Bilgi Teknolojileri Yönetişimi İçin Yeni Bir Adım: **COBIT 5**

Bankacılık sektörü başta olmak üzere hemen hemen tüm alanlarda işletmelerin bilgi teknolojilerine bağımlılığı giderek artmaktadır. Bilgi Teknolojileri odaklı işletme yatırımlarından gereken faydayı sağlayabilmek için iş ve BT uyumuna olan ihtiyaç her zamankinden daha kritik bir noktaya gelmiş durumda. Bunun sonucu olarak, BT yönetişimini kurumsal yönetişimden ayırmak artık neredeyse imkânsız hale gelmeye başladı. Böyle bir ortamda yeni ihtiyaçlara cevap vermek amacıyla ortaya çıkan COBIT 5, BT yönetişimine yepyeni bir yaklaşım getirmektedir.

Bilgi Teknolojileri yönetişiminde ulaşılması gereken hedefleri ortaya koymak üzere oluşturulan bir çerçeve olan COBIT'in (Control Objectives for Information and Related Technology) ilk sürümü 1996 yılında yayımlandı. COBIT 1'in kapsamı temel olarak, denetim ile sınırlı idi. Her yeni versiyon ile COBIT'in kapsamı farklı kavramlarla genişledi. 1998'de yayımlanan COBIT 2 "kontrol" kavramını ortaya çıkarttı. Ancak, COBIT bu aşamada halen bir BT denetim ve kontrol çerçevesi idi. 2000 yılında yayımlanan COBIT 3 ile birlikte, "yönetim" çerçeve kapsamı içine girdi ve COBIT, BT yönetim çerçevesi haline geldi. 2005 yılında yayımlanan COBIT 4 ve 2007 yılında yayımlanan COBIT 4.1 ile birlikte, artık "BT yönetişimi" kavramı çerçeve kapsamına alınıyordu. Serinin son ürünü olan COBIT 5 ise "kurumsal BT yönetişimi" kavramını öne çıkarıyor.

Bankacılık sektöründe, BT denetimi konusunda düzenleyici kuruluş BDDK'dır. BDDK'nın da desteklemesi sonucu, Türk bankacılık sektörü uzun bir zamandır COBIT çerçevesini yakından takip etmekte ve uyumlu hale gelmeye çalışmaktadır. BDDK'nın düzenleme ve çalışmalarının, Türk bankacılık sektöründe bilgi teknolojilerinin iş faaliyetlerini desteklemesi, bilgi güvenliği ve süreklilik konularında önemli katkılar sağladığı aşikârdır. Bankalar özellikle bu çalışmaların yürütülmeye başladığı 2006'dan bu yana BT yönetişimine ilişkin büyük yatırımlar yapmışlardır.

Şimdi ise, COBIT 5 ile BT yönetişiminde yeni bir sayfa açılmaktadır.
Haziran 2012'de yayımlanan COBIT 5'te en temel yenilik; yönetim ve yönetişim kavramlarının birbirinden ayrılarak farklı süreçler halinde ele alınmasıdır. Yeni süreç modelinde kurumsal yönetişim ve BT yönetişimini entegre bir şekilde ele almayı sağlayan yeni bir süreç modeli ortaya konulmaktadır. Bu bağlamda COBIT 5 "yönetişim" ve "yönetim" terimlerine aşağıdaki şekilde bir bakış getiriyor:

• Yönetişim, işletme hedeflerinin belirlenmesinde paydaşların ihtiyaçlarının, durumlarının ve tercih haklarının değerlendirilmesini sağlar; önceliklendirme ve karar üretme yoluyla yönlendirir; üzerinde anlaşılmış yön ve hedeflere uyum ve performansı izler.

• Yönetim, işletme hedeflerine ulaşmak için yönetişim tarafından saptanmış yön ile uyumlu olarak planlama, inşa etme, işleme ve izleme faaliyetlerini gerçekleştirir.

Yönetim ve yönetişim konularının ayrıştırılması, COBIT 5'in yeni süreç modeline de yansımış durumdadır. Önceki versiyonda ME4 maddesi altında bulunan "BT Yönetişiminin Sağlanması" kontrol hedefi, yeni modelde "Değerlendirme, Yönlendirme ve İzleme (EDM)" adı altında yeni bir etki alanı olarak karşımıza çıkmaktadır. Bu etki alanındaki tüm kontrol hedeflerinden sorumlu ise Yönetim Kurulu olarak belirlenmiş durumdadır. Yönetişim ve yönetim uygulamalarının gerçekleştirilmesinde göz önünde bulundurulacak COBIT prensipleri, COBIT 5 ile işletmenin tümünü kapsayacak şekilde daha üst bir seviyeye çekilmektedir. Bu çerçevede COBIT 5'in beş temel prensibini aşağıdaki gibi tanımlayabiliriz:

• Paydaşların ihtiyaçlarını karşılamak.
• İşletmeyi uçtan uca kapsamak.
• Tek bir entegre çerçeve uygulamak.
• Bütünleşik bir yaklaşım sergilemek.
• Yönetişim ile yönetimi birbirinden ayırmak.

