeki etkisinin sınırlandırılması.

Bu önlemler, kayıp hafifletme ve risk tedavisi olarak bilinmektedir. Zarar azaltma stratejileri diğer tüm seçeneklerle birlikte kullanılabilmektedir, çünkü tüm riskler kabul edilebilir bir düzeye kadar engellenememektedir veya sadece azaltılabilmektedir (British Standards Institution, 2006).

2.1.2. İş sürekliliği için BT gerekliliklerini anlama

BCM programının bir parçası olarak kuruluşlar, faaliyetlerini kurtarma önceliklerine göre kategorilere ayırmak durumundadır. Üst düzey yönetim, kuruluşun iş sürekliliği şartlarını kabul etmektedir. Her kritik süreç için kuruluşun, işletmenin hayatta kalmasını tehdit etmeden önce sürecin mümkün olmadığı en uzun süreyi belirlemesi gerekmektedir. Bu rakam tolere edilebilir maksimum zaman aşımı (MTD) olarak bilinmektedir.

Kuruluş her kritik süreç için MTD'yi kurduktan sonra, her işlem için bazı özel iyileştirme hedefleri belirlemektedir. Kuruluşların BIA'da belirledikleri iki ana kurtarma hedefi ise şöyledir:

- Kurtarma zaman hedefi (RTO) - Bir olayın ardından ürünün, hizmetin veya etkinliğin verilmesinin tekrar başlatılması için belirlenen hedef zamandır.
- Kurtarma noktası hedefi (RPO) - Hizmetlerin sürdürülmesi için verilerin ve geri kazanılması gereken zaman noktasıdır.

Kuruluşlar BT hizmetlerini tanımlamakta ve BT hizmet adları kuruluş için anlamlı olmaktadır. BCM programının önceliği, her kritik etkinlik için RTO'nun başarılmasını desteklemek adına gerekli BT hizmetleri tanımlamaktır. Kuruluşlar kritik BT hizmetlerinin listesini, her hizmet için bir RTO ve RPO ile birlikte belgelemektedir. Yeniden başlatmada gerekli olan BT hizmetinin minimum kapasitesinin bir göstergesini ve bu kapasitenin ne kadar hızlı bir şekilde arttırılması gerekebileceğini de belirtmek gerekebilmektedir. BT

servis RTO'su, desteklediği kritik etkinlik için RPO'dan genellikle daha az olmak durumundadır. İş sürekliliği stratejisi tamamen BT hizmetine bağlı kalmak yerine manuel bir prosedür gibi geçici bir önlem gerektirdiğinde bu durum geçerli olmayabilmektedir.

Üst düzey yönetim, kritik BT hizmetleri ve bunlarla ilişkili BT devamlılığı gereksinimleri konusunda anlaşmak durumundadır. Üst düzey yönetici tarafından listelenmiş ve üzerinde anlaşmaya varılan her kritik BT hizmetinde kuruluş, uçtan uca hizmeti oluşturan BT bileşenlerini ve her bir hizmetin sunumu için nasıl yapılandırıldığını veya bağlantılandırıldığını tanımlamakta ve belgelemektedir. Bu analiz fiziksel ve mantıksal konfigürasyonları dikkate almaktadır. Normal BT hizmet sunum ortamı ve BT sürekliliği hizmet sunum ortamı yapılandırmaları belgelenmelidir.

Mevcut kesintisizlik yeteneği, hizmet kesintisi veya bozulma riskini değerlendirmek ve BT hizmet esnekliğini artırmak için fırsatları vurgulamak adına önleme açısından her kritik BT hizmeti için gözden geçirilmektedir. BT hizmetinin aksamasına erken teşhis ve tepki verme fırsatlarını da vurgulamaktadır. Kuruluş, hizmet esnekliğini artırmak için tanımlanan fırsatlara yatırım yapmak için bir mantık olup olmadığına karar verebilmektedir. Bu hizmet risk değerlendirmesi, BT servis kurtarma kapasitesini artırmak için ilgili paydaşlara bilgi verebilmektedir (British Standards Institution, 2008).

2.1.3. Boşlukları belirleme

Her kritik BT hizmetinde, yetersiz veri depolama kapasitesi gibi BT hizmetinin iyileştirilmesine zarar verebilecek boşlukları veya uyumsuzlukları belirlemek için, mevcut BT sürekliliği hizmet sunum ortamı yapılandırması, bir kurtarma perspektifinden normal BT hizmet sunum ortamıyla karşılaştırılmaktadır. Eleştirel BT hizmet süreklilik yetenekleri ve iş sürekliliği gereklilikleri arasında tanımlanan boşluklar belgelendirilmektedir. Bu boşluklar, her bir kritik BT servisinin iyileşme sırasında gerektireceği ek kaynakları gösterebilmektedir (Snedaker, 2007).

2.1.4. Seçeneklerin belirlenmesi

Kuruluşlar, kritik BT hizmetlerinin her biri için bir dizi seçenek düşünmek durumundadır. Kuruluşlar, aşağıdaki stratejilerin bir veya daha fazlasını veya tümünü isteyebilmektedir (British Standards Institution, 2006).

İş devamlılığı

Süreklilik stratejileri kritik faaliyetlerin BIA'da öngörülen ve kabul edilebilir bir minimum seviyede ve zaman çerçevesinde devam etmesini veya bu çerçevede bulunmasını sağlayarak, örgütün bir bozulmaya karşı direncini artırmaya çalışmaktadır (Snedaker, 2007).

Kabul

Başka bir hareket yapılmaksızın bir risk kabul edilebilmektedir. Kabul edilemez olsa bile, bazı riskler konusunda herhangi bir şey yapma kabiliyeti sınırlı olabilmekte veya herhangi bir harekete geçirme maliyeti, kazanılmış potansiyel fayda ile orantısız olabilmektedir. Bu durumlarda, üst yönetim riskini kabul edilebilir bulmaya ve organizasyonun risk iştahına dahil ederse mevcut risk düzeyini tolere etmeye yanıt olabilmektedir. Bazı durumlarda bir riskin etkisi organizasyonun normal risk iştahının dışında kalabilmektedir, ancak üst yönetim riskin oluşma ihtimalinin düşük olması ve/veya ekonomik olmayan kontrol maliyeti nedeniyle riski kabul de edebilmektedir (Snedaker, 2007).

Transfer

Bazı riskler için en iyi yanıt onları transfer etmek olabilmektedir. Bu transfer, konvansiyonel sigorta veya sözleşme düzenlemeleri ile yapılabilmekte veya riski başka bir şekilde almak üzere üçüncü bir tarafa ödeme yapılabilmektedir. Risklerin, organizasyonun riske maruz kalmasını azaltmak için veya başka bir organizasyonun riskleri etkili bir şekilde yönetme kabiliyeti nedeniyle aktarılması mümkündür. Bazı risklerin tamamen devredilebilir olmadığını kaydetmek önemlidir; özellikle bir hizmetin teslimatı ihale edilmiş olsa dahi itibar riski taşıyorsa genellikle mümkün değildir (Snedaker, 2007).

Değişiklik yapma, askıya alma veya feshetme

Bazı durumlarda BT hizmetini, ürünü, aktiviteyi, işlevi veya süreci değiştirmek, askıya almak veya sona erdirmek uygun olabilmektedir. Bu seçenek yalnızca kuruluşun hedefleri, kanuni uygunluk veya paydaş beklentisi ile çelişki olmadığında kabul edilmek durumundadır (Snedaker, 2007).

2.1.5. Egzersiz ve test

Bir organizasyonun BT süreklilik planları, yerine getirilene kadar güvenilir sayılmamaktadır. Bir egzersiz programı birkaç test içerebilmektedir. Kuruluş, yalnızca BT hizmetinin iyileştirilmesini değil, aynı zamanda hizmetin korunmasını ve esneklik unsurlarını da belirleyip, bunlara ek olarak aşağıda not edilenleri de belirlemek durumundadır:

- Olay şiddetine bakılmaksızın servis korunabilmekte, muhafaza edilebilmekte ve eski haline getirilebilmektedir.
- Süreklilik düzenlemeleri işe olan etkiyi en aza indirebilmektedir.

Bu egzersiz yalnızca BT bölümünün konusu değil, işletme çapında bir etkinliktir. BT bölümü egzersizin planlama ve uygulama yönlerini elinde tutabilmektedir, ancak organizasyonun diğer parçaları için hala önemli bir rolü vardır (Bradbury, 2008).

2.2. BT Felaket Kurtarma

Felaket, sistemin operasyonel kullanılabilirliğini kabul edilemez bir süre boyunca tehlikeye atan yıkıcı ya da zayıflatıcı bir olay olarak tanımlanmaktadır. Felaketler hem şiddette hem de etki derecesinde genel başarısızlıktan farklıdır. Sistem arızaları sistem yeteneğini bozabilmektedir. Mevcut arıza önleme sistemleri tarafından iyileştirilemeyen felaketler genellikle insan müdahalesi, şiddetli hava, sel baskını veya yangın da dahil olmak üzere ancak bunlarla sınırlı olmayan felaket olaylarının sonucudur. Bir felaket, bir BT merkezindeki ticari faaliyetlerin sürekliliğini yok ettiği ve kesintiye uğrattığı için yanıt, ilave altyapıların kullanılmasını gerektirmektedir.

Felaket kurtarma planı (DRP), BCP'nin bir parçasıdır ve etkinliğin derhal etkisini ele almaktadır. Bir sunucu kesintisinden, güvenlik ihlaline veya kasırgadan kurtulmak, bu kategoriye girmektedir. Genellikle DRP, planlama aşamalarında uygulanmaya hazır çeşitli öngörülen adımlardan oluşmaktadır. Felaket sırasındaki durum tam olarak planlandığı gibi olmamasına rağmen, bir felaket meydana geldiğinde bu adımların uygulanması hızlı olmaktadır. Bu yönde, kaynaklar hazırlanan adımlara uygun olarak kontrol edilebilmektedir. Halihazırda DRP, bir felaketin etkisini hızla göstermekte ve hemen sonuçlara hitap etmektedir (Alshammari ve Alwan, 2016).

Herhangi bir iş sürekliliği yanıtının önemli bir parçası, bir işletmenin kabul edilebilir bir hizmet düzeyi sağlamaya devam etmesini sağlamak için gerekli kaynakları edinmesidir. BT sistemleri çoğu kuruluş için önemlidir ve çok azı bilgisayar desteği olmaksızın kısa bir süre dışında herhangi bir şey için çalışabilmektedir. BT felaket kurtarma planlaması, teknoloji sistemlerinin varlığın gereksinimlerine uygun olarak geri kazanıldığı mekanizmadır. BT felaket kurtarma planları, işletme etkileri analizi içinde tanımlanan gerekli iyileştirme zamanı hedefinden ve kurtarma noktası hedefinden daha az bir başarıyı elde edemeyen varlığın ihtiyaçlarını karşılamak üzere tasarlanmaktadır. BT felaket kurtarma, hizmetlerin kesilmesinin ardından bilgisayar sistemlerinin ve ilgili altyapının kurtarıldığı süreçtir. Bazı durumlarda, BT felaket kurtarma planları telefon gibi diğer teknik olanakları da kapsayabilmektedir. BT sistemlerinin iyileştirilmesi, sistemlerin desteklediği varlığın gereksinimlerini odak almaktadır. Bununla birlikte gerekli kurtarma hızı, konuşlandırılan çözümün maliyeti ve karmaşıklığı üzerinde önemli bir etkiye sahip olacaktır (Hiles, 2010).

Kuruluşlar, diğer kuruluşlarla BT kurtarma için paylaşılan düzenlemelerin seçeneklerini keşfetmek isteyebilmektedir. Çok hızlı bir RTO ve sıfır veri kaybı gerektiren bir işletme için, tüm teknoloji ortamını alternatif bir yerde çoğaltmak gerekli olabilmektedir. Diğer taraftan bu yaklaşım, her iki alandaki verilerin gerçek zamanlı olarak güncellenmesini gerektirecek çok pahalı ve karmaşık bir çözüm olacaktır. Tersine, 48 saatlik bir RTO kabul edebilen ve son 24 saat zarfında birikmiş olan veri kaybını kabul eden bir kuruluş için, saha dışı bant tabanlı veri yedeklemelerinden geleneksel olarak düşük maliyetli bir kurtarma yapılması uygun olabilecektir.

Varlığın kritik öneme sahip gereksinimleri, BT felaket kurtarma planının gerektirdiği gelişmişliği belirlemektir. Her bir yazılım uygulaması için RTO ve RPO, iş etki analizi bölümünün bir parçası olarak belirlenmektedir. İş döngüsünün zaman noktası da izin verilen azami tahribata neden olabilmektedir.

BT felaket kurtarma planları, gerekli kurtarma süresi hedefi ve kurtarma noktası hedefi doğrultusunda kurtarma işlemini gerçekleştirmek için yapılması gereken görevleri ve işlemleri içermektedir. Çoğu durumda başarılı BT felaket kurtarma planlarının, sistemlerin kurtarıldığı ikinci bir siteyi tanımlaması gerekmektedir. Ayrıca altyapı, donanım, uzman ekipman, uygulama yazılımı, altyapı ve ilişkili verilere nasıl erişileceklerini ve/veya nasıl kurtarılacağını belirlemesi de gerekebilmektedir (Australian National Audit Office, 2009).

2.2.1. İş sürekliliği planıyla ilişki

Felaket kurtarma işlemi, geleneksel olarak yalnızca BT sistemlerine ve hizmetlerine ara vermeden kurtarma sürecini kapsarken, iş sürekliliği tüm işi kapsamaktadır. Bir iş sürekliliği planında, tüm kritik hizmetleri sürdürmek için gereken koşullar bulunurken, bir felaket kurtarma planı yalnızca BT üzerindeki etkileri değerlendirmektedir. Tesislere erişim reddedilirse ve insanlar erişemiyorsa bir BT sisteminin çalışması ve yürütülmesi için çok az amaç vardır demektir. İş sürekliliği proaktiftir ve bir olayın meydana gelmesinden önce riski azaltmayı içermektedir; felaket kurtarma ise reaktiftir ve bir olay meydana geldiğinde aksiyon almaktadır (Nollau, 2009).

İş sürekliliğinin özü, acil durum operasyonlarını aksatma durumunda çalıştırmaktır; öte yandan felaket kurtarma, özel olarak ve tarihsel olarak BT altyapısının bozulmasında ve BT hizmetlerinin bulunamamasında ortaya çıkmaktadır. İkisi arasındaki ilişki, dahili olarak BT tarafından sağlanıyorsa dahili SLA ya da üçüncü taraf bir tedarikçiyle, BT dış kaynaklı olması durumunda harici bir SLA ile tanımlanmaktadır (Royds, 2010).

BCP belirli bir iş süreci için yazılabilmekte veya tüm kritik iş süreçlerini ele alabilmektedir. BCP, ana alt bileşenlerinde DRP'nin bulunduğu bir şemsiye plandır. Bilgi sistemleri, BCP'de yalnızca bu iş süreçlerine olan destekleri açısından değerlendirilmektedir. BCP, aşağıdaki bileşen planlarından oluşmaktadır:

- İş devam planı,
- Kullanıcı acil durum planı,
- Olay yönetimi planı (IMP),
- Operasyon planının sürekliliği,
- Felaket kurtarma planı (DRP).

İş devam planı, kullanıcı acil durum planı ve operasyonel planın sürekliliği, BT altyapısı ile ilgilenmez. BT altyapısını ele alan IMP, bir kuruluşun BT sistemlerine karşı siber saldırılara yönelik yapı ve prosedürler oluşturur ve genellikle felaket kurtarma planının etkinleştirilmesini içermemektedir (Nollau, 2009; Alabdulwahab, 2016).

2.2.2. Felaket kurtarma süreci

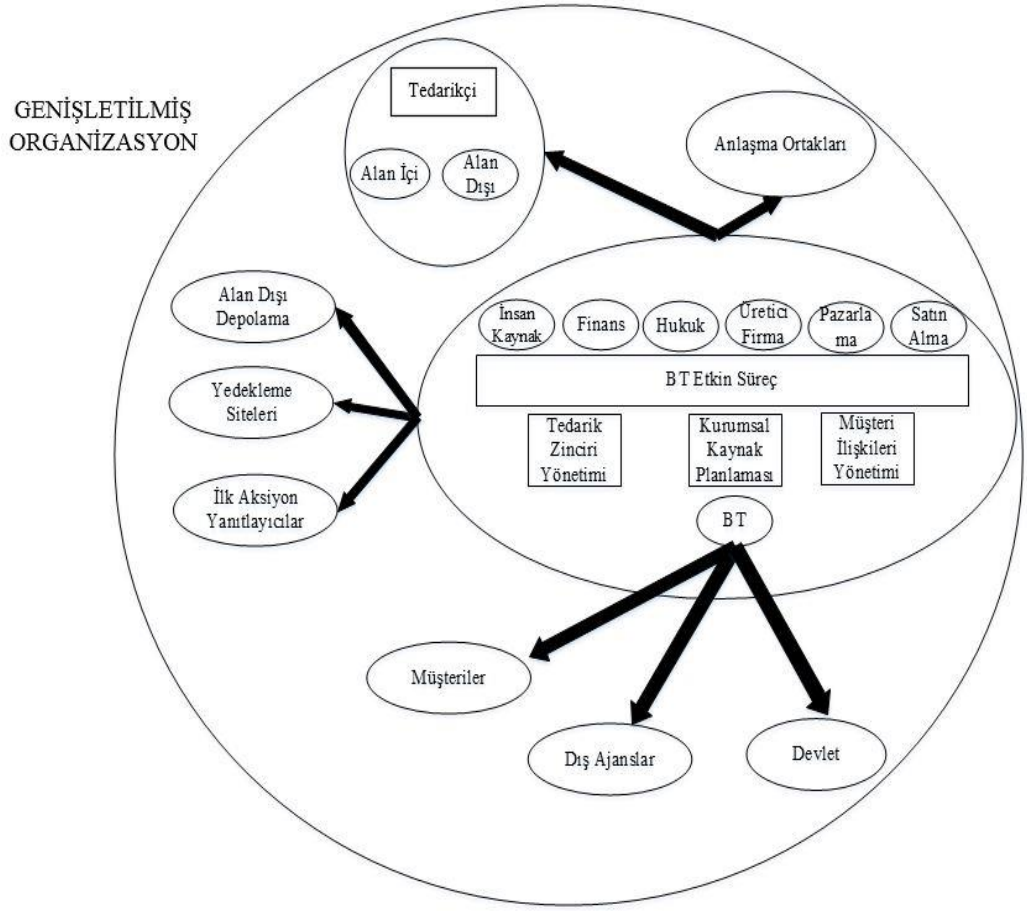
Felaket, örgütlerin kritik iş süreçlerini destekleyen sistemlerin normal üretim işlemlerini yapma olanağı da dahil olmak üzere görev ve kritik süreçlerini gerçekleştirme olanağı vermeyen ani, plansız bir olay olarak tanımlanmaktadır. Bir felaket, operasyonların bir kısmında büyük bir hasarın meydana gelmesi, bir tesisin tamamen kaybedilmesi veya çalışanların bu tesise erişememesini kapsayabilmektedir (Alabdulwahab, 2016).

Felaket kurtarma işlemi, işlemlerinin bağlı olduğu bilgi işleme veya telekomünikasyon kaynaklarının birinde veya daha fazlasında bir hata olması durumunda, kritik iş süreçlerinin işlevine devam etmesini sağlamak için kurallar, süreçler ve disiplinleri tanımlamaktan oluşmaktadır. Felaket kurtarma planının temel unsurları şunlardır:

- Planlama grubu oluşturulması,
- Risk değerlendirmesi ve denetimlerinin gerçekleştirilmesi,
- Uygulamalar ve ağlar için önceliklerin oluşturması,
- Kurtarma stratejilerinin geliştirilmesi,
- Planın envanterinin ve belgelerinin hazırlanması,
- Doğrulama kriterleri ve usullerinin geliştirilmesi,
- Planın uygulanması.

Her bir iş birimi tarafından hazırlanan kilit kişiler ekibin üyeleri olmakta ve tüm felaket kurtarma planlama faaliyetlerine dahil edilmektedir. Felaket kurtarma planlama

grubunun bir DRP oluşturmak için iş süreçlerini, teknolojiyi, ağları ve sistemleri anlaması gerekmektedir. Potansiyel riskler analiz edildikten sonra, her iş sürecine ve uygulama/sisteme öncelik seviyeleri atanmak durumundadır. Envanteri güncel tutmak, ekipmanların, konumların, sağlayıcıların ve iletişim noktalarının tam bir listesine sahip olmak önem arz etmektedir (Quarantelli E. L., 1999). Hedefin odağı, tüm teknoloji alanlarında uygulanabilir, etkili ve ekonomik kurtarma sağlamaktır. Aşağıdaki grafik organizasyon uygulamalarını ve/veya sistemlerini sınıflandırmak için kullanılabilmektedir (Fallara, 2003).



Şekil 2.2. BT Kurtarma Süreçleri ile Genişletilmiş Organizasyon (Sheth, McHugh ve Jones, 2008)

Felaket kurtarma süreci, üst yönetimin kabul edebileceği bir seviyeye getirmek için sonuçlarını hafifletecek riskleri ve maruz kalmaları belirleyecektir. Bu riskler ve maruz kalmalar gerekli iyileşme düzeyinin belirlenmesine yardımcı olacaktır. Gereksinimler, bu gereksinimleri desteklemek için hangi kurtarma stratejisini seçmenin gerekli olduğunu belirleyecektir.

