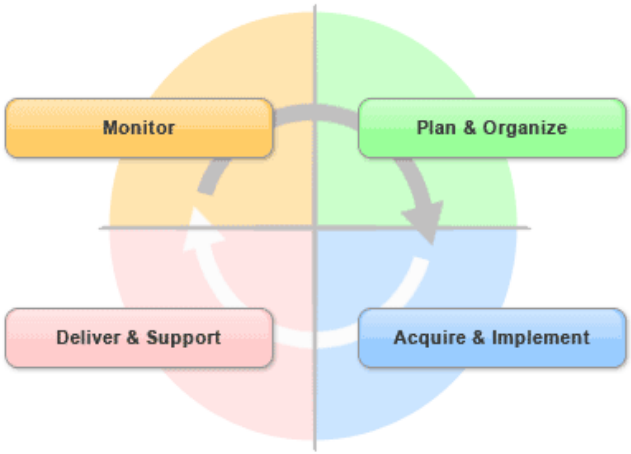
COBIT



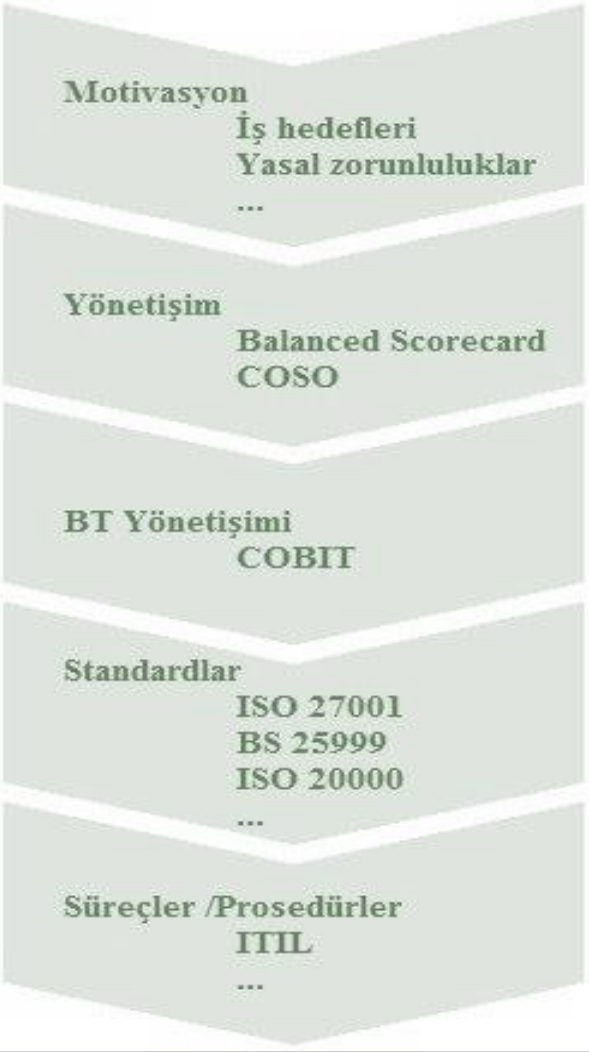
Bilgi Teknolojilerinde Kontrol

Dr.Yüksel YurtaY

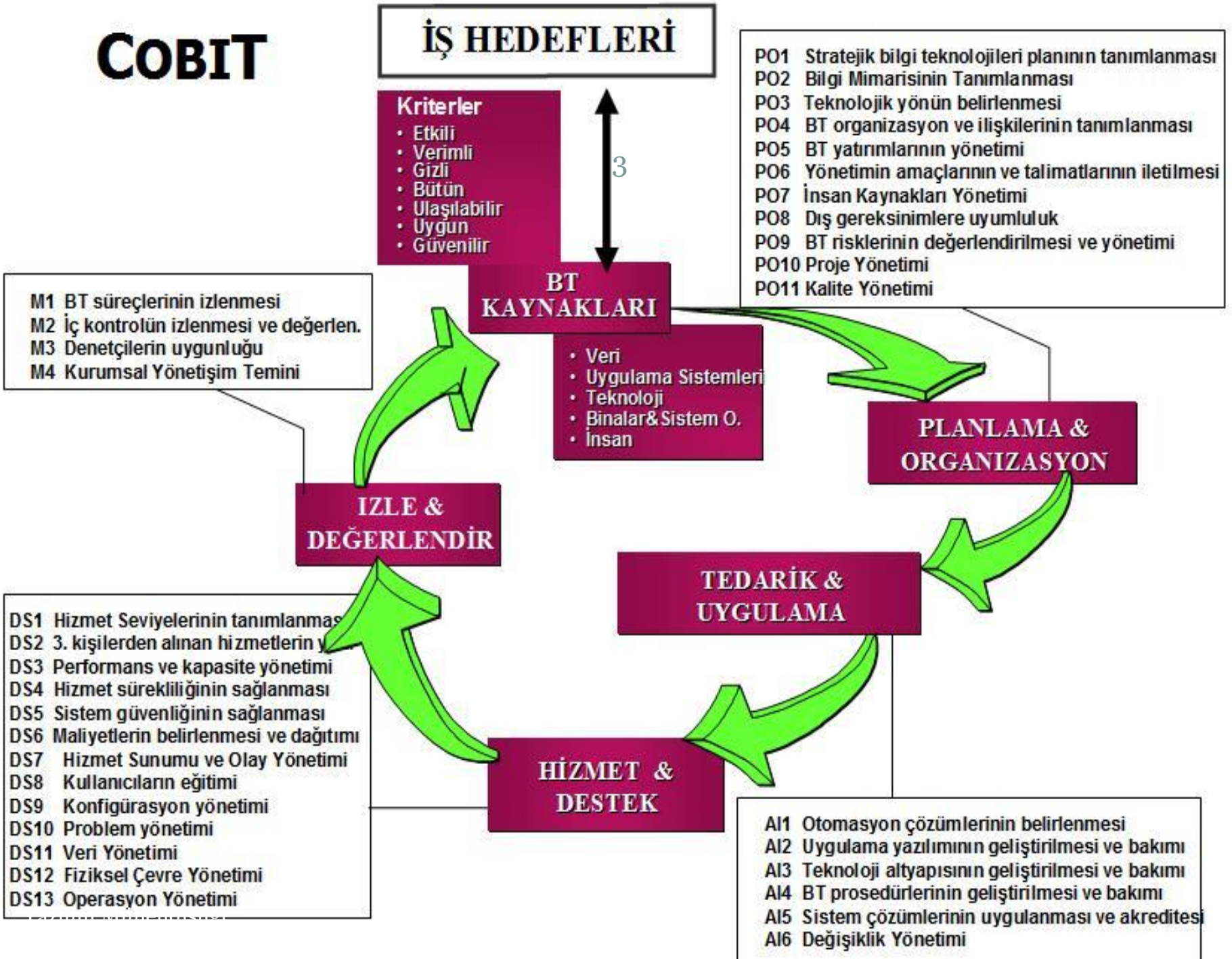
CobiT nedir?

- Tanım olarak CobiT, “Control Objectives for Information and Related Technology” nin kısaltılmış halidir.

- “Bilgi ve ilgili teknolojiler için kontrol hedefleri”. Bu tanım, CobiT’in amacını ifade etmesi açısından önemlidir. CobiT, Bilgi Teknolojileri yönetiminde ulaşılması gereken **hedefleri** ortaya koymaktadır.



