

Bankacılıkta Bilgi Sistemleri Yönetimi ve Denetimi/ Mevzuat Çerçevesinde BDDK Perspektifi



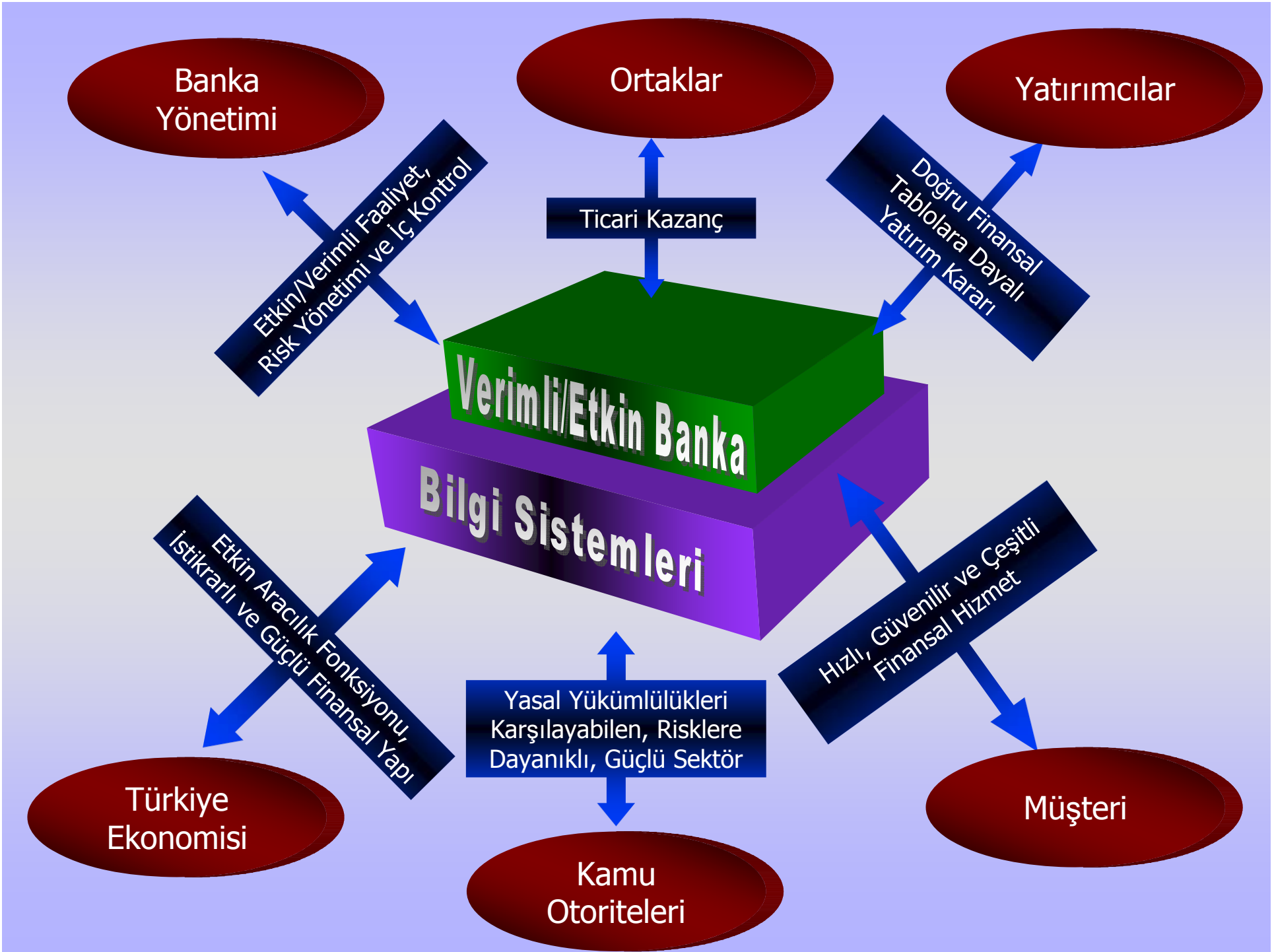
Ahmet Türkay VARLI
Bilgi Yönetimi Daire Başkanı / BDDK

Türkiye İç Denetim Enstitüsü, XI. Türkiye İç Denetim Kongresi
9 Kasım 2007, İstanbul



