İŞ SÜREKLILIĞI KONUSUNDA COBIT, ISO/IEC 27001/27002 VE ITIL NE DER?

Burak Bayoğlu, BTYÖN Danışmanlık

Kurumların kritik iş süreçlerinin devamlılığını sağlamak ya da kesinti durumunda yeniden çalışır hale getirmek için gerçekleştirilen iş sürekliliği çalışmaları, İSYS(İş Sürekliliği Yönetim Sistemi) olarak adlandırılan süreçler bütünü çerçevesinde devam ettirilmelidir. İSYS kurulumu ve işletiminin, tek bir referans standart ya da çerçeve dokümanına uygun şekilde yapılması, ilerleyen zamanlarda yapılacak uyumluluk çalışmalarında ek yükler getirebilir. Bu sebeple, İSYS konusunda yönlendirme yapan dokümanların proje sürecince etkin kullanımı, hem İSYS olgunluğunu artıracaktır hem de kurum kaynaklarının daha etkin kullanılmasını sağlayacaktır. Bu yazıda, İSYS kurulumu ve işletimi konusunda kullanılabilecek standard, çerçeve, konsept vb. yönetim sistemleri dokümanların uyum içinde nasıl kullanılabileceği hakkında bilgi verilmiştir.

İSYS kurulum projeleri, kurumların iş hedefleri, iş ortaklarının gereksinimleri, yasal zorunluluklar vb. motivasyonlarla başlayabilmektedir. Kurumsal Yönetişim (Enterprise Governance) ve BT Yönetişimi (IT Governance) altyapısının sağlanmış olması, İSYS kurulumu ve işletimi sırasında büyük oranda ihtiyaç duyulacak üst yönetim desteği, BT ile diğer departmanlar arası koordinasyon ve İSYS'nin kurum iş süreçlerine entegrasyonu konularında büyük fayda sağlayacaktır. İş sürekliliği planlaması konusunda yol haritası çizen ya da yönlendirme yapan çok sayıda standart, çerçeve, kılavuz dokümanı vb. kaynak bulunmaktadır. Bu kaynaklardan aşağıda bahsedilenler, farklı amaç ve detay seviyelerinin yanında birbirlerini büyük oranda tamamlayan ve çok sayıda ortak nokta barındıran dokümanlardır.

"BS 25999-1:2006 İş Sürekliliği Yönetimi İçin Uygulama Esasları" isimli İngiliz Standardı, BSI tarafından 2006 yılında yayınlanmıştır. Bu standarda göre İSYS kuran kurumların denetimi için standardın ikinci parçası BS25999-2, 2007 yılında yayınlanmıştır. Bu yazıda, BS 25999-1:2006 standardına uygun şekilde İSYS kurulumu sırasında, yasal olarak ya da kurum hedefi olarak uyumluluk iddia edilebilecek ISO/IEC

27001, COBIT 4.1, ITIL vb. standart ve çerçevelerin ilgili kontrollerinin İSYS kurulum sürecine etkileri tartışılmıştır. Ayrıca İSYS kurulumunun bir "proje" olarak ele alınma zorunluluğu dolayısıyla; genel "Proje Yönetimi" konseptlerinin her zaman göz önünde bulundurulması gereklidir. Bunun yanında sonuçta ortaya koyulacak İSYS'nin başlangıcı ve bitişi olan bir proje değil yaşayan bir süreç olacağı da unutulmamalıdır.

İSYS SÜREÇLERİ

BS 25999-1:2006 standardına uygun şekilde İSYS kurulum aşamaları Tablo 1'de özetlenmiştir. Bu makalede, İSYS kurulum aşamalarının detaylandırılması değil BS25999 standardı haricindeki kaynakların etkileşiminin incelenmesi amaçlanmıştır. İSYS yaşam döngüsü ve kurulum aşamalarıyla ilgili daha detaylı bilgi için [1] ve [2] kaynaklarına başvurulabilir.

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

Tablo 1 – İSYS Kurulum Aşamaları

COBIT 4.1

COBIT; kullanıcılar, denetçiler ve daha önemlisi yönetim ve iş süreçleri sahiplerine hitap etmektedir. Dört temel etki alanı içerisinde (PO: Plan and Organise, AI: Acquire and Implement, DS: Deliver and Support, ME: Monitor and Evaluate), 34 üst seviye kontrol hedefiyle (high-level control objective), IT kaynaklarının/süreçlerinin etkin yönetimini sağlamayı amaçlayan bir çerçeve dokümanıdır. BT Yönetişiminin kurum içerisinde sağlanması ve BT stratejilerinin iş ihtiyaçlarını karşılayacak şekilde yönlendirilmesi, ana hedefleri içerisindedir. Sağlıklı bir İSYS için mutlaka gerekli olan BT Yönetişimi ve diğer destekleyici süreçler haricinde, bu bölümde COBIT çerçevesinin iş sürekliliği konusuna değinen DS4 – Ensure Continuous Service (Kesintisiz Hizmetin Garanti Edilmesi) kontrol hedefi (süreci) incelenmiştir.

