



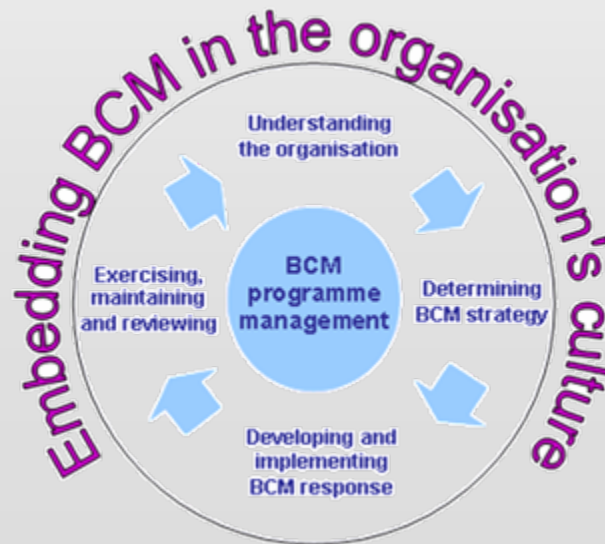
BS25999
İŞ SÜREKLİLİĞİ YÖNETİM SİSTEMİ
STANDARDI

Ali Dinçkan, CISA

dinckan@uekae.tubitak.gov.tr

6 HAZİRAN 2008

- İş Sürekliliği
 - Amacı
 - Niçin Endişelenmeliyiz
 - En Sık yapılan Hatalar
- İş Sürekliliği Kritik Başarı Faktörleri
- BS25999 – İş Sürekliliği Yönetim Sistemi



Tedarik zinciri

Operasyon

Üretim

Müşteriler



Altyapı

Binalar
Ekipmanlar
Bilgi Teknolojileri

Çalışanlar

Kayıtlar

Elektronik
Kağıt

Nakit Akışı

Tedarik zinciri

operasyon

Üretim

Müşteriler



Altyapı
Binalar
Ekipmanlar
Bilgi Teknolojileri

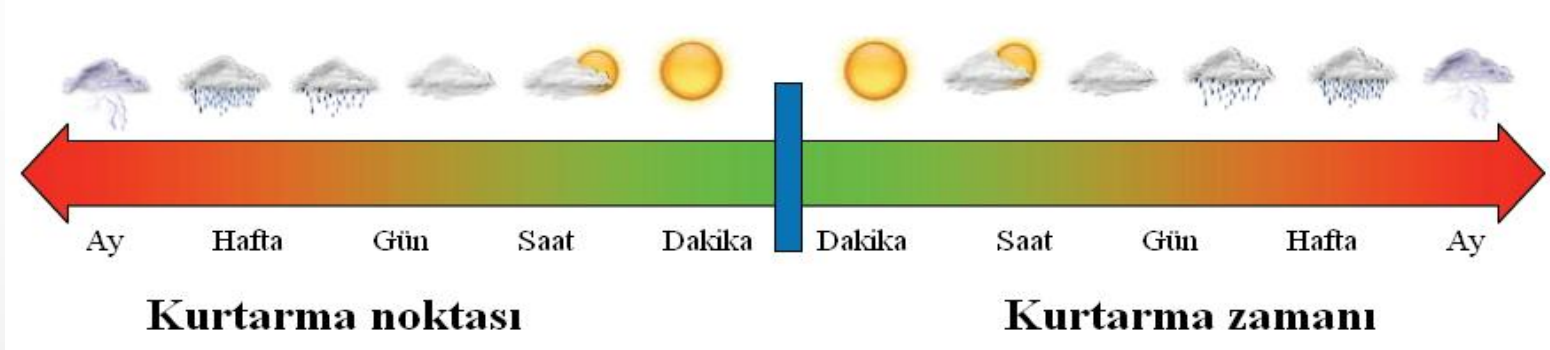
Çalışanlar

Kayıtlar
Elektronik
Kağıt

Nakit Akışı

- Kurumun kritik süreçlerinin devamlılığını sağlamak, sağlanamadığı durumlarda ön görülen sürelerde yeniden çalışır hale getirmek.
 - RTO (Kabul Edilebilir Kesinti Süresi)
 - RPO (Kabul Edilebilir Veri Kaybı)





