Bilgi Teknolojileri Yönetişim ve Denetim Konferansı

BTYD 2010

ISACA Serving IT Governance Professionals

Türkiye Bilişim Derneği 1971

Türkiye İç Denetim Enstitüsü 1995

eDem TODAİE eDevlet Merkezi

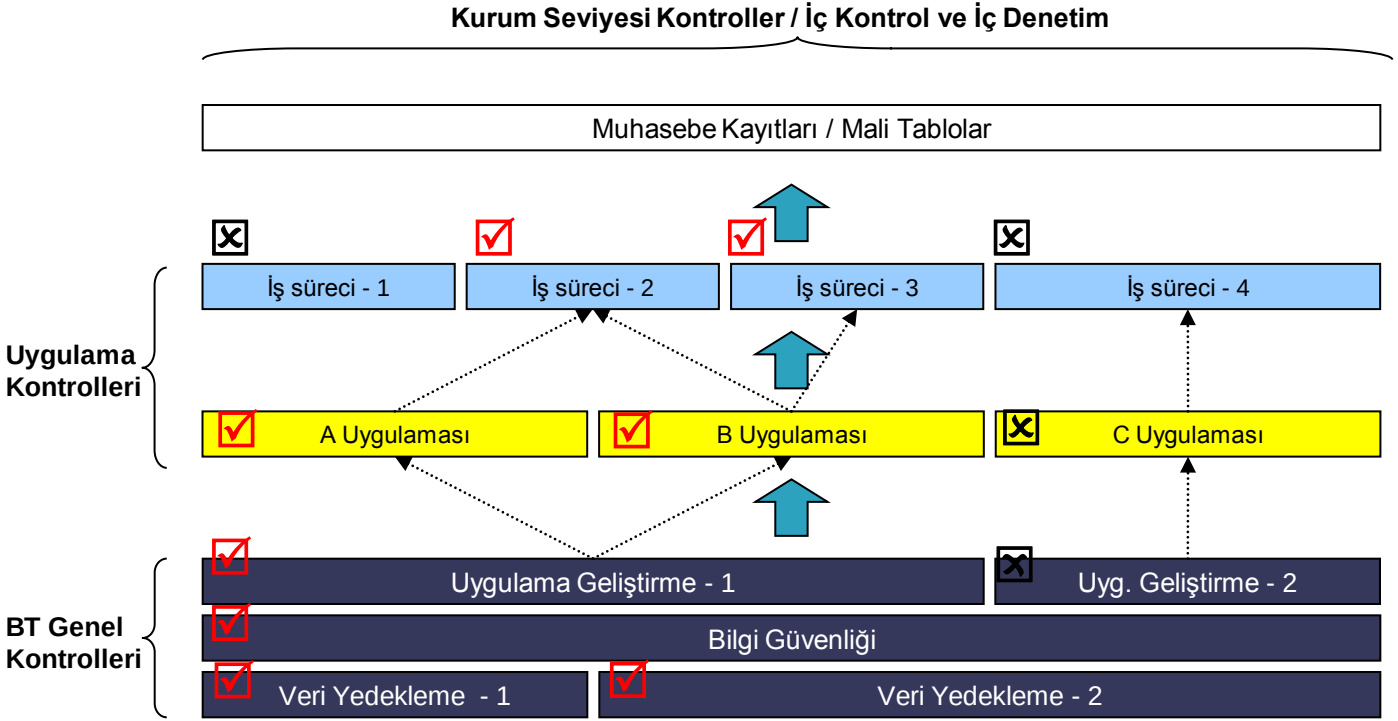
Bilgi Teknolojileri Denetiminde Kontrol Tipleri

Ümit Yalçın Şen
Müdür, Ernst & Young

Kontrol tipleri

- Bir bilgi teknolojileri denetimi çalışması sırasında incelenebilecek kontrol tipleri şu şekildedir:
  - Kurum seviyesi kontroller
  - Genel BT kontrolleri
  - Uygulama kontrolleri

Kontrol tipleri



Kontrol tipleri

Kurum seviyesi kontroller

- Kurum seviyesi kontroller, bir kurumun kontrol ortamı ile ilgili beklentileri ve duruşunu belirler. Bu kontroller, bu duruşun ve beklentilerin ne derece gerçekleştirildiğinin izlenmesi amacıyla kullanılabilir.
- Kurum seviyesi kontrolleri yönetimin paydaşlara şirketin etkin ve etkili çalışması için verdikleri sözleri yerine getirmesine yardımcı olur.