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

DS4.1 IT Continuity Framework / BT Süreklilik Çerçevesi

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

DS4.2 IT Continuity Plans / BT Süreklilik Planları

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

DS4.3 Critical IT Resources / Kritik BT Kaynakları

BT kaynaklarının, kritik iş süreçleri için belirlenen öncelik seviyeleriyle uyumlu olarak kurtarılması planlanmalıdır. Daha az önemli BT kaynaklarının öncelikli olarak kurtarılması doğru değildir. İş sürekliliği ve kurtarma çalışmaları planlanırken kritik iş süreçleri için tahammül edilebilecek kesinti süresi, önceliklendirme, maliyetlerin kabul edilebilir seviyelerde tutulması, yasal yükümlülük ve sözleşmelere uyum göz önünde bulundurulmalıdır.

DS4.4 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.

DS4.5 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 kurtarılacağının garanti edilebilmesi için düzenli olarak testler gerçekleştirilmelidir.

DS4.6 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.

DS4.7 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.

DS4.8 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.

DS4.9 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.

DS4.10 Post-resumption Review / Kurtarma Sonrası Gözden Geçirme

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

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

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

Tablo 2 – DS4 süreci girdileri ve çıktıları

*GA: Girdi alır. *ÇV: Çıktı verir.

ISO/IEC 27001/27002

ISO/IEC 27002 standardı, "Bölüm 0.1 What is information security?/Bilgi güvenliği nedir?" bölümünde, bilgi güvenliğini, iş sürekliliğinin sağlanması, iş risklerinin en aza indirilmesi, yatırım geri dönüşünün ve iş fırsatlarının artırılması amacıyla bilginin her türlü tehdide karşı korunması olarak tanımlamıştır. Görüldüğü üzere iş sürekliliği çalışmaları, bilgi güvenliği yönetim sistemi kurulumunun temel amaçlarından birisi olarak belirtilmektedir. ISO/IEC 27001 standardının Ek-A'sında verilen onbir temel başlıktan biri iş sürekliliği yönetimidir.

ISO/IEC 27001 standardının "A.14 İş sürekliliği yönetimi" başlığı, "A.14.1 İş sürekliliği yönetiminin bilgi güvenliği hususları" isimli bir adet güvenlik kategorisi/kontrol hedefi içermektedir. İş faaliyetlerindeki kesilmeleri önlemek ve önemli iş süreçlerini büyük bilgi sistemleri başarısızlıklarından ya da felaketlerden korumak ve bunların zamanında devam etmesini sağlamak amacıyla tanımlanan A.14.1 kontrol hedefi altında beş adet kontrol tanıtılmıştır. Bu kontroller aşağıda listelenmiştir.

A.14.1.1 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.

A.14.1.2 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.

A.14.1.3 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.

A.14.1.4 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.

A.14.1.5 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. **(5.1.1)**
2. İş sürekliliği planlamasıyla ilgili rollerin ve sorumlulukların tanımlanması. **(6.1.3)**
3. İlgili otoritelerin bağlantı bilgilerinin bulundurulması. **(6.1.6)**
4. İş sürekliliği planlarının varlık envanterinin bir parçası olması. **(7.1.1)**
5. Yeni bilgi sistemleri kurulumu, yükseltmeler, yeni sürüm sistem kurulumu vb. için belirlenecek kabul kriterleri arasında iş sürekliliği anlaşmalarının göz önünde bulundurulması. **(10.3.2)**
6. Zararlı yazılım saldırıları sonrasında kurtarma amaçlı iş sürekliliği planlarının hazırlanması. **(10.4.1)**
7. İş sürekliliği planlarının gereksinimlerinin karşılanacağından emin olmak üzere sistem yedeklerinin düzenli olarak test edilmesi. **(10.5.1)**
8. Uzaktan çalışma ihtiyacı için iş sürekliliği planlamasının yapılması. **(11.7.2)**
9. Kaybolan ya da hasar gören kriptografik anahtarlarla ilgili iş sürekliliği planlamasının yapılması. **(12.3.2)**
10. Sistemlerde yapılan değişiklikler sonrasında iş sürekliliği planlarının da uygun şekilde güncellenmesi. **(12.5.2)**

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

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.

