

T.C.
İSTANBUL YENİYÜZYIL ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ
İŞ SAĞLIĞI VE GÜVENLİĞİ ANA BİLİM DALI



**TELEKOM SEKTÖRÜNDE İŞ SÜREKLİLİĞİ VE ISO 22301-STANDARTLARININ
UYGULANMASI**

YÜKSEK LİSANS TEZİ

Özcan DİMEZ

Tez Danışmanı
Prof. Dr. Gönül KUNT KANDEMİR

Eylül 2019
İSTANBUL

T.C.
İSTANBUL YENİYÜZYIL ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ
İŞ SAĞLIĞI VE GÜVENLİĞİ ANA BİLİM DALI



**TELEKOM SEKTÖRÜNDE İŞ SÜREKLİLİĞİ VE ISO 22301-
STANDARTLARININ UYGULANMASI**

YÜKSEK LİSANS TEZİ

Özcan DİMEZ

Tez Danışmanı
Prof. Dr. Gönül KUNT KANDEMİR

**Eylül 2019
İSTANBUL**

T.C.
İSTANBUL YENİ YÜZYIL ÜNİVERSİTESİ
Sağlık Bilimleri Enstitüsü
Kabul ve Onay

İş Sağlığı ve Güvenliği Ana Bilim Dalı Yüksek Lisans Programı
çerçevesinde yürütülmüş olan bu çalışma aşağıdaki jüri tarafından Yüksek
Lisans Tezi olarak kabul edilmiştir.

Tez Savunma Tarihi: ..09 / 09 / 2019

İmza

Prof. Dr. Gönül KUNT KANDEMİR
İstanbul Yeni Yüzyıl Üniversitesi
Jüri Başkanı

İmza

Doç. Dr. H. Hakan YAVAŞOĞLU
İstanbul Teknik Üniversitesi

İmza

Dr. Öğr. Üyesi Beyrul CANBAZ
İstanbul Yeni Yüzyıl Üniversitesi

İÇİNDEKİLER

Kabul ve Onay

İçindekiler

Semboller ve kısaltmalar

Önsöz

8

1.GİRİŞ

2.GENEL BİLGİLER

2.1. İş Sürekliliği.....	8
2.1.1. İş Sürekliliği.....	8
2.1.2. İş Sürekliliği yönetim sistemi nedir.....	8
2.1.3. Neden İş Sürekliliği Yönetimi?.....	9
2.1.4 İş Sürekliliği Planlaması ve Yönetimi Nedir?.....	10
2.2 İş Sürekliliği Planı İçeriği.....	11
2.3 ISO 22301 in Yapısı ve standartları.....	13
2.4 İSYS Süreçleri	15
2.4.1 IT Continuity Framework / BT Süreklilik Çerçevesi	16
2.4.2 IT Continuity Plans / BT Süreklilik Planları	16
2.4.3 Critical IT Resources / Kritik BT Kaynakları	16
2.4.4 Maintenance of the IT Continuity Plan / BT Süreklilik Planının Devamlılığı	17
2.4.5 Testing of the IT Continuity Plan / BT Süreklilik Planının Test Edilmesi..	
2.4.6 IT Continuity Plan Training / BT Süreklilik Planı Eğitimi	17
2.4.7 Distribution of the IT Continuity Plan / BT Süreklilik Planının Dağıtımı	17
2.4.8 IT Services Recovery and Resumption/BT Hiz. Kurtarma ve Devam Ettirme	18
2.4.9 Offsite Backup Storage / Dış Lokasyonda Yedekleme	18
2.4.10 Post-resumption Review / Kurtarma Sonrası Gözden Geçirme	18
2.5 ISO/IEC 27001/27002	20
2.5.1.1 Bilgi güvenliğini iş sürekliliği yönetim prosesine dahil etme	20
2.5.1.3 Bilgi güvenliğini içeren süreklilik planlarını geliştirme ve gerçekleştirme	21
2.5.1.4 İş sürekliliği planlama Çerçevesi	22

2.5.1.5 İş sürekliliği planlarını test etme, sürdürme ve yeniden değerlendirme	
2.6 ITIL v3	23
3. GEREÇ VE YÖNTEMLER	28
3.1 İş Sürekliliği Başarı Faktörleri	28
3.1.1 Üst Yönetim Desteği.....	28
3.1.2 Stratejik İş Planın Parçası Olma.....	28
3.1.3 İş Sürekliliği Koordinasyonu.....	29
3.1.4 İş Etki Analizi.....	29
3.1.5 Yeterli Bütçe Ayrılması.....	29
3.1.6 Bilgi Teknolojileri Altyapı.....	30
3.1.7 Dokümantasyon.....	30
3.1.8 Periyodik tatbikatlar:.....	30
3.1.9 Eğitim ve bilinçlendirme.....	30
3.1.10 Plan bakım ve güncelleme:.....	31
3.2 Tatbikat Süreci.....	32
3.3. Düzeltici Faliyet.....	34
3.4 İş Sürekliliği Planları.....	35
3.5 Uygulama Süreci.....	35
3.6 Kriz Seviyeleri.....	36
3.7 İş Sürekliliği Organizasyonu;.....	37
3.8 İş Sürekliliği Yönetim Döngüsü.....	38
3.9 İş Sürekliliği Stratejileri.....	39
3.10 İş Sürekliliği Sorumlulukları.....	40

4 BULGULAR	42
4.1 Acil Eylem.....	41
4.2 Kriz yönetimi.....	43
4.2.1 Kriz Yönetimi Planı'nın Hayata Geçirilmesine Sebep Olan Olaylara Örnekler:.....	43
4.2.2 Acil Durum ve Kriz Durumunda Aksiyona Geçecek Gruplar Kriz Yönetim Takımı içerisinde Genel Müdür yardımcıları ve İş Kolu Koordinatörleri'nin Rol ve Sorumlulukları.....	44
4.3 Kriz Yönetim Takımı (KYT) Çalışma Prensipleri.....	45
4.5.1.1 İş kurtarma.....	46
4.5.1.2 Acil Durum ve Kriz Durumunda Aksiyona Geçecek Gruplar.....	46
İş Kurtarma Takım Üyesi.....	46
4.5.1.2 PUKÖ Döngüsü.....	47
4.5.2 Paydaşlar ve regülatif kurumlar.....	48
4.5.3 Acil Durum Yönetimi:.....	48
4.5.4 Kriz Yönetimi:.....	49
4.5.5 İş Sürekliliği Yönetimi:.....	49
4.5.6 Afet.....	49
4.6. Kapsam	50
4.7. Organizasyonun içeriği	50
4.7.1 Organizasyonu ve İçeriğini Anlamak.....	52
4.7.2 İlgili Tarafların İhtiyaç ve Beklentilerini Anlamak.....	52
4.7.3 İş Sürekliliği Yönetim Sisteminin Kapsamına Karar Verme.....	52
4.8 Liderlik	53
4.8.1 Liderlik ve Taahhüt.....	53
4.8.2 Yönetimin Taahhüdü.....	54
4.8.3 Politika.....	54
4.8.4.1 İSY Koordinatörünün sorumlulukları:.....	55
4.8.4.2 UHKE (Ulusal Haberleşme Koordinasyon Ekibi).....	56
4.8.4.3 KYE (Kriz Yönetim Ekibi).....	56
4.8.4.3 Medya ve İletişim Takımı.....	56

4.8.4.4Fonksiyon/Bölüm İS Koordinatörünün sorumlulukları:.....	56
4.8.4.5 İS Takım üyesinin sorumlulukları.....	57
4.8.4.6Tüm çalışanların sorumlulukları:.....	57
4.8.4.7ISO 27001 ve ISO 22301 bağı ve karşılıklı sorumluluklar.....	58
4.9 Planlama	58
4.9.1Risk ve fırsatları belirleme aksiyonları.....	58
4.9.2İş sürekliliği hedefleri ve gerçekleştirmek için planlar.....	59
4.10 Destek	59
4.10.1Kaynaklar.....	59
4.10.2Yetkinlikler.....	60
4.10.2.1Temel yetkinlikler.....	60
4.10.2.2 Koordinatör Yetkinlikleri.....	60
4.10.3 Farkındalık.....	61
4.10.4 İletişim10.5 Doküman ve Kayıt Yönetimi.....	61
4.11 Operasyon	62
1.1Operasyonel planlama ve Kontrol.....	63
4.11.2İş Etki analizi ve Risk Değerlendirmesi.....	64
4.11.2.1Genel.....	64
4.11.2.2 İş Etki Analizi	64
4.11.2.3 İş Etki analizi (IEA) – Kritik Bağımlılık ve Önceliklerin belirlenmesi	66
14.1.2.2.3 Anahtar Ürün ve Hizmetleri Destekleyen Faaliyetlerin Belirlenmesi	
4.11.2.2.4 İş Etki Analizi Onayı.....	67
4.11.2.2.5 İş Etki Analizi Periyotları.....	68
4.11.3 İş sürekliliği stratejileri.....	69

4.11.3.1 Karar verme ve seçme.....	69
4.11.3.1.1 Tedarikçi Sınıflandırma ve Değerlendirme.....	70
4.11.3.2 Kaynak ihtiyaçlarını sağlama.....	71
4.11.3.3 Koruma ve indirgeme.....	71
4.11.4 İş sürekliliği prosedürlerinin oluşturulması ve uygulanması.....	72
4.11.4.1 Genel.....	72
4.11.4.2 Olay müdahale yapısı.....	72
4.11.4.3 Uyarı ve iletişim.....	72
4.11.4.3.1 Teknik kesintiler,.....	73
4.11.4.3.2 Can sağlığı ve güvenliğini etkileyen olaylar.....	73
4.11.4.3.3 İş sürekliliği planları.....	73
4.11.4.4 Network Servis Süreklilik ve Kurtarma Planı Hazırlama:.....	74
4.11.4.4.1 İş Sürekliliği Plan Dokümanı Kapsam Bölümü.....	74
4.11.4.4.2 Roller ve Sorumluluklar.....	74
4.11.4.4.3 Aktivasyon Kriterleri ve Plan Aktivasyonu.....	74
4.11.4.4.4 Plan Seviyesi Stratejiler.....	74
4.11.4.4.5 Aksiyon planları.....	75
4.11.4.4.6 Kaynaklar.....	75
4.11.4.5 Kurtarma.....	75
4.11.5 Tatbikatlar ve testler.....	75
4.11.5.1 Yıllık İSY Tatbikat Programı.....	77
4.11.5.2 Adım-1 Tatbikata hazırlık.....	79
4.11.5.3 Adım-2 Tatbikatın İcra Edilmesi.....	80
4.11.5.4 Adım-3 Tatbikatın Değerlendirilmesi.....	83
4.11.5.5 Tatbikat Sonrası Faaliyetler.....	83
4.12 Performans değerlendirme	84
4.12.1 İzleme, Ölçme, Analiz ve Değerlendirme.....	84
4.12.1.1 Genel.....	86
4.12.1.2 İş Sürekliliği prosedürlerinin değerlendirilmesi.....	86
4.12.2 İç denetim.....	86
4.12.3 Yönetimin gözden geçirmesi.....	86
4.12.4 İyileştirme.....	88

4.12.4.1 Uygunsuzluk ve düzeltici faaliyetler.....	88
4.12.4.2 Sürekli iyileştirme.....	88
4.12. 5 gözden geçirme.....	88
4.2 Olaylar ve tatbikat	89
4.3 Olası İstanbul depreminde iş sürekliliği	

5.TARTIŞMA	100
6.SONUÇ.....	110
7.KAYNAKLAR.....	112
8.ÖZGEÇMİŞ.....	114

SEMBOLLER, KISALTMALAR

KISALTMALAR

ADM	: Acil Durum Masası
ADM Birimleri	: İtfaiye, Polis, Ambulans, AKOM vb
BTK	Bilgi Teknolojileri ve İletişim Kurumu
BGYS	: Bilgi Güvenliği Yönetim Sistemi
BT	: Bilgi Teknolojileri
BTHSY	: Bilgi Teknolojileri Hizmet Sürekliliği Yönetimi
CCR	: Kumanda Merkezi
DS4	: Ensure Continuous Service (Kesintisiz Hizmetin Garanti Edilmesi)
İEA	: İş Etki Analizi
İSYS	: İş Sürekliliği Yönetim Sistemi
İSYT	: İş Sürekliliği Yönetim Takımı
MAO	: Kabul edilebilir maksimum kesinti süresi
RPO	: Hedeflenen veri kaybı
RTO	: Hedeflenen kurtarma süresi
SCADA /ECS	: Denetsel Kumanda ve Veri Toplama Sistemi
MBCO	: Minumum İş sürekliliği hedefi
UEKAE	: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
KYE	: Kriz yönetim ekibi
AFAD	: Afet ve Acil Durum Yönetim Başkanlığı
BTK	: Bilgi Teknolojileri ve İletişim Kurumu
CEM	: Customer Experience Management
Data Center (DC)	: Veri Merkezi
Network Data Center (NDC):	Şebeke Veri Merkezi
Network Operasyon Merkezi (NOC):	Kapsam dahilindeki şebeke bileşenlerinin 7x24 izleme & kayıt açma faaliyetini yürüten, ilk müdahaleyi yapan, gerektiğinde operasyon ekiplerine yönlendirerek çözüm sağlanana

kadar süreci takip edip, olusan arızalarda etki analizi yapılarak bilgilendirme yapan ekiptir.

Siber Olaylara Müdahale Ekibi (SOME): Siber olayların önlenmesi veya zararlarının azaltılmasına yönelik olarak BTK talebi ile oluşturulan ve Teknoloji Güvenlik Bölümü altında yer alan ekip

SCSC-TAM: Service Control&Support Center, Technical Account Manager: Hizmet Kontrol&Destek Merkezi Teknik Müşteri Yöneticisi.

UHKE: Ulusal Haberleşme Koordinasyon Ekibi

Ulusal Siber Olaylara Müdahale Merkezi (USOM): BTK tarafından siber güvenlik olaylarına müdahalede ulusal ve uluslararası koordinasyonun sağlanması amacıyla kurulmuş merkez

RTO(Recovery Time Objective): Hedeflenen kurtarma süresi

MAO(Maximum Acceptable Outage): Kabul edilebilir kesintiye maksimum dayanma süresi.

RPO(Recovery Point Objective): Hedeflenen veri kurtarma miktarı.

MBCO(Minimum Business Continuity Objective): Minimum İş

Sürekliliği Hedefi KYE: Kriz Yönetim Ekibi

ÖNSÖZ

İş Sürekliliği yönetimi, Şirketlerin ve kamu kurumlarının sahip oldukları varlıklarının, faaliyetlerini, herhangi bir Doğal afet , kriz ve siber saldırı durumunda önceden belirlenen seviyede devam ettirebilme yeteneğidir. Özel veya kamu sektöründe faaliyet gösteren kurumlar, bazen farklı riskler ile karşılaşmakta ve bunun sonucu olarak da faaliyetlerinde veya işlerinde itibar ve para kayıpları yaşayabilmektedirler.

Bu riskler deprem, fırtına, sel gibi doğal afetler sonucu oluşabileceği gibi; insan hatalardan, sabotajlardan, enerji kesintilerinden veya dışarıdan gelebilecek zararlı yazılımlar veya siber saldırı sonucunda oluşabilmektedir. Şirketlerin bu tür risklere karşı önceden hazırlıklı olmadıkları sürece hizmetlerini ve kanuni yükümlülüklerini sürdürebilmeleri imkansız hale gelmektedir.

İş Sürekliliği Yönetimi yapısı ve metodoloji gereği insanı temel odağa alır. Bu Tezde İş Sürekliliği yönetimini gerçekleştirecek olan İş Sürekliliği organizasyonunun konumu, ortaya çıkış şekli, rolü ve sorumlulukları sektörel farklılıklar ile harmanlanarak irdelenmektedir. Özellikle Deprem kuşağında olan ülkemizde olası bir afet anında müdahale etme için Haberleşme sektöründe iş sürekliliğinin nasıl sağlanacağı kritik öneme sahiptir. Arama Kurtarma, Lojistik ve Güvenlik konularının aktif olarak çalışabilmesi için iletişimin kesintisiz devam etmesi zaruridir. Özellikle 2011 Van depreminde görüleceği üzere deprem anında hızlı bir şekilde haberleşmede iş sürekliliğinin sağlanması can ve mal kaybı ciddi bir şekilde azaltmaktadır. İş sürekliliği senaryolarının doğru bir şekilde tanımlanması göre ve sorumlulukların dağıtılması ve dönemsel olarak bunların yapılacak tatbikatlar ile desteklenmesi, arama kurtarma başta olmak üzere her alanda hızlı müdahalenin gerçekleşmesini sağlayıp can ve mal kaybının oranını ciddi şekilde azaltacaktır.

Çalışma konusunun seçiminde ve hazırlanmasının her aşamasında değerli bilgilerini ve zamanını benden esirgemedi her fırsatta çalışmamla yakından ilgilenen, yol gösteren, büyük bir ilgiyle bana faydalı olabilmek için çok fazla katkı sunan kıymetli hocalarım Prof. Dr. GÖNÜL KUNT KANDEMİR ve Dr. Öğr. Üyesi Beyrul CANBAZ hocalarıma aynı zamanda varlığından her zaman güç aldığım aileme sonsuz teşekkürlerimi sunarım.



1. GİRİŞ

İş Sürekliliği Herhangi bir doğal afet, doğal afet, sabotaj veya siber saldırılar durumunda kurumların, kurumların ve kuruluşların rezervlerini belirli bir seviyede tutma becerisi. Herhangi bir deprem işinin sürekliliği, doğal afetler, sunucu arızası, ekonomik siber saldırılar, enerji krizleri vb. Taşkınlar. Bu durumda organizasyon, kurum ve kuruluşların kritik ürün, hizmet ve faaliyetlerini çok az zarar harcamak için, kriz anı gerektirir.

İş sürekliliği sistemi olan bir organizasyon, deprem, sel, yangın, teknolojik altyapı kaybı, siber saldırı vb. Afetlerle karşılaştığında, daha önce soğuk kanda geliştirdiği kriz önleme yönetimi planları iş sürekliliği planlarıyla tutarlıdır. Hem kurumun güvenini hem de markanın değerini yok edebilecek durumları profesyonelce yönetir.

İş sürekliliği yönetimi, ilişkili olduğu çevresel değerler ışığında şekillenir. Bir işletme olarak tanımlanan her değer, bir yönetim modeli kullanarak hayata düşürülebilir. Yaşadığımız dönem, çevre ve yaşadığımız değerler bu kültürün oluşumuna yol açar. İş sürekliliği açısından, bu kültür ortak bir kültürde azaltılabilir. Kurumsal yaşamda bir kültür, davranışsal bir model veya uluslararasılaşmasıyla daha belirgin hale gelir: kuruluşlar kendilerini gösterse de, kendilerini taşıdıkları marka ile tanımlıyorlar.

Bir kurumu ve mevcut kültürünü tanımlamaya çalışıldığında, markasıyla da ilişkilendirilir. Böylece, bir marka tüm bu bileşenleri taşır ve söz konusu olduğunda, bireyler, ürünler, süreçler, kaynaklar, hizmetler, iş ortakları ve son kullanıcılar oluşmaya başlar. Marka onların arasında öne çıkıyor. Bütün bunların, iş sürekliliği kavramının ortaya çıkmasıyla kendini göstermeye başladığı görülmektedir. İş sürekliliği kavramı için işin ve sürekliliğin tanımı, neyin yapılacağına karar vermeden önce yapılmalıdır. İş unsurları ve süreklilik, tanımlanmadan önce kültür ve markaya çok katı bir bağımlılık göstermektedir. Süreklilik kültür, iş ise farklı bir marka demektir. Bir markayı kalıcı kılmak için "ruhunun kültürü içerdiğini" söylemek gerekir. İş sürekliliği kavramı, ülkemiz

řartlarına kıyasla yönetim süreçleri açısından farklılıklar göstermektedir. İşletme olarak tanımlanan birçok değer, küresel ölçekte çok uzun zaman önce gerçekleşti. Bu sadece acil durumlarda değil, aynı zamanda günlük yaşamda da ortaya çıkar. Batı'da bireysel girişimciliğin ortaya çıkmasıyla birlikte örgütsel bir modelin gelişimi ülkemizden çok daha erken başlamıştır. Küreselleşmenin bir sonucu olarak, iş sürekliliği yalnızca yerel olarak ele alınmamakta, aynı zamanda bölgesel ve hatta kıtalara da uzanmaktadır. Uluslararası kuruluşlar ve yönetim sisteminin belirli standartları gelişimlerini sağlamıştır.

Diğer disiplinlerde olduğu gibi iş sürekliliğinin ortaya çıkışı; belirli süreçlerin, kaynakların, ürünlerin ve hizmetlerin üst yönetim tarafından oluşturulmasıdır. Kısacası, inandırıcı kurallar yoksa, süreklilik ortaya çıkmaz ve saygı gösterilmesi gerekir. Açıkça ve açıkça, yokluğunda ne ve kime karşı, hangi önlemler ve hangi yaptırımlarla olacağını yazılı olarak. İş sürekliliğini sağlamak için, yasal bir terim ve taraflar ortaya koymak ve düzenleme anlamında bir düzenleyici ve bir eski ortaya koymak gerekir.

Ülke koşulları açısından, hizmetleri tanımlayan bir organ bulunmalıdır. Sektör düzenleyicisi BTK'dır (Bilgi ve İletişim Teknolojileri Yönetimi). Bu alandaki ana yasa 5809 sayılı EHK'dır (Elektronik ve Haberleşme Kanunu). Kanun, sektör için zorunlu ilkeleri getirmektedir. Kanun uyarınca; ulusal güvenlik ve kamu düzeni ile birlikte acil durum, sıkıyönetim, seferberlik, savaş ve doğal afet durumlarında elektronik iletişim hizmetlerinin sağlanmasına ilişkin özel bir kanunun hükümleri. Bu ilkelerden biri: "Une Yasalar veya nesnel nedenlerle aksi belirtilmediği sürece aksini gerektirmedikçe niteliksel ve niceliksel devamlılık, sağlanması şarttır" ilkesidir. (Kaynak.)

Bu araştırmada Telekom sektöründe İş sürekliliği ve ISO 22301 standartlarının uygulanması ve Haberleşmede devamlılığın sağlanması için gerekli metodolojinin oluşturularak can, mal ve itibar kaybının en aza

indirgenmesi, rol ve sorumlulukların netleřtirilmesi. Eđitim planlamalarının oluřturulması, risk analizleri tespiti ve giderilmesine katkı sunacaktır.

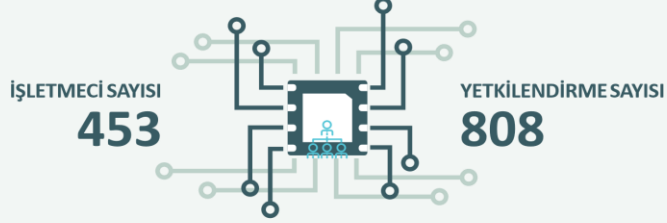


TÜRKİYEDE HABERLEŞME SEKTÖRÜ

5809 sayılı Elektronik ve Haberleşme Kanunu ile sektör için kurallar getirmektedir. Kanuni olarak bu işin denetim yetkisi Bilgi Güvenliği ve İletişim Kurumuna verilmiştir. Kanun uyarınca; ulusal güvenlik ve kamu düzeni ile birlikte acil durum, sıkıyönetim, seferberlik, savaş ve doğal afet durumlarında elektronik iletişim hizmetlerinin sağlanmasına ilişkin özel bir kanunun hükümlerinde belirtilmektedir. Bilgi Teknolojileri ve İletişim kurumunun 2019 Q1 Pazar verileri raporuna baktığımızda aşağıdaki veriler ile Telekom sektörünün büyüklüklerini görebiliriz.

Genel Pazar Verileri

2019 yılının ilk çeyreği sonunda elektronik haberleşme sektöründe faaliyet gösteren işletmeci sayısı **453** olup bu işletmelere verilen yetkilendirme sayısı **808**'dir.



2019 yılı birinci üç aylık dönemde Türk Telekom ve mobil şebeke işletmecilerinin net satış gelirleri toplamı yaklaşık **11,7 milyar ₺** olarak gerçekleşmiştir.

Diğer işletmecilerin aynı dönemdeki net satış gelirleri toplamı yaklaşık **3,7 milyar ₺** olmuştur.



2019 yılı ilk çeyreğinde Türk Telekom ve mobil işletmecilerin toplam yatırım miktarı yaklaşık **1,65 milyar ₺**'dir.

Diğer işletmeciler tarafından aynı dönemde yaklaşık **461 milyon ₺** yatırım gerçekleştirilmiştir.

2019 yılı ilk çeyreğinde toplam **mobil trafik miktarı 66,1 milyar dakika** olurken **sabit trafik miktarı ise yaklaşık 1,6 milyar dakika** olarak gerçekleşmiştir. Bir önceki üç aylık döneme göre mobil trafik miktarı **%1,5**, sabit trafik miktarı ise **%0,9** oranında azalmıştır. Trafikğin büyük bir kısmını (**%93,8**) mobilden mobile giden trafik oluşturmaktadır.



Genişbant pazar verileri;

2008 yılında 6 milyon olan genişbant internet abone sayısının 2019 yılı birinci çeyreğinde 74,7 milyona aştığı ve genişbant abone sayısının bir önceki çeyreğe göre **%0,3** oranında arttığı görülmektedir. Artış oranı “Eve Kadar Fiber” abone sayısında **%13** ve “Kablo İnternet” abone sayısında ise **%2,7** seviyelerinde gerçekleşmiştir. Aşağıdaki şekilde 2008 yılından itibaren

Türkiye'deki toplam genişbant internet abone sayılarına, sabit ve mobil ayrımına yer verilmektedir.



Türkiye'de bağlantı çeşidine göre internet abone sayısı

Mobil pazar verileri;

Mart 2019 sonu itibarı ile Türkiye'de yaklaşık %98,7 penetrasyon oranına karşılık gelen, makineler arası iletişim (M2M) aboneleri dâhil, toplam 80.926.48112 mobil abone bulunmaktadır. Temmuz 2009'da sunulmaya başlanan 3G hizmeti Mart 2016 sonu itibarıyla 65.949.652 aboneye ulaşmış, ancak 1 Nisan 2016 tarihinde 4.5G'nin hayata geçmesiyle 3G aboneliğinden 4.5G aboneliğine hızlı bir geçiş süreci yaşanmıştır. Mart 2019 sonunda 3G abone sayısı 6.380.681'e düşerken 4.5G abone sayısı 72.418.138'e çıkmıştır. Aşağıdaki Şekilde 2G, 3G ve 4.5G mobil abone sayısı ile penetrasyon oranları yıllar itibarıyla karşılaştırılmaktadır.



2. GENEL BİLGİLER

2.1. İş Sürekliliği

2.1.1. İş Sürekliliği

Bir örgütün ürün ve hizmetleri, hizmet dışı kalma süresinden sonra kabul edilebilir bir seviyede tutabilmesi. Kaynak: ISO 22301: 2012 ”

İş Sürekliliği Herhangi bir deprem, sel, yıldırım, sistem arızası, kritik çalışanların ayrılması, ekonomik krizler vb. Bu durumda, kurumlar, kurumlar ve organizasyonlar kritik ürün, hizmet ve az zarar ile harcanacak faaliyetler, kriz zamanında hazır olmaya hazırlar.

İş sürekliliği sistemi, deprem, sel, yangın, proses ekipmanı kaybı, yazılım arızası vb. Bir organizasyon. Daha önce geliştirdiği kriz felaketleri, kriz yönetimi planları, sürekli olarak iş sürekliliği planlarına uymak. Durumları kuruluşun güvenini ve marka değerini bozan profesyonel bir şekilde yönetir.

2.1.2. İş Sürekliliği yönetim sistemi nedir ?

İş Sürekliliği Yönetim Sistemi ISO 22301, __Bu, BS 25999 standartları gibi yönetim sisteminin uluslararası standartlarının ilkelerine verilen addır. Yani, yönetim sistemi politikaları, prosedürleri, talimatları, raporlama ve kontrol yapısını, iç denetim ve yönetim incelemesini içerir.

İş Süreklilik Yönetim Sistemi Yukarıdan aşağıya doğru büyüyen bir piramitle karşılaştırırsak, alt katman bir iş sürekliliği yönetim sistemini ortaya çıkarır ve aşağıdaki başlıkları içermelidir.

İş sürekliliği yönetim sistemine ilişkin üst yönetimin yaklaşımının bir ifadesi olan iş sürekliliği yönetim sistemi politikası, İş Sürekliliği Yönetim Sistemine uygun olarak oluşturulmuştur.

İş Sürekliliği Yönetim Sisteminin sınırlarını ve kapsamını tanımlamak, İş Etkisi Analizi Kritik hizmetleri, süreçleri ve eylemleri, aynı zamanda iş etkisi, risk değerlendirme ve risk değerlendirme süreçlerini kritik hizmetler, süreçler

ve eylemler üzerindeki olası tehditlere uygun olarak analiz eden, Süreklilik planları, test süreci ve süreklilik planlarının yerine getirilmesi

2.1.3. Neden İş Sürekliliği Yönetimi?

Şirketin normal operasyonunu aksatacak olayların öncesinde, bu durumları engellemeye veya aşmaya yönelik, iş kurtarma ve kriz senaryolarının geliştirilmesini, kurumsal iş sürekliliği planlarının, sürekliliğinin sağlanmasını ve uygulayıcıların eğitilmesini temin etmek, şirket içinde iş sürekliliği yönetimi bilinç ve farkındalık düzeyini arttırmaktır.



Şekil 2.1.3

ISYS'nin çabaları sayesinde ticari kesintileri önlemek, yasal yükümlülükleri yerine getirmek, müşteri kayıplarını önlemek, kurumsal itibarı korumak ve ticari işletmeler için pazar payı kaybını önlemek mümkündür. İş sürekliliği ile ilgili araştırmaların iki ana nedeni var. Birincisi, kuruluş düzenleyici sorumluluklarını yerine getirmek için bu eylemleri gerçekleştirir ve ikincisi, hizmet veya bakımın kesintiye uğraması nedeniyle maddi ve manevi zararlarla karşı karşıya kalır.

