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

BAĞIMSIZ DENETİMDE BİLGİ TEKNOLOJİLERİ DENETİMİ KAPSAM VE METODOLOJİ

Tanıl Durkaya, CISA, CGEIT, CRISC
Kıdemli Müdür, KPMG Türkiye

İçerik

- BT Denetim Hedefi
- Öncelik ve Önemlilik Değerlendirmesi
- Denetim Kapsamı
- Denetim Metodolojisi
  - Destek Hizmetleri Kuruluşlarının Denetimi
- Raporlama

BT Denetim Hedefi

- Finansal verilerin üretimi, doğruluğu ve güvenilirliği
- Yasal uyumluluğun sağlanması
- Bilgi güvenliğinin sağlanması
- Hizmet sürekliliğinin sağlanması
- BT Operasyonel verimliliğin sağlanması
- BT Yönetişimin sağlanması

Öncelik ve Önemlilik Değerlendirmesi

- Kaynak planlaması ve sınırlamalar
  - Denetim dönemi ve raporlama
  - Kaynak planlaması ve yönetimi
  - Kapsam belirlemesi

Öncelik ve Önemlilik Değerlendirmesi

- Önemlilik Kriterinin Belirlenmesi
  - BT Denetim Hedefi ile Uyum
    - Finansal verilerin doğruluğu ve güvenilirliği
    - Hizmet sürekliliği
    - Bilgi güvenliği

Öncelik ve Önemlilik Değerlendirmesi

- Finansal verilerin doğruluğu ve güvenilirliği
  - Hesap bakiyelerinin büyüklüğü
  - Finansal işlem adedi ve büyüklüğü
  - Olası hataların finansal verilere etkisi

Öncelik ve Önemlilik Değerlendirmesi

- Yasal uyumluluğun sağlanması
  - Yasal düzenlemelerde tanımlanmış önemlilik kriterleri
  - Yasal düzenlemenin amacı ve nihai hedefi
  - Öngörülen yaptırım ve cezaların boyutu
  - Dönemsellik ile ilgili düzenlemeler

Öncelik ve Önemlilik Değerlendirmesi

- Bilgi güvenliğinin sağlanması
  - Yasal düzenlemelerde tanımlanan veri hassasiyeti ve kritikliği
  - Hassas veriler
- Hizmet sürekliliğinin sağlanması
- Operasyonel verimliliğin sağlanması
- BT Yönetişimin sağlanması

Denetim Kapsamı

- Denetim Kapsamının Belirlenmesi
  - Kritik süreçler (müşteri bilgileri işleme, muhasebe, satın alma, stok yönetimi vb)
  - Kritik uygulama ve altyapılar
    - Uygulama/Program (örn: Oracle ERP)
    - Veritabanı (örn: Oracle)
    - İşletim sistemi (örn: UNIX)

Denetim Kapsamı

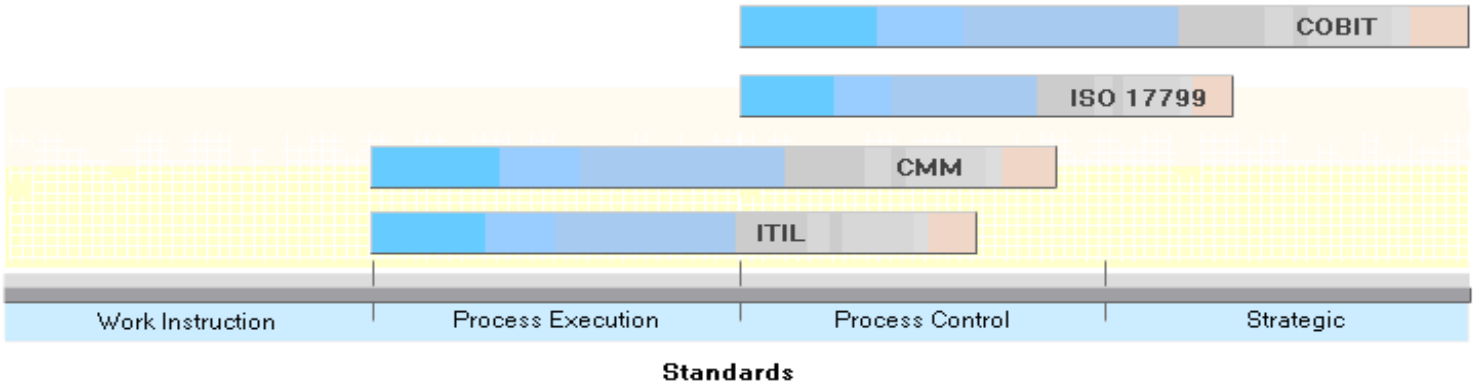
- Denetim Kapsamının Belirlenmesi
  - Kritik uygulama ve altyapıları destekleyen BT süreçleri (ITIL, COBIT vb)
  - Kritik uygulama ve altyapıların yönetim/işletim sorumlulukları ve lokasyonlar (yurtiçi, yurtdışı)
  - Destek hizmeti alımına konu sistemler ve süreçler

