

Bankacılıkta Bilgi Sistemleri Denetimi –BDDK Yaklaşımı– ve Bilgi Güvenliği



Rıfat DEREGÖZÜ

Bankacılık (Bilişim) Uzmanı



UYARI

Bu sunumda ifade bulan görüşler, Kurum dahilinde Bilgi Sistemleri (BS) Denetimi alanında sürdürülen çalışmalar çerçevesinde oluşmuştur. Resmi Kurum görüşünü temsil etmemektedir.



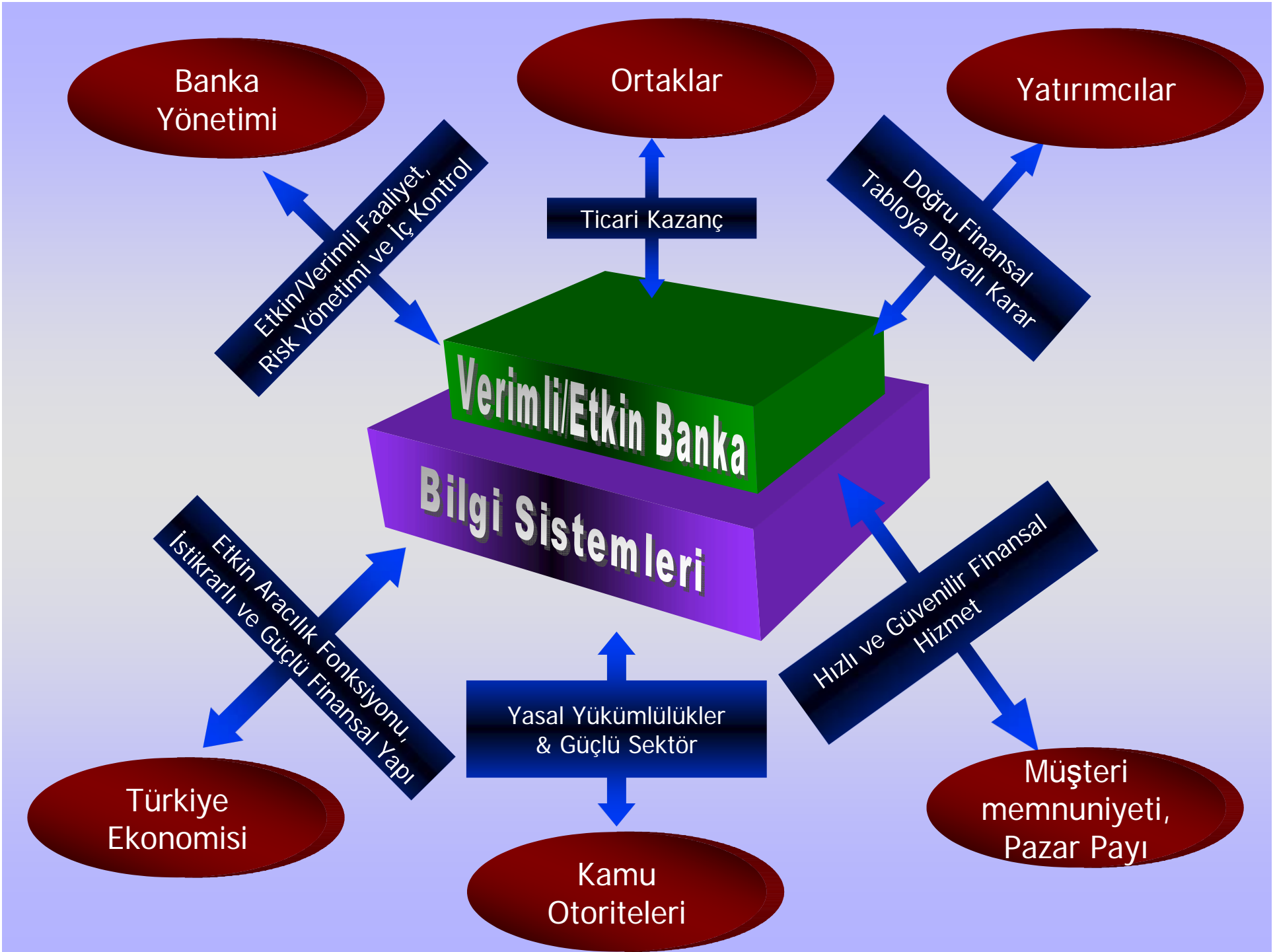
Ajanda

- Bankacılıkta BS Denetimi Gereksinimi
- BDDK Bünyesinde Gerçekleştirilen Çalışmalar – Temel Yaklaşım ve Esas Alınan İlkeler
