



Bankacılıkta Bilgi Sistemleri Denetiminde BDDK Yaklaşımı ve Bilgi Güvenliđi

AHMET TÜRKEY VARLI
BDDK Bilgi Yönetimi Dairesi
Daire Başkanı



İÇİNDEKİLER

- Bankacılıkta Bilgi Teknolojileri
- Bilgi Sistemleri (BS) Denetimi
- Bankacılıkta BS Denetimi
- Benimsenen Denetim Çerçevesi : COBIT
- Bilgi Güvenliği
 - COBIT ve Bilgi Güvenliği
 - Bankacılıkta Bilgi Güvenliği
 - BDDK'da Bilgi Güvenliği



Bankacılıkta Bilgi Teknolojileri



Bankacılıkta Bilgi Teknolojileri

- Temel Bankacılık Faaliyetlerinin İfası
- Alternatif Dağıtım Kanallarının Tesisi
(Elektronik Bankacılık)

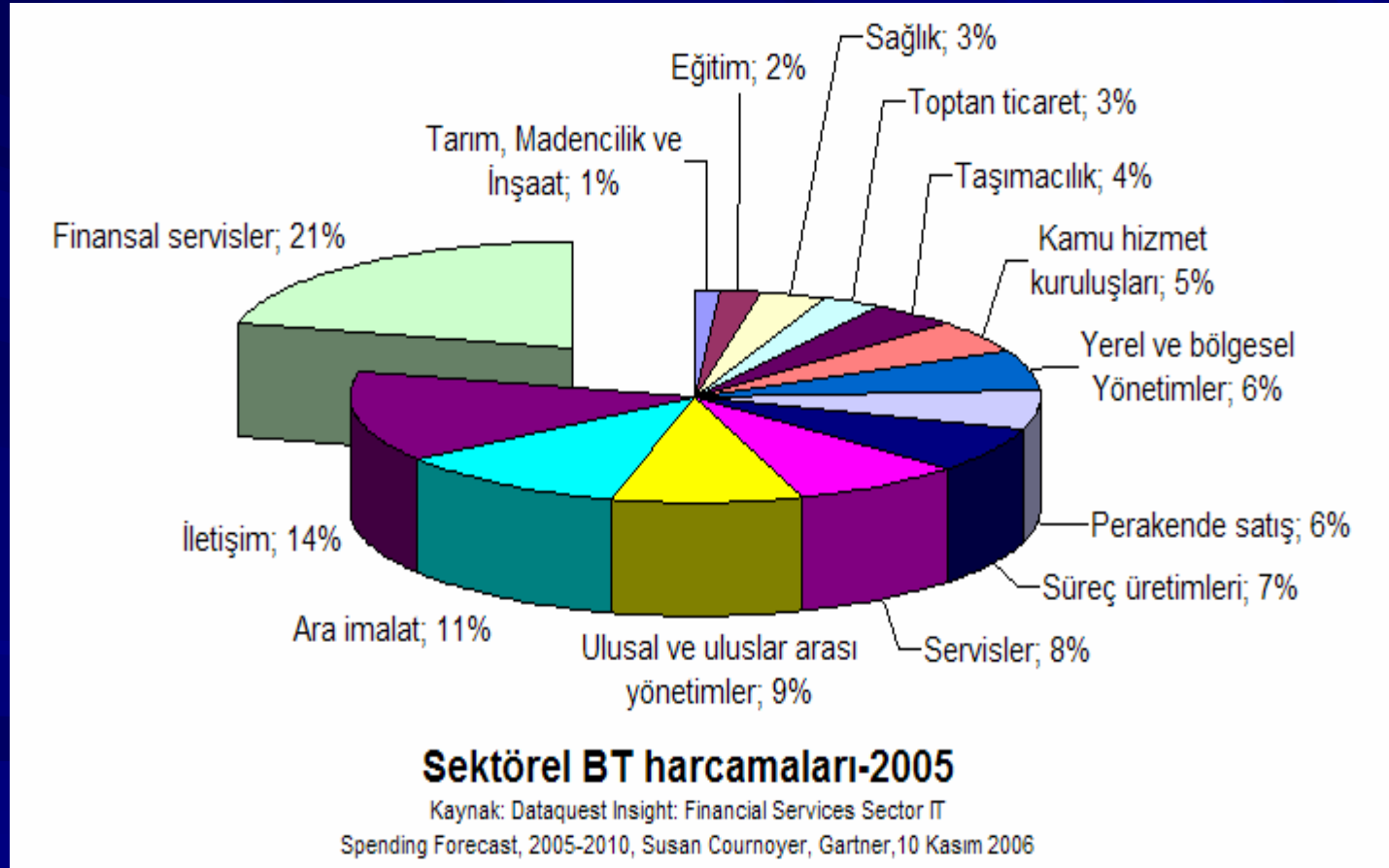


Bankacılıkta Bilgi Teknolojileri / Elektronik Bankacılık

- İnternet Bankacılığı
- ATM
- Telefon Bankacılığı
- Kiosk
- Kartlı Ödeme Sistemleri
- Televizyon Bankacılığı
- WAP/GPRS Bankacılığı



