

İŞ SÜREKLİLİĞİ YÖNETİM SİSTEMİ İÇİN KRİTİK BAŞARI FAKTÖRLERİ

Ali Dinçkan, BTYÖN Danışmanlık

İş sürekliliği, kurumun kritik süreçlerinin belirlenmesi, bu süreçlerin sürekliliği için gerekli çalışmaların gerçekleştirilmesi, sürekliliğin sağlanamadığı durumlarda kabul edilebilir kesinti süreleri içerisinde tekrar çalışır hale getirilmesi için gerçekleştirilecek tüm çalışmalara verilen genel isimdir.

İşletmenin iş süreçlerinin ne kadar kesintiye tahammül edebildiği ve süreçleri bu süre içerisinde tekrar çalışır hale getirmek için neler yapılması gerektiği iş sürekliliği çalışmalarının temelini oluşturmaktadır. İş sürekliliği Yönetim Sistemi (İSYS) gerekliliklerini tarif eden BS25999-2:2007 standardı iş sürekliliğini “iş süreçlerinin önceden tanımlanmış, kabul edilebilir bir düzeyde sürekliliğini/devamını sağlamak amacıyla, kuruluşun, olaylara ve iş kesintilerine karşı planlama ve müdahale etme konusundaki stratejik ve taktik kapasitesidir.” biçimde tanımlamaktadır.

Son yıllarda ülkemizde bilgi güvenliği bilincinin artması ve finans sektörüne getirilen düzenlemeler ile birlikte iş sürekliliğine verilen önemin arttığını görmekteyiz. Bu gelişmelere paralel olarak İngiliz Standartları Enstitüsü'nün (BSI) 2006 yılında BS 25999-1:2006 isimli İş Sürekliliği Yönetim Sistemi İçin Uygulama Prensipleri ve 2007 yılında BS 25999-2:2007 İş Sürekliliği Yönetim Sistemi İçin Gereklilikler standartlarını yayınlamış olması iş sürekliliğinin dünya genelinde de öneminin arttığını göstermektedir.

Günümüz işletmeleri genellikle iş süreçlerindeki kesintileri engellemek, rekabet avantajı sağlamak, yasal yükümlülüklerini yerine getirmek, müşteri kayıplarını engellemek, kurum itibarını korumak, pazar payı kayıplarını engellemek için iş sürekliliği ile ilgilenmektedir.

Bu yazıda İSYS'nin başarıya ulaşabilmesi için üzerinde önemle durulması gereken konular 10 ana başlık altında ele alınmıştır. Bu maddelerden bir veya birkaçında problem olması durumunda iş sürekliliği çalışmalarından beklenen faydanın sağlanamaması söz konudur.