- Mevcut Durum, 2006 Yılı Denetiminden Bazı Sonuçlar
- Geleceğe İlişkin Planlar
- BDDK Yaklaşımında Bilgi Güvenliğinin Yeri



Ajanda

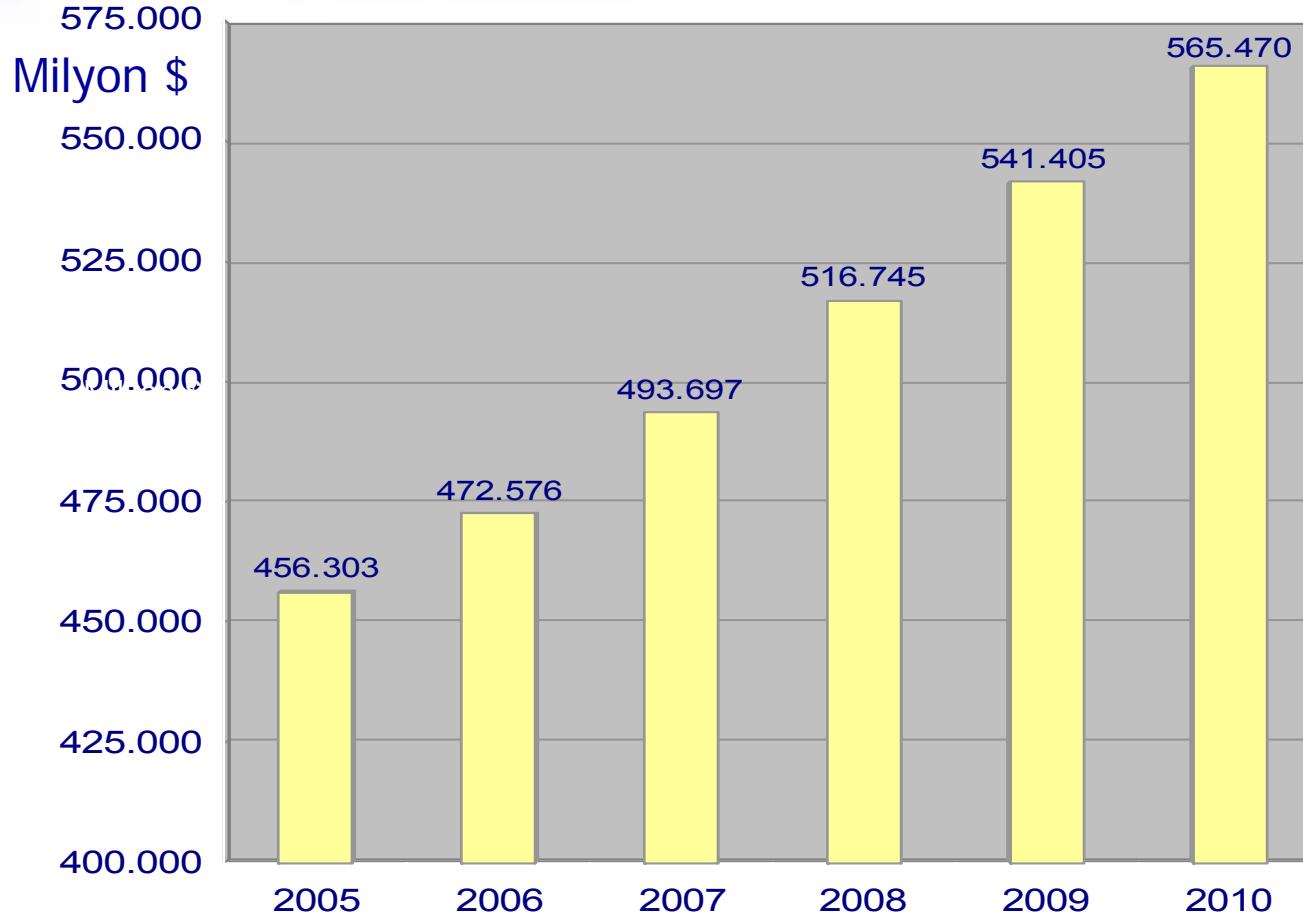
- **Bankacılıkta BS Denetimi Gereksinimi**
- **BDDK Bünyesinde Gerçekleştirilen Çalışmalar – Temel Yaklaşım ve Esas Alınan İlkeler**
- **Mevcut Durum, 2006 Yılı Denetiminden Bazı Sonuçlar**
- **Geleceğe İlişkin Planlar**
- **BDDK Yaklaşımında Bilgi Güvenliğinin Yeri**