- **RTO (Recovery Time Objective)**
 - Hedeflenen kurtarma zamanı
 - Kabul edilebilir kesinti süresi
 - Tanım: Kesintiye uğrayan iş sürecinin ne kadar süre sonra çalışır hale getirileceğine dair hedef süredir.
- **RPO (Recovery Point Objective)**
 - Kabul edilebilir veri kaybı
 - Tanım: İş sürecinin ne kadar veri kaybı ile eski haline getirileceğine dair hedef süredir.

NİÇİN ENDİŐELENMELİYİZ?

- Teknoloji bağımlılıđımız çok yüksek, kullandığımız veri miktarı sürekli artıyor,
- Yasal zorunluluklarımız var,
- İmzaladığımız servis seviyesi anlaşmaları (SLA) var,
- İş yapabilmek için bilgi sistemlerinin sürekli çalışmasına ihtiyacımız var,
- Kaybedilen her dakika
 - Zarar ediyoruz
 - Kurum prestijimiz zedeleniyor
 - Müşteri memnuniyet oranımız düşüyor
- Bilişim suçları her geçen gün artıyor
-



EN SIK YAPILAN HATALAR

- İş sürekliliğinin bir ürün, teknoloji veya servis olarak görülmesi,
- Başlangıcı ve sonu belirli olan bir proje olarak düşünülmesi,
- Sadece dokümantasyondan oluştuğu varsayımı.
- BT bölümünün işi olduğunun düşünülmesi.



- Üst Yönetim Desteği
- Stratejik İş Planının Parçası Olma
- İş Sürekliliği Koordinasyonu
- İş Etki Analizi
- Yeterli Bütçe Ayrılması
- Teknolojik Altyapı
- Plan dokümantasyonu
- Periyodik Testler
- Eğitim ve Bilgilendirme
- Plan güncelleme

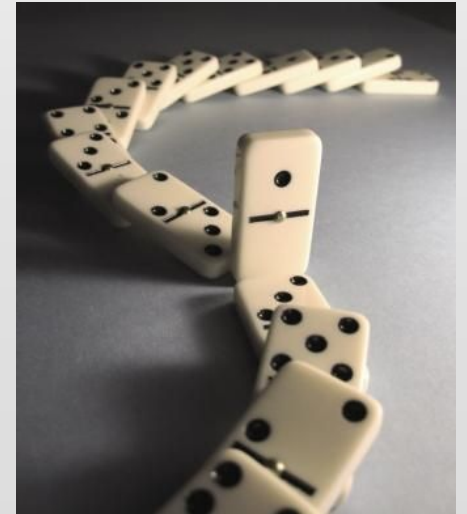


- ISO / IEC 27001
 - A.14 İş Sürekliliği Yönetimi
 - Ana 11 alandan bir tanesi
- COBIT
 - DS4 Servis Sürekliliğinin Sağlanması
- ITIL
 - Servis Tasarımı Altında Servis Sürekliliği Yönetimi
-

- İş Sürekliliği Yönetim Standardı
 - BS 25999-1:2006 Code of Practice for BCM
 - İş sürekliliği yönetimi uygulama esasları
 - BS 25999-2:2006 A Specification for BCM.
 - İş sürekliliği yönetimi denetim standardı
- Denetlenebilir
- Sertifikalandırılabilir



- İş sürekliliği politikasında tanımlanmış amaçların yerine getirilmesi
 - Sorumlulukların atanması
 - İş sürekliliğinin organizasyonda hayata geçirilmesi
 - İş sürekliliği planınının yaşatılması
 - Tatbikat
 - Güncelleme
 - Performansını izleme
 - İş sürekliliği dokümantasyonu



- İş etki analizi
 - Kritik aktivitelerin belirlenmesi
 - Süreklilik ihtiyaçlarının belirlenmesi
 - Kritik aktivitelere ait tehditlerin çıkarılması
 - Risk değerlendirmesi
- İş sürekliliği riskleri için seçeneklerin oluşturulması
- Üst yönetimin çalışmalara ait dokümanları onaylaması