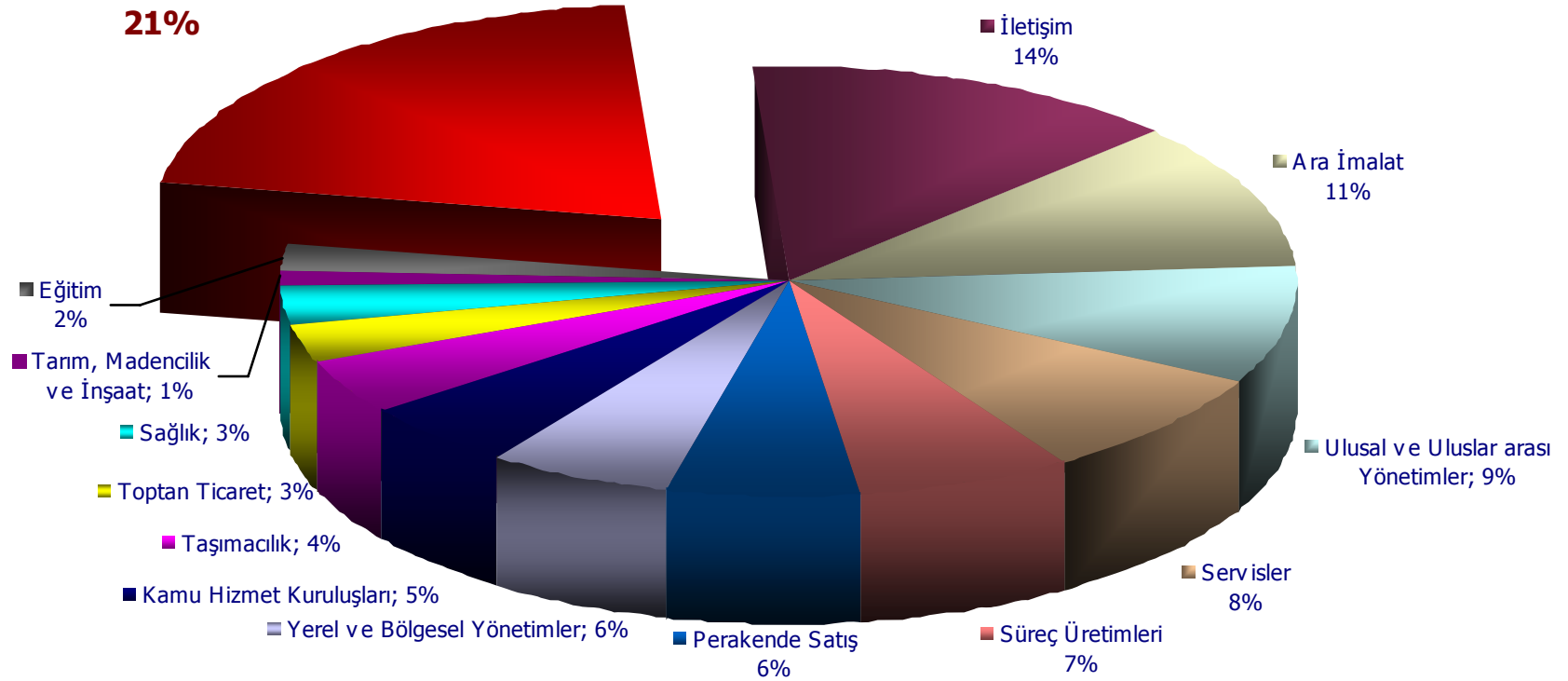
Ajanda

- **Bankacılıkta Bilgi Sistemleri (BS) ve Denetim Gereksinimi**
- **Bankacılıkta BS Yönetimi**
- **Bankacılıkta BS Denetimi**
- **Benimsenen Denetim Çerçevesi : CobiT®**