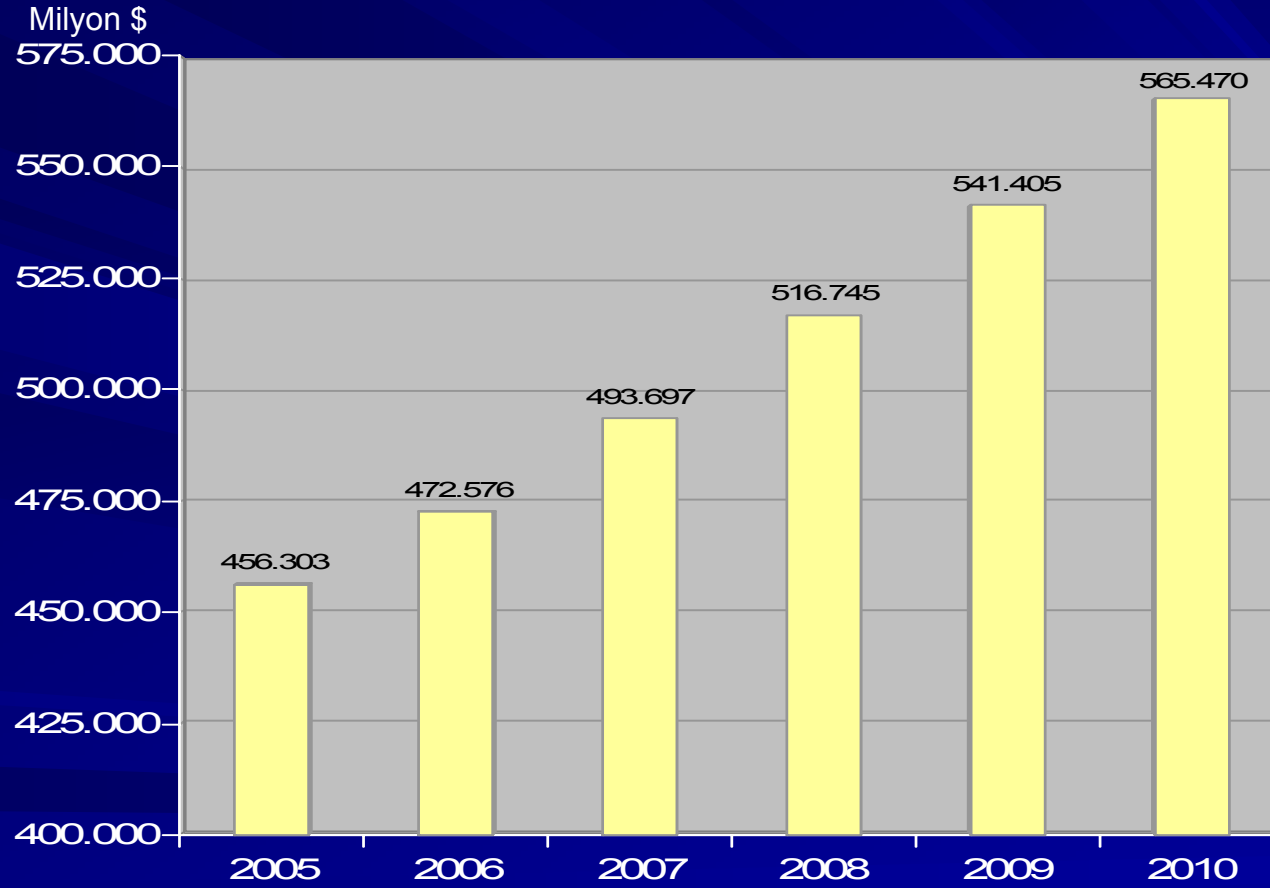
Bankacılıkta Bilgi Teknolojileri / BT'nin Vazgeçilmezliği





Bankacılıkta Bilgi Teknolojileri / BT Harcamaları

(Harcamalarda Yıllık Ortalama Artış:%4.4, Kaynak: Gartner)

