

Bilgi Sistemlerine İlişkin Yasal Düzenlemeler & COBIT **AB Seminer 2009**



Ender ŞAHİNASLAN

Arzu KANTÜRK

Ender ŞAHİNASLAN

11-13 Şubat 2009

Gündem



- ➔ Bankacılıkta Bilgi Sistemlerine İlişkin Düzenlemeler
- ➔ Etkin ve verimli bir Banka'dan beklenenler
- ➔ Bilgi Teknolojilerinden Beklenenler
- ➔ Bilgi Teknolojilerinin Yönetişi
- ➔ COBIT ve Olgunluk Seviyeleri
- ➔ Bilgi Sistemleri Denetimlerine Hazırlık Metodolojisi

Ender ŞAHİNASLAN

11-13 Şubat 2009

Eğitici [Ender Şahinaslan]



2007 – Devam	BANK ASYA - Bilgi Güvenliği – Müdür Yardımcısı
2005 – 2007	BANK ASYA Organizasyon, Kalite ve Sistem Geliştirme Müdürlüğü – II. Müdür
2004 - 2005	BANK ASYA - Yazılım Geliştirme Müdürlüğü – Sistem Analist
2000 - 2004	SABANCI ÜNİVERSİTESİ – Bilgi Teknolojileri - Uygulama Sorumlusu
1999 - 2000	MALTEPE ÜNİVERSİTESİ – Bilgisayar Mühendisliği – Öğretim Görevlisi
1997 - 1999	GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ – Bilgisayar Mühendisliği – Arş. Grv.
1995 - 1996	GAZİ ÜNİVERSİTESİ – Fen Bilimleri Enstitüsü – Araştırma Görevlisi

- **Doktora**, Trakya Üniversitesi – Bilgisayar Mühendisliği – 2008 - Devam
- **Yüksek Lisans**, Gebze Yüksek Teknoloji Enstitüsü – Bilgisayar Mühendisliği – 1998
- **Lisans**, Trakya Üniversitesi – Bilgisayar Mühendisliği – 1995

2

Ender ŞAHİNASLAN

11-13 Şubat 2009

BDDK-Bilgi Sistemlerine İlişkin Düzenlemeler

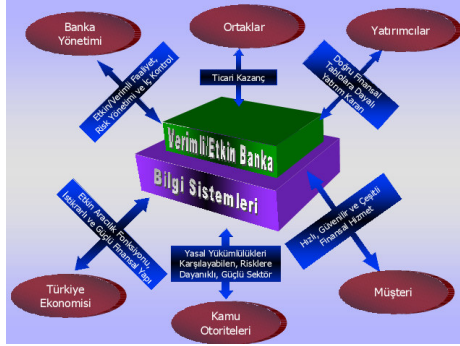


Kaynak: BDDK Bilgi Yönetimi Daire Başkanlığına ait bir sunumdan

Ender ŞAHİNASLAN

11-13 Şubat 2009

Etkin-Verimli bir Banka'dan beklenenler...



Kaynak: BDDK Bilgi Yönetimi Daire Başkanlığına ait bir sunudan

Ender ŞAHİNASLAN

11-13 Şubat 2009

Bilgi Teknolojileri ne durumda?

- ➔ Yarın sistemimiz/sistemlerimiz çalışıyor olacak mı?
- ➔ Acil Durumlarda **İş Sürekliliği**'ni nasıl sağlıyor olacağız?
- ➔ **İhtiyaçlar**'ımız ile kullandığımız teknoloji ne kadar uyumlu?



- ➔ Teknoloji Yatırımlarım **Kaç yıl** yaşayacak?
- ➔ **Teknoloji riskleri** için nasıl önlemler alınıyor?
- ➔ **Projelerin** taşıdığı **risklerden** haberdar mıyız?
- ➔ Altyapımız; ihtiyaçlarımız için **Optimum** çözüm mü?
- ➔ Teknoloji **Yatırım giderleri**?
- ➔ A kişisi **işten ayrılırsa** yandık ... diye bir kaygı duyuyor muyuz?
- ➔ Müşteri ve Kurum bilgileri **Güvende** mi?

Ender ŞAHİNASLAN

11-13 Şubat 2009

Bilgi Teknolojilerinden Beklenenler ...