Bankacılıkta Bilgi Sistemleri Sektörel BT Harcamaları

■ Finansal Servisler 21%

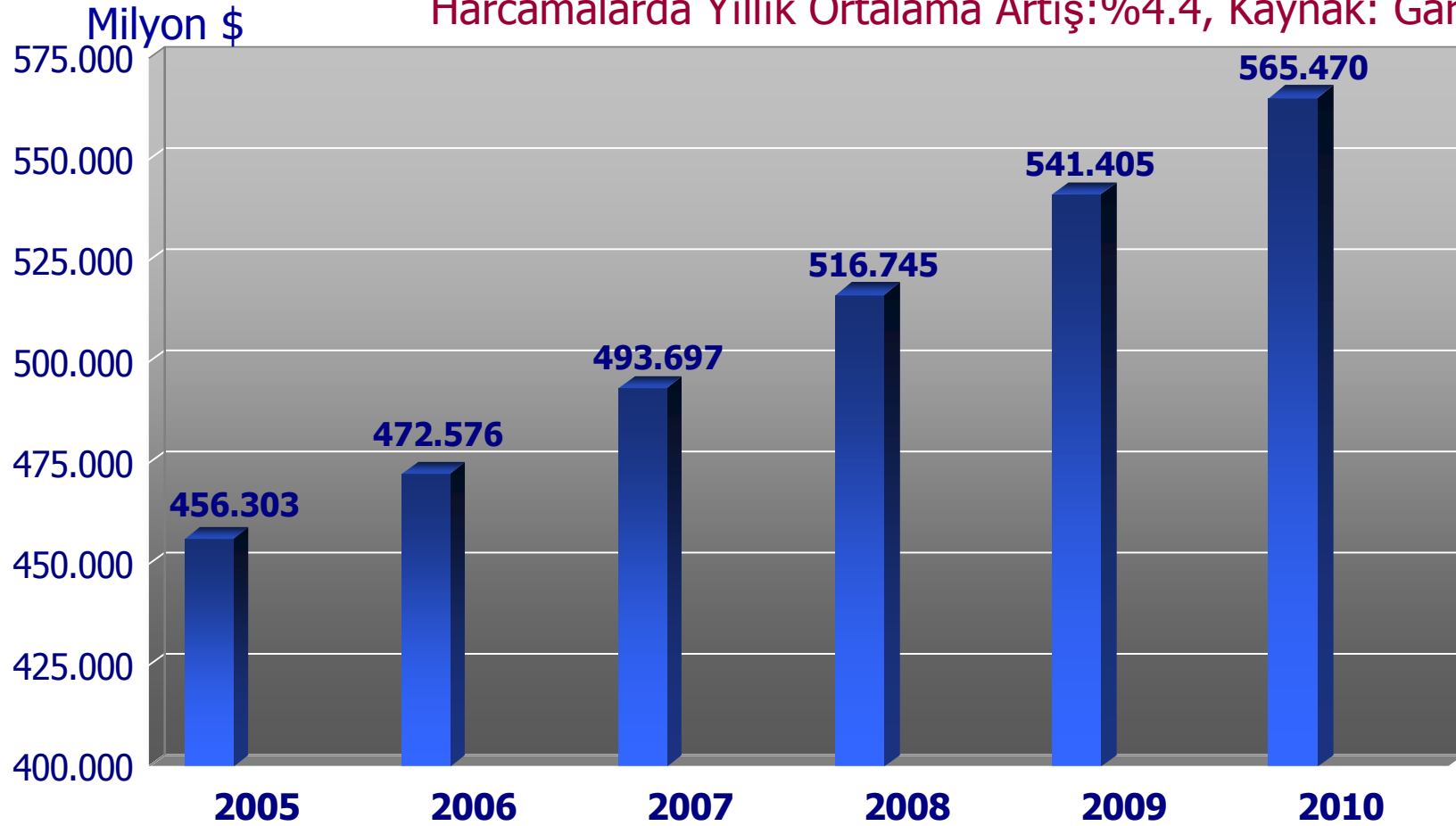


**KAYNAK: Dataquest Insight Financial Services Sector IT
Spending Forecast, 2005-2010, Susan Cournoyer, 10 Kasım 2006**



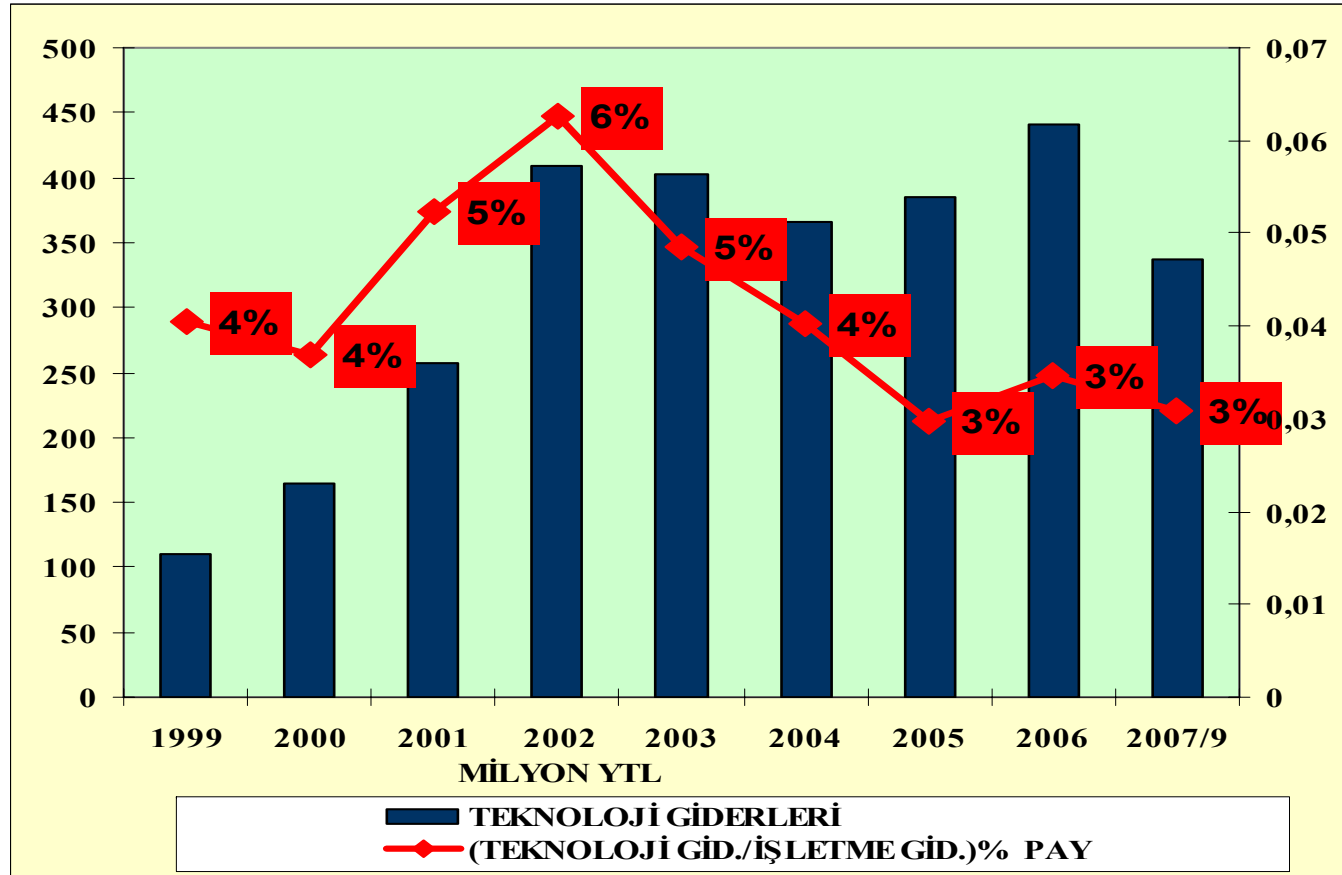
Bankacılıkta Bilgi Sistemleri Dünyada Finansal Sektörün BT Harcamaları