Genellikle bir hizmet veya ürünün değerinin eksik olduğu düşünülür. Bu nedenle, sürekli çalışmanın başlatılması alışılmış değildir, önceden yapılan çalışmanın önemini bilir. Kuruluşların bu çalışmaya kesintisiz ve zarar vermeden başlayabilmelerini sağlayacak çok fazla araştırma var. Bu çalışmalardan biri çok önemli bir sonuç gösterdi. Gartner tarafından yürütülen bu çalışmada, bir felaketten kurtulan veya ciddi bir başarısızlıktan kurtulan firmaların yüzde 43'ünün tekrar açılmadığı ve yüzde 29'unun iki yıl içinde operasyonları durdurması gerektiği açıklandı.

Kuzey Amerika'da faaliyet gösteren 260 orta ve büyük şirket ile yapılan bir ankete göre, şirketlerin% 52'sinde iş sürekliliği planları var. Bu kurumların% 26'sı çalışanlar için bir iş sürekliliği planı benimsemiş ve revize edemedi. Bu bağlamda, şirketlerin yalnızca% 39'u iş sürekliliği planları geliştirmiştir [7]. Ülkemizde TÜBİTAK UEKAE tarafından 2005 yılında yapılan bir araştırmaya göre, işletmelerin sadece% 11'i iş sürekliliğini askıya alma sürecini kullanmaktadır. Türkiye'de son yıllarda bilgi güvenliği konusunda farkındalığın arttığını ve iş sürekliliği yönetim sisteminde başlatılan yeni kurullarla telekomünikasyon endüstrisinin ciddi öneme sahip olduğunu görüyoruz. Bu çalışma ile bir iş sürekliliği yönetim sistemi oluşturmayı planlayan telekomünikasyon sektörü ülkemizde bu bilincin artmasına yardımcı olmayı hedeflemektedir.

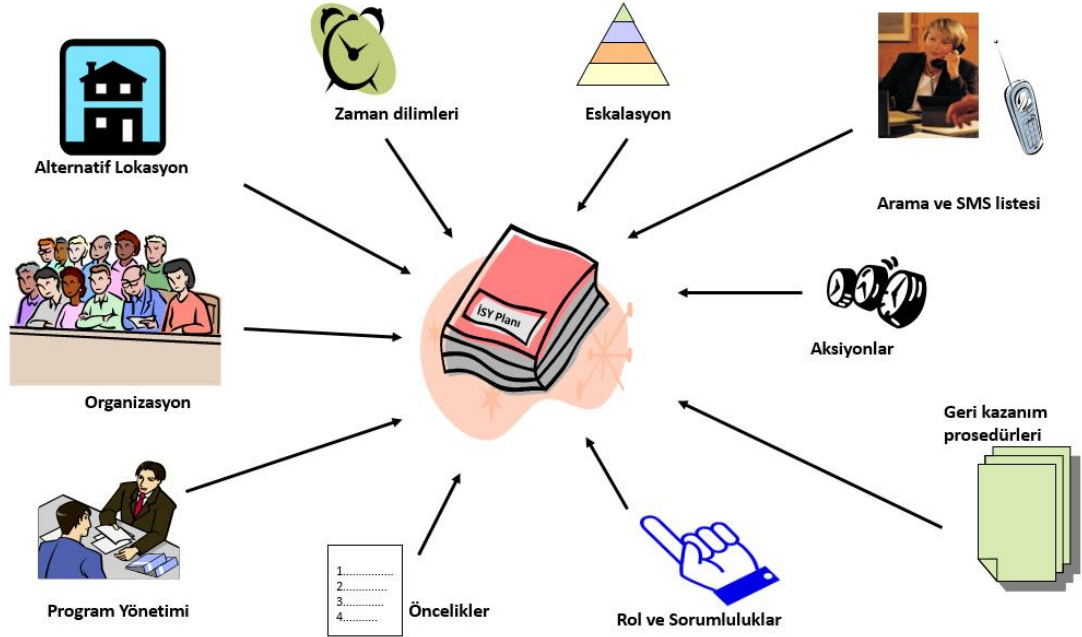
2.1.4 İş Sürekliliği Planlaması ve Yönetimi Nedir?

- Faaliyetin durması ve müşteri kaybına sebep olacak risklerin etkilerini azaltmak için alternatif önleyici eylem planların hazırlanması ve yönetilmesidir.
- Kritik sorumlulukların ve buna bağlı operasyonlarının Kurtarma Stratejileri çerçevesinde devamını sağlamak amaçlı oluşturulan aksiyonların tamamıdır
- Acil Eylem Planları, Kriz Yönetim Planları ve İş Kurtarma Stratejilerini içeren bilgiler ve aksiyonlar ile yönetime destek sağlayan bir sistemdir.

- Kurumsal değerlerin korunması için stratejik alt yapı oluşturarak rekabet için esneklik sağlamayı amaçlayan planlardır.

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 tanımlanmaktadır. İSYS kurulumu ve işletiminin, tek bir referans standart da uygulanmaz. Çeşitli standartlar ve prosedürler takip edilerek yönetim sistemi organizasyonları oluşturmak gerekmektedir. Bu sebeple, İSYS konusunda yönlendirme yapan argümanların proje sürecince kullanımı, hem İSYS gelişimini artıracaktır hem de organizasyonun kaynaklarının daha verimli kullanılmasına öncülük edecektir. İş sürekliliği ile alakalı standartlar şu şekilde sıralayabiliriz. Bu kaynaklardan Şekil 2.3.5'te bahsedilenler, farklı amaç ve detay seviyelerinin yanında birbirlerini büyük oranda tamamlayan ve çok sayıda ortak nokta barındıran dokümanlardır.

2.2. İş Sürekliliği Planı İçeriği



Şekil 2.1.5

Bir iş sürekliliği programı, bir İş Sürekliliği Yönetim Sisteminin tasarımı, geliştirilmesi ve uygulanmasında yapılması gereken eylemleri belirler. Bu çalışmaları yaparken genel kabul görmüş yönetim yöntemlerini kullanmanız önerilir. Bu faaliyetleri yürütürken, programın yönetimi ilgilenen taraflara gerekli bilgileri sağlamalı, ilgili çalışanlar için gerekli eğitimi sağlamalı ve iş sürekliliği fırsatlarını kullanmalıdır. Bir İş Sürekliliği Yönetim Sistemini sürdürmek ve entegre etmek için düzenli olarak yapılması gereken eylemler var. Bir kuruluşun iş sürekliliği kabiliyetlerinin her bölümü periyodik olarak kontrol edilmeli, fayda için test edilmeli ve güncellenmelidir. “Etki Yönetimi”, risk analizi, iş sürekliliği eğitimleri yapılması, alıştırmalar ve daha pek çok aktivite “Program Yönetimi” bölümünde ele alınmıştır. ISYS program yönetimi faaliyetleri şunları içerir: (Woodman 2007).

- a. İş sürekliliği yönetimi için kapsam, rol ve sorumlulukların tanımlanması ve yönetimi
- b. Süregelen işlerin yönetimi için çalışacak kişilerin saptanması
- c. İş sürekliliği tatbikatlarının yönetilmesi
- d. Periyodik gözden geçirme ve güncelleme faaliyetlerinin yönetilmesi
- e. İş etki analizi ve risk değerlendirmesinin gözden geçirilmesi ve gerektiğinde yeniden yapılması
- f. İş sürekliliği yönetim sistemi kapsamında hazırlanmış dokümanların yönetimi
- g. Kurumun iş sürekliliği kabiliyetlerinin performans değerlendirmesi
- h. İş sürekliliği ile ilgili maliyetlerin yönetimi
- i. İş sürekliliği yönetim sistemi ile ilgili değişiklik yönetiminin gerçekleştirilmesi

İş sürekliliği programı yönetimi stoklarını alın; Çalışmadaki olası kesintileri göz önünde bulundurarak ve yönetim tarafından onaylanmış kurtarma stratejilerine uygun olarak, ürünlerin, hizmetlerin ve iş süreçlerinin

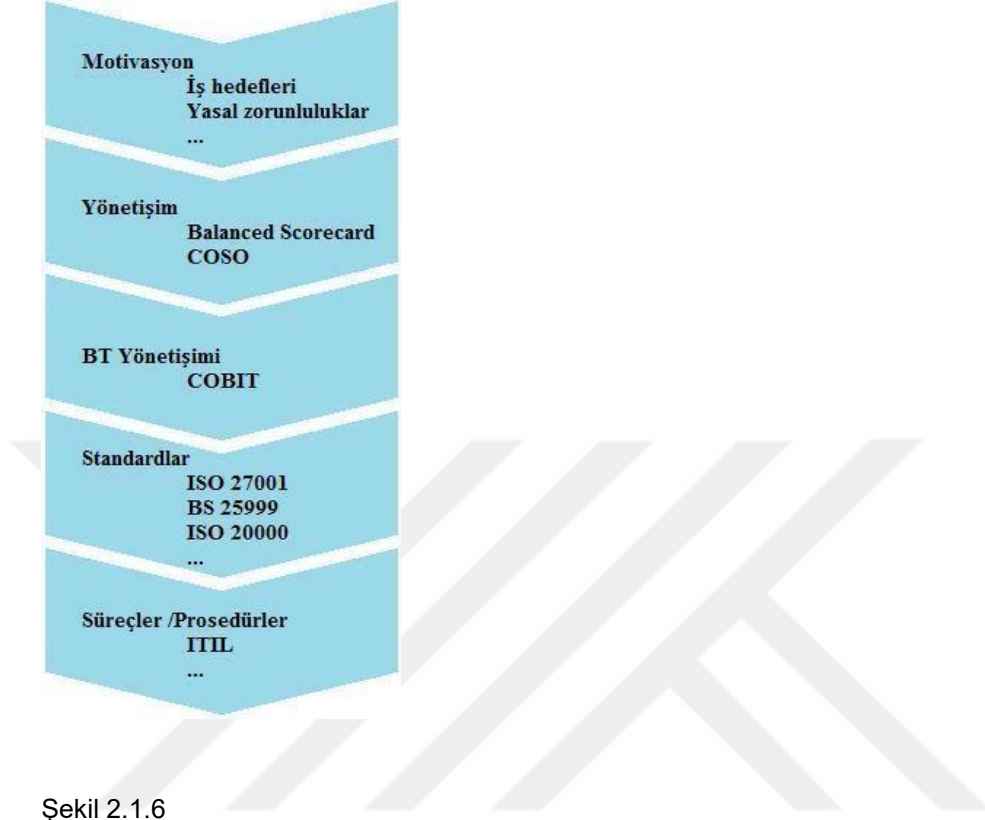
sürekliğini sağlamak için güncel planlar hazırlamak ve sürdürmek. Bütün bu faaliyetlere eğitim, alıştırma, bakım ve testler eşlik etmelidir. (Woodman 2007).

İş Sürekliliği Programı çerçevesinde gerçekleştirilecek faaliyetler yıllık olarak planlanmalı ve yıllık planlar çıkartılmalıdır. Özellikle İş Sürekliliği eğitimleri ve tatbikatları için program hazırlanması son derece faydalıdır.

2.3 ISO 22301 in Yapısı ve standartları

Kurumların kritik iş süreçlerinin sürekliliğini sağlamak veya bir kesinti halinde yeniden faaliyetlerini sağlamak için atılan iş sürekliliği eylemleri, İş Sürekliliği Yönetim Sisteminin bir parçası olarak devam etmelidir. Bir ISMS'nin tek bir referans standardına veya temel belgeye uygun olarak kurulması ve işletilmesi, gelecekteki uyum çalışmaları için ek iş yükü oluşturabilir. Bu nedenle, proje sürecinde ÇYSS'yi yönlendiren belgelerin etkin kullanımı, ÇYSS'nin vadesini artıracak ve kurumsal kaynakların daha verimli kullanılmasını sağlayacaktır. Bu makalede, ISYS'nin oluşturulmasında ve işletilmesinde kullanılacak standart, çerçeve, kavramlar vb.

Açıklanmaktadır. Doküman yönetim sistemleri uyum içinde kullanılabilir.



Şekil 2.1.6

İngiliz Standardı BS BS 25999-1: 2006 İş sürekliliğini yönetmek için bir uygulama kodu lanmış, BSI tarafından 2006 yılında yayınlanmıştır. Bu standarda göre BS25999-2, ISYS'yi oluşturan kurumların denetimi için standardın ikinci kısmı 2007'de yayınlandı. Bu makalede, BS 25999-1: 2006 standardına uygun olarak bir ISMS oluşturulması sırasında, ilgili kontrollerin, uygunluk olarak iddia edilebilecek ISO / IEC 27001, COBIT 4.1, ITIL, vb. Gibi standartlar ve sistemler üzerindeki etkisi veya yasal olarak kurumsal bir amaç olarak, ISYS kurulumu sırasında “proje İS. Kabul edilme ihtiyacından dolayı, genel olarak “proje yönetimi” kavramları dikkate alınmalı ve sonuç ISMS'nin başlangıcı ve bitişi olan bir proje değil, bir yaşam süreci olacağını unutmamalıdır.

2.4 İSYS Süreçleri

BS 25999-1: 2006'ya göre BSYS kurulumunun aşamaları Tablo 1'de gösterilmektedir. Bu makalede, İSYS'nin kurulum adımlarını ayrıntılandırmak yerine BS25999 dışındaki kaynakların etkileşimini ele alacağız. Bir ISM'nin kullanım ömrü ve kurulum aşamaları hakkında daha fazla bilgi için, lütfen [1] ve [2] 'ye bakın.

AŞAMA 1: - Proje Başlangıç Aşaması Proje grubunun oluşturulması

Üst yönetim bilinçlendirmesi Proje Planının hazırlanması

AŞAMA 2 – İş Etki Analizi İş Etki Analizi Risk Analizi

AŞAMA 3: İş Sürekliliği Yönetim Sistemi Kurulumu

İş Sürekliliği Organizasyonunun Oluşturulması

İş Sürekliliği Yönetim Sistemi Dokümantasyonu

AŞAMA 4: İş Sürekliliği Yönetim Sisteminin Hayata Geçirilmesi

İş Sürekliliği Eğitim ve Bilinçlendirme Faaliyetleri

İş Sürekliliği Tatbikat İşlemleri

COBIT; kullanıcılar, denetçiler ve daha da önemlisi, iş süreçlerinin yöneticileri ve sahipleri dört ana alanda 34 üst düzey yönetim görevi ile etkin BT kaynak / süreç yönetimi (PO: Planlama ve Organizasyon, AI: Satın Alma ve Uygulama, DS: Teslim ve Destek, ME: İzleme ve Değerlendirme) sağlanması amaçlanan temel bir belgedir. Bir kuruluşta BT yönetimini sağlamak ve iş gereksinimlerini karşılamak için BT stratejilerini yönlendirmek öncelikli hedefleri arasındadır. BT yönetimi ve işleyen bir ISMS için kesinlikle gerekli olan diğer destekleyici süreçlerin yanı sıra, bu bölüm COBIT ortamında iş sürekliliğini sağlamayı amaçlayan sürekli hizmet sağlayan kontrol (süreç) DS4'ü de açıklamaktadır.

DS4 süreci, kritik iş süreçlerine hizmet eden BT hizmetlerinde kesinti olasılığını ve bunların iş süreçleri üzerindeki etkisini en aza indirmeyi amaçlar. Bu amaçla, BT departmanı, dış mekanlarda süreklilik planları

oluřturmanızı, eğitim vermenizi, süreklilik planları ve bilgileri sürdürmenizi önerir. DS4 sürecinde verilen on ayrıntılı kontrol hedefi ařađıda listelenmiřtir.

2.4.1 IT Continuity Framework / BT Süreklilik Çerçevesi

Bir kurumdaki iş sürekliliđi yönetimini desteklemek için, BT sürekliliđinin yapısını tanımlayan bir süreç geliřtirmeniz gerekir. Felaket kurtarma ve BT sürekliliđi planları bu yapıya uygun olarak geliřtirilmelidir. İç ve dış servis sađlayıcılarının rol ve sorumluluklarının, yönetim seviyelerinin, müřterilerin tanımlanması gereken organizasyonel yapı.

2.4.2 IT Continuity Plans / BT Süreklilik Planları

BT sürekliliđi planlarının, BT sürekliliđi yapısına uygun olarak geliřtirilmesi gerekmektedir. İşletme üzerindeki etkinin analiz edilmesi, iş sürekliliđi risklerinin göz önünde bulundurulması, alternatif işlem yöntemlerinin belirlenmesi, kurtarma yöntemlerinin belirlenmesi, kullanım kılavuzlarının hazırlanması, ayrıntılı rol ve sorumlulukların tanımlanması, gerekli prosedürlerin tanımlanması, iletişim yöntemleri ve test yaklaşımının hedeflenmesi gerekmektedir.

2.4.3 Critical IT Resources / Kritik BT Kaynakları

BT kaynakları, kritik iş süreçleri için belirlenen öncelik seviyelerine uygun olarak geri yüklenmelidir. Daha az önemli BT kaynaklarının öncelikli kurtarılması dođru deđildir. İş sürekliliđi ve toparlanması için planlama yaparken, aksaklık süresini, önceliklendirmeyi, maliyetleri kabul edilebilir bir seviyede tutmayı, yasal yükümlülüklere ve sözleşmelere uygunluđu göz önünde bulundurmalısınız.

2.4.4 Maintenance of the IT Continuity Plan / BT Süreklilik Planının Devamlılığı

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.

2.4.5 Testing of the IT Continuity Plan / BT Süreklilik Planının Test Edilmesi

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

2.4.6 IT Continuity Plan Training / BT Süreklilik Planı Eğitimi

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.

2.4.7 Distribution of the IT Continuity Plan / BT Süreklilik Planının Dağıtımı

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

2.4.8 IT Services Recovery and Resumption/BT Hiz. Kurtarma ve Devam Ettirme

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.

2.4.9 Offsite Backup Storage / Dış Lokasyonda Yedekleme

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.

2.4.10 Post-resumption Review / Kurtarma Sonrası Gözden Geçirme

Bir olay veya kazadan sonra IT hizmetlerinin başarılı bir şekilde restorasyonundan sonra, planın yeterliliğini değerlendirmek ve gerekirse güncellemeleri yapmak için bir prosedür / süreç geliştirilmelidir.

Proses odaklı yaklaşımın bir sonucu olarak COBIT, DS4 sürecini tanıtan ve Tablo 2'de gösterildiği gibi DS4 işleminin sonuçlarından faydalanan diğer süreçleri (daha yüksek seviye yönetim hedefi) belirlemiştir. COBIT, bu süreçlerle olan ilişkiyi göz önüne alarak ISMS içerisinde kullanılmalıdır. DS4 hariç. DS4 kontrol hedefinin doğrudan COBIT'de tanımlanan 34 üst düzey kontrol hedefinin 11'yle doğrudan bağlantılı olması, ISMS'yi diğer iş süreçleriyle entegre etme ihtiyacını da göstermektedir.

Tablo 2.4.10 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 değerlendirilmesi.
	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 yönetilmesi.) ve	GA	Hizmet seviyesi anlaşmaları.
	ÇV	Felaket anında kullanılacak hizmetlerin gereksinimleri, roller ve sorumluluklar.
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.

2.5 ISO/IEC 27001/27002

ISO / IEC 27002, 0,1 Bölüm 0.1 Bilgi güvenliği nedir? ", Bilgi güvenliği, iş sürekliliği sağlar, iş risklerini azaltır, yatırım getirisini ve iş fırsatlarını artırır. belirledi. Görüldüğü gibi, iş sürekliliği çalışmaları, bilgi güvenliği yönetim sistemi kurmanın temel görevlerinden biri olarak adlandırılmaktadır. ISO / IEC 27001 standardının Ek A bölümünde listelenen on bir ana temadan biri iş sürekliliği yönetimidir.

ISO / IEC 27001 standardı "2.5 İş Sürekliliği Yönetimi", "2.5.1 İş Sürekliliği Yönetimi Bilgi Güvenliği Sorunları" adı güvenlik kategorisini / kontrol hedefini içerir. İş kesintilerini önlemek ve önemli iş süreçlerini ciddi bilgi sistemi başarısızlıklarından veya başarısızlıklarından korumak ve zaman içindeki sürekliliğini sağlamak için, özel kontrol hedefleri 2.5.1 uyarınca beş kontrol getirilmiştir. Bu kontroller aşağıda listelenmiştir.

2.5.1.1 Bilgi güvenliğini iş sürekliliği yönetim prosesine dahil etme

Kuruluş genelinde iş sürekliliği için, bu amaçla ihtiyaç duyulan bilgi güvenliği gereksinimlerini ifade eden bir yönetilen proses geliştirilmeli ve sürdürülmelidir.

2.5.1.2 İş sürekliliği ve risk değerlendirme

İş proseslerinde kesintilere yol açan olaylar, bu tür kesintilerin olasılığı ve etkisi ve bunların bilgi güvenliği için sonuçları ile birlikte tanımlanmalıdır.

2.5.1.3 Bilgi güvenliğini içeren süreklilik planlarını geliştirme ve gerçekleştirme

Önemli iş proseslerinde yaşanan kesintileri ya da başarısızlıkları takiben iş operasyonlarını sürdürmek ya da onarmak ve bilginin gerekli seviyede ve gerekli zaman ölçeklerinde kullanılabilirliğini sağlamak için planlar geliştirilmeli ve gerçekleştirilmelidir.

2.5.1.4 İş sürekliliği planlama Çerçevesi

Tüm planların tutarlı olmasını sağlamak, tutarlı şekilde bilgi güvenliği gereksinimlerini ifade etmek ve test ve bakım önceliklerini tanımlamak için tek bir “iş sürekliliği planları çerçevesi” oluşturulmalıdır.

2.5.1.5 İş sürekliliği planlarını test etme, sürdürme ve yeniden değerlendirme

İş sürekliliği planları, güncel ve etkili olmalarını sağlamak için, düzenli olarak test edilmeli ve güncelleştirilmelidir.

ISO/IEC 27001 standardının iş sürekliliği yönetimiyle doğrudan ilişkili bu kontrolleri haricinde ISO/IEC 27002 standardının ilgili başlıkları altında iş sürekliliğiyle ilgili şu gereksinimler belirtilmektedir.

1. Bilgi güvenliği politikası dokümanında iş sürekliliği yönetimiyle ilgili politika ve diğer dokümanların özet açıklamasının verilmesi.

2. İş sürekliliği planlamasıyla ilgili rollerin ve sorumlulukların tanımlanması.
3. İlgili otoritelerin bağlantı bilgilerinin bulundurulması.
4. İş sürekliliği planlarının varlık envanterinin bir parçası olması.
5. Yeni bilgi sistemleri kurulumu, yükseltmeler, yeni sürüm sistem kurulumu vb. için belirlenecek Kabul kriterleri arasında iş sürekliliği anlaşmalarının göz önünde bulundurulması.
6. Zararlı yazılım saldırıları sonrasında kurtarma amaçlı iş sürekliliği planlarının hazırlanması.
7. İş sürekliliği planlarının gereksinimlerinin karşılanacağından emin olmak üzere sistem yedeklerinin düzenli olarak test edilmesi.
8. Uzaktan çalışma ihtiyacı için iş sürekliliği planlamasının yapılması.
9. Kaybolan ya da hasar gören kriptografik anahtarlarla ilgili iş sürekliliği planlamasının yapılması.
10. Sistemlerde yapılan değişiklikler sonrasında iş sürekliliği planlarının da uygun şekilde güncellenmesi.

İş Sürekliliği Yönetim Sistemleri (ISMS), bilgi güvenliği yönetim sistemlerine (ISMS) benzer bir yönetim sürecidir. ISMS araştırmasının ana aşamalarından biri olan envanter varlıkları iş üzerindeki etki analizindeki süreçlerle ilişkilendirilmesi gereken kaynakları içerir. ISMS içinde geliştirilen bilgi güvenliği risk analizi yöntemi iş sürekliliği risklerinin belirlenmesinde de kullanılabilir. İşlemler için izin verilen kesinti (RTO), işlemi destekleyen bilgi varlıklarının değerleriyle eşleşecektir. Bu bölümden görülebileceği gibi, ISMS, ISMS'nin bir parçası olarak tasarlanabilir.

2.6 ITIL v3

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. ITIL v3 (Service Design) BT Hizmet Sürekliliği Yönetimi (BTHSY)'nin amacı aşağıdaki gibi özetlenebilir:

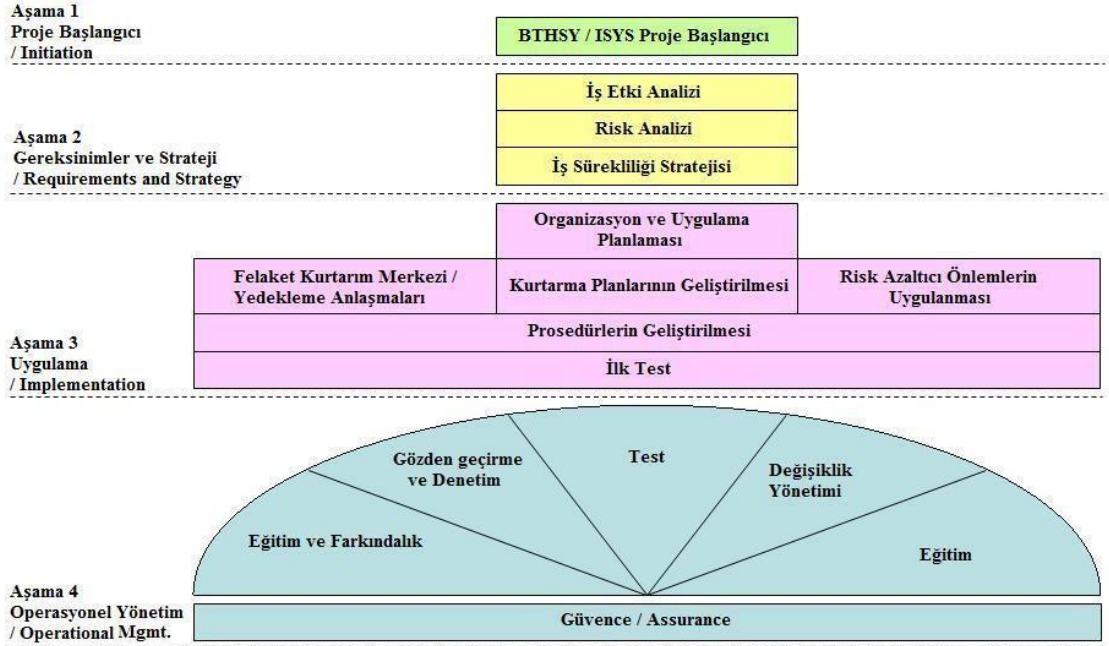
1. BT Hizmet Süreklilik planlarıyla, ilgili BT kaynaklarını ve hizmetlerini gerekli durumlarda iş ihtiyacını karşılayabilecek şekilde çalışır hale getirerek kurumun genel İş Sürekliliği Yönetim Sistemi sürecini desteklemek.
2. BT kaynaklarının iş süreçlerine olan etkisi ya da iş ihtiyaçlarındaki değişikliklerin planlara yansıtıldığından emin olmak üzere düzenli İş Etki Analizi(Business Impact Analysis) yapılması.
3. Düzenli (BT hizmet sürekliliği) risk analizlerinin yapılması.
4. BT hizmet sürekliliği ve kurtarma çalışmaları konusunda diğer departmanlara tavsiyeler verilmesi, rehberlik edilmesi.
5. BT hizmetlerinin erişilebilirliğini artırıcı proaktif önlemlerin maliyet etkin olduğu sürece uygulanması.

BTHSY süreçleri Şekil 1'de gösterilmiştir. Daha detaylı açıklamalar için [3] kaynağına başvurulabilir.

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

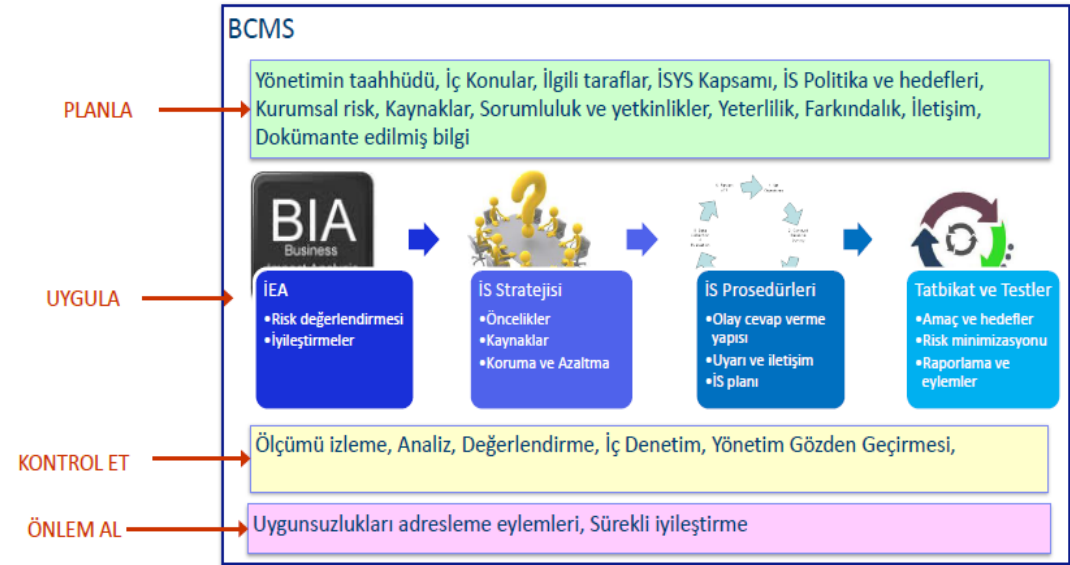
entegre olarak düşünölmelidir. ITIL BTHSY, iş sürekliliđi konusunda global kabul görmüş çerçeveye bađlı kalmakla birlikte daha genel bir İş Sürekliliđi Yönetim Sistemi'ne ihtiyaç duymaktadır. İş Sürekliliđi planlamasının kritik bir parçası olan BT hizmet/kaynak sürekliliđinin sađlanması için detaylı prosedürler tanımlanmıştır. BTHSY çalışmaları, İSYS sürecini destekler rol üstlenecektir. Genel İSYS kurulmadan yapılacak BTHSY çalışmalarında, yanlış varsayımlar yapılması, kullanılmayacak planların üretilmesi, kurum genelinde iş sürekliliđi süreci sahibinin BT/IT departmanı olduđu, gereksiz teknoloji çözümlerinin üretilmesi gibi muhtemel sorunlara yol açacaktır.



