

İNTERNET HİZMETLERİ SUNAN KURUMLAR İÇİN YÖNETİM STANDARTLARI: ISO 20000 VE ISO 27001

Betül Ertem Yıldız

Karya Bilişim

betuly@karyabilisim.com

ÖZET

İnternet hizmetleri sunan kurumlar, iş gereksinimlerinin zorunlu gereği olarak, bilişim teknolojilerini etkin biçimde yönetmek zorundadırlar. ISO 20000 ve ISO 27001, bilişim teknolojilerinin “Yönetim Sistemi Yaklaşımı” ile ele alınmasını sağlayan iki standarttır. Bu sunumda, ISO 20000 ve ISO 27001’in yönetim sistemi olarak uygulanmasına ilişkin çok kısa bir özet sunulmuştur.

ABSTRACT

The organizations that provide Internet services need to effectively manage their IT due to the requirements of this business. ISO 20000 and ISO 27001 are two standards that handle IT tasks with a “Management Systems Approach”. This presentation is a brief summary of how ISO 20000 and ISO 27001 can be implemented as management systems

Anahtar Kelimeler: Bilişim Teknolojileri; Yönetim Sistemi; ITIL; Bilgi Güvenliği; ISO 27001; ISO 20000

1. GİRİŞ

İnternet hizmetleri sunan kurumların, kendilerine özgü bir takım iş gereksinimleri vardır. Sürekli ve başarılı internet hizmetleri sunabilmek için, aşağıda belirtilen maddelerle kısaca özetlenmiş olan zorunlulukları yerine getirebilmek gerekir:

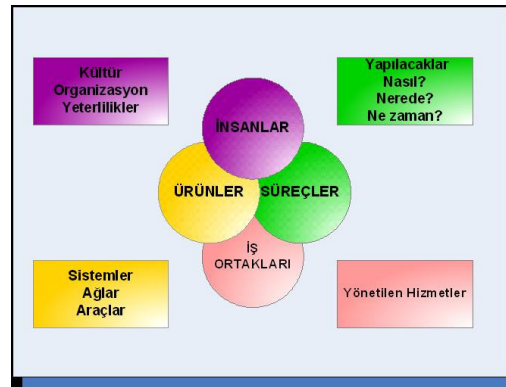
- İnternet hizmeti sunan bir kurumun, her hangi bir iş kolunda ulaşılmaması gereken sayıdan çok daha fazla sayıda müşteriye hizmet götürmesi gerekir.
- İnternet hizmetlerinin zaman sınırlaması yoktur. Günde 24 saat, haftada 7 gün sürekli hizmet sunmak zorundadır.
- Rekabet avantajı sağlayabilmek için sunulan hizmetin hızlı ve kaliteli olması şarttır.
- Tüm bu gereksinimleri karşılayabilmek için, çoğunlukla büyük ve karmaşık bilgi işlem sistemleri gerekir.
- Ancak bilişim ve dolayısıyla İnternet teknolojileri hızla değişmektedir. Kurulan sistemler ne kadar büyük

olursa olsun, esnek bir yapı oluşturmak, değişime uyum sağlayabilmek için kaçınılmazdır.

Tüm bunların sonucu olarak, bilişim teknolojisine (BT) yatırım yapmaksızın, İnternet hizmetleri sunulamaz, BT masraflarından kaçınılamaz. Dolayısıyla, başarılı İnternet hizmetlerinin sunulabilmesi için, başarılı bilgi işlem “**sistemlerinin**” kurulması ve yönetilebilmesi gerekir. Bilgi işlem sistemlerinin yönetilmesindeki başarı, iş başarısı olarak kuruma geri döner.

2. BÖLÜM 2

Bilgi işlemin bir masraf kalemi olarak değil, çok farklı bileşenlerden oluşan gerekli bir sistem olarak algılanması ve buna göre yönetim yaklaşımlarının oluşturulması İnternet hizmetleri sunan kurumlar için stratejik önem taşır. Çünkü söz konusu olan sistem sadece bilişim teknolojilerinin ürünlerinden oluşmaz. Bu ürünleri geliştirecek ve kullanacak olan “**insanlar**”, iş yapış şeklini belirleyecek olan “**süreçler**” ve bu hizmetlerden faydalanacak olan “**iş ortakları**”, sistem yaklaşımı içinde ele alınması ve yönetilmesi gereken bileşenlerdir.



Şekil 1. BT Bileşenleri.

İnsanlar, organizasyonun en önemli parçasıdır. Kurum kültürünün oluşmasında ve sürdürülmesinde, dolayısıyla iş yapış biçiminde etkin olan kişilerdir. Kişilerin teknik ve iş yeterliliklerinin izlenmesi ve geliştirilmesi gerekir.

