

### Bilgi Teknolojileri Kontrol Altyapısı'na Temel Bakış

Bilgi teknolojileri, hayatımızı kısa sayılabilecek bir sürede yeniden şekillendirmiş olmasına rağmen, bu kaynađı üretim ve tüketimlerinde kullanan birey ve kurumlar için son derece olađan ve vazgeçilmez bir araç haline gelmiştir. Yeniden biçimlendirme öyle bir düzeye ulaşmıştır ki, bilgi teknolojisi olmadan faaliyetlerini sürdürebilmesi imkansız veya çok zor olan kurumlar oluşmuş, bunlardan bazılarının var olması bizzat teknoloji sayesinde mümkün olmuştur. İşte bu yüzden verimlilik artışında önemli katkı sağlayan bilgi teknolojileri araçları ve bu araçların beklenen düzeyde hizmet üretimini sağlayan kaynaklar, bazı kurumlar için son derece kıymetli, iyi yönetilmesi ve korunması gereken varlıklar haline gelmiştir. Ne var ki bu kaynaklar, alışık olunan tehdit ve risklerin dışında, tabiatları geređi kendilerine has tehlikeler ile de karşı karşıyadır. Ayrıca bu kaynakların geliştirilme ve bakım süreçleri kendilerine has özellikler taşımaktadır. Bu durum mevcut Kurumsal Kontrol Altyapısı'na ek ve onu bütünleyici nitelikte olan Bilgi Teknolojileri Kontrol Altyapısı'nın, bilgi teknolojileri konusunda uzman kişilerin yardımı ile oluşturulması ihtiyacını doğurmuştur. Bilgi teknolojileri kontrol uzmanları ve bilgi teknolojileri kontrol meslek kurumları bu ihtiyaç neticesinde ortaya çıkmış, uzmanlar bu konuda ortak bir anlayış ve bilgi tabanlı geliştirme çabasına girmiştir. Bilgi Teknolojileri Kontrol ihtiyaçlarının karşılanması için kontrol ve denetim metodolojileri, özel teknoloji araç ve platformları için denetim planları, risk istatistikleri, bilgi teknolojilerine yönelik tehditlere karşı fiziksel ve mantıksal korunma araçları geliştirilmiş ve geliştirilmelerine devam edilmektedir. Gelişmiş ülkelerde ulusal veya kurumsal düzeyde teknoloji risk müdahale ekipleri, bilişim suç kanıtlarını toplama ve yargılama düzenlemeleri bilgi teknolojilerinin hayatımıza taşıdığı karmaşık düzenek ve yöntemler nedenleri ile doğmuş, kritik bilgi teknolojileri sistemleri süreklilik ve güvenlik konusundaki çözümleri de bünyelerine katmıştır.

#### Bilgi Teknolojileri Kontrol Altyapısı'nın Amacı

Kurumların sağlıklı faaliyet göstermesinden sorumlu olan veya kurumdan beklentisi olan kişiler, yani pay sahipleri, yönetim kurulu üyeleri, yöneticiler, kurum personeli, devlet yönetimi, hizmet sağlayıcılar, müşteriler ve toplum, gittikçe yükselen bir entelektüel yapıya kavuşmakta, kurumların beklentilerini karşılayabilecekleri ve kendilerini risklere karşı koruyabileceklerine dair güvence istemektedirler. Kurumsal Kontrol Altyapısı'nın entegre bir parçası olan Bilgi Teknolojileri Kontrol Altyapısı'nın sağlıklı biçimde işler olması, yukarıda sayılan risk alıcılara karşı nihai sorumluluđa sahip olan üst yönetimin aşağıdaki soruların yanıtlarına hakim olmasını sağlayacaktır:

- Bilgi teknolojileri desteđinin hedeflerine ulaşması ne derece olasıdır?
- Bilgi teknolojileri organizasyon ve varlıkları yeniliklere adapte olabilecek esnekliğe ve öğrenme kabiliyetine sahip midir?
- Bilgi teknolojileri riskleri makul biçimde yönetilmekte midir?
- Kurum bilgi teknolojileri olanaklarını kavrayabilme ve bu olanakları kendine avantaj sağlayacak biçimde değerlendirme yeteneğine sahip midir?