Şekil 2.6.1

İSYS açısından, bir ISMS oluşumunu tanımlayan veya İSYS kurulumunu farklı bakış açılarından (bilgi güvenliđi, BT hizmet sürekliliđi, BT yönetimi, vb.) Destekleyen destekleyen COBIT, ITIL, 27001/2 standartları ve yapıları dikkate alınmıştır. İSYS'in yaşam döngüsünü tanımlayan BS25999

standardına uygun olarak kullanılabilen bu kaynaklar, bu standardı farklı bakış açıları ve hedeflerle desteklemekte ve belirtilmeyen bazı noktalardaki eksikliklerini ortadan kaldırmaktadır. Artan pazar payı ve benzeri. Uyum motivasyonu günden güne artıyor ve İSYS araştırmasının başlangıcından itibaren, kurumlarda makul olmayan harcamaları önleyecek olan bu kaynakları dikkate almak için çeşitli sektörlerde mevzuatın zorunlu hale gelmesi bekleniyor. BT ve iş sürekliliği stratejilerini kurumsal iş stratejilerine uygun olarak tanımlamak, kalite yönetim sistemleri, BT yönetim süreçleri, ISMS, İSYS gibi yönetim sistemlerinin birbirinden bağımsız olarak tek bir yönetim sistemi içerisinde koordine edilmesini sağlayacaktır. İSYS konusunda yönlendirme yapan SS 540, NFPA 1600, HB292, ISO/IEC 20000, NIST SP 800-34 vb. kaynakların da incelenmesi, İSYS projelerine katma değer sağlayacaktır



Şekil 2.6.2

ISO 22301:2012 standardının Madde 4'ü gereğince iş sürekliliği yönetim sistemi ile ilgili tüm tarafların iş sürekliliği gereksinimleri analiz edilmelidir.

İş sürekliliğini etkileyen tüm iç ve dış taraflar analiz edilir. İç ve dış tarafların Şirketten beklentileri ve Şirket' in iş sürekliliği kapsamında ilgili taraflardan beklentileri analiz dokümanında bulunur. İlgili taraf analizinin yapılmasından Şirketin İş Sürekliliği Program yönetimi ve iş sürekliliği koordinatörleri sorumludur.

İlgili taraf analizlerine ek olarak uymakla yükümlü olunan yasalar düzenlemeler belirlenmelidir. Tabi olunan yasal yükümlülükler bir tablo halinde tutulur. Bu tablo Şirket İş Sürekliliği Yönetimi ve Hukuk ve Regülasyon ekibleri ile birlikte hazırlanır ve güncel tutulur.

Şirketlerin ana faaliyet alanını etkileyen düzenlemelerin ve yasaların takip edilmesi ve değişikliklerin Şirket ve grup içerisinde duyurulması, bunların olası yansımalarının analiz edilmesi ve bu kapsamda etkilenebilecek şirketlere ve ilgili birimlere bilgilendirme yapılması, olası risklerin bildirilmesi, gerekli aksiyonların alınmasının sağlanması, Hukuk bölümü tarafından gerçekleştirilir.

Yasal ve Regülatif düzenlemeler ilgili kurum tarafından resmi yazı ile iletilebilir veya değişen Kanun ve düzenlemeler Hukuk ve Regülasyon Stratejileri bölümü tarafından takip edilerek varsa uyulması gereken konular belirlenir. Uyumun gerçekleşeceği termin genellikle resmi Kurumlar tarafından net bir şekilde belirtilir. Resmi yazı Hukuk ve Regülasyon bölümüne ulaşır ulaşmaz ilgili departmanlar ile gerekirse açılış toplantısı yapılarak yükümlülüklerin net bir şekilde anlaşılması sağlanır, riskler belirtilir ve bir proje planı çizilir. Sorumlu kişiler ve termin belirlenir. Ardından uyum ekibi yükümlülüklerin zamanında ve tam bir şekilde sağlandığını açılan projeler ile

takip eder ve sonuçlandırır. Uyum projeleri ile ilgili düzenli bilgilendirmeler üst yönetime yapılarak gerektiğinde destekleri alınır.

Tabi olunan yasal ve regülatif yükümlülüklere uyum senelik olarak Hukuk ve Regülasyon bölümleri tarafından kontrol edilir. Grup şirketlerinde bu işlemi ilgili hukuk ve regülasyon birimi veya görev verilen birim yerine getirir.



3. GEREÇ VE YÖNTEMLER

3.1. İş Sürekliliği Başarı Faktörleri

İş sürekliliği yönetiminde, organizasyon farkı yönetmeksizin ele alınması gereken temel hususlar bulunmaktadır. Bu hususların diğer kuruluşlarda olduğu gibi Telekom operatörlerinde de gerçekleştirildiği taktirde faaliyetler aksamaya uğramadan güvenli bir şekilde devam edecektir. Bu maddelerden bir veya birkaçında problem olması durumunda iş sürekliliği çalışmalarından beklenen faydanın alınamayabilir.

3.1.1 Üst Yönetim Desteği: İş sürekliliği araştırması için üst düzey yönetim onayına ihtiyacınız vardır.

Proje sırasında farklı seviyelerde yönetim onayı gerekir. Yapılan iş için yönetim onayını almak, kurum genelinde iş almayı kolaylaştırır. BS25999, iş sürekliliği sürecine üst yönetimin katılımının, ISMS'yi örgüt kültürüne uygun bir şekilde anlamak, desteklemek ve uyarlamak için atılmış bir adım olduğunu belirtiyor.

Bu süreçler sırasında üst yönetim sürekli raporlar, toplantılar ve alıştırmalar sonuları şeklinde bilgi almalı ve bu süreçte sürekli olmalıdır.

3.1.2 Stratejik İş Planının Parçası Olma: İş sürekliliği kendi başına bir süreç olmamalı, stratejik hedeflere uygun olarak geliştirilmeli ve stratejik bir planın parçası olmalıdır. Kurumun işleyişinde herhangi bir problemden kaçınmak için daima güncel olmalı ve ihtiyaçları karşılamalıdır.

İş sürekliliğinin stratejik iş hedeflerine uygun olarak geliştirilmediği veya stratejik hedeflerde gerçekleştirilen değişikliklere uygun olarak gerekli çalışmaların yapılmadığı durumda iş süreçlerinde kesintiler yaşanması söz konusudur.

3.1.3 İş Sürekliliği Koordinasyonu: İş sürekliliği, bir grubun veya kişinin yalnız yapabileceği bir faaliyet değildir. Bu kurumun birçok bölümünü içeren bir çalışmadır ve insanlar farklı işler yaparlar. Son kullanıcı bile bir şeyler bilmeli ve yapmalı. Bazı kurumlar iş sürekliliğini yönetmek için ayrı gruplar oluşturdular. Bir kurumda iş sürekliliği yönetim sisteminin sürekliliğini sağlamak için gerekli insan kaynaklarını ve koordinasyonu sağlamak, acil durumlarda iş sürekliliğinden beklenen faydaları sağlamak için en önemli adımlardan biridir.¹

3.1.4 İş Etki Analizi: İş sürekliliği, iş etki analizi ismi verilen çalışmanın üzerine inşa edildiği için çok önemlidir. Kurumun ilgili bölümlerinden faaliyetlere hakim kişilerin çalışmalarda yer alması gereklidir. Bu çalışma sonunda kurum süreçlerinin kritikliği, süreçler için kabul edilebilir kesinti süreleri (RTO, RPO) ve maksimum kabul edilebilir kesinti süreleri (MTPoD) belirlenmektedir. Bu çalışma sırasında ayrıca risk analizi kullanılarak süreçlerde kesintiye neden olabilecek riskler ortaya çıkarılmaktadır. İş süreçlerinin önemini ve süreçlerde kesintiye neden olabilecek olayların belirlenmesi uygulanacak karşı önlemlerin seçilmesi için son derece kritiktir. Bu sebeple iş etki analizi, iş sürekliliğinin başarıya ulaşmasında üst yönetim desteği kadar önemli bir başarı faktörüdür (Woodman 2007).

3.1.5 Yeterli Bütçe Ayrılması: İş etki analizi çalışması sonucunda uygulanacak kontrollere karar verilmektedir. Bu kararlar genellikle iş sürekliliği stratejileri olarak adlandırılmaktadır. Kontrollerin yerine getirilmesi için yapılacak çalışmaların bazılarının maliyeti çok düşük olabileceği gibi gerektiğinde felaketten kurtarma merkezi kurulumu gibi yüksek maliyetli çalışmaların yapılması da gerekebilir. Bu sebeple iş etki analizinde belirlenen kabul edilebilir kesinti sürelerinin sağlanması için gerekli bütçenin ayrılması veya planlanması oldukça önemlidir (Woodman 2007).

¹ BS 259991 2006

3.1.6 Bilgi Teknolojileri Altyapı: Birçok iş sürecinin BT bağımlılığı yüksektir. Bilgi teknolojileri altyapısının süreklilik ihtiyaçlarına uygun olması süreklilik ihtiyaçlarının karşılanması için büyük öneme sahiptir. Sunucuların, haberleşme hatlarının, enerji altyapısının yedekli yapıda çalışması BT'nin sürekli hizmet verebilmesi için gereklidir. Bunlara ek olarak ana merkezde bulunan verinin felaketten kurtarma merkezine gönderilmesi gereklidir. Bu işlemleri gerçekleştirecek altyapıya sahip olmadan olağan üstü bir durumda kabul edilebilir kesinti sürelerini sağlamak oldukça güçtür.²

3.1.7 Dokümantasyon: 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 dağıtımını da yapılmalıdır.³

3.1.8 Periyodik tatbikatlar: Herhangi bir zamanda acil durumlara hazırlanmak için senaryolar hazırlanmalı ve delinmelidir. Alıştırmalar sonucunda oluşturulan kontrol sisteminin eksikliklerini tespit edebilirsiniz. Böylece, iş sürekliliği planının ve diğer ilgili belgelerin eksikliklerini, araştırma alanına dahil olan personelin bilgi seviyesini ve varsa teknolojik altyapıyı belirlemek mümkündür. Tatbikatlar belgelerin görüntülenmesi, bir planın bölümlerinin test edilmesi veya tüm planın test edilmesi gibi farklı türlerdir. Yıllık her egzersiz türü için egzersiz planları ve egzersizlerin hazırlanması, kurumun olası bir acil durum senaryosuna hazırlanmasını sağlar..⁴

3.1.9 Eğitim ve bilinçlendirme: İş sürekliliği çalışmalarını Kabul etmek için, kurum çalışanlarına ve iş sürekliliğini düzenlemede ekiplere yönelik eğitim yapılmalıdır. Kurum genelinde Kabul görmeyen ve gerekli eğitim faaliyetlerine

² BS 259992 2006

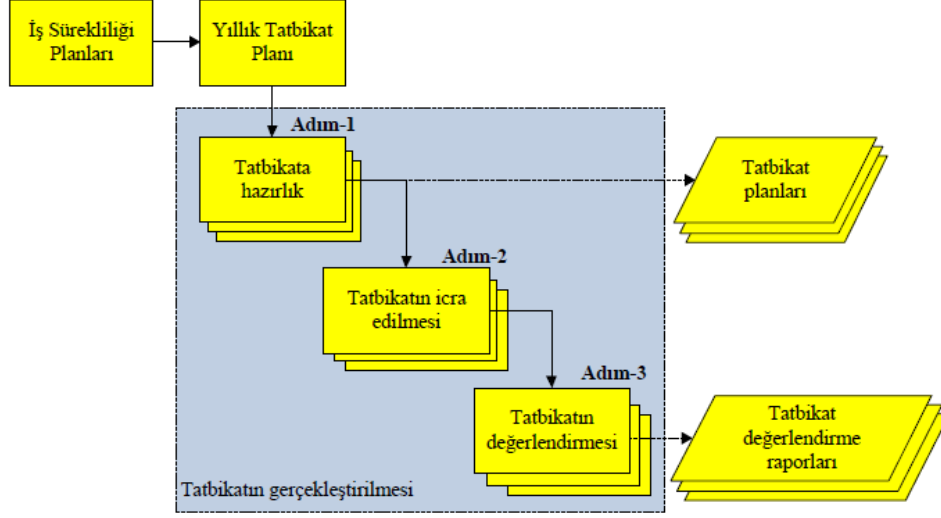
³ BS 259992 2006

⁴ BS 259991 2006

sahip olmayan iş sürekliliği planlarının başarılı olması muhtemel değildir. İş sürekliliğini sağlama planında öğretim yöntemleri tanımlanmalı ve plana dahil edilmelidir (anketler, sınıf eğitimi, sınav vb.). Eğitim faaliyetlerini yürütmek ve gerekirse eğitim faaliyetlerini düzenlemek için bir ekip oluşturmak yararlı olacaktır. İş sürekliliği bilgisi yılda en az bir kez olmalıdır..⁵

3.1.10 Plan bakım ve güncelleme: ISYS, kuruluşun kritik süreçlerinin sürekliliğini sağlamak için vardır. Bu nedenle, kuruluşun süreçlerindeki değişiklikler iş sürekliliği planını doğrudan etkiler. Süreç değişikliklerinin planın güncellenmesini gerektirdiği olgusunu asla kaybetmemelisiniz. Zaman içinde meydana gelen değişiklikleri bir iş sürekliliği planına aktarmak için güncelleme gereksinimlerini periyodik olarak gözden geçirmeli ve belirlemelisiniz. Egzersiz sonuçları genellikle planın güncellenmesini gerektirir. İş sürekliliğinin bir parçası olarak yapılması gereken değişiklikler mutlaka belgesel değişiklikler değildir. Kuruluşun süreçlerinin kritiklik seviyesindeki değişiklikler nedeniyle, servis sağlayıcıların öncelikleri ve alınan önlemler değişebilir. Bu nedenle, bazı durumlarda yeni yatırım gereksinimleri ortaya çıkabilir. Değişiklik bir sistem değişikliği ise, bütçe ve zaman çizelgesi hazırlanmalıdır..⁶

3.2 Tatbikat Süreci



Şekil 3.2

Afet ve acil durumlarda iş sürekliliği planlarının istenilen biçimde çalışabilmesi için, hazırlıkların düzenli olarak tatbikatının yapılması ve ortaya çıkan eksiklikler doğrultusunda planların güncellenmesi gereklidir İş sürekliliği tatbikatlarının amaçları aşağıda sıralanmıştır;

- Telekom Şirketinin iş sürekliliği konusundaki yeteneklerini değerlendirmek.
- Planda bulunması gerektiği halde bulunmayan bilgileri tespit etmek
- Planın geliştirilmesi gereken yönlerini tespit etmek
- Kurtarma takımlarının çalışma performansını gözlemek ve iyileştirmek
- İş sürekliliği bilincini arttırmak

İş sürekliliği çalışmalarının tamamını bir defada test etmek pratikte oldukça zordur. Bu sebeple çalışmaların her yönü ile kontrolü için düzenli aralıklarla ve planların farklı yönlerini test eden bir tatbikat programı hazırlanmalı.

İlerleyen bölümlerde tatbikatların planlama, gerçekleştirme ve değerlendirme faaliyetleri tanıtılmıştır. Tatbikatlar haberli veya habersiz

yapılabilir. Bir senaryo eşliğinde planlı olarak gerçekleştirilir. Bununla birlikte öncelikli bir faaliyetin veya servisin bir kısmının dar bir kapsamda çalışıp çalışamayacağını anlamak için senaryosu olmayan planlı testler yapılabilir. Ancak yılda en az bir defa yapılan testler, tatbikat ile pekiştirilmelidir. Adımın amacı iş sürekliliği planının etkinliğini ölçmek ve kurumun gerçek felaket durumları için hazırlıklı olmasını sağlamaktır. Yapılan çalışmaların kabul edilebilir kesinti zamanlarını karşılaması beklenmektedir.

İş sürekliliği planının tatbikatı bir prosedür hazırlanmalıdır. Bu prosedür yapılacak testler için genel çerçeveyi çizmeli ve tatbikatlar için gerekli minimum ihtiyaçları belirlemelidir.

Prosedürde aşağıdaki bilgilerin bulunması tavsiye edilmektedir:

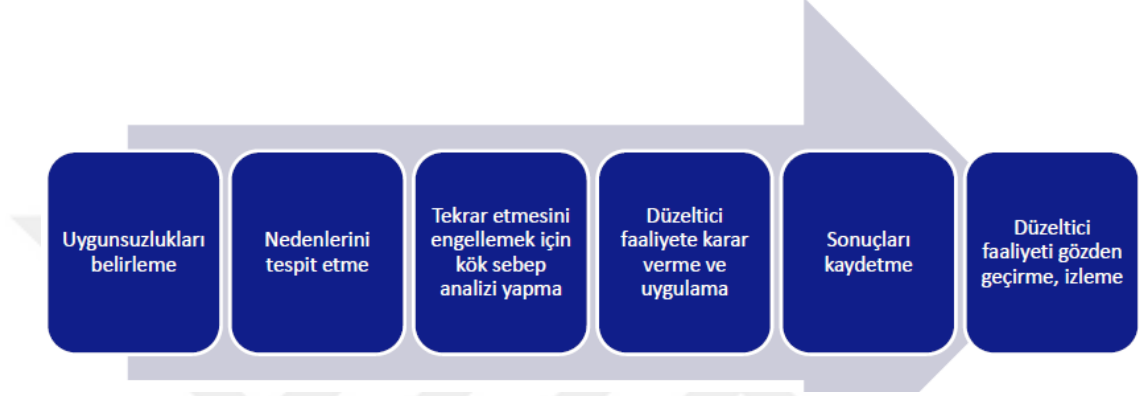
- Tatbikatlar hangi aralıklarla yapılacak
- Tatbikat faaliyetlerinin koordinasyonu nasıl gerçekleştirilecek
- Tatbikat sırasında hangi yöntem kullanılacak
- Tatbikat planı nasıl hazırlanacak
- Tatbikat planında nelere dikkat edilecek
- Tatbikat sonuçları nasıl değerlendirilecek (Rapor, Bağımsız gözlemci)
- Tatbikat kayıtları nasıl tutulacak
- Tatbikat sonucunda tespit edilen eksiklikler nasıl kapatılacak.

Her bir tatbikat için aşağıdaki işlemlerin gerçekleştirilmesi tavsiye edilmektedir:

- Tatbikat planının oluşturulması.
- Tatbikat planının onaylatılması.
- Tatbikat öncesi eğitimlerin düzenlenmesi.
- Tatbikatın gerçekleştirilmesi.
- Tatbikat sonrası değerlendirme ve eksik yanların raporlanması

3.3. Düzeltici Faliyet

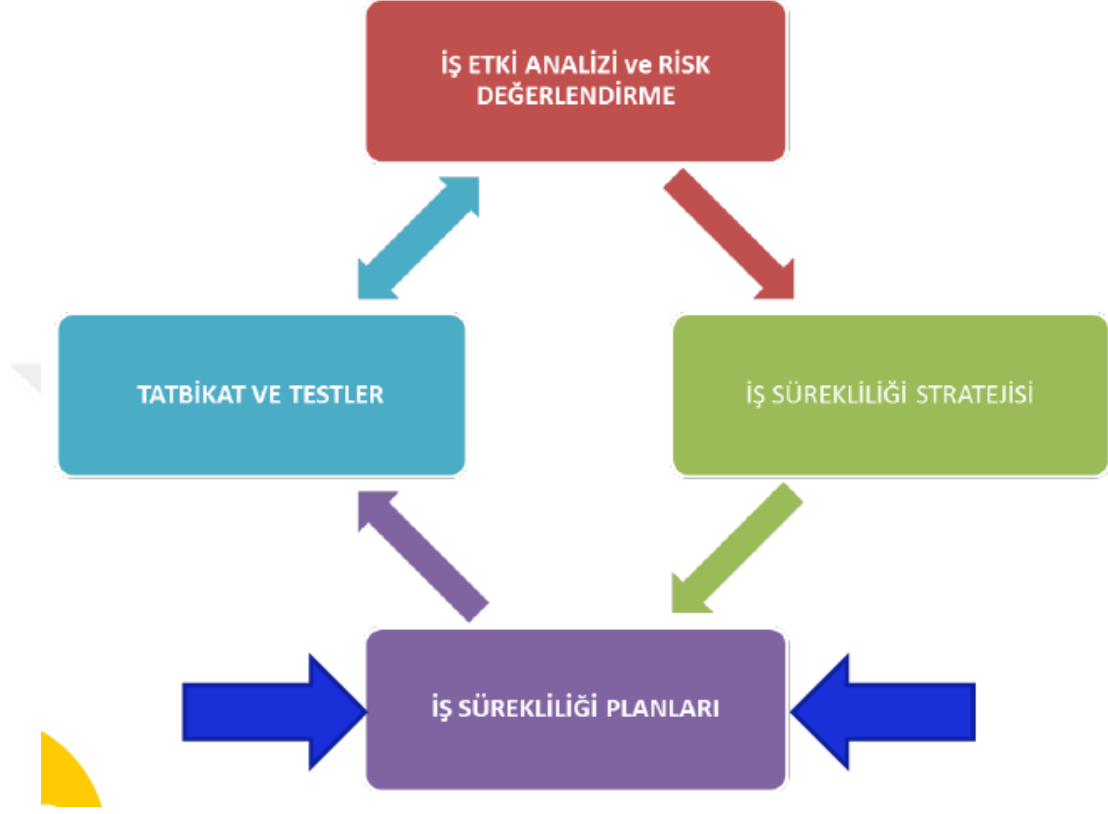
- **Amaç:** Uygunsuzlukların nedenlerini ortadan kaldırmak ve tekrar etmelerini engellemek.



Şekil 3.3

İş Sürekliliği Yönetim Sistemi ile ilgili uygunsuzlukların bildirilmesi ve kök sebep analizinin gerçekleştirilmesi, düzeltici faaliyetlerin planlanması, takibi ve kapatılması Uygunsuzluk ve Düzeltici Faaliyetler Prosedürüne göre gerçekleştirilir. QDMS sistemine sahip olmayan grup şirketinde kendi düzeltici faaliyetler altyapısı kullanılabilir. İş sürekliliği yönetim sistemi iş sürekliliği hedeflerinin belirlenmesi ve ölçümü, iç denetimler, yönetimin gözden geçirmeleri, tatbikatlar, farkındalık eğitimleri ve düzeltici faaliyetler ile sürekli olarak iyileştirilir

3.4 İş Sürekliliği Planları



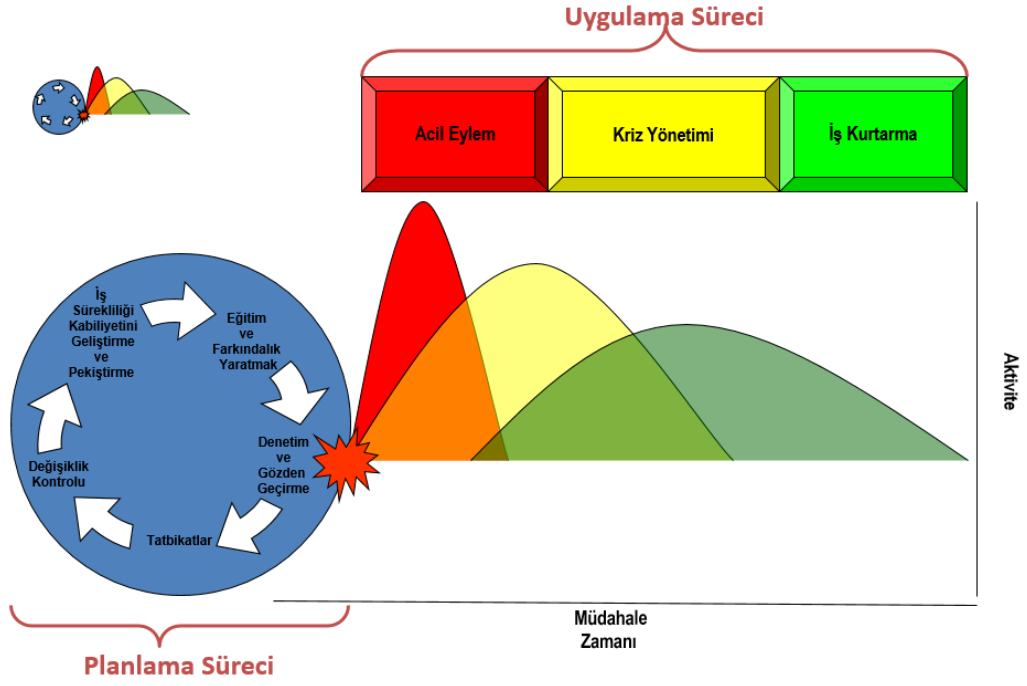
Şekil 3.4

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.

3.5 Uygulama Süreci

Program yönetimi sorumlulukların atanması, İş Sürekliliği Yönetim Sistemi'nin kurulması ve iş sürekliliği ile ilgili süregelen faaliyetlerin

yapılması olmak üzere üç parçadan oluşmaktadır. BS 25999 yaşam döngüsü Şekil 3.2'de görünmektedir

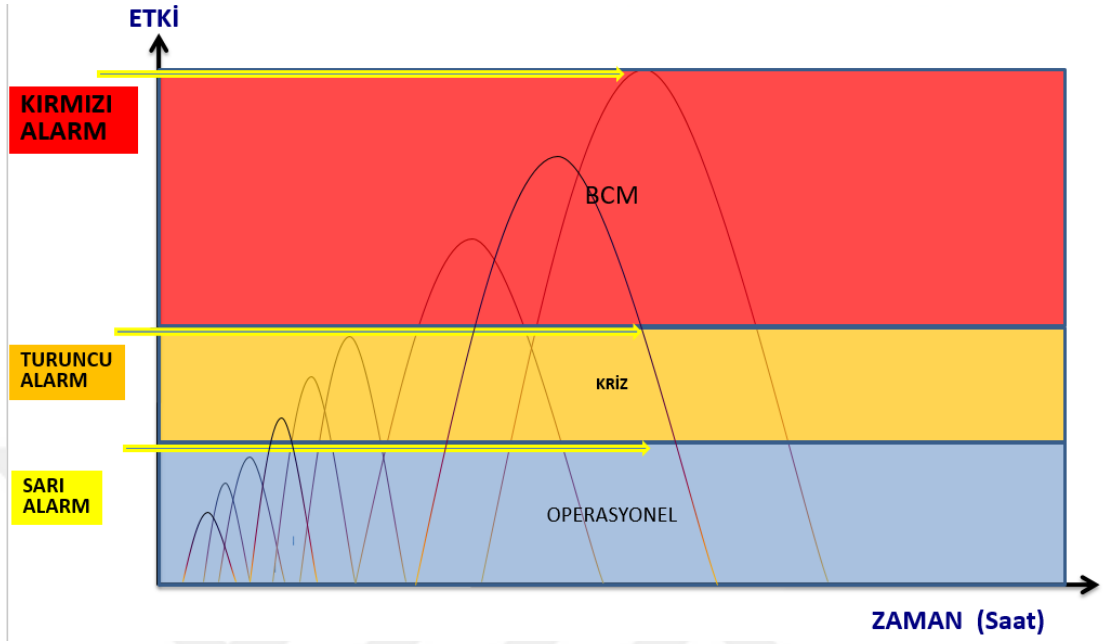


Şekil 3.5

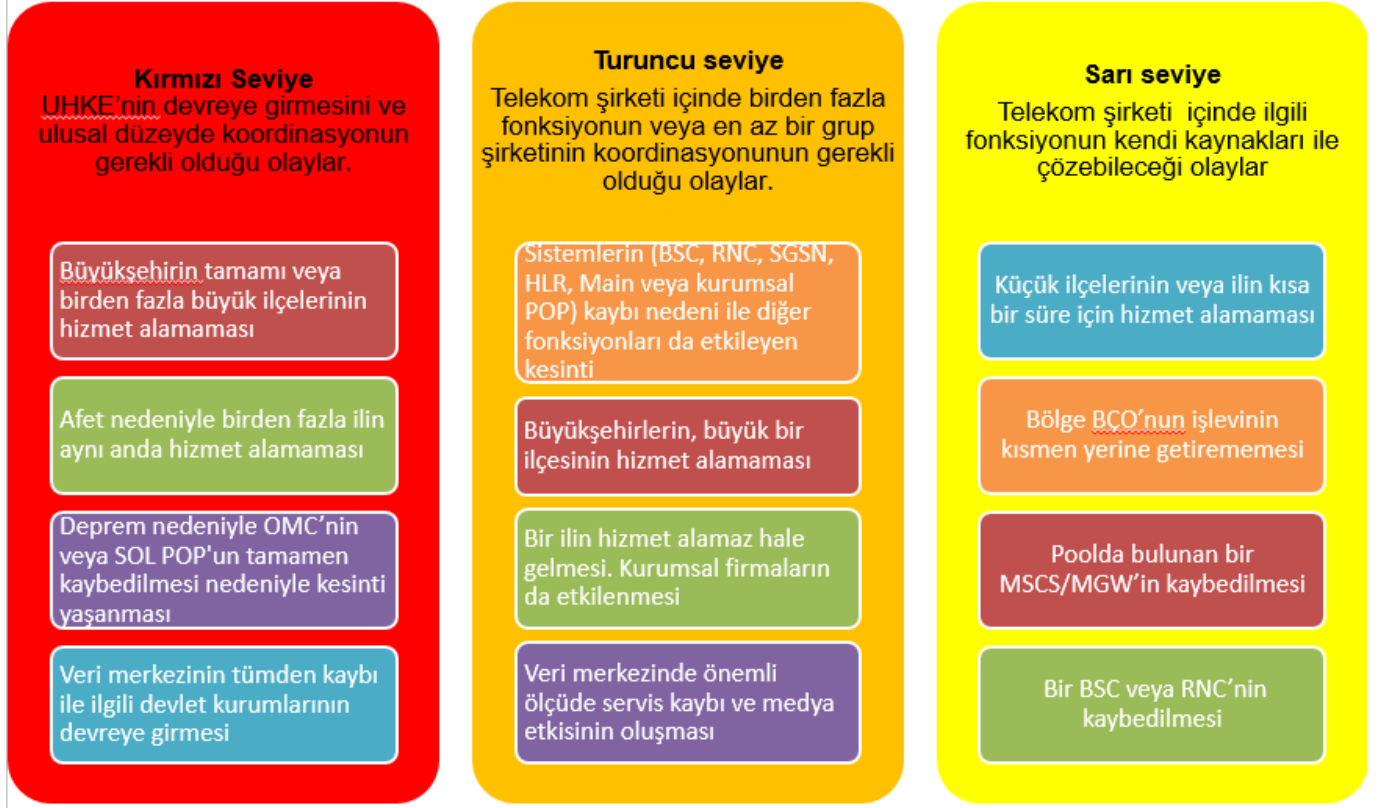
3.6 Kriz Seviyeleri

- Kırmızı: Ulusal düzeyde koordinasyonun gerekli olduğu olaylar
- Turuncu: Telekom operatöründe birden fazla fonksiyonun veya en az bir grup şirketinin koordinasyonunun gerekli olduğu olaylar
- Sarı: İlgili fonksiyonun kendi kaynakları ile çözebileceği olaylar
- İlgili iş sürekliliği planının aktivasyon kriterleri:
- Kırmızı, Turuncu ve Sarı seviyedeki olaylar aktivasyon kriterlerine yazılmalıdır.