- ➔ İş hedef ve stratejileriyle **uyumlu, birlikte** hareket etmesi,
- ➔ İş ihtiyaç ve beklentilerine zamanında **etkin ve verimli çözümler** sunabilmesi,
- ➔ Rekabette destek olabilmesi, gelişen teknolojiye **ayak uydurması**,
- ➔ Bilgi ve sistem alt yapı **güvenliğini** sağlaması,
- ➔ BT **hizmet seviyelerini** iş gereksinimlerini dikkate alarak sunması(SLA) **anlaşma** gereklerini karşılaması,
- ➔ Düşük maliyette yüksek kalitede **hizmet** sunabilmesi,
- ➔ Projeleri zamanında ve beklenen **kalitede** sunması,
- ➔ BT **risklerini** yönetmesi,
- ➔ Hizmet **sürekliliğini** sağlaması,
- ➔ BT bilgi varlıklarını **koruma** altına alması,
- ➔ Yasal mevzuata ve politikalara **uyumlu** olması

Ender ŞAHİNASLAN

11-13 Şubat 2009

Bilgi Sistemlerinde yaşanan önemli olaylar ...



- ➔ Ana Switch Problemi
- ➔ 18 Saat Boyunca Pek Çok Kredi Kartı Kullanım Dışı



- ➔ Finansal Bilgi Raporlamasında Sahtekarlık
- ➔ 2000 yılında kârı 42 M \$ iken 979 M \$ gösterilmiş
- ➔ Nakit akımı gerçekte - 3 milyar \$ iken 154 M \$ gösterilmiş



- ➔ Finansal Bilgi Raporlamasında Sahtekarlık
- ➔ 2002'de Kağıt üzerinde bilançosunu 3.8 milyar \$ fazla gösterdi



- ➔ Çifte Kayıt Sistemi

Ender ŞAHİNASLAN

11-13 Şubat 2009

BDDK-Bilgi Sistemleri Denetimleri

Denetimin kapsamı;

- Genel Kontroller Bölümü (COBIT)
- Uygulama Kontrolleri Bölümü
- İç Kontrolün Değerlendirmesi

COBIT (Genel kontroller) bölümü 2 yılda 1, Uygulama Kontrolleri denetimi ise her yıl yapılmakta.

2007 yılından itibaren bankalarla mali konsolidasyona giren her şirket bu yönetmelik kapsamında denetimleri yapılmakta.

Bilgi Sistemleri denetimlerden bankalarda bağımsız mali denetim yapan şirketler sorumlu.

Ender ŞAHİNASLAN

11-13 Şubat 2009

COBIT 4.1

Control **O**bjectives for Information and related **T**echnology – Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri)

- COBIT BT kaynaklarını Kurum hedeflerine göre kullanmayı sağlayan araç.
- İş hedefleri ile BT hedefleri arasında köprü vazifesi görmeye yarar.
- BT organizasyonunu yönetmek için bir altyapı sunar.
- BT'nin yönetimi ve kontrolü için **süreç tesisi ve denetim** odaklıdır.
- Süreçlerin ilgili bölümlerinde ilgili standart (ISO 9001/27001, ITIL, CMMI ve PMI vb) yaklaşımları tavsiye eden çerçeve yapı.

COBIT bir dokümantasyon sisteminden ibaret olmayıp etkili bir **BT Yönetişim Modelidir**. Ne yapmanız gerektiğini söyler, nasıl yapacağınızı belirtmez.

4 ana süreç ve 34 farklı alt süreçten oluşur.

215 adet detaylı kontrol hedefini içerir.

Ender ŞAHİNASLAN

11-13 Şubat 2009

Banka'nın yükümlülükleri

Banka,

Bilgi sistem dokümantasyonunu, finansal bilgi üretim süreçlerine ait dokümantasyonu ve ilgili her türlü kayıt, bilgi ve belgeyi denetime hazır hale getirmek,

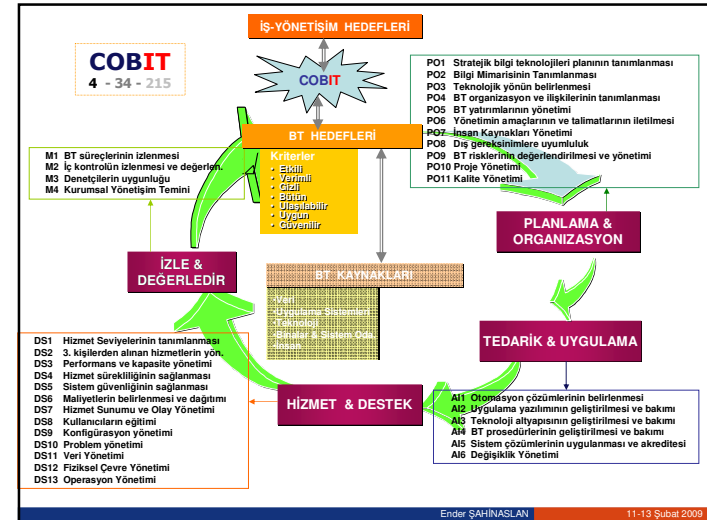
Bilgi sistemleri denetimi için talep edilen her türlü bilgi ve belgeyi denetçi ile paylaşmak,