Harcamalarda Yıllık Ortalama Artış:%4.4, Kaynak: Gartner



Kaynak: "Dataquest Insight: Financial Services Sector IT Spending Forecast", 2005-2010, Susan Cournoyer, Gartner, 10 Kasım 2006

Bankacılıkta Bilgi Sistemleri Türk Bankacılık Sektörünün BT Harcamaları ve İşletme Giderleri



* BT Harcamaları için 880054, 880055, 88009, 88109 hesaplar kullanılmıştır.



Bilgi Sistemlerinde Önemli Olaylar



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



WorldCom

- Finansal Bilgi Raporlamasında Sahtekarlık



Enron

- Finansal Bilgi Raporlamasında Sahtekarlık
- 60 Milyar USD Kamu Zararı



İmar Bankası

- Çift Kayıt Sistemine Bağlı Eksik Yükümlülük Beyanı



Bankacılıkta Bilgi Sistemleri Düzenleme Çalışmaları

- İki alanda yoğunlaşma;
 - Bilgi sistemlerinin yönetimi
 - Bilgi sistemleri denetimi



Bankacılıkta Bilgi Sistemlerinin Yönetimine İlişkin Mevzuat



Bilgi Sistemleri Yönetiminde Düzenleyici Mevzuat

5411 sayılı
Bankacılık Kanunu

Bankaların
Destek
Hizmeti
Almalarına
İlişkin
Yönetmelik

Bankaların İç Sistemleri
Hakkında Yönetmelik

Bankalarda Bilgi Sistemleri Yönetiminde
Esas Alınacak İlkelerle İlişkin Tebliğ



BS Yönetiminde Düzenleyici Mevzuat 5411 sayılı Bankacılık Kanunu(I)

■ Madde 29:

Bankalar etkin;

- İç kontrol
- Risk Yönetimi ve
- İç Denetim

sistemleri kurmak ve işletmekle yükümlüdür.



BS Yönetiminde Düzenleyici Mevzuat

5411 sayılı Bankacılık Kanunu(II)

■ Madde 30:

Bankalar, iç kontrol sistemi kapsamında;

- Faaliyetlerin mevzuata uygun yürütülmesini
- Muhasebe ve finansal raporlama sisteminin bütünlüğünü, güvenilirliğini ve bilgilerin zamanında elde edilebilirliğini
- Görevlerin fonksiyonel ayrımlarını ve sorumlulukların paylaşımını
- Varlıkların ve yükümlülüklerin kontrol altında tutulmasını sağlayacak bir altyapıyı kurmak zorundadır.



