TÜRKİYE BİLİŞİM DERNEĞİ

Kamu Bilgi İşlem Merkezleri Yöneticileri Birliği

Kamu Bilişim Platformu XIV

İŞ SÜREKLİLİĞİ YÖNETİMİ

ÇALIŞMA GRUBU RAPORU

2. ÇALIŞMA GRUBU

Nihai Rapor

http://www.tbd.org.tr

Nisan 2012

TBD Kamu-BİB

Kamu Bilişim Platformu XIV

İŞ SÜREKLİLİĞİ YÖNETİMİ ÇALIŞMA GRUBU

Bu rapor, TBD Kamu Bilgi İşlem Merkezleri Yöneticileri Birliği (TBD Kamu-BİB)'nin ***ondördüncü dönem*** çalışmaları kapsamında, **2. Çalışma Grubu** tarafından hazırlanmıştır. İş Sürekliliği konusundaki değerlendirmeleri önerileri ve kavramları içermektedir.

Hedef Kitle

Çalışmanın içeriği, rapor hazırlayan veya katkıda bulunan tüm üyelere yöneliktir.

Belge No : TBD/Kamu-BIB/2012-ÇG2

Tarihi : Nisan 2012

Durumu : Nihai Rapor

Yayını Hazırlayanlar

Başkan

Erman TAŞKIN EDUCORE

Başkan Yardımcısı

Suna SARIOĞLU Bilim, Sanayi ve Teknoloji Bakanlığı

Raporlörler

Arzu ALTUN T.C. Adalet Bakanlığı BİDB

Aslı ARTUN Teknopark Proje Yazılım ve Donanım

Kamu-BİB YK Temsilcileri

Adnan YILMAZ Yargıtay

Ragıp GÜLPINAR TOKİ

Grup Üyeleri

A.Erhan ALTUNOK	MEB
Abidin TOPAÇOĞLU	Adalet Bakanlığı
Aynur AYDIN	Eti Maden
Celal YILDIRIM	Kale Yazılım
Cemil ULU	TCMB
Cumhur ERCAN	TBD
Ebru ALTUNOK	MEB
Erol HAMURCU	Adalet Bakanlığı
Filiz ÇAKIR	Bilim Sanayi ve Teknoloji Bakanlığı
Hülya YARDIMOĞLU	Gümrük ve Ticaret Bakanlığı
Doç. Dr. M. Kemal ÖKTEM	Hacettepe Üniversitesi
Mesut KÜÇÜKİBA	Adalet Bakanlığı
Mete ÇAĞAN	PTT
Nejdet KARAKELLE	Başbakanlık
Refia KARACA	İDE Danışmanlık
Selcen TÜRKBEN	TBD
Selçuk AYDIN	Kale Yazılım
Suna SARIOĞLU	Bilim Sanayi ve Teknoloji Bakanlığı
Yusuf YAVUZ	Hazine Müsteşarlığı

TEŞEKKÜR

Bu kılavuzu hazırlamada yorumlarıyla ve önerileriyle yardımlarını esirgemeyen Ondördüncü Dönem TBD Kamu-BIB Yönetim Kurulu üyelerine teşekkürlerimizi sunarız.

İÇİNDEKİLER

TANIMLAR VE KISALTMALAR

Aktivite: Organizasyon tarafından (ya da adına) gerçekleştirilen, bir ya da daha çok sayıda ürün ya da hizmetin üreten ya da desteleyen proses ya da proses dizisi.

Denetim: Faaliyetlerin ve ilgili sonuçların planlanan düzenlemeleri karşılayıp karşılamadığını ve bu düzenlemelerin etkin olarak uygulanıp uygulanmadığı ve organizasyonun politika ve hedeflerini başarmaya uygun olup olmadığının belirlendiği sistematik değerlendirmeler.

İş sürekliliği: Önceden belirlenmiş kabul edilebilir seviyelerde iş operasyonlarının devam edebilmesine yönelik olarak, olay ve iş kesintilerine tepki gösterebilme ve planlama için organizasyonun stratejik ve taktiksel becerisi.

İş sürekliliği yönetimi: Organizasyona yönelik potansiyel tehditler ve bunların iş operasyonlarına etkilerini tanımlayan, organizasyonun ortaklarını, saygınlığını, markasını ve değer yaratan faaliyetlerini koruyan etkin tepki kabiliyeti ile organizasyon esnekliğinin sağlanması için bir çerçeve sağlayan bütün yönetim prosesidir.

İş süreklilik yönetimi döngüsü: İş süreklilik yönetim programının tüm öğelerini ve aşamalarını kapsayan iş süreklilik faaliyet dizisi.

İş süreklilik yönetim personeli: BCMS' de sorumlulukları tanımlanan, BCM politikası ve uygulanmasından sorumlu, BCMS' yi uygulayan ve sürekliliğini sağlayan, iş sürekliliğini ve olay yönetimini geliştiren ya da uygulayan, bir olay sürecinde yetki sahibi olan kişi ya da kişiler.

İş süreklilik yönetim programı: Üst yönetim tarafından desteklenen ve potansiyel kayıpların etkisinin tanımlanmasında, kurtarma strateji ve planlarının hazır bulunmasında gerekli adımların atılmasını ve eğitim, deneme, süreklilik ve gözden geçirme yoluyla ürün ve servislerin sürekliliğinin sağlanmasında işletilen devam eden yönetim ve idari proses.

İş süreklilik yönetim tepkisi: Kritik faaliyetlerin ve olay yönetiminin sürekliliğini sağlayan uygun planlama ve düzenlemelerin uygulanması ve geliştirilmesi ile ilgili BCM öğeleri.

İş süreklilik yönetim sistemi (BCMS: Business continuity management system): Genel yönetim sisteminin, iş sürekliliği ile ilgili bölümünü yayınlayan, uygulayan, işleten, izleyen, gözden geçiren, sürekliliğini sağlayan ve iyileştiren bölümü.

İş süreklilik planı (BCP: Business Continuity Plan): Organizasyonun önceden belirlenmiş kabul edilebilir bir seviyede kritik faaliyetlerini sürdürebilmesini sağlamak için kullanıma hazır bulundurulan geliştirilmiş, uygunluğu sağlanmış ve sürekliliği sağlanmış bilgi ve prosedürlerin dokümantasyonu.

İş süreklilik stratejisi: Bir afet ya da diğer önemli olay ya da iş kesintileri durumunda devamlılığı ve kurtarmayı sağlayan organizasyon yaklaşımı.

İş etki analizi (BIA: Business Impact Analysis): İş fonksiyonlarının analizi ve iş kesintilerinin bunlar üzerinde yaratabileceği etki.

Sonuç: Organizasyonun hedeflerini etkileyecek olay çıktısı.

Maliyet-fayda analizi: Bir çözümü uygulamanın maliyetini ölçen ve bu çözümden elde edilen fayda ile karşılaştıran finansal teknik.

Kritik faaliyetler: Organizasyonun en önemli ve zaman-kısıtlı hedeflerine ulaşmasını sağlayan anahtar ürün ve servislerin gerçekleştirilmesi için yürütülmesi gereken faaliyetler.

Kesinti: Organizasyonun hedefleri ile ilgili ürün ya da servislerin gerçekleştirilmesinde beklenenden plansız ve negatif yönde sapmaya neden olan, beklenilen (örn, finansal kriz ya da fırtına) ya da beklenilmeyen (örn; deprem) olaylar.

Deneme (tatbikat): Uygulamaya koyulduğunda istenilen sonuçları vermesini sağlamak için iş süreklilik planlarının kısmen ya da bütün olarak prova edildiği faaliyetler.

Kazanım: Pozitif sonuç.

Etki: Bir çıktının hesaplanan sonucu.

Olay: Bir iş kesintisine, kaybına, acil duruma ya da krize neden olabilecek ya da sevk edebilecek durum.

Olay yönetim planı (IMP: Incident Management Plan): Tipik olarak anahtar personel, kaynaklar, servisler ve olay yönetim prosesinin uygulanması için gerekli faaliyetleri kapsayan, olay anında kullanıma hazır halde bulunan, açıkça tanımlanmış ve dokümante edilmiş eylem planı.

İç tetkik: Organizasyonun yönetiminin gözden geçirilmesi ya da diğer dahili amaçlar için ya da organizasyonun kendi uygunluk beyanına temel oluşturabilecek, organizasyonun kendisinin ya da adına bir tarafça düzenlenen tetkik.

Başvuru: Organizasyonun anahtar ürün ya da servislerinin sürekliliği için iş süreklilik planlarının uygulamaya koyulmasının gerekliliğinin beyan edildiği eylem.

Olabilirlik: Tanımlanmış, ölçülmüş ya da nesnel ya da öznel olarak tahmin edilmiş ya da genel tabirlerle (örn; az, hemen hemen hiç, çoğunlukla, genelde, kesinlikle), sıklıklarla (frekans) ya da matematiksel olasılık değerleriyle ifade edilmiş bir şeyin olma şansı.

Kayıp: Negatif sonuç.

Yönetim sistemi: Politika ve hedefler kuran ve bu hedefleri yakalayan sistem.

Kabul edilebilir maksimum kesinti periyodu: Ürün ve servis gerçekleştirmenin devam ettirilemezse organizasyonun finansal kapasitesinde geri dönüşü olmayan tehdit süreci.

Uygunsuzluk: Bir gerekliliğin yerine getirilmemesi.

Organizasyon: Sorumluluk, yetki ve ilişki düzenlemelerine sahip bir grup kişi ve olanaklar.

Proses: Girdileri çıktılara dönüştüren ilişkili ya da etkileşimli faaliyetler dizisi.

Ürün ve servisler: Organizasyon tarafından müşterilerine, alıcılarına ya da kar ortaklarına sağlanan fayda sağlayıcı çıktılar. Örn; fabrika ürünleri, araba sigortası, yasal uygunluk ve kamusal yardım.

MTPD (Maximum Tolerable Period of Disruption): Maksimum tahammül edilebilir kesinti süresi

RPO (Recovery Point Objective): Kurtarma nokta hedefi

BCM (Business Continuity Management) : Business Continuity Management, İş sürekliliği yönetimi

RTO (Recovery Time Objective), Kurtarma süre hedefi: Bir olay sonrasında ürün, servis ya da faaliyet gerçekleştirmenin kaldığı yerden devamı için ayarlanmış süre hedefi.

Esneklik: Organizasyonun bir olaydan etkilenmeye karşı direnme kabiliyeti.

Kaynaklar: Organizasyonun çalışması ve hedeflerine ulaşması için kullanması gereken tüm değer, kişi, bilgi, teknoloji (yerleşke ve ekipman dahil)

Risk: Gerçekleşebilecek bir durum ve bunun hedeflerin başarılması üzerindeki etkisi/etkileri.

Risk değerlendirme: Risklerin belirlenmesi, analizi ve değerlendirilmesi ile ilgili tüm proses.

Risk yönetimi: Risklere yönelik tanımlama, analiz, değerlendirme ve kontrol görevlerine yönelik olarak yönetim kültürü, politikası, prosedür ve uygulamaların yapılandırılmış gelişimi ve uygulanması.

Kar ortakları: Organizasyon başarılarına tasarruf hakkını veren kişiler.

Sistem: Birbiri ile ilişkili ya da sıralı öğelerden oluşan bir faaliyet seti.

Üst yönetim: Organizasyonu en üst seviyede yöneten ve kontrol eden kişi ya da grup.

Acil ve Beklenmedik Durum Planı: Faaliyetlerde ani ve planlanmamış bir kesintiye, is kaybına veya krize neden olması muhtemel bir durumda risklerin ve sorunların yönetilebilmesi amacıyla alınacak tedbirlerin ve gerçekleştirilecek öncelikli eylemlerin belirlendiği, iş sürekliliği planının bir parçası olan plan.

Felaket: Faaliyet veya sistemlerde uzun süreli kesintiye sebep olabilecek düzeyde insan, doğa veya diğer faktörlerden kaynaklanan olay.

İş Etki Analizi: İş süreçlerinin ve bir faaliyet kesintisinin is süreçleri üzerinde yaratabileceği etkilerin analiz süreci.

İş Sürekliliği Planı: İş sürekliliği yönetiminin bir parçası olan ve bir kesinti durumunda kurumun öncelikleriyle uyumlu olarak faaliyetlerin sürdürülmesine ve mevzuata uyum sağlanmasına yönelik politika, standart ve prosedürlerden oluşan yazılı plan veya planlar bütünü.

ŞEKİLLER

TABLOLAR

ÖNSÖZ

İş sürekliliğinin önemi yakın dönemde yaşanan felaketlerle giderek daha fazla hissedilmeye başlansa da kesintilerin kurum aktivitelerine olan etkisi hep gündemde olan bir konu olmuştur. Çeşitli nedenlerle kesintiye uğrayan bir kurumun aktiviteleri, kendisine bağlı çalışan diğer kurumları da etkilemeye başlamıştır. Giderek yakınsayan kurumlar birbirlerinin faaliyetlerine daha fazla bağlanmaya ve bu gelişmelere paralel olarak, kesinti tahammülü de giderek azalmaya başlamıştır. Hem vatandaş/müşteri bakış açısıyla hem de kurum/şirket bakış açısıyla artık aksayan/duraksayan/kesilen aktvitelere tahammül eskisine oranla daha azalmıştır.

İş sürekliliği sadece mali bir konu olmasının ötesinde kamu güvenliği, kamu sağlığı ve piyasaların dayandığı kamu fonksiyonları nedeniyle devlet-özel tüm sistem için kritik bir konu haline gelmiştir.

Bu raporda iş sürekliliğinin temel kavramları, metodları ve standartları açıklanmaya ve özetlenmeye çalışılmıştır. Kamu BIB Çalışma Grubu olarak gerçekleştirilen bu çalışmanın grup üyeleri kamu çalışanlarından oluşmakla birlikte, hazırlanan bu rapor aynı zamanda özel sektöre de yol gösterebilecek niteliktedir.

Çalışma grubumuzda konuyu ele alırken sadece teorik arka planını değil uygulamaya yönelik boyutlarını ve uygulamada yukarıda bahsi geçen yaygın hatalara dikkat çekme gereksinimi de gündeme gelmiştir. İş sürekliliğinin ne olduğunun yanı sıra bu raporda uygulamada kullanılabilecek pratik bilgilere de (özellikle 5 ve 6. bölümlerde) yer verilmeye çalışılmıştır.

İş sürekliliği yönetiminin ne olduğu, nasıl uygulanacağı ve örnek uygulama dokümanları ile Türkiye'de kamu kurumları ve özel sektör için yön gösterebilecek bir rapor çalışması oluşturulmaya çalışılmıştır. Bu raporda sunulan bilgiler ve önerilen tavsiyeler kurumlara uygulamada bazı değişkenlikler gösterebilir. Raporun oluşturulmasında değerli katkıları ile çalışmaya yön veren değerli katılımcıların ve kaynak olarak bilgilerinden faydalandığımız değerli uzmanlarımızın katkıları olmasaydı bu rapor oluşmazdı. Raporumuzun okuyucuya katkı sağlayacağını umut ederiz.

Kamu BIB 14. dönem 2. Çalışma Grubu olarak yaptığımız araştırmalar ve toplantılar sonucunda ortaya çıkan raporun iş sürekliliği alanında çalışacak ve bu konuda faaliyet yürütecek başta Kamu Bilgi İşlem birimleri olmak üzere tüm ilgililere faydalı olmasını temenni ederiz.

BÖLÜM 1

GİRİŞ

Tüm dünyada olduğu gibi ülkemizde de, gerek kar amaçlı özel şirketler gerekse kar amacı gütmeyen kamu kurum ve kuruluşlarının ürettikleri ürün ve sağladıkları hizmetlerin sürekliliği kritik bir öneme sahiptir. Özel sektör bu sürekliliği çoğunlukla maliyet olarak değerlendirirken, kamu kesiminde temel olarak itibar, hükümet politikaları için etkin bir araç ve güven unsuru olarak yansımaktadır.

Kurumların bilgisayarlaşma ve otomasyon seviyesinin yükselmesi ve bunun sonucunda birlikte çalışabilirlik ihtiyacının artması kurumların kendi ihtiyaçlarının yanında bağlı bulundukları kurum ve kuruluşların da iş süreçlerinin sürekliliğini doğrudan etkileyebilmektedir.

2000'li yılların başına kadar olağanüstü durumlara karşı bir yedek merkez ve veri yedeklemesi kapsamında önlemler alınması yeterli görülürken, günümüzde iş ve hizmet sürekliliği odaklı yaklaşımlar dikkate alınmaktadır. Ancak, özellikle kamu kurum ve kuruluşlarında bu yaklaşım da genel olarak planlamanın ötesine gidememekte ve bu nedenle etkin olamamaktadır. Yeterli ve hiç tatbikat yapılmaması, sürekli iyileştirmenin gerçekleştirilememesi, personele yeterli eğitimin ve farkındalığın kazandırılamaması temel eksiklikler olarak göze çarpmaktadır.

1999'da ülkemizde Marmara bölgesinde yaşanan deprem ve 2001'de A.B.D.'nde ikiz kulelere yapılan saldırılar sonrasında önemi daha fazla anlaşılan, geçtiğimiz günlerde Van'da meydana gelen deprem ile bir kez daha hatırlanan iş sürekliliğinin hem özel sektör hem de kamu kurum ve kuruluşlarda kritikliği bir kez daha ortaya çıkmıştır. Bu tür doğal afet ve terörist saldırıların yanında, donanım arızası, öngörülemeyen ve test edilemeyen yazılım hataları, işletim hataları ve çevresel faktörler, sistemlerin ve dolayısı ile iş ve hizmetlerin sürekliliğini aksatacak riskler olarak öne çıkmaktadır. Kaynağı ne olursa olsun, bu tür riskleri belirleyen, analiz eden, etkilerini somutlaştıran ve buna karşı önlemler ortaya koyan etkin bir iş sürekliliği çalışması günümüzde tüm kurum ve kuruluşların kaçınılmaz önceliklerinden biri olacaktır.

Kurumlarda, olağanüstü bir duruma ya da beklenmedik bir olumsuz duruma karşı hazırlıklı olmak ve organize hareket etmeyi planlamak büyük önem

taşımaktadır. Ortaya çıkma olasılığı düşük olmakla birlikte gerek maddi boyutu, gerekse kuruluşların imaj ve itibarı göz önüne alındığında, olası kayıp ve etkisi yıkıcı boyutlarda olabilecek, acil ve beklenmedik bir duruma karşı iş sürekliliği planlamasının önemli bir gereklilik olduğu görülmektedir.

Her kurumun kendi özelliklerine göre farklı bir plana sahip olması gerekir. Sistemin devamlılığı açısından, kurumda beklenmedik durumlara karşı hazırlıklı olunması gereğinin üst yönetimce benimsenmesi, planlı ve organize hareket etme bilincinin çalışanlarda oluşturulması önemlidir. Burada temel olan kuruma uygun İş Sürekliliği Planlamasının yine kurum çalışanlarının katılımıyla ve üst yönetimin desteğiyle yapılması ve İş Sürekliliği Yönetim Sisteminin oluşturulmasıdır.

Ülkemiz, jeolojik ve topoğrafik yapısı ve de iklim özellikleri nedeniyle büyük can ve mal kayıplarına yol açan doğal afetlerle sık sık karşılaşan ülkelerin başında gelmektedir. Ülkemizde doğal afetlerin son 60 yıl içerisinde yol açtığı yapısal hasar istatistikleri dikkate alındığında, bu tür hasarların 2/3 ünün deprem nedeniyle meydana geldiği ve tarihsel kayıtlardan elde edilen sonuçlara göre de geçtiğimiz yüzyıl içerisinde ülkemizde 5.5 ve üzeri büyüklükte meydana gelen ve hasar yaratan depremlerin sayısının 118 olduğu görülmektedir.

Ülkemiz jeolojik ve topoğrafik yapısı ile iklim özellikleri nedeniyle büyük can ve mal kayıplarına yol açan doğal afetlerle sık sık karşılaşan ülkelerin başında gelmektedir. Ülkemizde etkili olan doğal afetleri önem sırasına göre depremler, heyelanlar, su baskınları, kaya düşmeleri, yangınlar, çığ, fırtına ve yer altı suyu hareketleri şeklinde sıralamak mümkündür. Son 60 yıl içerisinde doğal afetlerin yol açtığı yapısal hasar istatistikleri dikkate alındığında, bu tür hasarın 2/3'ünün deprem nedeniyle meydana geldiği görülmektedir. Bu nedenle de ülkemizde doğal afet denilince akla öncelikle depremler gelmektedir. Şu anda geçerli bulunan deprem bölgeleri haritası esas alındığında, ülkemiz topraklarının %96'sının farklı oranlarda tehlikeye sahip deprem bölgeleri içerisinde olduğu ve nüfusumuzun %98'inin bu bölgelerde yaşadığı görülmektedir. Bu oranlar, ülkemizin bir deprem ülkesi olduğu gerçeğini çarpıcı bir şekilde ortaya koymaktadır.

Depremler, başta afetin meydana geldiği bölgeler olmak üzere tüm ülkede etkisini hissettirmekte ve dolayısıyla ülkede yaşayan vatandaşların hepsi depremin sonuçlarından belli ölçüde etkilenmektedir. Ortaya çıkan maddi zararların telafi edilmesi, deprem bölgesinde normal hayata dönülebilmesi, acil yardıma ihtiyaç duyan kimselerin bu ihtiyaçlarının giderilmesi ve benzeri için yapılan harcamalar ülke ekonomisine ve devlete büyük bir mali yük getirmektedir. Bunun en son

örneğini oluşturan ve son yüz yılın felaketi olarak adlandırılan 17 Ağustos 1999 Marmara Depremi, ekonomik ve sosyal boyutları ile ülkemiz için büyük bir yıkım olmuştur.

İş sürekliliği, kurumun kritik iş süreçlerinin devamlılığını sağlamak, sağlanamadığı durumlarda öngörülen kesinti süreleri içerisinde yeniden çalışır hale getirmek için gerçekleştirilen çalışmalara verilen isimdir. Kritik iş süreçlerinin her zaman çalışır vaziyette bulunması arzu edilen durumdur. Fakat zaman içerisinde süre gelen olaylar nedeni ile süreçlerin kesintiye uğraması kaçınılmazdır. İş süreçlerinde kesintiye neden olaylar küçük ve kısa zamanda telafi edilebilir olaylar olabileceği gibi, ciddi felaketler de olabilir. En uç örnek olarak ana çalışma alanı tamamen kaybedilebilir. Nasıl bir olay yaşanırsa yaşansın kurumun en az zarar ile çalışmalarına devam edebilmesi için kurumda iş sürekliliği yönetim sistemi kurulmalıdır. Kurum içerisindeki iş sürekliliği aktivitelerinin yönetildiği sisteme, iş sürekliliği yönetim sistemi ismi verilmektedir.

1.1. Kriz Yönetimi

Kriz kavramına ilişkin literatürde bir tanım birliği bulunmamaktadır. Farklı araştırmacılar farklı tanımlar ortaya koymuşlardır.

Fikir birliğine varılan tanımlardan biri Rosenthal ve Kouzm'ın yaptığı tanıma göre kriz ''Temel yapıların, değerlerin ve normların beklenmedik gelişmeler sonucu, olumsuz yönde etkilenme durumu''[1] dur.

Reilly, krizi "Etkisi altına aldığı örgütün varlığını potansiyel olarak tehdit eden bir durum" olarak tanımlamaktadır. Brewton'e göre ise, "Karşılaşılan bir durumda faaliyetlerde ciddi aksama, devletin kurumsal alanda gerçekleştirdiği düzenlemelerde artma, kurum hakkında kamuoyunda olumsuz algılama, finansal açıdan zorlanma, yönetim zamanını verimsiz kullanma, iş görenin moralinde ve desteğinde zayıflamaya yol açıyorsa"[2] kriz olarak nitelendirilebilir.

Kriz örgüt için her zaman olumsuz bir durum anlamına gelmemektedir. Çincede tehlike ve fırsat kelimelerinin birleşiminden oluşan *wei-ji* kelimesi ile tanımlamaktadır. Bu bağlamda bir dönüş noktası olarak düşünülebilir.

Krize yol açan birçok faktör olmakla beraber bunları iç ve dış çevre faktörleri olarak ele almak mümkündür.

Dış çevre faktörleri;

- Sosyo-Kültürel Çevre Değişiklikleri,

- Politik ve Hukuki Çevre Değişiklikleri,
- Teknolojik Çevre Değişiklikleri,
- Rekabet Koşullarındaki Değişiklikler
- Tabii Felaketler şeklinde

İç Çevre Faktörleri;

- İşletmenin Büyüklüğü,
- İşletmenin İçinde Bulunduğu Hayat Safhası,
- İşin Özellikleri,
- Yetersiz İletişim, Koordinasyon ve Kontrol,
- Katı Örgüt Yapısı,
- Örgütün Merkezileşme Derecesi,
- Yönetimin Yetersizliği

şeklinde gruplandırılabilir. Bu gruplandırma da bize gösteriyor ki kriz ve kesintiler sadece doğal afetler nedeniyle ortaya çıkmamakta ve olası bir iş sürekliliği çalışması sadece doğal afetleri değil bu sayılan faktörler dikkate alınarak yapılmalıdır.

Bu faktörler krizin oluşumunda ve şiddetinde değişik ağırlıklara sahip olmakla beraber, krize yol açan faktörlerin temelinde değişim, mevcut durum ve istikrar kavramları önemli rol oynamaktadır.[2]

Krizin, her ne kadar ani olarak ortaya çıktığı söylense de yangın, sel, deprem gibi doğal felaketlerle oluşan krizler dışında diğer kaynaklara bağlı olarak oluşan krizlerin tamamı oluşum sürecinde bazı sinyaller gönderir. Fakat bu sinyallerin yeterince dikkate alınmaması veya sinyallerin krize ait olduğunun bilinmemesi sonucu kriz ortaya çıkar. Kriz oluşurken şu aşamalardan geçer.

1- Körlük

Bu aşamada yöneticiler iç ve dış çevrede meydana gelen ve örgütü tehdit eden sinyalleri alabilir, ancak bu değişimi ve gelişmeleri teşhis etme ve tanımlamada yetersiz kalırlar.

2- Atalet

Bazı durumlarda çevresel değişim ve gelişmelerin kuruma etkileri ve sonuçlarını değerlendirmeyen üst yönetim krize karşı gerekli tedbirleri alamamaktadır. Bunun çeşitli sebepleri vardır. Özellikle mevcut durumun geçici

olduğu ve standart önlemlerle zamanla düzelebileceği düşünülür. Kriz durumunun şiddeti arttıkça etki belirginleşmeye ve işler ters gitmeye başlar.

3- Yanlış Karar ve Faaliyetler

Bu safhada çevredeki değişiklikler ve iç problemlerin yorumlanmasındaki belirsizlikler, yönetimin yapması gereken davranışın yönü konusunda yöneticiler arasında hakim bir görüşün oluşumunu engeller. Kişisel sezgiler ve yorumlar ön plana çıkar. Karar verme durumunda olanları ikna etmek ve gerginliği azaltmak için herkesin iyi bildiği veya uygun gördüğü faaliyetlere yönelmesi durumu ortaya çıkar. Belirsizliği ortadan kaldırmak için ortak bir strateji geliştirilemez.

4- Kriz

Yaklaşmakta olan kriz sinyalleri alınıp, yorumlanıp, değerlendirilmemişse ve sağlıklı tepkiler verilmemişse, örgütün kriz dönemine girmesi kaçınılmazdır. Örgüt içinde panik, çatışma baş gösterir. Bu durum yöneticilerin günü kurtarmaya yönelmesine, amaçlar ve planların göz ardı edilmesine ve örgüt ikliminin bozulmasına yol açar.

Karar alma merkezileşir, denetimde merkezileşme eğilimi artar ve karar alma süreci bozulur. Bu aşamada krize karşı bir çözüm geliştirilerek kriz avantaja dönüştürülebilir.