2.2.3. Felaket kurtarma planı

Tam kapsamlı olarak bir DRP'nin odağı, kritik iş süreçlerini destekleyen sistemlerin kullanılabilirliğini geri kazandırmaktır. Amaç, organizasyonun mümkün olan en kısa sürede normal operasyonlara dönmesini sağlamaktır. Birçok kritik iş süreci uygulamalar, veri ve BT donanımı içeren bir teknoloji altyapısına dayandığından, felaket kurtarma planı BT odaklı bir plan olmak durumundadır. Her kuruluş, tüm uygulamalar için bir olağanüstü durum kurtarma planı geliştirmelidir. Sistemlerin restorasyonu mutlaka teknoloji artıklığını gerektirmemektedir. DRP, bazı prosedürlerin manuel olarak tamamlanmasını talep edebilmektedir. Bir BT altyapısını oluşturmaktan ve sürdürmekten ziyade, manuel prosedürlere geçme kararı, kuruluş tarafından yapılan maliyet odaklı bir karardır. Bir DRP'nin yerine getirilmesi, iş sürecinde bir aksamanın, kuruluştaki yönetim tarafından kabul edilebilir olduğu belirlenenin ötesine gitmeme riskini azaltmaktadır (Schwab, Topping, Eadie, Deyle ve Smith, 2003). Kurtarma safhasında, ilave bir kayıp riskini sınırlamak için ortaya çıkan olaylar üzerinde kontroller kurmaya odaklanmaktadır.

2.2.4. BT felaket kurtarma planlama süreci

Teknik bir felaket kurtarma stratejisi geliştirmek, genel BT felaket iyileştirme planlama sürecinde yalnızca bir adımdır. Bu süreç, tüm BT sistemleri için ortaktır ve aşağıdaki adımları kullanmaktadır:

1. İş acil durum planlaması politikası ve iş süreci öncelikleri geliştirme,
2. Risk değerlendirmesi yapma,
3. İş etki analizi (BIA),
4. İş sürekliliği ve kurtarma stratejilerini geliştirme,
5. İş sürekliliği planlarını geliştirme,
6. DRP'nin farkındalığını, test edilmesini ve eğitilmesini sağlama,
7. Felaket kurtarma planının idame ettirilmesi ve uygulanması.

Hedef, 4. adımda bir teknik kurtarma stratejisi tasarlamaktır. Bu adım, 3. adımda bir BIA yapılabilmesi için gerçekleştirildiğinden, kurtarma stratejisi BIA tamamlandıktan sonra etkinleştirilebilen standart bir hizmet paketine geliştirilmiştir. BIA'nın tamamlanması aylar sürebilmektedir ve bunun için yeterli bütçeye sahip olmayan bazı kuruluşlar vardır.

Bununla birlikte, yönetim bir BIA yürütmek için potansiyel yatırım getirisini anlamak durumundadır (Snedaker, 2007).

BIA'nın amacı, iş süreçlerini destekleyen uygulamaları çalıştıran ana bilgisayar sistemlerinin iyileştirilmesine yönelik hedefleri tanımlamaktır. Bu hedefler, RTO ve RPO olarak belirtilmektedir. RTO, yönetimin bir iş sürecini veya bir sistemi devam ettirmeyi koyduğu saat veya gün sayısıdır. RPO, felaket durumunda geri yüklenebilinmesi istenen verilerin yaşını tanımlamaktadır. RTO ve RPO teknik felaket kurtarma stratejisinin teknik özelliklerini karşılamaktadır. RTO ve RPO gereksinimleri, hangi felaket kurtarma planının uygulanacağını belirlemektedir.

Kurtarma süresi ve mevcut verilerin durumu, önemli bir bozulma durumunda bir iş sürecinin gerektirdiği hizmet düzeyini belirlemede temel bileşenlerdir. Bir felaket kurtarma planını düzgün bir şekilde uygulamak için, kuruluşun bir felaket durumunda kabul etmeye hazır olduğu RTO ve RPO'yu bilmesi zorunludur. Farklı kurtarma seçeneklerinin teknik felaket kurtarma stratejisi, bu gereksinimlerin bir kombinasyonuna dayanmaktadır (Schwab ve diğerleri, 2003).

İş sürekliliği açısından, iş ve BT birimleri genelde aynı kategoride değildir. Literatür, şirketler bilgiye daha çok bağımlı hale gelirken bilgi kaybı için iş sürekliliği toleransı, özellikle de iş dünyasında gittikçe azalmaktadır görüşünü sunmaktadır. Literatüre bakıldığında, sistem yönetimi disiplininin bir unsuru olan iyileştirme yönetimi (BT tabanlı bir acil durum planını ve BT iyileştirme planını korumakla birlikte) için bilgi kaybı adına kabul edilebilir risk derecesi kararı üst yönetimden gelmelidir görüşü ağır basmaktadır.

Çoğu organizasyon yönetimin iş sürekliliğinde dikkate alması gereken iki hedefi sınıflandırmak için RTO ve RPO kullanmaktadır. RTO, kritik iş süreçlerini sürdürmek için BT yeteneklerini ayarlamak adına gereken süreyi belirlemek için yönetim tarafından kullanılmaktadır. RPO, yönetimin unutmak eğiliminde olduğu bir şeydir ve iş süreçleri gerçekleştirilemediğinde, bir kesinti sırasında, kuruluşun kaybetmeyi göze alabileceği veri miktarı ve hangi verilerin geri kazanılması gerektiğini cevaplamaktadır. Yönetim, kabul edilebilir risk düzeylerine karar vermek durumundadır (Wold, 2006).

2.2.5. Uygulamaların tespit edilmesi

RTO'lar ve RPO'lar ile sınıflandırılan iş süreçleri, veri ile birlikte desteklenen uygulama sistemlerine eşlenmelidir. Daha önce belirtildiği gibi, uygulamalar kritik, önemli veya kritik olmayan olarak sınıflandırılmaktadır. Sıklıkla olduğu gibi, bir iş süreci, iş sürecini destekleyen birden çok uygulamaya bağlı olacaktır. Bu uygulama sistemleri, desteklenen iş süreçleri ile aynı RTO'lar ve RPO'lar ile tanımlanmalıdır (Schwab ve diğerleri, 2003).

2.2.6. Sistem kurtarma süresinin (SRT) belirlenmesi

Sistem kurtarma süresi (SRT) etkinliği, bir felaket onaylandıktan sonra gerçekleşmektedir. Kuruluşlar, iş süreci RTO'sunu karşılamak için donanım sistemlerini ve bileşenleri kurtarmak için kullanacağı öncelik sırasını planlamak durumundadır. RTO'nun kısa zaman dilimlerinde, DRP genellikle kurtarma ana bilgisayar sistemlerinin ve ilgili bileşenlerin kurulmasını gerektirmektedir. Ana bilgisayar sistemleri ve ilgili bileşenler, iş süreçlerini gerçekleştiren uygulamaları yürütmektedir. Uygulama sistemleri tarafından ihtiyaç duyulan donanım altyapısı bileşenleri ve iş sürecini desteklemek için gerekli veriler tanımlanmalıdır. Tüm uygulama bağımlılıkları, ağ altyapı bileşenleri ve destek personeli de tanımlanmalıdır. RTO, ana bileşeni SRT'yi belirlemek için kullanılmaktadır ve iş sürecinden uygulamaya taşınmaktadır (Wiboonratr ve Kosavisutte, 2009).

Bir ana bileşenin sistem kurtarma süresi, iş süreci tarafından belirlenen beklentileri karşılayamıyorsa, SRT'yi spesifikasyona getirmenin birkaç yolu bulunmaktadır. İş süreci RTO'sunu barındıracak farklı bir felaket kurtarma paketi seçilebilmektedir. Uyarı bildirimi, değerlendirme ve afet bildirimi zamanı azaltılabilmektedir. İş süreci RTO'ları bir maliyet/fayda analizi temel alınarak yeniden değerlendirilebilmektedir. Bir donanım bileşeni çeşitli iş süreçlerini destekleyen birkaç uygulamayı barındırabileceğinden, SRT bu ana bileşene bağımlı bir uygulama için en kısa RTO'dan belirlenmektedir. Ana bilgisayar bileşeni, tüm donanım öğelerinden oluşmaktadırr. Bu, ana bilgisayar işleme sistemi, uygulamalar, veri depolama sistemleri, yerel ve geniş alan ağı ve güvenlik duvarlarını içeren güvenlik altyapısını içermektedir. SRT'yi tanımlayacak ve başarıyla belirleyebilecek bileşenler şunlardır:

- İş süreçlerini tanımlama,
- RTO gereksinimlerini belirleme,
- RPO gerekliliklerini belirleme,
- İş süreçlerini destekleyen uygulama sistemlerini tanımlamak,
- Uygulamaları destekleyen ana makineleri tanımlama,
- Ana bilgisayar sistemleri ve uygulamaları için iyileşme süresini belirleme (Miller, Craighead ve Karwan, 2000).

2.2.7. Uygulamalar için veri değer biriminin tanımlanması

Uygulama RPO'sunu destekleyen işletme faaliyeti, iş kesintisinden önce veya felaket olayı öncesinde gerçekleşmektedir. Felaket ortaya çıktıktan sonra, etkilenen sitedeki uygulamalar ve veriler DRP'yi çalıştırmak için kullanılamamaktadır. Bu nedenle, bilgi işlem merkezlerinin normal çalışması için, uygulamaların ve verilerin üretim/bilgisayar merkezinden uzaktaki bir depolama tesisinee kopyalanması sağlanmalıdır. Dışarıdan depolama tesisi ya kurtarma hesaplama merkezinde ya da SRT içinde depolama ortamından ana altyapı sistemine veri geri kazanılmasına izin veren mesafeli ve nakliye parametrelerinde bulunabilmektedir. Kurtarma kritikliğine dayanan uygulamalar ve veriler, bilgisayar merkezinden kurtarma/bilgi işlem merkezine iki yöntemden biri kullanılarak kopyalanmaktadır:

- Uygulama ve verilerin üretim hesaplama merkezinden geniş alan ağı (WAN) kullanılarak kurtarma bilgi işlem merkezi ya da elektronik kasası tesisine elektronik olarak kopyalanması. Bu çoğaltma, başlangıçta tüm uygulama ve verilerin çoğaltılmasını, ardından dosyaların zamanlanmış şekilde çoğaltılmasını kapsamaktadır.
- Verilerin, üretim/bilgi işlem merkezinden uzaktaki bir saklama tesisine fiziksel olarak gönderilebilen kaset gibi fiziksel olarak çıkarılabilir ortamlara kopyalanması.

Üretim uygulamaları kopyaları ve üretim sistemi verileri, işletme RPO gereksinimlerini yerine getirmek için üretim/bilgisayar merkezi sitesini belirtilen RPO zaman çerçevesi içinde bırakmaktadır. Bu durum, bant ya da kaset gibi fiziksel olarak çıkarılabilir ortamlarda özellikle geçerlidir. Uygulamalar ve veriler, üretim sistemlerinden

fiziksel ortama yedeklenmek ve RPO içindeki üretim alanından kaldırılmak durumundadır (Schwab ve diğerleri, 2003; Snedaker, 2007).

2.2.8. Kritik personel ve kurtarma ekiplerinin belirlenmesi

Kritik iş süreçlerini destekleyen uygulamalar ve ana bilgisayar sistemleri benzersiz bir bilgi, beceri ve kabiliyete sahip personele bağımlıdır. İş süreçlerini destekleyen altyapıyı kurtarmaya yönelik bilgiye sahip personelin belirlenmesi bir DRP'nin anahtarıdır. Temel destek personeli, beceri setleri ile birlikte tanımlanmak durumundadır. Destek bilgisi coğrafi olarak örgüt içerisinde dağılmaktadır. Bu durum, ilan edilen bir felaket durumunda organizasyonun DRP'yi yürütmek için yeterli eğitilmiş personele sahip olmasını sağlayacaktır. Çalışan beceri seti bilgileri ayrıca belgelendirilmekte ve DRP'ye dahil edilmekte ve DRP ile aynı frekansla güncellenmektedir (Schwab ve diğerleri, 2003).

2.2.9. Felaket kurtarma planının test edilmesi

Bir felaket kurtarma testinden en yüksek değeri elde etmek için açık test hedefleri ve başarı kriteri gerekmektedir. Test amaçlarının ve başarı kriterlerinin kullanılması, her DRP unsurunun ve genel BCP'nin etkinliğinin değerlendirilmesini sağlamaktadır. İki önemli test kriteri, işletme sürecinin kendi RTO'sunda, RPO içindeki veri değer birimi ile kurtarılmasıdır. Kriterler aşağıdaki gibidir:

- Kurtarma süresi hedefi (RTO)
    - Uyarı bildirimi/değerlendirme/felaket beyanı süresi bir felaket kurtarma testi bağlamı dışında test edilmekte ve doğrulanmaktadır. Standart işlem prosedürleri ve çağrı ağaçları, prosedürlerin ve kişisel iletişim bilgilerinin geçerli ve doğru olduğunu doğrulamak için test edilmektedir.
    - SRT, RTO uygulaması içinde bulunmaktadır. SRT, kurtarma işlemlerinin belirtilen amaç dahilinde tamamlanıp tamamlanamayacağını belirlemek için bir sistem kurtarma egzersiziyle test edilmektedir.
- Kurtarma noktası hedefi, kendisinin bir sistem felaket kurtarma testi bağlamı dışında herhangi bir zamanda karşılanabileceğini onaylamaktadır. Standart

işletim prosedürleri ve operasyonel kayıtlar, verilerin belirtilen hesapta karşılanabilmesi için, verilerin üretim hesaplama merkezinden taşınıp taşınmadığını belirlemek adına denetlenmekte ve doğrulanmaktadır.

Bir DRP'yi sınamak çok karmaşık bir yükümlülük olabilmektedir. İş sürekliliği planının genel amacı iş süreçlerine devam etmekken, bir felaket kurtarma planının genel amacı, normal işlemler sürdürülene kadar mevcut BT üretim ortamının bir bölümünü veya bir kısmını alternatif bir sitede çoğaltmaktır (Wold, 2006; Fallara, 2003).

2.2.10. Felaket kurtarma planının sürdürülmesi

DRP'nin ve BCP içindeki diğer planların sürdürülmesi, gerçek bir kurtarmanın başarısı için kritik önem taşımaktadır. Planlar, planlar tarafından desteklenen ve güncel olan ortamların değişikliklerini yansıtmak durumundadır. Mevcut değişim yönetimi süreçlerinin, kurtarma planının sürdürülmesini göz önüne alacak şekilde gözden geçirilmesi kritiktir. Değişim yönetiminin bulunmadığı alanlarda, değişim yönetimi prosedürleri önerilmek ve uygulanmak durumundadır. Çoğu kurtarma yazılımı ürünü bu gereksinimi göz önünde bulundurmaktadır (Wold, 2006).

2.2.11. Veri yedekleme

Verilerin düzenli aralıklarla yedeklenmesi kritiktir. İşletmenin türüne bağlı olarak, yedekleme sıklığı belirlenebilmektedir. Herhangi bir bilgiyi kaybetmeyi göze alamayan bir sektörde, gerçek zamanlı yedekleme gerekecektir. Bulut yedeklemelerin giderek daha popüler hale gelmesinin sebeplerinden biri de budur.

Birçok kişi veri yedekleme ve felaket kurtarmanın tek ve aynı şey olduğunu düşünmektedir fakat bu büyük bir yanılgıdır. Veri yedekleme, sabit aralıklarla veya gerçek zamanlı olarak üretilen verilerin kopyalarını almak anlamına gelmektedir. Yedekleme bantlar, diskler veya bulutta saklayarak yapılabilmektedir. Öte yandan DR, bir felaket olduğunda uçtan uca çözümdür. Yedeklenen veriden veri kurtarma yönünü sadece kapsamakla kalmaz, üretim tesislerinin restorasyonunu da öngörür ve kalıcı bir düzeltme yapılıncaya kadar üretimin makul kabul edilebilir seviyelere getirilmesini sağlamaktadır (Chad, 2003).

Bulut bilgi işleminin başladığı günden beri, bulutta bir DRP'nin olması alternatif bir seçenekti. Bununla birlikte, bulut bilgi işlem servislerinin fiyatı düşmeye başladığında, veri yedekleme ve felaket kurtarma için en iyi seçeneklerden biri olmuştur.

Bulutta veri yedekleme

Verileri yedeklemenin geleneksel yöntemi, kasetler, diskler vb. üzerine kopyalar almaktı ve bu oldukça basit, açık bir yöntemdi. Bu yöntemle ilgili sorun, kopyaların yerinde veya ateşe dayanıklı dolaplarda yerinde depolanması gerektiği yönündeydi. Bununla birlikte bu tür yöntemleri kullanırken çok daha ciddi bir sorun, çoğaltmanın bütünlüğüdür. Medya veya bant yolsuzlukları, verilerin geri yüklenmesini engelleyen ciddi bir sorundur. Verilerin tek başına kopyalanması yeterli değildir, ancak bütünlük denetimleri sürecin bir parçası olmak durumundadır (Wood, et al., 2010).

Bulut bilişim hizmetleri, makul seviyelerde fiyatlandırılmaya başlandığında cazip bir öneri olmuştur. Verilerin gerçek zamanlı olarak yedeklenebilmesi ya da ihtiyaç duyulması durumunda önceden belirlenmiş aralıklarla yedeklenmesi mümkün olmuştur (Krutz ve Vines, 2010). Veriyi bulutta depolamak için farenin bir tıklaması yeterli hale gelmiştir. Avantajlar çok yönlüdür:

- Veriler restore edildiğinde yüzde 99'u aşan bir güvenilirliğe sahiptir. Bu, kasetlerin, disklerin vb. en büyük dezavantajlarından birini ortadan kaldırmıştır. Bir felaket senaryosunda, bu düzeyde güvenilirlik çoğu iş gereksinimini makul bir maliyetle karşılamıştır.
- İş ihtiyaçlarına bağlı olarak, RPO ve RTO bulutta kolayca eşleştirilebilmektedir. Ancak bu metrikler ne kadar küçülürse, hizmetin maliyeti orantılı olarak artmaktadır. BT yöneticileri çok küçük RPO'lar ve RTO'lar kullanma seçeneğine sahiptir, o kadar ki, müşteri bir felaket olayının gerçekleştiğini tahmin bile edememektedir.
- Doğal afet senaryosunda, etkilenen coğrafi alan yaygın olacaktır. Hazır bulundurulan yerinde üretim merkezi bile etkilenebilmektedir. Yedekleme bulutta olduğunda, veriler genellikle farklı bir coğrafi bölgede olan bir sunucuda saklanır ve fazlalık teklifin bir parçasıdır. Buna ek olarak, bulut hizmeti sağlayıcısı felaket yedekleme prosedürlerini yerine getirmekte ve bu

durum toplam veri kaybına karşı ek bir koruma katmanı sağlamaktadır (Wood, et al., 2010; Krutz ve Vines, 2010).

Bulutta felaket kurtarma planı

Buluttaki DRP bir felaketin bildirildiği andan itibaren harekete geçirilebilmektedir. Veriler, RTO ve RPO ölçümlerine göre geri yüklenebilmektedir. Yerinde donanım kısmen veya tamamen yok edilmişse, doğru kimlik doğrulama işlemlerine tabi tutularak verilere sanal masaüstleri kullanılarak erişilebilmekte ve veriler geri yüklenebilmektedir. Müşteri eylemi buluta yönlendirildiğinde, trafikte bir miktar artış olmaktadır. Ancak bulut kullanmanın avantajlarından biri, hizmetlerin neredeyse anında ölçeklenebilmesidir.

Üretim bir kez makul seviyelere getirildiğinde, BT yöneticileri organizasyonu iş sürekliliği aşamasına taşıyabilmektedir. Kuruluş, bulutun üretim için yerinde üretim merkezini tam olarak ayarlayabilecekleri zamana kadar kullanabilmektedir. Kuruluşlar maliyetlerini kontrol edebilmektedir, çünkü yalnızca kullanılan hizmetler için ödeme yapılır ve gereksiz kapasite vb. konusunda endişelenilmesine gerek yoktur (Wood, et al., 2010; Krutz ve Vines, 2010). Veri yedekleme ve felaket kurtarma farklı ama iç içe geçmiştir. Bulut seçeneği mevcut olduğunda, BT yöneticileri, veri yedekleme ve felaket kurtarma için elverişli, uygun maliyetli bir araca sahiptir.