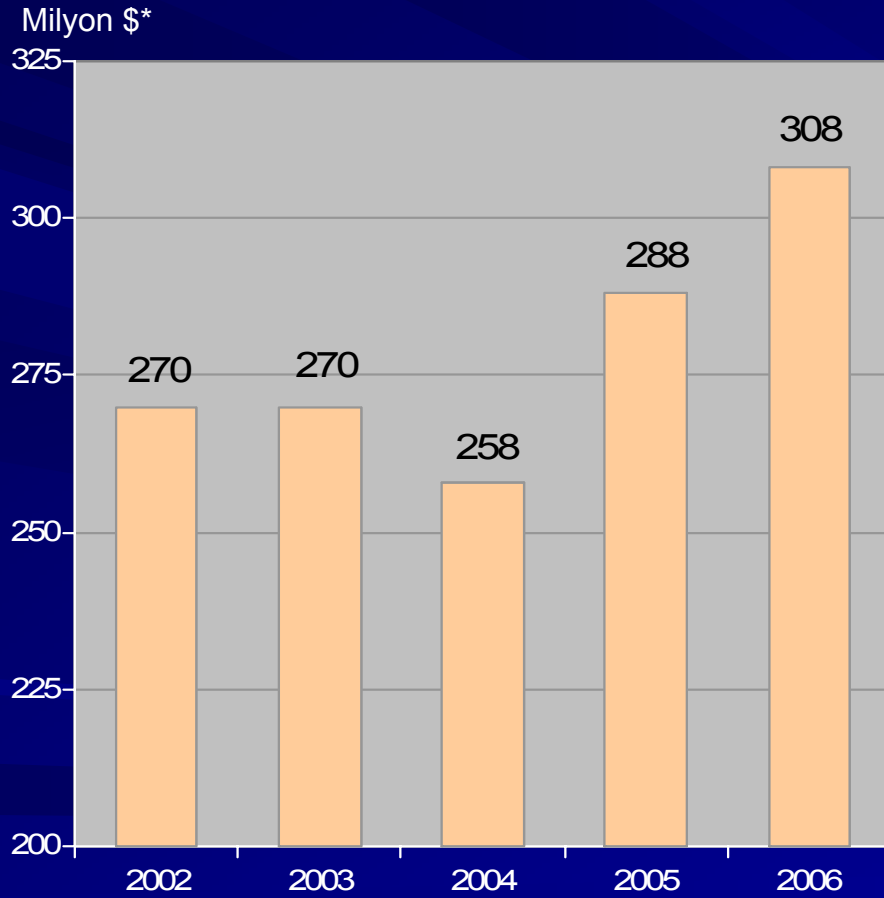


Dünyada finansal sektörün BT harcamaları (Gerçekleşen ve tahmin edilen)

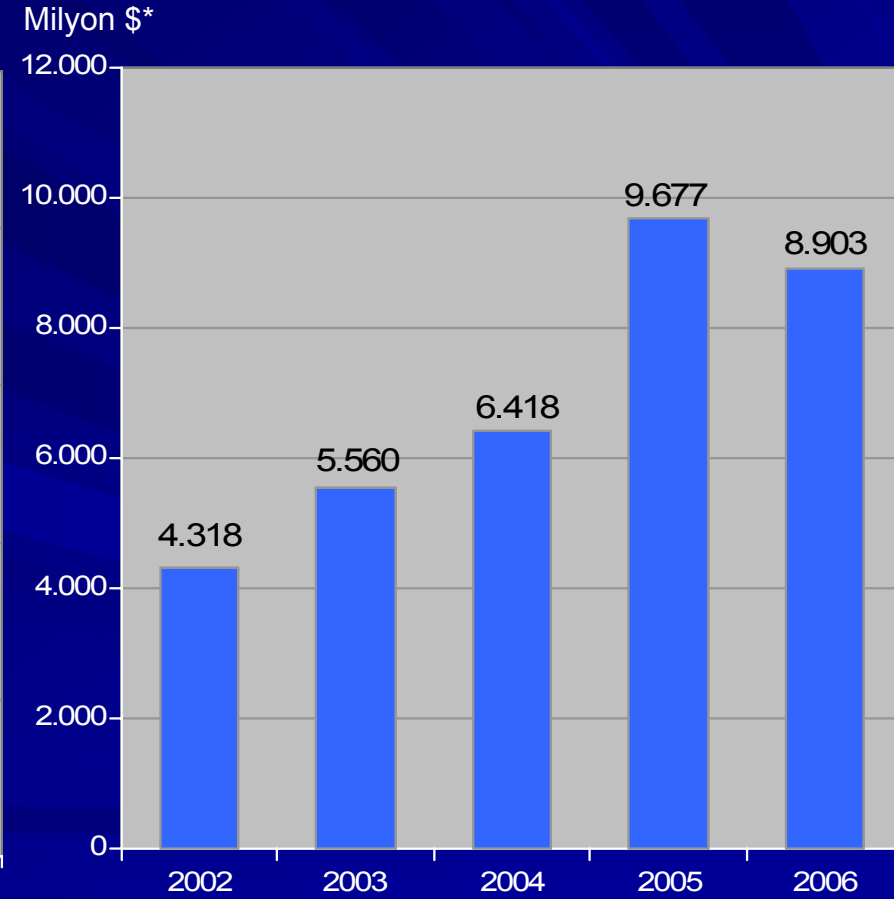
Kaynak: "Dataquest Insight: Financial Services Sector IT Spending Forecast", 2008-2010, Susan Courmoyer, Gartner, 10 Kasım 2006



Bankacılıkta Bilgi Teknolojileri / BT ve İşletme Giderleri (*)



Teknoloji Giderleri



İşletme Giderleri

BDDK / Bilgi Yönetimi Daire Başkanlığı

(*) Bankalardan gelen finansal verilerden, yıllık ortalama kur baz alınarak hesaplanmıştır.



Bilgi Sistemleri Denetimi



BS Denetimi /

BS Denetimi İhtiyacına İşaret Eden Olaylar

■ AT&T

- 1998'de Ana Switch Problemi
- 18 Saat Boyunca Pek Çok Kredi Kartı Kullanım Dışı