Bu prensiplerden de açık bir şekilde görülebileceği üzere artık COBIT, BT'nin konusu olmaktan çıkıp tüm işletmeyi ve paydaşlarını ilgilendiren bir çerçeve haline gelmiş durumdadır. Yeni COBIT, daha önceki COBIT 4.1, Val IT 2.0 (BT yatırımlarından en iyi değeri elde etmek için anahtar yönetim uygulamaları) ve Risk IT (BT risk yönetimi) çerçevelerini konsolide ederek tek bir entegre çerçeve haline getiriyor. Bunu yaparken de ITIL ve ISO 27001 gibi standartlar ve en iyi uygulamalar ile de temas halinde görünüyor. Yani ISACA adeta, "Kurumsal BT yönetişimi için ihtiyacınız olan her şey burada," diyor.

COBIT 5'in getirdiği bir diğer yenilik de, hedef/ölçü ve girdi/çıktı kavramlarında daha detaylı ve yönlendirici bilgiler içermesidir. Yeni COBIT'te kurum, süreç ve kontrol hedefi (ya da yeni adıyla yönetim ve yönetişim uygulaması) bazında hedef ve ölçülere yer verilmektedir. Bununla birlikte her bir yönetim uygulaması için girdi ve çıktılar tanımlanmış durumdadır. COBIT 4.1'de yalnızca süreç seviyesinde girdi ve çıktılar tanımlı idi. Ayrıca sorumluluk atama çizelgelerinin (RACI charts), iş birimlerini daha çok kapsayacak şekilde detaylandırılmış olması, sorumlulukların daha açık ve anlaşılır şekilde takip edilebilmesini sağlıyor. Bunun sonucu olarak COBIT 5, daha iyi bir yönetişim için bir kılavuz olarak eskisinden daha anlaşılır ve yol gösterici olarak karşımıza çıkıyor.

COBIT 5'in belki de en çok merak edilen ve ilgi çeken konularından biri de süreç olgunluk seviyesi modeline (PCM - Process Capability Model) getirilen değişim konusu idi. Yeni COBIT, daha önceki CMM tabanlı olgunluk modeli yaklaşımını tamamen bırakarak, ISO/IEC 15504 tabanlı yeni bir modele geçiyor. Yeni modeli incelediğimizde, özellikle eski modelde 3, 2 ve 1 olgunluk seviyelerine sahip süreçlerin yeni modelde aşağı düşebileceğini görüyoruz.

Sinem Cantürk

Örneğin, eski modelde 1 olgunluk seviyesine sahip olan ve beklenen süreç sonuçlarına ulaşılamayan süreçler, yeni modelde 0 seviyesine düşebilecektir. Modeldeki bu değişiklik, bankalar başta olmak üzere COBIT çerçevesi ile değerlendirilen kuruluşlar için önem arz ediyor ve uygulamadaki sonuçların nasıl olacağı hususunu en çok merak edilen konulardan biri haline getiriyor.

En çok merak edilen bir diğer konu ise COBIT 5'in tam olarak ne zaman hayatımıza gireceğidir. Halihazırda, BDDK'nın yayımlamış olduğu mevzuat doğrultusunda COBIT'in en güncel versiyonu ile yapılması gerekmektedir. COBIT 5 için güvence kılavuzu (COBIT 5 for Assurance) ve risk (COBIT 5 for Risk) dokümanlarının henüz yayımlanmamış olması ve 2013 yılı içerisinde yayımlanmasının planlanması nedeniyle COBIT 5'in tamamlanmamış olduğu ve son güncel versiyon olarak değerlendirilmemesi gerektiği görüşüne varılması nedeniyle, bankalarda 2012 yılı denetimleri COBIT 4.1'e göre gerçekleştirilmektedir. Ayrıca, bankaların COBIT 4.1'e büyük yatırımlar yapmaları ve sektörde uyumun yeni yeni sağlanmaya başlaması gibi nedenlerle, bir geçiş süresi tanınması gibi çeşitli görüşler şu an için gündemde yer almaktadır. Önümüzdeki dönemde geçerli olacak uygulamaların açıklığa kavuşması için herkesin gözü düzenleyici otoritelerin üzerinde olacaktır.

Sinem Cantürk
Bilgi Sistemleri Risk Yönetimi
Bölüm Başkanı, Direktör
T: +90 216 681 90 37
M: +90 533 294 36 08
E: scanturk@kpmg.com