2.3. BT Hizmet Sürekliliği Yönetimi (ITSCM)

Teknoloji, çoğu iş sürecinin temel bir bileşeni olduğundan, BT'nin sürekli veya yüksek oranda kullanılabilirliği, bir bütün olarak işletmenin hayatta kalması için kritik öneme sahiptir. Bu durum, risk azaltma önlemleri ve kurtarma seçenekleri ile sağlanabilmektedir. Hizmet sürekliliği, bir hizmetin garantisinin önemli bir parçasıdır. Bir hizmet sürekliliği, işletmenin gereklerine uygun olarak sürdürülemiyorsa ve/veya geri yüklenemiyorsa, iş söz verilen değeri deneyimleyememektedir. Süreklilik olmaksızın hizmetin faydasına erişilememektedir. ITSCM, işletmenin felaket olarak algılanacak kadar önemli olduğunu düşündüğü olaylara odaklanmaktadır. Bir felaketi oluşturan şey organizasyondan organizasyona değişmektedir. Finansal kayıp, itibar zedelenmesi veya

yasal ihlal gibi bir iş sürecinin kaybının etkisi, minimum kritik gereksinimleri belirleyen bir BIA çalışmasıyla ölçülmektedir. Belirli BT teknik ve hizmet gereksinimleri ITSCM tarafından desteklenmektedir. Bir kurum içindeki ITSCM'nin kapsamı, sağlanan hizmetler ve bunların zaman içinde nasıl gelişip değiştiği konusunda örgütsel yapı, kültür ve stratejik yön (hem iş hem teknoloji) tarafından belirlenmektedir. ITSCM'nin amacı, daha büyük iş sürekliliği planını desteklemektir (OpenCampus, IT service continuity management).

2.3.1. BT hizmet sürekliliği

BT hizmet sürekliliği yönetimi (ITSCM), felaket kurtarma planlamasının ötesinde bir şeydir. İş sürekliliği ömrü ile uyumludur ve en kötü senaryonun hazırlanmasına yardımcı olmaktadır; bu yalnızca bir felaketten kurtulmak değil, felaketin başta olmasını önlemek için mümkün olan en kısa sürede durdurulmasıdır. ITSCM, hizmet kesintisi önceden tanımlanmış bir noktaya ulaştığında kurtarma seçeneklerini araştırır, geliştirir ve uygular. Genel iş sürekliliği planının bir parçası olmakta ve ayrı ayrı ele alınmamaktadır (Motahari-Nezhad ve Bartolini, 2011).

ITSCM, kuruluşların kurulumu için afetin ne olduğunun açıklamasının belirlenmesine yardımcı olmaktadır. Bir felaket oluşturan ön koşulların tanımlanması, ITSCM sürecinin bir parçasıdır. Bu tür tanımlar, hizmetlerin sağlanmasına ilişkin herhangi bir SLA'nın ayrılmaz bir parçasını oluşturmaktadır. ITSCM, ani ve ciddi bir etkiye neden olabilecek, işin devamlılığını hemen tehdit edebilecek riskleri ele almaktadır (Holman ve Houser, 2011).

Etkili ITSCM planının ayrı bir şekilde geliştirilmesi mümkün değildir, işin gereksinimlerini tam olarak desteklemek durumundadır. BC yaşam döngüsünün dört aşamasının BT yönlerini özellikle vurgulamak gerekmektedir:

- Başlatma,
- İhtiyaç analizi ve strateji tanımı,
- Uygulama,
- Operasyonel yönetim.

Aşama 1 - Başlatma

Başlatma süreci sırasında dikkate alınması gereken faaliyetler, ihtiyati tesislerin kuruluşta ne ölçüde uygulandığına bağlıdır. İşletmenin bazı bölümleri manuel çalışma ortamları temelli bireysel süreklilik planları oluşturmuş olabilmekte ve BT kritik olarak algılanan sistemler için acil durum planları geliştirmiş olabilmektedir. Bu durum süreç için iyi bir giriştir, ancak etkin ITSCM, kritik iş işlevlerini desteklemeye ve mevcut bütçenin en uygun şekilde uygulanmasını sağlamaya bağımlıdır.

Başlatma süreci kuruluşun tamamını kapsamakta ve aşağıdaki faaliyetlerden oluşmaktadır:

- Politika belirleme – Bu olgu, mümkün olan en kısa sürede kurulmak ve iletilmek zorundadır. Böylece BC konularında yer alan veya etkilenen kuruluşun tüm üyeleri, ITSCM'ye uyma ve bunlara destek olma sorumluluklarının farkına varmaktadır. En azından politika, yönetimin niyetini ve hedeflerini belirlemektedir.
- Referans ve kapsam şartlarının belirtilmesi – Bu adım, organizasyon içindeki yöneticilerin ve personelin kapsam ve sorumluluklarının tanımlanmasını ve çalışma yöntemini içermektedir. Risk değerlendirmesi ve iş etkisi analizini gerçekleştirme ve bir iş kesintisini desteklemek için gereken komuta ve kontrol yapısını belirleme gibi görevleri kapsamaktadır. Ayrıca, göze çarpan denetim noktaları, düzenleyici veya müşteri gereksinimleri, sigorta organizasyonu şartnameleri ve diğer standartlara uyma gibi konuları dikkate almak gerekmektedir.
- Kaynakların tahsis edilmesi - Etkili bir iş sürekliliği ortamı kurmak hem para hem de insan gücü açısından önemli bir kaynak gerektirir. Kuruluşun olgunluğuna bağlı olarak, ITSCM ile ilgili olarak, 2. aşama görevlerini yerine getirmek için personelin bilinmesi ve/veya eğitilmesi gerekebilmektedir. Alternatif olarak deneyimli dış danışmanların kullanımı, analizin daha çabuk tamamlanmasına yardımcı olabilmektedir. Bununla birlikte, kuruluşun tamamen harici desteğe güvenmeksizin süreci devam ettirebilmesi önemlidir.
- Proje organizasyonunun ve kontrol yapısının tanımlanması - ITSCM ve BCM projeleri potansiyel olarak karmaşıktır ve iyi organize edilip kontrol edilmelidir.

Denetim komitesine rapor veren ve çalışma gruplarına yön veren deneyimli bir proje yöneticisinin atanması başarıya ulaşmanın anahtarıdır. BT genel sürecin önemli bir bileşenini oluşturduğundan, projenin BT alanının raporlamasından yönetimin en üst düzeylerine en iyi biçimde yönlendirilmesi olabilmektedir.

- Proje ve kalite planlarının kabul edilmesi - Planlar, projenin kontrol edilmesine ve çeşitliliklerin ele alınmasına olanak tanımaktadır. Kalite planları, sonuçların ulaşılabilir olmasını ve kabul edilebilir bir kalite seviyesinde olmasını sağlar. Aynı zamanda, proje kaynak gereksinimlerini ve teslimatları iletmek için bir mekanizma sağlarlar; böylece gerekli tüm taraflardan satın alımı temin etmektedirler (Motahari-Nezhad ve Bartolini, 2011; Holman ve Houser, 2011).

Aşama 2 – İhtiyaç analizi ve strateji tanımı

Bu aşama, ITSCM'nin temelini sağlar ve bir kuruluşun bir iş kesintisinden veya felaketten ne kadar iyi geçeceğini gösteren ve gerçekleşmesi gereken maliyetleri belirlemek için kritik bir bileşendir. Bu aşama etkili bir şekilde iki bölüme ayrılabilmektedir:

- Gereksinimler - İş etki analizi ve risk değerlendirmesinin yapılması,
- Strateji - Gereksinimleri desteklemek için risk azaltma önlemleri ve kurtarma seçeneklerinin belirlenmesi ve kabul edilmesi.

Gereksinimler

Risk temelli bu yaklaşımda en kritik süreç iş etki analizinin ve risk değerlendirmesinin yapılmasıdır (Motahari-Nezhad ve Bartolini, 2011; Holman ve Houser, 2011).

İş etki analizi (BIA)

ITSCM gereksinimlerini belirlemedeki en önemli etken, bir felaket veya diğer hizmet kesintileri ve bu kayıpların tırmanma hızının bir sonucu olarak kuruluşun ne kadar kaybetmesi gerektiğidir. Bir iş etki analizinin (BIA) amacı, aşağıdakileri belirleyerek bunu değerlendirmektir:

- Kritik iş süreçleri,
- Kritik iş süreçlerinin bozulması sonucunda organizasyona neden olabilecek olası zarar veya kayıplar.

BIA şunları da tanımlamaktadır:

- Kayıp gelir, ek masraflar, hasar gören şöhret, şerefiye kaybı, rekabet avantajı kaybı da dahil olmak üzere hasar veya kayıpların alabileceği şekil,
- Bir hizmet kesintisinden sonra hasar veya kayıp derecesinin muhtemel olarak nasıl artacağı,
- Kritik ve önemli iş süreçlerinin minimum kabul edilebilir düzeyde çalışmaya devam etmesini sağlamak için gerekli olan personel, beceri, tesis ve hizmetler (BT hizmetleri dahil),
- Minimum personel, tesis ve hizmet seviyelerinin geri kazanılması gereken süre,
- Gerekli tüm iş süreçlerinin ve destek personelinin, tesislerin ve hizmetlerin tam olarak geri kazanılması için gereken süre.

Son üç madde, düşünülmesi veya uygulanması gereken ITSCM mekanizmalarının seviyesine yönelik sürücüleri sağlamaktadır. Bu seçenekler sunulduktan sonra işletme, daha düşük hizmet düzeylerinin veya artan gecikmelerin bir maliyet/fayda analizini temel alarak daha kabul edilebilir olduğuna karar verebilmektedir.

Bu tanımlar ve bileşenler kritik hizmet, uygulama ve altyapı bileşenlerini kritik iş süreçlerine eşleştirmeyi mümkün kılmaktadır ve böylece verilmesi gereken ITSCM öğelerini belirlemeye yardımcı olmaktadır. İş gereksinimleri sıralanır ve ilgili ITSCM unsurları, risk değerlendirme/azaltma ve kurtarma planlaması açısından teyit edilir ve önceliklendirilir. Etkiler, her bir iş süreci için belirli bir senaryoya göre ölçülür; bu işlemler, bir para piyasası işlem sürecinde esnafın çözümlenememesi ya da bir süre için faturanın alınamaması gibidir. İş etki analizi, kritik iş süreçlerindeki etkinin en yüksek olduğu senaryolara odaklanmaktadır. Etkiler senaryolara göre ölçülür ve genellikle süreç kategorilerinin bir veya daha fazlasına girmektedir. Bu süreç, bir işletmenin hangi hizmetin kullanılamamasının ne derece savunulamaz hale geleceğini anlamasını sağlamaktadır. Bu da, bu iş gereksinimlerini karşılamak için en uygun olan ITSCM mekanizmalarının belirlenmesini sağlamaktadır (Tjoa, Jakoubi ve Quirchmayr, 2008).

Etkilerin zaman içinde nasıl değiştiğini anlamak da önem arz etmektedir. Çıkış aşamasında süreçleri çok fazla sekteye uğratmayan bir etki, önlem alınmadığında ya da göz ardı edildiğinde kuruluşun hantallaşmasına hatta kritik süreçlerinin tökezlemesine sebep olabilmektedir.

Dengeli bir senaryoda, işe olan etkiler ortaya çıkıp zamanla daha da büyür, ancak tüm organizasyonlar bu şekilde etkilenmemektedir. Bazı organizasyonlarda, rapor yayınlama ihtiyacının ertelenebildiği ve şirket üzerindeki etkilerin belirli bir süre için tahakkuk etmeye başlamadığı bir danışmanlık organizasyonu gibi etkiler hemen belirgindir. Yatırım bankaları gibi diğer kuruluşlarda, hizmetin kısa bir süre zarfında kesilmesi, büyük etkilerin hemen tahakkuk etmesine ve önleyici çizginin uygulanmasına neden olmaktadır. Bununla birlikte bir noktada herhangi bir kuruluş için etkiler, işletmenin artık çalışamayacağı bir seviyeye gelecektir. ITSCM, acil durum seçeneklerinin tespit edilmesini sağlar ve böylelikle ticari etkilerin hizmet kesintisinden minimum düzeyde etkilenmesi için uygun önlemin uygun bir zamanda uygulanması sağlanır (Motahari-Nezhad ve Bartolini, 2011; Holman ve Houser, 2011).

Çoğu durumda, iş süreçleri tam bir personel, sistem ve diğer kolaylıklar olmadan yeniden kurulabilmektedir ve yine de müşterilere kabul edilebilir düzeyde hizmet sunabilmektedir. Bu nedenle iş kurtarma hedefleri aşağıdakilerle ifade edilmektedir:

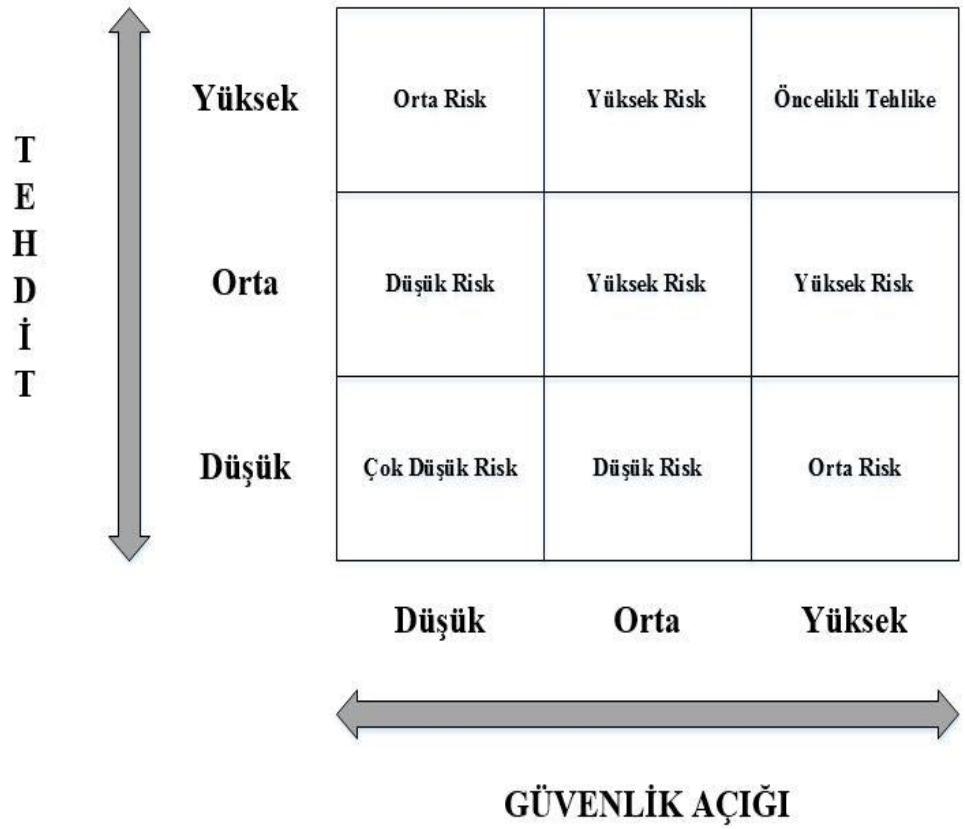
- Önceden tanımlanmış bir çekirdek personel ekibi ve belirtilen minimum tesislerin kurtarılacağı süre,
- Kalan personel ve tesislerin iyileştirilmesi için zaman çizelgesi.

Kurtarma gereksinimlerini ayrıntılı bir seviyeye getirmek her zaman mümkün olmayabilmektedir. Maliyetlerin kabul edilebilir olmasını sağlamak için olası etkinin geri kazanım masrafıyla dengelenmesine ihtiyaç duyulmaktadır. Bununla birlikte, kurtarma hedefleri farklı iş kurtarma ve ITSCM seçeneklerinin değerlendirilebileceği bir başlangıç noktası sağlamaktadır.

Risk değerlendirmesi

ITSCM gereksinimlerini belirleyen ikinci etken, bir felaketin veya ciddi bir hizmet kesintisinin gerçekten gerçekleşme ihtimalidir. Bu ihtimal, tehdit seviyesinin ve bir organizasyonun bu tehdide karşı savunmasızlık derecesinin değerlendirmesidir. Aşağıdaki risk değerlendirmesi faaliyetlerinin yapılması mühimdir:

- Risklerin belirlenmesi - diğer bir deyişle, hizmet kesintisine neden olan iş sürecini destekleyen belirli BT hizmet bileşenleri (varlıkları) için riskler,
- Tehdit ve güvenlik açığı düzeylerinin değerlendirilmesi - tehdit bir hizmet kesintisinin oluşma ihtimali olarak tanımlanmaktadır ve güvenlik açığı organizasyonun gerçekleşen tehditten ne ölçüde etkilenecek veya etkilenmeyeceği olarak tanımlanır. Bir tehdit, aşağıdaki faktörlere bağlıdır:
    - Bilgisayar sistemlerine yapılan kötü amaçlı zarar, önemli bir teknoloji sağlayıcının ticari başarısızlığı, bir kuruluşun web sunucularına yönelik saldırı ve yanlışlıkla hizmet kesintileri yaratan internet sitelerinin bozulması, kuruluşun konumu, ortamı, iç sistemler ve prosedürlerin kalitesi, kasıtlı hizmet kesintileri yaratan muhtemel motivasyon, kapasite ve kaynaklar,
    - BT servislerinin teslimatı için tek bir başarısızlık noktası olduğu yerde iş süreçleri savunmasızdır (örneğin, bir seyahat acentesi, uçuş rezervasyonları için bilgi akışlarına dayalıdır, eğer bağlantı başarısız olursa ve yedekleme mevcut değilse, uçuşlar satılamaz).
- Risk düzeylerinin değerlendirilmesi - genel risk daha sonra ölçülebilmektedir. Bu nicel veri toplanıyorsa, örneğin düşük, orta veya yüksek sübjektif bir değerlendirmeyi kullanarak nitel bir ölçüm olarak yapılabilmektedir. Risk düzeyini ifade etmek için kullanılan bir tablo biçimi örneği aşağıda gösterilmektedir. Her bir risk, ilgili tehdit ve kırılganlık açısından değerlendirilebilmektedir. Aşağıdaki tablo kullanılarak belirli risklerin oluşma ihtimalinin belirlenmesi mümkündür (örneğin yüksek bir tehdit ve yüksek güvenlik açığı yüksek bir olasılık anlamına gelmektedir) (Motahari-Nezhad ve Bartolini, 2011; Holman ve Houser, 2011).



Şekil 2.3. Risk Ölçüm Tablosu (Utz, 2008)

Risk analizini takiben, riskleri yönetmek için, yani riski kabul edilebilir bir asgari düzeye düşürmek veya riski azaltmak için uygun önlemleri veya risk azaltma önlemlerini (ITSCM mekanizmaları) belirlemek mümkündür.

ITSCM bağlamında, dikkate alınması gereken bir takım riskler vardır. Aşağıdaki tablo, BT yöneticisi tarafından göz önüne alınması gereken bazı risk ve tehditlerin bir kontrol listesini sunmaktadır.

Risk	Tehdit
Dahili BT sistemlerinin / ağlarının kaybı	Yangın gücü arızası Kundakçılık ve vandalizm, sel, uçak etkisi Hava durumundan kaynaklı hasar, çevresel felaket Terör saldırısı, sabotaj, katastrofik arıza Elektriksel hasar, kazara hasar, kötü kaliteli yazılım.
Harici BT sistemlerinin / ağlarının kaybı	Yukarıdakilerin tümü Hizmetlerin aşırı talep edilmesi Hizmet reddi saldırısı Teknik arıza
Veri kaybı	Teknik arıza İnsan hatası Virüsler Zararlı yazılımlar
Ağ hizmetleri kaybı	Ağa erişimin zarar görmesi veya reddedilmesi Servis sağlayıcıların tesisleri Servis sağlayıcının BT sistemleri / ağlarının kaybı Servis sağlayıcısının verileri kaybı Servis sağlayıcıların başarısızlığı
Anahtar teknik ve destek personelinin bulunmaması	Endüstriyel hareket Binaya erişimin reddi İstifa Hastalık / Yaralanma Ulaşım zorlukları
Servis sağlayıcıların başarısızlığı, örneğin dış kaynak BT kullanımı	Ticari arıza, örneğin iflas Binaya erişimin reddi Servis sağlayıcının kadrosunun bulunmaması Sözleşmeli hizmet seviyelerini karşılamada başarısızlık

Şekil 2.4. Risk ve Tehditler Tablosu (European Union Agency for Network and Information, 2008)

Risk değerlendirmesi kuruluşa özgü riskleri tanımlamaktadır. Bu risklerin birçoğu BT hizmetlerinin sürekliliğini sağlama konusuyla ilgilidir. İlgili tüm riskleri değerlendirmede başarısız olunması, kuruluşun bozulmaya maruz bırakıldığı eksik bir risk değerlendirmesine neden olacaktır.

İş sürekliliği stratejisi

Etki analizi ve risk değerlendirmesi ile seçilen ilişkili ITSCM mekanizmaları arasında harmanlanan bilgiler, optimum düzeyde bir risk azaltma ve kurtarma ya da süreklilik seçenekleri dengesi ile geliştirilecek ve organizasyon için uygun bir strateji sağlayacaktır. Buna göreli hizmet kurtarma öncelikleri ve göreceli hizmet değişiklikleri de dahildir (Ernest-Jones, 2005). Kuruluşlar teknolojinin kullanımı ve kullanılabilirliği (örneğin e-ticaret gelişmeleri) yoluyla daha fazla bağımlı hale geldikçe, ITSCM öğeleri iş sürekliliği stratejisinin tamamlayıcı bir parçası haline gelmektedir.

Risk azaltma önlemleri

Çoğu kuruluş, risk azaltma ve kurtarmanın birbirini tamamlayan ve her ikisinin de gerekli olduğu dengeli bir yaklaşım benimsemek zorundadır. Bu mümkün olduğunca BT hizmetinin sağlanmasına ilişkin risklerin azaltılmasını ve genellikle kullanılabilirlik yönetimi aracılığıyla sağlanmasını gerektirmektedir. Ancak iyi planlanmış olsa da, tüm riskleri tamamen ortadan kaldırmak mümkün değildir, örneğin, yakındaki bir binadaki yangın muhtemelen bir kordonun uygulanması sonucunda hasara veya en azından erişim reddine neden olacaktır. Genel bir kural olarak, bir kurtarma yeteneğinin çağrılması yalnızca en son çare olarak alınmalıdır. İdeal olarak bir kuruluş, işi ve/veya BT hizmetlerini kurtarma olasılığını artırmak için tüm riskleri değerlendirmektedir.