Bazı faaliyetler hiçbir zaman Turuncu ve Kırmızı seviyede olamayabilir o zaman sadece Sarı seviyenin yazılması yeterlidir



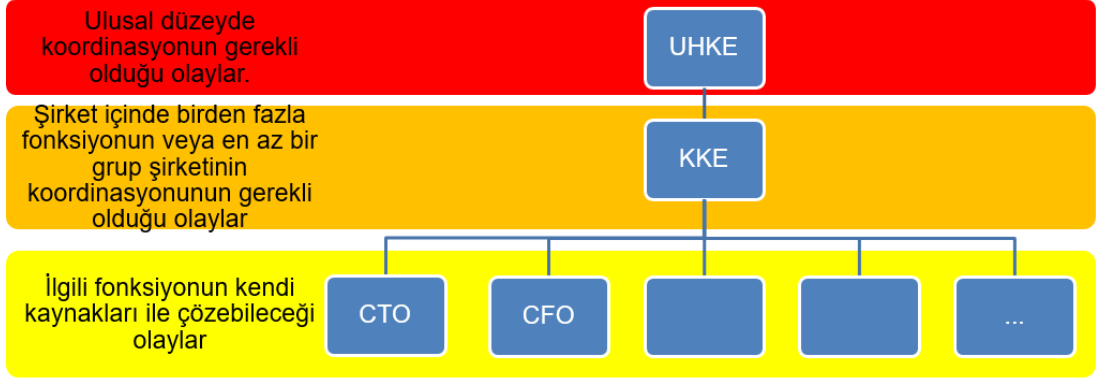
Şekil 3.6.1



Şekil 3.6.2

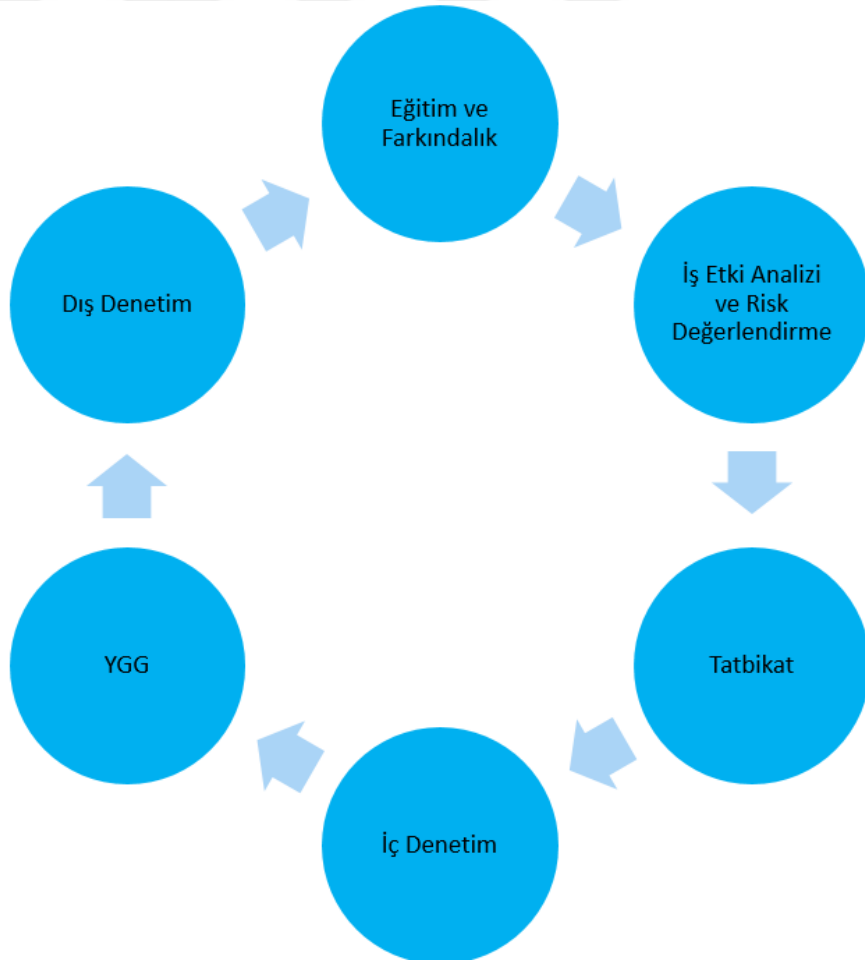
3.7 İş Sürekliliği Organizasyonu;

ISO 22301 standardı ile artık kurumlar sadece kendi kurumuyla değil, İş sürekliliği yönetim sistemi kapsamındaki organizasyon içinde yönetim sistemini etkileyecek kişi ya da gruplar ("interested parties" clause) maddesi ile yanındaki binanın güvenlik sistemi, risk değerlendirmesi, ilgili tüm süreçleri hakkında bilgi sahibi olması gerekmektedir. İş Sürekliliği yönetim sistemini kuran organizasyon hizmet aldığı tüm tedarikçileri İş Sürekliliği kapsamında anahtar ürün ve servisleri gerçekleştiren üst seviye aktivitelere göre derecelendirmeli ona göre de durum tespiti (Due Diligence) yapması gereklidir



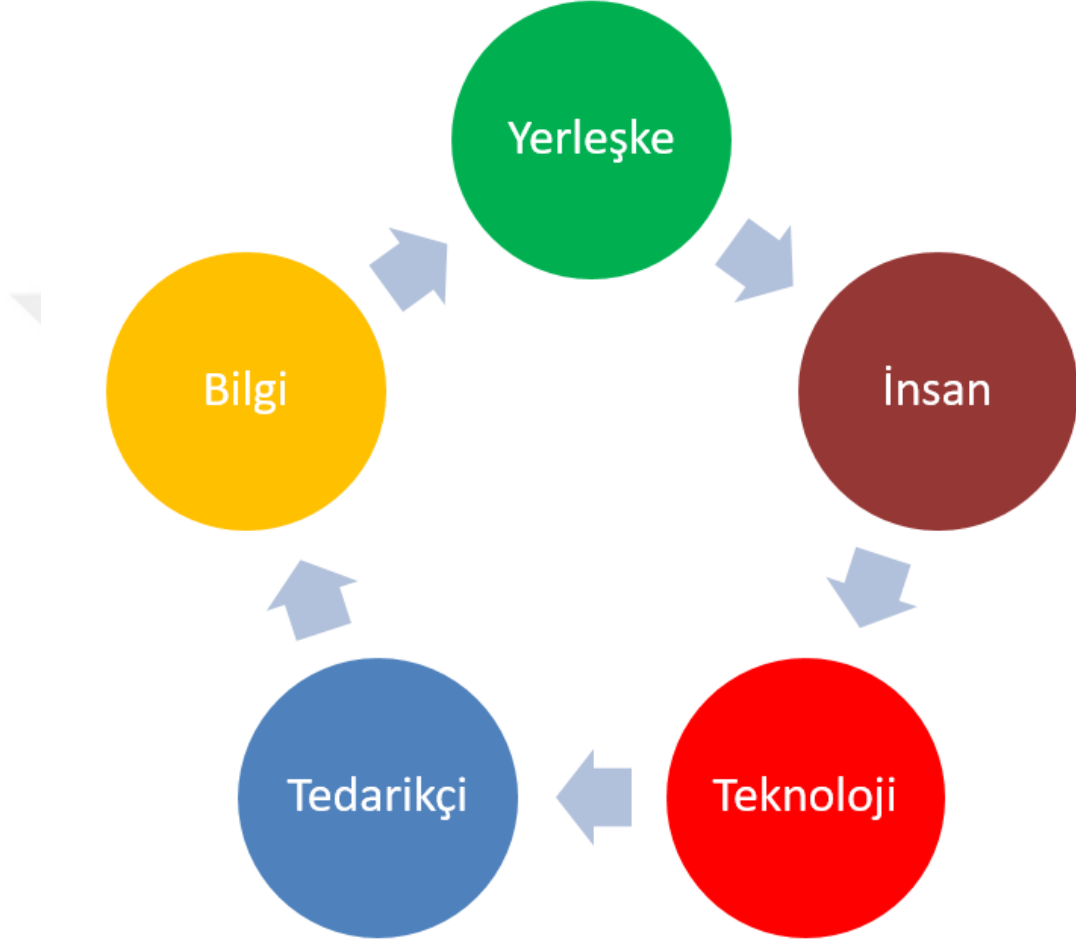
Şekil 3.7

3.8 İş Sürekliliği Yönetim Döngüsü



Şekil 3.8

3.9 İş Sürekliliği Stratejileri



Şekil 3.9

3.10 İş Sürekliliği Sorumlulukları

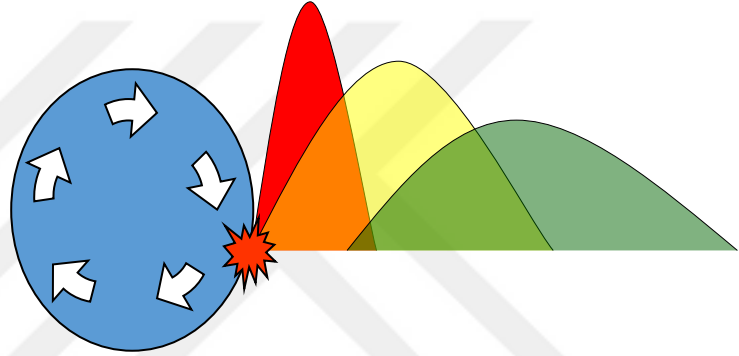
İş Sürekliliği Yönetiminin sorumluluğu bu amaçla oluşturulan Grup BCM biriminde olmakla birlikte, *yürütme* sorumluluğu tüm **şirket çalışanlarını** içerir.

İş Sürekliliği Yönetimi:

- Acil Eylem, Kriz Yönetimi ve İş Sürekliliği Yönetimi Planları'nın oluşturulmasını
- Bu planları işletecek grupların tanımlanıp oluşturulmasını
- İlgili gruplara eğitim verilerek gerekli bilgiye ve eylem planlarına hakim olmalarının sağlanmasını içerir.

Olay Sonrası

- **Acil Eylem**
- **Kriz Yönetimi**
- **İş Kurtarma**



Şekil 3.10

4. BULGULAR

4.1 Acil eylem

Şirketin normal operasyonuna devamını engelleyen olayları takip eden ilk dakika ve saatlerde çalışanların, fiziksel ortamın ve altyapının güvenliğine yönelik alınacak acil tedbirleri içermektedir.

Acil Eylem Takımı olaya operasyonel düzeydeki ilk müdahaleyi yapmakla görevlidir.

Acil Eylem aşağıdaki aksiyonları içerir:

- Tahliye
- Acil servislerin çağırılması
- Lokasyonun kapatılması
- Güvenliğinin sağlanması
- Hasar tespiti

Acil Eylem Planı'nın hayata Geçirilmesine Sebep Olan Olaylar;

- Bomba ihbarı
- Telefonun ve enerjinin kesilmesi
- Fırtına, tayfun ve sel
- Deprem, yangın
- Binanın işgal edilmesi
- Halk hareketi ve işyeri şiddeti
- Kaçırılma ve terörist saldırılar
- Siber saldırı

4.2 Kriz yönetimi

Şirket'in ana faaliyetlerinin kesintiye uğraması krizdir. *Şirketin normal operasyonuna devamını engelleyen olayların gerçekleşmesi durumunda Telekom operatörünün servis ve gelirleri üzerinde ciddi negatif etkilerin oluşma risklerinin gerçeğe dönüşmesi; ve/veya şirket dışından yardım/ kaynak ve destek gerekmesi durumlarına kriz adı verilmektedir.*

Kriz durumunda, acil eylemlerin ardından ya da eş zamanlı olarak Kriz Yönetimi Planı hayata geçirilir. Kriz kararını Kriz Yönetim Takımı üyeleri alır (en az 2 üyenin bağlantıya geçerek ortak kararı gerekir) ve bu süreci yönetir. Kriz Yönetimi, taktik ve stratejik bir seviyede yapılır.

Kriz Yönetimi Takımı tüm kararları alır ve Telekom operatörünün dışarıyla olan her türlü iletişimini tek noktadan sağlar (Kurumsal iletişim ve Genel müdürlük 1. derecede sorumludur).

4.2.1 Kriz Yönetimi Planı'nın Hayata Geçirilmesine Sebep Olan Olaylara Örnekler:

- Durumun acil eylem uygulamaları ile çözülemiyor olması
- Kritik fonksiyonlar üzerinde ciddi bir etki yaratmış olaylar sonrasında nakit akışı, gelirler, imaj ve müşteri memnuniyetinin etkilenmesi
- Telekom operatörünün hassas ve gizli bilgilerin medyaya yansması
- Ana lokasyonlardaki plazalara 12 saatten fazla girilemiyor olması
- Temel ürün ve hizmetlerden abone miktarının %10'inden fazlasının 4 saatten fazla yararlanamıyor olması
- IT sistemleri veya teknik sistemlerin 4-6 saatten fazla hizmet dışı kalması
- Önemli yaralanma veya ölümler
- Diğer negatif medya yansımaları/haberleri

4.2.2 Acil Durum ve Kriz Durumunda Aksiyona Gececek Gruplar Kriz Yönetim Takımı içerisinde Genel Müdür yardımcıları ve İş Kolu Koordinatorleri'nin Rol ve Sorumlulukları

Ana Sorumluluk: İş Sürekliliği Yönetimi stratejilerini onaylar; kurumsal krizlerde ve gerektiğinde genel ve bölgesel krizlerde, kriz yönetimine dair stratejik kararları alarak ilgili grupların işleyişine yön verir.

Kapsam: İş Sürekliliği Yönetimi Süreci'nde stratejilerin geliştirilmesi ve Kurumsal Kriz Yönetimi

Sorumluluklar: Kriz Yönetimi Kılavuzu doğrultusunda;

- Şirketin için kurumsal boyutta oluşturulan İş Sürekliliği Yönetimi strateji ve hedeflerini onaylar.
- Şirket operasyonları, mali durumu, yönetim yapısı gibi ana konularda, şirket dışında yetkililere, müşterilere, hissedarlara yapılacak açıklamalara onay verir; gerektiğinde Kurumsal İletişim Bölümü ile koordineli olarak açıklamaları yapar.

Sunulan raporlar ışığında şirketin krizden etkilendiği alanları değerlendirir, iş kurtarma aksiyonlarını takip eder; şirketin kriz öncesindeki durumuna geri dönebilmesi için stratejik seviyede kararları alır ve uygulanmasını sağlar

4.3 Kriz Yönetim Takımı (KYT) Çalışma Prensipleri;

- En az 2 Kriz Yönetim Takımı Üyesi'nin varlığında Kriz Yönetim Planı uygulamaya geçirilebilir. Tüm üyelerin bir araya gelmesi şart değildir.
- Kriz Yönetim Planı'nı uygulamaya geçirme kararının alınmasıyla eş zamanlı olarak üyelerden 1'i Kriz Yönetim Takımı Lideri ilan edilir.

- KYT Lideri, planın uygulamaya geçirilmesinde koordinasyonu sağlayıcı ve yönlendirici kişi olarak kabul edilir.
- Kriz kurumsal boyutta ise ya da kurumsal boyuta geçiyorsa, CEO ya da CEO'yu temsilen CXO'lardan biri KYT Liderliği'ni üstlenir.
- Kriz Yönetimi Takımı üyeleri aynı zamanda yöneticisi olduğu fonksiyonel grubun İş Kurtarma Takımı Lideri'dir.

4.5.1.1 İş kurtarma

Acil eylemlerde ve kriz yönetimi boyunca, şirketin kısıtlı da olsa işleyişinin devam edebilmesi amacıyla normalin dışında operasyonlar yürütülebilir. Ancak mümkün olduğunca kısa sürede operasyonların normale dönebilmesi için kriz süresince ve/veya krizin ardından fonksiyonel gruplar iş kurtarma çalışmalarına başlarlar.

Acil eylemin ardından operasyonların normale dönmesi amacıyla belirli kişiler muhakkak operasyonların başında yer alırlar. Bu kişiler doğal operasyonel sorumlulukları sebebiyle İş Kurtarma Takımı Üyesi olarak adlandırılırlar.

İş kurtarma çalışmalarının genel içeriği:

- Başlıca ekipmanların/sistemlerin onarılması, işlerlik kazandırılması
- Binaların normal operasyonların gerçekleştirilebilmesi için organize edilmesi
- Kritik dokümanların, çizimlerin yenilenmesi/organize edilmesi
- Operasyonel kadronun kurulması

4.5.1.2 Acil Durum ve Kriz Durumunda Aksiyona Gececek Gruplar İş Kurtarma Takım Üyesi

Ana Sorumluluk: Acil eylem gerektiren olayın, bir krizin ardından operasyonların normal akışına dönmesini sağlamak amacıyla bölgeler bazında operasyonel müdahaleleri gerçekleştirmek.

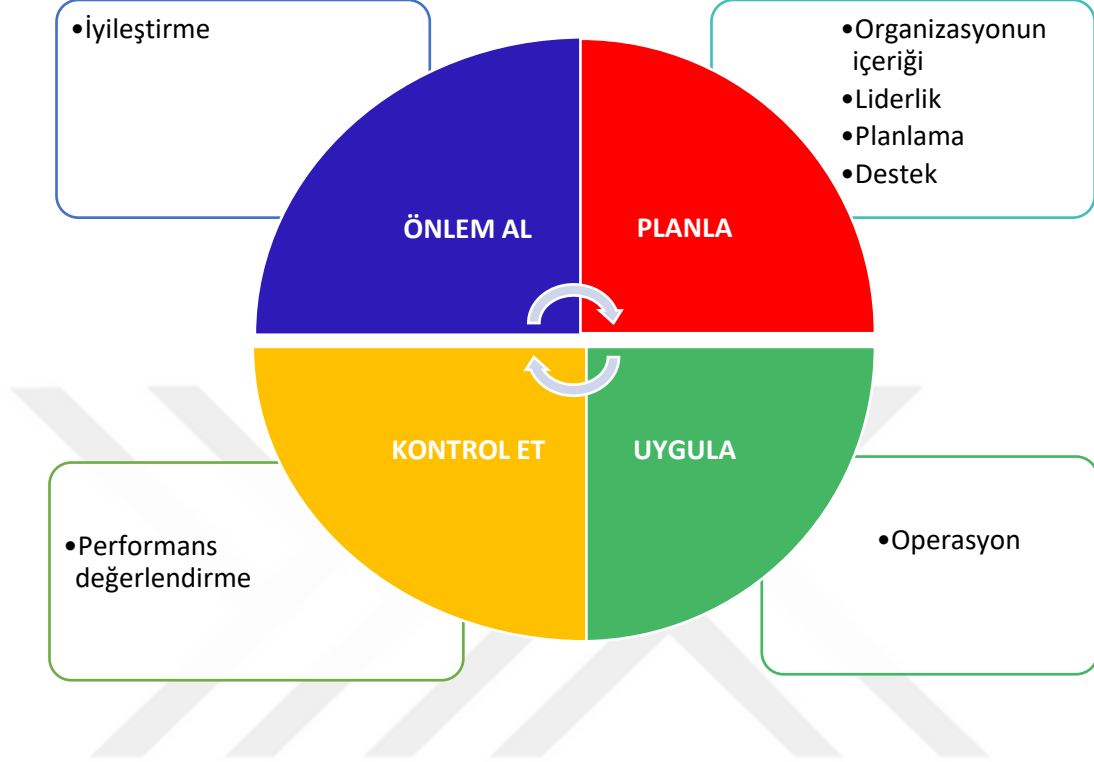
Kapsam: İş Kurtarma Planı'nın bölgesel bazlı olarak hayata geçirilmesi

Sorumluluklar: kriz süresince ve/veya krizin ardından,

- sorumluluğu dahilindeki altyapı/ sistemlerin onarımını yapar/ işlerlik kazanmasını sağlar.
- kritik dokümanları, çizimleri yeniler/organize eder.
- varsa sorumluluğu dahilindeki binaların normal işlerliğini kazanmasını sağlar.
- operasyonların sürekliliğini sağlamak amacıyla kadroyu kurar/eksik kadroyu tamamlar.
- tanımlı kritik sürelerde operasyonların normale dönmemesi durumunda yöneticisini/Kriz Yönetim Takımı'nı bilgilendirir.
- Etkileşimde bulunduğu diğer operasyonel grupları ve dış kaynak desteği veren şirketleri bilgilendirir.

Not: İş Kurtarma Takımı Üyeleri acil eylem gerektiren olayın ardından iş sürekliliğini sağlayabilmek amacıyla görev bölgelerinde hazır bulunurlar

4.5.1.2 PUKÖ Döngüsü



4.5.2 Paydaşlar ve regülatif kurumlar

- Sabit Kule ve baz istasyonları kurulumu(Hastane, Toplanma Merkezi...)
- AFAD koordinasyonunda il Afet planlarının yapılması(ISTAMP...).
- Karayolları ağırlık kontrollerinden muafiyet
- AFAD koordinasyonunda ortak tatbikatlar
- Roaming özellikli mobil istasyonlar



Şekil 5.2

İş sürekliliği organizasyonu iş sürekliliğini etkileyen bu 3 temel kavram ve onlarla ilgili süreçlerle de son derece yakından ilgilidir. Kurum içinde iş sürekliliği organizasyon modeli kurulurken bunların da kapsanacak şekilde ele alınması gereklidir.

4.5.3 Acil Durum Yönetimi: Can kaybı, yaralanma, yapısal veya yapısal olmayan fiziksel hasarlar, çevresel zararlar ile kişi ya da kurumların faaliyetlerini kısıtlayan her türlü beklenmedik olay ve tehlike “Acil Durum”; bunun komuta, kontrol ve koordinasyonunu sağlama düşüncesinden hareketle; can, mal ve çevre güvenliğini sağlamaya yönelik bir eğitim ve davranış sistemini de “Acil Durum Yönetim Sistemi” olarak tanımlayabiliriz.

İş Sürekliliği Yönetimi, standart tanımının dışında, kuruluşun olaylara karşılık verme ve bunun planlamasını gerçekleştirme konusunda

stratejik ve taktik becerisi ve iş kesintileri için önceden tanımlanmış kabul edilebilir seviyede iş uygulamalarına devam etme becerisi olarak tanımlanır.

4.5.4 Kriz Yönetimi: Kurumların normal iş operasyonlarının dışında gerçekleşen ve onların markasını, itibarını, güvenliğini tehdit eden, anlık karar verilerek çözülmesi gerekli olaylar bütünü olarak tanımlayabiliriz.

4.5.5 İş Sürekliliği Yönetimi: Acil durumdan, kısaca insandan başlayarak, kurumun en kritik iş süreçlerine kadar bu sürecin her aşamasında bulunmaktadır. En net tanımıyla iş sürekliliği, kurumların varlığını devam ettirebilmesi için gereken süreçlerin bütünüdür.

Doğal olarak İş Sürekliliği yönetimi bu sürecin tümünde var olmak zorundadır. Bu noktada önemli bir kavramın daha açıklanması gereklidir. O da "Afet" kavramıdır.

4.5.6 Afet: Acil durumlara müdahale için yaratılmış mevcut kaynakların yetersiz kaldığı ve kapasitelerinin aşıldığı durum veya olaylardır. İş Sürekliliği tüm bu yönetim süreçleri ile iç içedir. Bunun gelişmesinde en çok ortaya çıkan noktalardan birisi de doğal afetlerdir.

4.6. Kapsam

Telekom operatörü bünyesinde yürütülen tüm iş sürekliliği faaliyetlerini ve kritik kayıplara neden olabilecek Şirket tedarikçilerini kapsamaktadır. Kesintisi, anahtar ürün ve hizmetlerimizi anında etkileyen faaliyetler, iş sürekliliği planlaması ve tatbikat kapsamındadır. Bu prosedürün hazırlanması, güncel tutulması, grup içerisinde yaygınlaştırılması ve uygulandığının kontrolü Şirket İç Denetim müdürlüğü bulunan Grup İş Sürekliliği Yönetimi biriminin sorumluluğundadır. Bu prosedür, Telekom operatörünün İş Sürekliliği Yönetimi politikası ile uyumlu olup kapsam dahilindeki yerlerde, nasıl uygulanacağını açıklamaktadır.

ISO 22301 standardının Telekom operatörü içerisinde nasıl uygulanacağı standardın madde numaraları ile uyumlu şekilde aşağıda sunulmuştur.

4.7. Organizasyonun içeriği

4.7.1 Organizasyonu ve İçeriğini Anlamak

ISO 22301 standardının ihtiyaç duyduğu organizasyonun içeriği ile ilgili bilgilere inside üzerinden erişilebilir. Inside üzerinde bulunan bilgilere ek olarak web sayfası, tedarikçi listeleri, iş etki analizi ve risk yönetimi dokümanlarında organizasyonun içeriği ile ilgili bilgiler bulunmaktadır.

Telekom operatörü iş sürekliliği politikası şirket hedefleri doğrultusunda oluşturulmuş ve tüm ilgili taraflara duyurulmuştur. Politika aynı zamanda kurumsal web sayfasında bulunmalıdır.

Şirket'in kabul edilebilir risk seviyesi Kurumsal Risk Yönetimi Prosedürü'nde tanımlanmalıdır Orta, düşük ve çok düşük önem derecesine sahip olanlar kabul edilebilir risk seviyesi olarak belirlenmiştir.

İş Sürekliliği Yönetim Sisteminin kurulmasında iç ve dış konuların dikkate alınması, İş Sürekliliği hedeflerinin buna göre belirlenmesi, risklerin ve belirsizliklerin bu gereklilikler dikkate alınarak analiz edilmesi, çerçevenin ve kapsamın belirlenmesi açısından kritiktir. Belirsizlik ve risk arttıran faktörler oluştuğunda etkin bir iç iletişim için, iç ve dış konular üst yönetim kademeleri ile ayrıca paylaşılır.

Telekom operatörü ve grup şirketleri dış konular; uyulması gereken yasal, mevzuat ve sözleşme gereklilikleri, uyulması gereken ulusal ve uluslararası standartlar, kurumsal müşterilere karşı olan sorumluluklar, iş ortakları ve tedarikçilere karşı olan sorumluluklar, halka karşı olan sosyal sorumluluklar, düzenleyici kurumlar, yerel yönetim ve hizmet sağlayıcılara, komşu firmalara karşı olan sorumluluklar, çevresel sorumluluklar, yurt dışı işler nedeni ile faaliyet gösterilen ülkedeki benzer sorumluluklar, hissedarlara karşı olan sorumluluklar olarak sıralanabilir. Ayrıca, yerel veya global ekonomik, politik, siyasi gelişmeler, jeopolitik konum, iklimsel olaylar, jeolojik olaylar, dünyada veya yurtda yaşanan sanal ya da fiziksel güvenlik olayları, bu olaylardaki trend, İş Sürekliliği Yönetim Sisteminin kurulmasında, işletilmesinde ve iyileştirilmesinde mutlaka dikkate alınmalıdır.

İç konular ise, şirketin politikaları, hedefleri, bu hedefler ışığında gerçekleştirilecek aksiyonlar, faaliyetler, projeler, şirketin çalışanlarına karşı sorumluluğu, etik gereksinimler, şirket kültürü, süreçler, şirketin yapısı, organizasyonu, roller ve sorumluluklar, farklı şehirlerdeki/ülkelerdeki kültürel gereksinimler, lokasyonların fiziksel yapısından kaynaklanan gerekliliklerdir. Ayrıca, şirketin sahip olduğu kaynaklar (sermaye, varlıklar, insan kaynağı, yetkinlikler, bilgi birikimi, sistemler, süreçler ve teknolojiler) bilgi sistemleri, bilgi akışları, karar alma mekanizmaları, uygulanan standartlar, modeller, kılavuzlar, prosedürler, talimatlar, kayıtlar İş Sürekliliği Yönetim Sisteminin yönetilmesinde, risklerin belirlenmesinde dikkate alınması gereken diğer iç konulardır.

4.7.2 İlgili Tarafların İhtiyaç ve Beklentilerini Anlamak

ISO 22301:2012 standardının Madde 4'ü gereğince Operatörün iş sürekliliği yönetim sistemi ile ilgili tüm tarafların iş sürekliliği gereksinimleri analiz edilmelidir.

İş sürekliliğini etkileyen tüm iç ve dış taraflar analiz edilir. İç ve dış tarafların Şirketten beklentileri ve Şirketin iş sürekliliği kapsamında ilgili taraflardan beklentileri analiz dokümanında bulunur. İlgili taraf analizinin yapılmasından Şirket İş Sürekliliği Program yönetimi ve iş sürekliliği koordinatörleri sorumludur.

İlgili taraf analizlerine ek olarak uymakla yükümlü olunan yasalar düzenlemeler belirlenmelidir. Tabi olunan yasal yükümlülükler bir tablo halinde tutulur. Bu tablo Şirketin İş Sürekliliği Yönetimi ve Hukuk ve Regülasyon ekibleri ile birlikte hazırlanır ve güncel tutulur.

Operatör ve Grup Şirketlerinin ana faaliyet alanını etkileyen düzenlemelerin ve yasaların takip edilmesi ve değişikliklerin Şirket ve grup içerisinde duyurulması, bunların olası yansımalarının analiz edilmesi ve bu kapsamda etkilenebilecek şirketlere ve ilgili birimlere bilgilendirme yapılması, olası risklerin bildirilmesi, gerekli aksiyonların alınmasının sağlanması, Regülasyon bölümü tarafından gerçekleştirilir.