Kriz yönetimi; Türk Dil Kurumu sözlüğünde “Bir ülkenin karşılaştığı ulusal, uluslararası herhangi bir sorun veya doğal afet durumunda sorunun en az zararla atlatılabilmesi için gerekli kararların alınması işi” olarak tanımlanmıştır. Kriz yönetimi “Olası kriz durumuna karşılık, kriz sinyallerinin yakalanarak değerlendirilmesi ve örgütün kriz durumunu en az kayıpla atlatabilmesi için gerekli önlemlerin alınması ve uygulanması sürecidir.”[3] şeklinde de tanımlanabilir. Temel amacı, örgütü, kriz durumuna karşı hazırlamaktır. Kriz yönetimi süreci özetle şunlardır;

- **Kriz Sinyalinin Alınması**

Kriz durumu tüm şiddetiyle ortaya çıkmadan önce erken uyarı sinyalleri gönderir. Kriz sinyalleri, gelmekte olan krizin varlığı ve şiddeti ile ilgili bilgileri içermesinden dolayı, yöneticilerin bu sinyallere karşı son derece duyarlı olmaları gereklidir. Kriz bu sinyallerin takip edilememesi, doğru biçimde değerlendirilmemesi sonucunda ortaya çıkar. Kriz sinyallerinin yakalanabilmesi için örgütte değişik sinyalleri alabilen çeşitli erken uyarı sistemlerinin kurulması ve işletilmesi gereklidir. Normal seyrinden farklı olan oluşumlar ve bazı istatistiksel yöntemlerle yapılacak ön çalışmalar bu sinyallerin gözden kaçmasına engel olacaktır.

- **Krize Hazırlık ve Korunma**

Örgütün erken uyarı sistemleri aracılığıyla yakaladığı verileri kullanarak krize karşı hazırlık yapabilmesine ve önlemler alabilmesine yardımcı olan mekanizmaları kurması gereklidir. Kurulacak olan önleme ve korunma mekanizmaları erken uyarı sisteminden gelen bilgileri kullanarak, olası bir krizle ilgili alınacak önlemler konusunda yönetime bilgi iletir. Krize hazırlık ve korunma mekanizmalarının sağlıklı biçimde işlemesi için erken uyarı sinyallerinin etkili biçimde izlenmesi zorunludur. Bunun yanında örgütte önceden kurulu bir korunma planı olmalıdır.

- **Krizin Denetim Altına Alınması**

Örgütün erken uyarı sistemleri aracılığıyla yakalanan kriz sinyalleri, kriz önleme ve korunma mekanizmalarını harekete geçirir. Üst yönetim gelen bilgiler doğrultusunda krizi önlemeye yönelik harekete geçer. Bazı durumlarda erken uyarı, önleme ve korunma mekanizmaları etkili biçimde çalışsa da kriz durumundan tamamen kurtulmak olanaklı olmayabilir. Bu nedenle üst yönetimin, kriz yönetiminin ilk iki aşamasında elde ettiği verileri kullanarak krizin seyrini takip etmesi ve gerekli önlemleri alması gereklidir.

- **Normal Duruma Geçiş**

Krizin denetim altına alınması ve atlatılmasından sonra örgütün istikrarlı duruma getirilmesi gereklidir. Kriz döneminde örgüt alt sistemleri arasındaki bağlar zayıflamış, örgütsel iklim ve düzen bozulmuş olabilir. Örgütün yeniden yapılandırılarak değişen çevre koşullarına uygun duruma getirilmesi, krizin yarattığı olumsuz etkilerin giderilmesine çalışılmalıdır.

- **Öğrenme ve Değerlendirme**

Kriz yönetimi sürecinin son aşaması, kriz döneminde alınan karar önlem ve uygulamaların gözden geçirilmesi ve kriz döneminden dersler çıkarılması faaliyetlerini içerir. Kriz yönetimi, oldukça karmaşık bir süreçtir. Örgütün krizi en az kayıpla aşabilmesi için yönetimin kriz dönemlerinde sakin olması, kriz durumu ortaya çıkmamış olsa da kriz durumları için planlar hazırlaması, kriz döneminde, ayrıntılarla uğraşmak yerine doğrudan krizin özü ile ilgilenmeleri, disiplinli ve cesaretle çalışmaları yararlı olabilir.

1.2. Risk Yönetimi

Belirsizliği azaltmak bakımından zararlar ve zarar nedenleri hakkında bilgi sahibi olmak ve önlemler almak gerekmektedir.

Riskle karşı karşıya olan kurumlar, örgütler ve kişiler, gerek kendi özellikleri ve hedefleri gerekse koşullar ve risklerin nitelikleri kapsamında riski yönetmeye yönelebilirler.[4] Risk yönetiminde çeşitli yönetim yaklaşımları vardır. Bunlar;

- Riskten kaçınma,
- Riske katlanma,
- Riskin aktarılması,
- Zararın kontrolü (Önleme, Azaltma),
- Kendi kendine sigorta,
- Yukarıdaki yöntemlerin karışımıdır.

Genel olarak ifade edilebilecek risk yönetimi aşamaları ise; riskin tanımlanması (riskin teşhisi), risk analizi (riskin değerlendirilmesi) ve risk stratejilerinin geliştirilmesi (riske karşı çözüm üretme), diğer bir ifadeyle ekonomik kontrol faaliyetlerinden oluşmaktadır.[4]

Tamamı ile ileriye dönük bir stratejik karar aracı olan risk yönetimi, karar verme aşamasında risklerin sistematik olarak değerlendirilmesini ve kararlara yansıtılmasını amaçlayan bir proje yönetim tekniğidir. Risk yönetiminin temel amacı risklerin tanımlanmasını, büyüklüklerinin sayısal olarak ifade edilmesini ve risklerin gerçekleşmesi durumunda takip edilecek stratejilerin önceden belirlenmesini sağlamaktır ve genel kanının aksine yalnızca risklerin ortadan kaldırılmasına yönelik değildir. Uygulandığında tüm riskleri yok eden sihirli bir yöntem olarak algılanmamalı ve sigorta ile eş anlamlı olarak düşünülmemelidir.[4]

1.3 Beklenmedik Durum

“Beklenmedik” kelimesi “Birdenbire, ansızın olan”, “durum” kelimesi ise “Bir şeyin içinde bulunduğu koşulların hepsi, vaziyet, hâl, keyfiyet, mevki, pozisyon” anlamına gelmektedir. Bu bağlamda beklenmedik durum kavramı “Bir şeyin içinde bulunduğu koşullarda birdenbire, ansızın ortaya çıkan olay” şeklinde tanımlanabilir.

Bir başka tanımla, acil durum kavramından hareketle; “Çalışanlar, müşteriler, ziyaretçiler veya halk arasında, ölüm ve ciddi yaralanmaya neden olabilecek veya işin durmasına, faaliyetlerin aksamasına, fiziksel veya çevresel olarak zarar görmesine, tesisin mali yapısının bozulmasına ve toplum içinde itibarının düşmesine neden olabilecek, plan dışı, istem dışı gelişen olaylardır.”[5]

Yangın, deprem, sel/su baskını, yoğun kar yağışı, fırtına, heyelan, toplu gıda zehirlenmesi, kimyasal madde kazaları, parlayıcı ve patlayıcı madde kazaları,

radyasyon kazaları, anarşik olaylar, iletişim sistemini çökmesi, bilgisayar sisteminin çökmesi, müşteri veya tedarikçilerin kaybedilmesi, büyük üretim arızaları, enerji kesilmesi, sabotaj, salgın hastalık, trafik kazası, aşırı sıcak veya soğuk, seferberlik hali gibi pek çok olay beklenmedik durum olarak yorumlanabilir. Beklenmedik durum yönetimi ise; olayın etkilerini azaltmak, müdahale etmek sürecinin koordinasyonudur. Dinamik bir süreç olup, planlamanın en kritik aşamaları eğitimler, tatbikatlar, ekipmanların denenmesi ve faaliyetlerin koordine edilmesidir.

BÖLÜM 2

STANDARTLAR

Kamuda hesap verebilirlik incelemeleri kamu kesimi kuruluşlarında yoğunlaşsa da, özel kesimin de kamu hizmeti sunumunda rolünün artması, hem kamu, hem de özel kesimin karşılaştırılabilme gereksinimini doğurmaktadır. Özel kesimde, kuruluşlar alt çizgide daha hesap verebilir görünmekte; kamu kesiminde ise, ilke-koşul ve standartların özellikle süreç ve genel uygulamada daha sıkı olduğu bulgulanmaktadır (Mülgan 2000: 87). Kamu kesimi yönetiminin, özel kesimdeki standartlarla değerlendirilmesi sürdürüldükçe, özel kesim, siyasal-toplumsal-ekonomik kamusal amaçlar yüklendikçe, kamu ve özel kesim ayrımında baskının artacağı öngörülmektedir (Mulgan 2000: 96). Kurumlar, davranışsal açıdan değerlendirildiğinde, biçimsel (formal) örgüt; yapı – hiyerarşi, işbölümü, kurallar/usuller, iş süreçleri, kültür ve süreçler – haklar/yükümlülükler, imtiyazlar/sorumluluklar, değerler, normlar/standartlar, insanlardan oluşan, çevresel kaynakları sonuçlara dönüştüren bir sistem görülmektedir (Laudon ve Laudon 2007: 85).

BT ve kurumlar etkileşimi açısından ise, dijitalleştirmenin her türden kamu ve özel kurumda bilginin yönetimi açısından önemini giderek artırdığı bilinmektedir. Bu konuda gerek kurumsal gerekse bireysel düzeyde değişimin farkında olmak durumundayız. Kurumlarda bilginin/belgenin üretimi, düzenlenmesi, saklanması, dijital arşivlemesi, dijital erişiminde standartlar konusunda bir farkındalık, temel kavramlara ve sürece belirli düzeyde hakimiyet gerekmektedir.[6] Kurumların sağlam iş sürekliliği süreçleri kurduğunu göstermek için ne yapması gerektiği ve kendi süreçlerini kendisi ya da diğer bağımlı birimlerin nasıl değerlendirebileceği konusunda örnek bir standart İngiltere'de iki bölümde ele alınmıştır:

- Bölüm 1: Uygulama Kodu (Code of Practice (BS 25999-1:2006): "sağlam bir İSY geliştirmek ve korumada, iyi uygulamaya dayalı rehberlik ve öneriler formundadır. [6]
- Bölüm 2: Belirli Direktifler (Specification) (BS 25999-2:2007): kurumların biçimsel (resmi) ve gayri resmi ölçülebildiği yönetim sistemleri yaklaşımı gerekliliklerini tanımlar. [6]

Standart, üzerinde anlaşılmış teknik spesifikasyonlar içeren ya da kesin kriterler ile tasarlanmış tekrarlanabilir tutarlı kurallar, kılavuzluk bilgileri veya tanımlamalar içeren basılı bir dokümandır. Standartlar kullandığımız birçok eşyanın ya da hizmetin etkinliğini ve güvenilirliğini artırmak ve hayatı kolaylaştırmak için hazırlanırlar. Genel uygulamaları değil, üzerinde anlaşılmış en iyi uygulamaları tarif eder. Standartlar, konusunda uzman kişilerin bir araya gelmesiyle oluşturulur; Üretici komiteleri, kullanıcılar, araştırma kurumları, hükümet birimleri, tüketiciler bir araya gelerek teknolojinin ve sosyal hayatın ihtiyaçlarına en iyi cevabı verebilecek uygulamaları bir araya getirir ve bir taslak oluşturur. Üreticiler, satıcılar, alıcılar, kullanıcılar ve bu üründe kullanılacak her bir ürünün özelliklerini, süreçleri ya da hizmeti kapsayan yasal gerekliliklerle ilgilenirler. Tüm resmi standartlar kamudan veya endüstriden gelen talepler doğrultusunda geliştirilmeye başlanır. Tüketiciler, akademisyenler, özel ilgi grupları, hükümet, iş ve endüstri temsilcileri gibi tüm ilgili taraflar ve uzmanlar bir araya gelerek ortak bir görüş oluşturur; sonuç olarak standartlar mevcut en iyi uygulamalar üzerindeki ortak görüşü temsil eder.

Standartlar gönüllü kullanım için tasarlanırlar, herhangi bir yasal düzenleme tarafından dayatılmazlar. Ancak bazı durumlarda yasalar, uygunluğun sağlanabilmesi için standartları referans olarak gösterebilir ve zorunlu tutabilir. Standartlar her büyüklükteki kuruluş için yenilikçiliği destekleyen ve verimliliği artıran en güçlü araçlardır. Standartlara uyumlu çalışma, rekabet gücünü, karlılığı artırıp yeni pazarlara girmeyi sağlayabilir. En iyi uygulamaları geliştirmeye ve sürdürmeye yardım eder.

2.1. Standartlar Nasıl Kullanılır?

Standartların kullanımı, dünya çapındaki ticarete ön koşul oluşturduğu için gittikçe artmaktadır. Uluslararası ticaret, uluslararası standartlara göre yürümektedir.

Her ne kadar standartlar gönüllü kullanım için tasarlanmış olsa da, yasalar tarafından zorunlu tutulmasa da; bazı kanunlar ya da sektörler standartları referans olarak gösterir.

2.2. Ortak Görüş Standartları

Tüm resmi standartlar kamudan veya endüstriden gelen talepler doğrultusunda geliştirilmeye başlanır. Tüketiciler, akademisyenler, özel ilgi grupları, hükümet, iş ve endüstri temsilcileri gibi tüm ilgili taraflar ve uzmanlar bir araya gelerek ortak bir görüş oluşturur; sonuç olarak standartlar mevcut en iyi uygulamalar

üzerindeki ortak görüşü temsil eder. Bunlar ulusal, uluslararası, Avrupa Standartları, yetkili standartlar olabilir.

2.3. Kamuya açık spesifikasyon - Publicly available specification (PAS)

PAS'lar da British Standards ile aynı gelişim sürecinden geçer ancak bunun için bir dış destekleyici tarafından yetkilendirilmesi gerekir. Bu konuda ortak görüşe gerek duyulmaz. PAS ile ortak görüş British Standards arasındaki fark, PAS'lar o dönemdeki sektör ihtiyaçlarını hemen karşılayabilmek için çok hızlı hazırlanır ve yayımlanır. Bazı PAS standartları daha sonra evrimlerini tamamlayıp ortak görüş standardına dönüşürler. (Örn. PAS 56 - İş Sürekliliği, 2003'te yayınlanmış daha sonra British Standard (BS25999) olarak 2006'da yeniden yayınlanmıştır.)

Uluslararası kamuya açık spesifikasyon ise, "ISO/PAS" olarak kısaltılmaktadır.

2.4. BS 25999 İş Sürekliliği Yönetimi Standardı

İngiliz Standartlar Enstitüsü (British Standards Institution) tarafından yayımlanmış olan BS25999 standardı, beklenmedik durumlarda işlerin devamlılığını sağlamak, çalışanları korumak, kurumun itibarını sürdürmek, faaliyetlerin ve ticari etkinliklerin devam etmesini sağlamaya yardımcı olmak için tasarlanmıştır. Standart iki bölümden oluşmaktadır:

Bölüm 1: Uygulama Kuralları (Code of Practice BS 25999-1:2006) [6]

Bölüm 2: Belirtimler (Specification BS 25999-2:2007) [6]

İş sürekliliği konusunda çalışan ve uygulayan uzman kişiler ve kurumlar ile akademik toplulukların teknik ve uygulama deneyimlerinden yararlanılarak hazırlanmıştır. İş sürekliliği yönetimi konusunda en iyi uygulamalar dikkate alınarak hazırlanan bu standart, büyük, orta ve küçük her sektörden organizasyonun (kamu veya özel) iş sürekliliği yönetiminde tek bir kaynak olması hedeflenmiştir.

2.5. Uygulama Kuralları (Code of Practice BS 25999-1:2006)

2006 yılında yayınlanan bu ilk bölüm temel olarak kılavuz ve öneriler olarak hazırlanmıştır. En iyi uygulamalar çerçevesinde güçlü bir İş Sürekliliği Yönetim sisteminin nasıl geliştirilip sürdürülebileceğini göstermektedir. 10 alt bölümden oluşan standart uygulama kurallarına yönelik tüm bileşenlere değinmektedir. Bunlar arasında:

- Kapsama alanı,
- Politika,
- Kritik iş faaliyetlerin belirlenmesi,
- İşe özel süreklilik planının geliştirilmesi ve yönetilmesi,
- Performansın izlenmesi ve korunması,
- Kurum bünyesinde iş sürekliliği farkındalığının kurum kültürü olarak yerleşmesi bulunmaktadır.

Standartta bahsedilen ve vurgulanması gereken önemli konulardan birisi BS 25999 yaşam döngüsüdür[6] (Bkz. Şekil 1) 6 bileşenden oluşan yaşam döngüsü farklı ölçekte ve türde kuruma uygulanabileceği gibi kurumun özelliklerine göre kapsamı ve yapısal özelliklerine göre kurumdan kuruma farklılıklar gösterebilmektedir. Program yönetimi, yaşam döngüsünün merkezinde bulunmaktadır ve iş sürekliliği politikası ile belirlenmiş amaçların gerçekleştirilmesini sağlamak üzere yapılması gereken çalışmaları tanımlamaktadır. Yaşam döngüsü ile ilgili detaylı bilgiler BS25999-1'in 3. bölümünde yer almaktadır.

Şekil 1: BS25999 Yaşam Döngüsü

2.6. Belirtimler (Specification : BS 25999-2:2007)

2007 yılında yayımlanan ikinci bölüm iş sürekliliği yönetim sistemi için en iyi uygulamalara ait gereksinimleri sağlamaktadır. Standardın bu bölümü, uygunluğun

kanıtlanması amacıyla tetkik ve belgelendirme kriteri olarak kullanılmaktadır. BS 25999-2 ile bir organizasyonun kurallara, yasalara, müşterilere ve iş gereksinimlerine uygun etkin bir iş sürekliliği yönetim sistemini tasarlayıp kurabilmesi hedeflenmiştir. 6 alt bölümden oluşan BS 25999-2 bu amaca ulaşmak için aşağıdaki hususları özellikle vurgulamaktadır:

- İş sürekliliği hedefleri ve politika oluşturma doğrulturunda kurumun iş sürekliliği ihtiyaçlarının belirlenmesi,
- Kurumun tüm iş sürekliliğine yönelik risklerin yönetilmesi için kontrol ve önlemlerin uygulanması ve işletilmesi,
- İş sürekliliği yönetim sisteminin etkinliğinin ve performansının izlenmesi ve düzenli olarak üzerinden geçilmesi,
- Sürekli bir iyileştirme sürecinin oluşturulması.

Organizasyonlar tarafından BS 25999 Standartlarının başarılı şekilde uygulandığının kanıtlanmak istendiği durumlarda bu standartların uygulamaları referans olarak gösterilebilir tüm diğer yönetim sistemi standartlarında olduğu gibi bu standart da süreç yaklaşımı benimsenmiş ve ilkeleri Planla-Yap-Kontrol et-Uygula (PUKO) döngüsü paralelinde geliştirilmiştir.

BS 25999 İş Sürekliliği Yönetim Sistemi Standardı etkin bir iş süreklilik yönetim sisteminin (BCMS) oluşturulması ve yönetilmesi için gereklilikleri tanımlar.

Bu; aşağıda sıralananların önemini vurgular:

- İş süreklilik ihtiyaçlarının ve iş sürekliliği için politika ve hedefler oluşturulmasının gerekliliğinin anlaşılması;
- Organizasyonun tüm iş süreklilik risklerinin yönetilmesi için kontrol ve ölçümlerin uygulanması ve çalıştırılması;
- BCMS' nin performansının ve etkinliğinin izlenmesi ve gözden geçirilmesi;
- Objektif ölçümleri temel alan sürekli iyileşme.

Bir BCMS, diğer yönetim sistemleri gibi, sıralanan anahtar öğelere sahiptir:

- Politika,
- Tanımlanmış sorumluluklar ile personel,
- Aşağıdakilere ilişkin yönetim prosesleri,
  - Politika,
  - Planlama,
  - Uygulama ve operasyon,
  - Performans değerlendirme,

- Yönetimin gözden geçirmesi,
- İyileştirme.

- Denetlenebilir kanıt sağlayan bir dizi dokümantasyon;
- Konuyla ilişkili, bu durumda iş sürekliliği ile ilişkili, özel süreçler

Örneğin; iş etki analizi (BIA) ve iş süreklilik planı geliştirme.

2.7. Planla-Yap-Kontrol et-Uygula Döngüsü (PUKO)

BS 25999 İş Sürekliliği Yönetim Sistemi Standardı, organizasyonun BCMS inin kurulması, uygulanması, işletilmesi, izlenmesi, denenmesi, sürekliliğinin sağlanması ve etkinliğinin iyileştirilmesi için PUKO döngüsünü kullanır. Bu uygulama, diğer yönetim sistemleri ile (BS EN ISO 9001:2000, BS EN ISO 14001:2004, BS ISO/IEC 27001:2005, BS ISO/IEC 20000:2005) uygunluğu sağlar; böylece ilgili yönetim sistemleriyle entegre bir uygulama bu uygunluk ile desteklenmiş olur.

Tablo 1: PUKO Döngüsü

Planla	Organizasyonun tüm politika ve hedefleri ile uyumlu sonuçlar alabilmek için risk yönetimi ve iş sürekliliğini iyileştirici politika, amaç, hedef, kontrol, proses ve prosedürler oluştur.
Yap	İş süreklilik politika, kontrol, proses ve prosedürlerini uygula
Kontrol et	İş süreklilik hedef ve politika performansını izle, gözden geçirme için yönetime raporla, iyileştirme ya da değişiklik eylemlerini belirle.
Uygula	Gözden geçirme sonuçlarını temel alan düzeltici ve önleyici faaliyetler ile BCMS sürekliliğini ve iyileşmesini sağla.

Her bir faaliyet için PUKO döngüsünün kabul edilen geniş kapsamlı yaklaşımı BS 25999-1 standardı ile açıklanmıştır. Bu adımsal proses iş sürekliliğinin kurulmasını ve devamlı olarak yönetilmesini sağlar (iş süreklilik yönetim döngüsünün her bir öğesi ile ilgili açıklama için)

BS 25999 İş Sürekliliği Yönetim Sistemi Standardı ile paralellik sağlanması adına, bundan sonraki numaralandırmalarda BS 25999-2 standart maddeleri paralelinde numaralandırma yapılmıştır.

BS 25999 İş Sürekliliği Yönetim Sistemi Standardı, organizasyonun tüm iş risklerinin yönetimini kapsayan dokümante edilmiş bir BCMS'nin planlanması,

kurulması, uygulanması, operasyonu, izlenmesi, gözden geçirilmesi, denenmesi, sürekliliğinin sağlanması ve iyileştirilmesi için gereklilikleri tanımlar.

2.8. Bilgi güvenliği: ISO/IEC 27001/27002

ISO/IEC 27002 standardı, "Bilgi güvenliği nedir?" bölümünde, bilgi güvenliğini, iş sürekliliğinin sağlanması, iş risklerinin en aza indirilmesi, yatırım geri dönüşünün ve iş fırsatlarının artırılması amacıyla bilginin her türlü tehdide karşı korunması olarak tanımlamıştır. Görüldüğü üzere iş sürekliliği çalışmaları, bilgi güvenliği yönetim sistemi kurulumunun temel amaçlarından birisi olarak belirtilmektedir.

İş sürekliliği yönetim sistemleri (İSYS), bilgi güvenliği yönetim sistemleri (BGYS) benzeri olarak bir yönetim sürecidir. BGYS çalışmalarının temel adımlarından biri olan bilgi varlıkları envanteri (inventory of assets), iş-etki analizinde süreçlerle ilişkilendirilecek kaynakları da kapsar. BGYS kapsamında geliştirilen bilgi güvenliği risk analizi yöntemi, aynı zamanda iş sürekliliği risklerinin belirlenmesi aşamalarında da kullanılabilir. Süreçler için belirlenen kabul edilebilir kesinti süresi (RTO-Recovery Time Objective), ilgili süreci destekleyen bilgi varlıklarının değerleriyle paralellik gösterecektir. Bu bölümde görüldüğü üzere İSYS, BGYS'nin bir parçası olarak projelendirilebilir.

2.9. ISO 22301

BS 25999 bir İngiliz standardı olarak oluşturulmuştur ve iş sürekliliği konusunda tüm dünyada lider bir kaynak olmuştur. Birçok standartta olduğu gibi bu konuda da bir geçiş (BS 7799-2'den ISO 27001'e gibi) kaçınılmaz olmuş ve International Organization for Standardization (ISO) BS25999'un yerine geçecek ISO 22301'i hazırlamaya başlamıştır. 2011 yılı içerisinde taslak sürümü kamuoyu ile paylaşılan standardın 2012 yılı başında son hali yayınlanacaktır.

ISO 22301 temel olarak BS25999-2'nin yerine geçeceği düşünüldüğünde BS25999-2 ile arasındaki benzerlikler ve farklılıklardan bahsetmek yerinde olacaktır.

2.10. Benzerlikleri:

En büyük benzerlik temel iş sürekliliği bileşenlerinin ISO 22301'de de korunması olmuştur. İş sürekliliği politikası, iş etki analizi, risk değerlendirmesi, ISO 22301'de "iş sürekliliği seçenekleri" olarak adlandırılan iş sürekliliği stratejisi, iş sürekliliği planları, tatbikatları ve testleri bunlar arasındadır.

İş etki analizi detaylandırılarak daha kesin ifadeler konmuştur. İş sürekliliği planları, hatadan kurtulma planları, hataya cevap verme yordamları detaylandırılmıştır.

BS25999-2'nin yönetim bölümü ISO 22301'e taşınmıştır. Bunlar arasında, belge kontrolü, iç denetim, yönetim gözden geçirmesi, önleyici ve düzeltici bakım, insan kaynakları yönetimi sayılabilir.

2.11. Farklılıklar:

PUKÖ (Planla, Uygula, Kontrol et, Önlem al) modeli ISO 22301'de daha az vurgulanmıştır. ISO 22301 hedef koyma, performans ve metrikleri izleme konusunu daha fazla vurgulamıştır. Böylece iş sürekliliğine daha fazla üst yönetim bakış ve düşünce açısı kazandırmıştır. Ek olarak, üst yönetimden beklentileri daha açık olarak ortaya koymuştur.

BS25999-2'nin eksikliği olarak görülen planlama ve kaynak hazırlama konusunda ISO 22301 daha fazla bilgi vermektedir. Son olarak, ISO 22301 uluslar arası bir standart olmaktadır. Bu nedenle hızla popüler olması beklenmektedir.

BS 25999-2'nin temel iş sürekliliği konuları ISO 22301'de yer alması nedeniyle BS25999 uygulayan ve daha fazla detay isteyen birçok organizasyon için ISO 22301 sadece bir geçiş ya da yükselme olacaktır. Elbette bu işlem sistemlerini korumak isteyen bu organizasyonlar için ek yatırım gerektirecektir.

2.12. Bilgi Teknolojileri Altyapı Kütüphanesi: ITIL

Bilgi Teknolojileri Altyapı Kütüphanesi (Information Technology Infrastructure Library, ITIL) en iyi uygulamaların (best practices) ve deneyimlerinin bir araya getirilmesi ile oluşturulmuş bir kütüphanedir. ITIL bir standart değildir. Ancak gelinen noktada bir kütüphane olmaktan çıkıp BT yönetim metodolojisi olmuştur. Bunun altında ITIL uygulayan organizasyonların BT servislerinde gözle görülen bir iyileşme olması yatmaktadır. Bu iyileşmeler arasında hizmet seviyesi kalitesinin artması, erişebilirliğin yükselmesi, doğru kapasite ve planlama yapılarak maliyetlerin kontrol altına alınması sayılabilir.