Bir diđer deyişle, Bilgi Teknolojileri Kontrol Altyapısı'nın amacı, bilgi teknolojileri yatırım ve çabalarına yön vererek bilgi teknolojileri desteđinin aşağıdaki hedeflere ulaşabilme güvencesini sağlamaktır:

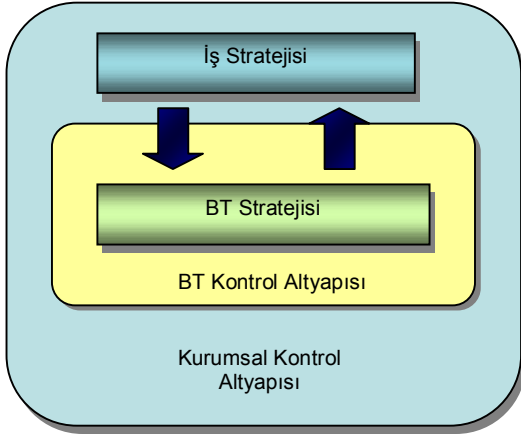
- Bilgi teknolojileri desteđinin kurum ihtiyaçlarına paralel biçimde geliştirilmesi ve planlanan faydaları sağlaması.
- Kurumun var olan bilgi teknolojileri imkanlarından haberdar olması ve bu imkanlardan en üst düzeyde faydalanması.
- Bilgi teknolojileri kaynađının sorumlu ve verimli biçimde kullanılması.
- Bilgi teknolojilerinden kaynaklanabilecek risklerin etkin biçimde yönetimi.

## Kurumsal Kontrol Altyapısı – Bilgi Teknolojileri Kontrol Altyapısı İlişkisi

Kurumların bilgi teknolojileri desteğinden beklentileri aşağıdaki başlıklar altında sınıflandırılabilir<sup>1</sup>:

- Etkililik
- Etkinlik
- Gizlilik
- Bütünlük
- Devamlılık
- Yasal düzenlemelere uyum
- Üretilen bilginin güvenilirliği

Kurumlar faaliyet alanları ve kendilerine has diğer özelliklere bağlı olarak yukarıdaki beklenti kriterlerine karşı değişen oranlarda hassasiyet taşımaktadırlar. Bu beklentilerin karşılanamaması konusundaki hassasiyetlerin belirlenmesi, bilgi teknolojileri kontrollerinin kurulması ve izlenmesi için gerekli harcama ve çabalarının doğru hedefler için ve gereken miktarlarda yapılmasını sağlayacaktır. Kurumun bilgi teknolojileri beklentilerinin karşılanabilme güvencesi, bu kontrol altyapısının sağlıklı biçimde kurulması ve işletilmesi sonucunda mümkün olan en üst düzeyde verilebilecektir. Bilgi Teknolojileri Kontrol Altyapısı'nın en üst düzey kontrol araçlarından biri Bilgi Teknolojileri Stratejisi'dir. Bilgi teknolojileri stratejisini kurumun bu kaynaktan uzun vadeli beklentileri şekillendirmekte, bu beklentileri ise kurumsal iş stratejisi belirlemektedir. Bu temel bağlantı nedeniyle bilgi teknolojileri ile ilgili kontrol altyapısı, kurumun stratejik hedefine ulaşabilmesi için kurulmuş Kurumsal Kontrol Altyapısı'ndan ayrı düşünülemez. Dolayısı ile bilgi teknolojileri kontrol hedefleri iş hedeflerine ulaşılabilmesi için gerekli beklentileri karşılamaya yönelik olmalıdır.



Şekil-1

Kurumsal Kontrol Altyapısı ile Bilgi Teknolojileri Kontrol Altyapısı'nın ilişkisi bilgi teknolojilerinin kurum içinde kullanım oranı, işlenen bilginin kuruma sağladığı rekabet avantajı ve güvenlik ihtiyacı ile doğru orantılı olarak güçlenme eğilimindedir. Farklı özellik ve riskleri barındıran bilgi teknolojileri süreçlerinin özel bir altyapı gerektirmesi sonucunda, farklılaşmış ancak Kurumsal Kontrol Altyapısı'na entegre bir kontrol altyapısı ortaya çıkmıştır.

### Bilgi Teknolojileri Kontrol Altyapısı'nın Oluşturulması ve Uygulanması

Bilgi Teknolojileri Kontrol Altyapısı'nın oluşturulma ve etkin biçimde uygulanmasının sorumluluğu, Kurumsal Kontrol Altyapısı'nda olduğu gibi kurumun yönetim kurulu ve üst yönetiminin sorumluluğundadır. Bilgi Teknolojileri Kontrol Altyapısı'nın oluşturulmasının en temel gerekleri; sorumluların gerekli liderliği ortaya koymaları ve bilgi teknolojileri desteğinin kurumun hedefleri yönünde etkin biçimde sağlanmasını güvence altına alacak organizasyonel yapı ve süreçlerin uygulamaya alınmasını temin etmeleridir. Kontrol altyapılarının işlerliği için en önemli unsur, yönetim desteğinin güçlü biçimde bulunmasıdır.