COBIT


İŞ HEDEFLERİ
Kriterler
• Etkili
• Verimli
• Gizli
• Bütün
• Ulaşılabilir
• Uygun
• Güvenilir
3
PO1 Stratejik bilgi teknolojileri planının tanımlanması
PO2 Bilgi Mimarisinin Tanımlanması
PO3 Teknolojik yönün belirlenmesi
PO4 BT organizasyon ve ilişkilerinin tanımlanması
PO5 BT yatırımlarının yönetimi
PO6 Yönetimin amaçlarının ve talimatlarının iletilmesi
PO7 İnsan Kaynakları Yönetimi
PO8 Dış gereksinimlere uyumluluk
PO9 BT risklerinin değerlendirilmesi ve yönetimi
PO10 Proje Yönetimi
PO11 Kalite Yönetimi
BT KAYNAKLARI
• Veri
• Uygulama Sistemleri
• Teknoloji
• Binalar&Sistem O.
• İnsan
M1 BT süreçlerinin izlenmesi
M2 İç kontrolün izlenmesi ve değerlen.
M3 Denetçilerin uygunluğu
M4 Kurumsal Yönetişim Temini
PLANLAMA & ORGANIZASYON
TEDARİK & UYGULAMA
HİZMET & DESTEK
IZLE & DEĞERLENDİR
DS1 Hizmet Seviyelerinin tanımlanmas
DS2 3. kişilerden alınan hizmetlerin y
DS3 Performans ve kapasite yönetimi
DS4 Hizmet sürekliliğinin sağlanması
DS5 Sistem güvenliğinin sağlanması
DS6 Maliyetlerin belirlenmesi ve dağıtımı
DS7 Hizmet Sunumu ve Olay Yönetimi
DS8 Kullanıcıların eğitimi
DS9 Konfigürasyon yönetimi
DS10 Problem yönetimi
DS11 Veri Yönetimi
DS12 Fiziksel Çevre Yönetimi
DS13 Operasyon Yönetimi
AI1 Otomasyon çözümlerinin belirlenmesi
AI2 Uygulama yazılımının geliştirilmesi ve bakımı
AI3 Teknoloji altyapısının geliştirilmesi ve bakımı
AI4 BT prosedürlerinin geliştirilmesi ve bakımı
AI5 Sistem çözümlerinin uygulanması ve akreditesi
AI6 Değişiklik Yönetimi

Benzer standartlardan farkı nedir?

CobiT'i, **ITIL, CMMI** ve **ISO** standartlarından ayıran en büyük özelliği tüm BT fonksiyonlarını kapsayan bir çerçeve sunmasıdır.

Farklı şekilde ifade etmek gerekirse CobiT içerisinde yer alan 34 süreci bir arada değerlendirdiğinizde BT yönetiminin her alanını kapsama almış olursunuz.

Bu nedenle diğer standartlardan farklı şekilde, CobiT'in tek veya grup halinde BT süreçlerine değil BT'nin yönetilmesine odaklandığını söylemek doğru olur.

Benzer standartlardan farkı nedir?

CobiT'in diğer bir özelliği de, içerisindeki süreçlerin nasıl uygulanması gerektiğine dair detaylı çözüm yöntemleri içermemesidir.

Esas olarak kontrol hedeflerinden oluşmaktadır ve bu hedefler o süreç içerisinde sağlanması gereken en iyi uygulamaları açıklamaktadır.

Fakat birkaç istisna dışında bu süreçlerin hiçbiri için kontrol hedeflerine ulaşılmasını sağlayacak bir yöntem, şablon veya tasarım önermemektedir