ITIL'ın yaşam döngüsü bileşenlerinden hizmet tasarımının "hizmet tasarımı Süreçleri"nden bir tanesi BT hizmet sürekliliği yönetimi (IT Service Continuity Management, ITSCM) olarak yer almaktadır. ITSCM'in amacı, tüm iş sürekliliği yönetimi için gerekli desteği, BT teknik ve hizmet araçlarını (bilgisayar sistemleri,

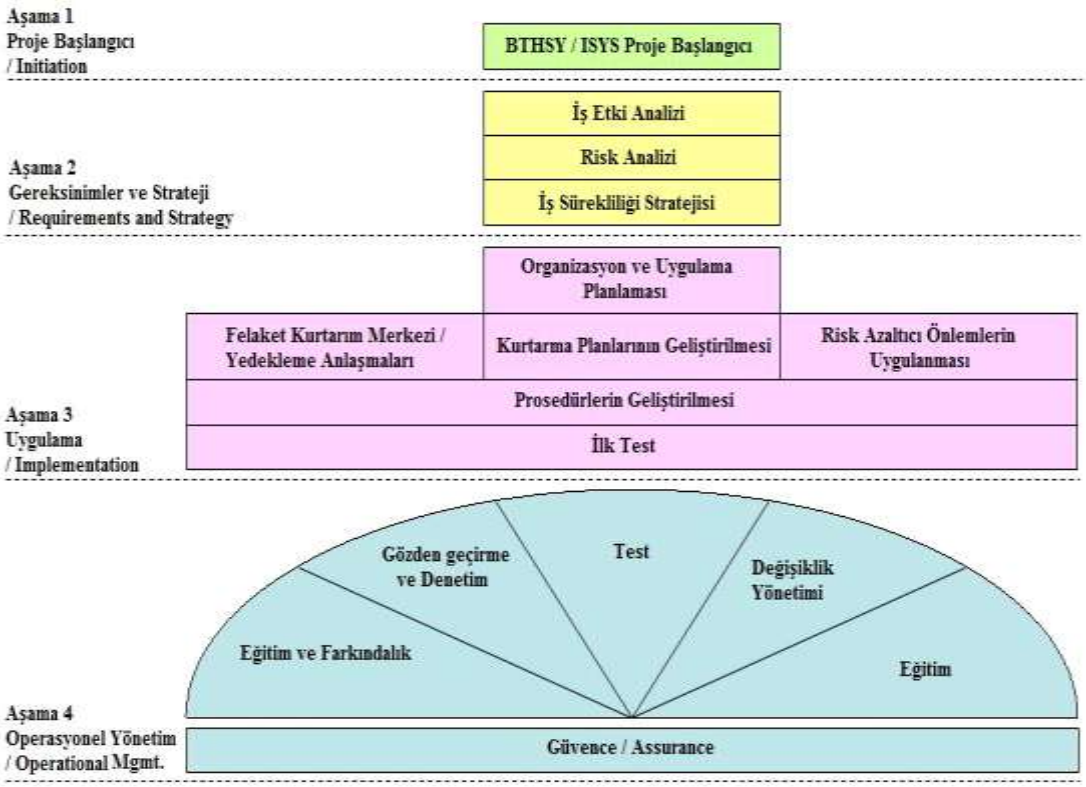
iletişim ağları, uygulamalar, hizmet masaları, vb.) iş için uygun ve istenen zamanda tekrar çalışır hale getirmek suretiyle sağlamak olarak belirtilmektedir.[7]

ITSCM süreci kapsamında aşağıdaki işlemler yer almaktadır:

- ITSCM'in kapsamı ve politikası belirlenmesi,
- İş etki analizi,
- Risk analizi,
- ITSCM stratejisinin geliştirilmesi ve iş sürekliliği stratejisi ile bütünlük sağlanması,
- ITSCM planının oluşturulması,
- Planların test edilmesi,
- İşletimin sürekli hale getirilmesi ve planların bakımı ve sürekli geliştirilmesi,

ITIL v3 içerisinde iş sürekliliği planlaması doğrudan adreslenmemiştir. Service Design/Hizmet Tasarımı aşamasından başlayarak Service Transition/Hizmet Geçişi, Service Operation/Hizmet İşletme ve Continual Service Improvement/Sürekli Hizmet İyileştirmesi süreçlerini/aşamalarını içeren bir yaşam döngüsü içinde bulunan IT Service Continuity Management/BT Hizmet Sürekliliği Yönetimi süreci tanımlanmıştır.

BTHSY süreçleri Şekil 2'de gösterilmiştir. BTHSY, ITIL v3 çerçevesinde Hizmet Seviyesi Yönetimi/Service Level Management, Değişiklik Yönetimi/Change Management, Problem Yönetimi/Problem Management, Erişilebilirlik Yönetimi/Availability Management ve diğer ilgili ITIL disiplinleriyle entegre olarak düşünülmelidir. ITIL BTHSY, iş sürekliliği konusunda global kabul görmüş çerçeveye bağlı kalmakla birlikte daha genel bir İş Sürekliliği Yönetim Sistemi'ne ihtiyaç duymaktadır. İş Sürekliliği planlamasının kritik bir parçası olan BT hizmet/kaynak sürekliliğinin sağlanması için detaylı prosedürler tanımlanmıştır. BTHSY çalışmaları, İSYS sürecini destekler rol üstlenecektir. Genel İSYS kurulmadan yapılacak BTHSY çalışmalarında, yanlış varsayımlar yapılması, kullanılmayacak planların üretilmesi, kurum genelinde iş sürekliliği süreci sahibinin BT birimleri kabul edilmesi, gereksiz teknoloji çözümlerinin üretilmesi gibi muhtemel sorunlara yol açacaktır.



Şekil 2: ITIL BTHSY süreçleri

2.13. Bilgi Teknolojileri İçin Kontrol Hedefleri: COBIT

COBIT (Control Objectives for Information and Related Technology), ISACA (Information Systems Audit and Control Association) ve ITGI (IT Governance Institute) tarafından geliştirilmiş Bilgi Teknolojileri Yönetimi için en iyi uygulamalar kümesidir. Türkçe karşılığı Bilgi Teknolojileri ve İlgili Teknolojiler İçin Kontrol Hedefleri olan COBIT, BT yönetimine odaklanan kontrol hedeflerinden oluşmaktadır.

İş sürekliliği yönetimi için mutlaka gerekli olan BT Yönetimi ve diğer destekleyici süreçler dışında COBIT çerçevesinde iş sürekliliği konusuna DS4 – Ensure Continuous Service (Kesintisiz Hizmetin Garanti Edilmesi) kontrol hedefinde değinilmektedir. DS4 süreci, kritik iş süreçlerinde yer alan BT hizmetlerindeki kesintilerin olasılığını ve iş süreçlerine etkisini en aza indirgemeyi amaçlamaktadır. Bunu sağlamak için BT sürekliliğinin planlanması, eğitimlerinin verilmesi, testlerinin yapılması, süreklilik planlarının ve bilgilerin güvenli dış ortamlarda saklanması önerilmektedir. DS4 süreci içerisinde verilen on adet detaylı kontrol şu şekilde özetlenebilir:

- DS 4.1 BT süreklilik çerçevesi
- DS 4.2 BT süreklilik planları
- DS 4.3 Kritik BT kaynakları

- DS 4.4 BT süreklilik planının devamlılığı
- DS 4.5 BT süreklilik planının test edilmesi
- DS 4.6 BT süreklilik planının eğitimi
- DS 4.7 BT süreklilik planının dağıtımı
- DS 4.8 BT hizmet kurtarma ve devam ettirme
- DS 4.9 Dış ortamda yedekleme
- DS 4.10 Kurtarma sonrası gözden geçirme [8]

DS4 kontrol hedefinin COBIT içerisinde tanımlanan 34 üst seviye kontrol hedefinden 11 tanesiyle doğrudan ilişkili olması, İş Sürekliliği Yönetim Sisteminin diğer iş süreçleriyle entegre olacak şekilde kurulmasını gerektirmektedir.

DS4 süreci, kritik iş süreçlerine hizmet veren BT hizmetlerindeki kesintilerin olasılığını ve iş süreçlerine etkisini en aza indirgemeyi amaçlamaktadır. Bu amaçla BT süreklilik planlarının hazırlanması, eğitimlerinin verilmesi, testlerinin yapılması, süreklilik planlarının ve bilgilerin dış lokasyonlarda saklanmasını tavsiye etmektedir. DS4 süreci içerisinde verilen on adet detaylı kontrol hedefi aşağıda özetlenmiştir.

2.13.1. DS4.1 BT Süreklilik Çerçevesi (IT Continuity Framework)

Kurum genelinde iş sürekliliği yönetimini desteklemek amacıyla BT süreklilik çerçevesini tanımlayacak bir sürecin geliştirilmesi gerekmektedir. Felaketten kurtarma ve BT süreklilik planları, bu çerçeveye uygun şekilde geliştirilmelidir. İç ve dış hizmet sağlayıcıların, yönetim kademelerinin, müşterilerin rollerinin ve sorumluluklarının bulunacağı organizasyonel yapı tanımlanmalıdır.

2.13.2. DS4.2 BT Süreklilik Planları (T Continuity Plans)

BT Süreklilik çerçevesine uygun şekilde BT süreklilik planlarının oluşturulması gereklidir. İş sürekliliği risklerini göz önünde bulundurarak iş etki analizinin yapılması, alternatif işlem metotlarının tanımlanması, kurtarma yöntemlerinin belirlenmesi, kullanım kılavuzlarının hazırlanması, detay rollerin ve sorumlulukların tanımlanması, gerekli prosedürlerin, haberleşme yöntemlerinin ve test yaklaşımının tanımlanması hedeflenmelidir.

2.13.3 DS4.3 Kritik BT Kaynakları (Critical IT Resources)

BT kaynaklarının, kritik iş süreçleri için belirlenen öncelik seviyeleriyle uyumlu olarak kurtarılması planlanmalıdır. Daha az önemli BT kaynaklarının öncelikli olarak kurtarılması doğru değildir. İş sürekliliği ve kurtarma çalışmaları planlanırken kritik iş süreçleri için tahammül edilebilecek kesinti süresi,

önceliklendirme, maliyetlerin kabul edilebilir seviyelerde tutulması, yasal yükümlülük ve sözleşmelere uyum göz önünde bulundurulmalıdır.

2.13.4 DS4.4 BT Süreklilik Planının Devamlılığı (Maintenance of the IT Continuity Plan)

BT süreklilik planlarının sürekli olarak iş ihtiyaçlarını karşılayabilecek şekilde güncel tutulması için gerekli değişiklik yönetimi sürecinin tanımlanması, ilgili rollerin ve sorumlulukların açık şekilde belirlenmesi gereklidir.

2.13.5. DS4.5 BT Süreklilik Planının Test Edilmesi (Testing of the IT Continuity Plan)

BT süreklilik planlarındaki eksikliklerin tespit edilmesi, planın güncelliğinden emin olunması ve BT sistemlerinin etkili bir şekilde kurtarılacağının garanti edilebilmesi için düzenli olarak testler gerçekleştirilmelidir.

2.13.6. DS4.6 BT Süreklilik Planı Eğitimi (IT Continuity Plan Training)

İş sürekliliği planları içerisinde görev alan tüm taraflara rolleri ve sorumlulukları konusunda gerekli eğitimler sağlanmalıdır. Bu eğitimler, iş sürekliliği testlerinin sonucuna göre iyileştirilmeli ve eğitimlerin yeterliliğinden emin olunmalıdır.

2.13.7. DS4.7 BT Süreklilik Planının Dağıtımı (Distribution of the IT Continuity Plan)

Gerekli olduğu zamanlarda ve yerlerde, BT süreklilik planlarının ilgili kişilere güvenli bir şekilde dağıtılmasını garanti edecek strateji/süreç tanımlanmalı ve yönetilmelidir.

2.13.8. DS4.8 BT Hiz. Kurtarma ve Devam Ettirme (IT Services Recovery and Resumption)

BT hizmetlerinin kurtarılması ve devam ettirilmesi sırasında gerçekleştirilecek aktivitelerin detaylı şekilde tanımlanması gereklidir. BT kurtarma zamanları ve gerekli teknoloji yatırımlarının BT dışındaki departmanlar tarafından anlaşıldığından emin olunmalıdır.

2.13.9. DS4.9 Dış Lokasyonda Yedekleme (Offsite Backup Storage)

İş sürekliliği planları ve BT kurtarma planlarıyla ilgili tüm kritik yedeklerin, dokümantasyonun ve gerekli BT kaynaklarının belirlenen bir dış lokasyonda tutulması gereklidir. Dış lokasyon kullanımında, dışarıda tutulan bilgilerin ve kaynakların güvenliğinin sağlanması için gerekli önlemler alınmalıdır. Dış

lokasyonda bulundurulan sistemlerin gerektiği zaman yedeklenmiş veriyi çalışır hale getirebileceğinden emin olunmalıdır.

2.13.10. DS4.10 Kurtarma Sonrası Gözden Geçirme (Post-resumption Review)

Yaşanan bir olay ya da felaket sonrasında BT hizmetlerinin başarılı olarak kurtarılmasının devamında, planın yeterliliğin değerlendirilmesi ve gerekiyorsa güncellemelerin yapılmasını sağlayacak prosedür/süreç geliştirilmelidir.

COBIT, süreç odaklı yaklaşımın bir sonucu olarak, DS4 sürecine girdi veren ve DS4 sürecinin çıktılarından faydalanan diğer süreçleri (üst seviye kontrol hedefi) Tablo 2'deki gibi belirlemiştir. İSYS kapsamında COBIT, DS4 dışındaki bu süreçlerle olan ilişkiler de göz önünde bulundurularak kullanılmalıdır. DS4 kontrol hedefinin COBIT içerisinde tanımlanan 34 üst seviye kontrol hedefinden 11 tanesiyle doğrudan ilişkili olması, İSYS kurulumunun diğer iş süreçleriyle entegrasyon ihtiyacını da gözler önüne sermektedir.

Tablo 2: DS4 süreci girdileri ve çıktıları

Süreç Adı (Kontrol Hedefi)		Girdi / Çıktı adı
PO2 Define the information architecture. (Bilgi mimarisinin tanımlanması.)	GA	Belirlenmiş veri sınıfları.
PO9 Assess and manage IT risks. (BT risklerinin değerlendirilmesi ve yönetilmesi.)	GA	Risk değerlendirmesi.
	ÇV	Süreklilik test sonuçları.
AI2 Acquire and maintain application software. (Uygulama yazılımlarının edinimi ve bakımı.)	GA	Erişilebilirlik, devamlılık ve kurtarma spesifikasyonları.
AI4 Enable operation and use. (Operasyon ve kullanımın sağlanması.)	GA	Kullanıcı, operasyonel, teknik ve yönetim kılavuzları.
DS1 Define and manage service levels. (Hizmet seviyelerinin tanımlanması ve yönetilmesi.)	GA	Hizmet seviyesi anlaşmaları.

DS2 Manage third-party services. (Üçüncü parti hizmetlerin yönetimi.)	ÇV	Felaket anında kullanılacak hizmetlerin gereksinimleri, roller ve sorumluluklar.
DS9 Manage the configuration. (Konfigürasyon yönetimi.)	ÇV	Kritiklik derecesi.
DS11 Manage data. (Veri yönetimi.)	ÇV	Yedek saklama ve koruma planı.
DS13 Manage operations. (Operasyon yönetimi.)	ÇV	Yedek saklama ve koruma planı.
DS8 Manage service desk and incidents. (Hizmet masası ve olay yönetimi.)	ÇV	Olay/Felaket ilan etme eşik değerleri.
ME1 Monitor and evaluate IT performance. (BT performansının izlenmesi ve değerlendirilmesi.)	ÇV	Süreç performans raporları.

*GA: Girdi alır. *ÇV: Çıktı verir.

2.14. Kamu İç Kontrol Standartları

10.12.2003 tarihinde yürürlüğe giren 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu, kamu kaynaklarının etkili ve verimli bir şekilde elde edilmesi ve kullanılmasını ve mali saydamlığı sağlamak amacıyla yeni düzenlemeler getirmektedir. Kurumlar geleceğe yönelik misyon ve vizyonlarını oluşturmak, hedefler saptamak, performanslarını ölçmek ve sürecin değerlendirmesini yapmak için stratejik plan hazırlamakla yükümlüdür. Ayrıca, idareler stratejik plan ve bütçelerinin hedeflerine ve hizmet gereklerine uygun olmasından, kaynakların ekonomik kullanımının sağlanmasından, kontrol sisteminin izlenmesinden sorumludur. Hazırlanan planların uygun bir kontrol ortamında takibi için hazırlanan Kamu İç Kontrol Standartları Tebliği 2007 yılında Resmi Gazete'de yayımlanmıştır.[9]

İlgili mevzuat doğrultusunda kurulacak olan İç Kontrol Sistemi 5 bileşen – 18 standart – 79 alt başlıktan oluşmaktadır. İç kontrol kurumun tüm faaliyetlerini kapsayan ve devamlılık esasına dayanan bir süreçtir. 5 bileşen şunlardır:[10]

- Kontrol ortamı standartları

- Risk değerlendirme standartları
- Kontrol faaliyetleri standartları
- Bilgi ve iletişim standartları
- İzleme standartları

Bu bileşenlerden Risk değerlendirme standartları içinde bulunan Risklerin belirlenmesi ve değerlendirilmesi ile Kontrol Faaliyetleri Standartları altında yer alan Faaliyetlerin Sürekliliği maddeleri iş sürekliliği ile ilgilidir.

Standart, kurumların faaliyetlerinin sürekliliğinin sağlanmasına yönelik önlemlerin alınmasına ilişkin olup personel yetersizliği, görevden ayrılma, yeni bilgi sistemlerine geçiş, mevzuat ve yöntem değişiklikleri ile olağanüstü durumlar gibi faaliyetlerin sürekliliğini etkileyen çeşitli nedenlere karşı gerekli önlemlerin alınması, gerekli durumlarda vekil personelin görevlendirilmesi, ayrılan personelin yaptığı işlere ilişkin rapor hazırlaması konularında şartlar getirmektedir.

Şekil 3:İç Kontrol Standardı

2.15. Diğer Standart ve Rehberler

İş sürekliliği ile ilgili yayınlanmış çeşitli uluslararası standartar ve rehberler bulunmaktadır. Tamamlayıcı ve açıklayıcı bu rehber ve standartların da incelenmesi ve kullanılmasında fayda vardır.

- ISO/FDIS 22300 Terminology
- **ISO 22301 Business continuity management systems — Requirements**
- ISO/TR 22312:2011— Technological capabilities
- **ISO/DIS 22313— Business continuity management systems — Guidance**
- ISO/NP 22315 Societal security — Mass evacuation
- ISO 22320:2011 Societal security — Emergency management — Requirements for incident response
- ISO/CD 22322 Societal security — Emergency man.— Public warning
- ISO/WD 22323 Organizational resilience management systems – Requirements with guidance for use
- ISO/NP 22324 Emergency managament
- ISO/NP TS 22351 Disaster and emergency management
- ISO/NP 22397 Public Private Partnership
- ISO/CD 22398 Guidelines for exercises and testing
- ISO/PAS 22399:2007 Guideline for incident preparedness and operational continuity management
- ISO/IEC 27031:2011 Guidelines for information and communication technology readiness for business continuity
- ISO/IEC 24762:2008 Guidelines for information and communications technology disaster recovery services

BÖLÜM 3

STRATEJİ VE ANALİZ

3.1. İş Sürekliliği Politikası

İş sürekliliği kurumun stratejik hedefleri açısından çok önemlidir. Bir iş kesintisini başarıyla yönetemeyen bir kurum mevcut ve potansiyel müşterilerinin bir kısmını kaybetmeye mahkûmdur. İş sürekliliğini sağlayabilmek için fonksiyon bazında değil, süreç bazında yaklaşıp kuruma süreklilik kazandırmak gerekir. Bu da kurumun genelini etkileyen daha geniş bir çalışmayı işaret etmektedir. Bu bağlamda; kurumlar ve organizasyonlar, iş sürekliliği çalışmalarını daha etkin ve verimli yürütülebilmek için iş sürekliliği politikasına sahip olmalıdırlar.

İş Sürekliliği Politikası, "İş sürekliliği ilkesini ve iş sürekliliği ile ilgili yönetimin beklentilerini iletmek için hazırlanan uzun vadeli ve yaşam döngüsü odaklı yazılı bir üst yönetim belgesidir." şeklinde tanımlanabilir.[11]

İş sürekliliği politikasının amacı, bir organizasyonun iş sürekliliği programını resmileştirmek ve iş sürekliliği planının geliştirilmesi, korunması, egzersizi için kılavuz sağlamak olup bir iş kesintisi durumunda beklenmedik durumlara müdahale, organizasyonun iş ile ilgili operasyonları ve iş faaliyetlerinde kalıcı iyileşme sağlamak için gerekli temel ilkeleri ve çerçeveleri kurar.[12]

Pek çok kuruluş, bir organizasyon çapında iş sürekliliği politikası ihtiyacına şüpheci yaklaşmaktadır. Kilit rol ve sorumlulukları açıklayan yazılı bir İş Sürekliliği Politikası;[13]

- İş sürekliliği üst düzey yönetimi, iş sürekliliği programına katkıda bulunacak personel ve tüm diğer çalışanlar için açık beklentiler ve tüm organizasyon boyunca iletilerek, beklentileri ortak bir dizi sağlar.
- Değerli zamanın israf edilmesini önler. Örgüt kültürü ve örgütsel esneklik etrafında kurtarılabilirlik işlemleri için, tek bir basit ve tekrarlanabilir bir vizyon etrafında uyumla çalışmayı sağlar.
- Kuruluşun stratejisini operasyon ve diğer risk yönetim disiplinleri ile entegre ederek iş sürekliliği programı için en büyük düşman olan tutarsız yürütmeyi engeller ve program için tutarlı bir temel sağlar. İş sürekliliği programlarında kıyaslamanın

oldukça zor olduğu düşünüldüğünde; programın yetenekleri ve kuruluş genelindeki unsurları kıyaslanırken, ilerleme veya performansı değerlendirmek açısından iç yönetim programının incelenmesi için kriter olarak hizmet verebilir.

- İş sürekliliği programını kuruluşun hedefleri ile hizalayarak ölçülebilir bir kriter sağlar.

3.2. Mevcut Durum Analizi ve Tespiti

Kurum iş süreçlerinin ne kadar kesintiye tahammül edebildiği ve süreçleri tekrar çalışır duruma getirmek için neler yapılması gerektiğini tespit etmek amacıyla ayrıntılı mevcut durum analizi yapmalıdır.

Yapılacak iş sürekliliği çalışmaları bu analizin sonuçlarına ve çıktılarının değerlendirilmesi ile gerçekleştirilecektir.

Mevcut durum analizi yapılırken kurumun;

- İş Süreçleri,
- Yaşamsal Etkinlikleri,
- Önem ve Öncelikleri,
- Tedarikçi ve Müşterileri,
- İç ve Dış Bağımlılıkları,
- Mali Bağımlılıkları vb…

belirlenmelidir.[14]

Ayrıca, İş sürekliliği risklerinin ve tedavi planının hazırlanırken iş etki analizinin gerçekleştirileceği kritik süreçlerin, maksimum dayanılabilir kesinti sürelerinin ve hedeflenen kurtarma sürelerinin belirlenmesi gereklidir.

- BT altyapısının yedekli yapıda (sunucular, iletişim hatları, enerji v.b) olması hususunda neler yapıldığı,
- Kurumun hangi iş süreçlerinde, iş sürekliliğine yönelik hangi çalışmaların yapıldığı,
- Sunulan BT hizmetin kullanıcıları/müşterileri,
- Sunulan hizmetin aktarımı sırasında karşılaşılan tüm ara aşamalar belirlenir.

3.3. Risk Analizi

Risk “belirli bir tehdidin sistemin belirli bir zayıflığından faydalanarak sisteme zarar verme ihtimali”[15] veya “kurumun stratejik, mali ve operasyonel hedeflerinin gerçekleştirmesini engelleyecek, her türlü olayın gerçekleşme olasılığı”[16] şeklinde tanımlanabilir.

Zararın ortaya çıkma olasılığı yoksa risk de yoktur. Zararın ortaya çıkmasına neden olan etmenlerin tanımlanması risk analizi bakımından önemlidir. Zarara neden olabilecek etmenleri şöyle sıralayabiliriz;[17]

- Riske tabi olma (Kişisel zarar, mal zararı, sorumluluk zararı riski),
- Tehlikeler (Zararın yakın nedenleri),
- Riskler (Tehlikeden zarar ortaya çıkmasının arkasında yatan nedenler).

Risk analizi, risklerin ölçeklerinin ve önlem alınması gereken alanların belirlenmesi sürecidir.[15]

Bu süreçte belli ilkelere dikkat etmek gerekmektedir. Bunlar;[18]

- Riski azaltmak için yönetim anlayışının şeffaflığı benimsenmesi fayda sağlamaktadır.
- Risk analizinde önemli faktör kullanılan teknikler değil, riski değerlendirenlerin deneyimleridir. Dolayısıyla deneyimli yönetici ve danışmanlarla çalışma tercih edilmelidir.
- Neyi bilmediğini iyi anlamak önemlidir.
- Her tekniğin ve modelin varsayımlar üzerine kurulu olduğunu unutmamak ve bu varsayımları sorgulamak gereklidir.
- İşin farklı riskleri dengeli bir şekilde üstlenecek yapıda kurulmasına dikkat edilmelidir.
- Disiplinli bir yaklaşımla düzenli olarak kontrolün sağlanması önem taşımaktadır.
- Risklerle birlikte, getirilerin de düzenli olarak ölçülmesi ve takip edilmesi de iyi bir yönetim için gereklidir.

Risk analizi süreci kapsam belirlenmesi ile başlar. Belirlenen kapsamda bulunan varlıklar belirlendikten sonra, açıklıklar ve tehditler ile bunların oluşturacağı riskler belirlenir. Daha sonra risk değerlendirmesi ve derecelendirmesi yapılarak dokümante edilir. Son olarak alınacak önlemler belirlenir. Genel olarak Risk Analizi adımları aşağıdaki şekildedir:

3.3.1. Kapsam Belirlenmesi:

Kapsamın ilk aşamada doğru ve kurum hedeflerine uygun olarak belirlenmesi ileride gereksiz çaba harcanmasını önler ve risk analizinin kalitesini arttırır. Kapsamda risk analizine tabi her şey açık olarak belirlenmelidir. Örneğin risk analizinde dikkate alınacak tüm BT varlıkları (yazılım donanım gibi), personel, tesisler, operasyonlar açıkça belirtilmelidir.

3.3.2. Varlıkların Belirlenmesi:

Varlık, sistemin bir parçası olan ve kurum için değeri olan her şeydir. Varlık kurum için değer taşıdığından korunması gerekir. Bir BT sisteminde sadece yazılım ve donanımlar varlık olarak düşünülmemelidir. Bilgi, donanım, yazılım, haberleşme cihazları, dokümanlar, üretilen mallar, servisler, mali değerler, personel, kurumun prestiji / imajı da varlık olarak nitelendirilir.

3.3.3. Açıklıkların Belirlenmesi:

Açıklık, sistem güvenlik prosedürlerinde, tasarımda, uygulamada veya iç kontrollerde bulunan ve bilgi güvenliği ihlal olayına sebep olabilecek zayıflık, hata veya kusurlardır. Açıklıklar tek başlarına tehlike oluşturmazlar ve tehlike oluşturmaları için bir tehdidin mevcut olması gerekir.

3.3.4. Tehditlerin Belirlenmesi:

Tehdit, herhangi bir tehdit kaynağının kasıtlı olarak veya kazayla bir açıklığı kullanarak varlıklara zarar verme potansiyelidir. Tehdit kaynağı ise varlıklara zarar verme olasılığı olan olaylar ve durumlar olarak tanımlanabilir. En bilinen tehdit kaynakları doğal tehditler (Deprem, sel, toprak kayması, yıldırım düşmesi, fırtına gibi tehditler), çevresel tehditler (Uzun süreli elektrik kesintileri, hava kirliliği, sızıntılar vs.), insan kaynaklı tehditlerdir (İnsanlar tarafından yapılan veya yol açılan bilinçli veya bilinçsiz olaylar. Yanlış veri girişi, ağ saldırıları, zararlı yazılımların yüklenmesi, yetkisiz erişimler vs.). Tehdit değerlendirmesi sırasında hiçbir tehdidin küçümsenerek göz ardı edilmesi doğru değildir. Göz ardı edilen tehdit kurum güvenliğinde zayıflık yaratabilir.