■ Enron

- Finansal Bilgi Raporlamasında Sahtekarlık
- 60 Milyar USD Kamu Zararı

■ WorldCom

- Finansal Bilgi Raporlamasında Sahtekarlık

■ İmar Bankası

- Çifte Kayıt Sistemi



BS Denetimi /

Ülke Uygulamalarında Benimsenen Esaslar

ÜLKELER	Kullanılan Yaklaşımlar
FİNLANDİYA	"İç Kontrol ve Risk Yönetimi" İle İlgili Geliştirdikleri Kendi Standartları
NORVEÇ	CoBIT Baz Alınmıştır
MACARİSTAN	CoBIT Baz Alınmıştır
ÇEK CUMHURİYETİ	IT Yönetimi ve Operasyonel Risk Kapsamında Sınırlı Düzenlemeler
MAKEDONYA	ISO 17799 Baz Alınmıştır
SLOVAKYA	Her Yıl Bilgi Sistemleri Güvenliğini Kapsayacak Bir Denetim Raporu
DANİMARKA	Finansal Denetimin Yanında Sistem, Operasyon, Veri ve İş Devamlılığı Denetimi
PORTEKİZ	Üç Yılda Bir BS Denetimi Yapılmasını Zorunlu Kılan Kanun Tasarısı
İSRAİL	ISO 17799 Baz Alınmıştır
HOLLANDA	Sınırlı Anlamda BS Denetimi'ne de Referansta Bulunan Standardlar
İTALYA	Sınırlı Anlamda Kontrolleri İçeren Düzenlemeler
SLOVENYA	ISO 17799 Baz Alınmıştır
YUNANISTAN	BS Denetimi'ne de Değinen Bankacılık İle İlgili İki Kanun
ALMANYA	Almanya Denetim Kuruluşu (IDW) Tarafından Geliştirilen PS 330 Standardı



Bankacılıkta BS Denetimi / BDDK Hazırlıkları (I)

- 2004 yılında başlandı (Teşkilat Yönetmeliği Değişikliği)
- Örgüt yapısı yenilendi
- BS Denetimi ekibi oluşturuldu
- FFIEC, COBIT, BS7799, ITIL, COSO, standartları ve yaklaşımları incelendi
- Bankalar BT envanteri anket çalışması yapıldı



Bankacılıkta BS Denetimi



Bankacılıkta BS Denetimi / BDDK Hazırlıkları (II)

- Uzman ve uzman yardımcıları için sertifikasyon sağlanması
- Eğitim çalışmaları sürdürüldü
 - UEKAE: Sınır güvenliği, Windows güvenliği, MS sistemleri güvenliği, UNIX/LINUX güvenliği, Veritabanı Güvenliği, Web Uygulamaları Güvenliği, Bilgi Sistemleri Adli İnceleme
 - ISACA Training Week (Network Security, DB Audit, IT Audit practice)
 - MIS: SOX for IT Audit, How to audit automated application controls



Bankacılıkta BS Denetimi (II)

- Bankalarda Bağımsız Denetim Kuruluşlarınca gerçekleştirilecek Bilgi Sistemleri Denetimine ilişkin Yönetmelik (Yönetmelik)
- Rapor Formatı Hakkında Tebliğ
- Yönetmelik kapsamında bağımsız denetim kuruluşlarının yetkilendirilmesi



Bankacılıkta BS Denetimi (III)

- 2005 yılında sınırlı kapsamlı Uygulama Kontrolleri denetimi gerçekleştirildi
- Yönetmelik kapsamında 2006 yılı denetimleri gerçekleştiriliyor; bulgular Nisan 2007 de raporlanacak
- BDDK olay bazlı 6 adet kuruluş denetimi gerçekleştirdi



Bankacılıkta BS Denetimi / Gelecek Planları

Kısa Vadeli

- 2006 denetim raporlarının değerlendirilmesi ve bulgularla ilgili önlemlerin alınması
- BDDK'nın BS Denetimleriyle ilgili yol haritası oluşturuluyor.
- Normlar Tebliği

Orta Vadeli

- Bankalar Bilgi Teknolojileri Envanteri çalışmasının olgunlaştırılması ve periyodikleştirilmesi
- BDDK BS denetimlerinin planlanması ve gerçekleştirilmesi



Bankacılıkta BS Denetimi / Temel Prensipler (I)

- Üç saç ayağı
 - İç denetim
 - Bağımsız Denetim
 - Kamusal Denetim

- Denetçiler arası İşbirliği

- Tek başlılık
 - Denetim alanlarının bütünselliği
 - Sorumlulukların Tespiti



Bankacılıkta BS Denetimi / Temel Prensipler (II)

■ Risk odaklı denetim

- Üstlenilen Riskler (Bankalar risk almak zorundadır)
- Oluşturulan Süreçler Politikalar

■ Süreç denetimi yaklaşımı



Bankacılıkta BS Denetimi / Yönetmelik - (Ana Başlıklar)

- Yetkilendirme ve Meslek Mensupları
- Tarafların Yükümlülükleri
- Bilgi Sistemleri Denetimi
- Genel İlkeler ve Sorumluluklar



Bankacılıkta BS Denetimi / Yönetmelik - (Ana Başlıklar II)

- Denetlenenin Destek Hizmeti Alması ve Bunların Denetimi
- Bilgi Sistemleri Denetiminde İşbirliği
- Bilgi Sistemleri Denetiminde Dış Hizmet Alımı
- Bilgi Sistemleri Denetimi Raporu ve Bildirimi



Bankacılıkta BS Denetimi / Yönetmelikte BS Denetimi (I)

- Finansal Denetim ile BS Denetiminde bütünsellik
- Bağımsız Denetim Şirketlerinin, BS denetimini dış kaynak kullanımı yoluyla gerçekleştirebilmesi
- BS Denetimi Türleri;
 - uygulama kontrollerinin denetimi,
 - genel kontrol alanlarının denetimi,
 - genel kontroller ile uygulama kontrollerinin birlikte gerçekleştirildiği geniş kapsamlı denetim



Bankacılıkta BS Denetimi / Yönetmelikte BS Denetimi (II)

■ Etik kurallar

- Ticari ilişki
- Denetçilerin bankalarda görev alması

■ Denetim Takvimi

- Uygulama Kontrolleri her yıl ve Genel Kontroller iki yılda bir yapılır.
- Kurul özelleştirilmiş denetim isteyebilir.