BS Yönetiminde Düzenleyici Mevzuat

5411 sayılı Bankacılık Kanunu(III)

■ Madde 41:

Yönetim Kurulu,

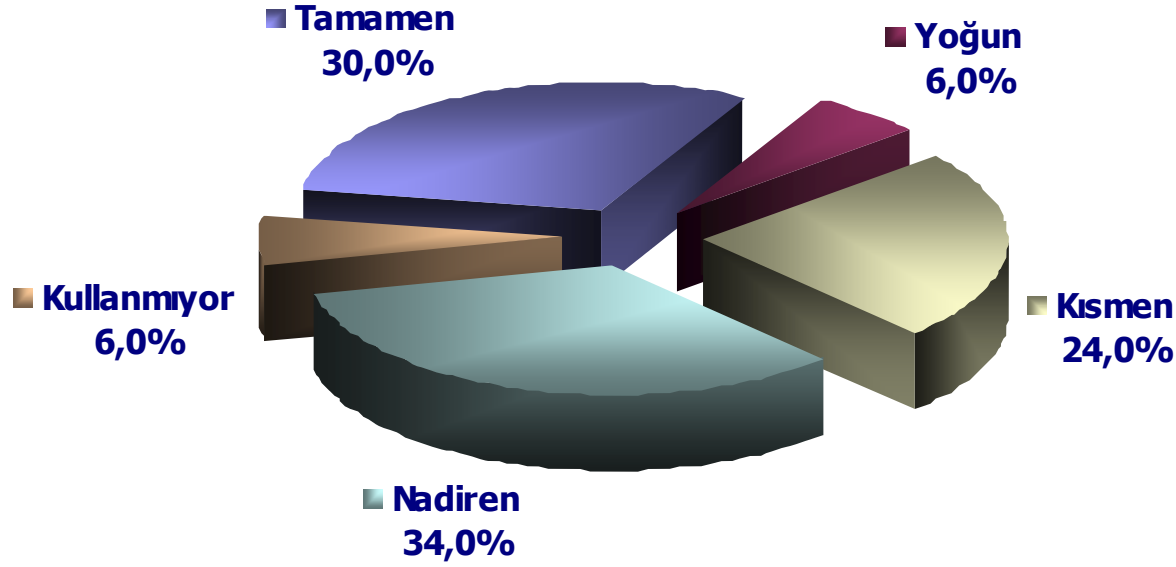
- faaliyetlerin mevzuata uygun muhasebeleştirilmesi,
- Finansal raporlama sistemini görev, yetki ve sorumluluklarının belirlenmesi ve
- Bilgi sistemlerinin yeterli hale getirilmesi ve uygulamanın gözetlenmesi ile yükümlüdür.



BS Yönetiminde Düzenleyici Mevzuat Destek Hizmeti Alımına İlişkin Yönetmelik

- Destek hizmeti alımında ön koşullar (Md 5)
- Destek hizmeti kuruluşlarında aranacak şartlar (Md 6)
- Sözleşmenin unsurları (Md 9)
- Destek hizmeti alınan kuruluşlarda denetim hakkı (Md 12)
- Mesleki sorumluluk sigortası (Md 10)

Bankacılık Bilgi Sistemlerinde Destek Hizmeti Kullanımı (2006)



- ❖ Bilgi sistemlerinde destek hizmeti kullanmayan banka oranı sadece **%6**'dır.
- ❖ Bankaların **%94**'ü en az bir faaliyetini gerçekleştirmek için destek hizmeti almaktadır.
- ❖ Tamamen destek hizmeti olarak yürüten bankaların çoğunluğunu **yabancı bankalar** teşkil etmektedir.
- ❖ Destek hizmeti kullanmayan 3 banka ise kalkınma ve yatırım bankalarıdır.



BS Yönetiminde Düzenleyici Mevzuat İç Sistemler Yönetmeliği

- İç kontrol, iç denetim ve risk yönetimi fonksiyonları
- İşlevsel görev ayrımı (Md 10)
- Bilgi sistemlerinin asgari tesis etmesi gereken noktalar (Md 11)
- Acil ve beklenmedik durum planları (Md 13)
- İletişim kanallarının ve bilgi sistemlerinin kontrolü (Md 16)



Bankacılıkta BS Yönetimi

Bankalarda Bilgi Sistemleri Yönetiminde
Esas Alınacak İlkelere İlişkin Tebliğ

(+İnternet Bankacılığı)



BS Yönetimi/İlkeler Tebliği Hazırlıkları Diğer Ülke Yaklaşımları

- **Düzenleme (Regulation)**
- **Kılavuz (Guideline)**
- **Sertifikasyon (WebTrust, BBBOnline, TrustUK,...)**



BS Yönetimi/İlkeler Tebliği Hazırlıkları

Diğer Ülke Yaklaşımları (II)

Ülke	Kurulus	Tanim	Kategorisi
ABD	AICPA	WebTrust / SysTrust	Audit / Certification / Guideline
ABD	FFIEC	E-Banking	Handbook
ABD	OCC	Internet Banking Audit Program	Guideline
ABD	ISACA	IS Auditing Guidance Internet Banking Document G24	Guideline
ABD	FFIEC	Authentication in an Internet Banking Environment	Guidance
ABD	OCC	Final Rule on Electronic Banking	Regulation
ABD	OCC, FRS, FDIC, OTS	Guidelines Establishing Standards for Safeguarding Customer Information	Guideline
EU	BIS	Risk Mgmt Princ. For E-Banking	Guideline
EU	BIS	Cross Border Electronic Activities	Guidance
EU	ECBS	Security Guidelines for E-Banking	Guideline
EU	COMMISSION OF THE EUROPEAN COMMUNITIES	transactions by electronic payment instruments and in particular the relationship between issuer and holder	Regulation / Recommendation