Yasal ve Regülatif düzenlemeler ilgili kurum tarafından resmi yazı ile iletilebilir veya değişen Kanun ve düzenlemeler Hukuk ve Regülasyon Stratejileri bölümü tarafından takip edilerek varsa uyulması gereken konular belirlenir. Uyumun gerçekleşeceği termin genellikle resmi Kurumlar tarafından net bir şekilde belirtilir. Resmi yazı Hukuk ve Regülasyon bölümüne ulaşır ulaşmaz ilgili departmanlar ile gerekirse açılış toplantısı yapılarak yükümlülüklerin net bir şekilde anlaşılması sağlanır, riskler belirtilir ve bir proje

planı çizilir. Sorumlu kişiler ve termin belirlenir. Ardından uyum ekibi yükümlülüklerin zamanında ve tam bir şekilde sağlandığını açılan projeler ile takip eder ve sonuçlandırır. Uyum projeleri ile ilgili düzenli bilgilendirmeler üst yönetime yapılarak gerektiğinde destekleri alınır.

Tabi olunan yasal ve regülatif yükümlülüklerle uyum senelik olarak Hukuk ve Regülasyon bölümü tarafından kontrol edilir. Grup şirketlerinde bu işlemi ilgili hukuk ve regülasyon birimi veya görev verilen birim yerine getirir.

4.7.3 İş Sürekliliği Yönetim Sisteminin Kapsamına Karar Verme

İş sürekliliği yönetim sistemi kapsamının belirlenmesi sırasında tabi olunan yasal ve regülatif yükümlülükler ile ilgili tarafların beklentileri dikkate alınır.

Kapsam dahilinde bulunan ürün ve hizmetler, faaliyetler, yerleşkeler dokümante edilir. Kapsamdan hariç bırakmalar ve hariç bırakmanın gerekçeleri de yazılır.

4.8 Liderlik

4.8.1 Liderlik ve Taahhüt

Operatör bünyesinde uygulanan İş sürekliliği Yönetim Sistemi Yönetim desteği ile gerçekleştirilmektedir. Şirket İç Denetim bölümü sorumludur.

Şirket Yönetimi iş sürekliliğinin yaklaşımını "İş Sürekliliği Politikası" dokümanında açıkça ifade etmektedir. Çalışanların motivasyonun artırılması ve iş sürekliliği yönetiminin kurum kültürü haline gelmesi için gerekli çalışmaları desteklemektedir.

4.8.2 Yönetimin Taahhüdü

Şirket yönetimi, İSYS'nin oluşturulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için aşağıdaki ilkeleri kabul ve taahhüt etmektedir;

- İş sürekliliği politikası, kuruluşun (stratejik) iş planları ile uyumlu olacak şekilde oluşturulur. İş planlarında iş sürekliliği hedefleri ile uyumluluk sağlanır.
- İSYS'nin kuruluşun diğer süreçleri ile bir bütünlük içinde çalışması sağlanır.
- İş sürekliliği politikası ve hedefleri, tüm çalışanlara ve ilgili taraflara duyurulur.
- İhtiyaç duyulan kaynaklar sağlanır.
- İSYS hedefleri ve sistemin etkinliği, sürekli iyileştirme sağlayabilmek amacıyla, her yıl gözden geçirilir.

4.8.3 Politika

Şirket yönetiminin iş sürekliliği yaklaşımı dokümente edilmiş ve İş Sürekliliği Politika dokümanı olarak yayınlanmıştır. Bu politika ile Şirket Yönetimi İSYS'nin uygulanması ve sürekli iyileştirmesi ile ilgili desteğini açıkça ifade etmektedir.

Telekom operatörünün İş Sürekliliği Politikası, tüm kurum çalışanlarına iç haberleşme kanalları kullanılarak, ilgili dış taraflara kurumsal web sayfası aracılığı ile duyurulur.

İş Sürekliliği Organizasyonu ve Sorumlulukları

İş Sürekliliği Yönetim Sisteminin (İSYS) oluşturulması ve genel koordinasyonu politika dokümanı ile İş Sürekliliği Yönetimi (İSY) Koordinatörüne verilmiştir. İş sürekliliği ile ilgili Grup şirketlerinde

gerçekleştirilen faaliyetler bu politika ve ilgili Grup dokümanları dikkate alınarak, İSY Koordinatörü ile irtibat halinde gerçekleştirilir.

4.8.4.1 İSY Koordinatörünün sorumlulukları:

- Afet ve acil durum öncesinde kurum bilgi birikimini ve hazırlıklı olma kapasitesini artırır.
- Afet ve acil durum anı ve sonrasındaki sorumluluklar ilgili operasyonel takımlardadır.
- İş sürekliliği yönetim sistemi çerçevesinde ihtiyaç duyulan eğitimlerin koordinasyonunu sağlar.
- İSYS şablonlarını oluşturur ve dokümanların yayınlanmasında onay zincirine dahil olur.
- Tatbikatları planlar, tatbikat sonucunun üst yönetime raporlanmasını sağlar.
- İSYS' nin bütçe ve zaman planlarını, İSYS ile ilgili satın almaları onaylar, süreci takip eder, geri bildirimlerde bulunur.
- İş Sürekliliği Planlarının (İSP) oluşturulmasını, alternatif konumlarda, iş süreçleriyle, iç-dış-grup kaynaklarıyla ve/veya tedarikçilerle tatbikatının yapılmasını sağlar.
- Mevcut İS ile ilgili hizmeti sağlayan tedarikçi firmaların sözleşme koşullarının uygunluğu ve performansı değerlendirir, gerekli görülürse alternatif firma arayışına gider.

- Uluslararası kurumlarla, sivil toplum kuruluşlarıyla, kamu kurumlarıyla, kurumsal firmalar ve üçüncü parti kişilerle; İş sürekliliği, afet, acil durum konularında iletişimi ve koordinasyonu sağlar.

4.8.4.2 UHKE (Ulusal Haberleşme Koordinasyon Ekibi)

Ulusal düzeyde koordinasyonun gerekli olduğu durumlarda çalışan ve üst seviye yönetimden oluşan ekiptir. KYE' nin sağladığı bilgiler ışığında ulusal düzeyde karar ve koordinasyon işlerini gerçekleştirir. UHKE üyeleri ve iletişim bilgileri Şirket İş Sürekliliği Planında verilmektedir.

4.8.4.3 KYE (Kriz Yönetim Ekibi)

Afette, acil durumda ve normalleştirmede: Faaliyetleri ve kriz yönetimini koordine eder. Kriz durumları ve ekip bilgileri Kriz Yönetim Planında yer almaktadır.

4.8.4.3 Medya ve İletişim Takımı

Medya ve iletişim takımı halkın bilgilendirilmesi gerektiği durumlarda görev alan takımdır. Bu takım basın bülteninin hazırlanmasından ve periyodik olarak halkın bilgilendirilmesinden sorumludur. Bu takım acil durumlarda Kurumsal İtibar Kriz Yönetimi Prosedürü'ne uygun olarak kamuyu bilgilendirmekten sorumludur.

4.8.4.4 Fonksiyon/Bölüm İş Koordinatörünün sorumlulukları:

- Afet ve acil durum anı ve sonrasında: Bulunduğu fonksiyonun/organizasyonun içerisindeki ve KYE/UHKE ile olan koordinasyonu sağlamak.

- Bulunduđu fonksiyonda, organizasyonda veya Grup Őirketinde, yerleŐik İS k¼lt¼r¼n¼ oluŐturmak ve farkındalıđı arttırmak.
- G¼rev ve organizasyon deđiŐikliklerinde; Őirket İSY Koordinat¼r¼n¼ ve ilgili kiŐileri bilgilendirmek.
- İŐ s¼rekliliđi risk analizini yapmak, raporlamak ve g¼ncel tutmak.
- Kurum Őablonuna uygun olarak İEA'ları, İSP'leri hazırlamak ve g¼ncel tutmak.
- Test ve tatbikatları planlamak, gerŐekleŐtirilmesini sađlamak ve raporlamak.

4.8.4.5 İS Takım ¼yesinin sorumlulukları:

- Afet ve acil durum sonrasında iŐletilecek İSP'leri, sorumlu kiŐilerce tetiklemeyle, gerŐekleŐtirmek.
- G¼rev deđiŐikliklerinde ilgili İS Koordinat¼r¼n¼ bilgilendirmek, deđiŐiklikleri İS dok¼manlarına yansıtmak.
- İSP'leri oluŐturulmasına ve g¼ncellemesine katkıda bulunmak ve g¼ncel tutmak.
- Őirket İSYS kapsamında verilen g¼revleri (İEA, İSP, risk, tatbikat vb.) yapmak.

4.8.4.6 T¼m ŐalıŐanların sorumlulukları:

- Afet ve acil durumlarda sorumluların y¼nlendirmelerine uymak.

- Afet ve acil durumlarda ne yapılacağını öğrenmek için eğitimlere katılmak, gerektiğinde tatbikatlara katılmak.
- Bulunduğu yerleşkenin toplanma noktasını, hangi durumda nereye haber verilmesi gerektiğini bilmek.
- Şirket İSYS çalışmalarına yardımcı olmak.

4.8.4.7 ISO 27001 ve ISO 22301 bağı ve karşılıklı sorumluluklar

Telekom operatörü bünyesinde işletilen ISO 27001 Bilgi Güvenliği Yönetim Sistemleri ile ISO 22301 İş Sürekliliği yönetim Sistemi arasında yakın bir bağ bulunmaktadır. ISO 27001 kapsamında erişebilirliği sağlanan kaynakların bir kısmı Telekom Operatörü veya Operatör Grup şirketlerinin anahtar ürün ve hizmetlerini desteklemektedir. Bilgi güvenliği kaynaklı olaylardan ilgili grup şirketinin anahtar ürün ve hizmetlerde kesintiye neden olaylar için gerekli müdahale ve süreklilik planları bilgi güvenliği yönetim sistemi kapsamında hazırlanır. Bu planların hazırlanması aşamasında Telekom operatörü İş Sürekliliği Yönetimi bölümünden de görüş alınır. İş sürekliliği tatbikat senaryolarında bilgi güvenliği kaynaklı kesinti senaryoları da düşünülür ve bu senaryolarda ISO 27001'den sorumlu ekiplerde tatbikatlara katılır. Anahtar ürün ve hizmetlerde kesintiye neden olan bilgi güvenliği olaylarında bilgilendirme zincirinde Şirket İş Sürekliliği Yönetimi bölümü de bulunur.

4.9 Planlama

4.9.1 Risk ve fırsatları belirleme aksiyonları

Telekom Operatörü iş sürekliliği ile ilgili riskleri ve fırsatları belirlemek üzere iç ve dış çevre bağımlılıklarını, ilgili tarafların ihtiyaç ve beklentilerini göz önünde bulundurur. Bu çalışma ile aşağıda sıralanan faydalar hedeflenir;

- İSYS'nin beklenen sonuçlara ulaşmasını sağlamak,
- Beklenmeyen etkileri önlemek ve azaltmak,
- Sürekli iyileştirme sağlamak.

Bu çalışmalar kapsamında periyodik risk değerlendirmeleri yapılarak, saha ziyaretleri, müşteri ziyaretleri ve düzenleyici kurum ziyaretleri yapılabilmektedir. Analiz, değerlendirme ve ziyaretler sırasında ortaya çıkan fırsatlar için aksiyonlar planlanır ve hayata geçirilir.

4.9.2 İş sürekliliği hedefleri ve gerçekleştirmek için planlar

Şirket İş Sürekliliği hedefleri İş Sürekliliği Yönetimi Politikası'nda verilen üst seviye hedefler dikkate alınarak belirlenir ve senelik olarak gözden geçirilir. İş sürekliliği hedefleri ölçülebilir nitelikte belirlenir ve uygun seviye yönetim kademelerine iletilir. Hedeflerin ölçümünden Şirketin İş Sürekliliği Yönetimi Bölümü sorumludur. Hedef ölçüm sonuçları YGG toplantılarında sunulur.

4.10 Destek

4.10.1 Kaynaklar

İSYS' nin oluşturması, uygulanması, bakımı ve sürekli iyileştirmesi için gereken merkezi kaynaklar, Grup İş Sürekliliği Yönetimi koordinatörü tarafından üst yönetime sunulur. Üst yönetimin onayı ile bütçe, yatırım ve iş planlarına dönüşür.

Bölümlerin yönetim sistemini işletmesi sırasında risk değerlendirme, tatbikat vb. çalışmalar içerisinde tespit edilmiş ihtiyaçları ilgili bölüm yöneticileri tarafından bütçelendirilir ve en geç bir sonraki yıl içerisinde

çözömlenir. Bu çalıřmaları gerçekteřtirirken risk yönetimi esaslı bir yaklařım uygulanır.

4.10.2 Yetkinlikler

İř süreklilięi organizasyonunda yer alan çalıřanların yetkinlikleri ařaęıda belirtilmiřtir. Yařanılan olaylar, tatbikatlar ve iç denetimler yetkinlik deęerlendirmesinde araç olarak kullanılır. İř süreklilięi kapsamında ihtiyaç duyulan eęitimler řirketin Akademi ile řirketin BCM ekibi tarafından koordine edilir. ISO 22301 İř Süreklilięi Yönetim Sisteminin yaygınlařması için ISO 22301 farkındalık eęitimi, ISO 22301 İç denetçi eęitimi düzenlenir.

4.10.2.1 Temel yetkinlikler

- Soęukkanlı
- Bulunduęu birimin iç iřleyiřine hakim
- Hızlı durum analizi yapabilen ve inisiyatif kullanabilen
- Bulunduęu takımın gerektirdięi teknik yetkinliklere ve bilgilere sahip
- ISO 22301 Toplumsal Güvenlik – İř Süreklilięi Yönetim Sistemi standardı hakkında bilgi sahibi

4.10.2.2 Koordinatör Yetkinlikleri

Koordinatörler temel yetkinliklere ilave olarak ařaęıdaki yetkinliklere sahip olmalıdır.

- Bulunduęu fonksiyonun içi iřleyiře hakim
- Durumsal farkındalık yetkinlięine sahip
- ISO 22301 Toplumsal Güvenlik – İř Süreklilięi Yönetim Sistemi standardının gereksinimlerine hakim
- Hem fonksiyon içi hem de řirketin İř Süreklilięi Koordinatörü ile takip, koordinasyon ve güçlü iletiřim kurabilecek özelliklerde.

- Operatörün anahtar ürün ve hizmetleri olan Konuşma, Mesajlaşma, İnternet ve Toplumsal Güvenlik hizmetlerinden birinde operasyonel görev almış olması.

4.10.3 Farkındalık

İş sürekliliği yönetim sistemi kapsamında çalışan kişilerde ve üçüncü taraflarda gerekli farkındalığın sağlanması için çalıştaylar düzenlenebilir. Bu çalıştaylarda iş sürekliliği politikası, kendilerinin İSYS'ye katkıları, bir İSYS gereksiniminin karşılanmamasının etkileri ve kesinti durumunda nasıl hareket edileceği aktarılır. Çalıştaylarda ek olarak temel İSYS dokümantasyon yapısı ve acil durum hareket tarzları aktarılır. Farkındalık çalışmalarına katkı sağlamak amacı ile LCD'ler üzerinde bilgi çevrimi, broşürler ve afişler kullanılabilir. Farkındalık çalışmalarının koordinasyonunu Şirketin iş sürekliliği yönetimi gerçekleştirir.

4.10.4 İletişim

Telekom Operatörü, İSYS ile ilgili iç ve dış iletişim ihtiyaçlarını karşılamak için gerekli (kaynak planlaması, iletişim araçları, iletişim tarafları vs.) talimat ve sistemlerini tanımlamış ve uygulamaya almıştır. Erken uyarı sistemleri ve kurum içi hızlı bilgilendirme araçları hali hazırda kullanımdadır.

İş sürekliliği yönetim sistemi kapsamında ihtiyaç duyulan iletişim bilgileri iş sürekliliği planlarında bulunmaktadır. Acil durumlarda kullanılmak üzere ilgili yönetim kademelerine uydu telefonları tahsis edilmiştir.

4.10.5 Doküman ve Kayıt Yönetimi

İş sürekliliği yönetim sistemi kapsamında üretilen politika, prosedür, form, plan ve talimatlar Doküman Yönetimi Prosedürü ve Kalite Kayıtları Prosedürü'ne uygun olarak gerçekleştirilir. İç denetim planı, eğitim

planı, tatbikat planlama ve değerlendirme gibi kayıtlar Şirketin İş Sürekliliği Bölümünce kayıt olarak saklanır.

Grup şirketleri doküman ve kayıt yönetimi için ayrı prosedürler uygulayabilir. Doküman yönetimi için QDMS mevcut değil ise farklı bir platform kullanılabilir.

4.11 Operasyon

4.11.1 Operasyonel planlama ve kontrol

ISO 22301:2012 Madde 6 Uyarınca yapılan planlamalar Madde 8 kapsamında uygulamaya alınır. Şirket, Madde 6 da ki planlama süreçlerini gerçekleştirmek için kriterler belirleyerek, bu kriterlere göre sürecin kontrollü olarak yürütülmesini sağlar. İş sürekliliği yönetim sistemi çerçevesindeki süreçlerin işletiminin planlı şekilde yürütüldüğünden emin olmak için gerekli yazılı bilgiyi tutar, süreçlerdeki değişiklikleri kontrol eder ve değişiklik sonuçlarını gözden geçirir.

4.11.2 İş Etki analizi ve Risk Değerlendirmesi

4.11.2.1 Genel

Şirket grup, anahtar ürün ve hizmetlerini belirlemek ve bu ürün ve hizmetleri destekleyen faaliyetlerin önem derecelerini tespit etmek üzere sistematik bir iş etki analizi yaklaşımı uygular. Uygulanan iş etki analizi yöntemi madde 8.2.2'de verilmiştir.

Zamanda öncelikli (kritik) faaliyetlerinde kesintiye neden olabilecek riskler için kurumsal risk yönetimi ile entegre şekilde risk yönetimi çalışmalarını sürdürür.

4.11.2.2 İş Etki Analizi

Bu bölüm, iş sürekliliği yönetim sistemi çerçevesinde ISO 22301 standardına uygun İEA' nın nasıl gerçekleştirileceğini açıklamak amacı ile hazırlanmıştır.

İEA yönteminin uygulanmasından ISO 22301 İş Sürekliliği Yönetim Sistemi kapsamında bulunan tüm fonksiyonlar sorumludur.

İEA çalışması, anahtar ürün ve hizmetlerin abonelere ve paydaşlara sunulmasını sağlayan iş süreçleri, servis ve faaliyetleri ve bu süreç, servis ve faaliyetlerin kesintisi halinde yaşanacak etkinin zamana dağılımını belirlemek için gerçekleştirilir.

A1	Ani Etki	Faaliyet kesintiye uğradığı AN , desteklenen anahtar ürün ve hizmetin TÜMÜ veya ÖNEMLİ bölümü kaybedilir, yada büyük ölçekli (MBCO'nun altına düşülen) kapasite, kalite, iş kaybı nedeni ile geniş etki oluşur
A2	Ani Etki	Faaliyet kesintiye uğradığı AN , desteklenen anahtar ürün ve hizmetin BİR KISMI kaybedilir.
D1	Dolaylı Etki	Faaliyet kesintiye uğradığı AN , desteklenen anahtar ürün ve hizmet ANINDA KESİNTİYE UĞRAMAZ , fakat İLERLEYEN SAATLERDE kesintiye uğrayabilir yada kapasite, kalite iş kaybı yaşanmaya başlanabilir. Veya ilgili faaliyet yerine getirilemediği için İLERLEYEN SAATLERDE itibar, yasal ve regülatif etkiler oluşmaya başlar.
D2	Dolaylı Etki	Faaliyet kesintiye uğradığı AN , desteklenen anahtar ürün ve hizmet ANINDA KESİNTİYE UĞRAMAZ , fakat İLERLEYEN GÜN(LER) ve HAFTA(LAR) kapasite, kalite, iş kaybı yaşanmaya başlanabilir.
Z	Zayıf Etki	Faaliyet kesintiye uğradığı AN , desteklenen anahtar ürün ve hizmet ANINDA KESİNTİYE UĞRAMAZ , fakat İLERLEYEN AY(LAR) ve YIL(LAR) kapasite, kalite, iş kaybı yaşanmaya başlanabilir.
i	İlişkisiz	Faaliyetin eksikliği ilgili anahtar ürün veya hizmeti ETKİLEMEZ

Şekil 11.2.2

11.2.3 İş Etki analizi (IEA) – Kritik Bağımlılık ve Önceliklerin belirlenmesi (RPO)

Servis Sürekliliğinin sağlanması kapsamında t anında yaşanan kesinti sonrası data kaybı oluşmuş ve datanın restore edilmesi gerekiyorsa Data Kaybı önemi seçilir. Veri tabanı ya da veri tipi bazında RPO değeri set edilir.

SERVICE/ACTIVITY PRESENTATION FORM	
DATE	
SERVICE/ACTIVITY NAME	MANAGER NAME
UNIT	
NUMBER OF EMPLOYEES	
CRITICAL PERSONNEL	
MANUAL TO THE WORKS	
Özell. bilg., tecrübe, deneyim	
Süreçler	
Süreç Gözden	
Süreç Çıktıları	
Yasal Şartlar	ETK
min Sü./Target	KAYNAK İHTİYAÇLARI
Sözleşme Taahhüdü	İLGİLİ DÖKÜMAN(LAR)
Working Hours	YEDERLEŞİLECEKLERİ OPERASYONLAR/birim
YÖBÜN DÖNEMLERİ	Bu birim/yederleştirecek OPERASYONLAR/birimler
Dependencies	Müşterileri
İç	Dış

Ardından aşağıdaki formda yer alan alanlar etki derecesi kullanılarak doldurulur. Kritik anahtar ürün ve servis etkisi var ise işaretlenir. Üst yönetimin önceliklendirdiği servis/faaliyet için yönü biliniyor ise "1" olarak işaretlenir bilinmiyor ya da yok ise "0" verilir.

Servis/faaliyetin zaman aralıklarında kesinti yaşanması durumundaki etkisi finansal, müşteri ilişkileri, reputasyon ve regülasyon açısından 1-5 arasındaki etkiye göre değerlendirilir. Örneğin; P2P SMS servisinin 1-5 saat arasında kesilmesinin finansal etkisi, Etki derecesi skalasında yer alan puana göre yazılır.

Aktivite/ Faaliyet	Zaman Aralığı	Kaynaklar	Ağırlık Yüzdeleri %					ÜST YÖNETİM GÖRÜŞÜ	Anahtar Ürüne Etkisi?	Ağırlıklı Ortalama Puanı (100 üzerinden) * Bu kısım otomatik hesaplanıyor..	KRİTİKLİK?	RTO	MAO
			30	15	15	10	30						
			FINANSAL ETKİ	MÜŞTERİ ETKİSİ	İMAJ	YETENEK/KABİLİYET	YASAL	1-0					
X Faaliyeti	1-5 saat	Y Kaynağı	1	3	4	2	2	1	0	43	1	1 saat	
	5-12 saat		2	3	4	3	2			51		5 saat	
	12-24 saat		2	4	5	4	2			59			
	1-2 gün		2	4	5	5	2			61			
	2-7 gün		2	4	5	5	2			61			
	1-2 hafta		2	4	5	5	2			61			
	2-4 hafta		2	4	5	5	3			67			
> 1 ay	2	4	5	5	4	73							

Ağırlıklı Ortalama Puanı (100 üzerinden)	$(FEX30+MEX15+İEX15+KEX10+YEX30)/5$
KRİTİKLİK?	Ağ.Ort.Puanı>=60 ise veya, Ağ.Ort.Puanı>=50 ise ve ÜYG veya AÜE 1 ise Kritik (1)
RTO	(Faaliyet Kritik ise yukarıdan aşağı satırda ilk "3" değerinin bulunduğu zaman aralığının minimum değeri)
MAO	(Faaliyet Kritik ise yukarıdan aşağı satırda ilk "4" değerinin bulunduğu zaman aralığının minimum değeri)

Tablo 11.2.3

İş Etki Analizinin değerlendirilmesinde kullanılan hesaplama metodu:

İş etki analizi değerlendirilirken, "Ağırlıklı Ortalama Puan" Sistemi kullanılmaktadır. Bunun için "Finans Müşteri-İmaj-Yetenek/Kabiliyet-Yasal" etkileri toplanan yüz olacak şekilde Ağırlıklandırma; Finans Etkisi için %30, Müşteri Etkisi için %15, İmaj Etkisi için %15, Yetenek/Kabiliyet Etkisi için %10, Yasal Etkisi için %30 olarak alınmıştır.

Her bir zaman aralığı için, verilen puanlarbu ağırlıklandırmadaki değerler kullanılarak toplam bir puan elde edilir.

Yukarıdaki tablodaki örnek olarak verilen "X faaliyeti" için 1-5 saat aralığında Ağırlıklı ortalama puanı; $(FEX30+MEx15+İEX15+KEX10+YEX30)/5$ formülü ile $(1x30+3x15+4x15+2x10+2x30)/5= 215/5= 43$ bulunur.

Bir faaliyetin-kaynağın Kritikliğinin

Herhangi bir zaman aralığında en az bir defa ağırlıklı ortalama puan 60 veya üzerinde çıkması durumunda ilgili kaynak ve faaliyet "Kritik" olarak kabul edilir.

İlgili faaliyet için "Ust Yönetim görüşü" veya "Anahtar Ürün Etkisi'nin "1" verilmesi durumunda, kritiklik eşik değeri 50'ye iner.

Kritik çıkan ilgili faaliyet için "RTO değeri", zaman aralığına göre değerlendirilme tablosunda yukarıdan aşağı satırda ilk "3" değerinin bulunduğu zaman aralığının minimum değeri olarak kabul edilir.

Kritik çıkan ilgili faaliyet için "MAO değeri" ise, zaman aralığına göre değerlendirilme tablosunda yukarıdan aşağı satırda ilk "4" değerinin bulunduğu zaman aralığının minimum değeri olarak kabul edilir.

"3" ve "4" değerinin yukarıdan aşağı satırda ilk olarak aynı anda bulunması durumunda ilgili zaman aralığının minimum değeri RTO, maksimum değeri MAO olarak kabul edilir.

Services/Activity	Kritik anahtar ürün ve servislerden hangisi/hangilerine etkisi var ise işaretlenmeli					RESOURCES	IMPORTANCE OF FINANCIAL	IMPORTANCE OF CUSTOMER RELATIO	REPUTATION	REGULATION	TOP MANAGEMENT	MBCO	RPO
	VOICE	DATA	SMS	INTERNET	SOCIAL SECURITY								
	X										1-0		
1-5 hours													
5-12 hours													
12-24 hours													
1-2 dates													
2-7 dates													
1-2 weeks													
2-4 weeks													
> 1 months													

Tablo 11.2.3.2

Katsayı	Kayıp (ticari)	Müşteri etkisi	Kanuni riskler	Müşteri ve itibar etkisi	Kriz süresi
5 Çok Yüksek	> 100 Milyon \$ finansal etki	%20+ Dış Müşterinin etkilenmesi Dış Müşteri memnuniyetinin kritik düzeyde etkilenmesi %10'dan fazla müşteri kaybı etkisi İç Müşterinin büyük çoğunluğunun veya tamamının etkilenmesi İç Müşteri memnuniyetinin kritik düzeyde etkilenmesi	Lisans kaybı, lisansın askıya alınması ve çok büyük maddi ceza ile sonuçlanabilecek riskler İmtiyaz ve hakların kaybedilmesi	Yurtiçi/dışı basında geniş haber etkisi ile ciddi marka imajı itibar kaybı Yeni Ürün memnuniyetinin kritik düzeyde etkilenmesi Geri kazanımı çok düşük itibar kaybı	>24 saat iş/servis aksaması Kabiliyet ve Kaynak olgunluğunun kritik %10 düzeyde etkilenmesi
4 Yüksek	10-100 Milyon \$ arasında finansal etki	Dış Müşteri portföyünün %20'sinin etkilenmesi Dış Müşteri memnuniyetinin önemli oranda etkilenmesi %5-%10 arası müşteri kaybı etkisi Bir veya birden fazla İç Müşteri Başkanlığının etkilenmesi İç Müşteri memnuniyetinin önemli oranda etkilenmesi	Kayda değer maddi ceza ile sonuçlanabilecek ve uzlaşma sağlanması çok zor sonuçlar doğuran riskler İmtiyaz ve hakların süreli askıya alınması	Geri kazanımı güçlü itibar kaybı Yeni Ürün memnuniyetinin önemli oranda etkilenmesi	12-24 saat arası iş/servis aksaması Kabiliyet ve Kaynak olgunluğunun önemli oranda/%5-%10 etkilenmesi
3 Orta	5-10 Milyon \$ arasında finansal etki	Dış Müşteri portföyünün %10'unun etkilenmesi Dış Müşteri memnuniyetinin kısmi olarak etkilenmesi %3-%5 arası müşteri kaybı etkisi Bir veya birden fazla İç Müşteri Dairesinin (Departmanının) etkilenmesi İç Müşteri memnuniyetinin kısmi olarak etkilenmesi	Makul maddi cezalar ile sonuçlanabilecek veya mahkemede çözülebilecek sonuçlar doğuran riskler	Geri kazanılabilir marka imajı/itibar kaybı Yeni Ürün memnuniyetinin kısmi olarak etkilenmesi	6-12 saat arası iş/servis aksaması Kabiliyet ve Kaynak olgunluğunun kısmi olarak/%2-%5 etkilenmesi
2 Düşük	1-5 Milyon \$ arasında finansal etki	Sadece bir Dış Müşterinin etkilenmesi Dış Müşteri memnuniyetinin kabul edilebilir düzeyde etkilenmesi %1-%3 arası müşteri kaybı etkisi Bir veya birden fazla İç Müşteri Bölümünün etkilenmesi İç Müşteri memnuniyetinin kabul edilebilir düzeyde etkilenmesi	Uyarı getirebilen ve maddi cezaya yol açmayan riskler İmtiyaz ve hak kaybı ile ilgili uyarı/kınama/ mahkeme de hallolacak problemler	Kolay geri kazanılabilir itibar kaybı Yeni Ürün memnuniyetinin kabul edilebilir düzeyde etkilenmesi	2-6 saat arası iş/servis aksaması Kabiliyet ve Kaynak olgunluğunun kabul edilebilir düzeyde/%0-%2 etkilenmesi
1 Çok düşük	< 1 Milyon \$ finansal etki	Dış Müşteri memnuniyetinin hemen hemen hiç veya çok az etkilenmesi Dış Müşteri memnuniyetinin hemen hemen hiç veya çok az etkilenmesi Bir veya birden fazla İç Müşteri Takımının etkilenmesi İç Müşteri memnuniyetinin hemen hemen hiç veya çok az etkilenmesi	Herhangi maddi kanuni/ cezai bir problem yaratmaması İmtiyaz ve hak kaybı ile ilgili herhangi kanuni/ cezai bir problem yaratmaması	Gözardı edilebilir marka imajının itibar kaybı Yeni Ürün memnuniyetinin hemen hemen hiç etkilenmemesi	<2 saat iş/servis aksaması Kabiliyet ve Kaynak olgunluğunun hemen hemen hiç etkilenmemesi

Anahtar ürün ve hizmetleri destekleyen faaliyetlerin hedeflenen kurtarma süresi (RTO) ve maksimum kabul edilebilir (MAO) kesinti süresi bağlantılı olduğu ürün ve hizmetlere bağımlı olarak belirlenmektedir.