Finansal Sektörde 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", 2005-2010, Susan Cournoyer, Gartner, 10 Kasım 2006



BS Yönetiminde

Düzenlemeler Yapılmasını Tetikleyen Olaylar Zinciri



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

- Çift Kayıt Sistemine Bağlı Eksik Yükümlülük Beyanı



Ajanda

- Bankacılıkta BS Denetimi Gereksinimi
- **BDDK Bünyesinde Gerçekleştirilen Çalışmalar – Temel Yaklaşım ve Esas Alınan İlkeler**
- Mevcut Durum, 2006 Yılı Denetiminden Bazı Sonuçlar
- Geleceğe İlişkin Planlar
- BDDK Yaklaşımında Bilgi Güvenliğinin Yeri



BDDK B nyesinde Gerekleřtirilen alıřmalar

- Kurum teřkilat yapılanmasında gerekli deęiřiklik
- Ekibin kurulması, yoęun bir eęitim ve arařtırma faaliyeti
 - Benzer  lke uygulamalarının arařtırılması
 - Muadil kurum yaklařımlarının incelenmesi
- Bankalar BT Envanteri Anket alıřması
- T rkiye řartlarına ve ihtiyalara cevap verebilecek yapının tasarlanması



Temel Yaklaşım ve Esas Alınan İlkeler - I

■ Üçlü Saç Ayağı

- İç Denetim
- Bağımsız Denetim
- Otorite Denetimi

■ Denetçiler Arası İşbirliği

■ Tek Başlılık

- Denetim Alanlarının Bütünselliği (Finansal Denetim + BS Denetimi)
- Sorumlulukların Atanması

Temel Yaklaşım ve Esas Alınan İlkeler - II

- **Risk Odaklı Yaklaşım**
 - Üstlenilen Riskler
 - Tesis Edilen Süreçler ve Politikaların Yeterliliği
- **Süreç Denetimi Yaklaşımı**
- **Bağımsız Denetim Ayağının Devreye Alınması**
- **Bankalarca BS İlişkili Riskleri Yönetmek Üzere Gerekli Önlemlerin Alınması**
- **BS Üzerindeki Kontroller, İç Kontrol Ortamının Önemli Bir Ögesidir**
- **Benimsenen Denetim Çerçevesi : Cobit**

Kavramlar





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 sağlaması)
- Teknolojiden bağımsız
- ISO 17799, ITIL, SOX, COSO yaklaşımlarına uygun
- AB Mevzuatında uygunluğuna onay verilen BS yönetim çerçevelerinden biri



COBIT vs ISO 17799

(Kaynak : ISACA)