BS Yönetimi/İlkeler Tebliği Hazırlıkları

Diğer Ülke Yaklaşımları (III)

Ülke	Kurulus	Tanim	Kategorisi
İsveç	UN/EDIFACT Finance Group SWG-F	MESSAGE IMPLEMENTATION GUIDELINE OF THE UN/EDIFACT SECURE AUTHENTICATION & ACKNOWLEDGEMENT MESSAGE	Guideline
İsveç	UN/EDIFACT Finance Group SWG-F	RECOMMENDED PRACTICE FOR MESSAGE FLOW AND SECURITY FOR EDIFACT PAYMENTS	Guideline
Romanya	Ministry of Communication and IT	MCTI 218/2004	Order(Kanun)
Suudi Arabistan	Saudi Arabian Monetary Agency	Internet Banking Security Guidelines	Gudeline
Lubnan	Banque du Liban	Circular no. 1810 to Banks, Financial Institutions and Institutions Dealing with Electronic Banking and Financial Transactions	Circular
Hindistan	Reserve Bank of India	Internet banking in India	Guideline
Singapur	Monetary Authority of Singapore	Internet Banking Technology Risk Management Guidelines	Guideline
Singapur	Monetary Authority of Singapore	TWO-FACTOR AUTHENTICATION FOR INTERNET BANKING	Circular
HongKong	HongKong Monetary Authority	Management of Security Risks in Electronic Banking Services	Guidance
Çin	ICBC- Industrial&Commercial Bank of China	E-banking Regulation	Regulation
Bahama Adalari	The Central Bank of The Bahamas	GUIDELINES FOR ELECTRONIC BANKING	Guideline



BS Yönetimi/İlkeler Tebliği Hazırlıkları Temel Alınan Uluslararası Yaklaşımlar

■ Risk Management Principles for Electronic Banking – Temmuz 2003

*Bank For International Settlements (BIS) – Electronic Banking Group of
Basel Committee on Banking Supervision*

■ Security Guidelines For E-Banking: Application of Basel Risk Management Principles – Ağustos 2004

European Committee For Banking Standards (ECBS)



BS Yönetimi/İlkeler Tebliği Hazırlıkları Elektronik Bankacılık İçin Risk Yönetim Prensipleri (I)*

- Yönetim gözetimi
- Güvenlik kontrol sürecinin tesis edilmesi ve yönetilmesi
- Destek hizmeti alımı sürecinin yönetimi
- Kimlik doğrulama
- İnkâr edilemezlik ve sorumluluk atama
- Yetkilendirme

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



BS Yönetimi/İlkeler Tebliği Hazırlıkları

Elektronik Bankacılık İçin Risk Yönetim Prensipleri (II)*

- İşlemlerin, kayıtların ve verilerin bütünlüğü
- Denetim izlerinin oluşturulması
- Veri gizliliği
- Müşterilerin bilgilendirilmesi
- Müşteri bilgilerinin mahremiyeti
- Bilgi sistemlerine ilişkin iş sürekliliği ve kurtarma planı
- Acil ve beklenmedik durum planı

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



BS Yönetimi/İlkeler Tebliği Hazırlıkları Önemli Konu Başlıkları ve Riskler

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



BS Yönetimi/İlkeler Tebliği Hazırlıkları

Öne Çıkan Teknikler

■ Çok Faktörlü Kimlik Doğrulama

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

■ E-İmza

■ Şifreleme

BS Yönetimi/İlkeler Tebliği

Ana Başlıklar (I)

- **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
 - Görevler ayrılığı ilkesi
 - Yetkilendirme

BS Yönetimi/İlkeler Tebliği

Ana Başlıklar (II)

- **Bilgi Sistemlerine İlişkin Risk Yönetimi - *dvm***
 - İşlemlerin, kayıtların ve verilerin bütünlüğü
 - Denetim izlerinin oluşturulması
 - Veri gizliliği
 - Müşterilerin bilgilendirilmesi
 - Müşteri bilgilerinin mahremiyeti
 - Bilgi sistemlerine ilişkin iş sürekliliği ve kurtarma planı
 - Acil ve beklenmedik durum planı

BS Yönetimi/İlkeler Tebliği

Ana Başlıklar (III)

■ Bilgi Sistemlerine İlişkin İç Kontrollerin Tesisi ve Takibi

- Uygulama Kontrolleri
 - *İş Bilgisi+Uyum+İş Akışları+Kontroller*
- Genel Kontroller (CobIT®)
 - *IT+İş Hedefleri ile*
İlişkilendirme+Uyum+Ölçüm+Kontroller
- Kontrollerin Takibi