■ Benimsenen Denetim Çerçevesi COBIT



Benimsenen Denetim Çerçevesi: **COBIT**



Benimsenen Denetim Çerçevesi: COBIT

■ Neden COBIT ?

- Süreç denetimi odaklı
- Süreç tesisine yönelik ve bütüncül yaklaşım
- Dengeli ve hiyerarşik yapılandırılmış alanlar
- Ölçme ve Derecelendirme Mekanizması
- Etkili Kurumsal Yönetişim aracı (Yönetilebilirliğin sağlanması)
- Teknolojiden bağımsız
- ISO 17799, ITIL, SOX, COSO yaklaşımlarına uygun
- AB Mevzuatında uygunluğuna onay verilen BS yönetişim çerçevelerinden biri



COBIT vs ISO 17799

(Kaynak : ISACA)

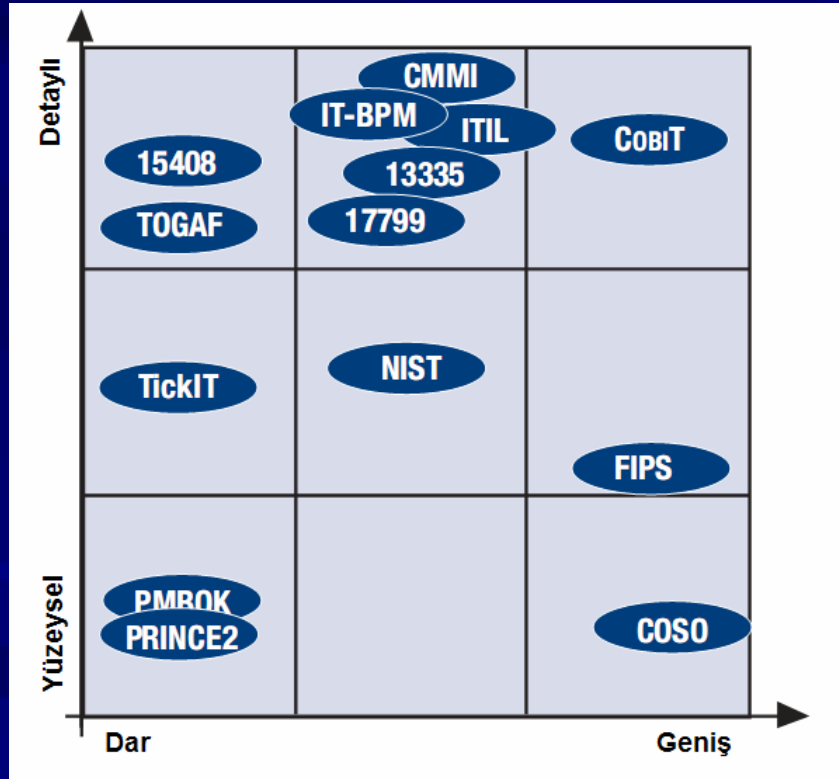
COBIT	ISO 17799
Kurumsal Yönetişim	Bilgi Güvenliği Odaklı
İş Strateji ve Süreçlerinin Değerlendirilmesi	Bilgi Güvenliği Standardı
Ölçüm Yöntemi	Güvenlik Kontrollerinin Değerlendirilmesi

Not: ISACA'ya göre %100 uyumlu, beraber kullanılabilirler

Standart Kapsamları

Kaynak: ISACA

Standartların kapsamlarına göre sınıflandırılması



Diğer standartlarda kapsanan COBIT Alanları

	PO	AI	DS	ME
COSO	+	+	0	0
ITIL	0	0	+	-
ISO/IEC 17799	0	+	+	0
FIPS PUB 200	0	+	+	0
ISO/IEC 13335	0	0	0	-
ISO/IEC 15408	-	0	-	-
PRINCE2	0	-	-	-
PMBOK	0	-	-	-
TickIT	-	+	-	0
CMMI	-	+	-	0
TOGAF 8.1	0	-	-	-
IT BPM	0	-	0	-
NIST 800-14	0	+	+	0

(+): Değinilen Alanlar (O): Kısmen Değinilen Alanlar

(-) : Nadir Değinilen veya Değinilmeyen alanlar



BS Denetiminde Güçlükler (I)

- Uygulanan denetim araçlarının ve metotlarının çeşitliliği, tam standardizasyonun sağlanamamış olması
- Önemlilik (Materyalite) tanımının belirlenmesi
- Mesleki mevzuat eksikliği
- Bankalara yönelik 'Uyulması Gereken Kriterler Seti' eksikliği
- Görüş vermedeki güçlük



BS Denetiminde Güçlükler (II)

- Yetişmiş eleman eksikliği
 - Örgütlenme eksikliği
 - Sertifikasyon zorunlu tutulamıyor
- Finansal/BS Denetçileri ortak çalışma gerekliliği
- Konunun tüm taraflar (Denetçi, Denetlenen, Otorite) için ve uluslararası arenada yeni olması