Kontrol tipleri

Kurum seviyesi kontroller

- The Committee of Sponsoring Organizations of the Treadway Commission (COSO)'nun oluşturmuş olduğu "Kurumsal Risk Yönetimi – Bütünleşik Çerçeve" yapısına göre kurum seviyesi kontrolleri şu başlıklarda incelenmektedir:
  - Kontrol ortamı
  - Risk değerlendirmesi
  - Kontrol aktiviteleri
  - Bilgi ve iletişim
  - İzleme ve gözden geçirme
  - Hedef belirleme
  - Olay tanımlama
  - Risk cevabı

Kontrol tipleri

Kurum seviyesi kontrol örnekleri

- Kurum personelinin görev ve sorumlulukları tanımlanmış, ve tüm personele iletilmiştir
- Kurum çapında tüm personelden beklenen dürüstlük, etki değerler ve davranışlar ile ilgili davranış ve etik kuralları oluşturulmuş, yayınlanmış ve personele iletilmiştir
- Kurum işe alma, oryantasyon, eğitim, performans ölçme ve değerlendirme, rehberlik ve terfi gibi insan kaynakları yönetimi ile ilgili politika ve prosedürleri geliştirmiş ve uygulamaya almıştır
- Kurum iç kontrol sistemi dahilinde gerçekleştirilecek kontrol aktivitelerini aşağıdakilerle sınırlı kalmayacak şekilde tasarlamış ve devreye almıştır
  - Finansal ve operasyonel açıdan performansın ölçülmesi
  - Bilgi işleme sistemleri tarafından işlenen verilerin doğruluğu ve bütünlüğünün sağlanması ve işlemlerin yetkilendirilmesi
  - Fiziksel kontrollerin uygulanması

Kontrol tipleri

Genel bilgi teknolojileri kontrolleri

- Önleyici ve tespit edici kontrollerin otomatize edilmiş kısımlarının devamlılığını sağlayan ve elektronik denetim kanıtlarına güvence verilmesine katkıda bulunan kontrollerdir.
- Genel BT kontrolleri, uygulama ve BT bağımlı manüel kontrollerinin etkinliğinde belirleyici olması ve elektronik denetim kanıtlarının güvenilirliğini etkilemesi açısından önem taşımaktadır

Kontrol tipleri

Genel bilgi teknolojileri kontrolleri

- Denetim kapsamında kritik olarak değerlendirilen süreçler üzerinde belirlenen uygulama ve BT bağımlı manüel kontrollerin etkinliği ve süreç akışında rol oynayan elektronik denetim kanıtlarının güvenilirliğini değerlendirebilmek, ilgili süreçleri destekleyen uygulamalar üzerinde genel BT kontrolleri değerlendirme çalışması gerçekleştirmek suretiyle mümkün olmaktadır.

Kontrol tipleri

Genel bilgi teknolojileri kontrolleri

- BT genel kontrolleri;
  - Değişiklik yönetimi kontrolleri
  - Mantıksal erişim kontrolleri
  - Fiziksel erişim kontrolleri
  - BT operasyonları kontrolleri

  olmak üzere belirli kategorilere ayrılabilmektedir.

Kontrol tipleri

Genel bilgi teknolojileri kontrolleri

- Değişiklik yönetimi kontrolleri:
  - Değişiklik yönetimi kontrol hedefleri belirtilenlerle sınırlı olmamakla birlikte aşağıdakileri içerebilir:
    - Değişikliklerin yetkilendirilmesi,
    - Değişikliklerin test edilmesi,
    - Değişikliklerin onaylanması,
    - Değişikliklerin izlenmesi,
    - Değişiklik yönetimi prosedürleri dâhilîde görevler ayrılığı ilkesinin uygulanması.