1) Üst Yönetim Desteği

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

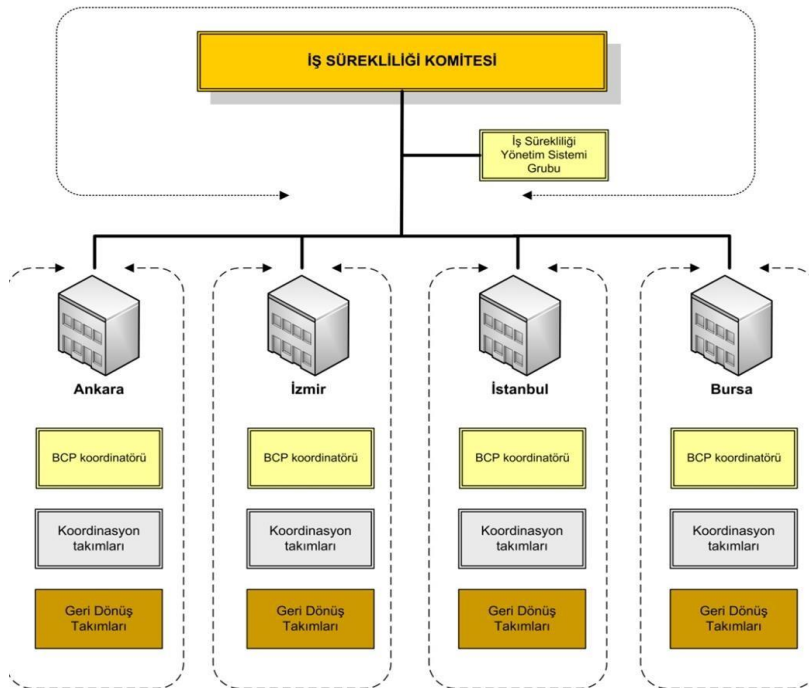
2) Stratejik İş Planın Parçası Olma

İş sürekliliği kurumun stratejik hedefleri için önemli bir çalışmadır. Kurumun işlevini devam ettirmesi veya yasal yükümlülüklerini yerine getirebilmesi için her zaman güncel ve ihtiyaca yanıt verebilir durumda olmalıdır. İş sürekliliğinin stratejik iş hedeflerine uygun olarak geliştirilmediği veya stratejik hedeflerde gerçekleştirilen değişikliklere uygun olarak gerekli çalışmaların yapılmadığı durumda iş süreçlerinde kesintiler yaşanması kaçınılmazdır. Örnek olarak bir yıl sonrasında satışlarını %30 arttırmayı hedefleyen bir firma düşünelim. Bu hedefi gerçekleştirmek için bilgi teknolojileri altyapısında da gerekli değişiklikler yapılacaktır. Bu değişiklikler sırasında iş sürekliliği planının ve ilgili dokümantasyonun, ayrıca felaketten kurtarma merkezinin bu hedefe uygun olarak değiştirilmesi gereklidir.

3) İş Sürekliliği Organizasyonu

İş sürekliliği çalışmaları bir grubun veya bir kişinin tek başına yerine getirebileceği bir faaliyet değildir. Kurumun birçok bölümünün içinde bulunduğu ve kişilerin farklı görevler aldığı bir çalışmadır. Son kullanıcının dahi bilmesi ve yapması gereken işler vardır. Bazı kurumlarda iş sürekliliği yönetimi için ayrı gruplar kurulmuştur. İş sürekliliği yönetim sisteminin kurum içinde yaşayabilmesi için gerekli personel gücünün ve koordinasyonun sağlanması, iş sürekliliğinin olağan üstü durumlarda beklenen faydayı sağlaması için kritik adımlardan birisidir. İş sürekliliği çalışmaları kapsamında en üst yönetimden son kullanıcıya kadar düşen görevler vardır. Bu detayda bir kurum kültürü oluşturulmadıkça sürecin işletilmesi mümkün değildir.

Aşağıda örnek bir iş sürekliliği organizasyonu verilmiştir. İş sürekliliği organizasyonunun kurumdan kuruma değişiklik gösterdiği ve kurumun iç işleyişine uygun bir organizasyon yapısının kurulması gerektiği unutulmamalıdır.



4) Risk Analizi ve İş Etki Analizi

İş sürekliliği Yönetim Sistemi, İş Etki Analizi (İEA) ismi verilen çalışmanın çıktıları üzerine inşa edilmelidir. İş etki analizinin doğru yapılması İSYS'nin sağlam temeller üzerine oturmasını sağlayacaktır. Bu sebeple kurumun ilgili bölümlerinden faaliyetlere hakim kişilerin çalışmalarda yer alması gereklidir. İş etki analizi / risk analizi takımında yer alacak personelin üst yönetim tarafından seçilmesi yönetimin konuya verdiği önemin anlaşılması açısından son derece önemlidir. Bu çalışma sonunda kurum süreçlerinin kritikliği, süreçler için hedeflenen kurtarma süreleri (RTO) ve maksimum kabul edilebilir kesinti süreleri (MTPoD) belirlenmektedir. Bu çalışma sırasında ayrıca risk analizi kullanılarak süreçlerde kesintiye neden olabilecek riskler belirlenmektedir. İş süreçlerinin öneminin ve süreçlerde kesintiye neden olabilecek olayların belirlenmesi uygulanacak karşı önlemlerin seçilmesi için son derece kritiktir. İş etki analizi ve risk analizi çalışmasının doğru yapılması iş sürekliliğinin başarıya ulaşmasında üst yönetim desteği kadar önemli bir başarı faktörüdür.

5) Yeterli Bütçe Ayrılması

İSYS'nin hem kurulumu hem de daha sonra işletimi sırasında bir takım giderleri vardır. Kurulması sırasında danışmanlık, eğitim ve benzeri hizmetlerin satın alınması, işletme içinde gerekli insan kaynağının sağlanması bu giderlere örnektir. Yönetim sisteminin kurulumu sonrasında ise gerçekleştirilecek tatbikatlar, periyodik gözden geçirmeler, kurum içi bilgilendirme faaliyetleri, süreçlerdeki değişikliklerden sonra hazırlanacak dokümanlar ve benzeri çalışmalar vardır. Ayrıca iş etki analizi ve risk analizi çalışmalarının sonunda uygulanacak kontrollere karar verilmektedir. 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.