3.3.5. Risklerin Belirlenmesi:

Tespit edilen açıklıklar ve tehditlerin oluşturacağı riskler belirlenir. Risk, açıklığın bir tehdit tarafından kullanılmasıyla oluşan ve tehdidin gerçekleşme olasılığı ile etki derecesidir. Riskler belirlenirken riske neden olan tehdit ve açıklıklardan yola çıkılmalıdır.

3.3.6. Risklerin Değerlendirilmesi:

Tespit edilen risklerin analizi ve derecelendirilmesi yapılmalıdır. Bu adım belirlenen risklerin yorumlanması olarak görülebilir. Riskin derecelendirilmesi veya değerinin belirlenebilmesi için öncelikle tehdidin gerçekleşme olasılığı ile etki derecesi hesaplanmalıdır. Bunlar sayısal değerler kullanılarak hesaplanabileceği gibi rakamlarla ifadenin zor olduğu durumlarda düşük, orta, yüksek gibi nitel değerlerle de belirlenebilir. Riskin kabul edilebilir olup olmadığı tespit edilmelidir. Tüm bu hesaplama ve değerlemeler uygulanmakta olan mevcut kontroller de dikkate alınarak yapılmalıdır. Kontroller risk değerini azaltabilir. Bu çalışmaların sonucunda "Risk Değerlendirme Dokümantasyonu" oluşturulur.

3.3.7. Önlemler:

Risk analizi sonucunda tespit edilen risklerin ortadan kaldırılmaları ya da hedeflenen kabul edilebilir seviyelere çekilebilmesi için iyileştirici önlemler alınmalıdır. Risk analizi sonuçlarına göre teknolojik yatırım, eğitim ihtiyacı veya personel ihtiyacı çıkabilmektedir. Kurumun özellikle iş sürekliliğini etkileyen riskleri bu çalışma kapsamında ortaya çıkarılmalıdır. Çalışma bir rapor haline getirilmelidir.

İş sürekliliği risk analizi çalışmasında;[19]

- İş süreçleri ve bu süreçleri oluşturan varlıklar belirlenir.
- Varlıkların taşıdığı risklerin belirlenmesi amacı ile varlıkta bulunan açıklıklar ve bu açıklıklar vasıtasıyla iş süreçlerine zarar verebilecek tehditler belirlenir.
- İş süreçlerinde kesintiye veya veri kaybına neden olabilecek riskler iş sürekliliği kapsamında dikkate alınarak belirlenir. Fiziksel ve çevresel riskler de ayrıntılı olarak değerlendirilir.
- Risk değerlendirme ve derecelendirmeleri yapılır.
- Risk iyileştirilmesi için öneriler ve önlemler belirlenir.
- Risk analizi sonuçlarına göre teknolojik yatırım, eğitim, personel v.b. ihtiyaçları da belirlenir.

Kurumun iş sürekliliği kapsamında yapılan risk analizi çalışmaları ile iş etki analizi çalışmaları birleştirilerek iş sürekliliği stratejilerini geliştirmekte kullanılır.

3.4. İş Etki Analizi

İş Etki Analizi (İEA), Kurumların mevcut durumdaki iş süreçlerinin incelenerek olası kesintilerin ve bunların her türlü etkilerinin analiz edilmesi olarak tanımlanabilir.

Kurumların iş sürekliliği çalışmalarının önemli bir bileşenini oluşturan İEA, kritik iş süreçlerinin belirlenmesi sonrasında bu süreçleri etkileyebilecek tehditler ile süreçlerde oluşacak ürün ve hizmet kesintilerinin yol açacağı zararların belirlenmesini hedeflemektedir.

İş sürekliliği kesintileri bir kuruma finansal zararların yanında itibar kaybı gibi doğrudan finansal olmayan zararlara da yol açabilmektedir. Kritik hizmetlerin sunulmasında oluşacak kesintinin süresi kuruma ne kadar para kaybı, ne kadar itibar kaybı olduğunu ve sektördeki konumuna etkisinin boyutunu gösterecektir.

İş sürekliliği yönetimi çerçevesinde varlıklarını ve süreçlerini belirleyen kurum, süreçlerini veya faaliyetlerini hataya dayanaklılık açısından önceliklendirir. Kısa süreli bir zaman dilimi içinde kesintisi en yüksek zarara yol açan ve çok kısa süre içerisinde hatadan kurtulması istenen faaliyetler "Kritik Faaliyetler" olarak adlandırılmaktadır. Bu faaliyetler temel olarak kurumun ana ürünleri veya hizmetlerini kapsamaktadır. Yüksek öncelik verilen Kritik Faaliyetler kurumun iş sürekliliği açısından temel olarak odaklanacağı, daha yüksek bütçe ayrılacağı ve planlama yapacağı faaliyetlerdir. Diğer faaliyetler de öncelik derecelerine ve maksimum kabul edilebilir kesinti sürelerine göre değerlendirilmelidir.

Kurumun kritik faaliyetleri başta olmak üzere hizmet kesintisi kuruma zarar verecek faaliyetler için maksimum kabul edilebilir kesinti süresi (İng. Maximum Tolerable period of disruption, MTPoD) belirlemelidir. MTPoD belirlenmesi aşamasında dikkate alınacak hususlardan önemlileri aşağıdadır:[20]

- Kesinti başladıktan sonra faaliyetin tekrar başlaması için ihtiyaç duyulan maksimum süre,
- Faaliyetin kesinti sonrası tekrar başlaması için ihtiyaç duyulan minimum performans seviyesi,
- Faaliyetin kesinti sonrası normal performansına ulaşması için gerekli olan süre.

Faaliyetlerin belirlenen MTPoD değerleri bu faaliyetlerin Hatadan Kurtulma Zaman Hedefi (eng. Recovery Time Objective, RTO) ile Hatadan Kurtulma Noktası Hedefi (eng. Recovery Point Objective, RPO) değerlerinin belirlenmesine katkıda bulunmaktadır. RTO, kesintinin yol açacağı zararı minimum seviyede tutmak için gerekli en düşük zaman hedefini koyarken, RPO bu zaman dilimi içerisinde oluşacak maksimum kabul edilebilir veri kaybı hedefini göstermektedir.

İEA ile kurum yukarıda belirtilen kritik faaliyetlerini gerçekleştirme sürecinde oluşan kesintilerin olumsuz etkileri rakamsal büyüklüklere çevrilmesi amaçlanmıştır.

Faaliyet kesintisinin yol açabileceği etkileri belirlerken dikkate alınabilecek hususlar şunlardır:

- Kurum çalışanları ve kamu yararı üzerindeki etkiler,
- Yerleşke, teknoloji ve veri üzerindeki etkiler veya kayıplar,
- Yasal yükümlülüklerin yerine getirme kapsamında oluşan olumsuz etkiler,
- Kurum itibarının zarar görmesi,
- Mali kapasitenin zarar görmesi,
- Ürün ve servis kalitesinde kötüleşme,
- Çevresel zararlar.

Ek olarak, kesinti süresi ile kesintinin yol açtığı zarar çoğunlukla doğru orantılı olmayıp, kesinti süresi artıkça etkisinin kapsama alanı da dâhil olmak üzere farklı boyut ve hızda olacağı göz önünde bulundurulmalıdır. Bu etkiler kesintinin meydana geldiği saat, gün, ay, yıl veya iş yaşam döngüsünde bulunulan noktaya göre farklılıklar gösterebilmektedir.

İş sürekliliği kapsamında gerçekleştirilen İEA adımları kurumun özelliklerine göre farklılıklar gösterebilmektedir. G. Wrenn bu çalışma için 10 aşamalı bir yaklaşım sunmaktadır:[21]

i. Çalışma için üst yönetimden onay alınması,

ii. Kurumun ana iş süreçlerinden sorumlu yöneticiler ile başlangıç toplantısı gerçekleştirimi ve çalışmanın amaçları, zaman tablosunu ve üretilecek belgeler hakkında bilgi verilmesi,

iii. Söz konusu yöneticilere iş etki analizi anketi uygulayarak bilgi ve veri toplanması,

iv. Kurumun yıllık toplam gelir ve karının mümkün olduğunca iş birimleri bazında belirlenmesi. Bu veriler bir iş süreci için kabul edilebilir üst zarar limitini ortaya çıkaracaktır.

v. Toplanan verilerin birim yöneticileri ile gözden geçirilmesi ve son haline getirilmesi,

vi. Verilerin elektronik tablo veya veritabanında birleştirilerek raporlama ve analiz için uygun hale getirilmesi,

vii. İlgili birim yöneticileri ile "İEA gözden geçirme ve önceliklendirme toplantısı" düzenlenmesi ve her bir sürecin birbiriyle olan bağlantılarını da göz önüne alarak "kritik", "orta" veya "düşük" olarak önceliklendirilmesi,

viii. Her bir süreç için Hatadan Kurtulma Zaman Hedefi (RTO) belirlenmesi,

ix. RTO'ları küçükten büyüğe doğru sıraladıktan sonra her bir süreç için Hatadan Kurtulma Noktası Hedefi (RPO) belirlenmesi,

x. Son olarak üst yönetime çalışma sonucunun sunulması. Bu sunumda kritik süreç ve faaliyetlerin önemi RPO, RTO MTPoD bilgileri ve finansal etkileri ile birlikte vurgulanmalıdır.

Sonuç olarak, süreçler üzerindeki potansiyel tehditlerin ve risklerin de beraber değerlendirilmesiyle ortaya çıkarılacak İEA raporu kurum iş sürekliliği planlarının ve modellerinin oluşturulmasına kritik öneme sahip girdiler sağlamaktadır.

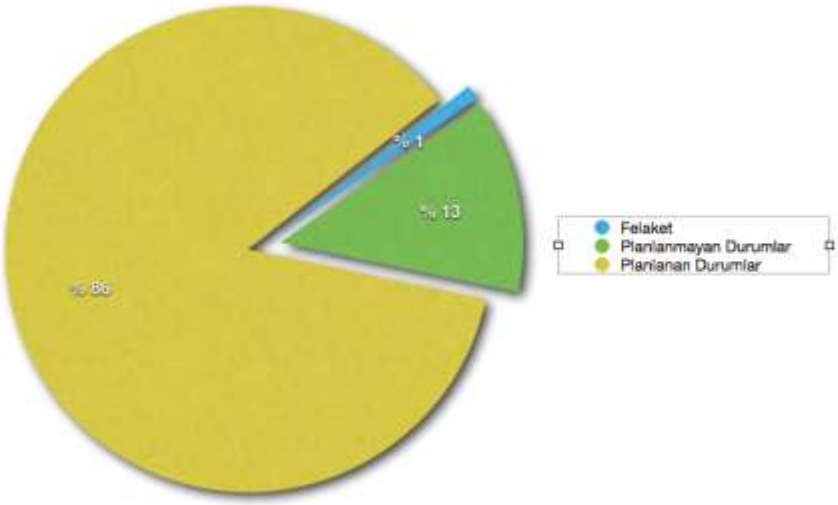
Özet olarak İş sürekliliği iş etki analizi çalışmasında;

- Kritik iş süreçleri ile bu süreçleri etkileyen hizmet ve faaliyetler belirlenir.
- İş süreçlerinde oluşabilecek kesintilerin etkileri belirlenir.
- Her bir süreç için maksimum kabul edilebilir kesinti süreleri(MTPD) belirlenir.
- İş süreçleri, hizmet ve faaliyetlerin bağımlılıkları belirlenir.
- Mevcut teknolojik altyapının belirlenen maksimum kabul edilebilir kesinti süresi değerlerini sağlamada eksik kalan yanları tespit edilir ve teknolojik yatırım gereken alanlar belirlenir.
- İş süreçlerinde kesintiye neden olabilecek riskler, risk analizi gerçekleştirilerek belirlenir ve yüksek risk teşkil eden risklerin düşürülmesi için uygulanması gereken önlemler belirlenir.

3.5. Beklenmedik Durum Senaryoları

Beklenmedik durumlar sadece doğal tehditler sonucu oluşmamaktadır. Doğal, insan kaynaklı ve çevresel tehditlerin tamamı beklenmedik durumların oluşmasına sebep olabilmektedir.

Örneğin veriye ulaşmayı engelleyen doğal olaylar işin sürekli olmasını engelleyen olaylar arasında %1 den azını oluşturmaktadır. Aşağıdaki şekilde iş sürekliliğinde veriye ulaşmayı engelleyen olayların dağılımı verilmiştir;[22]



Şekil 4: İş Sürekliliği Veriye Ulaşmayı Engelleyen Faktörler

Araştırmalara göre beklenmedik bir durumla karşılaşmış, firmaların her beş tanesinden ikisinin faaliyetlerini sürdüremediği, sürdürebilenlerden üç tanesinden birinin iki yılsonunda faaliyetini durdurduğu ortaya çıkmıştır. Bu tür durumlarda kaybedileni ölçmek zor olmaktadır. Yapılan bir kısım ölçümlere göre felakete uğramış bir şirketin bir saatte uğrayacağı kayıp, kargo şirketinde 28 bin USD iken, bu değer bir menkul değerler firmasında 6 milyon USD yi bulabilmektedir:[23]

Beklenmedik durumlar, yaşamsal alanların tamamen çökmesine, kurum ve kuruluşların müşterilere, karşı taraflara ve yasa koruyucu ve düzenleyicilere karşı hizmet ve sorumluluklarının kesintiye uğramasına neden olmaktadır.

Amerika'da yaşanan 11 Eylül olayı, depremler, sistem çökmeleri gibi beklenmedik durumlar ve sonrasında yaşanan sıkıntılar Dünyada ve Türkiye'de beklenmedik durumlar için önlem almanın önemini gözler önüne sermiştir.

Ancak, EMC'nin hazırladığı, İngiltere, Almanya, Fransa, İtalya, İspanya, Belçika, Hollanda, Lüksemburg ve Rusya'dan oluşan 9 ülkede toplam bin 750 BT yöneticisi ile yaptığı anketten oluşan bir rapora göre hala şirketlerin ve kamu kuruluşlarının yaklaşık dörtte üçü, olası bir BT krizinin ardından bilgisayar sistemlerini veya verilerini tam olarak düzenleyemeyecek durumdadır. Araştırma, şirketlerin yüzde 74'ünün ağlarını tam olarak toparlayabilecekleri konusunda kendilerine çok güvenmediğini ortaya koymakta, katılımcıların yüzde 54'ü 1 yıl içinde veri kaybettiğini veya sistemlerinde çökme ile karşılaştığını kabul etmektedir:[23]

Bu bağlamda hayati bir kayıp yaşamamak için olası kurumun karşı karşıya kalabileceği beklenmedik durumlar için senaryolar oluşturulmalıdır. İş etki ve risk analizleri sonucu öncelik sırasına göre oluşturulacak bu senaryolarla önemli olayların gerektirdiği başarılı mücadele yöntemleri tespit edilecek, iş kurtarma planlarının temelini oluşturulacaktır.

Tipik bir beklenmedik durum senaryosu tüm kritik iş fonksiyonları için oluşabilecek herhangi bir potansiyel tehdit ve potansiyel kötü sonuçlarını içerecektir. Bir kurum için bir senaryo hazırlanabileceği gibi, sadece bir birimi ilgilendiren spesifik bir senaryo da oluşturulabilir:[24]

BT için beklenmedik durum senaryosu oluşturabilmek için aşağıdaki her farklı bileşen için tahmin edilebilir beklenmedik durum senaryo başlıkları belirlenmelidir;

- Deprem, sel vb doğal afet kaynaklı beklenmedik durumlar
- Hizmet sağlayan şirket, kurum vb kaynaklı beklenmedik durumlar
- BT sistem merkezleri kaynaklı beklenmedik durumlar
- BT sunucu merkezleri kaynaklı beklenmedik durumlar
- BT network sistemleri kaynaklı beklenmedik durumlar
- Personel veya dış kaynağı bağımlılığı nedeniyle oluşan beklenmedik durumlar

Bu durumlarda şirketin bilgi sistemlerinde planlanmayan bir hizmet kesintisi olması durumunda, yedek sistemlerin devreye alınması için izlenmesi gereken adımlar ise aşağıda yer almaktadır.

- Bilgi İşlem merkezinde bulunan sistemlerin veri yedekleri dönemsel olarak yedeklenir,
- Planlanmayan uzun süreli bir kesinti meydana gelmesi durumunda bilgi işlem sorumlusu problemin nedeni ve sistemlerin durumu hakkındaki bilgiyi ilgili kişilere, birimlere ve beklenmedik durum sorumlusuna bildirir,
- Acil ve beklenmedik durum sorumlusu ve/veya bilgi işlem sorumlusu, acil ve beklenmedik durumun içeriğine göre gerekiyorsa toplantı yeri ve zamanını belirler,
- Acil ve beklenmedik durum sorumlusu, Bilgi İşlem birimi ile müzakere ederek kesintiye sebep olan sorunu ve çözüm yöntemini belirler,
- Acil ve beklenmedik durum sorumlusu ve/veya bilgi işlem sorumlusu gerektiği takdirde tedarikçi firmalar ve müşteriler ile temasa geçilmesi ve durumdan haberdar edilmesini sağlar.

3.6. İş Sürekliliği Stratejisinin Geliştirilmesi

Risk değerlendirmesi, kontrolü ve iş etkilenme analizi aşamaları tamamlandıktan sonra, sonraki aşama, iş sürekliliği stratejilerini geliştirmektir. Bu stratejiler, önemli olayların gerektirdiği başarılı mücadele yöntemlerini tespit edecektir. Bu stratejiler, kurumun ve aktiflerinin değerleri ile kritik kurum fonksiyonlarının sürekliliğinin sağlanması için gereken maliyeti mukayese ederek dengede tutmalıdır. Aşağıdaki sorulara verilecek cevaplar bu stratejilerin temelini teşkil edecektir:[25]

- Her şeyden önce, felaketin meydana gelmesi riskini azaltmak için ne yapabiliriz?
- Bizim asgari ihtiyaçlarımız kesin olarak nelerdir ve bunlara ne kadar süratle erişebiliriz?
- İstenilen şeyleri daha büyük süratle elde etmek için daha büyük masraflara katlanmanın gerekebileceğini göz önünde tutarak ne kadar para harcayabiliriz?

Faaliyetlerini çeşitli sebeplerle durdurma tehlikesi oluşturan durumların değerlendirerek, bu değerlerin, kurtarma alternatifleri, riski azaltma ve sigortalama maliyetleri ile karşılaştırılması gerekir. Bu aşamanın sonuna gelmeden daha birçok konuya değinmek gerekecektir:[25]

- Kurtarma ekibinin yapısının ve her bir ekip üyesinin ve departmanın görev ve sorumluluklarının tespiti
- Tüm planın başına bir plan koordinatörü tayin edilmesi
- Münferit planların ortaya konmasını yönetecek olan yöneticilerin tayini aralarında uyum ve koordinasyon sağlanması
- Kurtarmanın yürütülüp yönetilebileceği, üslerin bulunacağı yerleşkelerin tespiti. Buna kumanda merkezleri, geçici büro sahaları ve bilgisayar desteği verecek yerler dâhildir.
- Yeniden yerleşmenin süresini tayin eden zamanlamanın yapılması
- Bu planları destekleyecek olan ekiplerin asgari kaynak ihtiyacının tespiti.

3.7. Planlama İçin Temel İlke ve Yöntemler

İş sürekliliği analizi ve kurumsal iş süreklilik politikasına göre iş sürekliliği stratejisi belirlenmelidir. Bu strateji kapsamına bir sonraki bölümde anlatılacak planlama ilkeleri ve yöntemleri ortaya çıkarılmalıdır.

Planlama, önceden belirlenmiş amaçları gerçekleştirmek için yapılması gereken işlerin saptanması ve izlenecek yolların seçilmesidir. Planlama, geleceğe bakma ve olası seçenekleri saptama sürecidir yani geleceği düşünmedir. Özetle planlama, bir eylemle ilgili tüm etkinliklerin önceden hazırlanması sürecidir. Bu tanımlarda planlamayla ilgili olarak dikkat çeken ortak nokta, planlamanın geleceği bugünden görme ve kontrol etme aracı olmasıdır. Planlamayı ekonomik anlamda bir kaynak dağıtım mekanizması olarak da görmek mümkündür. Bu açıdan baktığımızda, planlama sınırsız ihtiyaçlar ile sınırlı kaynaklar arasında bir dengeyi sağlama mekanizmasıdır.

Geleceği yönetme ve kaynakları dağıtma aracı olan planlama neyin yapılacağının, nasıl yapılacağının, ne zaman harekete geçileceğinin, bütün bu çalışmalarda kimlerin sorumlu olacağının belirlenmesi ve saptanması sürecidir.

BÖLÜM 4

PLANLAMA

4.1. İş Sürekliliği Yönetimine Genel Bakış

İş Sürekliliği Yönetimi, bir felaket sonrasında operasyonların kesintiye uğraması sonucu, şirketlerin kritik iş süreçlerinin sürekliliğini sağlamayı amaçlayan planlar bütünüdür.[26]

Kurumların kritik iş süreçlerinin devamlılığını sağlamak ya da kesinti durumunda yeniden çalışır hale getirmek için gerçekleştirilen iş sürekliliği çalışmaları, İSYS(İş Sürekliliği Yönetim Sistemi) olarak adlandırılan süreçler bütünü çerçevesinde devam ettirilmelidir.[27]

İş Sürekliliği Yönetiminin Amacı;

- Beklenmedik durum ve iş sürekliliği planlama ve yönetimi stratejisi, organizasyonu ve sürecinin değerlendirmesi ve iyileştirilmesi,
- Beklenmedik durum ve iş sürekliliği planlamasının BT risk değerlendirmesi ve iş etki analizi ile uyumlu hale getirilmesi,
- Beklenmedik durum ve iş sürekliliği planlamasının iş hedefleri ve gereklilikleri ile uyumlu hale getirilmesi,
- BT yapısı için Beklenmedik Durum Planı hazırlanması veya iyileştirilmesi amacıyla yönlendirme,
- İş operasyonları için kriz yönetimi ve iletişim planları dâhil olmak üzere İş Sürekliliği Planlarının hazırlanması veya iyileştirilmesi amacıyla yönlendirme,
- Beklenmedik durum ve iş sürekliliği planları için test senaryolarının hazırlanması,
- Beklenmedik durum ve iş sürekliliği planları testlerinin gerçekleştirilmesi esnasında destek verilmesi,
- Beklenmedik durum ve iş sürekliliği yapısı dâhilinde görev ve sorumlulukların tanımlanmasıdır.

Yönetim sistemi bulunmayan kurumların karşılaşacağı tehditler şunlardır:[28]

Şekil 5: Kurumların Karşılaşacağı Tehditler

İş Sürekliliği Yönetim Sistemi kurulumu konusunda sıkça karşılaşılan hatalı yaklaşımlar ise dört ana başlıkta incelenebilmektedir;[29]

- İş sürekliliğinin bir ürün, teknoloji veya servis olarak görülmesi: İş sürekliliği, sadece verilerin başka bir çalışma alanına çevrim içi aktarılması veya kritik sunucuların devamlı olarak çalışmasını sağlamak üzere kümeleme (cluster), RAID, yedekli güç kaynağı, yedekli ağ hatları kullanmak olduğu düşünülmemelidir. İş sürekliliği kurum süreçlerinden hareketle süreçlerin devamlılık ihtiyaçlarının ortaya koyulması ve bunun sağlanması için gereken çalışmaların yapılmasıdır.
- Başlangıcı ve sonu belirli olan bir proje olarak düşünülmesi: İş Sürekliliği Yönetim Sistemi (İSYS) kurulumu yeterli bilgi birikimi olduğu durumda kurumun kendi kaynakları ile yapabileceği bir çalışmadır. Birçok kurumda söz konusu bilgi birikiminin olmaması nedeni ile bu konuda dış kaynak kullanımı yoluna gidilmektedir. Bu çalışmalar genellikle bir proje olarak değerlendirildiği için İSYS'ye de proje gözüyle bakma yanlışı söz konusudur.
- İş sürekliliği sorumluluğunun BT bölümü olduğunun düşünülmesi: İş sürekliliğinin sağlanmasında bilgi teknolojilerinin rolünün yüksek olmasından dolayı çalışmaların BT bölümü tarafından yapılması ve sorumluluğunun da BT bölümünde olması gerektiği inanışı yaygındır. İstatistikler iş sürekliliği çalışmalarına BT bölümünün katılımının diğer birimlerden fazla olduğunu göstermektedir. Öbür yandan iş sürekliliği sorumluluğunun çok yüksek oranda üst yönetim, yönetim kurulu veya iş sürekliliği komitesinde olduğu görünmektedir. İş süreçlerinin devam ettirilebilmesi veya olağan üstü bir durumda tekrar çalışır hale getirilmesi, personelin

alternatif çalışma ortamına naklinden, sunucuların hazırlanmasına, yeni cihaz satın alımına kadar birçok faaliyeti içermektedir. Bu sebeple iş sürekliliği kurum içinde mümkün olduğu kadar üst seviye yönetim tarafından temsil edilmeli ve tüm çalışma grupları ile birlikte çalışarak iş sürekliliğini sağlayacak bir iş sürekliliği organizasyonu kurulmalıdır.

- İş sürekliliği sorumluluğunun BT bölümünde olduğu düşüncesinin temelinde yatan bir diğer neden ise iş sürekliliği ile felaketten kurtarma kavramının karıştırılıyor olmasıdır. Felaketten kurtarma çalışmalarının kapsamında sadece BT sistem ve servislerinin kesinti durumunda ayağa kaldırılması yer almaktadır. İş sürekliliği kavramı ele alınacak olursak, tüm çalışmaların temelinde kurumun iş süreçleri düşünülmektedir. Felaketten kurtarma merkezi kurulumu, felaketten kurtarma planı ve prosedürlerinin hazırlanması BT bölümünün sorumluluğundadır. Bu çalışmalar iş sürekliliği için gerçekleştirilmesi gereken tüm çalışmaları içermemektedir. Bu bakış açısı ile felaketten kurtarma çalışmaları iş sürekliliğinin bir alt parçası olarak ele alınmalıdır.
- Sadece dokümantasyondan oluştuğu varsayımı: Bir diğer yanlış ise iş sürekliliğine sadece dokümantasyondan oluştuğu varsayımı ile yaklaşmaktır. Dokümantasyon, iş sürekliliğinin vazgeçilemez bir parçası olmasına rağmen yapılması gereken tüm işleri dokümantasyon olarak ele almak, çalışmanın teknolojik ve organizasyon boyutlarını gözden kaçırmaya, dolayısıyla iş sürekliliğinden beklenen faydanın sağlanamamasına neden olacaktır. Teknolojik altyapının ihtiyaçların üzerinde olması durumunda dahi tatbikatların yapılması, eğitimlerin verilmesi ve çalışmaların periyodik olarak gözden geçirilmesi ve benzeri birçok çalışma vardır.

4.1.1. Yönetişim

İş Sürekliliği Yönetimi Kurumsal Yönetişimin temel bir parçası olarak görülmektedir. Yönetim Kurulunun ve üst düzey yönetimin sorumluluğu olarak da tanımlanabilir. Temel hedef, İş Sürekliliği Yönetimi'ni güçlü organizasyonel yapı ve uygun politika ve prosedürlerle kurum kültürünün parçası haline getirebilmektir.[29]

İş Sürekliliği Yönetiminde Başarılı Yönetişim;[30]

- Karmaşık kurum organizasyonu içinde İSY sorumlulukları netleştirilmeli, paydaşlar kendilerinden beklentileri net olarak anlamalıdırlar.
- Üst Yönetim doğrudan hesap verebilir konumda olmalıdır, gerekli kaynak ve bütçe tahsisinin yapılması sağlanmalıdır.