4.11.2.2.4 İş Etki Analizi Onayı

Aşağıdaki adımlar tamamlandıktan sonra grup iş sürekliliği yönetimi üst yönetimine sunulur ve görüşleri alınır.

- Anahtar ürün ve hizmetler.
- Anahtar ürün ve hizmetler RTO değerleri
- Etki kriterleri tablosu
- Anahtar ürün ve hizmetler için kesintilerin zamana yayılmış etki sonuçları

4.11.2.2.5 İş Etki Analizi Periyotları

Ürün ve hizmetlere ve bunları destekleyen faaliyetler; sistemlerde, alt yapıda, yasal düzenlemelerde, süreçlerde ve insan kaynağında önemli bir değişiklik olmadığı sürece yılda en az 1 kere gözden geçirilir. Sistemler, alt yapı, yasal düzenlemeler, süreçler veya insan kaynaklarında önemli değişiklikler olduğu durumda bu değişikliklerden etkilenen faaliyetler için İEA yapılır. Kapsam dahilindeki ürün ve hizmetler ile bunları destekleyen faaliyetlerde önemli değişiklikler veya meydana gelen süreklilik olayları sonrasında bu durumlardan etkilenen süreçler için İEA güncellenir.

Risk Değerlendirmesi

İş sürekliliği risk yönetimi çalışmaları Şirketin İş Sürekliliği Yönetimi Bölümü tarafından ve Şirket Kurumsal Risk Yönetimi çalışmalarına Kurumsal Risk Yönetimi Prosedürü uyumlu olarak koordine edilir. Kurumsal risk yönetimi çalışmalarını desteklemek üzere iş sürekliliği riskleri bölümler ile yapılan toplantılar ve saha ziyaretleri sırasında analiz edilir ve İş Sürekliliği Risk Yönetimi tablosunda tutulur. İş sürekliliği risk yönetimi çalışmaları kurumsal risk yönetimi çalışmalarına girdi oluşturur.

İş Sürekliliği risklerinin hesaplanmasında beşli skalada etki ve olasılık değerlerinin çarpımı kullanılır. Kriterler ve risk seviyelendirme Kurumsal Risk Yönetimi prosedüründe bulunmaktadır. Teknoloji tarafındaki risklerin değerlendirilmesi Harmony risk modülü üzerinde yapılmaktadır. Kriterler ve risk seviyelendirme Risk Yönetimi Prosedüründe tariflenmiştir.

4.11.3 İş sürekliliği stratejileri

4.11.3.1 Karar verme ve seçme

İş sürekliliği stratejileri, iş etki analizi ve risk değerlendirme sonuçlarına uygun olarak belirlenir. İş Sürekliliği Stratejileri, muhtemel bir afet ve acil durumun yönetilmesi için aşağıdaki unsurları sağlayacak şekilde hazırlanır.

- Önce can güvenliğini sağlamak,
- İç ve dış iletişimi yönetmek,
- Durumu analiz edip kontrol altına almak ve yönetmek
- Durumdan etkilenmemiş; yerleşkenin, insanın, teknolojinin, tedarikçinin imkan ve kaynaklarını kullanmak

Stratejiler hem korumaya hem kurtarma yönelik olarak belirlenir. Korumaya yönelik stratejilere kesintileri en aza indirmesi için ağırlık verilir.

4.11.3.1.1 Tedarikçi Sınıflandırma ve Değerlendirme

Ürün ve hizmetleri destekleyen kritik tedarikçiler belirlenir. Kritik tedarikçilerin belirlenmesi aşamasında satınalma birimlerinden alınan bilgiler ve iş etki analizleri kullanılır. Tedarikçi değerlendirme kapsamında Tedarikçi Yönetim Sistemi Prosedürü kullanılmaktadır.

4.11.3.2 Kaynak ihtiyaçlarını sağlama

İş sürekliliği stratejilerinin uygulanması için gerekli kaynaklar bütçe dönemlerinde bütçelendirilir ve en geç takip eden yıl gerçekleştirilir.

Temel senaryolar olarak en az aşağıda ki durumlar için uygun stratejiler belirlenir ve bu stratejiler için gerekli kaynaklar yönetim tarafından ayrılır.

- Yerleşkenin ulaşılabilir olması
- İş gücü yetersizliği
- Teknoloji kayıpları/arızaları
- Tedarikçi kaybı veya yetersiz kalması

4.4.11.3.3 Koruma ve indirgeme

Risk değerlendirme kısmında belirlenmiş riskler için proaktif önlemler alınması sağlanır. Proaktif önlemler kesintinin olasılığını düşürebilir, kesintinin süresini azaltabilir veya etkisini sınırlandırabilir.

Kabul edilebilir seviyenin üzerinde ki riskler uygun seviye yönetime raporlanır ve risk iştahına uygun olarak risk seviyesi indirmesi yapılır.

4.11.4 İş sürekliliği prosedürlerinin oluşturulması ve uygulanması

4.11.4.1 Genel

Bir kesinti olayını yönetmek ve İş etki analizinde tanımlanmış kurtarma hedeflerini sağlamak üzere gerekli prosedür ve planlar hazırlanır. Planları hazırlarken aşağıda ki hususlara dikkat edilir.

- İç ve dış iletişim ihtiyaçlarını karşılayacak şekilde hazırlanır
- Kesinti sırasında alınacak aksiyonları tanımlar
- Tahmin edilemeyen tehditlere karşı uygulanabilir olması için gerekli esnekliğe sahip olur
- Bağımlılıklar ve belirlenmiş kabullenmelere göre geliştirilir
- Planda yazan tüm kişilerin planı bilmesi için gerekli farkındalık çalışmaları gerçekleştirilir.
- Tüm prosedür ve planlar senelik olarak gözden geçirilir.
- Normale (geri) dönüş aktiviteleri belirlenerek hazırlanır.

4.11.4.2 Olay müdahale yapısı

Telekom operatörünün Grup olay müdahale yapısı Şirketin İş Sürekliliği Planı dokümanında tanımlanmıştır. Olayın can sağlığı ve güvenliğini etkilemesi halinde Güvenlik Faaliyetleri El Kitabı'na uygun şekilde hareket edilir. Her plan ayrıca özel olarak olay müdahale yapısı içerir. Çatı planda standart olay müdahale akışı verilmiştir. Olay duyurusu, olay anında SMS, email üzerinden gönderilir. Şirketin İş Sürekliliği Yönetim Sistemi mobil uygulamasının çalışmadığı durumda, alternatif iletişim kanalları (sms, e-mail, gsm çağrı, uydu çağrı) kullanılarak duyuru yapılır.

4.11.4.3 Uyarı ve iletişim

4.11.4.3.1 Teknik kesintiler,

Telekom Operatörleri mobil, sabit ve servis şebekelerinin hizmet vermesini sağlamak amacıyla 7x24 event izleme incident açma, birinci seviye müdahalesi ve eskalasyonunu Çağrı Merkezi ekibi tarafından gerçekleştirilir.

4.11.4.3.2 Can sağlığı ve güvenliğini etkileyen olaylar

İş sağlığı ve güvenliği takımı çalışan sağlığı ve güvenliği ile ilgili çalışmaları sürekli yapmaktadır. Bununa birlikte afet ve acil durumlarda can güvenliği ile ilgili durumları, doktor ve iş sağlığı ve güvenliği ekipleri aracılığıyla bildirilmektedir.

Kurum binaları güvenlik numaraları, Exchange kontaklarına eklenmiş durumdadır. Acil durumda cep telefonlarından veya Outlook'tan BINA ŞEHİR isim formatında aratıp PSTN, nöbetçi amir ve uydu telefon numaraları görünmektedir.

4.11.4. İş sürekliliği planları

Şirketin İş Sürekliliği Planları (İSP), Şirketin İş Sürekliliği Planı Formuna göre hazırlanır ve resmi doküman yönetim sistemi olarak kullanılan QDMS'te yayınlanır. QDMS bulunmayan grup şirketlerinde doküman yönetimi uygun herhangi bir platform kullanılarak sağlanabilir.

Teknoloji birimlerinde, Şirketin İş Sürekliliği Planları Servis süreklilik planı formuna göre Harmony toolu üzerinden hazırlanır ve yayınlanır.

4.11.4.5 Network Servis Süreklilik ve Kurtarma Planı Hazırlama:

- İş ihtiyaçları kapsamında Harmony de BCM Kritik iş(CFS) servislerine hizmet eden RFS servisler için servis süreklilik ve kurtarma planları hazırlanır. Bu kapsamda BCM Kritik olarak belirlenmiş RFS ler için plan template leri harmony de oluşturulmuştur. Bununla birlikte servis süreç yöneticilerimiz servisleri kritik olarak belirlenmiş olsa bile yeni plan oluşturabilecektir.
- Süreklilik ve Kurtarma Planının hazırlanmasından SPM ekiplerimiz sorumludur. Planların etkiliğinden ve hazırlanmasını garanti altına almaktan servis sahiplerimiz accountable dir.
- Planlar her sene en az bir defa SPM atanacak tasklar ile review edilecektir. Serviste meydana gelecek değişikliklerin süreklilik ve kurtarma planlarına eşzamanlı yansıtılması gerekmektedir.

Süreklilik ve Kurtarma Plan İçeriği

- RPO
- Süreklilik ve Kurtarma Stratejileri (İnsan, Yerleşke, Teknoloji, Tedarikçi)
- Aksiyon Planlarının Hazırlanması
- Kurtarma ve Normale dönüş aksiyonları
- Ekip Bilgileri
- Kritik kaynaklar

Sürekli ve Kurtarma Plan İçeriği

- RPO
- Süreklilik ve Kurtarma Stratejileri (İnsan, Yerleşke, Teknoloji, Tedarikçi)
- Aksiyon Planlarının Hazırlanması
- Kurtarma ve Normale dönüş aksiyonları
- Ekip Bilgileri
- Kritik kaynaklar

4.11.4.4.1 İş Sürekliliği Plan Dokümanı Kapsam Bölümü

İş Etki analizinde belirlenen kritik faaliyetler iş sürekliliği planlarında aksiyon planı ismi ile tanımlanır. Personel ve yerleşke kaybı aksiyon planları kritik aksiyon planı olarak kabul edilmiş ve iş sürekliliği planlarında tanımlanmıştır. Bu nedenle İş etki analizi kayıtlarında ayrıca kritik faaliyet olarak tanımlanmazlar. İş Etki analizinde belirlenmiş kritik servisler, süreklilik ve kurtarma faaliyetleri de iş sürekliliği planlarının kapsamını oluşturur.

4.11.4.4.2 Roller ve Sorumluluklar

Roller ve sorumluluklar planın EKİP sekmesinde tanımlanmıştır. Bu bölümde planda görev alan kişilerin isimleri, ünvanları, sorumlulukları ve alternatif iletişim bilgileri belirtilmelidir. Her bir rolün yedeği bulunacak şekilde plan yapılmalıdır.

4.11.4.4.3 Aktivasyon Kriterleri ve Plan Aktivasyonu

Bu bölümde, ilgili iş sürekliliği planıyla ilgili aşağıdaki bilgiler bulunmak zorundadır:

- Kimlerin ilgili iş sürekliliği planını tetikleyebileceği (devreye alabileceği) bilgisi o Kriz Yönetim Ekibi Ekibi Kırmızı (ulusal koordinasyon gerektiren olaylar) ve Turuncu (diğer fonksiyonlara veya grup şirketlerine ihtiyaç duyulan olaylar) seviyedeki olaylarda Şirketteki tüm planları devreye alma yetkisine sahiptirler

- UHKE ve KYE üyelerini outlook'ta aşağıdaki gruplarda görülebilir. Bu gruplardaki değişiklikler T.C Başbakanlık Afet ve Acil Durum Yönetimi Başkanlığına (AFAD) bildirilmek zorundadır:

- TEAM-UHKE

- TEAM-KYE o KYE haricinde kimlerin ilgili iş sürekliliği planlarını, hangi seviyedeki olaylarda tetikleyebileceği bilgisi yazılmalıdır.

- Kırmızı: Ulusal düzeyde koordinasyonun gerekli olduğu olaylar

- Turuncu: Şirketin içinde birden fazla fonksiyonun veya en az bir grup şirketinin koordinasyonunun gerekli olduğu olaylar

- Sarı: İlgili fonksiyonun kendi kaynakları ile çözebileceği olaylar

- İlgili iş sürekliliği planının aktivasyon kriterleri:

- Kırmızı, Turuncu ve Sarı seviyedeki olaylar aktivasyon kriterlerine yazılmalıdır.

- Bazı faaliyetler hiçbir zaman Turuncu ve Kırmızı seviyede olamayabilir o zaman sadece Sarı seviyenin yazılması yeterlidir.

4.11.4.4.4 Plan Seviyesi Stratejiler

Kesinti durumlarında uygulanacak 5 temel strateji alanı aşağıdaki listelenmiştir:

- Yerleşke Strateji Alanı
- İnsan Strateji Alanı
- Teknoloji Strateji Alanı: (Birden fazla teknoloji stratejisi olabilir)
- Tedarikçi Strateji Alanı

Yukarıdaki her bir strateji alanına, bu alanı kaybettiğimizde (kesintiye uğradığında) stratejimizin ne olacağı yazılmalı.

Bir strateji alanında birden fazla strateji olabilir. Her bir stratejiyi gerçekleştirmek için aksiyonlar yazılmalıdır.

4.11.4.4.5 Aksiyon planları

Temel senaryolar ile ilgili aksiyon planları hazırlanır. Aksiyonlar ile ilgili aşağıdaki bilgiler belirtilmelidir:

- Aksiyonu kimin veya hangi ekibin yapacağı • Ne kadar sürede tamamlayacağı o Herhangi bir stratejiyi gerçekleştirmek için yapılan tüm aksiyonların sürelerinin toplamı (bağımlılıkları göz önüne alınarak toplanır) RTO'dan küçük olmalı o Bu süreler tatbikatlarda KPI olarak kullanılabilir
- Ön bağımlı olduğu diğer aksiyonlar
- Normale (Geri) dönüş aksiyonları

4.11.4.4.6 Kaynaklar

İş sürekliliği planı kapsamında ihtiyaç duyulan kaynaklar belirtilmelidir. Kaynaklar ayrı bir liste olarak belirtilebileceği gibi aksiyon planlarının her adımı içinde belirtilebilir.

4.11.4.5Kurtarma

4.11.5 Tatbikatlar ve testler

Afet ve acil durumlarda iş sürekliliği planlarının istenilen biçimde çalışabilmesi için, hazırlıkların düzenli olarak tatbikatının yapılması ve ortaya

ıkan eksiklikler doęrultusunda planların gncellenmesi gereklidir İř sreklilięi tatbikatlarının amaları ařaęıda sıralanmıřtır;

- Telekom Operatrnn iř sreklilięi konusundaki yeteneklerini deęerlendirmek.
- Planda bulunması gerektięi halde bulunmayan bilgileri tespit etmek
- Planın geliřtirilmesi gereken ynlerini tespit etmek
- Kurtarma takımlarının alıřma performansını gzlemek ve iyileřtirmek
- İř sreklilięi bilincini arttırmak

İř sreklilięi alıřmalarının tamamını bir defada test etmek pratikte olduka zordur. Bu sebeple alıřmaların her yn ile kontrol iin dzenli aralıklarla ve planların farklı ynlerini test eden bir tatbikat programı hazırlanmalı.

İlerleyen blmlerde tatbikatların planlama, gerekleřtirme ve deęerlendirme faaliyetleri tanıtılmıřtır. Tatbikatlar haberli veya habersiz yapılabilir. Bir senaryo eřlięinde planlı olarak gerekleřtirilir. Bununla birlikte ncelikli bir faaliyetin veya servisin bir kısmının dar bir kapsamda alıřıp alıřamayacaęını anlamak iin senaryosu olmayan planlı testler yapılabilir. Ancak yılda en az bir defa yapılan testler, tatbikat ile pekiřtirilmelidir.

Masabařı tatbikatı: İř sreklilięi planı ve ilgili dokmantasyonun gzden geirilmesidir.

Simlasyon: rnek bir olay zerinden iř sreklilięi planı alıřtırılır. Tatbikat sırasında sistemlerde herhangi bir kesinti gerekleřtirilmez. Kesinti gerekleřmiř gibi dřnlerek alıřtırılarak tatbikatı yapılır.

Kritik faaliyet tatbikatı: Kesintiye neden olabilecek örnek bir olay üzerinden kesinti yapılarak planın test edilmesidir.

Entegre tatbikat: Birden fazla senaryo veya planın test edilmesidir.

İletişim tatbikatı: İş Süreklilik Planlarındaki iletişim kısmının test edilmesidir.

Tam tatbikat: İş sürekliliği planının tamamının test edilmesidir. İlgili servis/sistemin ODM'den çalıştırılmasını da içermektedir.

4.11.5.1 Yıllık İSY Tatbikat Programı

Yıllık tatbikat programı iş sürekliliği çalışmalarını her yönü ile test etmek üzere hazırlanır. Program, iş sürekliliği çalışmalarının teknik, lojistik, yönetsel ve dokümantasyon parçalarının tamliğini ve güncelliğini kontrol eder.

Şirketin iş sürekliliği kabiliyetinin artırılması için gerekli olan yıllık tatbikat programı Şirketin İş Sürekliliği Yönetimi bölümü tarafından hazırlanır. Program iş sürekliliği yönetim sisteminin kapsamı ile uyumlu olmalı ve Telekom operatörünün uymakla yükümlü olduğu kanun ve yönetmeliklere uygun hazırlanmalıdır.

Hazırlanan program İş Sürekliliği Yönetimince onaylanmalıdır.

İSP tatbikat programı en az aşağıda listelenen bilgileri içermelidir;

- Tatbikatın kapsamı
- Tatbikatın amaçları
- Planlanan zaman aralığı
- Tatbikat ile ilgili kabullenmeler ve kısıtlar.

İş sürekliliği tatbikatının tatbikata hazırlık, tatbikatın gerçekleştirilmesi ve tatbikatın değerlendirilmesi olmak üzere üç adımı vardır. İş sürekliliği planı tatbikat faaliyetlerinin özeti aşağıda verilmiştir.

Gerekli hazırlıklar ve planlama sürekliliği tatbikatı yapmak, operasyonlarda beklenmeyen kesintilere yol açabileceği gibi Kurumun imajını zedeleyen problemlere dahi sebep olabilir. Bu sebeple tatbikat öncesi yeterli seviyede hazırlık yapılması tatbikattan elde edilmek istenen fayda için gereklidir. Yıllık tatbikat programında bulunan her bir tatbikat için öncelikle tatbikat planı hazırlanmalıdır. Bu plan Bölüm 8.5.2'de detayları verilen tatbikat hazırlık adımına göre hazırlanır. Tatbikat planlaması için Tatbikat Planlama ve Değerlendirme Formunun planlama alanları kullanılır.

Bir sonraki adım tatbikatın gerçekleştirilmesidir. Tatbikatın icra edilmesi ile ilgili detaylar Bölüm 8.5.3'de verilmiştir. Bu adım, tatbikat planı kapsamında iş sürekliliği faaliyetlerinin, planlarının, kritik sistem, servis ve kaynaklarının her yönüyle test edildiği adımdır.

Tatbikatın gerçekleştirilmesi ile ilgili son adım tatbikatın değerlendirilmesidir. Bu adım tatbikatın planlama aşamasına uygunluğunun, tatbikat hedeflerinin, tatbikatın başarılı ve başarısız yönlerinin dokümanede edildiği bölümdür. Her tatbikatın sonunda tatbikat Tatbikat Planlama ve Değerlendirme Formu'na değerlendirme bilgileri girilmelidir. Bu adım ile ilgili detaylar yapılmadan iş Bölüm 8.5.4'te incelenmiştir. Teknoloji grubunda tatbikat planlama ve raporlaması talimatı QDMS'te TCELL-TL-965 nolu talimatta yer almaktadır.

411.5.2 Adım-1 Tatbikata hazırlık

Tatbikata hazırlık adımının çıktısı Tatbikat Planlama ve Değerlendirme Formudur.

Adım-1.1: Geçmiş tatbikat planlarının ve sonuçlarının gözden geçirilmesi Daha önce gerçekleştirilmiş tatbikatların planları ve sonuçları, hazırlanacak yeni tatbikat planı için önemli bir bilgi kaynağıdır. Eğer daha önce gerçekleştirilmiş tatbikatta benzer amaçlar ve kapsam kullanıldı ise yeni planda strateji, lojistik ve zaman planı olarak kullanılabilir bilgiler bulunmaktadır. Ayrıca daha önce yaşanan problemlerin tekrarlanmaması için dikkat edilmesi gereken hususlar yeni planın hazırlanması aşamasında fayda sağlayacaktır.

Adım-1.2: Tatbikat stratejisinin geliştirilmesi

Tatbikat hedeflerine ulaşabilmek için gerekli olan stratejinin oluşturulduğu adımdır. Daha önceki tatbikatlarda oluşturulmuş stratejiler yeni oluşturulacak strateji için bir temel oluşturmaktadır. Tatbikat stratejisinin tatbikat zamanı, tatbikat senaryosu ve tatbikat bütçesi olmak üzere üç bacağı vardır.

1. Tatbikatın zamanı

Tatbikat zamanı, tatbikat kısıtları ve tatbikat için gerekli kaynakların uygunluk durumuna göre belirlenir. Genel kural normal iş operasyonlarına verilecek etkinin en az olacağı bir zaman diliminin seçilmesidir.

2. Tatbikat senaryosu

Tatbikat senaryosu aynı zamanda kesinti veya kriz senaryosu olarak ta bilinir. Tatbikat senaryosu iş kesintilerini kesinti türü, kesinti senaryosu, kesintinin işe vereceği zarar biçiminde içermelidir.

- Kesinti türü: İş sürekliliği planının test edilmesi için seçilecek kesinti türü gerçekçi olmalıdır. Bodrum katta bilgi sistemi barındıran bir işletme için sel riskini ele almak gerçekçi bir senaryo olarak ele alınabilir.

- Kesinti senaryosu: İş kesintisine neden olacak hayali bir veya daha fazla olaydan oluşan senaryodur. Kriz gün ve saat bilgisi senaryo içinde verilmelidir. Ayrıca kesinti sonrasında gerçekleşecek olayların sırası belirli bir kurgu çerçevesinde anlatılmalıdır.
- Kesintinin işe vereceği zarar: Tatbikat kapsamında, gerçekleştiği düşünülen olayın hangi iş operasyonlarını etkilediği, hangi çalışma ortamlarının zarar gördüğü, çalışanların zarar görüp görmediği gibi bilgiler verilmelidir.

4.3. Tatbikat bütçesi

Tatbikatın türüne göre her bir tatbikatın maliyeti vardır. Tatbikatın türü, kapsamı, hedefi, senaryosu tatbikat bütçesini etkileyen faktörlerdir. Tatbikat stratejisinin bir parçası olarak gereken bütçe hesap edilmeli, onayı alınmalı ve tatbikat planında belirtilmelidir. Tatbikat bütçesinin parçaları olabilecek genel harcama kalemlerine örnekler aşağıda listelenmiştir.

- Ulaşım ve taşıma masrafları
- Çalışanların tatbikat için ayıracakları zamanın maliyeti
- Üçüncü parti firmalardan alınacak destekler ile ilgili maliyetler
- Yemek ve barınma hizmeti gereken tatbikatlarda bu hizmetlerin maliyetleri

Adım-1.3: Tatbikat lojistiğinin belirlenmesi

İş sürekliliği tatbikatında lojistik hizmetlerinin kritik bir rolü vardır. Tatbikat lojistik faaliyetleri üç ana başlık altında incelenmelidir.

1. Tatbikat için gerekli kaynak ve ekipmanların temini (eğer gerekiyorsa)

Tatbikatın gerçekleştirilebilmesi için ekipman ve benzeri kaynakların temini gerekebilir. Söz konusu ekipmanların nereden temin edileceği planlanmalıdır. İhtiyaç duyulabilecek ekipmanlara örnekler aşağıda listelenmiştir.

- Ses ve veri iletişim ekipmanlarının temin edilmesi
- Gerekli yazılım ve donanım altyapısının bulunmasını sağlama

2. Personelin yer deęiřtirmesi

Olaęanüstü durum merkezini devreye alma gerektiren tatbikatlarda personelin ana merkezden yeni alıřma ortamına aktarılması gerebilecektir. Örnek faaliyetler aşağıdaki gibidir.

- Ulařım ile ilgili hizmetler
- Gidecek personelin sayısı
- alıřacak personel için gerekli izinlerin temin edilmesi
- Tařınacak takımların ulařım, yeme içme ve kalma ihtiyaçlarının sağlanması ile ilgili alıřmalar.

3. Tatbikat ortamının hazırlanması

Tatbikat ortamı, ana alıřma alanı olabileceęi gibi alternatif yerleřke de olabilir. Tatbikat ortamının hazırlanması ile ilgili faaliyetler tatbikat kaynaklarının tatbikatın gerçekleştirildięi ortamda bulunmasını sağlamalıdır. Bu kapsamda gerçekleştirilen işleri üç parada incelemek mümkündür.

1. Alternatif yerleřkede ihtiyaçların belirlenmesi
2. Alternatif yerleřkede mevcut kabiliyetlerinin deęerlendirilmesi
3. İhtiyaların analiz edilmesi ve eksiklerin belirlenmesi

Adım-1.4: Tatbikat takviminin belirlenmesi

Tatbikat takvimi, tatbikata hazırlık, tatbikatın icra edilmesi ve tatbikat sonu değerlendirme aşamalarını içermelidir. Takvim, kurtarma faaliyetlerinin başlama ve bitiş zamanlarını, ayrıca kurtarma işlerini ve önceliklerini belirtmelidir.

Adım-1.5: Tatbikat risklerinin belirlenmesi

Tatbikat planını hazırlamanın ana amacı, tatbikatın neden olabileceği istenmeyen kesintilerin önüne geçmektir. Her tatbikatın icra edilmesinde bazı riskler vardır. Bu riskleri tatbikat öncesinde belirlemek ve olası problemlere karşı hazırlıklı olmak tatbikatın istenmeyen sonuçlarının önüne geçmek için son derece önemlidir. Aşağıda potansiyel tatbikat risklerini tespit etmek için örnekler verilmiştir.

- Tatbikatın kapsamı gerektiğinden büyük mü?
- İlgili yerleşke tatbikat için yeterli teknik ortamı sağlıyor mu?
- Donanımı ve yazılımı hazır mı?
- Tatbikata katılacak personel ve takımlar durumdan haberdar mı?

Tatbikat riskleri belirlendikten sonra KKE ve koordinatörler riskleri en aza indirmek için gerekli tedbirleri almalıdır. Bu adımda tespit edilen aksaklıklar, tatbikat değerlendirmesi sırasında kullanılmalıdır.

Adım-1.6: Tatbikat planının hazırlanması

Daha önceki adımlarda hazırlanan bilgiler bir araya getirilmeli ve detaylı bir tatbikat planı hazırlanmalıdır. Tatbikat planı uygun yönetim kademeleri tarafından onaylanmalı ve tatbikata katılacak personele

ulařtırılmalıdır. Tatbikata katılacak üçüncü parti firmalara yeteri kadar erken haber verilmelidir.

4.11.5.3 Adım-2 Tatbikatın İcra Edilmesi

Tatbikatlar bir önceki adımda hazırlanan plana uygun olarak icra edilir. Tatbikatın icra edilmesi tatbikat öncesi son düzenlemeler ve tatbikatın gerçekleştirilmesi olarak iki ana başlıkta incelenmelidir.

1. Tatbikat öncesi son hazırlıklar
 - Tatbikata katılan personelin ve takımların hazır ve uygun olduğunun teyit edilmesi
 - Tatbikat öncesi bilgilendirme ve tatbikat akışının katılımcılara özetlenmesi
2. Tatbikatın gerçekleştirilmesi
 - Tatbikat planına uygun olarak tatbikatın başlatılması ve sürdürülmesi
 - Tatbikat değerlendirilmesi için daha önce belirlenmiş kriterlere uygun kanıtların toplanması
 - Tatbikatın bitmesi sonrasında katılımcıların ve ilgili tarafların bilgilendirilmesi.

4.11.5.4 Adım-3 Tatbikatın Değerlendirilmesi

Bu adımda, tatbikatta yaşanan problemler ve iş sürekliliği kabiliyetini geliřtirmek için gerekli iyileřtirme faaliyetleri belirlenir. Tatbikat değerlendirme adımı hazırlanan bilgiler tatbikat sonrası gerçekleştirilmesi gereken faaliyetleri tetikler. Bu sebeple iş sürekliliğinden beklenen faydayı elde edebilmek için bu adımda tatbikatların planda belirtilen kriterlere uygun şekilde değerlendirilmesi gerekir. Bu adımda elde edilen bulgular tatbikata hazırlık ve tatbikatın icrası sırasında elde edilir.

İş sürekliliği tatbikat bulguları potansiyel geliştirme adımlarına girdi oluşturur. İş sürekliliği koordinatörleri tatbikat bulgularını Tatbikat Planlama ve Değerlendirme Formu'na işler. Bu form aynı zamanda iş sürekliliği çalışmalarını güncellemek için gerekli olan iş adımlarını da içerir. Tatbikat planlama ve değerlendirme formu iş sürekliliği koordinatörleri tarafından hazırlanır. Form aynı zamanda katılımcılara ve diğer ilgili taraflara da ulaştırılır.