Tipik risk azaltma tedbirleri şunları içermektedir:

- Site dışı depolama da dahil olmak üzere kapsamlı bir yedekleme ve kurtarma stratejisi,
- Tek bir güç kaynağının binaya girmesi veya tek bir elektrik kuruluşundan gelen güç kaynağı gibi tek arıza noktalarının ortadan kaldırılması,
- Birden fazla sağlayıcıyla dış kaynak kullanımı hizmetleri,
- Esnek BT sistemleri ve ağların sürekli artan iş gereksinimlerini karşılamak için maksimum performans sağlamak üzere değiştirilmesi,
- Akıllı kartları kullanan fiziksel erişim kontrol sistemi gibi daha fazla güvenlik denetimi,
- Bastırma sistemleri ile birlikte yangın algılama sistemleri gibi yerel servis kesintilerini tespit etmek için daha iyi kontroller,
- Değişiklik kontrolü gibi hatalar veya arıza olasılığını azaltmak için prosedürleri iyileştirme.

Yukarıdaki tedbirler bir ITSCM sorununu mutlaka çözmeyecek veya riski tamamen ortadan kaldırmayacaktır, ancak hepsinin veya bunların bir kombinasyonu, hizmetlerin kuruluşa sunulma biçimiyle ilgili riskleri önemli ölçüde azaltabilmektedir. Kurtarma seçeneklerinde olduğu gibi, bir riskin azaltılmasının bir başka riski artırmaması önemlidir. Sistemlerin ve verilerin erişilebilirliği riski, üçüncü şahıslardan dış kaynak kullanımı yoluyla düşürülebilmektedir, ancak bu, sıkı güvenlik kontrolleri uygulanmadığı sürece

gizli bilgilerin tehlikeye atılma riskini artırabilmektedir (Schanze, Zeman ve Marsalek, 2007). Ana bilgisayar işlemlerinin uzaktan hizmet sağlayan üçüncü bir taraftan dış kaynak kullanımı, kuruluşun yapısını etkileyen bir hizmet aksamasının, ana bilgisayar sisteminin kullanılabilirliğini mutlaka etkilemeyeceği anlamına gelmektedir. Farklı üçüncü kişilere dış kaynak kullanımı, hizmetin bileşen parçalarının daima mevcut olması nedeniyle büyük bir arıza riskini azaltma noktasında yararı olacaktır. Elbette bu durum, hizmetin sürekliliğini korumak için esnek ağların ve üçüncü tarafın kendisinin etkili ve test edilmiş bir hizmet Sürekliliği planı olması gerçeğini varsaymaktadır.

Kuruluşların, seçilen kurtarma ve ITSCM seçeneklerini gerektiğinde uygulama ve entegrasyon yapabildiklerini ve gerekli servis kurtarma işleminin başarılabildiğini kontrol etmeleri önemlidir. Bir kuruluşun ITSCM stratejisi, risk azaltma önlemleri maliyeti ve kritik iş süreçlerinin kabul edilen zaman çizelgeleri dahilinde iyileştirilmesini desteklemek için kurtarma seçenekleri arasında bir dengedir (Motahari-Nezhad ve Bartolini, 2011; Holman ve Houser, 2011).

Kurtarma seçenekleri

Kısa ve uzun vadeli kurtarma için farklı seçenekleri düşünmeye ihtiyaç duyulabilmektedir. İş süreçleri harici servis sağlayıcılara oldukça bağımlı olduğu durumlarda, seçeneklerin hizmetlerin başarısızlığa veya en yoğun çatışmasına hitap etmeye yönelik bir düşünceye ihtiyacı vardır. Aşağıdaki durumlarda kurtarma seçenekleri dikkate alınmak durumundadır:

- Kişiler ve konutlar - sahip olunan, kiralanmış veya üçüncü bir tarafla mutabakata varılan alternatif binalar da dahil olmak üzere; diğer kuruluşlarla karşılıklı düzenlemeler; ve alternatif binaların hızlı bir şekilde tedarik edilmesi veya mevcut binaların yenilenmesi. Önerilen mekanların ilgili yerlerine, BT personeli de dahil olmak üzere kurtarılan işletme faaliyetlerini destekleyecek personelin hareketliliğine ve iş sürecini desteklemesi gereken toplam personel sayısına dikkat edilmek durumundadır.
- BT sistemleri ve ağları - bu seçeneklerin ITSCM'den sorumlu BT yöneticisi tarafından belirlenmesi ve kabul edilmesi ve BT sistemlerinin, donanımların, uygulamaların, yazılımların ve ağların ve bu sistemler ve tesislerde kullanılan

verilerin geri kazanılmasını içermesi gerekmektedir. Bu durum, hizmetin geri yüklenmesini sağlamak için etkin yedeklemelerin kullanılabilirliği ve kullanılabilirlik yönetimi ile birlikte gerçekleştirilmesi gerekenlere dayanmaktadır. Bu strateji aynı zamanda, disk yansıtma, UPS veya çift güç kaynakları, çift iletişim bağlantıları gibi kritik iş süreçlerini destekleyen BT hizmetlerinin yerel bozulmasını/kesilmesini desteklemek için süreklilik mekanizmalarının uygulanmasını içermektedir.

- Güç, telekomünikasyon, su, kurye ve görev gibi kritik hizmetler.
- Kağıt kayıtları ve referans materyal gibi kritik varlıklar.

Her seçeneğin maliyetleri ve faydaları analiz edilmek durumundadır. Bu analiz, aşağıdakilerin karşılaştırmalı bir değerlendirmesini içermektedir:

- İş kurtarma hedeflerini karşılama becerisi,
- Potansiyel etkide muhtemel azalma,
- Opsiyonun kurulma masrafları,
- Opsiyonun sürüdürülmesi, test edilmesi ve çalıştırılması maliyetleri,
- Bozulma veya felaket riskine karşı teknik, örgütsel, kültürel ve idari etkiler ve herhangi bir önlem alınmazsaki potansiyel etki.

Analizde bulunulurken, bir seçeneğin ortaya çıkmasının diğer riskleri olumsuz etkileyip etkilemeyeceğini dikkate almaya ihtiyaç bulunmaktadır (Motahari-Nezhad ve Bartolini, 2011; Holman ve Houser, 2011; Boshoff, 1996).

BT kurtarma seçenekleri

Acil durum sağlamak için BT tarafından düşünülebilecek birtakım seçenekler bulunmaktadır (Motahari-Nezhad ve Bartolini, 2011; Holman ve Houser, 2011; Boshoff, 1996).

❖Hiçbir şey yapmama

Günümüz iş ortamında organizasyonlar BT hizmetleri olmadan etkin şekilde ya da hiç çalışamamktadır. BT kurtarma seçeneği olarak hiçbir şey yapmama stratejisi

geçerliliğini yitirmiştir. Çünkü organizasyonlar nefes alabilmek için BT ve eklemlerine ihtiyaç duymaktadır.

❖Manuel çalışma alanları

BT tesisleri, kuruluşların bilgileri daha hızlı ve verimli bir şekilde işleyebilmelerini sağlamaktadır. Gerçekten de BT harcamalarının gerekçesi daha düşük bir personel sayısına dayanarak yapılmaktadır. Finans, bankacılık ve sigorta endüstrileri gibi bazı organizasyonlarda, karmaşık hesaplamalar, kısa bir süre elle yeniden üretmek zor olan uygulamalarla gerçekleştirilebilmektedir. Bunlar, aralarında beslenen bilgi ile farklı sistemlerle bir dizi hesaplamaya bağımlıdırlar veya onlara dış kaynaklardan beslenen bilgilere bağımlıdırlar. Bununla birlikte, BT servisine pratik ve mümkün olan her yerde yeniden başlayıncaya kadar manuel çalışma önlemleri etkili geçici bir önlem olabilmektedir.

❖Karşılıklı düzenlemeler

Benzer bir teknolojiyi kullanan başka bir kuruluşla bir sözleşme yapmak, bilgi işlem yükü arttığında ya da toplu işlem olduğunda etkili bir olasılık seçeneği oluşturmaktadır. Günümüzde dağıtılmış bilgi işlem ortamı, bunun pratik bir çözüm olmadığını ve etkin bir hizmetin yeniden başlatılmasını destekleyemeyeceğini gösteren, bireysel işlem gücü ve yüksek kullanılabilirlik için daha büyük bir gereksinim olduğundan bahsetmektedir. Buna ek olarak, karşılıklı düzenlemelerin adım adım yapılmasında ve güvenlik ihtiyacının artmasında bakım ve sürdürme zorlukları bulunmaktadır. Bununla birlikte, bazı karşılıklı düzenlemelerin sürdürülmesinde, örneğin yedeklemelerin ve diğer kritik bilgilerin yerinde depolanmasında, yararları olabilmektedir.

❖Kademeli kurtarma

Bu seçenek (soğuk bekleme), iş süreçlerinin derhal yenilenmesine ihtiyaç duymayan ve tam BT olanaklarının yeniden kurulması olmadan 72 saate kadar veya daha uzun süre çalışabilen kuruluşlar için geçerlidir. Bu seçenek, altyapı, telekomünikasyon bağlantıları ve bir kuruluşun kendi bilgisayar donanımını kurması için bir felaket durumunda mevcut olan, güç, çevre kontrolleri ve yerel ağ kablolaması ile tamamen

donatılmış boş alan sağlanmasını içerebilmektedir. Konaklama, ticari olarak üçüncü bir tarafça, bir ücret karşılığında sağlanabilmekte veya özel olabilmekte (kuruluş tarafından kurulmuştur) ve sabit veya taşınabilir bir hizmet olarak sağlanabilmektedir. Sabit bir tesis, hizmeti sağlayan üçüncü kişinin bulunduğu yerde veya özel olarak abonenin bulunduğu bir yerde kurulabilmektedir. Telekomünikasyon, veri pazarı vb. tüm hizmetlerin kurulduğundan ve kurtarma sürecinde yer alan personeli barındırmak için yeterli konaklama olanağının bulunmasını sağlamak için bir ihtiyaç vardır.

Taşınabilir bir tesis genellikle üçüncü bir taraf tarafından sağlanan ve organizasyon ile mutabık kalınan önceden belirlenmiş bir yerde ihtiyaç duyulduğunda bulunan prefabrik bir yapıdır. Bu yapı, bir araba parkında veya ev alanından biraz uzakta başka bir yerde, belki de başka bir binaya ait olabilmektedir. Kuruluşlar, bilgisayarlar, sunucular ve mini bilgisayarlar da dahil olmak üzere gerekli bilgisayar ekipmanlarının tedarik edilmesi için sözleşme çağrısında bulunabilmektedir. Kuruluş ya da yüklenici (hangisi önceden kararlaştırılmışsa), daha sonra donanımı kuruluş gereksinimlerine göre yapılandırmakta ve bir hizmet sunulmadan önce tüm verileri yüklemektedir. Kademeli bir kurtarma göz önüne alındığında, kuruluş tarafından hiçbir yedek parça güvenli bir şekilde tutulmazsa, değiştirilmesi imkansız değilse de zor olacak yüksek derecede özelleştirilmiş donanım veya ekipman öğelerine dikkat edilmelidir. Farklı ekipman kullanımıyla baş etmek için diğer ihtimal ölçümlerine ihtiyaç duyulabilmektedir. Aynı zorluklar, o zamandan beri işsiz kalan kuruluşlar tarafından tedarik edilen öğelere uygulanır ve muhtemelen hizmet sunumunu gecikmeler veya potansiyel sorunlar nedeniyle risk altına sokan alternatiflerin tespit edilmesi gerekir.

❖Ara kurtarma

Bu seçenek (sıcak bekleme) BT sürecini, iş süreçlerine etkileri önlemek için, önceden belirlenmiş bir süre içerisinde kurtarmaya çalışan kuruluşlar tarafından seçilmektedir. Bu tipik olarak, 24 ila 72 saatlik bir süre içinde kritik sistemlerin ve hizmetlerin yeniden kurulmasını gerektirmektedir. En yaygın olanı, üçüncü taraf kurtarma organizasyonları tarafından bir dizi abone için ve bu abonelere maliyeti dağıtarak sunulan ticari tesislerin kullanılmasıdır. Ticari tesisler genellikle işletme, sistem yönetimi ve teknik destek içermektedir. Maliyet, işlemci, çevre birimleri, iletişim gibi talep edilen imkanlara ve servislerin ne kadar hızlı geri yüklenmesi gerektiğine bağlı olarak değişmektedir.

Bu hizmetin avantajı, felaket durumunda müşterinin güvenli bir binada barındırdığı bir bölgeye neredeyse anında erişebilmesidir. Ancak sitenin, hizmeti başlatan kuruluş için yeniden yapılandırılması sırasında gecikmeler yaşanabileceğinden, sitedeki hizmetlerin restorasyonunun biraz zaman alabileceği ve kuruluşun uygulamaları ve verileri yedeklemelerden geri yüklenmesi gerekebileceği düşünülmektedir. Bir dezavantajı, sitenin neredeyse kesin olarak ev alanından bir miktar uzak olması ve bunun bir dizi lojistik problemi olmasıdır. Konumlar diğer kuruluşlarla paylaşılmaktadır, bu nedenle hizmet kesintisi iki organizasyonu aynı anda etkiliyorsa kullanılabilirlik garantisi verilememektedir. Kurtarma organizasyonunun, aynı coğrafi alandaki firmalara aynı hizmetleri vermediğinden emin olmaya ihtiyaç vardır. Bu durum, birden fazla çağrı riskini azaltmak için pozisyonların satışına iyi risk yönetimi uygulayan kurtarma organizasyonları tarafından iyi anlaşılmaktadır. Bu seçenek aynı zamanda oldukça pahalı bir seçenektir ve sigortaya benzetilebilmektedir. Bu tür düzenlemelerin, ihtiyatlılık alanındaki test için yeterli fırsatı içermesi önemlidir (Bryson, Millar, Joseph ve Mobolurin, 2001).

Ticari kurtarma hizmetleri, mutabık kalınan bir sistemin müşterinin sitesinde belirli bir süre içinde, genellikle 24 saat içinde teslim edildiği taşınabilir bir biçimde sağlanabilmektedir. Bilgisayar donanımı bir römorkta bulunur ve araziye kamyonla taşınır. Treyler, gerekli hizmetler ile birlikte bir bilgisayar ortamı olarak donatılmış olup, kurulacak hizmet için siteden römorka güç ve telekomünikasyon bağlantılarına ihtiyaç duyulmaktadır. Sitenin güvenliğini sağlamak için özel tedbirlerin alınması gerekebilmektedir. Bu yaklaşımın bir avantajı, römorkun gerekli park izinleri alınarak ana bölgeye yakın bir yerde kurulabilmesidir. Alternatif yerlerdeki kuruluşlar, etkilenmeyen binalarda kritik olmayan personelin yerinin değiştirilmesi ve mobil kurtarma yoluyla sağlanan bilgisayar tesislerinde konaklamanın sağlandığı karşılıklı bir geri dönüş düzenlemeyi tercih edebilmektedir.

❖Acil kurtarma

Bu seçenek hizmetleri derhal geri yüklemeyi sağlamakta ve genellikle üçüncü taraf kurtarma sağlayıcısı tarafından sağlanan ara kurtarma işleminin bir uzantısı olarak sağlanmaktadır. Acil kurtarma, bir hizmet aksamasından sonraki ilk 24 saat boyunca diğer kritik iş ve destek alanlarının kurtarılması ile desteklenmektedir. Anında kurtarmanın gerekebileceği durumlar, hizmet kaybının etkisinin bir bankanın işlem odası gibi para

kazanma yeteneğinde derhal etkili olduğu durumlardır. Bir serviste hızlı bir restorasyona gereksinim duyulduğunda, uygulama sistemleri ve iletişimleri halihazırda mevcut olan ve operasyonel sunuculardan yansıtılan verilere sahip sunucuları veya sistemleri kurmak mümkündür. Bir sistem hatası olması durumunda müşteriler, hizmet kaybından çok az kaybederek veya hiç kaybetmeyerek hemen yedekleme tesisine geçebilmektedir.

Bina kaybı veya erişim reddi durumunda, kuruluşlar bir kurtarma merkezinde sınırlı sayıda özel pozisyonlar için ödeme yapabilmektedir. Bu oldukça pahalı bir seçenektir ve kuruluşların çoğunluğu için uygun değildir. Bununla birlikte, bu pozisyonlar daima mevcuttur ve kullanmak için hazır bulunmaktadır. Bazı kuruluşlar dahili olarak sağlanan kendi özel acil kurtarma tesislerine ihtiyaç duyabilmektedir. Bu da pahalı bir seçenektir, ancak kısa süreli olmayan durumun önemli bir etkiye neden olabileceği belirli bir iş süreci için mantıklı olabilmektedir. Tesisin ayrı ayrı ve ana ev sahasından yeterince uzakta bulunması gerekmektedir; böylece o yeri etkileyen bir felaketten etkilenmeyecektir (Bryson ve diğerleri, 2001).

Oldukça kritik iş süreçleri için, canlı hizmetle güncel tutulacak alternatif bir yerde yansıtılmış bir servis kurulabilmekte ve düzenli aralıklarla veri aktarımı yapılabilmekte veya canlı hizmetten tekrarlar alınabilmektedir. Böyle bir hizmet yalnızca bir yedekleme hizmeti olarak kullanılabilmekte ve canlı işleme performansını etkilemeden sorgu erişiminde (raporlama gibi) de kullanılabilmektedir. Bu ayrıca, tüm finansal kayıtların eksiksizliğini ve bütünlüğünü korumak için yasal yükümlülüğün olması durumunda da yararlıdır. Aslında yedek kapasite olduğu için normal şartlar altında bu yedek kapasite geliştirme, eğitim veya test için kullanılabilmektedir, ancak servis devamlılığı durumu talep edilince hemen kullanılabilir hale getirilebilmektedir.

En iyi çözüm, canlı operasyonun bir parçası olarak yinelenen ekipmana sahip yansıtılmış bir siteye sahip olmaktır. Bununla birlikte, bu yansıtılmış sunucuların ve sitelerin seçeneklerinin kullanılabilirlik yönetimi ile yakın ilişki içerisinde uygulanması gerekmektedir. Sıcak bekleme ve acil kurtarma arasındaki daha önceki tanımları birbirinden ayırmak önemlidir. Sıcak bekleme, tipik olarak, 2 veya 4 saat gibi kısa bir zaman ölçeğinde hizmetlerin bulunabilirliği anlamına gelirken; buna karşılık acil kurtarma, hizmetlerin anında kullanılabilirliği anlamına gelmektedir. Kuruluşlar için bir kurtarma planı, bazı veya tüm senaryoların bir kombinasyonunu içerecektir. Literatürde, kritik iş

süreci için anında kurtarma, ek iş süreçleri için 4 saatlik kurtarma, anahtar destek hizmetleri için 8 saatlik kurtarma ve diğer işletme alanları içinse gerektiği zaman kurtarma farklılıkları ortaya konmuştur (Motahari-Nezhad ve Bartolini, 2011; Holman ve Houser, 2011; Boshoff, 1996).

Aşama 3 – Uygulama

Strateji kabul edildikten sonra iş sürekliliği yaşam döngüsü BT'yi ayrıntılı bir seviyede içeren uygulama aşamasına geçmektedir. Uygulama aşaması aşağıdaki süreçlerden oluşmaktadır:

- Organizasyonun kurulması ve uygulama planlarının geliştirilmesi,
- Destek olma düzenlemelerinin uygulanması,
- Risk azaltma tedbirlerinin uygulanması,
- BT kurtarma planlarının geliştirilmesi,
- Prosedürlerin geliştirilmesi,
- İlk denemeleri üstlenilmesi.

Bu süreçlerin her biri, BT'nin harekete geçmesi gereken belirli sorumluluklara göre değerlendirilmektedir.

Organizasyon planlaması

BT işlevi, BT etkileşimlerinin iş etki analizi ve gereksinim tanımında tanımlanan iş gereksinimlerini desteklemek üzere sağlanmasından sorumludur. Bununla birlikte BT kurtarma amaçları için, yalnızca komuta, kontrol ve iletişim yapısının bir parçasını oluşturmaktadır. Yapı üç katmana dayanmaktadır:

- Yönetici - Organizasyon içinde genel otoritesi ve kontrolu olan ve kriz yönetimi ve diğer bölümler (organizasyonlar, medya, düzenleyiciler, acil hizmetler vb.) ile irtibattan sorumlu olan üst düzey yönetim/yürütme kuruludur.
- Eşgüdüm - Genelde yönetici grubunun bir düzey altındadır ve kuruluştaki genel kurtarma çabalarını koordine etmekten sorumludur.
- Kurtarma - Kritik iş işlevlerini ve bu işlevleri desteklemek için kurulması gereken hizmetleri temsil eden bir dizi iş ve hizmet kurtarma ekibidir. Her ekip,

kendi alanlarında planları gerçekleştirmekten, personel, müşteriler ve üçüncü taraflarla irtibat kurmaktan sorumludur. BT içinde, kurtarma ekipleri BT servis ve uygulaması tarafından gruplandırılmaktadır; örneğin altyapı ekibi harici bağlantıları, ses hizmetleri, yerel alan ağlarını vb. kurtarmaktan sorumlu bir veya daha fazla kişiye sahip olabilmektedir, destek ekipleri işletim sistemi veya uygulama platformuna göre bölünebilmektedir. Buna ek olarak, iş etki analizi sırasında tanımlanan hizmet, uygulama veya bileşenler için iyileştirme öncelikleri iyileştirme planları içerisinde belgelendirilmekte ve uygulanması sırasında uygulanmaktadır (Peppard ve Ward, 1999).