Bankacılık faaliyetlerinde kullanılan uygulamaların detaylı listesi, ve çalışma prensiplerini hazırlamak,

ile yükümlüdür.

Ender ŞAHİNASLAN

11-13 Şubat 2009

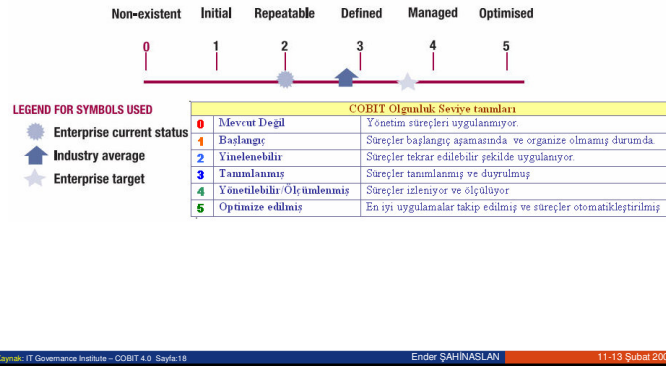


Ender ŞAHİNASLAN

11-13 Şubat 2009

COBIT Olgunluk Seviyeleri

Figure 9—Graphic Representation of Maturity Models



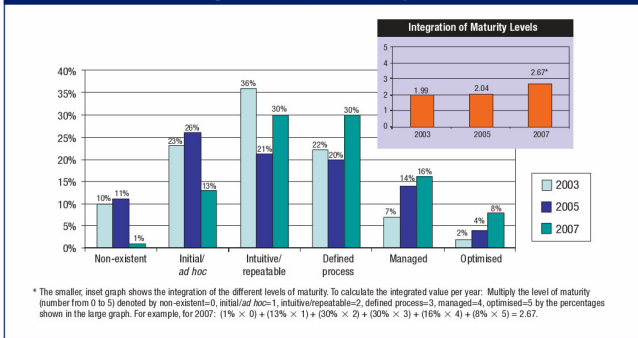
COBIT Olgunluk Seviyeleri [detay]

Olgunluk Seviyesi	İhtiyaçlar ve Beklentiler	İhtiyaçlar, Standartlar ve Özellikler	Avantajları ve Sorunları	Ölçülebilir ve Ölçülebilir	Değerlendirme ve Değerlendirme	İhtiyaçlar ve Beklentiler
0	Yok	Yok	Yok	Yok	Yok	Yok
1	Yok	Yok	Yok	Yok	Yok	Yok
2	Yok	Yok	Yok	Yok	Yok	Yok
3	Yok	Yok	Yok	Yok	Yok	Yok
4	Yok	Yok	Yok	Yok	Yok	Yok
5	Yok	Yok	Yok	Yok	Yok	Yok

Kaynak: IT Governance Institute COBIT 4.1 Sayfa:21 Ender ŞAHİNASLAN 11-13 Şubat 2009

COBIT Olgunluk Seviyeleri [2008 Araştırma Sonuçları]

Figure 20—IT Governance Maturity Level



BS Denetimlerine hazırlık metodolojisi

Denetim hazırlık ...

- Plan (mevcut durum teşhisi, önceliklendirme ve sorumlulukların atanması)
- Uygulama
- Kontrol (düzenli gözden geçirme)
- Önlem al

Referans Kaynak [Cobit 4.1]

- www.bddk.org.tr Bankacılık Düzenleme ve Denetleme Kurumu
- www.isaca.org Information Systems Audit and Control Association
- www.itgi.org IT Governance Institute (COBIT, CISA, CISM)

Ender ŞAHİNASLAN 11-13 Şubat 2009



SORULAR & CEVAPLAR TEřEKKÜRLER



Ender řAHİNASLAN

11-13 řubat 2009