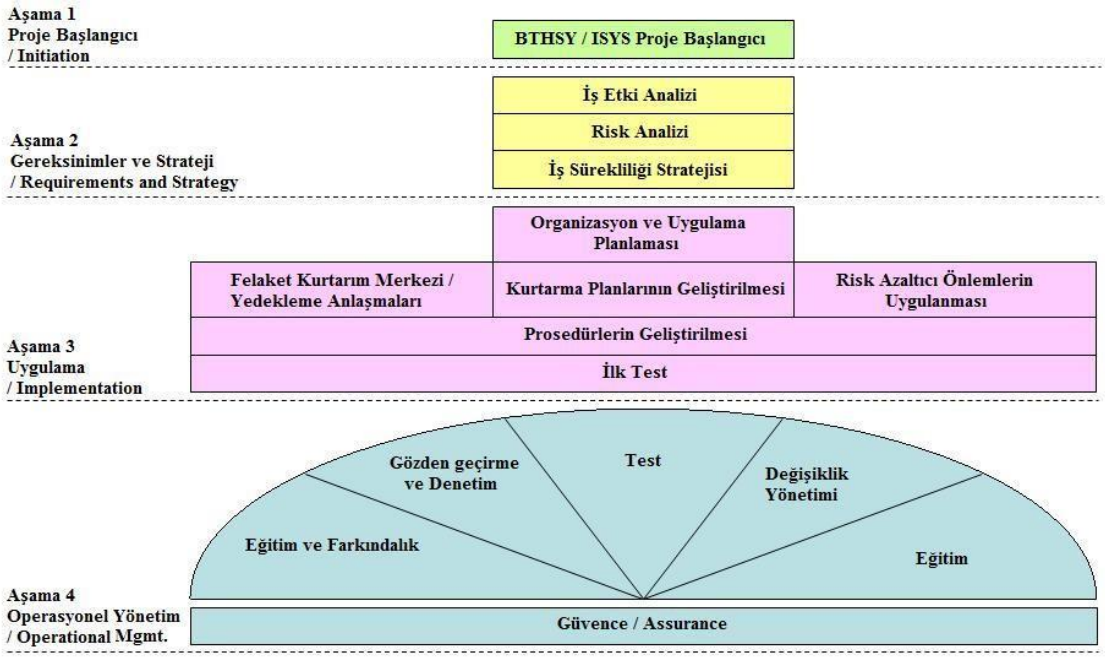
2. BT kaynaklarının iş süreçlerine olan etkisi ya da iş ihtiyaçlarındaki değişikliklerin planlara yansıtıldığından emin olmak üzere düzenli İş Etki Analizi(Business Impact Analysis) yapılması.

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 arttırıcı 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 düşünülmelidir. ITIL BTHSY, iş sürekliliği konusunda global kabul görmüş çerçeveye bağlı kalmakla birlikte daha genel bir İş Sürekliliği Yönetim Sistemi'ne ihtiyaç duymaktadır. İş Sürekliliği planlamasının kritik bir parçası olan BT hizmet/kaynak sürekliliğinin sağlanması için detaylı prosedürler tanımlanmıştır. BTHSY çalışmaları, İSYS sürecini destekler rol üstlenecektir. Genel İSYS kurulmadan yapılacak BTHSY çalışmalarında, yanlış varsayımlar yapılması, kullanılmayacak planların üretilmesi, kurum genelinde iş sürekliliği süreci sahibinin BT/IT departmanı olduğu, gereksiz teknoloji çözümlerinin üretilmesi gibi muhtemel sorunlara yol açacaktır.



Şekil 1 – ITIL BTHSY süreçleri

SONUÇ

İSYS kurulumuna rehberlik eden ya da İSYS kurulumunu değişik açılardan (bilgi güvenliği, BT hizmet sürekliliği, BT Yönetişimi vb.) destekleyen COBIT, ITIL, 27001/2 standard ve çerçeveleri İSYS bakış açısıyla incelenmiştir. İSYS yaşam döngüsünü tanımlayan BS25999 standardıyla uyumlu şekilde kullanılabilecek bu kaynaklar, farklı bakış açıları ve amaçları ile bu standardı destekleyip değinilmeyen bazı noktalarda eksikliklerini kapatmaktadır. Pazar payının artırılması vb. motivasyonlarla uyumluluk iddiaları gün geçtikçe artan ve yasal düzenlemelerle de zaman geçtikçe değişik sektörlerde zorunlu hale gelmesini beklediğimiz bu kaynakların İSYS çalışmalarında en baştan göz önünde bulundurulması, kurumlarda yersiz harcamaların yapılmasının önüne geçecektir. Kurum iş stratejileriyle hizalanmış bir BT stratejisi ve iş sürekliliği stratejisinin belirlenmesi, genellikle çalışmaları birbirinden bağımsız olarak başlatılan kalite yönetim sistemleri, BT yönetişim süreçleri, BGYS, İSYS gibi yönetim sistemlerinin birbirleriyle entegre şekilde tek bir yönetim sistemi çatısı altında uyumlu olarak çalışmasını 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.

REFERANSLAR

[1] BS 25999-1:2006 Standardı, Business continuity management – Part 1: Code of Practice

[2] Ali Dinçkan, BGYS-0009 İş Sürekliliği Yönetim Sistemi Kurulumu, Ulusal Bilgi Güvenliği Kapısı,http://www.bilgiguvenligi.gov.tr/dokuman-yukle/bgys/uekae-bgys-0009-is-surekliligi-yonetim-sistemi-kurulumkilavuzu/download.html

[3] ITIL v3, Service Design, Bölüm 4.5, Continual Service Improvement, Bölüm 5.6.3

[4] COBIT 4.1, IT Governance Institute

[5] ISO/IEC 27001:2005 Standardı

[6] ISO/IEC 27002:2005 Standardı