Uygulama planlaması

Plan geliştirme, uygulama sürecinin en önemli bölümlerinden biridir ve uygulanabilir planlar olmaksızın süreç kesinlikle başarısız olmaktadır. En üst seviyede aşağıdakileri içeren genel bir koordinasyon planına ihtiyaç vardır:

- Acil müdahale planı,
- Hasar değerlendirme planı,
- Kurtarma planı,
- Yaşamsal kayıt planı,
- Kriz yönetimi ve halkla ilişkiler planı.

Bu planlar, bir hizmet kesintisini tanımlamak ve bunlara yanıt vermek, etkilenen tüm personel ve ziyaretçilerin güvenliğini sağlamak ve iş kurtarma sürecini uygulamak için bir gereksinim olup olmadığını belirlemek için kullanılmaktadır. Son olarak her bir kritik iş alanı, kurtarma ekibini oluşturacak kişilerin ayrıntılı bir planının hazırlanmasından ve kurtarma düzenlemelerinin başlatılması için üstlenilecek ayrıntılı bir görev listesinden sorumludur. ITSCM, bilgisayar sistemlerini, ağı ve telekomünikasyon sistemini bir felaket durumunda kurtarmak için gerekli olan tüm bilgileri içermek zorundadır ve ardından hizmet kesintisi çözüldükten sonra işi normal işleme geri döndürmektedir. Planın geliştirilmesinde gerekli olan çeşitli bilgi kaynaklarını dikkate almaya ihtiyaç vardır ve bunlar, iş etki analizi, hizmet seviyesi anlaşmaları, güvenlik gereksinimleri, işletim talimatları ve prosedürleri ve harici sözleşmeler yoluyla belirlenen asgari gereklilikleri içermektedir. Bu plan, kilit BT kurtarma personelinin kurtarma alanına taşınması ve

barındırılması ihtiyacını giderecek, kritik personel için geceleme konaklama kullanımı gibi diğer planlarla tamamlanacaktır. Kurtarma sitesi uzun süre (örneğin haftalarca) kullanılmak zorundaysa, bu özellikle önem arz etmektedir.

Uygulama planlama sürecinin bir parçası olarak, kritik iş hizmetleri sunmak için gerekli olan önemli sözleşmeleri gözden geçirmek çok önemlidir. Bu sözleşmeler, uygun görülürse, bir BCM hizmeti sağladıklarından emin olmak için gözden geçirilmelidir; kabul edilen tanımlanmış bir hizmet seviyesi vardır ve operasyonlar kurtarma sitesine (kısmen veya tamamen) geçmek zorunda kaldıklarında sözleşme hala geçerli ve yürürlüktedir. Sözleşmelerde bu ayrıntılar yoksa, hizmetin kritikliği gözden geçirilmeli ve sağlanmayan hizmetle ilişkili riskler değerlendirilmektedir (Li, Yang, Sun ve Sohal, 2009).

Risk azaltma önlemlerini uygulamak

Aşama 2'de detaylandırılan risk azaltma tedbirleri uygulanmak durumundadır. Bunların çoğu, hizmetin kullanılabilirliğini etkileyen başarısızlık olasılığını azalttığı için, çoğu zaman kullanılabilirlik yönetimi ile bağlantılı olarak elde edilmektedir. Tipik risk azaltma tedbirleri aşağıdakileri içermektedir:

- UPS'in kurulması ve yedekleme gücünün artırılması,
- Minimum kesinti bile kabul edemeyen kritik uygulamalar (örneğin bir banka işlem sistemi) için hata toleranslı sistemler,
- Dış ortamda depolama ve arşivleme,
- Veri kaybına karşı önlem alma,
- Standart yapılandırmayla önceden yapılandırılmış ve hatalı bir sunucuyu minimum yapı ve yapılandırma süresi ile değiştirmek için kullanılabilen yedek bir yerel alan ağı (LAN) sunucusu gibi ekipman veya bileşen hatası durumunda kullanılacak yedek ekipman/bileşenler (Li, Yang, Sun ve Sohal, 2009).

Yedekleme düzenlemelerinin uygulanması

Kurtarma seçenekleri, Aşama 2'de detaylandırılmıştır. Kurtarmanın konaklama, sistem ve telekomünikasyon gibi bir dizi hazırlık düzenlemesine dayandığını hatırlamak önemlidir. Yedekleme düzenlemelerini uygulamak için bazı eylemler gereklidir, örneğin:

- Üçüncü taraf kurtarma tesisleri için pazarlık yapma ve sözleşme düzenlemeye girme,
- Yedek konaklama hazırlama ve donatma,
- Yedek bilgisayar sistemlerinin satın alınması ve kurulması,
- Harici servis sağlayıcılarla bilgi teknolojileri servis sürekliliği planları üzerinde müzakere etmek ve gereken özeni göstermek.

Yedekleme düzenlemelerini çalıştırmak, test etmek ve sürdürmek ve gerektiğinde başlatılmalarını sağlamak için eğitim ve yeni prosedürler gerekli olabilmektedir.

ITSCM planlarının geliştirilmesi

ITSCM planları, kritik sistemler, hizmetler ve tesisler için gerekli bilgilerin sağlanmasına veya işleyişin kabul edilebilir bir süre içinde sağlanmaya devam etmesini sağlamak için geliştirilmektedir. Genel olarak iş sürekliliği planları, BT sistemlerinin ve olanaklarının kullanılabilirliğine güvenmektedir. Bunun bir sonucu olarak ITSCM planları, gerekli sistemlerin ve tesislerin kabul edilebilir bir operasyonel durumda teslim edilmesini ve kuruluş tarafından kabul edildiğinde amaca uygun olduğundan emin olmak için tüm faaliyetleri ele almaktadır. Bu yalnızca sistemlerin ve tesislerin restorasyonunu değil, aynı zamanda teslimat öncesi gerekli olan testlerin (performans, işlevsel, operasyonel ve kabul testleri) ve veri bütünlüğünün ve tutarlılığının doğrulanması arasındaki bağımlılıkların anlaşılmasını da gerektirir.

Hizmetlerin, sistemlerin ve tesislerin kritikliği ve önceliği, ITSCM planlarına dahil edilmeleri için, iş sürekliliği planını düzenleyenler ve uygulayanlar tarafından iletilmektedir. Bu iletim, kesintilerin iş tarafından istenen öncelik sırasına göre ve sistem bağımlılıklarına tabi tutulmasını sağlamaktadır. Buna ek olarak, hizmet altyapısının sağlanması ve ITSCM planlamasının eksiksiz olması konusunda karşılıklı mutabakata varmak mümkündür.

Planların dağıtımının yönetimi, anahtar personelin her zaman yedeklerini bulundurmasını sağlamak adına önemlidir. Planlar, yalnızca en yeni sürümlerin dolaşımda olmasını sağlamak için, kontrollü dokümanlar olmalıdır ve her alıcı kişisel bir kopyanın

sahadan uzak tutulmasını sağlamak durumundadır. Tüm bunlara ek olarak şunlardan emin olmak gerekmektedir:

- Sisteme aşina olmayan teknik bir kişinin prosedürleri izleyebilmesini sağlamak için yeterli ayrıntılar oluşturulmaktadır. Sisteme aşina olmayan kişilerin bir kurtarma testi gerçekleştirmesi sağlanmaktadır.
- Kurtarma planları, veri kurtarma noktası, bağımlı sistemlerin bir listesi, bağımlılığın yapısı ve veri kurtarma noktaları, sistem donanım ve yazılım gereksinimleri, yapılandırma ayrıntıları ve sistemle ilgili diğer önemli bilgilere referanslar verilmesi gibi kilit ayrıntıları içermektedir.
- Sistemin kurtarma aşamalarında, örneğin sistem işletim durumuna getirildikten sonra, bağlantı denetimleri, işlevsellik denetimleri veya veri tutarlılığı ve bütünlük denetimleri gibi belirli eylemleri kapsayan bir denetim listesi dahil edilmektedir (Motahari-Nezhad ve Bartolini, 2011; Holman ve Houser, 2011; Boshoff, 1996).

Prosedürlerin geliştirilmesi

ITSCM planı, üstlenilen belirli teknik görevlere bağlıdır. Bunların tam olarak belgelendirilmesi ve kapsamlı olması gerekmektedir, böylece sadece okur-yazarlığı olan bir kişinin kurtarmayı üstlenmesi sağlanabilecektir. Prosedürlerin de aşağıdakileri içerecek şekilde geliştirilmesi gerekmektedir:

- Yedek donanım ve ağların kurulumu ve testi,
- Yazılım ve verilerin tüm iş süreçlerinde tutarlı olan ortak bir referans noktasına geri yüklenmesi,
- Çokuluslu bir organizasyonda farklı saat dilimleri,
- İş kesme noktaları.

Ekipmanların arızalanması durumunda sistemlerin ve verilerin geri yüklenmesine ilişkin prosedürler gibi birçok prosedür zaten mevcut olabilmektedir ve bunlar ek olarak bir başka ITSCM planına rafine edilmek ve eklenmek durumundadır (Park, Kim ve Choi, 2008).

İlk test

BT, teknik bileşenlerin sağlanmasından ve bunların etkili bir şekilde test edilmesinden sorumludur. İlk teknik test genellikle işletmeyi dahil etmeye gerek kalmadan yapılabilmektedir. Bununla birlikte, daha sonraki testler için, işi, kapasiteyi ispatlamak ve iş kazanımının ortak amacına ulaşmak için gerekli olan faaliyetleri ve kaynakları karşılıklı olarak anlamaya yardımcı olmak için dahil olmaktan kaçınılmazdır. Tam bir test için, iş süreçlerinin iyileştirilmesi ve dış tarafların katılımı da dahil olmak üzere, tüm yedekleme düzenlemelerinin mümkün olduğunca yerine getirilmesi gerekmektedir. Bu durum planların eksiksizliğini test etmekte ve onaylamaktadır.

Testler duyurulabilmekte veya habersiz olabilmektedir. Ancak bu durumda, üst yönetimin onayının önceden alınması gerekir, aksi takdirde taahhüdün yerine getirilmesi zor olabilmektedir. Tüm testlerin, olabildiğince gerçekçi olarak tanımlanan, tanımlanmış test senaryolarına karşı gerçekleştirilmesi gerekmektedir. Bununla birlikte, en kapsamlı test bile her şeyi kapsamamaktadır. Meslektaşlarının yaralanmasına veya ölümüne neden olan bir hizmet aksamasında personelin bir krize tepkisi sınanamaz ve planlar bunun için izin vermek durumundadır. Buna ek olarak testlerin, net bir şekilde tanımlanmış amaçlara ve başarıya veya egzersizin başka yollarını belirlemek için kullanılacak eleştirel başarı faktörlerine sahip olması gerekmektedir (Motahari-Nezhad ve Bartolini, 2011; Holman ve Houser, 2011; Boshoff, 1996).

<u>Aşama 4 - Operasyonel yönetim</u>

Uygulama ve planlama tamamlandıktan sonra sürecin her zamanki gibi işin bir parçası olarak sürdürülmesini sağlamaya ihtiyaç vardır. Bu durum, operasyonel yönetim yoluyla sağlanmaktadır ve aşağıdakileri içermektedir:

- Farkındalık - Farkındalık, hizmet sürekliliğine özgü öğeler için organizasyonu ve bilhassa BT organizasyonunu kapsamak durumundadır. Bu, tüm personelin iş sürekliliği ve hizmet devamlılığının etkilerini fark etmesini ve bunları normal çalışma rutininin ve bütçesinin bir parçası olarak görmesini sağlamaktadır.

- Eğitim - BT, BT okur yazarı olmayan işletme kurtarma ekibi üyelerinin, kurtarmayı kolaylaştırmak için gerekli yeterlilik düzeyine sahip olduklarından emin olmak için eğitim vermesine yardımcı olabilmektedir.
- İnceleme - Güncel kalmalarını sağlamak için ITSCM sürecinden elde edilen tüm çıktıların düzenli olarak gözden geçirilmesi gerekmektedir. BT ile ilgili olarak, yeni sistemler veya ağlar gibi BT altyapısı, varlıkları veya bağımlılıkları veya hizmet sağlayıcılarındaki bir değişiklik gibi önemli bir değişikliğin yanı sıra iş yönü, iş stratejisi veya BT'de bir değişiklik olduğunda önemli olan inceleme yapmaktır. Kuruluşlar tipik olarak hızlı bir değişikliğe sahip olduklarından, devam etmekte olan bir inceleme programına yatırım yapmak ve ITSCM'yi örgütsel işletme gerekçelendirme süreçlerine dahil etmek gerekmektedir. Değişiklik kontrol süreci uyarınca yeni şartlar uygulanabileck durumda tutulmaktadır.
- Test - İlk sınamayı takiben, stratejinin kritik bileşenlerinin en az yılda bir kez ya da üst düzey yönetim ya da denetim tarafından yönetilen şekilde test edilmesini sağlamak için düzenli bir test programı hazırlamak gereklmektedir. BT altyapısındaki tüm değişikliklerin, BT hizmetlerinin genel olarak sağlanması kapsamında doğru şekilde işlev görmesini sağlamak için uygun bir şekilde uygulanan stratejiye dahil olması önem arz etmektedir.
- Kontrolün değiştimi - Testleri ve incelemeleri izleyerek ve günlük değişikliklere yanıt olarak ITSCM'nin güncellenme planlarına ihtiyaç duyulmaktadır. Altyapıdaki herhangi bir değişikliğin BT veya üçüncü kişiler tarafından sağlanan olasılık düzenlemelerine yansımasını sağlamak için ITSCM, değişim yönetimi sürecinin bir parçası olarak dahil edilmek durumundadır. Yanlış planlar ve yetersiz kurtarma yetenekleri ITSCM'nin başarısızlığına neden olabilmektedir.
- Güvence - ITSCM yaşam döngüsündeki son süreç, ITSCM çıktılarının kalitesinin üst düzey işletme yönetimi tarafından kabul edilebilir olduğuna ve operasyonel yönetim süreçlerinin tatminkar bir şekilde çalıştığına dair güvence sağlamayı içermektedir (Dattero, Galup, Quan ve Conger, 2009).

2.3.2. Çağrı

Çağrı, iş sürekliliği ve ITSCM planlarının nihai testidir. Tüm hazırlık çalışmaları başarıyla tamamlandıysa ve planlar geliştirilmiş ve test edilmişse, BCP'nin çağrılması basit bir süreç olmak durumundadır.

Çağırma planların önemli bir bileşenidir, ki bu da çağrı sürecini ve rehberliği içermektedir. Özellikle üçüncü taraf bir kurtarma tesisi kullanılacaksa, çağırma kararı sert ve ciddi bir şekilde alınmak durumundadır. Bu çağrıya maliyetler dahil olmakta ve süreç iş bozulmasını içermektedir. Bu karar tipik olarak, hasar değerlendirmesi ve diğer kaynaklar yoluyla toplanan bilgileri kullanarak iş ve destek departmanlarından (BT de dahil olmak üzere) üst düzey yöneticileri içeren bir kriz yönetimi ekibi tarafından yapılmaktadır.

Günün veya gecenin herhangi bir saatinde bir bozulma meydana gelebilmektedir, bu nedenle çağrı işlemi hakkında rehberlik hazır olmak durumundadır. Planlar hem ofiste hem de evde mevcut olmaktadır, ve kriz yönetimi ekibinin kilit üyeleri, her zaman planı detaylandırırken birlikte olması gereken ve aşağıdakileri içeren kısa bir yardım mektubunu vermektedir:

- Bu planların yerleri,
- İlgili anahtar eylemler ve karar noktaları,
- Kriz yönetimi ekibinin iletişim bilgileri.

Geri çağırma kararı bir kurtarma alanındaki tesislerin kurulmasıyla ilgili bir öncülük olabileceğinden hızlı bir şekilde yapılmaktadır. Bir bina yangınında kararın verilmesi oldukça kolaydır, ancak elektrik kesilmesi durumunda, bir kararın kısa bir süre içinde beklendiği durumlarda, sorun çözülmezse çağrının gerçekleşeceği bir son tarih belirlenmektedir. Bu son tarih, kriz yönetimi ekibi tarafından, örgütte kabul edilemez bir etkinin önlenmesi için iş süreçlerinin yeniden kurulması gereken kritik noktadan geri dönerek oluşturulacaktır. Çağrının gerekli olabileceği bir durum ortaya çıktığında çağırma kararı verilirse, tesislerin mümkün olan en kısa sürede sunulabilmesi için kurtarma hizmeti sağlayıcısını derhal faaliyete geçirmek gerekmektedir (Motahari-Nezhad ve Bartolini, 2011; Holman ve Houser, 2011; Boshoff, 1996). Çağrı yapma kararı, aşağıdaki birtakım faktörleri göz önüne almaya ihtiyaç duymaktadır:

- Potansiyel çağrının zararı ve kapsamı,
- Kesintinin olası uzunluğu ve tesislerin ve/veya hizmetlerin bulunmaması,
- Günün saati/ay/yıl ve potansiyel ticari etkisi (Yıl sonunda, yıl sonu işlemesinin zamanında tamamlanmasını sağlamak için çağırma ihtiyacı daha fazla olabilmektedir.),
- Kesin bir tarihte yapılan işe bağlı olarak işin özel şartları.

Kriz yönetimi ekibi iş kurtarma tesislerini başlatmaya karar verdikten sonra bunu örgüt içinde iletmek gerekmektedir. Bu genellikle, çağrı ağaçlarının kullanılmasıyla gerçekleştirilmektedir. Bu durumi organizasyonun tamamında tanımlanmış kurtarma personeli ile hızlı ve verimli iletişim kurma mekanizmasıdır. Kriz yönetimi planı, işe başlamak için irtibat kurulacak kilit personelin ayrıntılarını ve ITSCM kurtarma planlarını içermektedir. Bu planların her birine, planların başlatılabilmesi için gerekli personelin (ve vekillerinin) iletişim bilgileri dahil edilmek durumundadır. Mesajın kurtarma sürecinde yer alan tüm önemli personele geçtiğinden emin olmak hayati önem taşımaktadır. Mesajı alacak son kişi, başlatıcıyla iletişim kurarak ve alınacak eylemi onaylayarak son noktayı kapatmaktadır. ITSCM planı, aşağıdakiler dahil olmak üzere üstlenilmesi gereken faaliyetlerin detaylarını içermektedir:

- Yedekleme bantlarının alınması veya verilerin alınması için veri tonlama kullanımı,
- Gerekli belgelerin, prosedürlerin, iş istasyonu görüntülerinin vb. sahadan uzakta saklanması,
- Gerekli teknik servis personelinin gerekli sistem ve hizmetlerin kurtarılmasına başlanması adına kurtarma alanına gidebilmesi için harekete geçirilmesi,
- Destek hizmetleri, uygulama ve telekomünikasyon tedarikçileri ile temas kurmak ve uyarıda bulunmak, kurtarma işleminde eylemlerde bulunmak veya yardımda bulunmak için gerekli olabilmektedir.

İlk kurtarma boyunca tüm faaliyetlerin kaydedilmesi önem arz etmektedir. Bu kayıtlar, nelerin iyi gittiğini analiz etmek ve kurtarılması ya da iyileştirilmesi gereken alanları belirlemek için hizmet kesintilerinin ardından kullanılacaktır. Planlar, faaliyetleri kaydetmek için tüm personele verilmesi gereken boş kütükleri (telefon konuşmaları,

etkinlikler için zamanlamaları vb.) ve yaşanmış konuları içermektedir (Motahari-Nezhad ve Bartolini, 2011; Holman ve Houser, 2011; Boshoff, 1996).

Çağrı yapma ve ilk kurtarma olasılığı, birçok insan için uzun saatler içeren yüksek bir etkinlik zamanı olabilmektedir. Kesintilerin yola koyulması kurtarma ekibi liderleri tarafından tanınmakta ve yönetilmektedir. Vardiya ve teslimat planlaması, mevcut tesislerin en iyi şekilde kullanılmasını sağlamak için yapılmaktadır. Çalışanların taahhüdü, hizmetin bozulması bittikten sonra kabul edilmekte ve potansiyel olarak ödüllendirilmektedir. Ayrıca, bilgi güvenliğinin doğru seviyede tutulduğundan ve veri korumasının korunduğundan emin olmak için, normal işletme ve teknoloji kontrollerinin çağrı, kurtarma ve normale dönme sırasında yerinde olmasını sağlamak çok önemlidir. Bilgi güvenliği ve veri koruma kontrol ve mekanizmalarının hizmet devamlılığının normal aşamalarında çağırılması, iyileştirilmesi ve geri getirilmesi sırasında muhafaza edilmesi ve uygulanmasının sağlanması hayati önem taşımaktadır (Boshoff, 1996).