Öne çıkan özellikleri

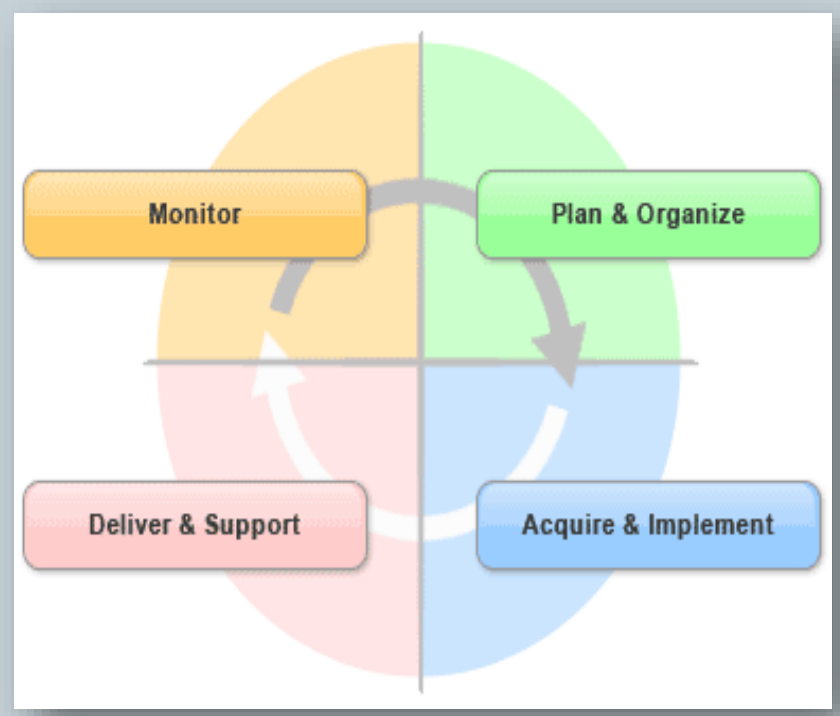
CobiT aşağıdaki genel özellikleri gösterir:

- Bilgi Teknolojileri'nin şirketin iş (ticari) amaçlarına hizmet etmesi gerektiğini benimser,
- BT stratejisi ile iş stratejisinin uyumunu sağlamaya çalışır,
- Bu özellikleriyle modern BT Yönetiminin kabul görmüş kurallarını içerir,
- İçerisindeki 34 süreç ile neredeyse tüm BT fonksiyonlarını kapsar,
- Diğer BT yönetimi standartları ile (ISO, ITIL, CMMI, MOF, vb) uyumludur,
- Her sektörden ve her boyuttaki şirket tarafından kullanılabilir,
- Denetim, süreç iyileştirme, süreç yönetimi, ölçüm, karşılaştırma vb farklı kullanım amaçları vardır.

CobiT süreçleri

CobiT içerisinde 4 ana başlık altında toplam 34 süreç bulunmaktadır.

Bu 34 süreç, pek çok şirket için BT fonksiyonlarının hemen hepsini kapsar.



1. Planlama ve Organizasyon

- PO 1 Stratejik BT planının tanımlanması
- PO 2 Bilgi mimarisinin tanımlanması
- PO 3 Teknolojik yönün belirlenmesi
- PO 4 BT süreçlerinin organizasyonunun ve ilişkilerinin tanımlanması
- PO 5 BT yatırımlarının yönetimi
- PO 6 Yönetimin amaçlarının iletilmesi
- PO 7 BT İnsan kaynakları yönetimi
- PO 8 BT Kalite yönetimi
- PO 9 BT riskinin değerlendirilmesi ve yönetimi
- PO 10 Proje yönetimi

2.Edinim ve Kurulum

- AI 1 Çözümlerin belirlenmesi
- AI 2 Uygulama yazılımının geliştirilmesi ve bakımı
- AI 3 Teknoloji alt yapısının oluşturulması ve bakımı
- AI 4 Operasyon ve kullanımın sağlanması
- AI 5 BT kaynaklarının satın alınması
- AI 6 Değişiklik yönetimi
- AI 7 Çözümlerin ve değişikliklerin uygulanması ve akredite edilmesi