- Merkezi koordinasyon ile proje yönetimi gerçekleştirmeli, gerek kurum içinde gerekse yasal otoritelerle tek kanaldan iletişim sağlanarak karışıklık önlenmelidir.
- İSY'nin kendini güncelleyecek kuralları oluşturması ve bunun kurumun yaşayan bir mekanizması haline getirilmesi etkin yönetişim ile sağlanacaktır.

Etkin Yönetişim Modelinde Yönetişim Yaklaşımı İş Sürekliliği Yönetişim Kararları şu şekilde özetlenebilir;[30]

Politika

- İSY'nin temel işleyen kuralları neler olmalıdır?
- Hangi dahili İSY standartları, kuralları ve protokolları gereklidir?

Liderlik

- Kurumda işin ve ilgili BT'nin yönü nedir?
- Risk yönetimine ilişkin kültürel değerler nedir?
- Kritik hissedarlar nasıl temsil edilmelidir?

1. Gözlem & Kontrol

- Niteliksel karşılaştırma nasıl yapılmalıdır? (Benchmarking)
- Periyodik İSY ilerleme raporu nasıl oluşturulmalı ve gözden geçirilmelidir.
- Kritik bulguları gidermek üzere hangi düzeltici önlemler alınmalı?
- Organizasyon düzeltici önlemlerin alındığından nasıl emin olmalı?

2. Planlama

- Kurumsal iş kurtarma stratejisi neler içermelidir?
- Kurumsal BT kurtarma amaçları neler olmalıdır?
- İSY programı yönetimi nasıl ölçülmeli?

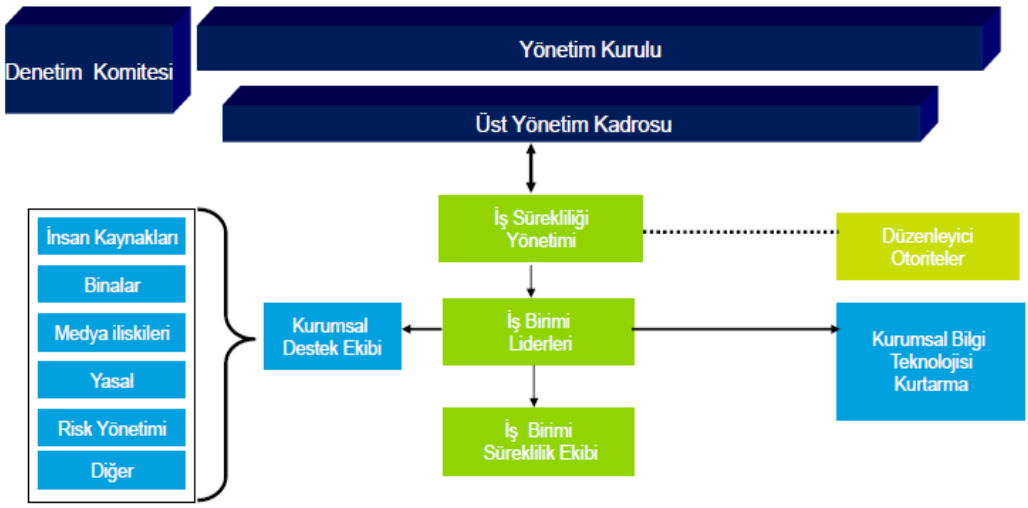
3. Bütçe Ayrılması

- Limitli kaynaklar etkili bir şekilde nasıl ayrılmalı?
- Yatırım için ne kadar kaynak var?
- İSY yatırım kararlarını belirlemek için hangi kriterler kullanılmalıdır?
- Harcamaları gözden geçirmek için nasıl bir süreç kullanılmalı?

4. Koordinasyon & Uygunluk

- İSY standartlarının ve yükümlülüklerinin uyumunu sağlamak için nasıl bir süreç uygulanmalı?
- Kurumsal İSY kurum iş birimleri arasında kurtarma aktiviteleri konusunda nasıl bir koordinasyon sağlamalıdır?

Bu çerçevede olması gereken yönetişim yapısı ise aşağıda gösterilmiştir;[30]



Şekil 6: Yönetişim Yapısı

4.1.2. Görev ve Sorumluluklar

Beklenmedik durumlara müdahale amaçlı olarak özel müdahale ekipleri oluşturulmalı, Kurum içi ve kurum dışında karşılaşılan teknoloji sorunları, iletişim sorunları, bilişim saldırılarına yönelik olarak özel ekipler oluşturularak sorumluluk alanları ve ekip üyeleri belirlenmelidir. Ayrıca her ekibin görevleri, müdahale planlarının ilgili yerlerinde net çizgilerle tanımlanmalıdır.

Oluşması muhtemel tüm acil durumlar için ayrı müdahale planları hazırlanmalı, her müdahale planı, sorumlu ekipler, görev tanımları ve görev adımları net olarak ifade edilmelidir.

Hazırlanan yönergeler doğrultusunda tanımlanmış ekiplerin hangi durumlara doğrudan müdahale edebileceği, hangi durumlarda ise dış ürün/hizmet sağlayıcı kurum ile irtibata geçeceği tanımlamalıdır.

4.1.2.1. Üst Yönetim

İş sürekliliği çalışmaları için en yüksek seviyede yönetim onayı ve desteğinin alınması şarttır. Gerçekleştirilen çalışmalar ile ilgili yönetim onayı alınması,

çalışmaların kurum çapında kolay kabul edilmesini sağlayacaktır. BS 25999 standardı üst yönetimin iş sürekliliği sürecine katılımının İSYS'nin doğru olarak anlaşılması, desteklenmesi ve organizasyon kültürüne adaptasyonu için anahtar bir adım olduğunu belirtmektedir. Üst yönetim desteği sadece politika ve benzeri dokümantasyonun onaylanması biçiminde olmamalıdır. Çalışmaların gözden geçirildiği toplantılara katılmak, tatbikat sonuçlarını incelemek, bazı bilgilendirme notlarının veya çalışma sonuçlarının bizzat yönetim tarafından bildirilmesi konunun öneminin anlaşılması açısından faydalı olacaktır. Üst yönetim desteği ayrıca gerekli iş gücünün ayrılması, ihtiyaç duyulan bütçenin tahsis edilmesi gibi konular içinde oldukça önemlidir.[31]

Üst düzey yöneticileri Yönetim Kuruluna karşı sorumlu olup sorumlukları şunlardır;[30]

- Öncelikleri belirleme
- Bütçe Tahsisi
- Politika belirleme
- Yaklaşım onaylama

4.1.2.2. İş Sürekliliği Yönetimi Program Ofisi / İş Sürekliliği Yöneticisi

İş Sürekliliği Yönetimi Program Ofisi / İş Sürekliliği Yöneticisi sorumlulukları şunlardır[31]:

- Etkin iş süreklilik programı sağlar Başlıca stratejik riskin belirlenmesi ve çözümlenmesini kolaylaştırır.
- Risk için süreçleri geliştirir ve kurumsallaştırır
- Riskleri belirlemek için iş birimleri arasında iletilişimi kolaylaştırmak
- Objektif gözden geçirmeyle sponsorlara raporlama yapmak
- Risk planlamasının kalitesini sağlamak
- Tüm İSY çıktılarından final sorumluluğudur
- Üst yönetim ile çalışarak İSY stratejisini kurumun stratejisini ile uyumlandırır
- Yönetim kuruluna iş sürekliliği ile ilgili açık konuların raporlanmasını ve gözlemlenmesini sağlamak
- Düzenleyiciler ve yasal zorunluluklarla ilgili raporlama yapmak
- İSY test takvimi belirlemek
- İş süreklilik stratejilerini geliştirmek, gözden geçirmek ve onaylamak

- İş süreklilik politika ve prosedürlerini geliştirmek, gözden geçirmek ve onaylamak
- İş süreklilik politika ve prosedürlerinin uygulanmasını ve uyumunu sağlamak
- İSY girişimlerini önceliklendirmek
- İSY politika ve prosedürlerinin hayat döngüsünü yönetmek
- İSY farkındalık ve eğitim programını yönetmek

4.1.2.3. İş Birimi Yöneticileri

İş Birimi Yöneticileri sorumlulukları şunlardır:[30]

- Sürekli olarak riskleri önceden belirlemek ve yönetmek
- İlgili riskler için bütünsel İSY planlarını oluşturmak ve güncellemek
- İlerleme ve aktiviteleri İSY proje yönetim ofisi (PMO) ile paylaşmak
- İş süreklilik politikası ve standartlarının uygulamasından ve yasal düzenlemelere uyumdan sorumlu olmak
- Kriz sırasında çalışmayı sağlayabilmek için iş kurtarma planlarını uygulamak
- İş biriminin iş sürekliliği faaliyetleri ve kaynakları için bütçelemeyi onaylamak ve öncelik vermek
- İş kurtarma planlarını onaylamak
- İş biriminin kurtarma önceliklerini belirlemek
- Departmanın iş sürekliliği programının yönetimi için yeterli personel sağlamak
- Risk değerlendirmesinin onayını ve iletilmesini sağlamak
- İş süreklilik politikasından sapma olduğu durumlarda risk kabulünü sağlamak.
- İşleri için iş sürekliliği eğitimini ve farkındalık programlarını gözlemlemek

4.1.3. Dokümanlar

Her yönetim sisteminde olduğu gibi İSYS içinde dokümantasyon çok önemlidir. İş sürekliliği planının, olağan üstü durum yönetim planının ve bu planlarla ilgili diğer talimat ve prosedürlerin hazır ve güncel olması gereklidir. Dokümanların hazır olması yanında ilgili kişilere dağıtımı da yapılmalıdır. Dokümantasyonun hazırlanması aşamasında sadelik ve kolay uygulanabilirlik çok önemlidir.[31]

İş Sürekliliği Yönetim Sistemi için hazırlanması gereken dokümanlara ait örnek liste aşağıda verilmiştir;[31]

- İş sürekliliği politikası

- İSYS kapsam dokümanı
- İş sürekliliği rehberi
- Uygulanabilirlik bildirgesi
- İş sürekliliği planı veya planları
- İş sürekliliği Olay yönetim / müdahale planı
- İş kurtarma planları
- İş etki analizi dokümantasyonu
- İş sürekliliği risk değerlendirme dokümantasyonu
- Yıllık tatbikat programı

4.1.3.1.İş Sürekliliği Planı

İş Sürekliliği Planlaması, "İş hacmini, kabul edilebilir bir seviyede tutmak için gerekli olan iş süreçlerini ve kaynakları tanımlamak ve muhafaza etmek; işlerin kötüye gittiği zamanlarda, kaynakları korumak ve kuruluşun ayakta kalmasını güvenlik altına almak için bir takım prosedürler oluşturmak." şeklinde tarif edilebilir.[25]

Bir organizasyonun felaket durumlarının yanı sıra, olağan günlük operasyonların düzenlenmesinde de büyük önem taşıyan İş Sürekliliği Planı, sadece olağanüstü haller ve durumlarda değil günlük süreçlerin iyileştirilmesine de katkı sağlar. İş sürekliliği sadece risklerin yaşanması sonrası kalanı kurtarmaya odaklanmaz, risklerin en az düzeyde gerçekleşmesini ve riskler gerçekleşse bile en az iş etkisiyle yolunuza devam etmeyi amaçlar.[32]

Günümüzde, her kuruluşun tüm yaşamsal süreçlerini kapsayan bir İş Sürekliliği Planı olmalıdır. Çünkü;[33]

- Kuruluşların kapanma ya da zarar görme nedenlerinin başında yaşamsal süreçlerindeki kesintiler gelmektedir.
- Kuruluşların birbirlerine olan bağımlılıkları da İş Sürekliliği planlarını zorunlu hale getirmektedir.
- Yakın bir gelecekte, İş Sürekliliği Planı bulunmayan şirketler uluslararası ya da ulusal ilişkilerinde ciddi sorunlar yaşayacaklardır.
- Diğer kuruluşlarla iş ilişkisi olan kuruluşlar, sözleşmelere İş Sürekliliği Planı önkoşulu koymaya başlamışlardır.

Etkili bir İş Sürekliliği Planı bulunmadığı hallerde, aşağıdaki riskler ve durumlarla karşılaşılabilir;[25]

- Mevcut müşterilere hizmet vermeyi imkânsız hale getiren iş kesintileri meydana gelebilir. Bu durum ise müşteri kaybı, itibar kaybı, rekabet gücünün kaybı gibi etkilere sebep olabilir.
- Alacakların takip edilememesi, geç ödemelerden kaynaklanan cezalar, kaçırılan indirim olanakları, hesap bakiyelerinin güncel hale getirilememesi, kaybedilmiş veya kayıt dışı kalmış satışlar olabilir.

İş Sürekliliği Planı bir İş Sürekliliği Projesi ile oluşturulur. Proje bu planın sürekli olarak güncellenme mekanizmasını da kurar. Plan belirli aralıklarla sınanır. İş Sürekliliği konusundaki yazılımlar, planlar oluşturulurken yardımcı araçlardır, tek başlarına bir anlamları yoktur. İş Sürekliliği planları otomatik olarak oluşturulamamakta, her kuruluş için ayrı yapılara sahip olmaktadırlar. Bir kuruluşun İş Sürekliliği Projesi o kuruluşun en üst yöneticisi tarafından başlatılmalıdır. Bu düzeyde başlamayan bir projenin başarılı olma şansı yoktur.[33]

Bir İş Sürekliliği Planı olan kuruluşlar da planlarının geçerliliğini ve standartlara uygunluğunu bağımsız ve yetkin kuruluşlara denetletmelidirler.[33]

Bir iş sürekliliği planı her kurum için özel olmalıdır. Ancak mutlaka temel iş gereksinimlerinin bir listesini, risklerin tanımlanması ve iş etkisinin değerlendirmesini, Stratejiyi içermelidir.[34]

Ayrıca bir İş Sürekliliği Planında şunlar da olmalıdır:[35]

* Kuruluşun İş Sürekliliği Yaklaşımı
* İş Sürekliliği Yönetimi (Örgüt, insan kaynağı, süreçler, donanım, mekan)
* Kuruluşun yaşamsal süreçlerinin ayrıntıları
* Her birimde hangi kesinti düzeyinde İş Sürekliliği Planının devreye gireceği
* Kuruluşun her biriminde kesinti durumunda uygulanacak planın ayrıntıları (süreç, donanım, insan kaynağı)
* Dönemsel sınanma yöntemi
* Kesinti durumunda iletişim planı (iç, dış)

Kurumların ciddi bir felakete uğraması durumunda sigorta önemli bir seçenek olmakla birlikte genel olarak bina ve donanım gibi fiziki varlıklara yönelik olması, ödemede yaşanabilecek aksaklıklar ve iş süreçlerinde yaşanabilecek kesintinin gerçek anlamdaki maliyetinin bilinememesi gibi nedenlerle felaketlerin telafisinde tam bir alternatif olmaktan uzaktır.[25]

Oysa İş Sürekliliği Planlaması ile kurumların;

- Olası felaketleri engelleyebilmesi

- Felaketlere hızlı ve doğru karşılık vermesi
- Varlıklarını ve nakit akışını koruması
- Kesinti süresini en aza indirerek normal operasyonlara dönüşün sağlanması mümkün olacaktır.[33]

İş sürekliliği planının faydaları aşağıdaki şekilde özetlenebilir.[36]

- İş ortamınızda en kritik fonksiyonların etkili ve ayrıntılı analizi
- Uzun süreli bir kesintide karşılaşacağınız finansal kayıpların ve gözle görülemeyen etkilerin anlaşılması
- İş süreçlerini desteklemesi için yaşamsal önemi en yüksek kaynakların belirlenmesi
- Kurtarma stratejilerinizi tasarlamak için kurtarma sürelerinin ve önceliklerinin tanımlanması
- İş operasyonlarına en iyi biçimde dönmek için sağlam yatırım kararlarının alınması
- En üst düzeyde korumayı gerektiren iş süreçlerini ve varlıklarını belirlenmesi
- Olası kurtarma stratejileri ve seçenekleri üzerinde öneriler sunması ve sonucunda uygulanabilir bir planlamanın oluşması
- İş korumasına yönelik doğru yatırım düzeylerini seçmenize yardımcı olması için finansal veriler sağlaması
- Tüm kuruluşunuzdaki süreklilik etkinliklerinizi düzenlemek için kriz öncesi Olağanüstü Durum Merkezi'nin oluşturulması
- Kredilendirme ve sigorta masraflarının düşmesi
- İş operasyonlarınıza en iyi biçimde dönmeniz için kararların bilinçli ve hızlı bir şekilde alınması

4.1.3.2. İş Kurtarma (Felaket Kurtarma) Planları

"İş Sürekliliği planlamasının aşamalarından biri de "Felaket Kurtarma planlamasıdır. Felaket Kurtarma, bir şekilde kurum sistemlerinin çalışamaz hale gelmesi durumlarında, sistemlerin tekrar çalışır hale getirilmesi için atılması gereken adımları belirleyerek alt yapıyı planlar.

Bilişim Teknolojileri tarafından bakıldığında, Felaket Kurtarma, kurum BT sistemlerinden hayati olanların çalışır tutulması veya kısa sürede çalışır hale

getirilmesini amaçlar. Bunun için öncelikle kurum BT yazılım ve donanım sistemlerinin önem bakımından derecelendirilmesi yapılır.[37]

Sistemlerin maksimum ne kadar süre kapalı kalabileceği belirlenir. Bunun sağlıklı bir şekilde yapılması Felaket Kurtarma sisteminin maliyetleri açısından çok önemlidir. Bu çalışma sonucunda şuna benzer bir tablo oluşturulur:[38]

- Felaket Anında Bir Gün İçinde Çalıştırılması Gereken Sistemler
- Felaket Anında Bir Hafta İçinde Çalıştırılması Gereken Sistemler
- Felaket Anında 30 Gün İçinde Çalıştırılması Gereken Sistemler

Felaket Kurtarma Planı için bir Felaket Kurtarma Merkezi tesis edilir. Merkez sistem odasında sistemlerin başına bir sıkıntı geldiğinde, acil süreçler bu Felaket Kurtarma Merkezinde yapılır. Felaket Kurtarma Merkezinin yapılandırılmasında acil ihtiyaçlar ve veriler göz önünde tutulur. Buna göre gerekli donanım ve bağlantı teknolojisi belirlenir.[38]

Felaket Kurtarma Planında kullanılan farklı teknolojiler vardır. Bu planlama, kurumun var olan teknik altyapısına göre değişir. Kullanılan sunucu işletim sistemleri, uygulamalara göre farklı çözümler kullanabilir. Temel olarak kullanılan bazı teknolojiler şunlardır:[38]

- Sanallaştırma: Sunucuların donanım-bağımsız olmasını sağlamaktadır.
- Cluster Çözümleri: Bir sistemin bir benzerinin de farklı bir sistemde çalışmasını sağlayan çözümlerdir.
- Storage Replikasyon: Depolama üniteleri arasında verilerin birebir kopyalanmasını sağlayan çözümlerdir.
- Yedekleme (*Backup*) Çözümleri: Verilerin bir yedeğinin saklanıp gerektiğinde tekrardan alınmasını sağlayan çözümlerdir.
- Bağlantı Çözümleri: Verilerin Felaket Kurtarma merkezine sağlıklı bir şekilde aktarılabilmesi için uzak lokasyon bağlantı teknolojileri kullanılır. Bunun için Felaket Kurtarma Merkezi'nin yerine göre fiber, Noktadan-noktaya MetroEthernet, Noktadan-noktaya g.shdsl, VPN ve GSM üzerinden APN vb. teknolojiler kullanılabilir.

Özet olarak, Felaket Kurtarma sistemleri, kurumun var olan BT altyapısı ve Felaket Kurtarma Merkezi'nin yerine göre şekillendirilir.[38]

Genel olarak birçok Felaket kurtarma merkezi şu ürünleri içerir:

- Sunucu ve Aktif Cihaz kabini ve kablolaması
- Sunucu ve Depolama Ünitesi

- Güvenlik Duvarı Cihazı
- Ağ Anahtarlama (switch) ve Bağlantı (modem) Cihazları
- Veri Tabanı Sunucusu
- Uygulama Sunucuları

4.2. Eğitim ve Bilinçlendirme

İş sürekliliği planlarının sorunsuz ve etkili uygulanması için;[38]

- Tüm çalışanların ve personelin İş Sürekliliği Planının içeriği hakkında bilgi sahibi ve bireysel sorumluluklarının farkında olması,
- Doğrudan sorumlulukları yerine getirmek için gerekli olacak görevler için eğitilmiş olması,
- Çalışanların ve diğer takımların fonksiyonlarının farkında olması önemlidir.

Bu bağlamda; kurum çalışanlarına ve iş sürekliliği organizasyonunda bulunan takımlara eğitim verilmelidir. Kurum çapında benimsenmemiş ve gerekli eğitim çalışmaları yapılmamış iş sürekliliği planlarının başarıya ulaşma olasılığı düşüktür. İş sürekliliği planı içerisinde eğitim konusunda izlenecek yöntemler (anket, sınıf eğitimi, sınav vb.) belirlenmeli ve plan içerisinde yer almalıdır. Eğitim faaliyetlerini yürütmek üzere bir takım kurulması ve gereken zamanlarda eğitim işlerini organize etmesi faydalı olacaktır. Kurum çapında yapılacak iş sürekliliği bilgilendirmesi senede bir defadan az olmamalıdır.[31]

4.3. Tatbikatlar ve İyileştirme

4.3.1. Tatbikat Senaryosunun Hazırlanması ve Uygulanması

Olağanüstü durumlara her an hazır olabilmek için senaryolar üretilmeli ve tatbikatı yapılmalıdır. Tatbikatlar sonucunda kurulmuş olan yönetim sisteminin eksikliklerini tespit etmek mümkün olacaktır. Her bir tatbikat türü için senelik olarak tatbikat planlarının hazırlanması ve tatbikatların yapılması kurumun olası bir acil durum senaryosu için hazır olmasını sağlayacaktır.[31]

4.3.2. Raporlama ve Değerlendirme

Tatbikat sonrası değerlendirme raporu hazırlanmalı ve iş sürekliliği başarı seviyesinin arttırılması için gerekli adımlar belirlenmelidir.[31]

4.3.3. İyileştirme

Bir kurum kilit uygulama ve önemli verilerine sürekli ve kesintisiz erişebilmeye bağımlıdır. Felaketin etkilerini hafifletmek için iş sürekliliği ve iyileştirme planlaması, iş süreçlerine sürekli erişimi sağlamak için çok gereklidir. Sürekli iyileştirme rejimine sahip olmak, kurumun değişen koşullara cevap verebilmesini sağlar.

4.4. Denetim ve Öz değerlendirme

Denetim bağımsız bir grup tarafından da yapılabilir ve tercih edilmelidir.

Her yıl tekrarlanacak öz değerlendirme süreci sonunda ortaya çıkan iyileştirmeye açık alanlar önceliklendirilir, iyileştirme planları yapılır ve uygulamalar hayata geçirilir. Hedefe ulaşılmadığı durumlarda hedef gözden geçirilir.

Maliye Bakanlığı'nın 26 Aralık 2007 tarih ve 26738 sayılı tebliği çerçevesinde ise COSO modelinden de yararlanılarak hazırlanan “Kamu iç Kontrol Standartları Tebliği’nde BT kontrol ve denetimlerine ilişkin maddelere de yer verilmiştir. Bilgi sistemleri kontrolleri baslığı altında, “idareler, bilgi sistemlerinin sürekliliğini ve güvenilirliğini sağlamak için gerekli kontrol mekanizmaları geliştirmelidir.” denilmektedir. İlgili standart kapsamında BT açısından önemli sayılabilecek bazı şartlar su şekilde açıklanmıştır:

- Bilgi sistemlerinin sürekliliğini ve güvenilirliğini sağlayacak kontroller yazılı olarak belirlenmeli ve uygulanmalıdır.
- Bilgi sistemine veri ve bilgi girişi ile bunlara erişim konusunda yetkilendirmeler yapılmalı, hata ve usulsüzlüklerin önlenmesi, tespit edilmesi ve düzeltilmesini sağlayacak mekanizmalar oluşturulmalıdır.
- İdareler bilişim yönetişimini sağlayacak mekanizmalar geliştirmelidir.

BÖLÜM 5

UYGULAMA

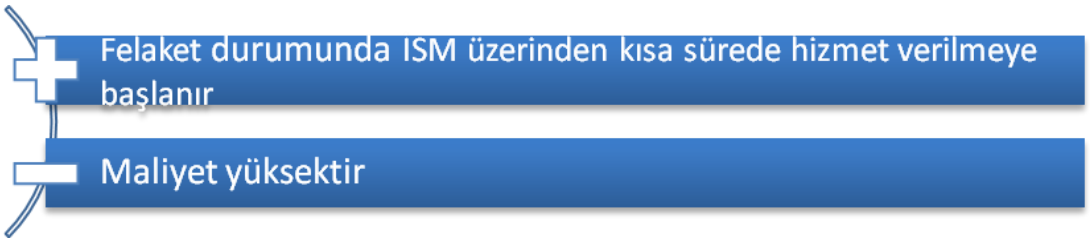
5.1. Uygulama Modelleri ve Mimarileri

5.1.1. İş Sürekliliği Merkezi Sistem Mimarileri

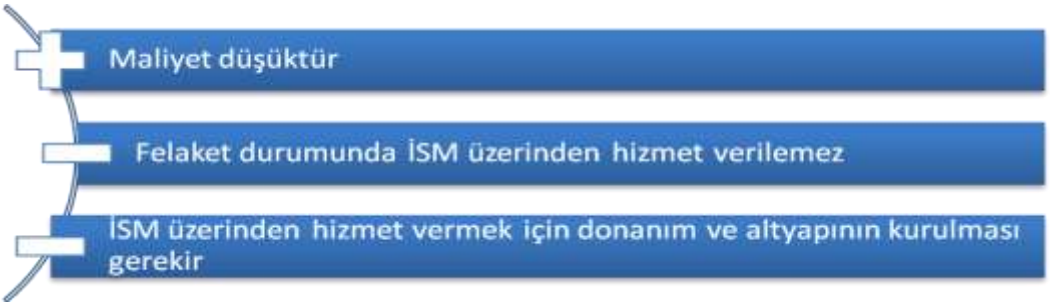
İş Sürekliliği Merkezi (İSM) için kurumun stratejik kararları, yapılacak yatırım miktarı ve hizmet verilen sistemlerin bir felaket durumunda ne kadar sürede yeniden hizmet vermeye başlaması gerektiği kriterlerine farklı mimariler tercih edilebilir.

İş Sürekliliği Merkezi, mevcut hizmet veren sistem merkezindeki tüm donanım ve altyapının birebir aynısı olarak kurulabileceği gibi sadece felaket durumunda verilerin kurtarılması hedeflenerek veri yedekleme merkezi olarak kurulabilecektir.

İş Sürekliliği Merkezine, tüm donanım ve altyapının aynı şekilde kurulması durumunda;



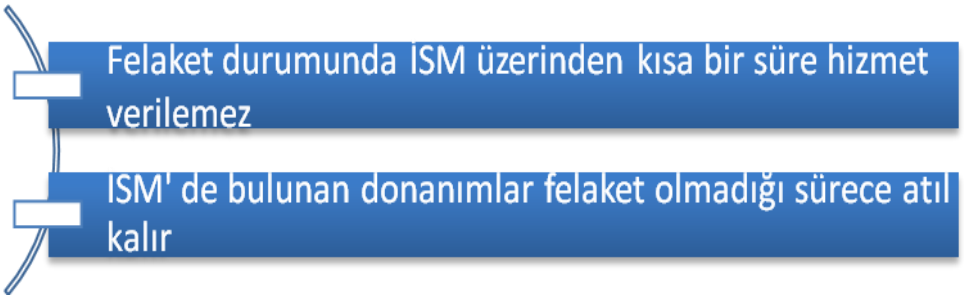
Sadece verilerin yedeklenmesi için gerekli donanımların kurulması durumunda;



Ayrıca İş Sürekliliği Merkezinin felaket durumu haricinde aktif olma durumuna göre farklı mimariler oluşturulabilir. Aşağıda verilen avantaj ve dezavantajlar İSM' ye tüm donanım ve altyapının kurulması durumuna göre verilmiştir.