Kurtarma tamamlandıktan sonra işletme kurtarma sahalarıi iş sürekliliği stratejisinde belirlenen ve kabul edilen seviyede çalışabilir olmaktadır. Bununla birlikte amaç, işi normal seviyelere çıkarmak ve kurtarma sitesini mümkün olan en kısa sürede boşaltmak olacaktır. Kurtarma süresi orijinal servis kesintisine bağlı olacaktır. Bir elektrik kesintisi durumunda normale dönme oldukça hızlı bir şekilde başarılabilir, oysa bir yangın durumunda etkilenen binanın yeniden çalışması imkansız olabilir ve alternatif konaklama aranmalıdır. Ne olursa olsun, normale dönme dikkatli bir şekilde planlanmakta ve kontrollü bir biçimde gerçekleştirilmektedir (Motahari-Nezhad ve Bartolini, 2011; Holman ve Houser, 2011; Boshoff, 1996).

Bilgi teknolojisi hizmet sürekliliği planı, kuruluşların yalnızca büyük sistem arızaları olduğunda cevap verme becerilerini geliştirmeleri değil, aynı zamanda önemli olaylara karşı dayanıklılıklarını geliştirmeleri, kritik sistemlerin ve hizmetlerin başarısız olması durumunda bu arızalar kabul edilebilir RTO limitleri dahilinde geri kazanılmasını sağlamasıdır.

BIA bilgisi, RTO sürecini tanımlamak ve kurtarma önceliğini belirlemek için kullanılmaktadır. Bu durum kurtarma işlemini ve kullanıcı gereksinimlerini karşılayan bir etkinliğin kuruluş gereksinimlerini eşleştirmesini sağlamaktadır.

Kurtarma planları bir hiyerarşide düzenlenmiştir. Bir site kaybı planı, bir binanın kaybından etkilenebilecek sistemleri ayrıntılarıyla açıklamaktadır. Her bir hizmet için ayrı bir plan, bir olayın her aşamasında ayrıntılı prosedürler ve adım adım yönergeler sağlamakta ve böylece kurtarma ekipleri hizmetleri geri yükleyebilmekte ve böylece kabul edilen süreç ve bileşen RTO'larını karşılayabilmektedir. Planlar açık ve öz olmalıdır ve bir miktar bilgi beklenmekle birlikte açık yerel bilgiyi tahmin etmemektedir, aksine sistemlerin yeniden yapılandırılması için dış yardım gerekmektedir (aynı durum felaket kurtarma planları için de geçerlidir). Her bir prosedür, tek bir sistemin veya bileşenin kurtarılmasını gerçekleştirmek için kullanılabilmektedir (örneğin sunucu başarılı bir şekilde çalışmaktadır ancak veritabanı yönetim sistemi çökmüştür) ve bağımsız olarak bulunmalıdır. Her belgede ayrıca ön koşulların ayrıntıları bulunmak durumundadır; birden fazla bileşen hatası olması durumunda doğru sıraya uyulabileceği anlamına gelmektedir (örneğin başarısız disk değiştirme, işletim sistemini yeniden oluşturma, veritabanı yükleme, güvenlik ayarlarını yapılandırma ve daha sonra verileri geri yükleme). Bir ITSCM planının başarısını ölçmek çok zordur. Herhangi bir olay RTO sürecinde geri kazanılacak ve bir BC olayı başlatılmayacaktır. Tek ölçü, kesinti süresinin kısaltılması ve SLA'ya uyumun iyileştirilmesidir (European Union Agency for Network and Information, 2008).

2.3.3. Destekleyici dokümanlar

BT gereksinimleri ve boşluk analizi ve risk kayıtları belgeleri herhangi bir standartta resmi olarak BCP'nin parçası değildir ancak literatürdeki deneyim, süreci desteklemek için gerekliliğini göstermektedir.

BT gereksinimleri ve boşluk analizi

BT gereksinimleri ve boşluk analizi, BC ve ITSCM arasındaki bağlantı olan çalışma belgeleridir. Bununla birlikte BT felaketten kurtarma bunu dikkate almamaktadır. Bu belgeler herhangi bir spesifikasyonda tanımlanmasa da, ihtiyaçlar belgesi ITIL'de ima edilmektedir. Pratik bir perspektiften bakıldığında, şartların ve risk tepkisinin resmi şartnamesi oldukları için önemlidirler ve bu nedenle üst düzey yöneticileri ve üst düzey bir imzalamayı gerektirmektedir.

BT gereksinimleri BIA'lardan alınan ayrıntıları içermektedir. Bu ayrıntılar, genel olarak uygulamaları ve BT bileşenlerini listelemektedir ve her ilgili BT bileşeni için her kritik süreç tarafından belirlenen bir RTO ve RPO bulunmaktadır. Bu bilgi, kritik bileşenleri ve bunların RTO'larını belirlemek için kullanılmaktadır. Bu durum sonuç olarak hizmet kataloğu, hizmet seviyesi sözleşmeleri ve BT stratejisinin yanı sıra ITSCM planlarını da yönetecektir. Mevcut altyapı nedeniyle BT bu gereksinimleri her zaman karşılayamamaktadır. Bu durum kuruluşları boşlukları vurgulayan bir boşluk analizi raporuna götürmektedir. Üst düzey yönetici daha sonra riskin nasıl hafifletileceğine karar verebilmektedir. Bu süreç altyapıyı yükseltmek için stratejik bir karar olabilmekte (bazı maliyetlerle) veya işletme birimleri gerçek kurtarma süresini karşılamak için manuel geçici çözümler sunmak zorunda kalabilmektedirler. Boşluk analizindeki maddeler risk kayıtlarına kaydedilmektedir (Brown ve Swartz, 1989).

Risk kayıtları

Kurumsal risk kayıtları, organizasyonun tüm risklerinin ayrıntılarını içermektedir. Bu kayıtlar, risklerin hesaplanması, gerekli olduğu yerlerde yapılan işlemler, eylemlerin tamamlandığı ve risk maddesinin kapatıldığı gözden geçirme tarih ve tarihlerinin birlikte tanımlanarak oluşturulduğu şekliyle bunları tanımlayan ve değerlendiren bir araçtır.

Bir iş sürekliliği riski kaydı, son değerlendirmenin tarihi, riskin açıklaması, etki ve olasılık tahmini, olumsuzlama kontrolleri ve istenen eylem talimatını hedef, tarih ve sahibi ile birlikte içermektedir. Düzgün korunan bir risk kaydı, iletişim için yararlı bir araç sağlamaktadır (International Organization for Standardization, 2018).

BT riski kaydı, bilgi teknolojisi ve sistemleri ile tanımlanan riskleri kaydetmektedir. Birçok kuruluş bunu kurumsal risk kaydına dahil ederken, daha büyük kuruluşlar departman başına bir kayıt yaptırmaya meyillidir ve en yüksek önem derecesi riski kurumsal risk kayıtlarına terfi etmektedir. Risk kayıtlarının bazıları iş alanlarını etkileyeceği için, bu risk kayıtları üst yönetim ekibince bulunmaktadır; çünkü bu risklerin içerdiği risklerin kabulü BT'in sorumluluğu değildir (European Union Agency for Network and Information, 2008).

3. ÇERÇEVE, STANDARTLAR VE KILAVUZLAR

Günümüzde, bir BT ortamında hareket eden her rekabetçi kuruluş, karakteristik ihtiyaçlarına göre BT standartlarının ve uygulamalarının en iyi şekilde kullanılmasını sağlamak durumundadır. BT en iyi uygulamalarının gittikçe artan bir şekilde benimsenmesi, BT endüstrisinin iş dünyasındaki BT'nin kalitesini ve güvenilirliğini daha iyi yönetmesini ve giderek artan sayıda düzenleyici ve sözleşmeye dayalı gereksinimlere yanıt vermesini gerektirmektedir. Mevcut BT ortamı ve bilgi sistemlerine uygulanabilecek çok sayıda standart göz önüne alındığında, her bir organizasyonun ihtiyaçlarını karşılayan en uygun standart setini seçmesi bir zorluktur.

BT'nin amaçlarını, servislerini ve sürekli gelişme ihtiyacını tanımlaması basit değildir; bu nedenle, mevcut ekonomide dünya genelindeki işletmeler, müşteri ve şirketlerinden, bütünlüğünden ve güvenliğinden ödün vermeden uygun bir maliyetle büyüme ve yönetişim elde etmek için uğraşmaktadır (Nastase, Nastase ve Ionescu, 2009).

3.1. BT Yönetim Çerçevesi

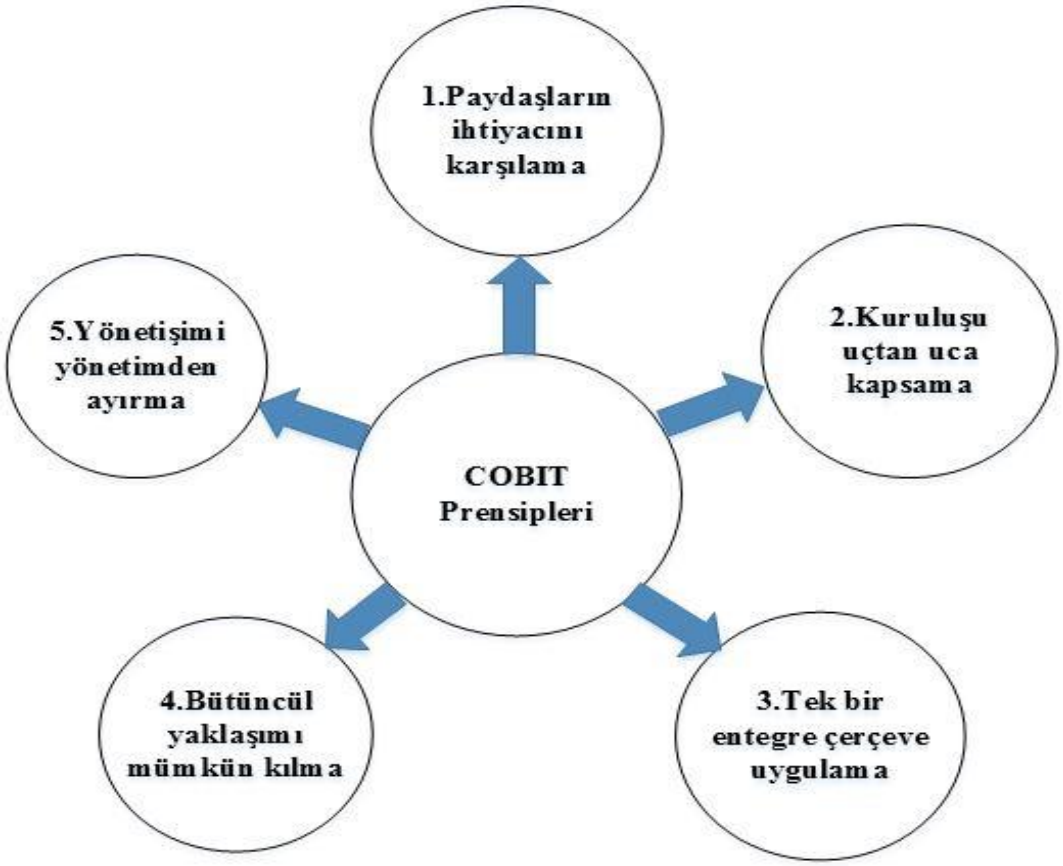
Tutarlı bir süreç kullanarak kurumsal bazda geniş iş sürekliliği yönetimini desteklemek adına BT sürekliliği için bir çerçeve geliştirilmektedir. Çerçevenin amacı, altyapının gerekli esnekliğini belirlemeye yardımcı olmak ve felaket kurtarma ve BT ihtimal planlarının geliştirilmesini sağlamak olmaktadır. Çerçeve, dahili ve harici servis sağlayıcılarının ve onların yönetiminin ve müşterilerinin rollerini, görevlerini ve sorumluluklarını ve felaket kurtarma belgesini belgelemek, test etmek ve yerine getirmek için kuralları ve yapıları oluşturan planlama süreçlerini kapsayan süreklilik yönetimi için örgüt yapısına ve BT acil durum planlarına değinmektedir. Plan aynı zamanda, kritik kaynakların belirlenmesi, kilit bağımlılıkların belirlenmesi, kritik kaynakların mevcudiyetinin izlenmesi ve raporlanması, alternatif işleme ve yedekleme ve kurtarma ilkelerine ilişkin konuları ele almaktadır ki bazıları aşağıda listelenmiştir.

- Etkinleşmeden önce plan koşullarınının açıklanması,
- Acil durum prosedürlerinin ve uygun mercilerle yükümlülüklerin belirlenmesi,
- İşlem kaynaklarının ve yerlerinin tanımlanması,
- Depolama için yedekleme ve konum bilgisinin tanımlanması,

- Yeniden başlatma prosedürlerinin ve bakım çizelgesinin belirlenmesi,
- Farkındalık ve eğitim faaliyetlerinin yerleştirilmesi,
- Bir bileşen planını alternatiflerle yürütmek için bireysel sorumlulukların tanımlanması (Willcocks, Feeny ve Olson, 2006).

3.2. COBIT

COBIT, ISACA tarafından BT yönetimi ve BT yönetişimi için oluşturulmuş bir çerçevedir. Bu çerçeve, yöneticilerin kontrol gereksinimleri, teknik sorunlar ve iş riskleri arasındaki boşluğu doldurmasına olanak tanıyan bir destekleyici araç setidir. COBIT, işletmelerin hedeflerini gerçekleştirmelerine ve kurumsal BT yönetiminin etkin yönetimi yoluyla değer katmalarına yardımcı olan kapsamlı bir çerçeve sunmaktadır. Yönetim sistemi, fayda, kaynak ve risk değerlendirme kararları alırken tüm menfaat sahiplerini göz önüne almaktadır. COBIT, bilgi ve ilgili teknolojilerin yönetilmesi ve yönetimine kurumsal çapta ve uçtan uca perspektiften bakmaktadır.



Şekil 3.1. COBIT Prensipleri (ISACA, 2012)

COBIT kuruluşlar tarafından, BT ile ilgili çerçeveler gibi, en son kullanılan ilgili diğer standart ve çerçeveler ile uyumludur. COBIT uygulanması durumunda bir şeyin işe yarayıp yaramayacağını etkileyen faktörler, yönetişim ve BT üzerindeki kurumsal yönetim ilişkisidir (Lainhart IV, 2000).

3.3. ITIL

ITIL, BT hizmetlerini iş gereksinimleriyle uyumlu hale getirmeye odaklanan BT hizmet yönetimi için bir dizi uygulamadır. ITIL'in faydalarından aşağıdakiler gibi sıralanabilmektedir:

- Kaynak kullanımını geliştirmesi,
- Daha rekabetçi olunması,
- İşin azaltılması,
- Yedekli çalışmayı ortadan kaldırması,
- Proje çıktılarını ve zamanını iyileştirmesi,
- Görevi kritik BT hizmetlerinin kullanılabilirliğini, güvenilirliğini ve güvenliğini geliştirmesi,
- Hizmet kalitesini haklı kılması,
- Ticari müşteri ve kullanıcı taleplerini karşılayan hizmetler sunması,
- Merkezi süreçleri bütünleştirmesi,
- Hizmet sunumunda rol ve sorumlulukları belgelemesi ve iletmesi,
- Önceki deneyimlerden öğrenmesi,
- Kanıtlanabilir performans göstergeleri sağlaması göze çarpmaktadır.

COBIT ve ITIL, BT servis yönetimi (ITSM) alanındaki bilgi teknolojisi uzmanları tarafından uzun yıllar kullanılmaktadır. Birlikte kullanılan COBIT ve ITIL, şirketlerin BT tarafından yönetilen hizmetler ile bu hizmetlerin kendi bünyesinde sağlanıp sağlanmadığı veya hizmet sağlayıcılar veya iş ortakları gibi üçüncü taraflardan edinilmiş olup olmadığı ile ilgili olarak yönetim konularında rehberlik sağlamaktadır.

ITIL, yaşam döngüsü boyunca BT hizmetlerini yönetmenin yolu olarak görülebilmektedir. COBIT ise, BT tarafından aktifleştirilen ve kuruluş tarafından en yüksek değeri yaratmak için kurumsal BT'nin nasıl yönetileceği ile ilgilidir ve bu arada

riskleri ve kaynakları optimize etmektedir. COBIT, paydaş ihtiyaçlarını karşılamada bir kuruluşu destekleyen ilkeleri ve etkinleştiricileri, özellikle tüm varlık boyunca BT varlıklarının ve kaynaklarının kullanımı ile ilgili olanları açıklamaktadır. ITIL, kurumsal BT'nin hizmet yönetimi planlayıcıları olan bölümlerini (süreç faaliyetleri, organizasyon yapıları vb.) daha ayrıntılı olarak açıklamaktadır (Gehrmann, 2012).

3.4. ISO/IEC 27031

ISO/IEC 27031, iş sürekliliğinin sağlanmasında bilgi ve iletişim teknolojisinin rolündeki kavramlar ve ilkeler hakkında rehberlik etmektedir. Standart:

- Herhangi bir kuruluş için bir yapı veya çerçeve (aslında bir dizi yöntem ve süreç) önermektedir.
- İş sürekliliğinin sağlanmasına yardımcı olan kurumun BCM'sinin bir parçası olarak BT hazırlığını iyileştirmek için performans kriterleri, tasarım ve uygulama ayrıntıları da dahil olmak üzere tüm ilgili yönleri tanımlamaktadır ve belirtmektedir.
- Bir organizasyonun BT sürekliliğini, güvenliğini ve dolayısıyla bir felaketten tutarlı ve tanımlanmış bir şekilde ayakta kalmaya hazır olduğunu ölçebilmesini sağlamaktadır.

Standart, BT altyapısı ve sistemleri üzerinde etkili olabilecek tüm olayları kapsamaktadır (yalnızca bilgi güvenliği ile ilgili değildir). Bu nedenle, bilgi güvenliği olayı işleme ve yönetimi, BT hazır planlama ve hizmetleri uygulamalarını genişletmektedir. İş sürekliliği için hazırlanan bilgi ve iletişim teknolojileri hizmetlerinin uygun olduğu kadar esnek olmasını sağlayarak BCM'yi desteklemekte ve kuruluş tarafından gerekli görülen ve kabul edilen zaman çizelgeleri içerisinde önceden belirlenmiş seviyelere ulaşılmasını sağlamaktadır. BT hazırlığı iş sürekliliği amaçları için önemlidir, çünkü:

- BT yaygındır ve birçok organizasyon kritik iş süreçlerini destekleyen BT'ye büyük ölçüde bağımlıdır,
- BT ayrıca olayı, iş sürekliliğini, felaket ve acil müdahaleyi ve ilgili yönetim süreçlerini destekler,

- İş sürekliliği planlaması, BT kullanılabilirliğini ve sürekliliğini yeterince dikkate almadan ve korumadan eksik kalabilmektedir (Disterer, 2013).

3.5. Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) - NIST SP 800-34

NIST, tüm operasyonlar ve varlıklar için yeterli bilgi güvenliği sağlamak adına standartların ve kılavuzların geliştirilmesinden sorumludur. NIST, federal kurumlara bilgi sistemleri güvenliğinin birçok yönü için standartlar ve yönergeler sağlayan özel yayınlar (SP) ve federal bilgi işleme standartları (FIPS) serilerine sahiptir.

NIST SP 800-34 - BT sistemleri için isteğe bağlı planlama kılavuzu - haziran 2002'de ilk kez yayınlanmıştır ve ABD hükümeti BT ihtimal planlaması için talimatlar, tavsiyeler ve düşünceler sağlamıştır. Acil durum planlaması, bir acil durum veya sistem bozulması sonrasında BT servislerini kurtarmak için geçici tedbirleri ifade etmektedir. Federal sistemler için tasarlanmış olmasına rağmen, NIST SP 800-34 özel sektörün büyük bölümünde, özellikle BT, acil durum planlaması için kılavuz olarak kullanılmıştır (National Institute of Standards and Technology , 2010).

3.6. Basel II: İş Sürekliliği Yönetimi için Temel Oluşturulması

Basel II, karşı karşıya kalabilecekleri operasyonel ve finansal risklerden korumak için bankalara sağlanan yönergelerdir. Basel komitesi ayrıca, operasyonel riske ilişkin farklı alanlarda güvenilir uygulamaları içerecek dokümantasyonu yani operasyonel riskin yönetimi ve denetimi için güvenilir uygulamaları yayınlamıştır. Böyle bir alan iş sürekliliğini temsil etmektedir. Kılavuzların, gerçekleşebilecek risklerin analizini ve potansiyel etkisini göstermesini sağlayan bu dokümantasyonda bazı ilkeler bulunmaktadır. Tüm ilkeler değil ama bazıları kesinlikle bu parametreler üzerinde durmaktadır:

İlke 1 : Operasyonel risk hakkında yönetim kurulunun bilinçlendirilmesi.

İlke 3 : Operasyonel risk yönetimi çerçevesinin uygulanması için üst düzey yönetim sorumluluğu, farkındalık ve politika geliştirilmesi.

İlke 7 : Odaklanma, acil durum planlaması ve iş sürekliliği planlaması üzerinedir.

İlke 9 : Operasyonel risk yönetim politikaları, usulleri ve uygulamaları değerlendirilirken yönetimin rolü.