Süreçler, işin ne zaman, nerede ve nasıl yapılacağını ifade eden işlem bilgileridir. Süreçlerin etkin biçimde tanımlanmış olması işin doğru ve her zaman, herkes

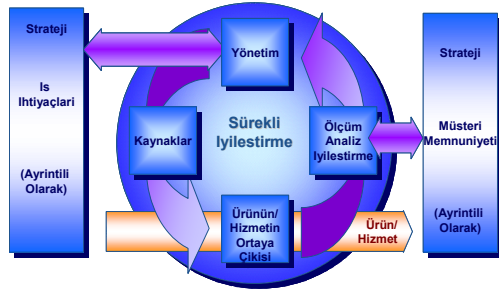
tarafından aynı biçimde yapılması için gereklidir. Ancak, bir diğer önemli konu da, süreçlerin iş ihtiyaçlarına göre sürekli olarak gözden geçirilerek iyileştirilmesi gerekliliğidir.

Ürünler, hizmetlerin geliştirildiği, test edildiği ve sunulduğu tüm platformları kapsar. Kullanılan bilgi işlem sistemleri, ağlar ve araçlar bu kategoride yer alır. Doğru ürünlerin seçilmesi ve bu ürünlerin sürekli bakımının ve güncelliğinin sağlanması gerekir.

Hizmetler, bu bileşenlerin bir araya gelmesi ile oluşturulan ve son kullanıcıya ulaştırılan bütün ürün ve servisleri içerir.

3. BÖLÜM 3

İş gereksinimleri ve bileşenleri bu denli karmaşık olduğu için, İnternet hizmetleri sunan kurumların kendini denetleyen, yenileyen ve değişime adapte edebilen bir “**yönetim sistemi**” yaklaşımını benimsemesi ve uygulaması başarısına büyük katkıda bulunacaktır. Toplam kalite yönetim sistemlerinde uygulanan “**PUKÖ**” (Planla, Uygula, Kontrol et, Önlem al) döngüsü, bu iş kolunda uygulanabilecek yaklaşımlardan bir tanesidir.



Şekil 2. PUKÖ Döngüsü

Bu yaklaşım, bir tarafta iş gereksinimleri, diğer tarafta müşteri memnuniyeti ile sınırlanmış olan bir işin sürekli iyileştirilerek yönetilmesi için geliştirilmiş bir yaşam döngüsüdür. Yönetim kadrosu, iş gereksinimlerine göre bir strateji belirler; gerekli kaynakları temin eder; hedeflenen ürün veya hizmetin geliştirilmesini sağlar; ve kullanıcıya/müşteriye sunar. Kullanıcıdan/müşteriden gelen geri bildirimler ile, yönetim yeni stratejiler geliştirir, kaynak ayırır, ürün ve hizmetlerini iyileştirerek kullanıcıya ulaştırır. Bu döngü, kendini sürekli iyileştirerek devam eder.

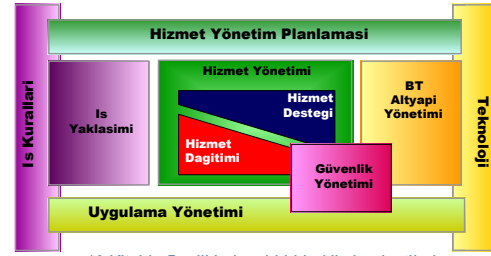
4. BÖLÜM 4

ISO/IEC 20000 - Bilgi Teknolojileri Hizmet Yönetimi”ve “ISO/IEC 27001 - Bilgi Güvenliği Yönetim Sistemleri”, PUKÖ yaşam döngüsüne göre tasarlanmış ve bilişim teknolojileri ile doğrudan ilintili iki standarttır.

ISO 20000, ITIL (IT Information Library) süreçlerini temel alır ve ITIL uygulamalarının belgelendirilmesi için kullanılan tek standarttır.

ITIL, BT hizmetlerini, yüksek, kaliteli, bütünlük bir sistem yönetimi için, işin ihtiyaçlarının tamamına ait bir parça olarak anlayan ve geliştiren kitaplardan oluşan bir kütüphanedir. Bu kitaplar başlıca, “Hizmet Desteği” ve “Hizmet Sunumu” olmak üzere iki ana kategori oluşturur. Kategorilerin alt başlıklarını tanımlayan kitaplar aşağıda belirtilmiştir:

- Hizmet desteği
 - Yardım Masası
 - Çağrı Yönetimi
 - Sorun Yönetimi
 - Konfigürasyon Yönetimi
 - Değişiklik Yönetimi
 - Sürüm Yönetimi
- Hizmet Dağıtımı
 - Kapasite Yönetimi
 - Erişilebilirlik Yönetimi
 - BT Hizmetlerinin Finansal Yönetimi
 - Hizmet Seviyesi Yönetimi
 - BT Hizmetlerinin Süreklilik Yönetimi



Şekil 3. ITIL

ISO 20000, merkezinde “Kontrol Süreçleri” olarak sınıflandırılan konfigürasyon yönetimi ve değişikliklik yönetimi olmak üzere, yukarıda belirtilen süreçleri ve bunlara ek olarak “Bilgi Güvenliği Yönetimi” süreçlerini kapsar.