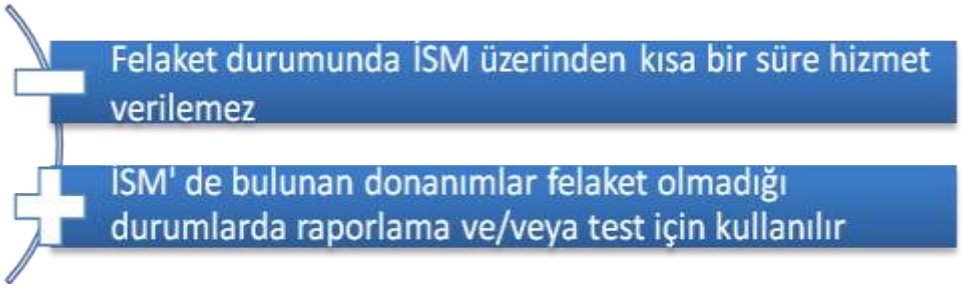
5.1.1.1. Aktif – Pasif

Sistem merkezinin Aktif, İSM'nin felaket durumu haricinde pasif olduğu mimaridir. Felaket durumunda İSM aktif hale geçer.



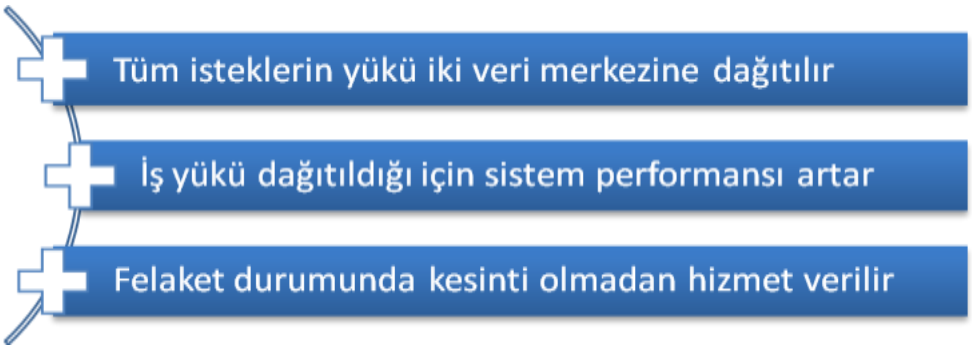
5.1.1.2. Aktif – Yarı Aktif

Sistem Merkezi Aktif olarak çalışırken, verilerin yedeklendiği İSM üzerinden, anlık veri değişikliklerin çok önemli olmadığı istatistik ve raporlar alınabildiği veya test ortamı olarak kullanılabildiği mimaridir.



5.1.1.3. Aktif – Aktif

Sistem merkezi ve İSM'nin gelen istekleri yük dağılımlı olarak karşıladığı ve her iki tarafta anlık olarak verilerin eşit olduğu mimaridir. Bu durumda felaket anında devreye girecek bir İSM yerine eşit ağırlıklı iki sistem merkezine sahip olunur. Her iki merkez bir birinin yedeği durumundadır. Merkezlerden herhangi biri hizmet veremez duruma gelse bile son kullanıcı farkına varmaz ve hizmet kesintiye uğramadan diğer veri merkezinden verilmeye devam eder. Hat problemi, UPS veya ağ cihazları arızası gibi küçük sorunlarda bile sistem kısa da olsa kesintiye uğramaz.



5.1.2. İş Sürekliliği İçin Veri Yedekleme Yöntemleri

İş sürekliliği için en önemli konu verilerin kaybedilmemesidir. Verilerin yedeklenmesi asenkron veya senkron yedekleme işlemi yapılabilir. Asenkron yedeklemede, veriler bir süre gecikmeli olarak İSM' ye aktarıldığı için felaket anında, aktarılmayan veriler kaybedilir. Senkron yedeklemede ise veri her iki sisteme de eşzamanlı yazılacağından, veri yazma hızında artış ve performansta bir miktar düşüş olabilecektir.

Veri yedekleme yöntemleri için seçenekler aşağıda kısaca anlatılmıştır.

5.1.2.1. Diskten Diske Veri Yedekleme

Disk sistemlerinin sağladıkları araçlar ile veri merkezindeki disk sisteminde yapılan değişiklikler senkron veya asenkron olarak İSM disk sistemine yazılır. Bu yöntemde veri tutarsızlığı oluşmaması için İSM tarafındaki disk sistemine yazma işlemleri engellenir. Asenkron yedekleme yöntemi için veri merkezindeki disk sisteminde yapılan değişen izler (track) tutulur ve senkronizasyon başladığında sadece bu izler kopyalanarak iki disk sistemi eşitlenir.

5.1.2.2. Veri Tabanı Seviyesinde Senkronizasyon Araçları ile Yedekleme

Veri tabanı senkronizasyon araçları ile veri merkezinde yapılan değişiklikler İSM veri tabanına senkron veya asenkron olarak işlenir. Bu yöntemde veri tutarsızlığı oluşmaması için İSM ' deki veri tabanına yazma işlemleri engellenir. İSM veri tabanından sorgulama ve raporlama işlemleri yapılabilir.

5.1.2.3. Veri Tabanı Kümelenmesi (Clustering) ile Yedekleme

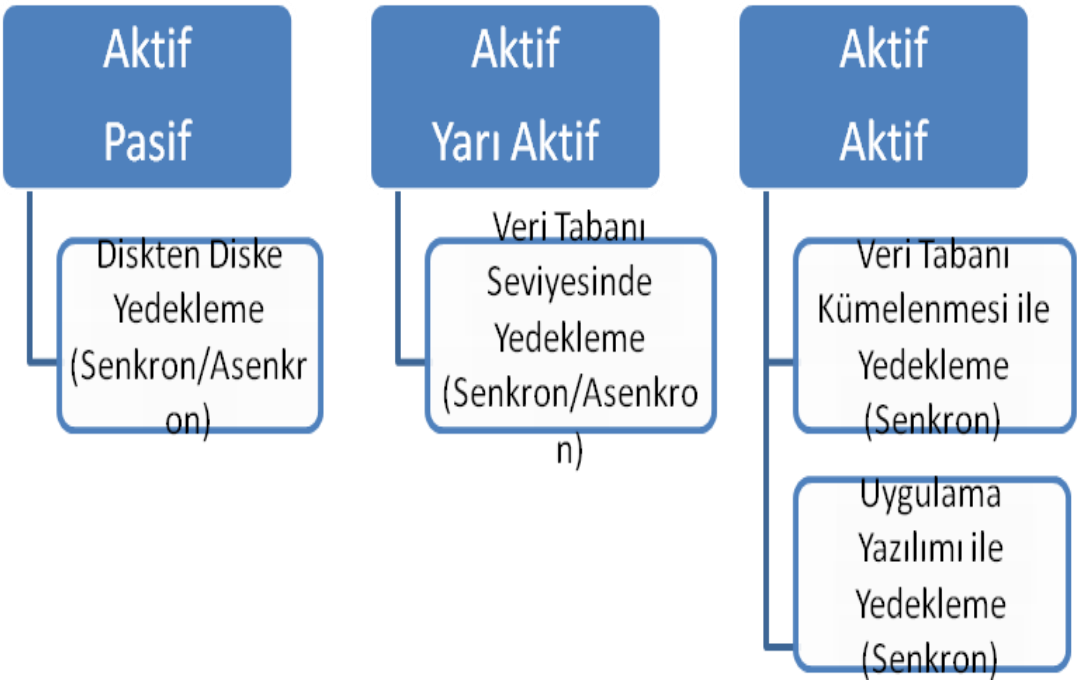
Veri tabanı kümelenmesi yöntemi ile kümelenme yazılımının desteklediği mesafe içinde kurulacak veri merkezi ve İSM' de yer alan veri tabanları gelen isteklere yük paylaşımlı olarak hizmet verir. Veriler her iki veri tabanına eş zamanlı yazıldığından senkron yapıda bir yedekleme oluşturulur. Farklı bir şehirde kurulması düşünülen İSM' ler için mesafeden dolayı uygun bir çözüm değildir.

5.1.2.4. Uygulama Yazılımı Seviyesinde Yedekleme

Kullanılan uygulama yazılımlarında yapılacak altyapı değişiklikleri ile yazma isteklerinin veri merkezi ve İSM' deki veri tabanlarına senkron olarak yazılması sağlanır. Bu yöntemde veri tutarsızlıklarının engellenmesi için dağıtılmış işlem (distributed transaction) yöntemi kullanılır.

5.1.2.5. Sistem Mimarileri ve Veri Yedekleme Yöntemleri İlişkisi

İş Sürekliliği Merkezi Sistem Mimarileri ile veri yedekleme yöntemleri arasındaki ilişkiyi aşağıdaki şekilden görebilirsiniz.



Şekil 7: Sistem mimari ve veri yedekleme yöntemleri

5.1.3. Güvenlik

İş Sürekliliğinin sağlanabilmesi için veri merkezi ve İSM' deki sistem donanım ve yazılımlarının güvenliğinin sağlanması gerekmektedir. Ayrı bir İSM olmadığı durumlarda, sistemlerin kesintisiz bir şekilde hizmet vermeye devam edebilmesi için alınması gereken güvenlik tedbirleri daha önemli hale gelmektedir.

5.1.3.1. Fiziksel Güvenlik

Sistem merkezinin fiziksel güvenliğinin sağlanabilmesi için aşağıda belirtilen sistem ve araçlar kullanılabilecektir.

- Giriş çıkış kontrol sistemleri,
- Kameralı izleme sistemleri,
- Soğutma Sistemleri,
- Isı, Nem vb. detektörler ve sistem merkezi izleme araçları,
- Yangın söndürme ve önleme sistemleri.

5.1.3.2. Sistem ve Bilgi Güvenliği

Sistem ve bilgi güvenliğinin sağlanabilmesi için aşağıda belirtilen tedbirler alınabilecektir.

- Disk sistemi, sunucu, ağ cihazları, hat, elektrik altyapısı gibi sistemin çalışmasını etkileyebilecek her şeyin yedekli yapıda olması,
- Jeneratör ve UPS kullanılması,
- Verilerini düzenli olarak farklı bir ortama yedeklenmesi, yedekten geri dönülebildiğinin test edilmesi,
- Saldırı Takip ve Önleme Sistemleri, Ateş Duvarı (Firewall) gibi donanım ve yazılım çözümleriyle yapılacak saldırıların kayıt altına alınması ve/veya önlenmesi,
- Antivirüs yazılımları ile sistemleri durdurabilecek veya gizli verilerin açığa çıkmasını sağlayacak virüslerin engellenmesi,
- Düzenli yapılacak güvenlik testleri yapılarak, sistemin açıklarının tespit edilmesi ve sonrasında bu açıkların kapatılması.

5.2. Koordinasyon

5.2.1. Kurumlar Arası Koordinasyon

Oluşturulması düşünülen ülke bilgi sistemi içerisinde, kamu kurum ve kuruluşlarının taşra ve merkez birimleri arasında çevrimiçi (*on-line*) bilgi akışı sağlanmalıdır.

Günlük faaliyetler içinde üretilen tüm bilgiler İnternet aracılığı ile yetkiler çerçevesinde paylaşılmalıdır.

Bu veri paylaşımının alt yapısı güçlendirilmelidir, veri erişim hızları artırılmalıdır.

Kurumlar belirlenecek politikalar kapsamında kendi görev ve faaliyet alanlarına giren işlerde ancak yeterli teknik ve personel altyapısı ve kurumsal statüsü ile kurumlar arasındaki yeri tanımlandıktan sonra bu teknolojilerin yatırımına girmeye teşvik edilmelidir.

Sistemin gelişiminin ilk basamaklarından itibaren, fikirlerin, gereksinimlerin ve sorunların hem düşey olarak (daha yüksek yönetimlere ve politik seviyelere ve memurlara) hem de yatay olarak (diğer bölümlere, örgütlere ve kullanıcılara) iletilmesi, sistemin başarılı olmasına yardım edecektir. İşbirliğinin siyasi veya yasal nedenlerle sınırlandırılabilmesine rağmen, sadece iletişim vasıtasıyla gönüllü işbirliği elde edilebilecektir. Sürekli sistem desteği, kullanıcı kitleleri, idare ve kurumlar arasında bir iletişim ağının varlığına bağlıdır.

Kurumların kendi oto-kontrol sistemlerinin geliştirmesi ve bu sistemleri sürekli revize ederek oluşabilecek senaryolara hazırlıklı olmaları ve bu çalışmaları işbirliği veya çözüm ortağı olan kurumlarla paylaşmaları koordinasyon açısından önem arz etmektedir. Kurumların gizlilik planları ve güvenlikleri göz ardı edilmeden zamanında kurulan iletişim kanallarının kriz anında müdahale kolaylığından, etkin müdahaleye ve kriz sonrası çözümler için tepkisel sürelerde rahat hareket etme kolaylığı sağlayacaktır.

Kurumlar arasında iletişim gerek teknik ve gerekse yönetim anlamında tek bir terminoloji ile sağlanmalıdır. Koordinasyon gereken durumlarda iletişim kazaların engellenmesi ancak tek bir terminoloji ile mümkündür. Unutulmamalıdır ki etkin müdahale ancak krizin doğru tanımlanabilmesi ile olasıdır.

5.2.2. Kurum İçi Koordinasyon

İş sürekliliğinin sağlanmasında bilgi teknolojilerinin rolünün yüksek olmasından dolayı çalışmaların BT bölümü tarafından yapılması ve sorumluluğunun da BT bölümünde olması gerektiği inanışı yaygındır.

İstatistikler iş sürekliliği çalışmalarına BT bölümünün katılımının diğer birimlerden fazla olduğunu göstermektedir. Öte yandan iş sürekliliğinin sorumluluğunun çok yüksek oranda üst yönetim, yönetim kurulu veya iş sürekliliği takımında olduğu görünmektedir. İş süreçlerinin devam ettirilebilmesi veya olağan üstü bir durumda tekrar çalışır hale getirilmesi, personelin alternatif çalışma ortamına naklinden, sunucuların hazırlanmasına, yeni cihaz satın alımına kadar birçok faaliyeti içermektedir. Bu sebeple iş sürekliliği kurum içinde mümkün olduğu kadar üst seviye yönetim tarafından temsil edilmeli ve tüm çalışma grupları ile birlikte çalışarak iş sürekliliğini sağlayacak bir ekip kurulmalıdır.

Kurum içi koordinasyon kurumsal eylem planının hayata geçirilmesi ile mümkün olmaktadır. İş sürekliliği bir kurumun temel hedeflerinden biri olduğuna

göre bu sorumluluk her çalışana gerek seminerler ve gerekse görevlendirilmelerle bildirilmelidir.

Görev yetki ve sorumluluklar çerçevesinde kurulan iş sürekliliği zincirleri arasında oluşabilecek boşlukların her hangi bir kritere bağlı kalmadan etkin ve yetkin personel ile güçlendirilmesi ve bu sürekliliğin kişi ve mevkiden bağımsız "kurum politikası" olarak benimsenmesi önemlidir.

Bu konuda çalışma yapan kurumların uluslararası kabul gören standartlara bağlı kalması ve alt yapılarını bu standartlara göre hazırlaması da ayrıca önem arz etmektedir. Bu konu raporumuzun standartlar başlığı altında ele alınmaktadır.

5.3. Sürdürülebilirlik

Son yıllarda dünyada hızla gelişen ve sıklıkla İş Sürekliliği ile karıştırılan bir kavram "Sürdürülebilirliktir (Sustainability). Sürdürülebilirlik, kısaca, kuruluşların, toplum önünde ekonomik, toplumsal ve çevresel hedeflerini belirlemeleri, bu hedeflere erişim durumlarını düzenli olarak raporlamaları ve zaman içinde bu hedeflerini daha da üst düzeylere çıkarmaları olarak tanımlanır. Sürdürülebilirlik kavramını benimseyen kuruluşlar bu üçlü yapı içinde daha da üst düzeylere gelerek sahiplerinin, müşterilerinin ve toplumun gözünde saygınlıklarını arttırırlar.

5.3.1. İş Sürekliliği – Sürdürülebilirlik İlişkisi

Sürdürülebilirlik ile İş Sürekliliği arasındaki en önemli ilişki, İş Sürekliliği'nin yaşamsallığından kaynaklanmaktadır. Bir kesintiden ötürü piyasadan silinen ya da itibarını yitiren bir kuruluşun sürdürülebilirliğinden söz edilemez. Bu nedenle Sürdürülebilirliğin ön koşulu İş Sürekliliği'dir. Yurtdışında sürdürülebilirlik çalışması yürüten her kuruluşun İş Sürekliliği planları vardır. Ülkemizde de yeni gelişen Sürdürülebilirlik çalışmaları mutlaka beraberinde İş Sürekliliği kavramını da getirmelidir. Aksi halde süreçlerinde kesinti yaşayan kuruluşların işlerini ve itibarlarını yitirmesiyle birlikte Sürdürülebilirlik kavramı da itibarını yitirir.

BÖLÜM 6

KAMU-BİB İŞ SÜREKLİLİĞİ MODEL ÖNERİSİ

6.1.Hangi Standardı ve Rehberi Seçmeliyiz?

İş sürekliliği çalışmalarında genel kabul görmüş bir standart kullanmak ve iş hedeflerine ve ihtiyaçlarına göre bu standardı uyarlamak bir kurum için kredibilite, kurumsallaşma yönünde seviye artırımı, birlikte çalışabilirlik ve denetime açıklık gibi temel unsurlara önemli katkı sağlamaktadır.

İş sürekliliği için oluşturulan standartlardan 2.bölümde açıklananlardan öne çıkan uluslararası kabul gören BS 25999 standardı (ve onun devamı ve halefi olacak olan ISO 22301) öncelikle değerlendirmeye alınabilir. Bu standartların kullanımında rehber niteliğinde ITIL ve COBIT'in ilgili bölümleri kullanılabileceği gibi yine ISO tarafından yayınlanan ve listesi yukarda verilen standart ve rehberler kullanılabilir.

İş sürekliliği göreceli olarak yeni bir alan olup sektördeki gelişmelere paralel olarak özellikle son 20 yıl içerisinde gelişmeler göstermiş ve standartlar oluşmaya başlamıştır. Diğer alanlarda olduğu gibi iş sürekliliği konusunda da başlangıçta ülkeler kendi standartlarını ve en iyi uygulamalarını içeren kılavuzlarını oluşturmuşlardır. BS 25999 bunlar arasında öne çıkan ve kendini kabul ettiren standart olarak göze çarpmaktadır. Bu standardı kullanırken göz önünde bulundurulması gereken eksiklikleri şunlardır: Olay Yönetimi Süreci'ni bir plan kapsamına alıp bağlamından koparmış ve felaket öncesi yapılacaklar olarak Erişilebilirlik Yönetimi, Problem Yönetimi, Değişim Yönetimi ve Konfigürasyon Yönetimi gibi sürekliliğin zemini oluşturan süreçlere yer vermemiştir.

Tablo 3: Standart Çerçeve Rehberi

Standart Çerçeve Rehber	Esas Kullanım Amacı	İş Sürekliliği Boyutu
BS 25999-1	İş sürekliliği uygulama rehberidir.	25999-2'nin gereksinimlerini izah eder
BS 25999-2	İş sürekliliği uygulama temel kurallar setidir.	İş Sürekliliği Yönetim Sistemi kurulumu için minimum kuralları oluşturur.
ISO 22301	BS25999 standardının ISO tarafından geliştirilmiş yeni sürümü	BS25999 yerine 2012'den itibaren kullanılacak yeni standart ailesinin ilk üyesidir. TC 223 tarafından geliştirilen pek çok diğer rehber bu aile altında yer alır.
ITIL	Bilgi Teknolojileri Altyapı Kitaplığı	ITIL'da detaylı ele alınan ; IT Hizmet Sürekliliği Yönetimi Süreci, Erişilebilirlik Yönetimi Süreci, Değişim ve Konfigürasyon Yönetimi Süreçleri ile Olay -Problem ve Event Yönetimi süreçleri etkin bir iş sürekliliği için gereklidir.
COBIT	Bilgi ile İlişkili Teknolojiler için kontrol hedeflerini ve süreçlerin detaylarını içerir	DS4 ve ITIL'da bahsi geçen süreklilikle ilişkili süreçlerin kontrol hedefleri, performans kriterleri, riskleri ve denetimi konusunda yol gösterir.

Genel olarak iş sürekliliği konusunda standart seçiminde kurum yöneticileri gerçekleştirdikleri anahtar ve kritik aktiviteleri göz önüne alarak karar vermektedirler. Bununla birlikte aşağıdaki soruların doğru karar verme yönünde yöneticilere yardımcı olacağı düşünülmektedir.[39]

Tablo 4: Standartların Seciminde Kullanılacak Kontrol Listesi

Cevaplanması gereken soru	Kurumun cevapları
Kullanılması düşünülen standart uluslararası özelliği olan ve kuruma uygun bir çerçeve sunmakta mıdır?	
Standart sadece iş sürekliliği değil, bunun yanında risk analizi ve risk azaltıcı etkinlikleri içeren bütünlüğü ve kesinliği olan bir çerçeve sunuyor mu?	
Standart risk yönetimi konusunda yönetimin yaklaşımını içeriyor mu?	
Kullanılması planlanan standart sadece iş sürekliliği terimleri değil, bunun yanında iş ile ilgili kavramsal tabirler üzerine konumlandırılmış mı?	
Düşünülen standart yağın olarak kabul görmüş iş sürekliliği yönetim sistemini belirtirken bunun yanında risk yönetimi hedeflerine nasıl ulaşacağını gösterip üst yönetimin güvenini sağlayacak bir içerik sunuyor mu?	
Standart bir iş sürekliliği programı geliştirmeyi, uzun vadeli bir yönetim ile sürekli bir iyileştirmeyi hedefliyor mu?	

Küresel olarak kabul görmüş standartlar ile ITIL gibi en iyi uygulamaları içeren kılavuzlar temel olarak farklı ölçekteki tüm organizasyonları hedef almaktadır. Özellikle kamu kurum ve kuruluşları, hedefleri, hizmetleri, hitap ettiği kitle ve bu kitlenin büyüklüğü nedeniyle oldukça farklılaşmaktadırlar. Yukarıda belirtilen sorular kurumun kendi yöneticileri tarafından iş sürekliliği konusunda kullanılacak metodolojinin veya standardın belirlenmesinde yardımcı olabilecek soruları ihtiva etmektedir. Bu soruların yanı sıra, iş sürekliliği çalışmalarına başlayacak olan bir kurumun sürece başlangıç noktası olarak kullanabileceği, iş sürekliliği kapsamında yer alan temel bileşenler ile bu bileşenlerin standartlardaki ilgili bölümlerinin sunulduğu karşılaştırma tablosu.[40] Tablo 5'de gösterilmektedir:

Tablo 5: İş Sürekliliği Bileşenleri ve Standartlar Karşılaştırma Tablosu

İş Sürekliliği Bileşeni	ISO 22301	BS 25999:2	NFPA 1600:2010
Giriş	Bölüm 0.1	Giriş	Giriş
Planla-Uygula-Kontrol et-Önlem al	Bölüm 0.2	Giriş	Ek-D
Kapsam	Bölüm 2	Bölüm 3.1	Ünite 1.1
Referanslar	Bölüm 2	Bölüm 3.1	Ünite 2
Kavramlar ve Tanımlar	Bölüm 3	Bölüm 2	Ünite 3
İş sürekliliği yönetim sistemi	Bölüm 4	Bölüm 3	Ek 4
Politika	Bölüm 5.3	Bölüm 3.2.2	Ünite 4
Planlama	Bölüm 6	Bölüm 3	Ünite 5
Risk analizi	Bölüm 8.4.3	Bölüm 4.1.2	Ünite 5.4
İş etki analizi	Bölüm 8.4.3	Bölüm 4.4.1	Ünite 5.5
İş sürekliliği stratejileri	Bölüm 8.4.4	Bölüm 4.2	Ünite 5
Uygulama	Bölüm 8.5	Bölüm 4	Ünite 6
Kaynakların belirlenmesi	Bölüm 7.1	Bölüm 4.3	Ünite 6.1
Rol ve sorumluluklar	Bölüm 5.4	Bölüm 3.2.4	Ünite 6.6
İş sürekliliği tepkileri	Bölüm 8.5.4	Bölüm 4.3.3	Ünite 6.9
Acil durum bildirimleri	Bölüm 8.5.7	Bölüm 4.3.2	Ünite 6.8
İş sürekliliği planları	Bölüm 8.4	Bölüm 4.3.3	Ünite 6.7
İzleme ve Ölçme	Bölüm 9.1	Bölüm 4.4	Ünite 7.1
Uyumluluk değerlendirmeleri	Bölüm 8.7.2	Bölüm 5.1	Ünite 7.1
Test ve tatbikatlar	Bölüm 8.6.1	Bölüm 4.4	Ünite 7
Kayıt yönetimi	Bölüm 7.5	Bölüm 3.4.2	Ünite 4.8
Eğitim ve bilinçlendirme	Bölüm 7.3	Bölüm 3.2.4	Ünite 6.11
Denetim	Bölüm 9.2	Bölüm 5.1	Ünite 8.1
Sürekli iyileştirme	Bölüm 10.2	Bölüm 6.2	Ünite 8

Tablo'da da görüleceği üzere yoğun olarak kullanılan bu standartlar iş sürekliliğinin temel bileşenleri ile ilgili olarak ilgili bölümler sunmaktadır. Ancak bu her standardın konuyu aynı derinlikte ve benzer şekilde ele aldığını göstermemektedir. Kesin karara kurumun büyüklüğü, sektörün yapısı, ülkenin yasal altyapısı gibi tüm faktörler değerlendirilerek ulaşılmalıdır.

6.2. İş Sürekliliği Yönetim Sistemi Kurma Projesi Modeli

Kurumda iş sürekliliği yönetimi ilk defa oluşturulacaksa bu çalışma proje yönetimi disiplini ile yürütülmelidir. Burada dikkat edilmesi gereken nokta ilk defa sistemin kurulmasından sonra projenin bitmesi ile çalışmanın son bulmaması ve sürekli işleyen ve yönetilen bir yapı oluşturulması gerekliliğidir.

Şekil 8: Proje Adımları

- **Proje Yöneticisi, Proje Ekibi ve Proje Kapsamının Belirlenmesi**

Kurum yönetiminin atayacağı proje yöneticisi iş sürekliliği yönetim sistemine ilişkin yasal mevzuat, ulusal ve uluslar arası standartlar ile kurum hakkında gerekli araştırmaları yaparak ihtiyaçları tespit etmelidir. İhtiyaçlar doğrultusunda projenin kapsamı belirlenmelidir.

- **Yönetim Onayı ve Proje Ekibinin Oluşturulması**

Proje beyanı kurum yönetiminin onayına sunulmalı, projenin kapsamı, hedefleri, ekiplerin görevleri, raporlama ve çıktılara ilişkin takvim yönetimin beklentileri de dikkate alınarak netleştirilmelidir.

İş sürekliliği projeleri kurumların özelliklerine göre geniş katılımı ve birbirine bağlı görevlerin uyumlu bir şekilde yürütülmesini gerektirir. Bu nedenle, projede fiilen çalışarak katma değer üretecek kişilerden oluşan bir proje ekibi oluşturulmalıdır.

- **Yönlendirme Ekibi**

Proje etkinliği için proje yürütülürken karar alma, yönlendirme, danışma görevlerini yüklenecek **yönetici seviyesinde** bir ekibin oluşturulması çok önemlidir.

- **Projenin Duyurusu**

Yönetimin olduğu ve projede yer alan tüm tarafların katıldığı bir toplantıyla projenin önemi, amacı, kapsamı, ekip üyeleri ve sorumlulukları, çıktılar ve proje takvimi anlatılmalıdır.