CobiT®

Kurumsal Yönetişim

İş Strateji ve Süreçlerinin
Değerlendirilmesi

Ölçüm Yöntemi

ISO 17799

Bilgi Güvenliği

Bilgi Güvenliği Standartı

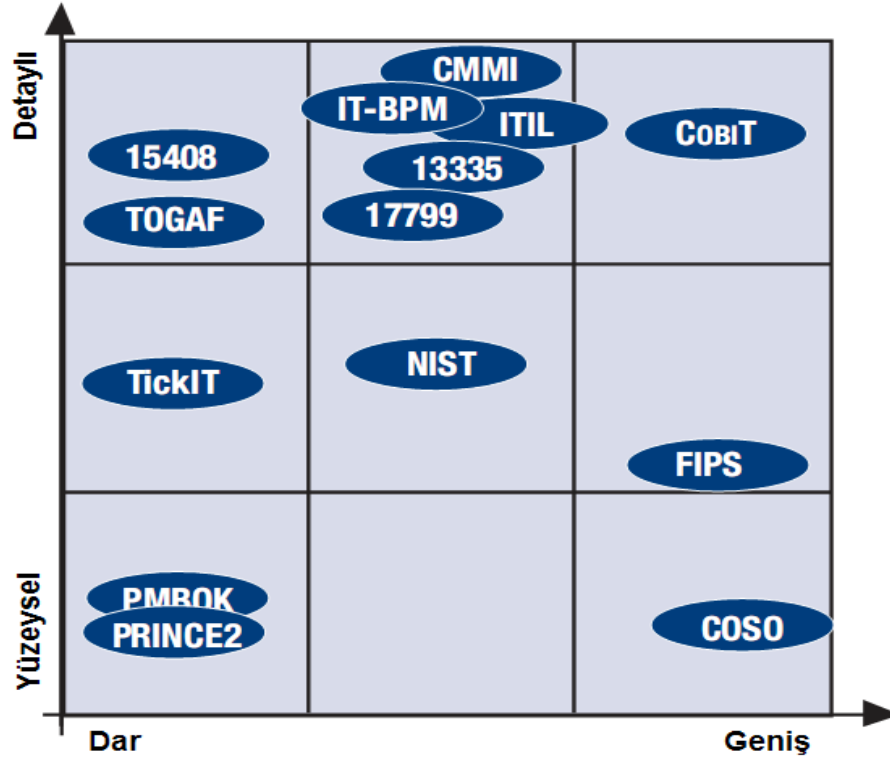
Güvenlik Kontrollerinin
Değerlendirilmesi

★ ISACA'ya göre %100 uyumlular ve beraber kullanılabilirler

Standartların 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



Bağımsız Denetim Ayağı

- 2005 Yılı Sınırlı Kapsamlı BS Denetimi
- Mevzuat Hazırlama Çalışmaları
 - Bağımsız BS Denetimine İlişkin Yönetmelik (Mayıs 2006)
 - Rapor Formatı Tebliği (Aralık 2006)
 - Konsolide Denetime İlişkin Genelge (**Kasım 2007**)
 - Görüş Vermeye Yönelik Düzenleme (**Kasım 2007**)
- Bağımsız Denetim Kuruluşlarının Yetkilendirilmesi
- 2006 Yılı Raporları Değerlendirildi, Bulguların Takibi
- 2006 Yılı Raporlarına Dayalı Genel Değerlendirme
- 2007 Yılı Raporları Gelmeye Devam Ediliyor



Bağımsız BS Denetimine İlişkin Yönetmelikte Öne Çıkan Noktalar-I

- Finansal Denetim ile BS Denetiminde Bütünsellik
- Bağımsız Denetim Şirketlerinin, BS Denetimini Destek Hizmeti Olarak Alabilmeleri
- BS Denetimi Türleri;
 - Uygulama Kontrollerinin Denetimi
 - Genel Kontrol Alanlarının Denetimi
 - Genel Kontroller İle Uygulamam Kontrollerinin Birlikte Denetlendiği Geniş Kapsamlı Denetim
 - Konsolide Bilgi Sistemleri Denetimi



Bağımsız BS Denetimine İlişkin Yönetmelikte Öne Çıkan Noktalar-II

■ Etik Kurallar

- Ticari ilişkiler
- Denetçilerin bankalarda görev alamaması

■ Denetim Takvimi

- Uygulama kontrolleri her yıl, genel kontroller iki yılda bir denetlenir
- Kurul özelleştirilmiş denetim isteyebilir



İç Denetim Ayağı

- İç Sistemler Yönetmeliği (Kasım 2006)
- BS Yönetimine İlişkin İlkeler Tebliği (**Eylül 2007**)