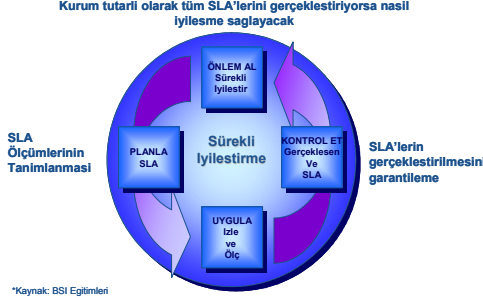


Şekil 4. ISO 20000

ISO 27001, bilgi güvenliği yönetimi için ISO 20000'in de referans olarak gösterdiği standarttır. Bilginin gizlilik, bütünlük, kullanılabilirlik özelliklerinin güvence altına alınmasını; yasalara, sözleşmelere, düzenlemelere ve iş gereksinimlerine

bağlı kalınmasını; kurumun tanımladığı bilgi güvenliği politikalarına ve süreçlerine uyulmasını sağlamak için kurulacak olan bir yönetim sisteminin özelliklerini ve kontrol noktalarını tanımlar.

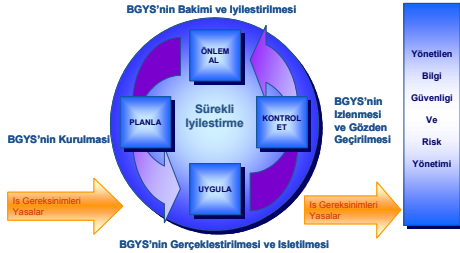
ISO 20000'in yönetim sistemi yaklaşımı PUKÖ döngüsünü şu şekilde kullanır:



Şekil 5. ISO 20000'in PUKÖ Döngüsü

- Planlama aşamasında, yapılan BT yatırımlarına göre sunulabilecek hizmet seviyesi anlaşmaları (SLA) ve bunların nasıl ölçüleceği tanımlanır.
- Uygulama aşamasında hizmet seviyeleri gerçekleştirilmeye çalışılır, izlenir ve ölçülür.
- Kontrol et aşamasında hizmet seviyelerinin ne oranda gerçekleştirildiklerine bakılır.
- Önem al aşamasında elde edilen ölçümlere göre BT yatırımları ve maliyetleri hesaplanarak, gerekirse hedeflerde değişiklik yapılır.

ISO 27001, aynı yaklaşımı Bilgi Güvenliği Yönetim Sistemlerinde (BGYS) kullanır.



Şekil 6. ISO 27001'in PUKÖ Döngüsü

- Planlama aşamasında, işin gereklerine ve yasalara göre gereksinimler belirlenir ve bunlara uygun risk analiz yöntemi ve BGYS'nin diğer ayrıntıları tasarlanır.
- Uygulama aşamasında, risk analizinde elde edilen sonuçlara göre standardın ön gördüğü kontrol maddeleri uygulanır.
- Kontrol et aşamasında BGYS gözden geçirilerek kontrollerin etkinliği ölçülür.
- Önem al aşamasında, belirlenen düzeltici ve önleyici faaliyetler belirlenir. Bu faaliyetler için gerekirse yeniden planlama başlatılır.

5. SONUÇLAR

Yönetim sistemleri yaklaşımından beklenen en büyük fayda, iyileştirme fırsatlarının belirlenebilmesi ve sürekli izleme ile verimlilik artışlarının ölçülebilmesidir. Bu yaklaşım, teknoloji odaklılıktan hizmet odaklı yönetim şekline geçiş anlamına gelir. Çünkü kurumun odaklandığı nokta, kullanılan teknoloji ne olursa olsun, tüm bileşenleri bir arada yönetebilmektir. Bunun başarılabilmesi durumunda sistemlerin güvenilir ve erişilebilir olması sağlanabilir.

Ayrıca, yönetim sistemleri yaklaşımı ile hizmet seviyesi ve bunun arka planında yer alan BT kalitesi sürekli izlenebilir. BT'nin gerçek maliyetleri ölçülebilir ve yönetilebilir.

İnternet hizmetleri saunan kurumlar için büyük önem taşıyan bu noktaların sonucu olarak, kurum içinde ve dışındaki kullanıcıların, müşterilerin ve paydaşların gereksinimlerinin tam olarak karşılanması, etkinlik ve verimliliğin sürekli olması beklenir.

KAYNAKLAR

ISO 20000 ve ISO 27001: www.bsi-global.com; www.iso.org

ITIL: www.itsmf.org

"Aligning COBIT®, ITIL® and ISO 17799 for Business Benefit" :

<http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=22493&TEMPLATE=/ContentManagement/ContentDisplay.cfm>