Daha sonra proje tüm kurum personeline duyurularak projenin sahiplenilmesi ve personelin desteğinin alınması sağlanmalıdır.

- **Proje Ekibinin Eğitimi**

Projenin ilgili tüm tarafları ile proje üyelerine kurum içi veya kurum dışından bir eğitimci ile organize edilecek iş sürekliliği, iş sürekliliği yönetim sistemi, hakkında uygulama eğitimleri verilmelidir.

- **Analiz**

İlgili tarafların katılımı ile kurum için risk analizi ve iş etki analizi çalışmaları yapılarak iş sürekliliğine yönelik detaylı bilgilerin toplanması son derece önemlidir. Kurumun risk ve iş etki analizi sonuçları proje yönlendirme ekibine sunularak karar alma ve yönlendirme gerektiren konularda ekibin desteği alınmalıdır.

- **Strateji ve Planların Oluşturulması**

Analizler sonucunda oluşan bilgiler dikkate alınarak yasal mevzuat, ulusal ve uluslar arası standartlar ve kurum ihtiyaçlarını en iyi şekilde karşılayacak fayda-maliyet analizleri yapılmış strateji ve iş sürekliliği planları oluşturulmalıdır.

- **Strateji ve Planların Yönlendirme Ekibine Sunulması**

Analiz sonuçları, yasal mevzuat, ulusal ve uluslar arası standartlar, kurum ihtiyaçlarına yönelik hazırlanan strateji ve planlar yönlendirme ekibine sunularak uygunluk alınmalıdır. Bu aşamada gerekli bilgi sistemleri, insan kaynağı, donanım hakkında ve iş sürekliliğinin kurumda sürdürülebilirliğinin sağlanması için kararlar alınmalıdır.

- **Planların Onaylanması, Duyurulması ve Eğitim**

Planlar Yönlendirme Ekibinin uygun görüşü ile kurum üst yönetiminin onayına sunulmalıdır. Onaylanmış planlar güncel olarak tutulacak şekilde dağıtımı yapılmalıdır. Dağıtımı yapılan planların nasıl kullanılacağı, iş sürekliliği yönetimindeki sorumlulukları doğrultusunda tüm personele eğitimler planlanmalıdır.

- **Örnek Senaryo ve Tatbikatların Gerçekleştirilmesi**

Planların geçerliliğini, kurumun olağanüstü durum karşısındaki tepkilerini test etmek, kurum personelinin iş sürekliliği konusunda bilgisini, görevli personelin tecrübesini arttırmak amacıyla planlı ve programlı tatbikatlar yapılmalıdır.

- **İç Denetim**

İş sürekliliği yönetim sistemi sistematik olarak uygunluk, yeterlilik ve etkinlik yönünden değerlendirilmeli, aksayan ve geliştirilmesi gerekli alanların tespit edilmesi ve düzeltilmesi sağlanmalıdır.

- **Projenin Kapanışı**

İş sürekliliği yönetimine ilişkin tüm raporlamanın sunumunun yapıldığı toplantı ile proje kapanışı yapılmalıdır. Bundan sonra iş sürekliliği yönetimi ve geliştirme faaliyetleri ekip tarafından yürütülmelidir.

İş sürekliliğine ilişkin hazırlanan tüm belgeler “İş Sürekliliği Yönetim Sistemi El Kitabı”nda toplanmalı, ilgili kişilerin olağanüstü durumda ulaşabileceği bir yerde bulunmalı ve bilgi güvenliği açısından görev, yetki ve sorumlulukları çerçevesinde kişilerin erişimi mümkün olmalıdır.

6.3. İş Etki Analizi Nasıl Yapılır?

Bir İş Etki Analizi (İEA) yapılması için öncelikle aşağıdaki anahtar ipuçlarını aklınızda tutun.

Şekil 9: İş Etki Analizi İçin İpuçları

İş etki analizi için veri toplama süreci çok önemlidir. Veri toplama; anket, form, ön görüşme, yüz yüze görüşme gibi yöntemlerle yapılabilir. Aşağıda örnek bir anket/form verilmiştir.

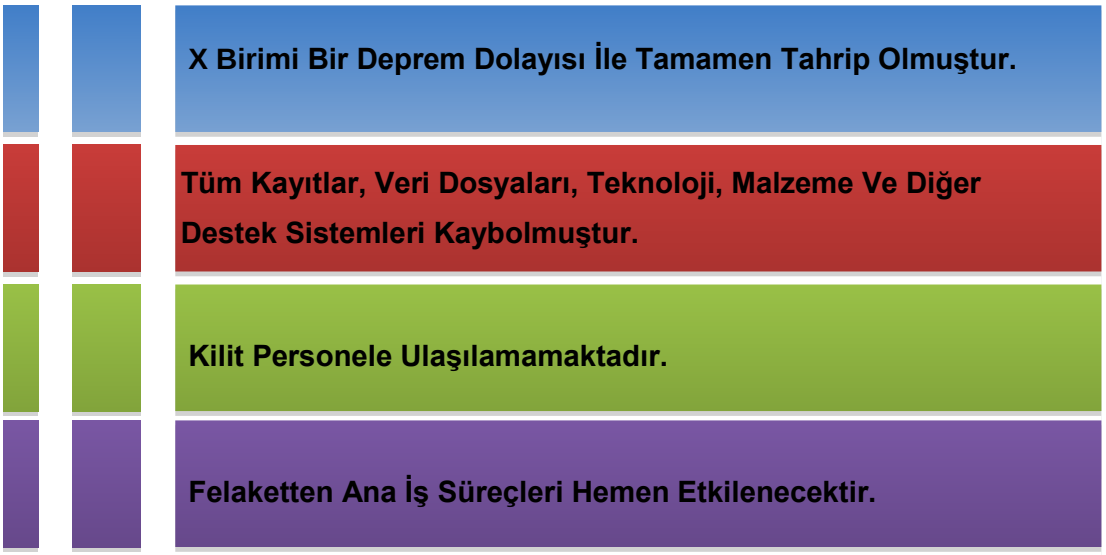
Tablo 6: Örnek İş Etki Analizi Formu

BİRİM ADI: *(İs biriminin adını girin)*		
PERSONEL SAYISI:*(Tam zamanlı personel ve isteğe bağlı olarak varsa yarı zamanlı ve müteahhit sayısını girin.)*		
ANASÜREÇ ADI:*(Birimin temel faaliyetlerini tanımlayın. Örneğin, satış, yüklenici ara yüzü veya yatırımcı ilişkileri yönetimi.)*		
ÖNCELİK SIRALAMASI:*(Sürecinin önemine göre sübjektif bir sayı girin)*		
MAKSİMUM TAHAMMÜL EDİLEBİLİR KESİNTİ SÜRESİ (MTPOD):*(Bu bölümde bir saat, bir hafta gibi bir zaman dilimi girin. Bir kesinti sonrasında bir üst süreçte "neredeyse her zamanki gibi iş" durumuna dönülecek zamanı açıklayın.)*		
KURTARMA SÜRESİ HEDEFİ (RTO): *(Bu bölümde bir saat, bir hafta gibi bir zaman dilimi girin. Bir kesinti sonrasında zararın minimum seviyede tutulması için gerekli zaman hedefini girin.)*		
KURTARMA NOKTASI AMACI(RPO):*(Bu bölümde maksimum kabul edilebilir veri kaybı hedefini girin. Bir kesinti sonrasında, belirlediğiniz hangi üst süreçlerin işe geri alınma noktasıdır)*		
BAĞLILIKLAR:*(Süreçlerin normal işlemler için bağlı olduğu kuruluşların ve / veya süreçlerin isimlerini girin. Örneğin uygulamalar, donanımlar ve personel.)*		
(İsteğe bağlı) **Alt Süreç Adı:** *Birim yaptığı faaliyetleri destekleyen süreçlerin açıklamasını girin. Örneğin, satış analizi, finansal analiz*		
(İsteğe bağlı) **Alt Sürecin Öncelik Sıralaması:** *İş birimi için öznel alt sürecin sıralamasını ve önemini belirtmek için buraya bir sayı girin.*		
(İsteğe bağlı) **Alt Süreç İçin;**		
KANTİTATİF ETKİSİ: (*Ana süreç ile ilişkili bir mali miktar girin. Örneğin, işlem ile oluşan satış ve gelir kaybı, gecikmeli satış veya gelir, artan giderler (örneğin; mesai, emek, dış kaynak kullanımı, sevk masrafları.), düzenleyici para cezaları, sözleşmeli ceza veya sözleşmeden ikramiye kaybı, yeni iş planları gecikmesi)***KALİTATİF ETKİSİ:** (*Mali olmayan etkileri girin. Örneğin; itibar kaybı, üst süreç ile ilgili müşteri kaybı)*	MTPOD İçinde;	MTPOD Dışında;
Kurtarmak İçin Gerekli Zamanda İhtiyaç Duyulan Personel: (*Süreler dâhilinde "neredeyse her zamanki gibi iş" durumuna dönmek için gerekli personel sayısını girin)*		
Kurtarma stratejisi: (İşin eski haline dönmesi için yapılabilecek eylemleri girin. Örneğin; işi alternatif bir alana taşıma, evden çalışma, elektronik ortamda yapma.)		
Teknoloji / Hizmetler kurtarma zamanı:*Belirli bir zaman çerçevesinde ele alınması gereken sistem ve hizmetleri girin*		
Yorum: *Yorumunuzu girin.*		

Tablo 7: Örnek İş Etki Analizi Çalışması

BİRİM ADI	X
PERSONEL SAYISI	100
ANASÜREÇ ADI	X1 PROJESİ (Diğer Kurumlar ve vatandaşlar tarafından kullanılan bir web uygulaması)
ÖNCELİK SIRALAMASI	1
MAKSİMUM TAHAMMÜL EDİLEBİLİR KESİNTİ SÜRESİ (MTPOD)	12 saat
KURTARMA SÜRESİ HEDEFİ (RTO)	4 saat
KURTARMA NOKTASI AMACI (RPO)	6 saat
BAĞLILIKLAR	-İnternet erişimi -Güvenlik sistemleri -Sunucu sistemleri -Elektrik altyapısı
KANTİTATİF ETKİSİ	-Fazla Mesai -İş planlarının Gecikmesi -Dış Kaynak Kullanımı
KALİTATİF ETKİSİ	-Kurum'un prestiji -Diğer kurumların ve vatandaşların maddi ve manevi zarar görmeleri
KURTARMAK İÇİN GEREKLİ ZAMANDA İHTİYAÇ DUYULAN PERSONEL	5
KURTARMA STRATEJİSİ	Alternatif bir alana taşıma

Form veya anket dışında veya yanında kullanılabilecek görüşme yönteminde ise derinlemesine bilgi ve analiz için kurumun fonksiyonları ile tecrübesi olan insanlar ile görüşerek İş Etki Analizinin oluşturulmasında fayda vardır. Görüşmede görüşülen kişiye soru sorarken görüşülenin tepkisini çerçevelemek amacı ile bir olay açıklaması verilmesi yararlıdır.



Şekil 10: İş Etki Analizi İçin Örnek Olay açıklaması

İş Etki Analizinin amacını belirlemek, önceliklendirmek ve iş birimleri tarafından yürütülen çeşitli iş süreçlerinin önemini göreli olarak belgelendirmektedir. İş etki analizi yapmak bir iş hakkında bilgi almak için mükemmel bir yol olup, bunlara ek olarak süreç iyileştirme için fırsatları da saptama da yardımcı olur.

6.4 Risk Analizi Nasıl Yapılır?

Risk Analizi için tehditlerin gerçekleşme olasılıkları ve bunlrın iş etki analizinden gelen etki puanları dikkate alınarak öncelikli müdahale edilecek ve azaltılacak zayıflıklar göz önünde bulundurulur. Aşağıdaki gibi bir tablo ile basit seviyede riskler listelenip öncelikler çıkartılabilir. Bu tablonun sürekli olarak güncel tutulması ve tehditlerin faydalandığı zayıflıkların sürekli değişmekte olduğu gözden kaçırılmamalıdır. Bunun yanı sıra yeni tehditler ortaya çıkabilmektedir. Tehditlerin ortadan kaldırılması değil gerçekleşme olasılıklarının azaltılmasının mümkün olduğu unutulmamalıdır. Uygulanan kontroller zaman içerisinde geçersiz veya etkisiz duruma gelmiş olabilir, bu nedenle risklerin düzenli periyotlarda gözden geçirilmesi faydalı olacaktır.

Tablo 8: Risk Analizi Tablosu

Süreç/Servis/Fonksiyon	Tehditler	Zayıflıklar	Mevcut Kontroller	Gerçekleşme Olasılığı	Etkisi	Riskin Boyutu

Bu tabloda mevcut kontrollerin eksikliği tehditin gerçekleşme olasılığını belirleyecektir. Olasılık değeri bu bağlamda düşük, orta ve yüksek seviyelerde çıkacaktır. Bunlara 0-10 arası değerler verilebilir. Aynı şekilde süreç veya servisle ilgili iş etkisi bir önceki analizde belirlenmiş olduğundan kolaylıkla buna da düşük, orta, yüksek skalasında 0-10 arası bir puana karşılık gelen bir sayısal değer verilebilir. Riskin boyutu genellikle bu iki değerin çarpımı ile temsil edilebilmektedir.

Riskin Boyutu = Olasılık x Etki

Bu formüle gore ele alındığında risklerden hangileri öncelikli ele alınacaktır sorusuna cevap bulunabilir.

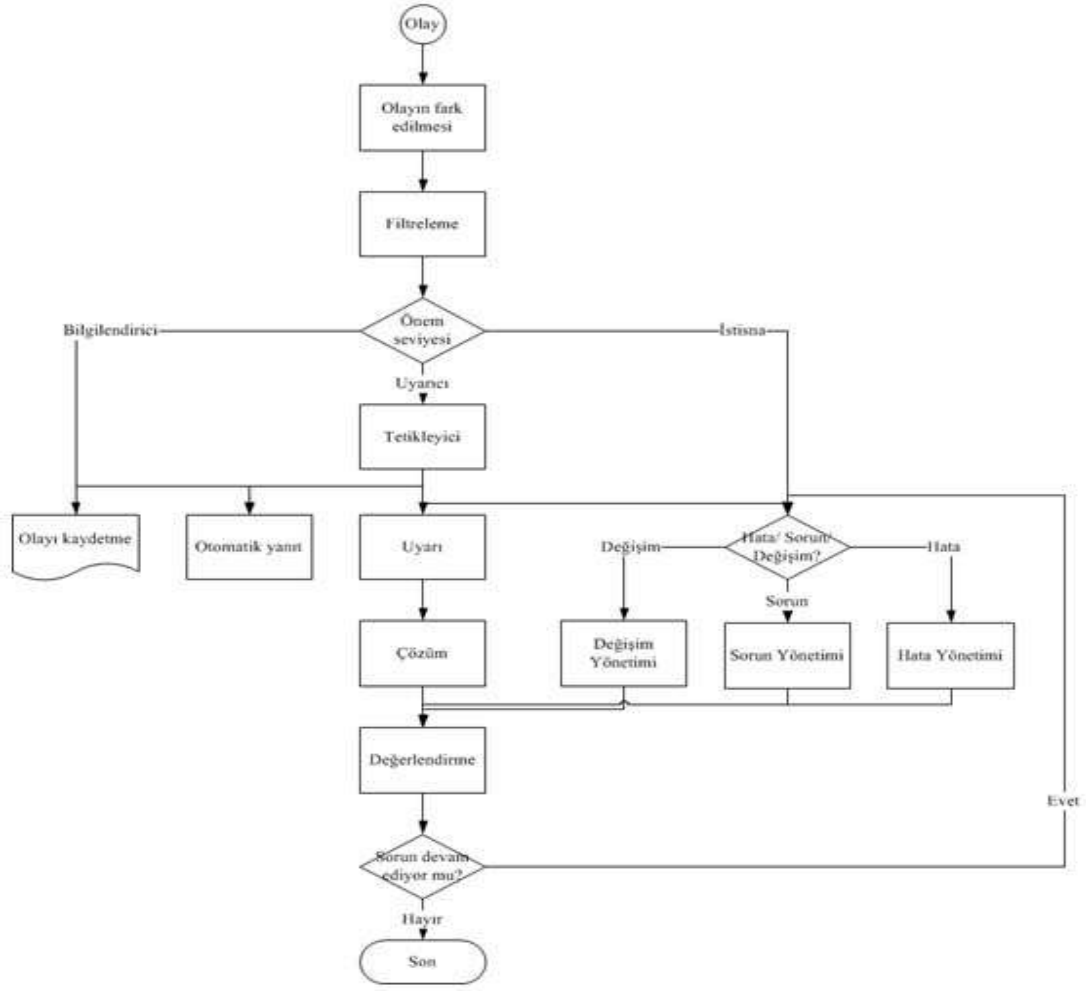
6.4 Olay Yönetimi Nasıl Yapılır?

Verilen hizmetlerde kesinti oluşması veya hizmet kalitesinin düşmesine neden olacak her türlü durum olay olarak nitelendirilmektedir. Olay Yönetimi ise, hizmet süresince meydana gelen olayların tespit edilmesi, analiz edilmesi ve ortadan kaldırılması için doğru kararlar alınmasını sağlar. Olay yönetiminde temel hedefler;

- Tüm olayların kayıt altına alınması,
- Hizmetin en kısa sürede ve aynı kalitede yeniden verilmeye başlanması,
- Hizmet kesintilerinin iş akışları üzerindeki etkisini en az indirmektir.

Olay yönetimi verilen hizmet kapsamındaki kontrol edilebilen tüm bileşenleri kapsar. Sistem odası için gerekli çalışma şartlarının oluşturulması, gerekli seviyede özelliklere sahip iklimlendirme, yangın söndürme sistemleri ve donanımların temin edilmesi alınacak önlemlere örnek olarak verilebilir.

Bir olayın ortaya çıkmasından itibaren aşağıda verilen sürece uygun şekilde olay yönetim süreci gerçekleştirilebilir.



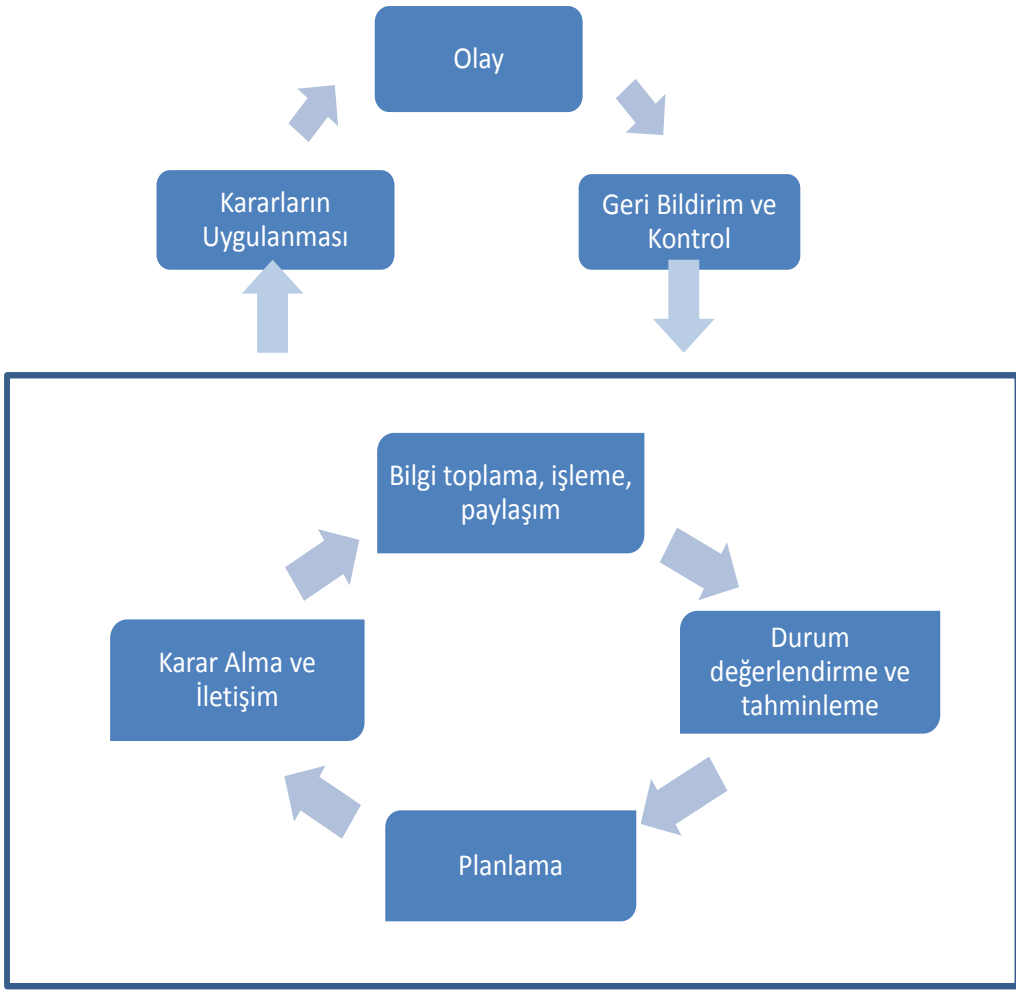
Şekil 11:Olay Yönetim Süreci

Olay yönetimi kapsamında gerçekleştirilen temel faaliyetler;

- Gözlem yapılması,
- Bilgi toplanması, işlenmesi ve paylaşımı,
- Durumun değerlendirilmesi ve tahminleme yapılması,
- Planlama yapılması,
- Kararların alınması ve alınan kararların iletişimi,
- Kararların uygulanması,

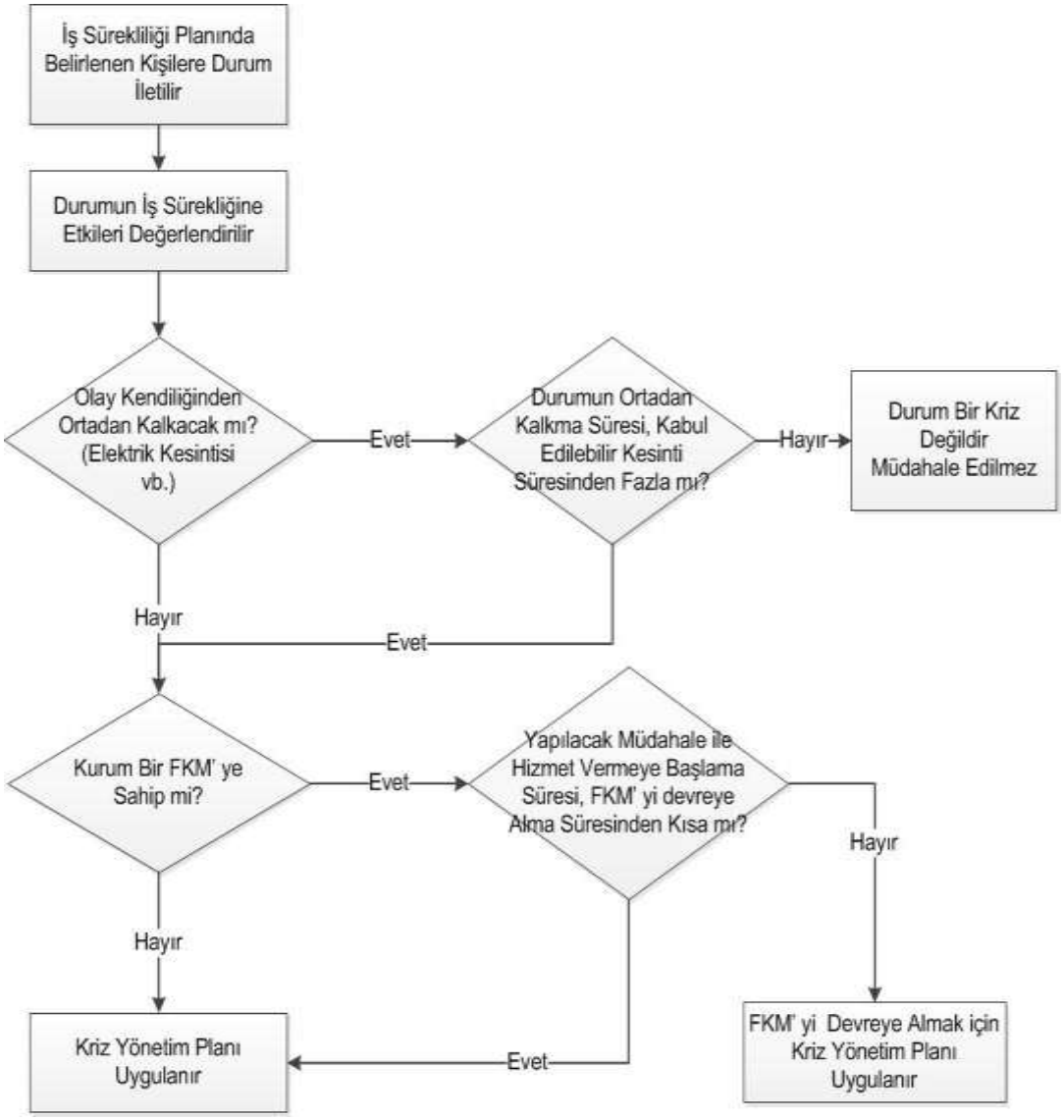
- Geri bildirimlerin toplanması ve kontroldür.

Bu faaliyetler aşağıda verilen örnekte olduğu gibi bir döngü içerisinde gerçekleştirilir.



Şekil 12: Olay Yönetim Döngüsü

Değerlendirme aşamasında, olay tespit edildikten sonra elde edilen bilgiler doğrultusunda, olayın etkileri, ne kadar süre ile hizmet verilemeyeceği, olayın kendiliğinden ortadan kalkma ihtimali, sorunun giderilmesi için gerekli müdahale süresi, Felaket Kurtarma Merkezinin (FKM) devreye alınma süresi dikkate alınarak olayın bir kriz olup olmadığı belirlenir. Yapılan değerlendirme doğrultusunda gerekli planlamalar yapılarak, kararlar verilir. Bu süreç için aşağıda bir örnek verilmiştir.



Şekil 13: Değerlendirme, Planlama ve Karar Alma Süreci

Alınan kararlar uygulanıp, yeniden hizmet verilmeye başlandıktan sonra, uygulanan plan, yürütülen çalışmalar ve varsa karşılaşılan sorunlar değerlendirilerek, Kriz Yönetim Planında gerekli iyileştirmeler yapılmalıdır.

6.5. İş Sürekliliği Planı Nasıl Yapılır?

Amaç ve Kapsam farklılıklarına göre pek çok farklı plandan bahsedilebilir. Bu şekilde oluşturulan planların birimlere, varsayımlara, lokasyonlara, konulara, servislere ve süreçlere göre farklılık göstermesi mümkündür. Aşağıdaki tabloda planların birbirlerinden farklılıkları gösterilmiştir.

Tablo 9: İş Sürekliliği ile İlişkili Diğer Planlar

Planın Adı	Amacı	Kapsamı
İş Sürekliliği Planı	Temel iş operasyonlarının sürdürülmesi için prosedürler	İş süreçleri BT esaslı iş süreçleri
İşe Yeniden Başlama Planı	Felaketten hemen sonra kurtarma prosedürleri	İş süreçleri BT odaklı değil BT esaslı süreçler
Süreklilik Operasyonları Planı	30 güne kadar işlerin sürdürülebilirliği için iş gerekleri, stratejik fonksiyonlar için prosedürler.	BT odaklı değil Kurumsal misyon için kritik Genellikle üst yönetimler için
Destek Sürekliliği / BT Sürekliliği Planı	Genel destek veya major uygulamaları kurtarmak için prosedürler	BT odaklı BT Sürekliliği Planı BT Sistem kesintileri
Kriz İletişim Planı	Kullanıcılar ve halk için ilgili raporları yayınlama ve bilgilendirme prosedürleri	BT odaklı değil Personel ve halk için iletişim araçları
İnternet temelli İhlallere Yönelik Karşılık Planları	Kötü niyetli saldırılara karşı önlemler, taramalar, limit sınırlamaları.	Bilgi güvenliği esaslı Sistemlere veya ağlara yönelik ihlallerin etkileri
Felaket Kurtarma Planı	Alternatif sistemler , imkanlar, varlıklar için ayrıntılı kapasite ve prosedürler	BT bazlı Büyük kesintiler Uzun süreli etkiler
Acil Durum Planı	Fiziksel tehditler için minimum kayıplar, hasarlar için koordinasyon prosedürleri	Personel odaklı BT esaslı Özel durumlar

Her ne kadar farklı amaçlara da hizmet etseler genel olarak planların yapısında bulunması gereken maddeler aşağıda listelenmiştir. Bu listedekiler temel alınarak planlama çalışmaları başlatılabilir. Planlamada dikkat edilecek husus mutlaka teste tabi tutulmaları ve kâğıttan ibaret kalmamalarıdır.