Elektronik Bankacılık İçin Risk Yönetim Prensipleri

- 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

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



Bankacılık BS Yönetiminde Önemli Konu Başlıkları ve Riskler

- Kimlik Doğrulama
- İnkâr Edemezlik
- Güvenlik (Gizlilik)
- Mahremiyet
- Veri Bütünlüğü



Bankacılık BS Yönetiminde Öne Çıkan Teknikler

■ Çok Faktörlü Kimlik Doğrulama

- Müşterinin Bildiği Bir Unsur
- Müşterinin Sahip Olduğu Bir Unsur
- Müşterinin Biyolojik Tekil Bir Özelliği

■ E-İmza

■ Şifreleme



Bankalarca BS Risklerini Yönetmek Üzere Önlemlerin Alınması – İlkeler Tebliği

■ Bilgi Sistemlerine İlişkin Risk Yönetimi

- Yönetim Gözetimi
- Güvenlik Kontrol Sürecinin Tesis Edilmesi ve Yönetilmesi
- Destek Hizmeti Alımı Sürecinin Yönetimi
- Kimlik Doğrulama
- İnkâr Edilemezlik ve Sorumluluk Atama
- Yetkilendirme



Bankalarca BS Risklerini Yönetmek Üzere Önlemlerin Alınması – İlkeler Tebliği

- **Bilgi Sistemlerine İlişkin Risk Yönetimi – *dvm***
 - İşlemlerin, Kayıtların ve Verilerin Bütünlüğü
 - Denetim İzlerinin Oluşturulması
 - Veri Gizliliği
 - Müşterilerin Bilgilendirilmesi
 - Müşteri Bilgilerinin Mahremiyeti
 - Bilgi Sistemlerine İlişkin İş Sürekliliği ve Kurtarma Planı
 - Acil ve Beklenmedik Durum Planı



Bankalarca BS Risklerini Yönetmek Üzere Önlemlerin Alınması – İlkeler Tebliği

Bilgi Sistemlerine İlişkin İç Kontrollerin Tesisi ve Takibi

- Uygulama Kontrolleri
- Genel Kontroller (Cobit)



Bankalarca BS Risklerini Yönetmek Üzere Önlemlerin Alınması – İlkeler Tebliği

Özellik Arz Eden İşlemler

- İnternet Bankacılığı
- ATM



İlkeler Tebliği - Zorluklar

- E-İmzanın beklenen yaygınlık seviyesine ulaşmamış olması
- Teknolojinin gelişen ve değişen yapısı
- Halka açık ortam (İnternet)
- Müşteri bilincinin arttırılması



Otorite Denetimi Ayađı

- Olay bazlı denetim faaliyetleri
- Denetim rehberleri tamamlanma aşamasında
- Hazırlanacak planlar doğrultusunda yıl içerisinde denetimlere başlanması hedeflenmektedir



Ajanda

- Bankacılıkta BS Denetimi Gereksinimi
- BDDK Bünyesinde Gerçekleştirilen Çalışmalar – Temel Yaklaşım ve Esas Alınan İlkeler
- **Mevcut Durum, 2006 Yılı Denetiminden Bazı Sonuçlar**
- Geleceğe İlişkin Planlar
- BDDK Yaklaşımında Bilgi Güvenliğinin Yeri

İlgili Mevzuat

- Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik
- Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimine İlişkin Rapor Formatı Hakkında Tebliğ
- Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ
- Bankaların İç Sistemleri Hakkında Yönetmelik
- İlgili diğer genelge ve talimatlar

Mevcut Durum

- **Bankalarda BS Yönetimine İlişkin Çerçeve Tanımlı**
 - İki Yıllık Geçiş Süresi Tanındı (2010 başı)
- **Bağımsız Denetim Çerçevesi Tanımlı**
- **Otorite Denetimine Yönelik Hazırlıklar Sonlanma Aşamasında**



Diğer Kamu Kurumlarında BS Denetimi Hazırlıkları

- Sayıştay
- Sermaye Piyasası Kurumu
- Sosyal Güvenlik Kurumu
- Diğer ...