Bu ilkeleri burada dahil etmenin nedeni, operasyonel risk ve iş sürekliliği arasında bir ilişki olmasındandır. Basel komitesi operasyonel riski "yetersiz veya başarısız iç süreçler, insanlar ve sistemler veya dış olaylardan kaynaklanan kayıp riski" şeklinde tanımlamaktadır. Basel komitesi aynı zamanda yedi adet spesifik risk olayı kategorisini belirtmektedir. Bu yedi kategoriden üçü doğrudan iş sürekliliği ile ilgilidir:

- İstihdam uygulamaları ve iş yeri güvenliği.
- Çevresel ve insan yapımı olayların yol açtığı fiziksel varlıkların zarar görmesi.
- İş kesintileri ve sistem hataları (donanım, yazılım, ağ ve yardımcı program sorunlarından kaynaklanan).

Basel e-bankacılık komitesi, e-bankacılık ve hizmetlerin kullanılabilirliğini sağlamak için bankaların etkin kapasiteye, iş sürekliliğine ve acil durum planlama süreçlerine sahip olmalarını şart koşmaktadır ve aynı zamanda, bankaların iş devamlılığı konusunda periyodik denetimler yapmaları gerektiğinin altını çizmektedir (Ranjan, Kumar, ve Abhishek, 2012).

SONUÇ VE ÖNERİLER

Bugünkü iş dünyası, en çok bilgi sistemlerine ve bilgi teknolojisine bağımlıdır. Standart iş risklerine ek olarak, BT platformlarına bağımlılık BT tabanlı iş risklerini de üretmektedir. BT ile ilgili tehditleri tanımlamak bir organizasyonda bilgi kaynaklarını yönetmenin önemli parçası olmuştur ve başka bir tehdit gibi (fiziksel, doğal, ticari, rekabet) bir işletmenin sorunlarına neden olabilecek bir tehdit olarak değerlendirilmelidir. İşletmeler, BT ile ilgili riskleri ve diğer iş risklerini önlemek (azaltmak, hafifletmek, yönetmek) için çeşitli yaklaşımlar uygulamaktadırlar. Bilgi kaynaklarını yönetmek için arzu edilen yöntemleri belirten çeşitli standartlar ve tavsiyeler bulunmaktadır. Bu alanda, uluslararası standartlaştırma kurumlarının öngördüğü standartlara ek olarak çeşitli ulusal standartlar ve tavsiyeler ile çeşitli özel şirketlerin en iyi uygulamaları kullanılmaktadır.

BCM, işletmelerin kritik fonksiyonlarının ve çıktılarının neler olduğunu ve onlara yönelik tehditlerin tanımlanmasına yardımcı olmaktadır. Bu tehditlerle başa çıkmak için etkin önlemler tasarlamak adına kanıtlanmış bir planlama çerçevesi sağlamaktadır. Ve eğer riski hafifletmek mümkün değilse, bozulma oluştuğu zaman sonuçlarını yönetmek için uygulanabilir acil durum planları sağlanmaktadır.

İş sürekliliği yönetiminin kökleri veri kurtarma alanına girmiştir ve bu nedenle bir organizasyon içindeki bilgi sistemleri (BS) ve BT uzmanlarının sıkıca kontrolü altına alınmıştır. Büyük bir olay sırasında ve sonrasında tüm kritik işlevlerin devam etmesi halinde bir organizasyonun tüm kritik görev unsurlarının BS ve BT ile aynı seviyede göz önüne alınması gerektiği konusunda giderek artan bir farkındalık oluşmaktadır. Bu artan bilinçle, iş sürekliliği her işletme birimi içerisinde sıklıkla yönetilir ve veri ve sistem kurtarma işlemi BS ve BT personeli tarafından ele alınmaktadır. Son yıllarda bu bölünme kaybolmaya başlamıştır, çünkü her iki grup da açıkça birbiriyle ilişkili olan konular üzerinde birlikte çalışmanın değerini görmeye başlamaktadır. BS/BT ve iş stratejisi, işletmeleri hizalamanın iş değerini giderek daha fazla anlamaları nedeniyle daha entegre hale gelmektedir. Buna ek olarak, risk, sağlık ve güvenlik yönetimi stratejileri ile yakınsama bulunmaktadır.

Kuruluşların tüm yöneticileri, işletme için en kritik olan sistemleri tanımlamak ve korumak için birlikte çalışmalıdır. BIA ve BCP, kriz sırasında kritik işlevlerin devam

etmesine yardımcı olmalı veya mümkün değilse bir olaydan sonra iyileşme önceliklerine rehberlik etmelidir.

BCM küçük çaplı ve başlıklı olaylarla baş etmektedir ve tüm küçük ve orta büyüklükteki işletmeler (KOBİ) için tek seferlik bir planlama egzersizi değil gerçek bir iş sürecidir. Maksimum etkinlik için, normal iş planlaması ve karar verme işi dokusuna uymalıdır. BCM, BT sistemleri gibi belirli varlıklardan ziyade tüm iş süreçlerine odaklanmaktadır, çünkü çalışması için bir işletme kritik iş süreçlerini yürütmeye devam etmelidir. Bu süreçler, tek bir iş fonksiyonu içerisinde bulunabilir veya bunların birçoğunu bütünleştirebilir veya etkileyebilir. Personelin uygun çalışma koşulları yoksa, kritik kağıt kayıtları yok edilmişse veya kuruluş müşteri ve tedarikçileriyle iletişim kuramazsa BT sistemlerini tek başına kurtarmak bu tür iş süreçlerini kısıtlamaz. BCM önleme ile ilgilidir, sadece bir tedavi değildir. Sadece olayların meydana geldiği durumlarla başa çıkmakla kalmaz, aynı zamanda krizi ve afetleri önler, müşterilere ürün ve hizmet sunumunun sürekliliğini garantilemek için daha fazla esneklik kurmayı amaçlayan bir işletme kültürü kurmaya çalışır.

Her önemli iş biriminden personel ekibin üyeleri ve tüm afet kurtarma planlama faaliyetlerinin bir parçası olarak dahil edilmelidir. Felaket kurtarma planını oluşturmak için bu insanlar iş süreçlerini, o süreçlerin, ağların ve sistemlerin arkasındaki teknolojiyi anlamalıdır. Uygulamalar ve sistemler, görev kritikliği ve işletme için kritik olan ekip tarafından belirlenmelidir. Sistem RTO'su ve verinin RPO'su planlama aşamasında yönetim tarafından tanımlanmalıdır ve iş yeniden başlatma stratejilerinin geliştirilmesinde kullanılmalıdır. Kurtarma planı ve stratejileri RTO ve RPO'yu karşılamak üzere tasarlanmalıdır. İyi geliştirilmiş, donanımlı ve sürdürülen bir felaket kurtarma planı, felaket durumunda kayıpları en aza indirecek ve kritik iş süreçlerinin devamlılığını sağlayacaktır.

Tüm faaliyetler, teknoloji arızası, yangın, sel, işletme arızası, hastalık ve kötü niyetli saldırı gibi iç ve dış olaylardan bozulmaya duyarlıdır. BT sürekliliği, bir bozulma meydana gelmeden önce veya bir olayla ilişkili olayların tespit edilmesinde tepki verme ve bu olayların aksatılmasına neden olduğunda cevap verme ve kurtarma olanağı sağlar. BT sürekliliği, organizasyonel stratejiyle uyumlu olan BT stratejisi ve BT hizmet yönetiminin ayrılmaz bir parçası olmalıdır. Bir organizasyonun olumsuz koşullar oluştuğunda hedeflerine ulaşmaya ve ürünlerini ve hizmetlerini sunmaya devam etmesini sağlayan BT stratejisi ve hizmet yönetimi unsurlarıdır. BT sürekliliği bir kuruluşun genel BCM sürecini

desteklemelidir. BCM, organizasyonun süreçlerinin aksamadan korunmasını ve bozulma olduğunda organizasyonun olumlu ve etkili bir şekilde yanıt alabilmesini sağlamayı amaçlamalıdır. Oraganizasyonlar, BCM önceliklerine karar vermeli ve bu bağlamda BT faaliyetlerini gerçekleştirmelidir. BT süreklilik yönetimi ve BCM, etkili yönetimin, sağlam yönetişimin ve kurumsal ihtiyatlılığın önemli bir parçasını oluşturmalıdır. Üst yönetim, organizasyonun bozulma karşısında çalışmaya devam etme yeteneğini korumaktan sorumludur.

Bazen BCP geliştirme çalışması, çıkışı bulunmayan bir tünel olarak düşünülür, çünkü kapsamlı araştırma analizleri ve BCP gelişimiyle ilişkili çok sayıda dökümantasyona rağmen, bir BCP etkinliği acil bir durum ortaya çıkana kadar gösterilemez. Bununla birlikte, tamamen farklı bir bakış açısıyla, BCP geliştirme çalışmaları, yönetimin yeniden yapılandırılması için büyük bir fırsat sunmaktadır. Belirtildiği gibi iş, kaynak hasarının bir işletmede yaratacağı etkiyi analiz etmek için kritik işletme faaliyetlerinin iş süreçleri ile gerekli kaynaklar arasında bir ilişki modeli oluşturmayı içermelidir. Aslında bu model, yönetim ortamındaki değişikliklerle baş etmek ve kaynakları optimum ve derhal tahsis etmek için bir simülasyon modeli olarak kullanılabilir. Temel olarak BCP geliştirme çalışması, önemli iş faaliyetlerini acil durumlarda bile en az kaynakla nasıl devam ettireceğinizin çekirdeğini elde etmek için yapılan bir etkinlikten başka bir şey değildir. Bu etkinlik, tüm işten çıkarmaları ortadan kaldıran bir işletmenin temel çerçevesini ortaya çıkarmakta ve bir şirketin ticari kökenlerini gözden geçirmemizi sağlamaktadır. BCP geliştirme çalışmalarına sadece afetlerle ilgili önlemler değil aynı zamanda yönetimin yeniden yapılanması açısından bakmak acil durumlarda iş sürekliliğini artırabilir. Ayrıca, karmaşıklığın ve yönetim faaliyetlerinin kendiliğinden düzene sokulmasını sağlayabilir. Bununla birlikte, iş sürekliliği en baştan bir yönetim geliştirme faaliyeti olarak görülerek bir avantaja dönüştürülebilir.

Birçok kuruluşun destekleyici BT hizmetleri üzerindeki stratejik bağımlılığı göz önüne alındığında, bu hizmetlerin kullanılabilirliği ve işlevselliği bugün iş dünyası için hayati önem taşıyor. Bu nedenle işletmeler, hizmetlerin büyük ölçüde bozulduğu ve belki de uzun bir süre kullanılamadığı durumlara hazırlanmalıdır. Modern BT servis sürekliliği yönetimi önlemeye önem vermektedir. BT, işle koordinasyon halinde, sistem hatalarının olasılığını ve etkisini azaltmak için önlemler alır. Acil durumda bunlar, kararlaştırılan süre içinde gerekli BT altyapısını yeniden kurmaya ve hizmetleri bu koşullar altında sürdürmeye yardımcı olur.

BCP üst yönetim tarafından yönetilecek bir süreçtir. Bu önemlidir çünkü bir organizasyon öncelikle iş sürekliliği için planlama hedeflerini tanımlamalıdır. BCP denetimi de BT yönetişim sürecinin temel bir unsurudur ve paydaşlar, iş ortakları ve düzenleyici makamlar için BT'nin bağımsız bir değerlendirmesini temsil eder.

BT hizmet sürekliliği yönetimi, bir felaket haline gelmesi açısından iş tarafından yeterince önemli görülen acil durumlara odaklanmalıdır. Felaket olarak nitelendirilen şeyin kararı, iş dünyasında işletmeden işletmeye değişir. Satış kaybı veya tazminat talepleri gibi bir ticari hizmet başarısızlığının sonuçları, iş durgunluğuna bağlı olarak, bir ticari etki analizi kapsamında işle birlikte belirlenmelidir. Potansiyel tehditler, bilinen zayıflıklar ve analiz edilen risk temelinde tespit edilir. BT hizmet sürekliliği, öncelikle BT varlıklarını ve bu iş süreçlerini destekleyen yapılandırmaları kapsamalıdır. Bir felaket durumunda BT hizmet sürekliliği öngörülen tedbir ve bekleme çözümlerinin, üzerinde anlaşmaya varılan iş sürekliliği stratejisine uygun olarak, önleyici amaçlarla tanımlanmasını sağlamalıdır.

BT hizmetlerinin gelişiyle, işletmelerin bu hizmetler üzerindeki bağımlılığı önemli derecede artmıştır. BT hizmetleri, işletmelerin verimliliğini artırmalarına ve organizasyonel rekabet gücünü artırmalarına yardımcı olur. İşletmelerin sayısallaştırılması nedeniyle, BT herhangi bir organizasyon için vazgeçilmez bir rol oynamaktadır. Finansal kurumlar (bankalar), gün boyunca yapılan işlemler için BT servislerine büyük önem veren önde gelen servis endüstrisinden biridir. Bu nedenle, öngörülemeyen durumlar için BT sürekliliğinin önemi kritik öneme sahip bir nokta haline gelmiştir. BCM'nin bir parçası olan BCP) ve DRP, kritik iş süreçleri ve BT sistemleri için önceden tanımlanmış kurtarma süresi çerçevesinde hükümler sağlamak üzere tasarlanmalıdır. Bankaların BT sistemleri ve hizmetleri için BCP'nin tasarlanması ve uygulanması, sadece bir uygulama değil, devam eden bir süreç olmalıdır. Bankalarda BT iş sürekliliği planlarının uygulanması için çeşitli standartlar, çerçeveler ve yönergeler tasarlanmalı ve önemsenmelidir. Standartlar belirli teknolojilerin, araçların kullanımını belirtmektedir. Standartlar kalite uygulamalarını sağlamaya yardımcı olur. Standartlar, bankalar genelinde tekdüzeliğin korunmasına yardımcı olur. İyi yönetişim, belirli prosedürlere, kontrollere veya standartlara uyum seviyesini kapsamalıdır.

BCP özellikle felaketlerden kaynaklanan aksaklıkları ve ekonomik kayıpları en aza indirgemek için bankalara kurumsal ve şube düzeyinde fayda sağlıyor. Uygun çerçevelerin,

standartların ve kılavuzların seçimi, BCP'nin temel bileşenlerini planlama ve uygulama aşamasında üst yönetimin sorumluluğunda olmalıdır.

Süreklilik ve onu destekleyen sistemler söz konusu olduğunda işletmelerin esnek olduklarından emin olmaları gerekiyor. Bu durum, olumsuz ortamlarda çalışmaya devam edecek katılaşmış sistemlerin uygulanması anlamına geliyor. Böylece felaket oluştuğunda hizmetler hala mevcut olabiliyor. Bunun ötesinde, bir konumdan diğerine hızlı ve kolay bir şekilde geçirilebilen sistemlerin uygulanması iyi bir fikirdir. Bunun iyi bir örneği, bulut depolamayı ve yedeklemeyi, diğer sistemlere asgari karışıklık ile kurtarmayı mümkün kılmaktır. Sistemlerinizin devamlılığını ve süreklilik planlarını arttıran teknoloji uygulamaya değerdir.

Bir felaket sırasında ve sonrasında işletmelerin verilerine erişebilmesi hayati önem taşır. Verileriniz verimli bir şekilde korunmazsa veya yedeklendiğinde kolayca erişilebilir durumdaysa, iş etkinliğinde bir azalma ve tamamen iyileşme sürecinde gecikme görebilirsiniz. Mevcut sistemleriniz üzerinde veri koruması ve kullanılabilirliği artıran teknoloji veya sistemler, en çok ihtiyaç duyduğunuzda kullanılabilen verilerin avantajlarından yararlanabilmeniz için güncelleme yapmaya değerdir.

Bir felaket sırasında ve sonrasında iletişim, işiniz hayatta kalması ve tam operasyonları geri kazanmanız durumunda hayati önem taşımaktadır. Bir işletme felaketle karşı karşıya kaldığında iletişim ağlarının mevcut ve güçlü olması gerekir. Böylece, iletişiminizin kolaylığını ve etkinliğini artıracak sistemleri bulabilirsiniz ve bunun için yükseltme yapmaya değer olabilir.

Geçmişte bir süreklilik planı geliştiren işletmeler, bunun zaman alan bir görev olabileceğini bilir. Esaslı olmakla birlikte, pek çok işletme sahibi bunu taahhüt etmek için gerekli zamana sahip değildir. Bu nokta, sistemlerin ve teknolojinin yardımcı olabileceği yerdir. Planların denetlenmesini ve geliştirilmesini kolaylaştıran bir sistem, bir güncellemeye dahil olmaya değer olabilir.

Daha dar marjlarda faaliyet gösteren işletmelerde birçok işletme sahibi, sistemlerin maliyetleri düşük tutmasını veya en azından maliyetlerin artmamasını sağlamayı istemektedir. Aradığınız sistemlerin işletme maliyetlerini düşürdüğü kanıtlanmışsa, onları göz önünde bulundurmak iyi bir fikir olabilir. Ancak tasarruf için sadece teknolojiyi

bütünleştirmemeniz önemlidir. Uygun fiyatlı çözümler hedeflemelisiniz, bu da faydaları veya daha fazlasını sunacaktır.

Verilerinizi yedeklemek, BT sistemlerinizdeki riskleri azaltmak için yapabileceğiniz temel şeylerden biridir. Verilerinizi her gün uzaktaki bir bölgeye yedeklemelisiniz, böylece bir sorun meydana geldiğinde bir günden fazla işinizi kaybetmezsiniz. Daha güvenli olmak için sisteminizi, farklı konumlarda bulunan iki sunucudan aynı anda saklar şekilde ayarlayabilirsiniz. Ana sunucunun bir sorunu varsa yedekleme sunucusu sorunsuz bir şekilde veri kaybına ve işiniz üzerinde çok az bir etkiye sahip olabilir. İşletmenizde, şifreler, internet kullanımı, yazılım indirilmesi, eklentilerin açılması, uzaktan erişim, veri saklama, verilerin gizliliği ve işyerinin dışındaki ekipmanın güvenliğini kapsayan bir BT güvenlik politikası olmalıdır. Çalışanların politikayı bildiğinden ve uyguladığından emin olmalısınız. Düzenli hatırlatmalar ve denetimler, uyumluluğu sağlamak için iyi bir yoldur. Ayrıca, güvenlik politikanızın ve uygulamanızın işletmeniz için geçerli tüm dijital güvenlik kanunlarını ve standartları karşıladığından emin olmalı ve politikanızı düzenli olarak incelemeli ve güncellemelisiniz. İşletmenizi olabildiğince çabuk işletmek için çeşitli senaryolarda ne yapacağınızı belgelemeniz gerekiyor. İşlemlerinizi nereye taşıyacağınız, veri yedeklerinin nerede olduğu ve yeni BT sisteminizi kimin kuracağı gibi konuları not edin. Hırsızlık, yangın veya su hasarına bağlı olarak fiziksel kayıp veya ekipmana zarar verme riskinizi en aza indirgemek için gerekli önlemler düşünülmelidir. Ayrıca, yeterli işletme sigortanız olduğundan emin olmanız gerekir.

Günümüz BT dünyasında BT hizmetleri olmaksızın bankacılık yapmak mümkün değildir. Bankanın iş sürekliliği taahhüdü ve BT tabanlı hizmetlerin felaketten kurtarılması, en uygun bilgi güvenliği ve iş sürekliliği politikalarına, standartlara, çerçevelere, iyi uygulamalara ve yönergelere bağlıdır. BT yönetişim çerçeveleri, bankalarda iş sürekliliği ve felaket kurtarma için politikalar ve standartlar tasarlamak ve uygulamak için mantıklı bir yapı sağlamalıdır. Bu araştırma, BT tabanlı sektörler için iş devamlılığı ve felaket kurtarma adına mevcut standartlara, politikalara ve çerçevelere odaklanmıştır. Daha ileri zamanlarda yapılacak çalışmalar, BT tabanlı organizasyonlar için iş sürekliliğinin ve felaket kurtarma uygulamalarının başarıyla uygulanması sorunlarını ve bu sorunların çözümünü vurgulayabilir.

KAYNAKLAR

Adkins, G., Thornton, T. and Blake, K. (2009). A content analysis investigating relationships between communication and business continuity planning. The Journal of Business Communication.

Alabdulwahab, M. (2016). Disaster Recovery and Business Continuity. International Journal of Scientific and Engineering Research.

Alesi, P. (2008). Building enterprise-wide resilience by integrating business continuity capability into day-to-day business culture and technology. *Journal of Business Continuity and Emergency Planning*.

Alexander, D. (2005). Towards the development of a standard in emergency planning. Disaster Prevention and Management:An International Journal.

Alshammari, M. and Alwan, A. (2016). IT Disaster Recovery and Business Continuity Based On VMware SRM Solution for Kuwait Oil Company (KOC). https://www.researchgate.net.

Arif, M. (2007). Recovery Strategies. Computer Weekly.

Aronson, E. (1999). *The Social Animal.*

Arveson, P. (1998). The Deming Cycle. Obtenido de Balanced Scorecard Institute.

Austin, D. (2011). Will your communications plan meet the new 2012 standart? Everbridge.

Australian National Audit Office. (2009). Business continuity resilience in public sector entities.

Barnes, J. (2001). *A Guide to Business Continuity Planning.* John Wiley and Sons.

Basel Committee on Banking Supervision. (2006). High-level principles for business.