Denetim Metodolojisi

- Planlama ve Metodoloji
  - Temel alınacak çerçeve ve standartlar (COBIT, ITIL, ISO27001, PCI vb)
    - Kontrol hedefleri
    - Denetim programları
    - Detay kontrol noktaları

Denetim Metodolojisi

- Planlama ve Metodoloji
  - Çerçeve ve standartlar (COBIT, ITIL, ISO27001, PCI vb)



Denetim Metodolojisi

- Planlama ve Metodoloji
  - İhtiyaç duyulan kaynaklar
    - İç kaynaklar
    - Dış kaynaklar
    - Destek alınacak konular
  - Diğer denetçilerin çalışmalarının kullanımı
  - Yeterli denetim kanıtlarının elde edilmesi

Denetim Metodolojisi

- Planlama ve Metodoloji
  - Kritik uygulama ve altyapıların yönetim/işletim sorumlulukları ve lokasyonlar (yurtiçi, yurtdışı)
    - Yönetim/işletim faaliyetlerinin gerçekleştirilmesi
    - Sistemlerin bulunduğu yerleşimler / sistem odaları
    - Grup şirketlerinden sağlanan hizmetler (uluslar arası şirketler için)
    - Destek hizmetleri kapsamında gerçekleştirilen faaliyetler

Denetim Metodolojisi

- Planlama ve Metodoloji
  - Dış kaynak kullanımı
    - Uzmanlık gerektiren sistem ve altyapılar
    - Uzmanlık gerektiren konular
  - Diğer denetçilerin çalışmalarının kullanımı
    - İç denetim tarafından gerçekleştirilen çalışmaların kullanımı (denetim raporları)
    - Diğer denetim ve teknik değerlendirme çalışmalarının kullanımı (sızma testleri, güvenlik değerlendirmeleri vb.)

Denetim Metodolojisi

- Destek Hizmeti Kuruluşlarının Denetimi
  - Destek hizmeti kuruluşlarından sağlanan hizmetler
    - Sistem yönetimi
    - Sistemlerin barındırılması
    - Veri veya çıktı hazırlama
    - Ağ ve güvenlik yönetimi

Denetim Metodolojisi

- Destek Hizmeti Kuruluşlarının Denetimi
  - Denetim Standartları
    - SAS 70 – Tip 1
      - Belirli bir tarih itibarıyla, kontrollerin tasarımına ilişkin
    - SAS 70 – Tip 2
      - Bir dönem için kontrollerin tasarım ve etkinliğine ilişkin

Denetim Metodolojisi

- Destek Hizmeti Kuruluşlarının Denetimi
  - Denetim Standartları
    - ISAE3402
      - 15 Haziran 2011'den itibaren geçerli
      - Finansal ve operasyonel süreçlerin etkinliğine yönelik
    - Üzerinde anlaşılan prosedürler (AUP)
      - Kontrol detaylarını ve test sonuçlarını içerecek şekilde
      - Kontrollerin etkinliğine yönelik bilgi içeren

Raporlama

- Kurum içi raporlama
  - Finansal denetim ekibi ile BT Denetim ekibi arasında
  - İç kontrol ortamına ilişkin görüş ve değerlendirmeler
  - Yönetim mektubu aracılığı ile şirket yönetimi ve yönetim kurulu ile

Raporlama

- Kurum dışı raporlama
  - Denetim kapsamına göre hazırlanan
  - Risklilik derecelerine göre sınıflandırılmış
  - Bağımsız denetim görüşü içerebilecek
    - Eğer belirli bir standarda göre yürütülmüş ve görüş oluşturulacak bir çalışma ise

BTYD 2010

www.btyd.org