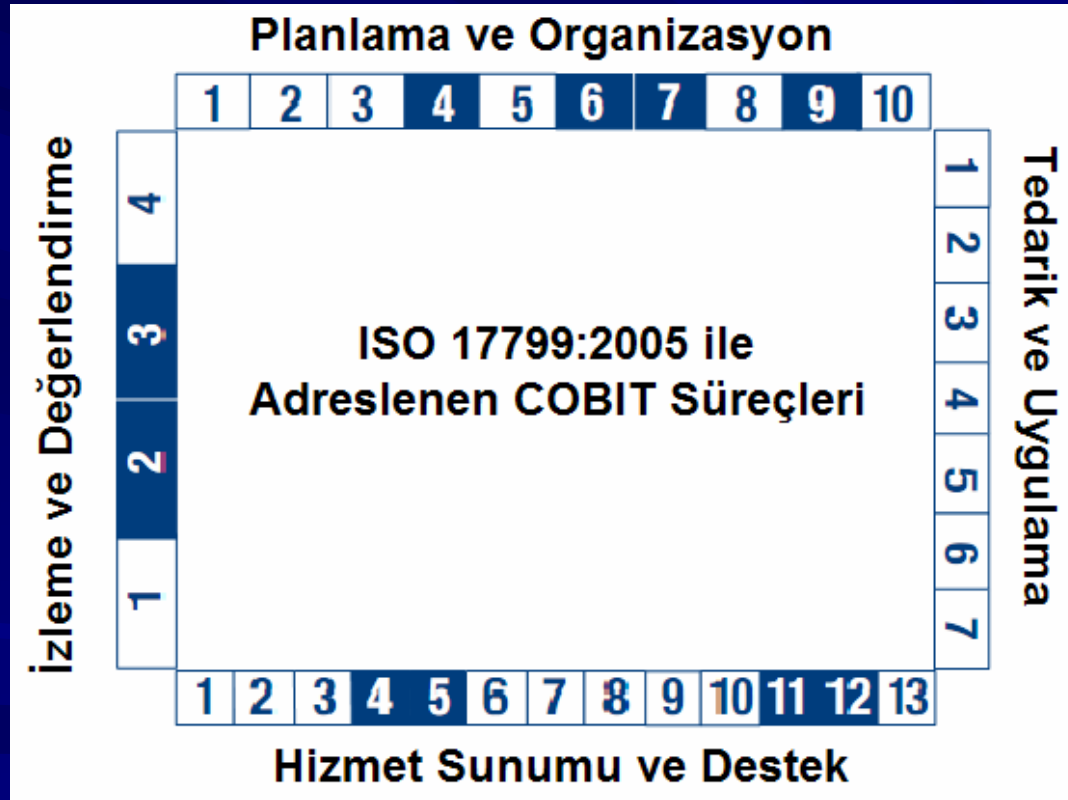
COBIT ve Bilgi Güvenliđi

DS5

- Hizmet sunumu ve destek faaliyetleri 5 (DS5) :
Sistem güvenliğinin sağlanması
 - BT güvenliğinin yönetilmesi
 - BT güvenlik planı
 - Kimlik Yönetimi
 - Kullanıcı hesapları yönetimi
 - Güvenlik testleri ve takibi
 - Güvenlik olaylarının tanımlanması
 - Güvenlik teknolojilerinin korunması
 - Kripto Anahtar yönetimi
 - Zararlı yazılımların önlenmesi, tespiti ve düzeltilmesi
 - Ağ güvenliği
 - Gizli bilgilerin paylaşımı



ISO 17799 ile paralel COBIT süreçleri ve COBIT bilgi kriterleri



Bilgi Kriteri
- Etkinlik
- Verimlilik
+ Gizlilik
+ Bütünlük
+ Erişilebilirlik
+ Uyumluluk
o Güvenilirlik