Baskerville, R., Stage, J. and DeGross, J. (2000). Organizational and Social Perspectives on Information Technology: IFIP TC8 WG8. Springer.

Bielski, R. (2008). Extreme Risks, American Bankers Association. ABA Banking Journal.

Birkmann, J. (2005). Danger need not spell disaster-But how vulnerable are we? Tokyo: United Nations University.

Boshoff, C. (1996). An experimental study of service recovery options. International Journal of Service Industry Management.

Botha, J. and Solms, R. (2004). A cyclic approach to business continuity planning. Emerald Group Publishing Limited.

Bradbury, C. (2008). Disaster! Creating and testing an effective recovery plan. *British Journal of Administrative Management*.

Brazeau, P. (2008). *Holistic Protection.*

British Standards Institution. (2006). *BS 25999-1:2006-Business Continuity Management:Code of Practice.* British Standards Institution.

British Standards Institution. (2008). BS 25777:2008-Information and Communications Technology Continuity Management:Code of Practice. British Standards Institution.

British Standarts Institution. (2005). BSI-Standard 100-2:2005, IT-Grundschutz Methodology.

Brouggy, P. (2009). Resilient maturity model analysis.

Brown, S. W. & Swartz, T. A. (1989). A gap analysis of professional service quality. The Journal of Marketing.

Bryson, K.M., Millar, H., Joseph, A. and Mobolurin, A. (2001). Using formal MS/OR modeling to support disaster recovery planning. *European Journal of Operational Research.*

Burke, S., Wilson, K. and Salas, E. (2005). The use of a team-based strategy for organizational transformation: guidance for moving toward a high reliability organization. Theoretical Issues in Ergonomics Science.

Business Continuity Institute. (2013). Good Practices Guidelines.

Cerullo, V. and Cerullo, M. (2004). Business Continuity Planning:A Comprehensive Approach.

Chad, B. (2003). The Disaster Recovery Plan-GSEC Practical Assignment version 1.4b. SANS Institute.

Charters, I. (2007). Risk evaluation and control:practical guidelines for risk assessment.

Chen, S.S. (2007). Digital Preservation: Organizational Commitment, Archival Stability, and Technological Continuity. Journal of organizational computing and electronic commerce.

Coles, E. and Buckle, P. (2004). Developing community resilience as a foundation for effective disaster recovery. Australian Journal of Emergency Management.

Collicutt, J. (2009). Community resilience:The future of business continuity. Journal of Business Continuity and Emergency Planning.

Copenhaver, J. and Lindstedt, D. (2010). From cacophony to symphony: how to focus the discipline of business continuity. *Journal of Business Continuity and Emergency Planning.*

Coutu, D. (2002). How Resilience Works. Harvard Business Review.

Crichton, M., Ramsay, C. and Kelly, T. (2009). Enhancing organizational resilience through emergency planning:learnings from cross-sectoral lessons. Journal of Contingencies and Crisis Management.

Cummings, J. (2003). *Nurturing a culture of continuity.* Network World October.

Daft, R. (2001). Essentials of organization theory and design. South Western Educational Publishing.

Dattero, R., Galup, S. D., Quan, J. J. and Conger, S. (2009). An overview of IT service management. Communications of the ACM - Security in the Browser.

De Waal, A. (2006). Towards a comparative political ethnography of disaster prevention. *Journal of International Affairs*.

De Witte, K. and Van Muijen, J. (1999). Organizational culture:Critical questions for researchers and practitioners. *European Journal of Work and Organizational Psychology*.

Deal, T. and Kennedy, A. (1982). Corporate cultures:The rites and rituals of organizational life.

Dey, M. (2011). Business Continuity Planning methodology-Essential for every business.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. Journal of Information Security.

Dye, K. and Langsett, M. (2008). A roadmap to measure and achieve enterprise operational resiliency. Journal of Business Continuity & Emergency Planning.

Elliott, D. (2009). The failure of organizational learning from crisis–a matter of life and death? Journal of Contingencies and Crisis Management.

Elliott, D., Swartz, E. and Herbane, B. (2010). *Business Continuity Management:A crisis management approach, (2. baskı).* Routledge.

Elwood, A. (2009). Using the disaster crunch/release model in building organisational resilience. Journal of Business Continuity and Emergency Planning.

Ernest Jones, T. (2005). Business continuity strategy–the life line. Network Security.

European Union Agency for Network and Information. (2008). Business and IT Continuity:Overview and Implementation Principles. ENISA.

Fallara, P. (2003). Disaster recovery planning. IEEE potentials.

FDIC. (2002). *Rules and Regulations : Notification of Performance of Bank Services*.

Federal Financial Institutions Examination Council. (2008). *Business Continuity Planning.* FFIEC.

Financial Times. (2000). Glitch halts share trading in London. Financial Times.

Fink, S. (1986). Crisis Management: Planning for the Inevitable. AMACOM.

Forbes, G. & Buchanan, S. (2006). A framework for business continuity management. *International journal of information management*.

Fritzon, A., Ljungkvist, K., Boin, A. and Rhinard, M. (2007). Protecting Europe's Critical Infrastructures: Problems and Prospects. Journal of Contingencies and Crisis Management.

Gallagher, M. (2003). Business Continuity Management-How to protect your company from danger. Pearson Education Limited.

Garrett, D. (2012). *The evolution of business continuity management in large Irish enterprises between 2004 and 2009*.

Gehrmann, M. (2012). Combining ITIL, COBIT and ISO/IEC 27002 for structuring comprehensive information technology for management in organizations. Navus-Revista de Gestão e Tecnologia.

Gibson, C. and Love, G. (2006). HB 292—2006:A practitioners guide to business continuity management . Standards Australia.

Ginn, R. (1992). *Continuity planning:Preventing, surviving and recovering from disaster.* Elsevier.

Gosling, M. and Hiles, A. (2008). Business Continuity Statistics:Where Myth Meets Fact. http://www.continuitycentral.com.

Haag, S., Cummings, M. and Mccubbrey, D. (2005). Management Information Systems for the Information Age. McGraw-Hill.

Hanwacker, L. (2010). Business Continuity Planning Software Criteria:The Next Level In The Selection Process.

Hayes, B. and Kotwica, K. (2013). *Business Continuity:Playbook (Risk Management Portfoliio) (2nd Edition).* Elsevier.

Herbane, B. (2010). *The evolution of business continuity management:A historical review of the practices and drivers.*

Hiles, A. (2010). *The definitive handbook of business continuity management.* John Wiley and Sons.

Holman, E. and Houser, K. (2011). ITSM Overview:ITIL's IT Disaster Recovery and Business Continuity Management. Share in Orlando.

Horne, J. (1997). The coming age of organizational resilience. Business forum.

Howe, J. (2007). *Project initiation and management.* John Wiley and Sons.

Hunton, J., Wright, A. and Wright, S. (2004). Are Financial Auditors Overconfident in Their Ability to Assess Risks Associated with Enterprise Resource Planning Systems? Journal of Information Systems.

International Organization for Standardization. (2009). ISO Guide 73:2009. International Organization for Standardization.

International Organization for Standardization. (2012). ISO 22301:2012.

International Organization for Standardization. (2018). ISO/IEC 27000:2018-Information technology-Security techniques-Information security management systems-Overview and vocabulary. International Organization for Standardization.

International Organization for Standardization, and International Electrotechnical Commission. (2009). ISO/IEC FDIS 31010 International Standard:Risk Management–Risk.

ISACA. (2003). IS Audit and Assurance Guideline 2003 Professional Independence. ISACA.

ISACA. (2012). COBIT 5:Kurumsal BT Yönetişimi ve Yönetimi için Bir İş Çerçevesi. ISACA.

ISO/IEC 27031:2011(E). (2011). *Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity*.

IT Governance CEN 667. (2012). Introduction to IT Governance.

İnternet: OpenCampus, IT service continuity management. URL; http://www.webcitation.org/query?url=https%3A%2F%2Fwww.greycampus.com%2Fopencampus%2Fitil-foundation%2Fit-service-continuity-management-itscm-goals-and-objectives&date=2018-03-14 Son erişim tarihi: 14.03.2018

İnternet: Business continuity institute, What is BC?. URL; http://www.webcitation.org/query?url=http%3A%2F%2Fwww.thebcicertificate.org%2Findex.php%2Fresources%2Fwhat-is-business-continuity&date=2018-03-14 Son erişim tarihi: 14.03.2018

İnternet: U.S. Securities and Exchange Commission, Interagency paper on sound practices to strengthen the resilience of the U.S. financial system. URL; http://www.webcitation.org/query?url=https%3A%2F%2Fwww.sec.gov%2Fnews%2Fstudies%2F34-47638.htm&date=2018-03-14 Son erişim tarihi: 14.03.2018

İnternet: SearchDataCenter, Building a disaster recovery architecture with cloud and colocation. URL; http://www.webcitation.org/query?url=http%3A%2F%2Fsearchdatacenter.techtarget.com%2Fguide%2FBuilding-a-disaster-recovery-architecture-with-cloud-and-colocation&date=2018-03-14 Son erişim tarihi: 14.03.2018

İnternet: ThinkIT by Singlehop, What is business continuity?. URL; http://www.webcitation.org/query?url=https%3A%2F%2Fwww.singlehop.com%2Fblog%2Fbusiness-continuity%2F&date=2018-03-14 Son erişim tarihi: 14.03.2018

Järveläinen, J. (2013). IT incidents and business impacts: Validating a framework for continuity management in information systems. International journal of information management.

Johar, G., Birk, M. and Einwiller, S. (2010). How to save your brand in the face of crisis. MIT Sloan Management Review .

Johnson, G., Scholes, K. and Whittington, R. (2002). *Exploring Corporate Strategy.* Pearson Education Limited.

Jones, V. (2011). How to avoid disaster:RIM's crucial role in business continuity planning. www.arma.org.

Jordan, E. (2005). IT service continuity assessment. Macquarie Graduate School of Management.

Jordan, E. and Silcock, L. (2005). Beating IT risks. John Wiley & Sons.

Kavanagh, D. (2004). How to Prioritize the BCP Effort with Recovery Timeframe Objectives.

Kello, J. (2009). How to assess your culture. *Industrial Safety and Hygiene News.*

Kjærgaard, A. (2009). Organizational Identity and Strategy. *International Studies of Management and Organization*.

Koch, R. (2001). Best practices in business continuity. *Disaster Recovery Journal*.

Kotnour, T. (2009). Putting Culture to Work in Our Organizations. *Engineering Management Journal*.

Krutz, R. and Vines, R. D. (2010). *Cloud security: A comprehensive guide to secure cloud computing.* Wiley Publishing.

La Porte, T. (1996). High reliability organizations:Unlikely, demanding and at risk. Journal of contingencies and crisis management.

La Porte, T. and Consolini, P. (1991). Working in practice but not in theory:theoretical challenges of high-reliability organizations. Journal of Public Administration Research and Theory:J-PART.

Lagadec, P. (2009). A new cosmology of risks and crises:Time for a radical shift in paradigm and practice. Review of Policy Research.

Lainhart IV, J. W. (2000). COBIT:A methodology for managing and controlling information and information technology risks and vulnerabilities. Journal of Information Systems.

Laye, J. (2002). Avoiding Disaster:How to Keep Your Business Going When Catastrophe Strikes. John Wiley and Sons.

Lebihan, R. (2004). SCO rides out the Mydoom storm. Australian Financial Review.

Lengnick Hall, C. and Beck, T. (2009). Resilience capacity and strategic agility:Prerequisites for thriving in a dynamic environment. UTSA, College of Business.

Li, G., Yang, H., Sun, L. and Sohal, A. S. (2009). The impact of IT implementation on supply chain integration and performance. Elsevier.

Lindell, M., Prater, C. and Perry, R. (2007). Introduction to Emergency Management. John Wiley & Sons.

Lindstedt, D. (2007). *Grounding the discipline of business continuity planning:What needs to be done to take it forward?* Journal of Business Continuity and Emergency Planning.

Luthans, F. (2002). The need for and meaning of positive organizational behavior. *Journal of organizational behavior*.

M.E.M. Project Team. (2011). A Framework for Major Emergency Management. National Steering Group.

Marlin, S. (2004). Disaster recovery spending on the rise. Information Week.

Marsh Danışmanlık. (2010). İş Sürekliliği Eğitim Notları.

McNaughton, B., Ray, P. and Lewis, L. (2010). Designing an evaluation framework for IT service management. Information and Management.

Mellish, S. (2008). The Business Continuity Institute. http://www.thebci.org.

Miller, J., Craighead, C. and Karwan, K. R. (2000). Service recovery:a framework and empirical investigation. Journal of operations Management.

Mitroff, I. (2001). *Managing Crises Before They Happen:What Every Executive and Manager Needs to Know About Crisis Management.* AMACO.

Motahari Nezhad, H. R. and Bartolini, C. (2011). Next best step and expert recommendation for collaborative processes in it service management. International Conference on Business Process Management.

Myers, K. (2006). *Business Continuity Strategies: Protecting Against Unplanned Disasters.* John Wiley and Sons.

Nastase, P., Nastase, F. and Ionescu, C. (2009). Challanges generated by the implementation of the IT standards COBIT 4.1, ITIL V3 and ISO/IEC 27002 in enterprises. Economic Computation and Economic Cybernetics Studies & Research.

National Institute of Standards and Technology . (2010). Contingency Planning Guide for Federal Information Systems. NIST Special Publication.

Nollau, B. (2009). Disaster recovery and business continuity. Journal of GXP Compliance.

O'Hehir, M. (2007). What is a business continuity planning (BCP) strategy.

Office of Critical Infrastructure Protection. (2003). A guide to business continuity planning. Government of Canada.

Oldfield, R. (2008). So what is resilience and what benefits does it offer?

Oriesek, D. and Schwarz, J. (2008). *Business Wargaming:Securing Corporate Value.* Ashgate Publishing Company.

Orr, J. and Horne, J. (1998). Assessing Behaviours That Create Resilient Organisations. Employment Relations Today.

Panko, R. (1987). Directions and issues in end user computing. *INFOR.*

Park, J.O., Kim, S.G. and Choi, B.H. (2008). The Study on the Maturity Measurement Method of Security Management for ITSM. IEEE.

Peppard, J. and Ward, J. (1999). "'Mind the Gap': diagnosing the relationship between the IT organisation and the rest of the business. The Journal of Strategic Information Systems.

Peppard, J., and Ward, J. (2004). Beyond strategic information systems: towards an IS capability. The Journal of Strategic Information Systems.

Perman, G. (2009). Why Succession Management Matters. CIO Insight.

Pollard, C. and Cater Steel, A. (2009). Justifications, strategies, and critical success factors in successful ITIL implementations in US and Australian companies: an exploratory study. Information systems management .

Porter, M. and Millar, V. (1985). How information gives you competitive advantage. Harvard Business Review.

Preimesberger, C. (2009). Unfettered data growth challenges business continuity technology. eWeek.

Quarantelli, E. L. (1999). he disaster recovery process:What we know and do not know from research.

Quarantelli, E. and Dynes, R. (1977). Response to social crisis and disaster. Annual review of sociology.

Ranjan, P., Kumar, P. and Abhishek, K. (2012). Business continuity planning in Indian perspective. Journal of Advances in Computational Research: An International Journal.

Rhinard, M. (2009). European cooperation on future crises: toward a public good? Review of policy research.

Riolli, L. and Savicki, V. (2003). Information system organizational resilience. Omega.

Rittinghouse, J., Ransome, J. and CISSP CISM. (2011). *Business continuity and disaster recovery for infosec managers.* Elsevier.

Roberts, K. (1990). Some characteristics of one type of high reliability organization. Organization Science.

Royds, J. (2010). Business Continuity Management, An Introductory Guide. ICAEW.

Sandesh, S., McHugh, J. and Jones, F. (2008). A dashboard for measuring capability when designing, implementing and validating business continuity and disaster recovery projects. *Journal of Business Continuity and Emergency Planning*.

Schanze, J., Zeman, E. and Marsalek, J. (2007). Flood risk management: hazards, vulnerability and mitigation measures. Springer Science and Business Media.

Schwab, J., Topping, K., Eadie, C., Deyle, R. and Smith, R. (2003). Planning for the Post-Disaster Recovery and Reconstruction. American Planning Association.

Seow, K. (2009). Gaining senior executive commitment to business continuity:Motivators and reinforcers. *Journal of Business Continuity and Emergency Planning*.

Sheffi, Y. (2007). *The Resilient Enterprise.* The MIT Press.

Sheffi, Y. and Rice, J. (2005). Building the Resilient Enterprise. MIT Sloan Management Review.

Sheth, S., McHugh, J. and Jones, F. (2008). A dashboard for measuring capability when designing, implementing and validating business continuity and disaster recovery projects. Journal of Business Continuity and Emergency Planning.

Simonsson, M., Johnson, P. and Ekstedt, M. (2010). The effect of IT governance maturity on IT governance performance. Information systems management.

Sinha, D. (2011). Business Continuity:The Lifecycle.

Smith, D. (2005). Business (not) as usual:crisis management, service recovery and the vulnerability of organisations. *Journal of Services Marketing*.

Smith, M. and Shields, P.A. (2007). Strategies for IT and communications.

Snedaker, S. (2007). *Business Continuity and Disaster Recovery for IT Professionals.* Syngress.

Somers, S. and James, S. (2009). Assessing and managing environmental risk:Connecting local government management with emergency management. Public Administration Review.

Spigener, J. (2009). Can you recognize "exposure creep"? *Industrial Safety and Hygiene News*.

Spremić, M. (2009). IT governance mechanisms in managing IT business value. WSEAS Transactions on Information Science and Applications.

Spremic, M., Bajgoric, N. and Turujla, L. (2012). Implementation of IT governance standarts and business continuity management in transition economies:The case of banking sector in Crotia and Bosnia-Herzegovina. Ekonomska istraživanja–Economic Research.

Swartz, E., Herbane, B. and Elliott, D. (1995). *Out of sight, out of mind:the limitations.*

Syed, A. and Syed, A. (2004). *Business Continuity Planning Methodology.* Sentryx.

Taleb, N. N. (2007). *The black swan:The impact of the highly improbable (2. baskı).* Random house.

Tencati, A., Perrini, F. and Russo, A. (2007). CSR strategies of SMEs and large firms. Evidence from Italy. Journal of business ethics.

The EU Cyber Security Agency. (2017). Guidelines for TSPs based on standarts.

Tjoa, S., Jakoubi, S. and Quirchmayr, G. (2008). Enhancing business impact analysis and risk assessment applying a risk-aware business process modeling and simulation methodology. ARES 08. Third International Conference .

Turner, B. (1976). The organizational and interorganizational development of disasters. Administrative Science Quarterly.

University of Wollongong. (2005). Business Continuity Management Policy, Version 1.1.

Utz, E. (2008). Modelling and Measurement Methods of Operational Risk in Banking. Herbert Utz Verlag.

Vaid, R. (2008). How are operational risk and business continuity coming together as a common risk management spectrum? *Journal of Business Continuity and Emergency Planning*.

Van Grembergen, W., De Haes, S. and Moons, J. (2005). Linking business goals to IT goals and COBIT processes. Information Systems Control Journal.

Vizard, M. (2008). Why there's no business continuity.

Vogus, T. and Sutcliffe, K. (2007). Organizational resilience:towards a theory and research agenda. ISIC. IEEE International Conference.

Von Rossing, R. (2007). *BC Audit.* John Wiley and Sons Ltd.

Wack, P. (1985). Scenarios:Uncharted Waters Ahead. *Harvard Business Review*, 73-89.

Whittet, L. (2008). Operational risk management and business continuity. http://www.continuitycentral.com.

Wiboonratr, M. and Kosavisutte, K. (2009). Optimal strategic decision for disaster recovery. International Journal of Management Science and Engineering Management.

Wilder, D. (2008). The New Business Continuity Model.

Willcocks, L., Feeny, D. and Olson, N. (2006). IT Governance and Management Framework. European Management Journal.

Winniford, M., Conger, S. and Erickson Harris, L. (2009). Confusion in the ranks:IT service management practice and terminology. Information Systems Management.

Wold, G. (2006). Disaster recovery planning process. Disaster Recovery Journal.

Wood, T., Cecchet, E., Ramakrishnan, K. K., Shenoy, P., Van Der Merwe, J. and Venkataramani, A. (2010). Disaster Recovery as a Cloud Service:Economic Benefits and Deployment Challenges.

Woods, P. (2013). Business Continuity Management:The Concept and Context of BCM. Bucks New University.

Youngblood, M. (2000). *Winning cultures for the new economy.* Strategy and Leadership.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı	: DUMRUL, Osman
Doğum Yılı ve Yeri	: 1987 / Ceyhan
Telefon Numarası	: 0 (312) 508 72 47
Mail	: odumrul@ilbank.gov.tr

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Yüksek Lisans	Ankara Sosyal Bilimler Üniversitesi-İşletme(İngilizce)	Devam ediyor
Lisans	Türkiye Odalar ve Borsalar Birliği Ekonomi ve Teknoloji Üniversitesi-İşletme (Tam Burslu)	2014
Lise	Mersin75. Yıl AÖL	2005

İş Deneyimi

Yıl	Yer	Görev
2014 - Halen	İller Bankası	Uzman Yardımcısı

Yabancı Dil

İngilizce, Almanca

Yayınlar

-

Hobiler

Satranç, masa tenisi


İLBANK
TÜRKİYE'NİN YAPICI GÜCÜ