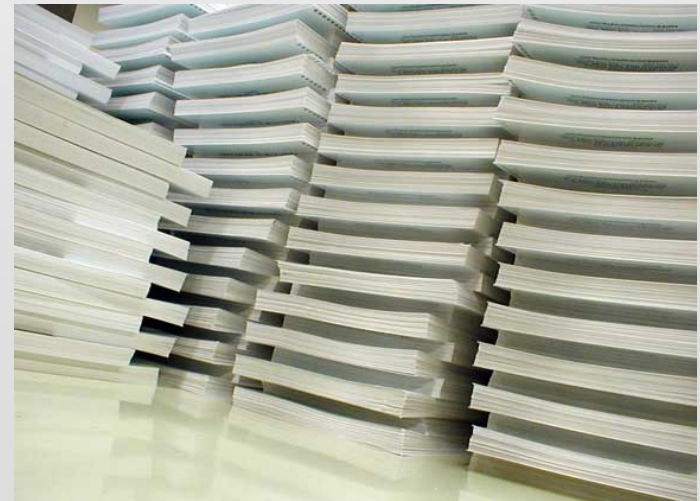
- Risklere önlem almak için hangi yöntem uygulanacak?
- Kriterler
 - Maksimum kabul edilebilir kesinti süresi
 - Stratejiyi uygulamanın maliyeti
 - Önlem almama konusunda fikir birliğine varma



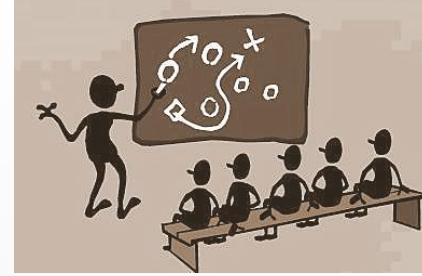
- Acil bir durum oluştuğunda ne yapılacak?
 - Kim? Ne? Nasıl? Sonuç?
- Tüm planlar
 - Olay yönetim planı, iş sürekliliği planı, iş kurtarma planları şunları içermelidir:
 - Amaç ve kapsam
 - Roller ve sorumluluklar
 - Planın aktivasyonu
 - Planın sahibi ve işleticileri
- Acil durum yönetim planı
 - İş ve aksiyon listesi
 - Acil durum iletişim listesi
 - Basın ile ilişkiler
 - Ortakları bilgilendirme



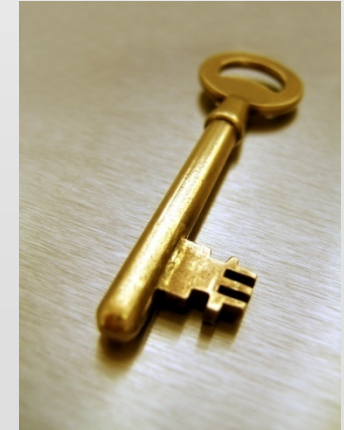
- İş Sürekliliği Planı
 - Aksiyon planları
 - İş listeleri
 - Kaynak ihtiyaçları
 - Sorumluluklar
 - Kullanılacak formlar ve iletişim listeleri



- Programın tatbikati
 - Dokümantasyon
 - Plan dokümanının üzerinden geçerek
 - Bir sürecin veya planın bir parçasının tatbikati
 - Planın tamamının uçtan uca tatbikati
- Kurum süreçlerinde gerçekleşecek değişiklikler planın güncellenmesini gerektirebilir !!!
- Plan her daim güncel ve erişilebilir tutulmalıdır
- Bağımsız denetim



- Bilinçlendirme faaliyetleri
 - Üst yönetime
 - Son kullanıcılara
 - İş ortaklarına
- Detay eğitim programları
 - İSY program yönetimi
 - İş etki analizi
 - Planın geliştirilmesi ve uygulanması
 - Risk yönetimi
 - İş sürekliliği tatbikatları



Teşekkürler Sorular?

Ali DİNÇKAN, CISA
dinckan@uekae.tubitak.gov.tr