4.11.5.5 Tatbikat Sonrası Faaliyetler

Tatbikat sonrasında hazırlanan ve içeriğinde geliştirme önerilerinin de bulunduğu değerlendirme formunda yer alan bilgiler kullanılarak QDMS sistemi üzerinde yönetim sistemi alanı ISO22301 seçilerek düzeltici faaliyet açılır. Bu aşamadan sonra düzeltici faaliyet süreci işler.

4.12 Performans değerlendirme

4.12.1 İzleme, Ölçme, Analiz ve Değerlendirme

4.12.1.1 Genel

Bu bölüm iş sürekliliği yönetim sistemi kapsamında uygulanan faaliyetlerle ilgili olarak yapılacak performans değerlendirme çalışmalarının hangi sıklıkta, hangi metriklere göre ve kim tarafından yapılacağını belirlemek üzere hazırlanmıştır.

Belirli zaman aralıklarında, olay meydana geldiğinde veya önemli değişiklikler ortaya çıktığında değerlendirme ve analiz yapılmalı, bulgular ışığında sürekli iyileştirme faaliyetleri ile bu durum yönetim sistemine yansıtılmalıdır.

İş sürekliliği koordinasyon takımı üyeleri ve iş sürekliliği planlarında görev alan personel gözden geçirme, değerlendirme ve ilgili dokümanları güncelleme görevine sahiptir.

İyileştirme yapılabilmesi için sistemli bir analiz yöntemi ile sonuçlara varılmış olması, analiz edilebilecek sağlıklı verilere ise önceden belirlenmiş kriterlere göre yapılan ölçüm yöntemleriyle ulaşılmış olması gerekmektedir.

Yönetim sisteminin izlenmesi ve performansının ölçümü için kontrol listesi aşağıda verilmiştir.

İş Adımı	Hedef
İş sürekliliği hedeflerinin gözden geçirilmesi ve güncellenmesi	Her yıl en az bir defa
İş sürekliliği hedeflerinin ölçülmesi	Her yıl en az bir defa
İç denetimin gerçekleştirilmesi	Her yıl en az bir defa ve kapsamdaki birimleri içerecek biçimde
YGG toplantısının gerçekleştirilmesi	Senede en az 1 defa
İş etki analizi	Tüm faaliyetlerin senede en az bir defa yeniden değerlendirilmesi
Risk değerlendirmesi	Tüm kritik faaliyetleri kapsayacak şekilde risk değerlendirmesinin yapılması
İş sürekliliği planları	Planların her birinin senede en az bir defa gözden geçirilmiş olması
İş sürekliliği tatbikatları	1 sene içerisinde tüm kritik faaliyetlerin kapsanması

4.12.1.2 İş Sürekliliği prosedürlerinin değerlendirilmesi

İş sürekliliği yönetim sistemi kapsamında oluşturulmuş tüm dokümanlar senede en az bir defa uygunluk açısından kontrol edilir. Bu dokümanların başlıcaları aşağıda listelenmiştir;

- İş sürekliliği kapsam dokümanı
- İş sürekliliği politikası
- Yasal yükümlülükler
- İş sürekliliği prosedürü
- İş etki analizi ve risk değerlendirme çıktıları
- Risk işleme planı
- İş sürekliliği planları
- Tatbikat kayıtları
- Olay kayıtları
- İç denetim planı, prosedürü ve raporu
- YGG toplantı içerikleri
- Düzeltici faaliyetler prosedürü ve kayıtları

4.12.2 İç denetim

Telekom operatörünün İş Sürekliliği Yönetim Sistemi iç denetimleri, ISO 22301 standardına göre ve ISO 22301 iş sürekliliği iç denetim prosedürüne göre gerçekleştirilir. İSYS iç denetimlerini Şirketin İş Sürekliliği Yönetimi bölümü koordine eder. Teknoloji birimlerinde iç denetim faaliyeti iç kontrol birimi tarafından yapılmaktadır.

4.12.3 Yönetimin gözden geçirmesi

İş sürekliliği yönetim sisteminin etkinliğini değerlendirmek ve sürekli iyileştirilmesini sağlamak üzere senede en az bir defa Yönetimin Gözden Geçirme (YGG) toplantısı gerçekleştirilir. Toplantı gündemi aşağıda belirtildiği gibidir;

- Bir önceki yönetim gözden geçirme toplantısında alınan aksiyon kararlarının durumu,
- İş sürekliliği politika ve amaçları ile ilgili değişiklik ihtiyaçları,
- Yönetim sistemini iyileştirme fırsatları ve tavsiyeleri,
- İş Sürekliliği Yönetim Sistemi (İSYS) denetimleri ve gözden geçirmelerinin sonuçları (tedarikçi değerlendirme sonuçları dahil)
- Düzeltici faaliyetlerin durumu
- Tatbikat ve testlerin sonuçları
- Bir önceki risk değerlendirmesinde kabul edilebilir seviyenin üzerinde kalan risklerin gözden geçirilmesi
- İSYS'nin kapsamını etkileyebilecek iç ve dış konular,
- Yaşanılan kesinti olaylarından öğrenilenler ve alınan aksiyonlar,
- İş sürekliliği ile ilgili yükselen iyi uygulamalar ve kılavuzlar

Yönetimin gözden geçirme toplantısında İSYS'nin sürekli iyileştirilmesi ve İSYS'de gerekli olan değişiklikler hakkında kararlar alınmalıdır. Gözden geçirme çıktıları aşağıdakileri içermelidir;

- İSYS'nin kapsamı ile ilgili değişiklikler,
- İSYS'nin etkinliğinin artırılması ile ilgili kararlar,
- Risk değerlendirmesi, iş etki analizi, iş sürekliliği planları ve ilgili prosedürlerin güncellenmesi, •

Dahili ve harici olaylara yanıt verebilmek için kullanılan kontroller ile ilgili değişiklikler (iş ihtiyaçları, risk indirgeme, operasyonel şartlar, yasal ve düzenleyici hükümler, kaynak ihtiyaçları vb) YGG

toplantısının çıktıları ilgili taraflara iletmeli ve alınan kararlar takip edilmelidir. YGG'de alınan kararların takip edilmesi Şirketin İş Sürekliliği Yönetimi'nin sorumluluğundadır.

4.12.4 İyileştirme

4.12.4.1 Uygunsuzluk ve düzeltici faaliyetler

İş Sürekliliği Yönetim Sistemi ile ilgili uygunsuzlukların bildirilmesi ve kök sebep analizinin gerçekleştirilmesi, düzeltici faaliyetlerin planlanması, takibi ve kapatılması Uygunsuzluk ve Düzeltici Faaliyetler Prosedürüne göre ve QDMS sistemi üzerinden gerçekleştirilir. QDMS sistemine sahip olmayan grup şirketinde kendi düzeltici faaliyetler altyapısı kullanılabilir.

4.12.4.2 Sürekli iyileştirme

İş sürekliliği yönetim sistemi iş sürekliliği hedeflerinin belirlenmesi ve ölçümü, iç denetimler, yönetimin gözden geçirmeleri, tatbikatlar, farkındalık eğitimleri ve düzeltici faaliyetler ile sürekli olarak iyileştirilir.

4.12. 5 Gözden geçirme

Bu prosedür, Doküman Yönetim Prosedüründe verilen gözden geçirme süresine uygun olarak ilgili süreç sahibi tarafından gözden geçirilir.

Dokümandan sorumlu süreç sahibi, uygulama ile plan/prosedür/talimat/yönetmelik/politika arasındaki uyumun sağlanmasından

sorumludur. Bu sorumluluk, ilgili diğer süreçlerle koordinasyonun sağlanması, gerekli dokümantasyon işlemlerini prosedürlere uygun olarak gerçekleştirilmesini de kapsar.

4.2 Olaylar

1- Doğal afet (sel, deprem, heyelan) & yangın

Yaşanan felaket sonrası “Hasar Tespit Ekibi” tarafından NOC iletişim kanallarına (e-posta, BİP, SMS, telefon) felaketin yaşandığı yerdeki lokasyon ile ilgili enerji durumu, bina, sistemin durumu, ölü/yaralı çalışan sayısı, veri merkezinin genel durumu konusunda bilgilendirme sağlanır. NOC ekibi, bu bilgilerle birlikte Kriz Yönetim Ekibi’ne e-posta, BİP, SMS, telefon kanallarını kullanarak durum bilgilendirmesi yapar.

KYE durum değerlendirmesi yaparak kriz ilanı ve aksiyonların belirlenmesi için süreci başlatır ve aşağıdaki adımları işletir:

- Felaketin yaşandığı bölgedeki çalışanların gerekiyorsa evlerine veya durumlarına göre sağlık kuruluşlarına gönderilerek belirlenecek tarihe kadar izinli sayılması ya da mobil çalışma uygulanması kararı,
- İlgili iş süreklilik/servis süreklilik planlarının devreye alınması kararı,
- Yazılı/görsel medya ve sosyal medyaya bilgi verilip verilmeme kararı, bilgi verilecek ise Kurumsal İletişim Müdürlüğü ve Dijital İletişim Müdürlüğü tarafından taslak metin hazırlanması ve hazırlanan taslak metin için onay verilmesi,
- Çalışanlara bilgi verilip verilmeme kararı, bilgi verilecek ise İç İletişim ekibi tarafından taslak metin hazırlanması ve hazırlanan taslak metin için onay verilmesi,

- Resmi kurum ve kuruluşların bilgilendirmesi, verilecek bilgilerin içeriği bunların dışında hukuki aksiyon alınması gereken durumlarda alınacak hukuki aksiyonların belirlenmesi ve uygulanacak hukuki aksiyonların gecikmeksizin hayata geçirilmesi Hukuk&Regülasyon GMY'liği Kriz Yönetim Ekibinin yönlendirmesi doğrultusunda gerekli aksiyonları alır.
- Bireysel ve kurumsal abonelerin bilgilendirilmesine karar verilmesi. Bilgilendirmeler çağrı merkezi, Kurumsal Satış(Major, Public, Strategic, M.Business), teknik destek ekipleri ve SCSC-TAM(Service Control&Support Center, Technical Account Manager: Hizmet Kontrol&Destek Merkezi Teknik Müşteri Yöneticisi) tarafından yapılır. Çağrı merkezine aboneler tarafından gelen sorulara uygun cevaplar, CEM/Çağrı Merkezi&Fiziksel Kanallar Yönetimi tarafından Kurumsal İletişim ve Sektörel Hukuk ekiplerinden alınan yön ile hazırlanır.
- Deprem, sel, heyelan durumları için hazırlanan ve AFAD ile paylaşılan "Sıfırıncı Dakika Raporu'nun içeriğine onay verilmesi.
- Krizin sona erdirilmesine karar verilmesi.

Kriz Yönetim Ekibi krizi yönetirken AFAD, Kandilli Rasathane ve Meteoroloji tarafından yayınlanan verileri anlık olarak takip eder.

2- Terör

Yaşanan terör olayı ile ilgili "Hasar Tespit Ekibi" tarafından NOC iletişim kanallarına (e-posta, BİP, telefon) olayın yaşandığı yerdeki lokasyon ile ilgili enerji durumu, bina, sistemin durumu, ölü/yaralı çalışan sayısı, veri merkezinin genel durumu konusunda bilgilendirme sağlanır. NOC ekibi, bu bilgilerle birlikte Kriz Yönetim Ekibi'ne e-posta, BİP, SMS, telefon kanallarını kullanarak durum bilgilendirmesi yapar.

Şirketin ofis/plazalarına veya veri merkezlerine yapılan her türlü fiziksel saldırı, bu lokasyonlara içeriden veya dışarıdan yapılan işgâl durumu, kötü niyetli hareketler ve halk ayaklanması durumunda kriz ilan şartı sağlanmış olur.

KYE durum değerlendirmesi yaparak kriz ilanı ve aksiyonların belirlenmesi için süreci başlatır ve aşağıdaki adımları işletir:

- Terör olayının yaşandığı bölgedeki çalışanların gerekiyorsa/güvenli ise evlerine veya durumlarına göre sağlık kuruluşlarına gönderilerek belirlenecek tarihe kadar izinli sayılması ya da mobil çalışma uygulanması kararı,
- İlgili iş süreklilik/servis süreklilik planlarının devreye alınması kararı,
- Yazılı/görsel medya ve sosyal medyaya bilgi verilip verilmeme kararı, bilgi verilecek ise Kurumsal İletişim Müdürlüğü ve Dijital İletişim Müdürlüğü tarafından taslak metin hazırlanması ve hazırlanan taslak metin için onay verilmesi,
- Çalışanlara bilgi verilip verilmeme kararı, bilgi verilecek ise İç İletişim ekibi tarafından taslak metin hazırlanması ve hazırlanan taslak metin için onay verilmesi,
- Resmi kurum ve kuruluşların bilgilendirmesi, verilecek bilgilerin içeriği bunların dışında hukuki aksiyon alınması gereken durumlarda alınacak hukuki aksiyonların belirlenmesi ve uygulanacak hukuki aksiyonların gecikmeksizin hayata geçirilmesi Hukuk&Regülasyon GMY'liği Kriz Yönetim Ekibinin yönlendirmesi doğrultusunda gerekli aksiyonları alır.
- Bireysel ve kurumsal abonelerin bilgilendirilmesine karar verilmesi. Bilgilendirmeler çağrı merkezi, Kurumsal Satış(Major, Public, Strategic, M.Business), teknik destek ekipleri ve SCSC-TAM tarafından yapılır. Çağrı merkezine aboneler tarafından gelen sorulara uygun cevaplar, CEM/Çağrı Merkezi&Fiziksel Kanallar Yönetimi tarafından Kurumsal İletişim ve Sektörel Hukuk ekiplerinden alınan yön ile hazırlanır.
- Krizin sona erdirilmesine karar verilmesi.

3- Gıda zehirlenmesi/salgın hastalık

Hasar Tespit Ekibi (İşyeri Hekimi & İş Sağlığı & Güvenliği) NOC iletişim kanallarına (e-posta, BİP, telefon) salgının/zehirlenmenin yaşandığı lokasyondaki vaka ve durum hakkında bilgilendirme yapar.

NOC ekibi, bu bilgilerle birlikte Kriz Yönetim Ekibi'ne e-posta, BİP, SMS, telefon kanallarını kullanarak durum bilgilendirmesi yapar. KYE kriz ilanını aşağıdaki turuncu ve kırmızı kriterlere göre yapar.

İzlenen Sistem – Durum	Alarm durumunu gözlediğimiz uygulama	İzleyen bölüm / birim izleme metodu	Threshold (eşik değer) tetikleyen durum	Durum
Salgın hastalık	İronik	Sağlık Birimi	1 vaka	SARI
			5 vaka	TURUNCU
			Lokasyonda >5 vaka	KIRMIZI
Gıda/Su zehirlenmesi	İronik	Sağlık Birimi	Aynı lokasyonda %1 vaka	SARI
			Aynı lokasyonda %3 vaka	TURUNCU
			Aynı lokasyonda %5 vaka	KIRMIZI

Kriz Yönetim Ekibi aşağıdaki karar ve aksiyon süreçlerini başlatır;

- Vakanın yaşandığı bölgedeki çalışanların gerekiyorsa evlerine veya durumlarına göre sağlık kuruluşlarına gönderilerek belirlenecek tarihe kadar mobil çalışma uygulanması kararı,
- İlgili iş süreklilik/servis süreklilik planlarının devreye alınması kararı,
- Çalışanlara bilgi verilip verilmeme kararı, bilgi verilecek ise İç İletişim ekibi tarafından taslak metin hazırlanması ve hazırlanan taslak metin için onay verilmesi,
- Krizin sona erdirilmesine karar verilmesi.

Alarm üretilen salgın hastalık ile ilgili Sağlık Bakanlığı'nın bilgilendirilmesi İşyeri hekimi tarafından yapılır.

4- Operasyonel kesinti

NOC Ekibi, yaşanan kesinti ile ilgili Kriz Yönetim Ekibi'ne e-posta, BİP, SMS, telefon kanallarını kullanarak etkilenen bölge/ servis/ saha ile ilgili durum bilgilendirmesi yapar.

KYE durum değerlendirmesi yaparak kriz ilanı ve aksiyonların belirlenmesi için süreci başlatır ve aşağıdaki adımları işletir:

- İlgili iş süreklilik/servis süreklilik planlarının devreye alınması kararı,
- Yazılı/görsel medya ve sosyal medyaya bilgi verilip verilmeme kararı, bilgi verilecek ise Kurumsal İletişim Müdürlüğü ve Dijital İletişim Müdürlüğü tarafından taslak metin hazırlanması ve hazırlanan taslak metin için onay verilmesi,
- Çalışanlara bilgi verilip verilmeme kararı, bilgi verilecek ise İç İletişim ekibi tarafından taslak metin hazırlanması ve hazırlanan taslak metin için onay verilmesi,
- Etkinin büyük olduğu durumlarda ve/veya BTK'nın kesinti ile iletişime geçtiği durumlarda resmi kurum ve kuruluşların bilgilendirilmesi, verilecek bilgilerin içeriği için Regülasyon Yönetimi'nin aksiyon alması,
- Bireysel ve kurumsal abonelerin bilgilendirilmesine karar verilmesi. Bilgilendirmeler çağrı merkezi, Kurumsal Satış(Major, Public, Strategic, M.Business), teknik destek ekipleri ve SCSC-TAM tarafından yapılır. Çağrı merkezine aboneler tarafından gelen sorulara uygun cevaplar, CEM/Çağrı Merkezi&Fiziksel Kanallar Yönetimi tarafından Kurumsal İletişim ve Sektörel Hukuk ekiplerinden alınan yön ile hazırlanır.
- Krizin sona erdirilmesine karar verilmesi.

5- Siber saldırı

Gerçekleşen siber saldırı sonucu Hasar Tespit Ekibi içinde yer alan Bilgi Güvenliği ekibi Teknoloji Grup Yönetişim Güvenlik Direktörü & NT-ICT Servis Sahibi Direktörleri'nden onay alarak NOC iletişim kanallarına(mail, BİP, telefon) bilgilendirme yapar. NOC Ekibi, Kriz Yönetim Ekibi'ne e-posta, BİP, SMS, telefon kanallarını kullanarak durum bilgilendirmesi yapar.

KYE durum değerlendirmesi yaparak kriz ilanı ve aksiyonların belirlenmesi için süreci başlatır ve aşağıdaki adımları işletir:

- İlgili iş süreklilik/servis süreklilik planlarının devreye alınması kararı,
- Yazılı/görsel medya ve sosyal medyaya bilgi verilir verilmeme kararı, bilgi verilecek ise Kurumsal İletişim Müdürlüğü ve Dijital İletişim Müdürlüğü tarafından taslak metin hazırlanması ve hazırlanan taslak metin için onay verilmesi,
- Çalışanlara bilgi verilir verilmeme kararı, bilgi verilecek ise İç İletişim ekibi tarafından taslak metin hazırlanması ve hazırlanan taslak metin için onay verilmesi,
- Resmi kurum ve kuruluşların bilgilendirmesi, verilecek bilgilerin içeriği bunların dışında hukuki aksiyon alınması gereken durumlarda(dava engelleme v.b) alınacak hukuki aksiyonların belirlenmesi ve uygulanacak hukuki aksiyonların gecikmeksizin hayata geçirilmesi Hukuk&Regülasyon GMY'liği Kriz Yönetim Ekibinin yönlendirmesi doğrultusunda gerekli aksiyonları alır.
- Bireysel ve kurumsal abonelerin bilgilendirilmesine karar verilmesi. Bilgilendirmeler çağrı merkezi, Kurumsal Satış(Major, Public, Strategic, M.Business), teknik destek ekipleri ve SCSC-TAM tarafından yapılır. Çağrı merkezine aboneler tarafından gelen sorulara uygun cevaplar, CEM/Çağrı Merkezi&Fiziksel Kanallar Yönetimi tarafından Kurumsal İletişim ve Sektörel Hukuk ekiplerinden alınan yön ile hazırlanır.
- Krizin sona erdirilmesine karar verilmesi.

USOM bilgilendirmesi SOME üzerinden yapılmaktadır. USOM'a yapılacak bilgilendirmenin içeriği için Kurumsal İletişim ve Regülasyon Yönetimi&Sektörel Hukuk ekipleri destek verir. SOME'nin bilgileri Ek-2 Ekip Listesinde bulunmaktadır.

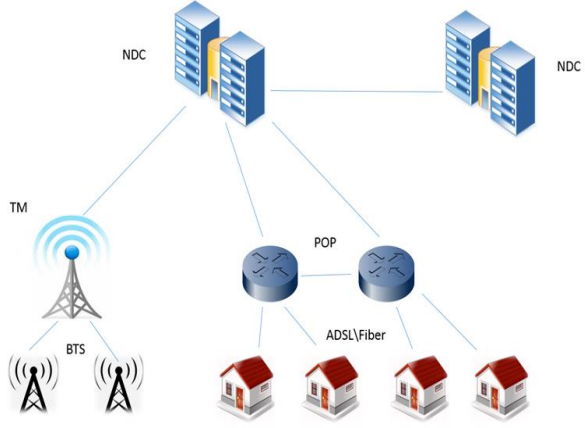
4.3 Olası İstanbul depreminde iş sürekliliği

Merkez üssü Marmara Denizi Adalar açıklarında 7.5 şiddetinde deprem oldu. Deprem genel olarak hem Asya hem de Avrupa yakasında E5 karayolunun güneyinde etkili olmuştur.

- ✓ Deprem genel olarak hem İstanbul Asya hem de Avrupa yakasında E5 karayolunun güneyinde etkili olmuştur.
- ✓ Sahil bölgesinde küçük dalgalar görünse de Tsunami yaşanmamıştır.
- ✓ İstanbul'daki ana devlet yolları açıktır. Tek hasar E5 Küçükçekmece-Avcılar arasında Göl hizasındaki çökmeden kaynaklı olarak yol kapalıdır.
- ✓ E5 ve altındaki ilçelerde ara sokaklarda yıkıntılar nedeniyle trafik akışı sağlanamamaktadır. E5 trafiğe açıktır. Her iki yakada da sahil yolunda göçük-kırıklar olsa da ulaşım sağlanabilmektedir.
- ✓ Ciddi bir hasar görünmese de Marmaray ve Metro seferleri durdurulmuştur. Metrobüs seferleri Anadolu yakasında Acıbadem'e kadar yapılabilir. Avrupa yakasında Sefaköy'e kadar yapılabilir. Havalimanları ciddi hasar görmemiş ancak uçaklar çevre şehirlere yönlendirilmiştir.
- ✓ Deniz taşıtları işler durumdadır. İstanbul'daki Operatöre ait tüm mobil baz istasyonlarının %28'si servis dışı kalmış ve trafiğin %27'si kayıptır.

Marmara Deprem Senaryosu

- ✓ NDC/POP/TM Riskleri
- ✓ 2001, 2007 Deprem Yönetmelikleri
- ✓ 1980 öncesi imarlı POP/TM'ler



İstanbul Depremi

Merkez üssü Marmara Denizi Adalar açıklarında 7.5 şiddetinde deprem oldu. Deprem genel olarak hem Asya hem de Avrupa yakasında E5 karayolunun güneyinde etkili olmuştur.

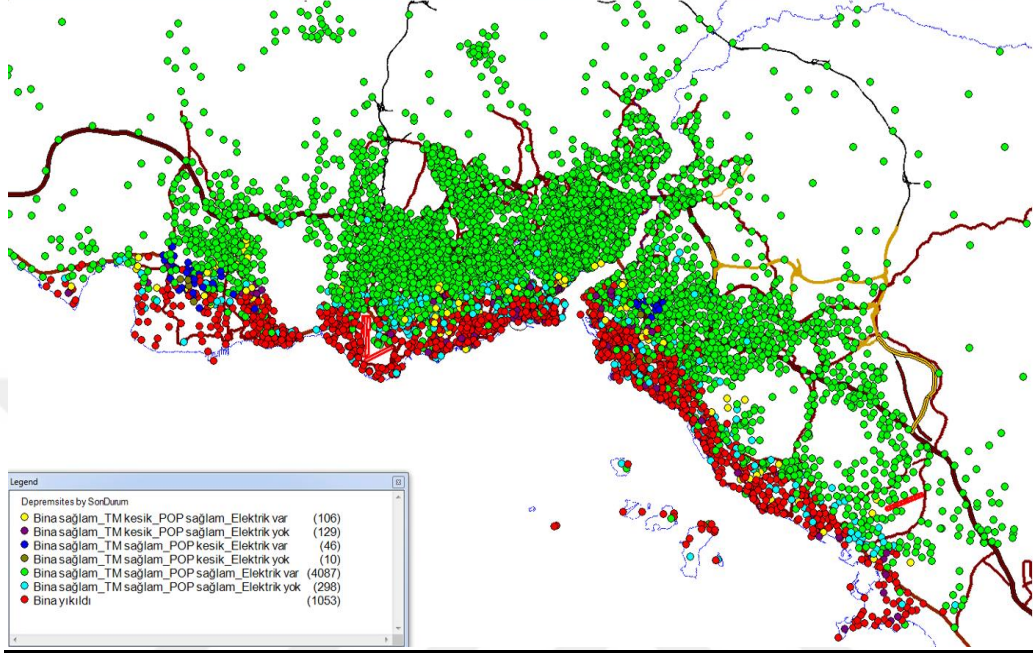


İstanbul'daki tüm istasyonların %28'si servis dışı kalmıştır.

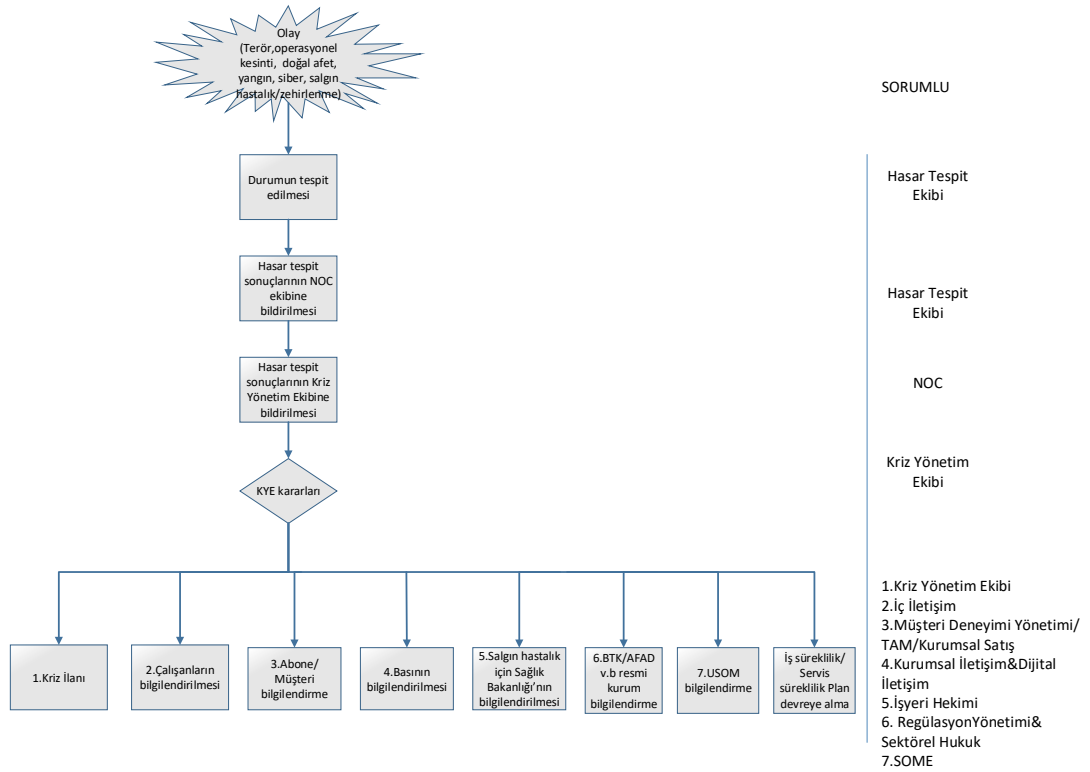
E5 Küçükçekmece-Avcılar arasında göl hizasındaki çökmeden kaynaklı olarak yol kapalıdır

E5 trafiğe açıktır her iki yakada da sahil yolunda göçük-kırıklar olsa da ulaşım sağlanabilmektedir. Tsunami yaşanmamıştır. İstanbul'daki ana yollar açıktır. Deniz taşıtları işler durumdadır.

Istanbuldaki sahalarnn %28'i kesilmiş/yıkılmıştır.



Süreç akışı



Diyarbakır, Erzurum, Kocaeli, Adana, Gaziantep, Elazığ, Samsun, Trabzon, Van illerimizde Ses, data ve mesajlaşma servislerinde kesinti yaşanmaktadır.

▪ Fırtına nedeniyle enerji hatlarının zarar görmesi sonucu ilgili il merkezlerimizde bulunan bazı POP, TM ve sahalarımıza elektrik verilemiyor. Bu illerde görev yapan BÇO'larımızın bir kısmı sahada sel nedeniyle mahsur kalmış durumda.

✓ BCM Kriz ilanı sonrası, Adana, Diyarbakır, Erzurum, Gaziantep, Kocaeli, İstanbul, İzmir, Samsun, Trabzon ve Van illerimizde ve ilgili BÇO ofislerimizde Kriz Masaları oluşturulmuş ve iş/servis sürekliliği planları devreye alınmıştır.

✓ Şebekede Enerji tüketiminin azaltılması amacıyla elektrik kesintisinden etkilenen 9 ilimizde, 158 (2G, 3G, LTE) sahada AFAD Elektrik kesintisi parametreleri başarılı olarak uygulandı.