Bağımsız Denetim Raporlarından Bazı Sonuçlar (2006 Yılı Denetimi)

- 25 bankada toplam 93 bilgi sistemleri denetçisi bulunmaktadır.
- Geriye kalan 25 bankada bilgi sistemleri denetçisi yok.
- 22 tanesi CISA, 1 CISM, 2 CIA ve 6 CISSP sertifikalı
- Bankaların yeni bilgi sistemleri denetçisi alımına ilişkin çalışmaları da mevcut.



Uygulama Kontrolleri Denetimi

(2006 Yılı Denetimi)

- Uygulama Kontrolleri denetimi kapsamı Bağımsız Denetim Kuruluşlarınca önemlilik kriterine göre belirlenmektedir.
- Hazine, Kurumsal Krediler ve Mevduat Süreçleri en çok seçilen süreçler
- Önemlilik kriterleri
 - Finansal tablolara etkisi
 - İşlem sıklığı
 - Muhtemel hataların finansal, operasyonel ve itibar riski



Genel Kontroller Denetimi

(2006 Yılı Denetimi)

En Çok Denetlenen Kontrol Hedefleri

- Bilgi sistemleri riskinin değerlendirilmesi (PO9)
- Otomasyon çözümlerinin belirlenmesi (AI1)
- Değişiklik yönetimi (AI6)
- Sistem çözümlerinin ve değişikliklerin uygulanması ve akredite edilmesi (AI7)
- Üçüncü kişilerden alınan hizmetlerin yönetimi (DS2)
- Hizmet sürekliliğinin sağlanması (DS4)
- Sistem güvenliğinin sağlanması (DS5)
- Veri yönetimi (DS11)
- Fiziksel çevre yönetimi (DS12)
- Operasyon yönetimi (DS13)
- İç kontrolün izlenmesi ve değerlendirilmesi (ME2)



Ajanda

- Bankacılıkta BS Denetimi Gereksinimi
- BDDK Bünyesinde Gerçekleştirilen Çalışmalar – Temel Yaklaşım ve Esas Alınan İlkeler
- Mevcut Durum, 2006 Yılı Denetiminden Bazı Sonuçlar
- **Geleceğe İlişkin Planlar**
- BDDK Yaklaşımında Bilgi Güvenliğinin Yeri

- Raporlanan bulguların etkin takibi
- Bağımsız denetim firma çalışmalarının etkin takibi
- Kurum eliyle denetimlere başlanması
- İlgili personel sayısını yeterli düzeye taşıyarak, denetimlerin genişletilmesi
- Kurum denetim felsefesinin geliştirilmesi
- Gelişmelere göre denetim kalitesinin sürekli iyileştirilmesi



Ajanda

- Bankacılıkta BS Denetimi Gereksinimi
- BDDK Bünyesinde Gerçekleştirilen Çalışmalar – Temel Yaklaşım ve Esas Alınan İlkeler
- Mevcut Durum, 2006 Yılı Denetiminden Bazı Sonuçlar
- Geleceğe İlişkin Planlar
- **BDDK Yaklaşımında Bilgi Güvenliğinin Yeri**



Bilgi Güvenliđi

- Cobit ve Bilgi Güvenliđi
- Bankacılıkta Bilgi Güvenliđi
- Kurumumuzda Bilgi Güvenliđi