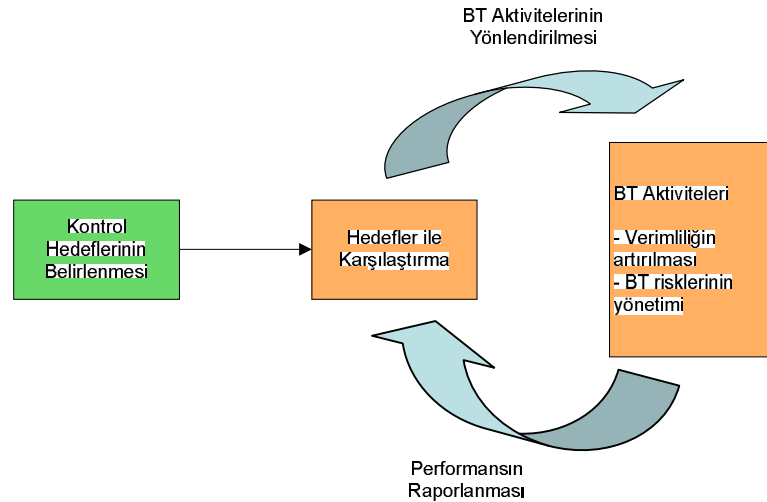
Bilgi Teknolojileri Kontrol Altyapısı kurulma ve denetlemesinde faydalanılabilecek pek çok standart ve

<sup>1</sup> COBIT (Bilgi ve Bilgi Teknolojileri Kontrol Hedefleri) 3. Sürüm'den alınmıştır.

metodoloji bulunmaktadır. Belli bir kontrol metodolojisine referans vermek taraflı bir davranış olabilir. Ancak kurumlar, kontrol ve denetim meslek örgütleri tarafından desteklenen ve güncel tutulan, belli sektörler için o sektörlerin çalışma prensiplerini tayin eden otoritelerin benimsediği ve desteklediği metodolojileri kontrol altyapılarını oluştururken rehber olarak kullanmalıdırlar. Genel kabul görmüş kontrol altyapı metodolojilerini kullanırken bu metodolojilerin jenerik oldukları, bazılarının belli kontrol alanlarına daha fazla odaklandıkları unutulmamalıdır. Kullanılacak kontrol metodolojileri gerekli alanlarda kurumsal ihtiyaçlar göz önüne alınarak zenginleştirilmelidir. Neticede her biri farklı özelliklere sahip ve organizasyonel yapıda olan kurumlar, iyi bir beklenti ve risk analizi yaparak, bilgi teknolojileri desteğinden beklentilerini, sahip oldukları somut ve soyut varlıkları, varlıklarına yönelebilecek ve beklentilerin karşılanmasını engelleyebilecek tehditleri ve bu tehditlerin gerçekleşme olasılıklarını belirlemelidir. Bilgi teknolojileri desteğinin kurumsal strateji açısından hangi ihtiyaçları karşılamasının beklendiği ortaya çıkarılmalıdır. Ancak bu analizlerden sonra kurumun bedenine uygun ve etkin bir kontrol elbisesi biçmek mümkün olacaktır. Bilgi teknolojileri desteğinden beklentiler, beklentileri karşılamak için kullanılacak bilgi teknolojileri varlıklar ve beklentilerin karşılanmasını engelleyebilecek riskler belirlendikten sonra daha detaylı ve etkin kontrol altyapısı ve denetim planları hazırlanabilir. Böylece operasyonel etkinlik ve denetim etkinliği mümkün olan en yüksek düzeyde tutulurken, kontrol harcamalarının verimsiz alanlara yönleneceği engellenebilecektir.

Kontrol altyapılarının vazgeçilmez parçalarından biri olan verimlilik hedefi, kontrol yapısının kendisi için de hayati önem taşımakta olup, kontrol uygulamaları ve denetimleri gerekli planlama ve kaynak aktarımı neticesinde gerçekleştirilmelidir. Kontrol ve denetim altyapısının verimlilik ve etkililiği konusunda uzmanların yetenekleri, ihtiyaçları algılayış kabiliyetleri ve mevcut teknoloji, risk ve metodolojilere hakimiyetleri, dolayısı ile insan faktörü büyük önem taşımaktadır. Kontrol ve denetim uzmanlarının gelişen teknoloji ve kuruma has koşullar göz önüne alınarak iş başı veya sınıf eğitimleri yöntemleri ile yeterli eğitim desteğine sahip olmaları sağlanmalıdır.

BT Kontrol Altyapısı'nın kurulması ve sağlıklı biçimde işler olmasının sağlanması ile kontrol hedefleri belirleme, gerekli kontrollerin mevcudiyetinin ve mevcut kontrollere uyumun denetlenmesi, yetersizliklerin giderilmesi için yönlendirme yapılması, kontrol aktivitelerinin uygulanması ve performanslarının ölçülmesi döngüsü başlatılabilir. Kontrol altyapısının uygulanması tek döngüden ibaret bir süreç değildir. Değişen koşullara uygun kontrol hedefleri benimsenmeli ve kontrol aktiviteleri uygulanmalı, denetim ve performans ölçümleri sürekli gerçekleştirilerek kontrol altyapısının yeterliliği takip edilmelidir.



Şekil- 2

Fatih Emiral