Kontrol tipleri

Genel bilgi teknolojileri kontrolleri

- Mantıksal erişim kontrolleri:
  - Örnek mantıksal erişim süreci kontrol hedefleri aşağıda listelenmiştir;
    - Genel sistem güvenlik ayarlarının uygunluğu,
    - Şifre parametrelerinin uygunluğu,
    - Ayrıcalıklı / imtiyazlı BT görevlerinin uygun personele sınırlandırılması,
    - Sistem kaynakları ve araçlara erişimin uygun personele sınırlandırılması,
    - Kullanıcı erişimlerinin uygun şekilde yetkilendirilmesi ve yönetilmesi,
    - Mantıksal erişim sürecinin izlenmesi,
    - Mantıksal erişim prosedürleri dâhilinde görevler ayrılığı ilkesinin uygulanması.

Kontrol tipleri

Genel bilgi teknolojileri kontrolleri

- Fiziksel erişim kontrolleri:
  - Uygulama ve verilerin barındırıldığı, saklandığı ve depolandığı fiziksel cihazların bulunduğu odalara erişimlerin kontrollü ve yetkilendirilmiş bir şekilde sağlandığının kontrol edilmesini içermektedir.

Kontrol tipleri

Genel bilgi teknolojileri kontrolleri

- BT operasyonları kontrolleri:
  - Verilerin yedeklenmesi ve periyodik geri dönüş testlerinin gerçekleştirilmesi,
  - Zamanlanmış işlerde gerçekleşen sapmaların düzenli olarak izlenmesi ve zamanında çözülmesi,
  - BT operasyonlarına dair problem ve olayların belirlenmesi, iletilmesi, çözülmesi, gözden geçirilmesi ve analiz edilmesi.

Kontrol tipleri

Uygulama kontrolleri

- Uygulama kontrolleri kendi içinde beş ana başlıkta incelenebilir:
  - Girdi kontrolleri
  - Doğrulama kontrolleri
  - Hesaplama kontrolleri
  - Ara yüz kontrolleri
  - Yetkilendirme kontrolleri

Kontrol tipleri

Uygulama kontrolleri – Görevler ayrılığı

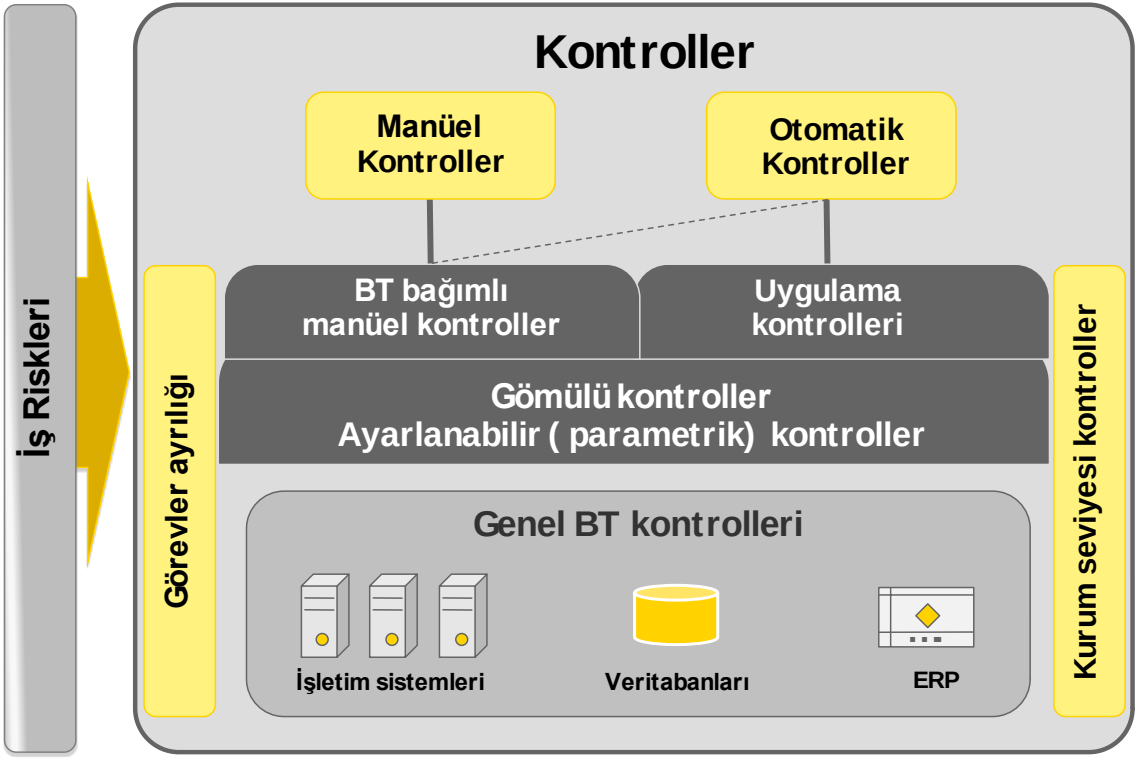
- Görevler ayrılığı ilkesi iş süreçleri içinde kritik fonksiyonların gerçekleştirilmesinde meydana gelebilecek hataların oluşmasını ve bu hataların tespit edilememesini engellemek üzere tasarlanmıştır. Eksikliği durumda aşağıda bahsedilen durumlar meydana gelebilir:
  - Varlıkların zimmete geçirilmesi
  - Finansal bilgilerin yanlış beyan edilmesi
  - Yanlış finansal raporlama
  - Fonların uygun olmayan kullanımı
  - Veri değişikliklerinin farkına varılamaması