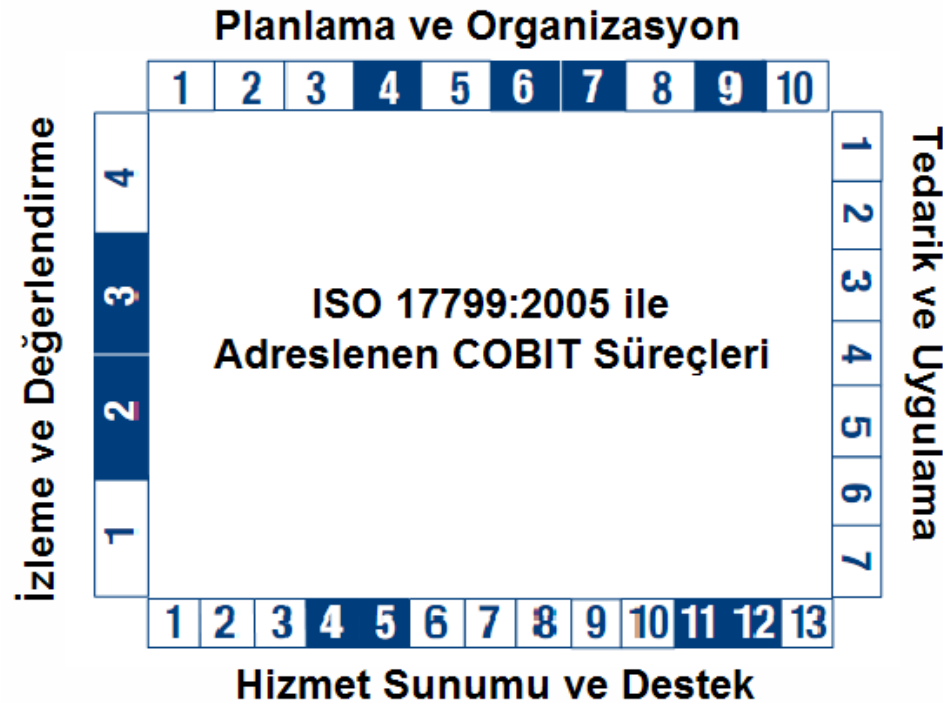
Cobit ve Bilgi Güvenliği - I

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 Paylaşılması

Cobit ve Bilgi Güvenliği - II

ISO 17799:2005 ile Paralel Cobit Süreçleri ve Cobit Bilgi Kriterleri



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

ISO 17799'da

(+): Bulunan

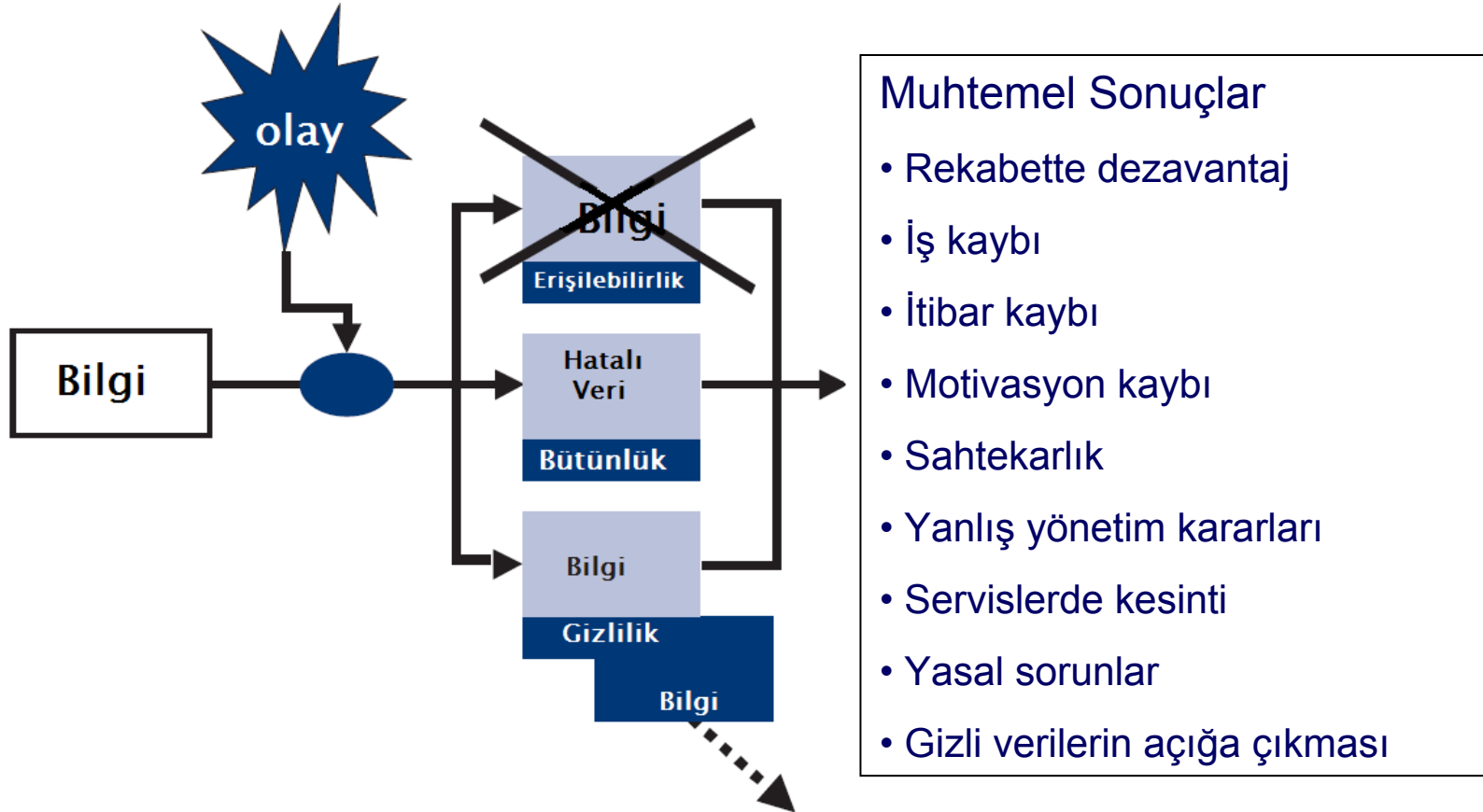
(O): Kısmen Bulunan

(-) : Nadiren değinilmiş ya da bulunmayan

Kaynak ve detaylı bilgi için: COBIT Mapping: Mapping ISO/IES 17799:2005 With COBIT 4.0
<https://www.isaca.org/Template.cfm?Section=Downloads3&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=63&ContentID=13742>

Bankacılıkta Bilgi Güvenliği - I

Gizlilik, Bütünlük, Erişilebilirlik (CIA)





Bankacılıkta Bilgi Güvenliđi - II

5411 sayılı Bankacılık Kanunu, Madde 73:

“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 yükümlölük görevden ayrıldıktan sonra da devam eder.”



Bankacılıkta Bilgi Güvenliği - II

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

“Üye işyerleri, kartın kullanımını 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.”



Bankacılıkta Bilgi Güvenliđi - III

Bankaların İ 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 güvenilirliđinin sağlanması ve düzenli olarak güncellenerek gerekli deđişikliklerin yapılması zorunludur.