ISO 17799'da

(+): Bulunan

(O): Kısmen Bulunan

(-) : Nadiren değinilmiş ya da bulunmayan



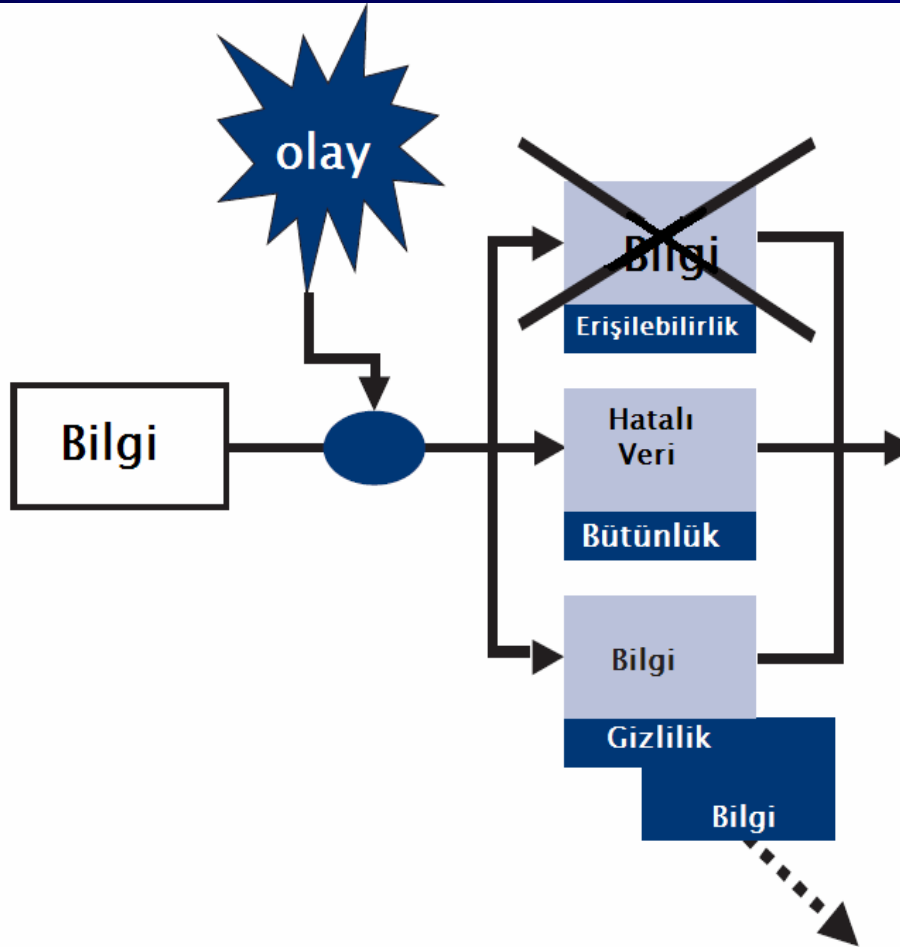
COBIT Security Baseline

- COBIT Güvenlik temeli (COBIT Security Baseline) : Güvenliğe doğru 39 adım
 - Risklerin değerlendirilmesi
 - Değişiklik yönetimi
 - Servisin sürekliliğinin sağlanması
 - Sistem güvenliğinin sağlanmasıgibi başlıklar altında toplanmış 39 adım
- BT güvenliğinin sağlanması için atılması gereken adımlar, rehber
- Her adımın COBIT'te ve ISO17799'daki yeri



Bankacılıkta Bilgi Güvenliđi

Bilgi Güvenliđi / Gizlilik, bütünlük, erişilebilirlik (CIA)



Muhtemel Sonuçlar

- Rekabette dezavantaj
- İş kaybı
- İtibar kaybı
- Motivasyon kaybı
- Sahtekarlık
- Yanlış yönetim kararları
- Servislerde kesinti
- Yasal sorunlar
- Gizli verilerin açığa çıkması



Bilgi Güvenliđi / Bankacılık Mevzuatı (I)

■ 5411 sayılı Bankacılık Kanunu, Madde 73:

“...Kurumun bu fıkra kapsamında elde edeceđi bilgi ve belgeler hiçbir kiři kurum ve kuruluřa verilemez. ...

Bankaların ortakları, yönetim kurulu üyeleri, mensupları, bunlar adına hareket eden kişiler ile görevlileri, sıfat ve görevleri dolayısıyla öğrendikleri ***bankalara veya müşterilerine ait sırları***, bu konuda kanunen açıkça yetkili kılınan mercilerden başkasına açıklayamazlar. Bankaların destek hizmeti aldığı kuruluş ve çalışanları hakkında da bu hüküm uygulanır. Bu yükümlülük görevden ayrıldıktan sonra da devam eder.”



Bilgi Güvenliđi / Bankacılık Mevzuatı (II)

■ 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu, Madde 23:

“Üye işyerleri, kartın kullanımı sonucunda kart ve kart hamili ile ilgili edindikleri bilgileri, kanunla yetkili kılınan kişi, kurum ve kuruluşlar hariç olmak üzere ***kart hamilinin yazılı rızasını almadan başkasına açıklayamaz, saklayamaz ve kopyalayamaz.*** Üye işyerleri, kart bilgilerini üye işyeri anlaşması yaptığı kuruluş dışındaki şahıs veya kuruluşlarla paylaşamaz, satamaz, satın alamaz ve takas edemez. Üye işyeri anlaşması yapan kuruluşlar, bu fıkranın uygulanmasını gözetmekle yükümlüdür.

Kart çıkaran kuruluşlar, edindikleri ***kişisel bilgileri gizli tutmak,*** kendi hizmetlerinin pazarlanması dışında başka amaçlarla kullanmamak ve kanunla yetkili kılınan kişi, kurum ve kuruluşlar dışında kalanların ***bu bilgilere ulaşmasını engellemek amacıyla gereken önlemleri almakla*** yükümlüdür.”



Bilgi Güvenliđi / Bankacılık Mevzuatı (III)

■ Bankaların İç Sistemleri Hakkında Yönetmelik Madde 11: Bilgi sistemlerinin tesisi

- Bilgi sistemleri asgari olarak bankayla ilgili tüm bilgilerin elektronik ortamda güvenli bir şekilde saklanılmasına ve kullanılmasına imkan verecek bir yapıda tesis edilir.
- Bilgi sistemlerinin güvenilirliğinin sağlanması ve düzenli olarak güncellenerek gerekli deđişikliklerin yapılması zorunludur.
- İş süreklilik ve beklenmedik durum planları oluşturulmalı ve dönemsel olarak test edilmelidir.



Bilgi Güvenliđi / Bankacılık Mevzuatı (IV)

- Bankaların destek hizmeti almalarına ve bu hizmeti verecek kuruluşların yetkilendirilmesine ilişkin Yönetmelik

Madde 5:

“Destek hizmeti sağlayan kuruluşlarca *bankaya ve müşterilerine ait sırların* korunmasına yönelik gerekli tedbirlerin alınmasını sağlamak, destek hizmeti alan ilgili bankanın sorumluluğundadır.”