BS Yönetimi/İlkeler Tebliği

Ana Başlıklar (IV)

■ Özellik Arz Eden İşlemler

- İnternet Bankacılığına özel hükümler
- ATM Güvenliği
- Kablosuz Haberleşme Teknolojileri

■ Uyum Süreci *(yaklaşık 2,5 yıl)*



BS Yönetimi/İlkeler Tebliğinde Karşılaşılan Zorluklar

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



Ajanda

- **Bankacılıkta Bilgi Sistemleri ve Denetim Gereksinimi**
- **Bankacılıkta BS Yönetimi**
- **Bankacılıkta BS Denetimi**
- **Benimsenen Denetim Çerçevesi : CobiT®**



Bankacılıkta BS Denetimi Mevzuat Çerçevesi

5411 Bankacılık Kanunu

Kamu Denetimi
(BDDK)

İç Denetimi
(Banka)

Bağımsız Denetim
(Bağımsız Denetim Kuruluşları)

İç Sistemler
Yönetmeliği

Bağımsız Denetimce
Gerçekleştirilecek
BS Denetimi Hk. Yönetmelik

Rapor Formatına
İlişkin Tebliğ

Denetim
Kapsamı

Denetimin
Türleri

Denetimin
Yükümlülükleri

Denetim
Yetkilendirmesi

Denetimde
İş Birliği

Önemlilik
İlkesi

Rapor
İçeriği

Bulguların
Sınıflaması

Denetim
Görüşleri

Bankacılıkta BS Denetimi

Temel Prensipler (I)

■ Üçlü saç ayağı

- İç denetim
- Bağımsız Denetim
- Kamu Denetimi

■ Finansal ve bilgi sistemleri denetçileri arasında işbirliği

■ Denetimde Bütünlük

- Denetim alanlarının bütünselliği (Finansal + BS Denetimi)
- Sorumlulukların Tespiti

■ Risk odaklı denetim

- Üstlenilen Riskler
- Oluşturulan Süreçler ve Politikaların Yeterliliği

■ Süreç denetimi yaklaşımı



Bankacılıkta BS Denetimi/Yönetmelik Ana Başlıklar (I)

- Yetkilendirme ve Meslek Mensupları
- Tarafların Yükümlülükleri
- Bilgi Sistemleri Denetimi
 - *uygulama kontrollerinin denetimi,*
 - *genel kontrol alanlarının denetimi,*
 - *genel kontroller ile uygulama kontrollerinin birlikte gerçekleştirildiği geniş kapsamlı denetim*
 - *konsolide bilgi sistemleri denetimi*
- Benimsenen Denetim Çerçevesi: CobIT®



Bankacılıkta BS Denetimi/Yönetmelik Ana Başlıklar (II)

■ Olgunluk seviyesi tespiti

■ Denetim Takvimi

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

■ Genel İlkeler ve Sorumluluklar

- *Sözleşme, bilgilendirme ve belgelendirme*



Bankacılıkta BS Denetimi/Yönetmelik Ana Başlıklar (III)

- **Bankaların Destek Hizmeti Alması ve Destek Firmalarının Denetimi**
- **BS Denetiminde İşbirliği**
- **BS Denetiminde Dış Hizmet Alımı**
- **Etik kurallar**
 - *Ticari ilişkide bulunmama*
 - *Denetçilerin bankalarda görev alamaması*
- **BS Denetimi Raporu ve Bildirimi**



Bankacılıkta BS Denetimi Yapılan Faaliyetler

- Sınırlı kapsamlı Uygulama Kontrolleri denetimi (2005, Yönetmelik öncesi faaliyet)
- Bağımsız denetim kuruluşlarının yetkilendirilmesi (6 yetki + 1 izin)
- Yönetmelik kapsamında 2006 yılı BS denetim faaliyetleri + bulgulara ilişkin takip işlemleri
- BDDK olay bazlı 7 adet kuruluş denetimi gerçekleştirdi
- 2006 yılı BS Denetimi Genel Değerlendirme Raporu



Bankacılıkta BS Denetimi İleriye Dönük Planlar

- **BDDK tarafından BS denetiminin yapılmaya başlanması**
 - Denetim yol haritasının oluşturulması
 - Denetim rehberlerinin hazırlanması
- **Denetçilerarası işbirliğinin sürdürülmesi**



Ajanda

- **Bankacılıkta Bilgi Sistemleri ve Denetim Gereksinimi**
- **Bankacılıkta BS Yönetimi**
- **Bankacılıkta BS Denetimi**
- **Benimsenen Denetim Çerçevesi : CobiT®**



BS Denetimi & CobiT®

- **FFIEC, SOX, PCAOB (AS1, AS2), CobiT®, BS7799, ITIL, COSO standartları ve yaklaşımları**
- **Diğer ülke uygulamaları**