- İş süreklilik ve beklenmedik durum planları oluşturulmalı ve dönemsel olarak test edilmelidir.



Bankacılıkta Bilgi Güvenliği - 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 feshedileceği hususlarının belirtilmesi,

...

zorunludur.



Bankacılıkta Bilgi Güvenliđi - V

Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliđ

- Güvenlik kontrol sürecinin tesis edilmesi ve yönetilmesi (Madde 7)
- Kimlik doğrulama (Madde 9)
- İnkâr edilemezlik ve sorumluluk atama (Madde 10)
- Görevler ayrılıđı prensibi (Madde 11)
- Yetkilendirme (Madde 12)
- İşlemlerin, kayıtların ve verilerin bütünlüğü (Madde 13)
- Denetim izlerinin oluşturulması (Madde 14)
- Veri gizliliđi (Madde 15)
- Müşteri bilgilerinin mahremiyeti (Madde 17)
- Bilgi sistemlerine ilişkin iş sürekliliđi ve kurtarma planı (Madde 18)
- Acil ve beklenmedik durum planı (Madde 19)
- İnternet Bankacılıđı için benzer hükümler (Madde 26, 27, 28, 29 ve 31)
- ATM güvenliğine yönelik düzenlemeler (Madde 32)
- Kablosuz haberleşme teknolojileri (Madde 33)



Kurumumuzda 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, VPN yapıları



Kurumumuzda Bilgi Güvenliği - 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



ilginiz için teşekkürler..

Rıfat DEREGÖZÜ

BDDK / Bankacılık (Bilişim) Uzmanı

sorular?