3.Hizmet ve Destek

- DS 1 Hizmet seviyelerinin tanımlanması ve yönetimi
- DS 2 Üçüncü kişilerden alınan hizmetlerin yönetimi
- DS 3 Performans ve kapasite yönetimi
- DS 4 Hizmet sürekliliğinin sağlanması
- DS 5 Sistem güvenliğinin sağlanması
- DS 6 Maliyetlerin belirlenmesi ve dağıtılması
- DS 7 Kullanıcıların eğitimi
- DS 8 Hizmet sunumu yönetimi ve olay yönetimi
- DS 9 Konfigürasyon yönetimi
- DS 10 Problem yönetimi
- DS 11 Veri yönetimi
- DS 12 Fiziksel çevre yönetimi
- DS 13 Operasyon yönetimi

4. İzleme ve Değerlendirme

- ME 1 Bilgi sistemleri performansının izlenmesi ve değerlendirilmesi
- ME 2 İç kontrolün izlenmesi ve değerlendirilmesi
- ME 3 Mevzuata uyumun sağlanması
- ME 4 Bilgi sistemlerine ilişkin kurumsal yönetişimin temini

Sürecin tanımı :

Süreç tanımı, her CobiT sürecinin ilk sayfasında bulunur ve sürecin genel hatlarını belirler. İçerisinde şu bilgiler bulunur:

İlgili süreç hedefleri :

- Etkinlik
- Verimlilik
- Gizlilik
- Bütünlük
- Erişilebilirlik
- Uyum
- Güvenilirlik

· Sürecin amacı
· Sürecin, iş süreçleri açısından önemi
· Odaklanılan konular
· İçerisindeki temel faaliyetler
· Başarı göstergeleri
· İlgili BT yönetişi alanları

- Stratejik uyum
- Değer üretimi
- Risk yönetimi
- Performans ölçümü
- Kaynak yönetimi
  · İlgili BT unsurları
- Uygulama
- Bilgi
- Altyapı
- İnsan

Sürecin tanımı :

Süreç tanımı, **CobiT**'in en çok kullanılan ve en faydalı alanlarından birisidir.

Kullanımına örnek olarak her iş yerinde bulunan bir süreci ele alalım: "Performans ve kapasite yönetimi". Elbette sistemlerimizin performans ve kapasitesini yönetiyoruz, peki şu soruların yanıtlarını verebiliyor muyuz?

- Kapasite ve performans yönetimi ne demektir?
- Biz bu süreci daha iyi işletince şirketin ticari faaliyetleri bundan nasıl yarar sağlamaktadır?
- Sürecin ana adımları nelerdir?
- Süreçte nelere odaklanılmalıdır?
- Performans ve kapasite yönetimini ne kadar iyi yaptığımızı nasıl ölçebiliriz?

Detaylı kontrol hedefleri :

Detaylı kontrol hedeflerinde sürecin işletilmesi ile ulaşılması gerekli hedefler yani iyi uygulamalar bulunmaktadır. Detaylı kontrol hedefleri, her süreç için farklı şekilde kategorilere göre ayrılmıştır.

Bu bölüm ayrıca, CobiT esaslı denetimlerde uyulması gerekli bir kriter listesi olarak kullanılır. Benzer şekilde CobiT uyumluluğunun sağlanması amacıyla gerçekleştirilen süreç iyileştirme çalışmalarının da dayanak noktası detaylı kontrol hedefleridir.

Sürecin tanımı :

Örnek olarak “DS3 Performans ve Kapasite Yönetimi” süreci üzerinden ilerlemek istersek, içerisinde şu kategoriler altında, ulaşılması gerekli hedefler bulunmaktadır:

- DS3.1 Performans ve kapasite planlaması
- DS3.2 Mevcut kapasite ve performans
- DS3.3 Gelecekteki kapasite ve performans
- DS3.4 BT kaynaklarının erişilebilirliği
- DS3.5 İzleme ve raporlama

Yönetim kılavuzları:

· Süreç girdileri ve çıktıları: Sürece girdi olabilecek bilgiler, dokümanlar veya diğer faaliyet sonuçları ile bu sürecin sonunda diğer süreçlere girdi olacak unsurlar.