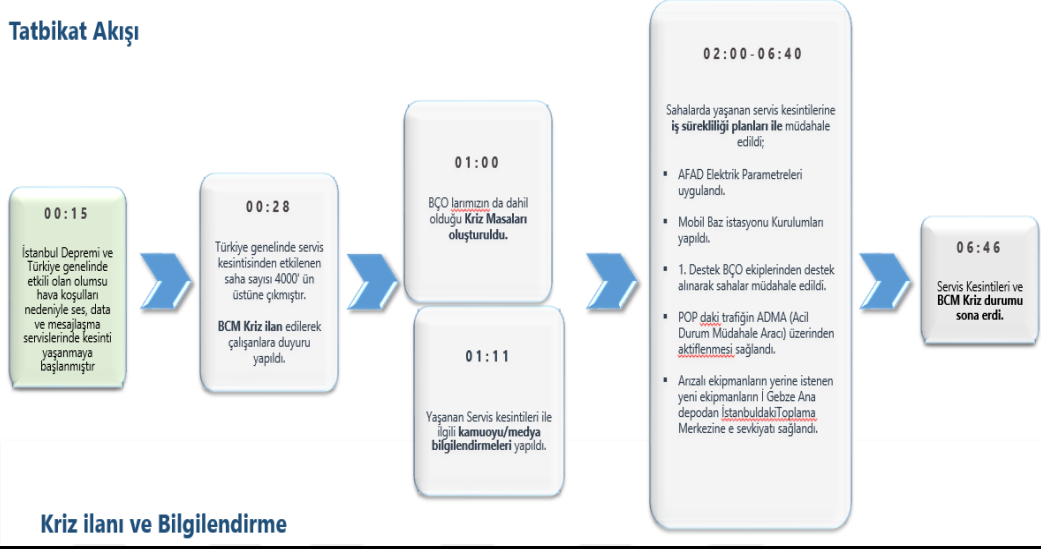
✓ Afetten etkilenen illerimizde ses, veri/internet ve mesajlaşma servis ihtiyaçlarını karşılamak üzere toplam 6 adet uydu ve normal Mobil baz istasyonu kurularak servise verilmiştir.

✓ Bölge Çözüm ortaklarımızın ve servis süreç yöneticilerimizin personel yedekliliği planları devreye alınmıştır; Afetten etkilenen tüm illerimize diğer illerde görevli 1.Destek Bölge Çözüm Ortaklarımız sevk edildi ve arızlara müdahale etti.

✓ Depremde hasar gören Bornova POP daki trafiğin ADMA (Acil Durum Müdahale Aracı) üzerinden aktiflenmesi sağlandı ve POP üzerinden verilen servislerin sürekliliği sağlandı.

✓ İzmir Bornova ilçesinde hasar gören Toplama Merkezimizdeki Network ekipman(TAN 7705) arızası sonrası yedek ekipmanların hedef kurtarma süresi içinde (9 saat) İstanbul Gebze Ana depodan İzmir Bornova Toplama Merkezine e sevkiyatı sağlandı.

Tatbikat Akışı



- ✓ Kriz Yönetim Planı uyarınca KKE(Kurum Koordinasyon Ekibi) dan onay alınarak BCM(Kriz) ilan edildi ve tüm operatör çalışanlarına mail ve sms yoluyla duyuru yapıldı. (full)

5.TARTIŞMA

İş Sürekliliği organizasyonun gelecekte nasıl olacağı konusunda düşünmek istediğimizde, şu sorunun cevabını aramalıyız: “Bu disiplin nasıl ortaya çıktı?”

En basit şekli ile hiç düşünülmeyen bir olayın meydana gelebilme ihtimalinden. “Verilerin kurtarılmasından”. 1970’lerde mainframelerde başlanılan yolculuk, şu anda çok daha büyük hızla ilerlemektedir. Disaster Recovery (Felaket Kurtarma) ile başlanılan süreç günümüzde İş Sürekliliği Yönetimi’ne kadar uzanmaktadır. Bu disiplin, asıl işi farklı olan bir süreçten aldı ve kendi disiplini üzerine standartlarla, en iyi uygulamalarla, kazanımlarla onu geliştirdi. Bu şekliyle, kendine özgü bir disiplini olmayacak olan başka bir disiplin yarattı.

Ülkemiz İş Sürekliliği yönüyle büyük bir birikime sahiptir. Karşılaşılması istenmeyen birçok olay, İş Sürekliliği yönetimine deneyim katmaktadır. Bunun onda biri bile gelişmiş ülkelerde yoktur (olması da gerçekte hiç bir zaman talep edilmez). Deprem, sel, teknoloji odaklı, ya da kullanıcılardan kaynaklanan; sonuç olarak İş Sürekliliği süreçlerini çalıştıran kesintiler, Doğal afet, siber terör, sosyal medya üzerinden marka ve itibarı tehdit eden olaylar (incident) son derece gündemdedir. Basında çıkan bir açıklamanın tweeter üzerinden yansıması, facebook veya bloglara düşmesi ciddi krizler oluşturabileceği gibi itibar kayıplarına sebep olmaktadır. Neticede yaratılan spekülasyona karşı bir karar mekanizmasının oluşması, basın sözcüsünün açıklama yapması ve bir stratejinin geliştirilmesi gereklidir ve tüm bu işlerin o anda yapılması zorunludur, bunun yanında işin hukuki boyutunu düşündüğümüzde Regülasyon kurumlarında gelebilecek ağır yaptırımlarla firmalar karşı karşıya kalmaktadır. Bu da ilgili tarafların (interested parties) başlangıçta çok iyi analiz edilmesi gerekliliğini ortaya koymaktadır. İş Sürekliliği, tüm şirketin/kurumun haritasını gözler önüne sermektedir. Yine hiç

bir zaman unutulmaması gerekli bir konu da, olası doğal afetler ve sanal tehditler işleri aksatmıyorsa o kurumda İş Sürekliliği olduğunu belirtebiliriz.

Gelecekte iş disiplini olarak baktığımızda İş Sürekliliği yönetimi, yapısı gereği çok yönlü olması, sektör bağımsızlığı ile araştırma ve analiz tutkusu olanlara büyük fırsatlar sunmaktadır. İş Sürekliliği ise daima gelecekteki krizlere karşı bugünden planlama yapmayı, bunları uygulamayı, izlemeyi, düzeltmeyi ve geliştirmeyi hedefler. Bu sayede krizlerin olmasına rağmen kurumların iş süreçlerinde herhangi bir problem yaşanmaz.

Örneğin Türkiye'deki Telekom operatörlerinin İş sürekliliği eylem planlarını incelediğimizde, acil durumlarda alınacak eylemlerde farklı öneriler oluşturulduğunu görebiliriz.

Turkcell 2019 yılında Doğal afetlerde iletişimi daha hızlı yapma adına "Dronecell" projesini açıklayarak gerek müşterilerden gerekse regülasyon kurumlarında ciddi takdir almıştır.

Bu Proje aşağıdaki şekilde özetlenmiştir;

Dronecell Amaç;

Turkcell, Türkiye'nin 4.5G hizmeti veren ilk uçan baz istasyonu Dronecell'i geliştirdi. Dronecell, güçlü bir baz istasyonu olarak istenen yerden havalanıp, ses ve data hizmeti sağlamak üzere tasarlandı.

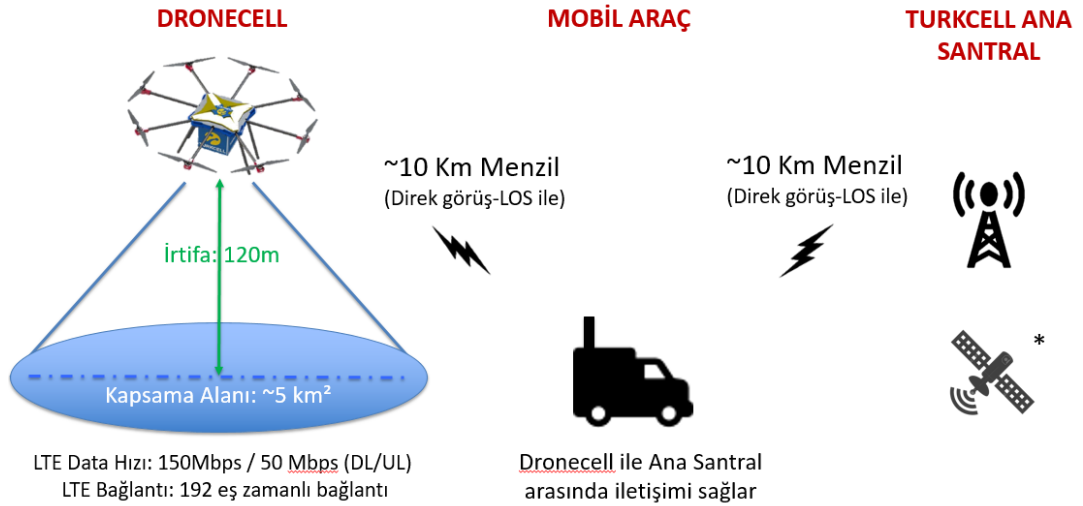
Birçok konuda fayda sağlamak üzere geliştirilen Dronecell özellikle deprem, sel, heyelan gibi doğal afetlerde ve acil durumlarda arama kurtarma ekiplerine iletişim desteği sağlamak için dizayn edildi. Otomatik pilot özelliği de bulunan Dronecell, koordinatları girilen noktaya kendisi ulaşabiliyor. İstenen noktaya ulaştığında motorlarını kapatan Dronecell, sabit bir çekim noktası gibi uzun süre 4.5G internet bağlantısı hizmeti sunuyor.

Bunun dışında konser, maç, miting gibi insanların geçici ama yoğun olarak toplandığı sosyal alanlarda daha hızlı iletişim sağlamak için de Dronecell hizmetinden yararlanılacak.

Dronecell Kullanım Alanları;



- Doğal afetlerde ek mobil kapsamanın devamlılığını sağlamak
- Arama kurtarma çalışmalarında ek mobil kapsama sağlamak
- Araçlarla ulaşılamayan bölgelerde ek mobil kapsama sağlamak



Bunların yanında sektöre aşağıdaki şekilde de hizmet sunuyor olacak; “Sosyal ortamlarda da hızlı iletişimin merkezi olacak”

Konser, maç, miting gibi insanların geçici ama yoğun olarak toplandığı sosyal alanlarda daha hızlı iletişim sağlamak için de Dronecell hizmetinden yararlanılacak

“Nesnelerin internetinde veri toplayıp, ulaştıracak” Havadan mobil 4.5G hizmeti sunan Dronecell, Turkcell şebekesi üzerinden veri haberleşmesi yapan akıllı cihazlarda bilgi toplayabilecek ve nesnelerin internetine mobil ulaşım sağlayabilecek. Özellikle tarım alanları, akıllı su ve elektrik saatleri, barajlar, inşaat şantiyeleri ve madenler gibi alanlarda bulunan IoT cihazlarının akıllı sensörlerinden toplanan bilgilerin, işlenip ilgili kişilerin cep telefonuna iletilmesi Dronecell teknolojisi ile sağlanacak.

Alternatif İletişim Sistemleri;

Olası afet durumlarında çoğullama teknolojisi ile çalışan sabit ve mobil telefonlarının alt yapıları zarar göreceği için ilk anda iletişim kurulamayacaktır. BCM planlarının uygulanması için görevli personeller arasında alternatif uydu telsiz ve gibi ekipmanların tedarik edilmesi ve işler durumda olması sağlanmalıdır.

Digital telsiz

- Bütün operasyon merkezlerinden telsiz sistemi olmalıdır.

Uydu telefonu

- Kriz Yönetim Ekibi olmalıdır.

ISYS Aplikasyon

- Bütün çalışanlarda olmalıdır.

İş Güvenliği ve Sürekliliği Mobil Uygulaması;

Telekom Sektöründe İş sürekliliğini gerektiren durumlarda ekosistemdeki bütün paydaşların bilgilendirilmesi ve gerektiğin bütün iş sürekliliği planlarının offline olarak alınabildiği Mobil uygulama olan ISYS (iş sürekliliği yönetim Sistemi) kullanılmak üzere Android ve IOS uyumlu Mobil uygulama geliştirilmelidir. Bu uygulama BCM planında ilgili bütün herkesi bilgilendirmeli, onların can sağlığı ile ilgili bilgileri almasını sağlamalıdır. Aynı zamanda iletişim bilgileri başta olmak üzere gerekli bilgilerin offline alınmasını sağlamalıdır

Uygulama içeriği

Acil durum SMS,

BCM durumunda personeli Acil durum sekmesinden personelin afetten zarar görüp görmediğini konumu paylaşmaktadır.

Olay Bildirme ;

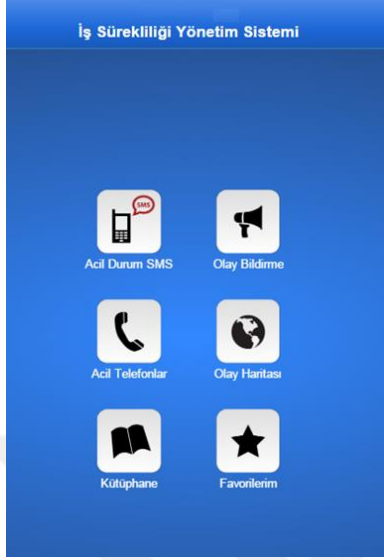
Bütün kullanıcıların Önleyici faaliyetlerin bildirilmesini

Acil Telefonlar;

Kritik kurum telefonları ve Kurum içindeki bütün personellerin Uydu ve alternatif telefonlarının saklanması

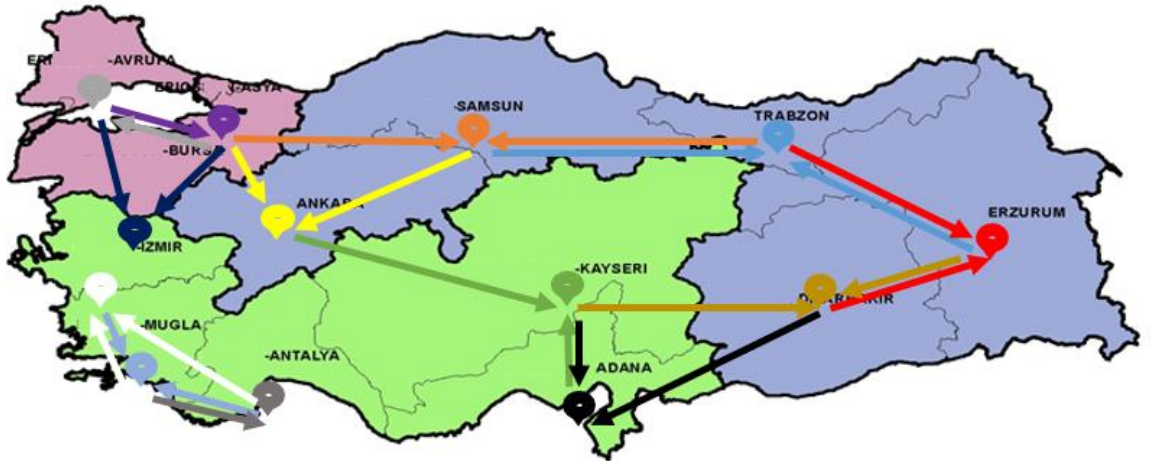
Olay haritası, web harita tabanlı çalışan uygulamada afetin etkilediği bölge ile ilgili detaylar girilmekte ve raporlanmaktadır.

Kütüphane; BCM arama zinciri, iş sürekliliği eylem planları olmak üzere konu ile ilgili bütün dökümanları bulunduğu alandır.



Alterantif Bakım Çözüm ortağı&Tedarikçi ve Bölge Yedekliliği Planları;

Olası bir afet durumunda ilgili bölgedeki çalışanların, tedarikçilerin ve çözüm ortaklarının bazı çalışanlarınınında etkileneceğini hatta bir kısmının vefat edeceğini düşündüğümüzde mutlak suretle Bölgesel yedeklemelerin yapılması gerekir. Bu yedekle farklı iki bölge olarak yapılmalıdır.



BÇO ve Bölge Ekip Yedekliliği

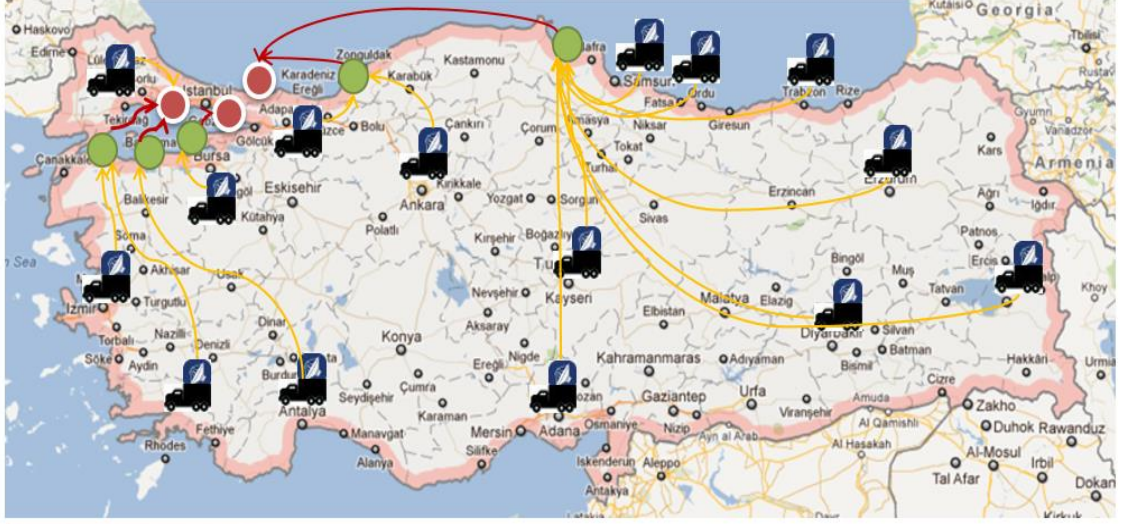
- Afet ve acil durumlarda İş Sürekliliği planına göre diğer bölge BÇO'larından destek ekibi yönlendirmesi başlar. Her bir il için 4 ilden destek verecek şekilde BÇO yedeklilik planı mevcuttur.

Destek Ekip Süreleri:

- Destek BÇO -1 Kategorisi :6 Saat
- Destek BÇO -2 Kategorisi :12 Saat
- Destek BÇO -3 Kategorisi :18 Saat
- Destek BÇO -4 Kategorisi :18 Saat

BCM durumunda Alternatif ulaşım araçlarının kullanılması;

Olası bir afet durumunda istanbuldaki bütün yolların ulaşımına kapanması bekleniyor. Bu şartlar altında yedek ve mevcut personelin müdahale edilecek noktalara ulaştırılması için alternatif ulaşım araçları kullanılmadığıdır. Bunlar Deniz ulaşım araçları ve motosiklet çözümü trafik etkisini ortadan kaldırılacaktır. Tatbikat doğrultusunda mevcut deniz ve motorsiklet tedarik anlaşmaları tamamlanmalıdır.



Vodafone International BCM politikasını inceldiğimizde gerek kendisi gerekse bütün ekosistem çalışanları için son derece önemli olan aşağıdaki manifestoyu yayınlamıştır.

Vodafone Tedarik Şirketi Tedarikçiler ile tedarik anlaşmaları.

Vodafone Grup uluslararası BCM Politikası

Bu Politikasında yer alan “Tedarikçi” ifadesi, ilgili hallerde tüm çalışanları, çalışanları, Yükleniciler, taşeronlar ve tüm satış kanalları kapsar.Vodafone Grubu Şirketlerinden mal veya hizmet sağlayayn veya yararlanan bütün herkesi kapsar.

1. BCM sisteminin derhal kurulmalı, doğru bir şekilde detaylı tanımlanır ve bu planlar Vodafone İş Sürekliliği Yönetimi ekibine iletilir. Ve bu çalışmalar her takvim yılında bir defadan fazla olmamalıdır.
2. Her ekip uluslararası standartlarda kabul edilen İş Sürekliliği Yönetim sistemine sahip olmalıdır. (örneğin, ISO 22301)
3. Her şirket Vodafone ile ürün ve hizmetler için İş Sürekliliği Yönetimi'ne sorumlu bir kişi atamak zorundadır
4. Bir işletmeye neden olabilecek riskleri belirlemek için periyodik olarak risk değerlendirmesi yapılmalıdır. Vodafone bunları kontrol edip uygulamaları denetler
5. Kesin hükümlerini sağlamak için belgelenmiş bir İş Sürekliliği Planının (BCM) olmasıdır. Bu planların tatbikatlarını izlemek ve değerlendirme Vodafone tarafında yapılacaktır.
6. Tedarikçi ve çalışan gruplar ilişkili plan etkinliğini sağlamak adına İş Sürekliliği Planını (BCP) periyodik olarak test etmek, sonuçlarını sunmak zorundadır
7. Vodafone, Tedarikçinin BCM'sindeki bir zayıflığı veya uygunsuzluğu tespit etmesi durumunda karşılıklı olarak belirlenen sürede riskin ve uygunsuzluğun giderilmesini sağlamak zorundadır.
8. BCM politikasının uygulanmaması durumunda Vodafone yapılan işi durdurur.
9. Vodafone sunulan Ürünlerin tedarikini etkileyen servis kesintileri durumunda Vodafone'a bilgi verilmelidir.
- 10.

Vodafone ekosisteminde çalışan herkes Vodafone tarafından yönetilen iş sürekliliği tatbikatlarına veya denetimlerine katılmak zorundadır

Woodman belirttiđi üzere; "iş sürekliliđinin başarıya ulaşmasında üst yönetim desteđi kadar önemli bir başarı faktörüdür" (ITIL, COBIT ISO 22301 gibi konu ile ilgili uluslararası standartlarında; İş Sürekliliđi yönetimi için en büyük zorluk ise kurumun üst yönetimi ve çalışanlarının bunu benimsemesi ve bunu kültür haline getirmesidir.

Ulaştırma Bakanlığı BTK, AFAD kurum misyonları incelendiđinde iş sürekliliđi planlarının zamanında doğru ve çok yönlü yapması, rol ve sorumlukların tanımlanması, bunları üst yönetici ve çalışanların katılımı ile yapılacak tatbikatlar ile pekiştirilmesi, gelecek dönemlerde yaşanacak doğa afet, siber saldırı gibi kurumu tehdit eden olayların üstesinde gelme becerisi artıracaktır. Bu sayede Şirketler bu süreçte Maddi ve manevi kayıpların önüne geçmiş olacaktır

6. SONUÇ

Büyük afetlerde ve acil durumlarda altyapı hasarları ve kullanım yoğunluğu gibi nedeniyle Telekomünikasyon altyapı ve iletişim hatları yoğun olarak kesintiye uğramaktadır. Doğal Afet ve acil durumlarda müdahalenin yapılabilmesi, koordinasyonun doğru olarak yapılabilmesi, kaynakların kullanılabilirliğinin tespiti ve bunların etkin kullanımı ve Kamu ve özel sektör çalışanlarının bilgi senkronizasyonunun yapılması, kısaca afet ve acil durumun tümüyle yönetilmesi açısından haberleşme sistemlerinin daima çalışır olması, olası can ve mal kayıplarının azaltılması noktasında hayati önem taşımaktadır. Telekom operatörler Cumhurbaşkanlığı, bakanlıklar BTK,AFAD, BANKALAR başta olmak üzere bütün şirketlerin Digital verileri ile şebeke altyapısı sunmaktadır. Bu hizmet ve servislerin verilememesi durumunda Ülkenin ciddi bir koasa süreklenmesi kaçınılmazdır. Bunun yanında Olası felâket veya kesintilerde dolayı müşterilerine hizmet veremeyen kuruluşlar bir süre sonra müşteri memnuniyetsizliğinden dolayı gelir ve Pazar kaybı ile karşılaşır ve krizin boyutuna göre uzun vadede yok olabilirler. Bu olaylar herhangi bir doğal afetten, yazılı/görsel/sosyal medyadaki olumsuz haberlerden, siber saldırılardan veya altyapı sistemlerindeki herhangi bir sebepten ortaya çıkabilir.

Yapılan tatbikatlarda görüleceği üzere, öncelikle çalışanların can güvenliğinden emin olunabilecek alternatif bir haberleşme kanalı kurulmalıdır. Bu haberleşme sistemi Telsiz uygulama ve uydu telefonu gibi alternafi yedek seçenekleri içermelidir. Olası bir depremde bölgedeki çalışanlarında deprem etkileneyeceği gözünüde bulundurduğumuzda şirketin farklı bölgelerinde çalışan ekiplerin müdahale etme planları oluşturulmalı ve kendilerine bildirilmelidir. Olay anında çalışan personel ve kullandığı araçlar için lojistik desteği devamı için önceden tedarikçiler ile görüşülmeli ve hazır olmalarını sağlanmalıdır. Aynı zamanda trafik problem yaşanacağı için deniz araçları ile anlaşmalar sağlanmalıdır. Olası bina yıkımlarında bazı bölgelere kara yolu

ile erişim sağlanamayacağı için drone/Zeplin gibi alternatif baz istasyonu modelleri geliştirilmeli ve bunlar hayata geçirilmelidir.

Özetle; Doğal afet, siber saldırılar başta olmak üzere bu tür kesintilerde en az düzeyde etkilenmek için iş sürekliliği takip sistemi tasarlanmalı, Tatbikatlar yapılmalı, riskler ortaya çıkarılması ve buna uygun planlamalar ve tedbirler hayata geçirilmelidir. Bu çalışmalar yapılırken mutlak suretle Üst yönetimin desteği tam alınmalıdır.

Tez döneminde yapılan incelemelerde sadece Telekom operatörlerinin iş sürekliliği planlarının hazırlanması, ilgili kritik riskler ele alınması ve bu konular çözümü için bilimsel metodlar geliştirilmiştir. Bu çözümlerin uygulanması ve geliştirilmesi ile olası Doğal afet veya benzeri durumların en az hasar ile atlatılması hedeflenmektedir.

KAYNAKÇA

- 1- ISO 22301 Societal Security, Business Continuity Management Systems (01.12.2018)
www.iso.org/standard/50038.html
- 2- TSE Türk Standartları Enstitüsü, 22301- İş Sürekliliği Yönetim Sistemi (01.12.2018) www.tse.org.tr/lcerikDetay?ID=2438&ParentID=1064
- 3- ISO22301 - Business Continuity Management , BSI (01.12.2018)
www.bsigroup.com/en-GB/iso-22301-business-continuity/
- 4- Senedaker, Susan.
Business.Continuity.And.Disaster.Recovery.Planning books
- 5- Aydemir , Zehre *Business continuity of Istanbul metrosu Yüksek Lisans tezi (2013)*
- 6- Nar, Melek *İş sürekliliği yönetiminde (BCM) kritik başarı faktörlerinin belirlenmesi ve önceliklendirilmesi 2018*
- 7- Akpınar, Haldun. Enformasyon Teknolojilerinde İş Sürekliliği Yönetimi ve Felaket Planlaması
http://haldunakpınar.com/felaket_planlamasi.pdf
- 8- Turkcell İş sürekliliği ve 22301 iş planları
www.turkcell.com.tr/tr/hakkimizda/genel-bakis/is-surekliligi-politikasi
- 9- Ergünay O., “Afet Yönetiminde İşbirliği ve Koordinasyonun Önemi”,
Afet Yönetiminin Temel İlkeleri, ed.
- 10-Kadioğlu, M. ve Diğerleri, 2005. *Eğitim Kurumları için Afet Acil Yardım Planı Kılavuzu*, İ.T.Ü. Afet Yönetim Merkezi, İstanbul:İ.T.Ü Press
- 11-Kadioğlu, M. 2009. *Sanayi ve İşyerleri için Afet Acil Yardım Planlama Rehberi*, İstanbul Afet ve Acil Durum Müdürlüğü (ADM) ve İstanbul İl Özel İdaresi İPKB: İstanbul: Beyaz Gemi Eğitim ve Danışmanlık.
- 12- Kadioğlu, M., 2009. *Eğitim Kurumları için Afet Acil Yardım Planlama Rehberi*, İstanbul Afet ve Acil Durum Müdürlüğü (ADM) ve İstanbul İl Özel İdaresi İPKB, İstanbul: Beyaz Gemi Eğitim ve Danışmanlık.

- 13- Kadiođlu, M, 2011. *Afet Yönetimi* T.C.:Marmara Belediyeler Birliđi Yayını, Yayın No: 65
- 14-Roberta Witty, Donna Scott, Disaster Recovery Plans and Systems Are Essential, 12 Eylül 2001, Gartner
- 15-Rood B., 2006 *Disaster Planning, the International Foundation of Employee Woodman, P., 2007 "Business Continuity Management"*, Chartered Management Institute, 2007
- 16-Bayođlu, B. (2010) İş sürekliliđi konusunda COBIT, ISO/IEC 27001/27002 ve ITIL ne der?
- 17-Demirci E, 2010. İ.T.Ü. Ayazađa Kampüsü İçin Örnek Acil Durum Yönetimi Planının Hazırlanması ve CBS Ortamına Aktarılması. *Yüksek Lisans Tezi*. İstanbul İ.T.Ü. FBE.
- 18-Dinçkan, A. (2008) *BGYS0009 İş Sürekliliđi Yönetim Sistemi Kurulumu, Ulusal Bilgi Güvenliđi Kapısı*, [internet].
- 19-Disaster Recovery Institute (drii), "*BCP901 Business Continuity Planning*" eğitim materyali EN Standartı
- 20-ISO/IEC 27002:2005 Information technology – Security techniques - Code of practice for information security management
- 21-<http://www.bilgiguvenligi.gov.tr/dokumanyukle/bgys/uekaebgys0009issurekliligiyonetimsistemikurulumkilavuzu/download.html>
- 22- <https://www.btk.gov.tr/kanunlar>, 5809 Elektronik Haberleşme Kanunu
- 23- <https://www.turkcell.com.tr/tr/hakkimizda/genel-bakis/is-surekliligi-politikasi> Turkcell İş sürekliliđi politikası
- 24-https://www.vodafone.com/content/dam/group/policy/downloads/VPC_Supplier_Policy_A6_Business_Continuity_V3.0.pdf Vodafone Business Continuity Management (BCM)

8. ÖZGEÇMİŞ

Adı Özcan

Soyadı Dimez

Doğum Yeri ve Tarihi Van /3 Nisan 1980

Eğitimi ;

2000-2004 19 Mayıs Üniversitesi Mühendislik Fakültesi Elektrik Elektronik Mühendisliği.

1996-2000 Van Fen Lisesi Fen bilimleri

Yabancı Dili İngilizce(İyi) Rusça(orta)

Üye Olduğu Bilimsel Kuruluşlar

Elektrik Mühendisleri Odası,

Bilimsel Etkinlikleri;

Rice University Finance for Non-Finance Professionals (Ağustos 2019)

Koç Üniversitesi Executive Mini MBA (Mayıs 2019)

Digital Business Transformation Turkcell Akademi Nisan (2018)

GSMA Mobile World Congress 2019 (Barcelona) Şubat (2019)

Broad Band World Forum 2017 (Berlin) Ekim (2017)