Madde 9:

Bankalar ile destek hizmetleri kuruluşları arasında imzalanacak sözleşmelerde;

...

Destek hizmeti kurulusu tarafından sağlanan hizmet dolayısıyla öğrenilen bankalara ve müşterilerine ait bilgi ve belgelerin, yapılan anlaşmada belirtilen amaçlar dışında kullanılmasının ve üçüncü kişilere açıklanmasının yasak olduğu, destek hizmeti kurulusunun söz konusu bilgi ve belgelerin korunmasında gerekli özeni göstermekle yükümlü bulunduğu ve bunlara aykırılık halinde banka tarafından sözleşmenin tek tarafı olarak feshedileceđi hususlarının belirtilmesi,

...

zorunludur.



Bilgi Güvenliđi / Diđer Ülke Uygulamaları

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995
- - Gramm-Leach-Bliley Act - Financial Privacy (ABD)
- - Federal Data Protection Act / BDSG (Almanya)
- Data Protection Act 1998 (İngiltere)



Bilgi Güvenliđi Politikası'nın İçermesi Gereken Konular

- Eriřim denetimi (Elektronik/Fiziksel)
- Őifreleme
- Bilgiler üzerinde yapılan deđiřikliklerin belli sũreçler dahilinde gerçekteřtirilmesi
- Çapraz kontrol/görevler ayrılıđı
- Sızma teőebbüslerini tespiti yönelik sistemler
- Saldırı cevap planları
- Doğal afetlere (yangın, su basması, deprem, teknolojik sorunlar) karşı alternatifli sũreklilik planları
- Personel eđitimi
- Güvenlik programına iliřkin kontrollerin periyodik testi
- Harici hizmet sađlayıcılar ile iliřkilerin yönetilmesi



Bilgi Güvenliđi Politikası

- Bilgi güvenliđi sadece bilgi sistemleri yönetiminin problemi deđildir, kurumsal politika dahilinde yönetilmesi gerekir
- Bilgi bir varlık olarak deđerlendirilmeli, gizliliđi, bütünlüđü ve kullanıma hazırlığına yönelik tehditlere önlemler alınmalıdır
- Farkındalık ve eđitim önemli, bankalar müşterilerini bilgilendirmeli ve eđitmeli
- Banka müşterileri elektronik güvenliğin önemini kavramalı, bilgisayarlarında gerekli önlemleri almalı (virüs, keylogger tehditleri gibi)



Elektronik Bankacılık İçin Risk Yönetim Prensipleri (I)*

- Güvenlik kontrollerinin oluşturulması
- Harici hizmet almaya ilişkin risklerin yönetilmesi
- İnternet üzerinden işlem yapmanın getirdiği risklerin yönetilmesi
- İnkâr edememe (e-imza, vb.)
- Görevlerin ayrıştırılması
- Kimlik doğrulama kontrolleri ve yetkilendirme
- Tutulan kayıtlar ve bilgiler için bütünlük
- Olayları takibe yetecek düzeyde log tutma
- Gizlilik
- Mevzuata uyum (müşteri mahremiyeti vb.)
- İş sürekliliği
- Saldırı cevap planları

* BIS'in Temmuz 2003 tarihli "Risk Management Principles for Electronic Banking" dokümanından



Elektronik Bankacılık İçin Risk Yönetim Prensipleri (II)

- Güvenlik öncelikli konulardan
- Pek çok ülkede bilgi güvenliğine ilişkin mevzuat mevcut
- Çözüm : (Uygulanan) İyi Bir “Bilgi Güvenliği Politikası”



Normlar Tebliđi (I)

(Taslak)

- Bankalarda BT Yönetiminde esas alınacak ilkeler
 - Genel kontrollerin tesisi (Planlama ve Organizasyon, Tedarik ve Uygulama, Hizmet sunumu ve Destek, İzleme ve Deđerlendirme)
 - Süreç sahipliđi ve süreçlerin izlenebilirliđi
 - Uygulama Kontrollerinin tesisi (Veri kaynak belirleme ve yetkilendirme, veri giriş, veri işleme, veri çıktı ve sınır kontrolleri)



Normlar Tebliği (II)

(Taslak)

- **BT ile ilgili iç kontroller**
 - Yönetimin sorumlulukları
 - Yönetimin İç Kontrollerin Etkinliğini Değerlendirmesi
 - İç kontrollerin denetimi ve denetimlerin raporlanması
 - Bilgi Güvenliği Politikası altında işaret edilen konulara ilişkin kontroller



BDDK'da Bilgi Güvenliđi (I)

- Kullanıcı sözleşmeleri
- Güvenlik politikaları
- Erişim kontrolleri
- Fiziksel güvenlik (Sunucu odasına ve yedekleme merkezine fiziksel erişimin kısıtlanması. Sunucu odasında sıcaklık sensörü)
- Teknik ekipte görevler ayrılığı ilkesinin benimsenmesi
- Firewall, IDS, Content Filtering, DMZ, VPN yapıları



BDDK'da Bilgi Güvenliđi (II)

- Virus koruma, veri yedekleme
- Veri aktarımlarında SSL teknolojisinin kullanılması
- Kurum bilgi sistemi kaynaklarına SmartCard aracılığıyla internet üzerinden VPN ile bağlanma
- E-imza uygulamaları (Evrak Yönetim Sistemi)
- UEKAE bağımsız denetimi



İLGİNİZ İÇİN TEŞEKÜRLER

SORULAR