6) Yeterli Bilgi Teknolojileri Altyapısı

Günümüzün iş gereklilikleri nedeni ile birçok iş sürecinin bilgi teknolojileri bağımlılığı yüksektir. Bilgi teknolojileri altyapısının süreklilik ihtiyaçlarına uygun olması, süreklilik ihtiyaçlarının karşılanması için büyük öneme sahiptir. Sunucuların, haberleşme hatlarının, enerji altyapısının yedekli yapıda çalışması bilgi teknolojileri altyapısının 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.

7) Dokümantasyon

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

İş Sürekliliği Yönetim Sistemi için hazırlanması gereken dokümanlara ait örnek liste aşağıda verilmiştir

İş sürekliliği politikası

İSYS kapsam dokümanı

İş sürekliliği rehberi

Uygulanabilirlik bildirgesi

İş sürekliliği planı veya planları

İş sürekliliği Olay yönetim / müdahale planı

İş kurtarma planları

İş etki analizi dokümantasyonu

İş sürekliliği risk değerlendirme dokümantasyonu

Yıllık tatbikat programı

Eğitim ve bilinçlendirme programı

Eğitim ve bilinçlendirme materyalleri

Acil durum haberleşme listesi

8) Periyodik tatbikatlar

Olağanüstü durumlara her an hazır olabilmek için senaryolar üretilmeli ve tatbikatı yapılmalıdır. Tatbikatlar sonucunda kurulmuş olan yönetim sisteminin eksikliklerini tespit etmek mümkündür. İş sürekliliği planının ve ilgili diğer dokümanların, çalışma kapsamında görev alan personelin bilgi seviyesinin, teknolojik altyapının varsa eksiklikleri bu şekilde tespit edilebilir. Tatbikatlar, dokümantasyonun gözden geçirilmesi, planın bir parçasının test edilmesi veya planın tamamının test edilmesi gibi farklı türlere sahiptir. Her bir tatbikat türü için senelik olarak tatbikat planlarının hazırlanması ve tatbikatların yapılması kurumun olası bir acil durum senaryosu için hazır olmasını sağlamaktadır. Tatbikat sonrası değerlendirme raporu hazırlanmalı ve iş sürekliliği olgunluk seviyesinin artırılması için gerekli adımlar belirlenmelidir.

9) Eğitim ve bilinçlendirme

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

10) Plan bakım ve güncelleme

İSYS kurumun kritik süreçlerinin devamlılığını sağlamak üzere vardır. Bu nedenle kurumun süreçlerinde meydana gelen değişiklikler iş sürekliliği planını doğrudan etkilemektedir. Süreç değişikliklerinin plan güncellemesi gerektirdiği hiçbir zaman göz ardı edilmemelidir. Zaman içerisinde meydana gelen değişikliklerin iş sürekliliği planına aktarılması için periyodik gözden geçirmeler yapılmalı ve güncelleme ihtiyacı tespit edilmelidir. Tatbikat sonuçları genellikle plan güncellemesi gerektirmektedir. İş sürekliliği kapsamında yapılması gereken değişiklikler her zaman doküman değişiklikleri olmak zorunda değildir. Kurumun süreçlerinin kritiklik seviyesinin değişmesi nedeni ile hizmet veren sunucuların öncelikleri dolayısıyla da alınması gereken önlemler değişebilir. Bu nedenle bazı durumlarda yeni yatırım gereksinimi ortaya çıkabilir. Sistem değişikliği olması durumunda bütçe ve zaman planının hazırlanması gerekir.

Yararlanılan Kaynaklar

- [1] BS 25999-1:2006 Code of practice for business continuity management
- [2] BS 25999-2:2007 Business continuity management — Part 2: Specification
- [3] Patrick Woodman, “Business Continuity Management”, Chartered Management Institute, 2007
- [4] Ali Dinçkan, UEKAE BGYS-0009 İş Sürekliliği Yönetim Sistemi Kurulum Kılavuzu, Ulusal Bilgi Güvenliği Kapısı