Tablo 10: İş Sürekliliği Planı İçinde Yer Alması Gerekenler

İŞ SÜREKLİLİĞİ PLANI ŞABLONU

1. **Plan Amaç ve Kapsamı**
2. **Plana Dahil Edilen Süreçler, Sistemler ve Öncelikleri**
3. **Tanımlar, Varsayımlar ve Kesinti Durumları**
4. **Erişilebilirlik Kontrol Yapısı ve Kesintisizlik Önlemleri**
5. **Olay ve Felaket Durumları Ekipleri ve Sorumlulukları**
6. **Felaket Kurtarma Sistem Mimarisi ve Olanakları**
7. **Felaket Durumlarında İzlenecek Prosedür**
    a. **Planın Devreye Alınması (invocation kararı)**
    b. **Felaket Durumunda Haberleşme**
    c. **Felaket Durumunda Sistemin Geri Yüklenmesi**
    d. **Felaket Sırasında Çalışma ve Operasyon**
    e. **Normale Dönüş Hazırlıkları**
    f. **Normale Dönüş ve Kurtarma Adımları**
8. **Kontrol Listeleri (Aktivite Checklist)**
9. **Akış Diyagramları**
10. **Haberleşme Listeleri**
11. **Felaket Durumunda Kullanılacak Formlar**
12. **Asıl Sistemlerin Envanteri ve Konfigürasyonu**
13. **Yedek Sistemlerin Envanteri ve Konfigürasyonu**
14. **Felaket Durumunda Destek Alınacak Resmi Kurumlar**
15. **Felaket Durumunda Destek Alınacak Tedarikçiler**
16. **Planın Test Edilme Durumu**
17. **Plan Değişiklik Yönetimi**
18. **Plan Dağıtım Listesi**

6.6. İş Sürekliliği Test/Tatbikatlari Nasıl Yapılır?

İş sürekliliği tatbikatlari, kurumun iş sürekliliği planlarını denemek, geliştirip güncelleştirmek ve planların uygulanmasında görev alacak personeli eğitmek amacıyla düzenli olarak yapılmalıdır. Tatbikatler belirlenmiş planlara göre yapılır ve sonuçları değerlendirilir. Bir tatbikat için aşağıdaki tabloda verilen bilgilerin planda yer alması beklenir.

Tablo 11: Tatbikat Planı Tablosu

İŞ SÜREKLİLİĞİ TATBİKAT PLANI TABLOSU		
Tatbikatın amacı / kapsamı		
Tatbikatın hedefleri		
Tatbikat tarihi / saati		
Tatbikat koordinatörü		
Tatbikata katılacak birimler		
Tatbikatteki Kişiler	Gerçekleşmesi Planlanan Adımlar	Gerçekleşenler
1.		
2.		
3.		
4.		
5.		
Tatbikat metodu		
Tatbikat senaryosu		
Diğer tatbikatlarla ilişkisi		
İncelenecek/ Kullanılacak dokümanlar		

Tatbikatın beklenen hedeflere ulaşıp ulaşmadığının ölçülmesi amacıyla değerlendirme büyük önem taşır. Değerlendirme safhasında tatbikat gözden geçirilerek, gösterilen başarılı tepkiler ile tespit edilen hata ve noksanlıklar belirlenir. Değerlendirmeler yapıcı, düzeltici, geliştirici, gerçekçi ve uygulanabilir olmalıdır.

Tatbikatı icra eden koordinatör birim tarafından Tatbikat Değerlendirme Sonuç Raporu hazırlanarak yayınlanır.

Tablo 12: Tatbikat Değerlendirme Tablosu

İŞ SÜREKLİLİĞİ TATBİKAT DEĞERLENDİRME SONUÇ RAPORU	
Tatbikat tarihi / başlangıç saati ve bitiş saati	
Tatbikatın hedefleri	
Tatbikat senaryosu	
Tatbikat koordinatörü	
Tatbikata katılan birimler	
Plana uygun gerçekleşen faaliyetlerin değerlendirilmesi	
Plana uygun gerçekleştirilemeyen faaliyetlerin değerlendirilmesi	
Kurtarma süre hedefine uyumluluk durumu	
Kurtarma noktası hedefine uyumluluk durumu	
Planda düzeltilmesi gereken uygunsuzluklar	
Uygulamada ve yedek sistemlerde düzeltilmesi gereken uygunsuzluklar	

6.7. Felaket Kurtarma Merkezi Nasıl Kurulur?

Tüm kurumlarda olduğu gibi kamu kurum ve kuruluşları için de hizmet sürekliliği başta itibar ve devletin vatandaşlara olan sorumluluğu olmak üzere kritik öneme sahiptir. Yazılım, donanım, işletim, doğal afet veya fiziksel sorunlardan kaynaklı hizmet kesintilerini en az seviyeye indirmek, mümkün olduğunca ortadan kaldırmak amacıyla kullanılan etkin yöndemlerden birisi felaket kurtarma merkezinin (FKM) oluşturulmasıdır.

Bu bölümde, FKM'lerin kurulması sürecinde dikkate alınması gereken faktörler belirtilirken, kamu kurum ve kuruluşlarının kendine özgü özellikleri çerçevesinde önerilerde bulunulmaktadır.

FKM planlaması iş sürekliliği çalışmasının strateji ve analiz aşamasının gerçekleştirilmesi sonrasında gerçekleştirilmelidir. Kurumun iş süreçlerinin ortaya çıkarılması, kritik iş süreçlerinin belirlenmesi, bu süreçlere ilişkin RPO ve RTO değerlerinin belirlenmesi FKM kurulum planlamasına önemli katkı sağlayacaktır. BT iş süreklilik çerçevesi, BT süreklilik planları, Kritik BT kaynakları, BT süreklilik planının devamlılığı, BT süreklilik planının test edilmesi, BT süreklilik planının eğitimi, BT süreklilik planının dağıtımı, BT hizmet kurtarma ve devam ettirme, Dış ortamda yedekleme, kurtarma sonrası gözden geçirme aşamaları bu raporda ayrıntılı olarak yer almıştır. Bu çerçevede, yedekleme klasik ilkesi, dört yedek (veri, nokta, kaynak, dosya) önerisi anımsanabilir. Dış ortamda yedekleme, bizatihi hedef göstermeye dönüşmemeli, yedekleme merkezi sayısı da artırılabilimelidir.

FKM tasarımı ve kurulumu sürecinin tüm aşamalarında;

- Doğru yazılım, donanım ve fiziksel altyapıya yatırım yapılması,
- Eldeki tüm varlıkların etkin şekilde kullanılması,
- Güvenlik önlemlerinin alınması,
- Harcamaların mümkün olduğunca düşük ama etkin olarak gerçekleştirilmesi hususlarının dikkate alınması gerekmektedir.

Aşağıda, FKM tasarımı ve kurulumu için ele alınması önerilen hususlar listelenmiştir:

a. FKM'ye dahil edilecek iş süreçlerinin belirlenmesi

FKM oluşturulmasındaki ilk adım İş Sürekliliği kapsamına dahil edilecek ve FKM tarafından desteklenecek sistemlerin ve uygulamaların ortaya çıkarılması ve bunlara ait önem derecelerinin belirlenmesidir. Bu çerçevede, öncelikler belirlenerek bütçe çerçevesinde FKM planı oluşturulabilecektir.

b.Yerleşke

Bir FKM tasarımı için kullanılacak yerleşkeye ait kararın verilmesi FKM için alınacak diğer kararlar için temel teşkil etmektedir. Ana yerleşkeden farklı bir yerleşke olması, farklı risk profiline sahip olması, ana merkez ile arasındaki uzaklık, tasarlanan binanın ortak FKM olarak kullanılması, teknolojik altyapı ve kısıtlamalar, FKM'nin deprem vb. etkenlere dayanıklılığı gibi hususlar kurumun iş sürekliliği planlamalarının esaslarını belirlemektedir.

Uzaklık: Kurulacak olan FKM'nin ana merkeze olan uzaklığı yedekleme amacıyla kullanılacak teknolojiyi de şekillendirmektedir. Farklı bir şehirde FKM kurulması deprem gibi doğal afetlere karşı önlem alınmasını sağlamakla birlikte senkron yedekleme gerçekleştirilmesinde kısıtlamalar getirebilmektedir. Uzaklık kararını belirleyen kesin bir ölçü olmamakla birlikte, kuruma ait kritik iş süreçlerinin önemi, ana merkezin risk profili (deprem bölgesi olması, su baskınlarına açık olması, vb.) yedek merkezin aynı şehirde mi, farklı bir coğrafyada mı olması gerektiği konusunda girdi sağlamaktadır.

Kullanım: Uzaklık ile ilgili karar alındıktan sonraki aşama FKM için kullanılacak alanın satın alınması, kiralık olarak tutulması veya ortak kullanım kararının alınmasıdır. Özellikle birbirleri ile ilişkili (örneğin aynı bakanlığa bağlı) kamu kurum ve kuruluşları ortak bir binada FKM kurma yöntemini seçebilirler. Maliyetlerin önemli ölçüde düşürülmesini sağlayabilecek bu yöntemin bir ileri adımı olarak ortak FKM sunucuları ve altyapıyı kullanmalarından bahsedilebilir. Özellikle kamuda vatandaşların kişisel bilgileri, güven ve itibar gibi hususlar değerlendirildiğinde kritik uygulamalar için kurumun kendine ait bir binada FKM kuruluşu tercih etmesi uygun bir yaklaşım olarak değerlendirilebilir. Bütçe, hizmetlerin kritikliği, güvenlik gibi unsurlar bu kararın alınmasında rol oynayan faktörler olmaktadır. Güvenliğin ve güvenilirliğin sağlandığı durumlarda *bulut bilişim* teknolojisi yerleşkeden bağımsız FKM oluşturulmasında alternatif ve maliyeti uygun bir çözüm olarak değerlendirilmelidir.

c.Personel

Personel planlaması bir FKM'nin amacına uygun bir şekilde çalışması için anahtar rol oynamaktadır. Kurum, FKM kurulumu ve işletimi sürecinde personel planlaması gerçekleştirirken aşağıdaki hususları göz önünde bulundurmaladır:

- FKM'de sürekli olacak çalışacak personelin yanı sıra olağanüstü durumlarda görev alacak çekirdek personelin (teknik ve iş) rahat çalışabileceği yeterli büyüklükte ve güvenli bir alan oluşturmalı, gerekli besin, sağlık ve enerji desteği hazır bulundurulmalıdır.

- Olağanüstü durumlarda çalışacak personelin çoklu özelliklere sahip olması olası bir uzman personel eksikliğinde işlerin yürütülebilmesi ve personel yedeklemesinde için avantaj oluşturacaktır.
- Söz konusu personelin iletişim bilgileri, uzmanlık alanları, adres bilgileri vb. güncel ve erişilebilir şekilde hazır olmalıdır.
- Personelin en azından bir kısmının olağanüstü ve acil durumlarda çalışma tecrübesi olması veya eğitim alması özellikle doğal afetlerde önemli faydalar sağlayacaktır.
- Personelin olağanüstü durumlarda FKM'ye ulaşımını sağlayacak tedbirlerin alınması gerekmektedir. Toplu taşımanın bu gibi durumlarda aksayacak olma olasılığı nedeniyle bütçenin uygun olması durumunda özel araçlar tahsis edilme seçeneği düşünülmelidir.
- Personelin FKM'ye ulaşamayacağı düşünülerek alternatif uzaktan erişim ve çalışma teknolojileri değerlendirilmelidir.

d.Fiziksel altyapı

Kurulacak FKM'nin fiziksel altyapısı olağanüstü durumlarda alanın gerek BT bileşenleri gerekse personelin çalışması için kullanışlı bir şekilde tasarlanmalıdır. Örnek fiziksel altyapı özellikleri aşağıda listelenmiştir.

Yükseltilmiş Taban: Su baskınlarına karşı donanım ve tesisat bileşenlerini korumak için yükseltilmiş tabana sahip sunucu odası inşa edilmelidir.

Klima: Sunucu odalarını uygun ve sabit sıcaklıkta tutacak klimalar bulunmalıdır.

Yangın : FKM yangın riskine karşı koruyacak teçhizatlar bulundurulmalıdır.

CCTV: Gerek ana merkezden gerekse FKM yönetim merkezinden sunucuları sürekli olarak izleyebilecek görüntü izleme altyapısı kurulmalıdır.

Kartlı Erişim Sistemi: FKM'ne ve sunucu odalarına sadece yetkili personelin girişine izin verecek biyometrik veya kartlı erişim sistemi kurulmalıdır.

Kesintisiz Güç Kaynakları ve Jeneratörler: FKM'de bulunan tüm sunucular ile diğer donanımların olası bir elektrik kesintisine karşı sürekliliği sağlayacak kapasitede KGK ve jeneratörler kurulmalıdır.

İletişim Ağı: Güvenilir ve yeterli bant genişliğinde iletişim altyapısı kurulmalıdır. Ucuz ve esnek olması nedeniyle, güvenlik önlemleri alınmış kablosuz iletişim ortamı etkin bir çözüm sağlayabilmektedir.

Telefon ve Faks: Olağanüstü bir durumda gerekli personelin rahat çalışması ve etkin bir iletişim sağlanabilmesi amacıyla yeterli kapasitede telefon ve faks cihazı bulundurulmalıdır.

Internet Hizmeti: Olağanüstü durumlarda hizmet verebilecek kapasitede bir Internet altyapısı FKM için kritik bir öneme sahiptir. Telefon trafiğinin yoğun olacağı bu durumlarda, önceden testleri yapılmış ve kurumun servislerini kullanan kullanıcıların birbirleri ile iletişimini sağlayabilecek Internet üzerindeki platformlar önemli faydalar sağlayacaktır. Bu platformlara FKM üzerinden erişim sağlanabilecek altyapı kurumun iletişiminde etkin bir rol oynayacaktır.

e.Veri Yedekleme ve Hatadan Kurtulma

FKM aracılığı ile iş sürekliliğini sağlanmasında temel öncelik verinin kurtarılmasıdır. Yerleşkenin uzaklığı, bütçe, kritik iş süreklerinin RPO ve RTO değerleri, verinin kritikliği, kaybolma durumunda verinin güvenilir olarak tekrar temin edilebilmesi, vatandaşlara veya diğer kurum ve kuruluşlarla olan bağımlılığı gibi faktörler verinin senkron veya asenkron yedekleme ihtiyaçlarını ortaya çıkarmaktadır. Raporun önceki bölümlerinde detaylı olarak açıklanan ana merkez FKM bağlantı şekillerinin (aktif-pasif, aktif-yarı aktif, aktif-aktif) kurulması kararı sözkonusu bu parametreler çerçevesinde alınabilecektir.

f.Güvenlik

FKM'nin fiziksel ve veri güvenliği ana merkez için kullanılan politikalar çerçevesinde değerlendirilmelidir. FKM'de görevlendirilecek personele yeterli güvenlik eğitimleri (gerek fiziksel güvenlik, gerekse BT güvenliği) verilmelidir. Sunucuların ve yazılımların güvenli olarak kuruluşu, işletimi ve sürekliliği sağlanmalıdır. Bu kapsamda, ana merkezde alınan önlemlerin birebir uygulanması olası bir FKM geçişinde aksaklık ve güvenlik zaafiyeti yaşanmasını engelleyecektir.

BÖLÜM 7

SONUÇ

İş sürekliliği teorik bilgilerinde ve gerçek uygulama çalışmalarında gözden kaçırılan sürekliliğin aşağıda açıklanan boyutlarına dikkat çekmekte yarar vardır.

Süreklilik sadece felaketlere odaklanan bir konu değildir. Felaket öncesi, felaket sırasında yapılacaklar ve felaket sonrası yapılacakları kapsayan bir disiplindir. Literatürde konu ele alınırken felaket öncesi sistem tasarımı erişilebilirlik süreci, kapasite yönetimi süreci, bilgi güvenliği yönetimi süreci dikkate alınmadan doğrudan kesinti durumlarına odaklanılmaktadır. Kesinti olduktan sonra veya felaket yaşandıktan sonra yapılacaklar genelde kurum için en pahalı yöntemleri içerir. Genellikle kesinti öncesi sağlam ve kesintiye dayanıklı sistem kurma maliyeti kesinti sonrası kurtarma, kesinti sonrası maliyetler ve prestij faktörleri dikkate alındığında çok daha kolay ve düşük maliyetlidir.

Süreklilik bir proje değildir. İş sürekliliği sistemi kurmak için yapılan çalışmalar ilk başta proje olarak başlayabilse de devamında bunun kritik bir iş süreci olarak üst yönetimin önemli işlerinden biri haline gelmesi gerekmektedir.

Bu süreç yukarıda adını andığımız tasarım süreçlerinin yanı sıra zorunlu olarak olay yönetimi, problem yönetimi, değişim yönetimi, konfigürasyon yönetimi ve sürüm yönetimi süreçlerinin desteğini gerektirir. Bu operasyon süreçlerinin verimli ve etkili olarak çalışmadığı kurumlarda her küçük kesinti felaket riskini taşır. Bu kurumlarda her kontrolsüz değişiklik sürekliliği ve yapılan süreklilik yatırımlarını tehdit eder. Her başarısız geçiş/sürüm felaket boyutuna varabilecek olayları da beraberinde getirir. Konfigürasyonun yönetilmediği sistemlerde ise iş sürekliliği planları ve uygulaması, dayanacağı kararlı sürüm hakkında bilgi sahibi olunmaması halinde işe yaramaz birer dokümana dönüşecektir.

Süreklilik bir ürün ya da yedeklilikle ilgili bir teknoloji değildir. Bu ve benzeri teknolojilerin yüksek erişilebilirlik için doğru ve verimli kullanımını da içinde barındıran başlı başına bir yönetsel konu (finans, satış, üretim vb.) olarak ele alınmalıdır. Altyapı yatırımları doğru bir risk ve iş etki analizi olmadan istenilen sonuçları veremez. Bu anlamda iş sürekliliği yönetim sistemi kurulmadan ve

yukarıda anılan gerekli süreçler kurulup işletilmeden altyapı yatırımları yapılarak oluşturulmuş felaket kurtarma merkezleri atıl yatırımlar olma riskini barındırırlar.

Süreklilik bir alt süreç değildir. Diğer bütün tasarım ve operasyon süreçleriyle koordineli çalışması gereken ve üst yönetimin doğrudan kontrolünde yürütülen bir "yönetim sistemi"dir.

Süreklilik plan dokümanından ibaret bir dokümantasyon çalışması değildir. Kurumlarda sıkça rastlanan bir diğer yanlış uygulamada senaryo bazlı planların dokümante edilmesinin iş sürekliliği olarak ele alınmasıdır. Bu dokümantasyon bir yönetim sistemi olarak kurulan iş sürekliliğinin faydalı ve gerekli bir parçası da olsa onlarca faaliyetten sadece birini oluşturur. Danışmanlık ve belgelendirme kurumlarının odaklandığı deliller genellikle doküman düzeyinde olduğundan kurumlarda iş sürekliliği zaman içersinde dokümantasyon çalışmasına dönüşme riski taşır.

Bu raporda gerçekçi bir iş sürekliliği uygulaması için gerekli bilgi ve uygulama tavsiyelerine yer verilerek rehber oluşturmak amaçlanmıştır. Tüm kurumlara faydalı olmasını temenni ederiz.

KAYNAKÇA

[1] Burhan AYKAÇ, “Kamu Yönetiminde Kriz ve Kriz Yönetimi”, G.Ü. İ.İ.B.F. Dergisi, Sayı 2, Sayfa 123-132, 2001(Erişim Tarihi:26.11.2011)

[2] Prof. Dr. Güven MURAT, Kamuran MISIRLI, “Küçük ve Orta Ölçekli İşletmelerde Kriz Yönetimi: Çaycuma Örneği ”, ZKÜ Sosyal Bilimler Dergisi, Cilt 1, Sayı 1, 2005(Erişim Tarihi:26.11.2011)

[3] İlknur SARIGEDİK, “1994 – 2001 Krizlerine Genel Bakış ve Kriz Yönetimi”, A.Ü. Tezsiz Yüksek Lisans Dönem Projesi, 2008(Erişim Tarihi:26.11.2011)

[4] Levent UZUNÇIBUK, “Yerleşim Yerlerinde Afet ve Risk Yönetimi”, A.Ü. Sosyal Bilimler Enstitüsü, Kamu Yönetimi ve Siyaset Bilimi Anabilim Dalı, Doktora Tezi, 2005(Erişim Tarihi:26.11.2011)

[5] http://www.bilgin.net/YTUMYO/1011/AcilDurum/AcilDurum.pdf, (Erişim Tarihi:26.11.2011)

[6] Standartlar (BS 25999 E. Taşkın ppt 1-4): Business continuity Management Part 1: Code of Practice [1] Business continuity Management – Part 2: Specification (Erişim tarihi: 09.12.2011)

[7] ITIL v3: Servis Design, 2007 (Erişim tarihi:08.12.2012)

[8] http://www.bilgiguvenligi.gov.tr, (Erişim tarihi: 4.11.2011)

[9] http://www.bumko.gov.tr, (Erişim tarihi: 5.11.2011)

[10] Kamu İç Kontrol Standartları Tebliği, 26.12.2007 tarih ve 26738 sayılı Resmi Gazete (Erişim tarihi 5.11.2011)

[11] 26 Ağustos 2008, http://www.continuitycentral.com/feature0607.html(Erişim Tarihi:26.11.2011)

[12] 3 Aralık 2007, http://www.knowledgeleader.com/KnowledgeLeader/content.nsf/Web+Content/PPBusinessContinuityManagementPolicy (Erişim Tarihi:26.11.2011)

[12] 26 Ağustos 2008, http://www.continuitycentral.com/feature0607.html,(Erişim Tarihi:26.11.2011)

[14] Aydın ERGİL, www.issurekliligi.org imtiyaz sahibi, Görüşme Notları,(Erişim Tarihi:26.11.2011)

[15] Gürsoy DURMUŞ, “Risk Analizi”,

www.tkgm.gov.tr/turkce/dosyalar/diger/icerikdetaydh275.pdf,(Erişim Tarihi:26.11.2011)

[16] T.C. İçişleri Bakanlığı İç Denetim Birimi Başkanlığı Sunumu,

isay.icisleri.gov.tr/ortak_icerik/icdenetim/Risk_Belirleme.ppt,(Erişim tarihi:26.11.2011)

[17] Levent UZUNÇIBUK, “Yerleşim Yerlerinde Afet ve Risk Yönetimi”, A.Ü. Sosyal Bilimler Enstitüsü, Kamu Yönetimi ve Siyaset Bilimi Anabilim Dalı, Doktora Tezi, 2005,(Erişim Tarihi:26.11.2011)

[18] http://tr.wikipedia.org/wiki/Risk_y%C3%B6netimi, (Erişim Tarihi:26.11.2011)

[19] Ali DİNÇKAN, TUBİTAK UEKAE, İş Sürekliliği Yönetim Sistemi Kurulumu, 2008,(Erişim Tarihi:28.11.2011)

[20] BS 25999-1 2006 Business continuity management Part 1: Code of Practice,(Erişim Tarihi:28.11.2011)

[21] http://searchdisasterrecovery.techtarget.com/tip/How-to-create-a-business-impact-analysis-for-disaster-recovery-in-10-easy-steps,(Erişim Tarihi:28.11.2011)

[22] 24.01.2011 http://www.datateknik.com.tr/tr/content.asp?ctID=604,(Erişim Tarihi:28.11.2011)

[23] Handan Aybars, http://www.btnet.com.tr/38537-sirketler-bt-sorunlarina-karsi-hazirliksiz.html,(Erişim Tarihi: 24.11.2011)

[24] http://en.wikipedia.org/wiki/Business_continuity_planning,(Erişim Tarihi:28.11.2011)

[25] Didem ESEN, İş Sürekliliği Planlama Metodolojisi,

http://www.nmt.com.tr/egitim/images/haberler/didemesenmakale.pdf,(Erişim Tarihi:26.11.2011)

[26] http://www.marsh.com.tr/service/ri/isyd/isy/index.php,(Erişim Tarihi:05.12.2011)

[27] Burak BAYOĞLU, TÜBİTAK-UEKAE, 2010, İş Sürekliliği konusunda COBIT, ISO/IEC 27001/27002 ve ITIL ne der?, http://www.bilgiguvenligi.gov.tr/bt-guv.-standartlari/is-surekliligi-konusunda-cobit-iso-iec-27001-27002-ve-itil-ne-der.html ,(Erişim Tarihi:05.12.2011)

[28] Dündar Şahin, MBCI, AKUT Arama Kurtarma Derneği Eğitim Kurulu Başkanı, Kurumsal Acil Durum Yönetimi, 2011,https://www.issatr.org/wp-content/themes/issa/images/ISSA-AKUT.pdf,(Erişim Tarihi:05.12.2011)

[29] Ali DİNÇKAN, BTYÖN Danışmanlık, 2010, İş Sürekliliği Yönetiminde Hatalı Yaklaşımlar, http://www.bilgiguvenligi.gov.tr/is-surekliligi/is-surekliligi-yonetiminde-hatali-yaklasimlar.html ,(Erişim Tarihi:05.12.2011)

[30] http://www.deloitte.com/assets/Dcom-Turkey/Local%20Assets/Documents/turkey-tr_ers_BCM-Etkin-Yonetisim-Modeli_041109.pdf ,(Erişim Tarihi:05.12.2011)

[31] Ali DİNÇKAN, BTYÖN Danışmanlık, 2010, İş Sürekliliği Yönetim Sistemi İçin Kritik Başarı Faktörleri, http://www.bilgiguvenligi.gov.tr/is-surekliligi/is-surekliligi-yonetim-sistemi-icin-kritik-basari-faktorleri.html,(Erişim Tarihi:05.12.2011)

[32] http://www.innova.com.tr/solution-detail/Is-Surekliligi-Danismanlik-Hizmetleri/ ,(Erişim Tarihi:05.12.2011)

[33] Aydın Ergil, 2010, İş Sürekliliği ve Sürdürülebilirlik,

http://issurekliligi.wordpress.com/2010/01/28/is-surekliligi-ve-surdurulebilirlik/,(Erişim Tarihi:05.12.2011)

[34] 29 Temmuz 2010, http://www.ag.gov.au/agd/www/nationalsecurity.nsf/Page/Information_For_BusinessBusiness_Continuity,(Erişim Tarihi:05.12.2011)

[35] Aydın Ergil, İş Sürekliliği Nedir?, http://www.issurekliligi.org/,(Erişim Tarihi:10.12.2011)

[36] İş sürekliliği rehberi, http://www.ahder.org/is-surekliligi-rehberi,(Erişim Tarihi:10.12.2011)

[37] http://www.beyaz.net/tr/dokumanlar/felaket-kurtarma-disaster-recovery.html ,(Erişim Tarihi:10.12.2011)

[38] http://www.publicsafety.gc.ca/prg/em/gds/bcp-eng.aspx ,(Erişim Tarihi:10.12.2011)

[39] How to deploy BS 25999. 2007-2010 Avalution, LLC & BSI Management Systems America, Inc (Erişim tarihi:06.04.2012)

[40] A comparison of today's business continuity standards, Paul Kirvan, Mayıs 2011.(Erişim tarihi:06.04.2012)