Kontrol tipleri

Uygulama kontrolleri – Görevler ayrılığı

- Görevler ayrılığı kontrolleri
  - İşlem yetkilendirmesi
  - Varlıkların muhafazası ve gözetimi
  - Verilere erişim
- Görevler ayrılığı kontrollerinin eksikliğinde uygulanabilecek telafi kontrolleri
  - Denetim izleri – işlem kayıtları
  - İstisna raporları
  - Bağımsız gözden geçirme

Kontrol tipleri



Kontrol tipleri
İnceleme teknikleri

- Kontrol tasarımlarının test edilmesi (üzerinden geçme)
  - Kontrol tasarımının uygunluğunun değerlendirilmesi, ve
  - Mevcut kontrollerin tasarlanan şekilde çalıştığının doğrulanması - tek bir örnek vasıtasıyla üzerinden geçme
- Kontrol tasarımlarının uygunluğunun testi sürecinde değerlendirilmesi gereken unsurlar aşağıdaki şekilde özetlenebilir:
  - Yazılı ve yönetim tarafından onaylanmış güncel bir kontrol sürecinin varlığı,
  - Kontrol süreci ile ilgili denetim kanıtlarının varlığı,
  - Sorumluluk ve hesap verilebilirlik ilkelerinin açıklığı ve etkinliği,
  - Gerekli noktalarda telafi edici kontrollerin uygulanması.

Kontrol tipleri

İnceleme teknikleri – örneklem belirlenmesi

- Denetçi tarafından yeterli, uygun, kabul edilebilir ve denetim açısından yararlı kanıtlar elde etmek amacıyla istatistiki ve istatistiki olmayan yöntemler ile örneklem seçilmesidir.
- Örneklem büyüklüğü ve yapısının belirlenmesinde, denetim amaçları, genel örneklem hacminin doğası, örneklem seçme yöntemleri ve örneklem riski (kabul edilebilir hata seviyesi) dikkate alınmaktadır.

Kontrol tipleri
İnceleme teknikleri

- Kontrol etkinliğinin test edilmesi üzerinden geçme çalışmaları sırasında etkin olarak tasarlandığı belirlenen kontrollerin:
  - Kontrol tipi ve frekansı temel alınarak seçilen örneklem vasıtası ile, ve
  - Denetim gerçekleştirilen dönem boyunca

  tasarlanan şekilde çalışıp çalışmadığının değerlendirilmesidir.

Kontrol tipleri
İnceleme teknikleri

- Kontrol etkinliğinin testi, ayrıca:
  - Test edilen kontrollerin belirlenen şekilde çalışmadığı durumlarda telafi edici kontrollerin belirlenmesi
  - Telafi edici kontrollerin test edilmesi
  - BT süreçlerinin uygunluğundan emin olmak adına gerekli durumlarda uygulanacak bağımsız denetim tekniklerinin düzeyinin belirlenmesini

  kapsamaktadır.

BTYD 2010

www.btyd.org