· Süreçteki roller ve sorumluluklar (RACI tablosu): Her bir süreçle ilgili öne çıkan faaliyetler ve bu faaliyetlerin gerçekleştirilmesi sırasında işletimden sorumlu, hesap vermekten sorumlu, danışılan ve bilgi verilen organizasyonel roller.

· Süreç hedefleri ve ölçüm kriterleri: Sürecin hangi şartlar gerçekleştiğinde başarılı sayılacağı ve sürecin ne kadar iyi işletildiğinin nasıl ölçülebileceği.

Olgunluk modeli :

CobiT, ayrıca her bir sürecin ne kadar olgun şekilde yönetildiğinin belirlenebilmesi ve benzer şirketlerle karşılaştırılabilmesi için bir olgunluk modeli sunmaktadır. Olgunluk modeli 0 ile 5 arasında 6 lı bir skala içermektedir ve her bir seviyeye ulaşılması için sağlanması gerekli kriterler, her bir sürece özel olarak detaylı şekilde belirtilmiştir.

Olgunluk modelinde seviyeler :

0. Tanımlanmamış

Süreç konusunda şirket bünyesinde herhangi bir bilinç bulunmamaktadır. Yönetim sürecin varlığından/gerekliliğinden haberdar değildir.

1. Düzensiz

Sürecin gerekliliği bilinmektedir ancak düzenli şekilde uygulanmamaktadır

2. Tekrarlanabilir

Süreç tekrarlanabilir şekilde uygulanmaktadır ancak sürecin kriterleri ve uygulama esasları tanımlanmamıştır

3. Tanımlı

Süreç tanımlanmıştır ve tanımlandığı şekilde işletilmektedir

4. Ölçülebilir

Sürecin ne kadar iyi işletildiği ölçülmektedir

5. Optimize edilmiş

Süreç, sürekli olarak iyileştirilmektedir

Bilgi Teknolojileri süreç eşleştirme tabloları :

CobiT içerisinde ayrıca, iş hedeflerinin bilgi teknolojileri hedefleri ile bağlantılarının kurulabilmesi amacıyla kılavuz olabilecek üç farklı tablo sunulmaktadır.

i) İlk tabloda iş hedefleri, bilgi teknolojileri hedefleri ve CobiT bilgi kriterleri ile eşleştirilmiştir. Bu tablo kullanılarak, örnek iş hedefleri için, bu hedefleri destekleyen bilgi teknolojiler hedefleri ve ilgili CobiT bilgi kriterleri görülebilir.

ii) İkinci tablo, CobiT içerisindeki BT süreçleri ile genel BT hedefleri ve bilgi kriterlerinin eşleştirilmesini içerir.

iii) Üçüncü tabloda ise her bir BT süreci için desteklenen BT hedefleri tersten gösterilmiştir.

Kullanım Alanları ve Denetim :

Kullanım alanları

CobiT pek çok farklı amaçlar için kullanılabilir. Günümüzde en yaygın görünen kullanım amaçları şunlardır:

Denetim: CobiT, içerisinde karşılaştırma yapılabilecek iyi uygulamaları barındırması nedeniyle bir denetim aracı olarak kullanılabilir. Ayrıca, BT süreçlerinin listelenmesi sayesinde denetim kapsamının belirlenmesinde kolaylık sağlamaktadır.

Bu özellikleriyle, birden fazla denetçi tarafından farklı şirketlerde yapılan denetimlerin kapsamlarının ve uyum kriterlerinin aynı şekilde değerlendirilebilmesini sağlar.