BS Denetimi & CobiT®

Ülke Uygulamaları ve Benimsenen Esaslar

Ülkeler	Benimsedikleri Yaklaşımlar
Finlandiya	“İç Kontrol ve Risk Yönetimi” İle İlgili Geliştirdikleri Kendi Standartları
Norveç	CobiT Baz Alınmıştır
Macaristan	CobiT Baz Alınmıştır
Çek Cumhuriyeti	IT Yönetişimi ve Operasyonel Risk Kapsamında Sınırlı Düzenlemeler
Makedonya	ISO 17799 Baz Alınmıştır
Slovakya	Her Yıl Bilgi Sistemleri Güvenliğini Kapsayacak Bir Denetim Raporu
Danimarka	Finansal Denetimin Yanında Sistem, Operasyon, Veri ve İş Devamlılığı Denetimi
Portekiz	Üç Yılda Bir BS Denetimi Yapılmasını Zorunlu Kılan Kanun Tasarısı
İsrail	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



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

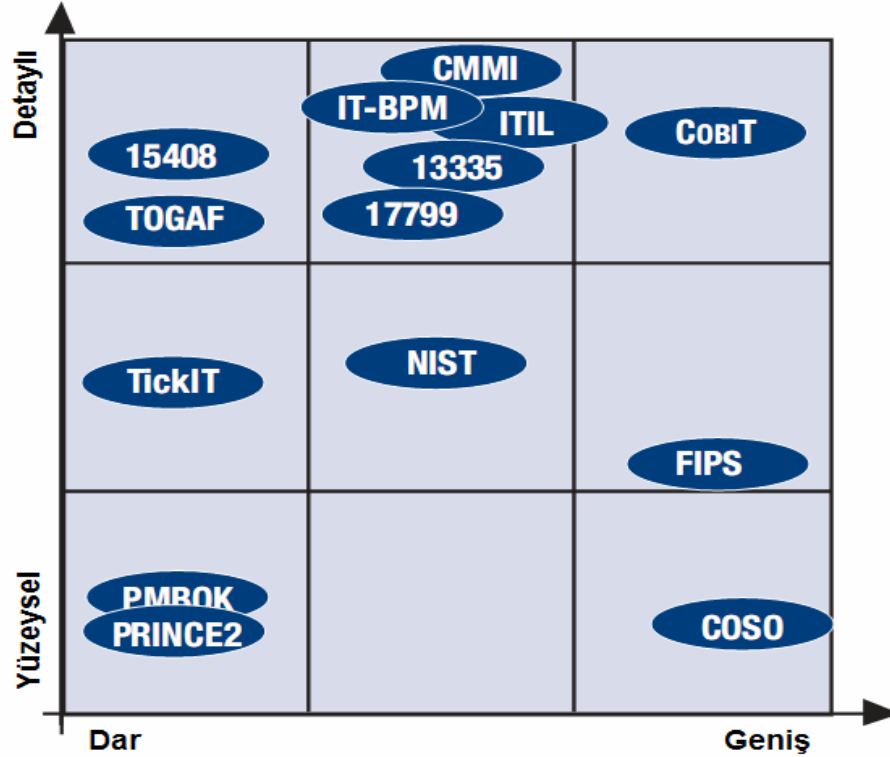
Güvenlik Kontrollerinin
Değerlendirilmesi

Not: ISACA CobiT'i, ISO 17799'a %100 uyumlu ve beraber kullanılabilir olarak tanımlıyor

Standartların Kapsam Karşılaştırması

(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 Denetimini Şekillendiren Yerel Kriterler (I)

- Finansal Denetim ile BS Denetiminin birlikte yapılması zorunluluđu (*dışarıdan destek alabilme imkanı*)
- Bağımsız Denetim Kuruluşlarının Yetkilendirilmesi

BS Denetimini Şekillendiren Yerel Kriterler (II)

- Uygulama Kontrollerinin sektöre özel olarak uyarlanması
- Uygulama kontrolleri ile birlikte denetlenenin iç kontrol ve iç denetim yapısının da değerlendirilmesi
- Konsolide BS Denetimi

Saęlanan Faydalar (I)

- **Mevzuatın oluşması**
- **Meslek örgütü tanımının ve ihtiyacının gündeme gelmesi**
- **Finansal denetimin kalitesinin ve sağladığı güvencenin artması**

Sağlanan Faydalar (II)

- **Kamu denetim kurumlarının, denetim yaklaşımlarını tekrar gözden geçirmelerini tetiklemesi**
- **Kamuda bu alanda gerçekleştirilecek çalışmalar için kaynak teşkil etmesi**
- **E-devlet altyapısının etkin olarak tesis edilebilmesine sağlayacağı katkı**

ilginiz için teşekkürler..

Ahmet Türkay Varlı

BDDK / Bilgi Yönetimi Daire Başkanı

sorular?