BT Süreç yönetimi:

CobiT'in hemen hemen tüm BT fonksiyonlarını içeren bir çerçeve sunduğundan bahsetmiştik. Bu çerçeve sayesinde BT yöneticileri aşağıdaki soruların yanıtlarını CobiT'te bulabilir:

- Hangi süreçleri oluşturmalıyım?
- Bu süreçlerde hangi adımlara yer vermeliyim?
- Rol ve sorumlulukları nasıl dağıtmalıyım?
- Bu süreçleri ne kadar iyi uyguladığımı nasıl ölçebilirim?

Uygulamalar :

İyi uygulamalar: CobiT, detaylı kontrol hedefleri sayesinde, her bir BT süreci için dünyada kabul görmüş en iyi uygulamaları da içermektedir. İyi uygulamalar, süreçte bulunması gerekli faaliyetleri, sorumlulukları, oluşturulması gereken rolleri, süreçlerin işlem sıralarını, süreçlerde kullanılması gereken girdileri ve oluşturulması gereken çıktıları ve buna benzer bilgileri içerir. Ek olarak, "CobiT control practices" dokümanında daha detaylı örnek alınabilecek kontrol tanımları bulunmaktadır.

Karşılaştırma aracı: İçerisindeki olgunluk modeli ile her bir BT sürecinin ne kadar olgun işletildiğinin belirlenmesi ve benzer şirketler ile karşılaştırılmasına da imkân vermektedir.

Türkiye'de CobiT :

Türkiye'de CobiT'in kamuoyuna ilk yansıması BDDK'nın, bazı bankaları CobiT esaslı bir özel denetime tabi tutmasıyla gerçekleşti. Benzer bir çalışmanın 2006 yılında tüm bankalara genişletilerek zorunlu tutulması ve her iki yılda bir kez tekrar edilmesi sonucunda tüm bankalar CobiT ile tanışmış oldu. Başlangıçta yaşanan zorlukların ardından, bugün bakıldığında bankalar BT süreçlerini bir standarda uygun olarak yürütmenin meyvelerini daha kontrollü, verimli ve etkin bir BT şeklinde toplamaktalar.

BDDK'nın denetim şartının çok öncesinde BT süreçlerini CobiT'e uygun şekilde yöneten bankalar bulunmaktaydı. Fakat bankacılık CobiT'in görülebildiği tek yer değil elbette. Bankalara ek olarak, finans ve üretim sektörlerinde "olgun" sayılabilecek pek çok şirkette CobiT'i süreç yönetimi için kullanmakta. Bu konuda hem şirketlerdeki bilinç hem de bankacılık dışındaki sektörlere yönelik düzenlemeler de hızla gelişiyor.

CobiT'in geleceği:

CobiT'in şu andaki en son versiyonu CobiT 4.1'dir. Ancak, yaklaşık iki yıl önce başlayan çalışmalar sonucunda 5.0 versiyonunun yayınlanmasına çok yaklaşılmıştır. 2011 yılında yayınlanması beklenen yeni versiyon ile ISACA tarafından yayınlanan Risk IT ve Val IT'nin CobiT içerisinde birleştirilmesi, CobiT sertifikasyonunun mümkün hale getirilmesi gibi pek çok yenilik bekleniyor.

Türkiye'de ise her geçen gün farklı sektörlerdeki pek çok şirkette CobiT'in kullanıldığına şahit oluyoruz. Yasal düzenlemeler tarafında ise BDDK'nın yanı sıra Hazine Müsteşarlığı ve SPK'nın da gelişmeleri izlediği ve BT'ye yönelik düzenlemelerinde CobiT'i göz önünde bulundurduğu bilinen konular.

SONUÇ :

Sonuç olarak,

CobiT tüm dünyada olduğu gibi Türkiye'de de her geçen gün daha fazla şirket tarafından tanınıyor ve uygulanıyor.

CobiT'in diğer standartlar ile uyumu, gözle görülebilen faydaları ve kendine özgü yaklaşımı ile bu gelişmelerin hız kesmeden devam edeceğini gösteriyor.

Kaynak :

Cozumpark.com, İ.TUTU, Ç.ISIKÇI