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

BANKACILIKTA BİLGİ SİSTEMLERİ MEVZUATI VE DENETİMİ

Mustafa Turan

BANKACILIK UZMANI

UYARI

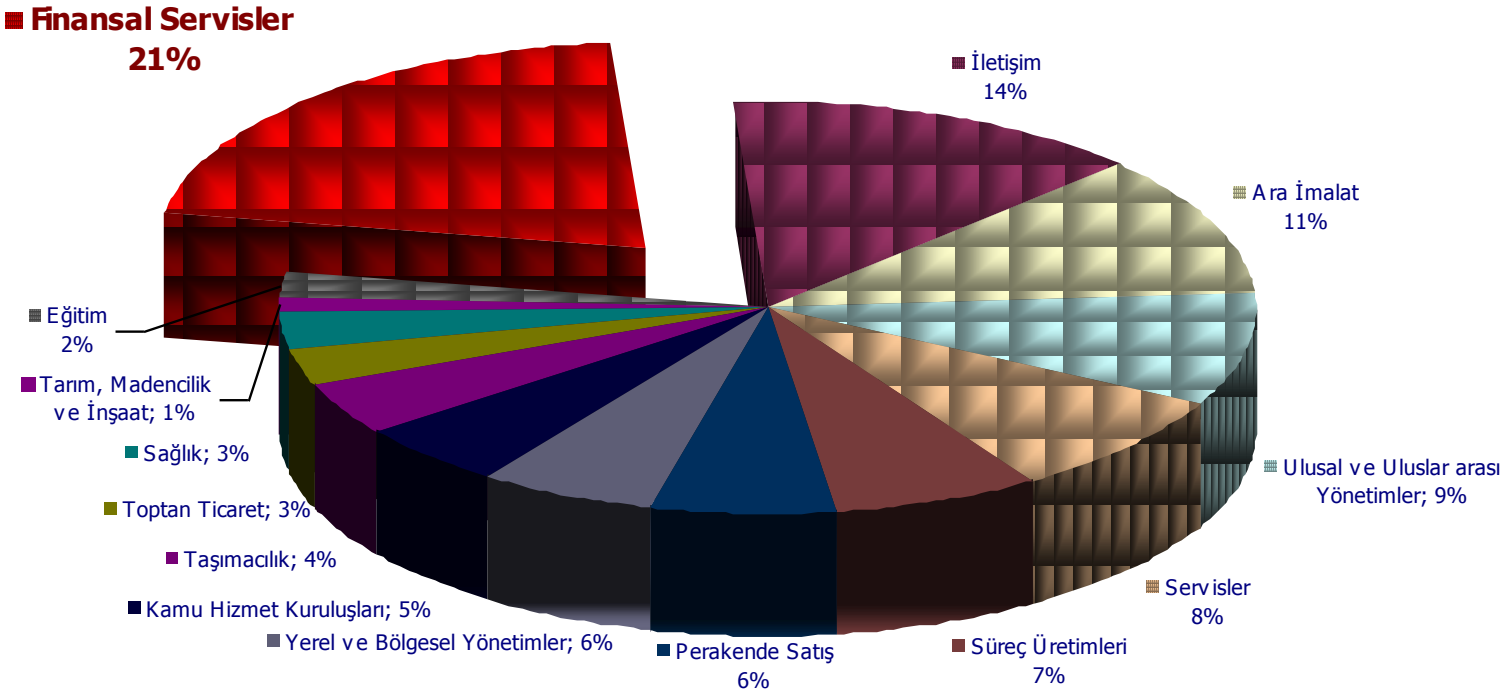
Bu sunumda ifade bulan görüşler, Kurum dahilinde Bilgi Sistemleri (BS) Denetimi ve güvenliği alanında sürdürülen çalışmalar çerçevesinde oluşturulmuştur. Resmi Kurum görüşünü temsil etmemektedir.

Konular

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

Bankacılıkta Bilgi Sistemleri

Sektörel BT Harcamaları



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

Bilgi Sistemlerinde
Önemli Olaylar

- at&t
  - 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

Konular

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

Bankacılıkta Bilgi Sistemlerinin Yönetimine İlişkin Mevzuat

Bilgi Sistemleri Yönetiminde
Düzenleyici Mevzuat

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)

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)

İlkeler Tebliği
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)

İlkeler Tebliği
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

İlkeler Tebliği
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

İlkeler Tebliği Hazırlıkları
Önemli Konu Başlıkları ve Riskler

- Kimlik Doğrulama
- İnkar Edilemezlik
- Gizlilik
- Mahremiyet
- Veri Bütünlüğü / Tutarlılığı

İlkeler Tebliği Hazırlıkları
Önemli Konu Başlıkları ve Riskler

- Çok Faktörlü Kimlik Doğrulama
  - Müşterinin Bildiği Bir Unsur
  - Müşterinin Sahip Olduğu Bir Unsur
  - Müşterinin Biyolojik Tekil Bir Özelliği
- E-İmza
- Şifreleme

İlkeler Tebliği Hazırlıkları
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
  - Yetkilendirme

İlkeler Tebliği Hazırlıkları
Ana Başlıklar (II)

- Bilgi Sistemlerine İlişkin Risk Yönetimi - *devamı*
  - 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

İlkeler Tebliği Hazırlıkları Ana Başlıklar (III)

- Bilgi Sistemlerine İlişkin İç Kontrollerin Tesisi ve Takibi
  - Uygulama Kontrolleri
  - Genel Kontroller (CobiT®)

İlkeler Tebliği Hazırlıkları
Ana Başlıklar (IV)

- Özellik Arz Eden İşlemler
  - İnternet Bankacılığı
  - ATM

İlkeler Tebliği Hazırlıkları Karşılaşılan Zorluklar

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

BS Yönetiminde Düzenleyici Mevzuat
İç Sistemler Yönetmeliği ve İlkeler Tebliği

- Yeni Değişiklikler (01 Haziran 2010)
  - Birincil ve İkincil Sistemler Tanımları
  - İş sürekliliği hususunun ön plana çıkarılması
  - Bilgi Sistemleri unsurlarının tesis edileceği yer
    - Birincil ve İkincil Sistemler yurtiçinde bulundurulmak zorunda

BS Yönetiminde Düzenleyici Mevzuat
İç Sistemler Yönetmeliği ve İlkeler Tebliği

- Birincil ve İkincil Sistemlerin Yurtiçinde bulundurulması zorunluluğu
  - Neden?
    - Bankaların iş sürekliliğinin yurt içinden sağlanır hale getirilmesi
    - BS'yi de içeren kurumsal bütünlüğün sağlanması
    - Sistemden olası bir çıkış durumunda el değiştirmeyi zorlaştıran hususların bertarafı
    - Etkin denetim
    - Mevzuata uyumun kolaylaştırılması
    - Yurtiçindeki bankacılığa ilişkin teknolojik bilgi ve birikimin korunması

Konular

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

Bankacılıkta BS Denetimi

- Kabul edilen temel prensipler
- Bilgi sistemleri denetimi alanındaki mevzuat
- Ana başlıklarıyla BS Denetimi Yönetmeliği

Bankacılıkta BS Denetimi
Kabul Edilen Temel Prensipler (I)

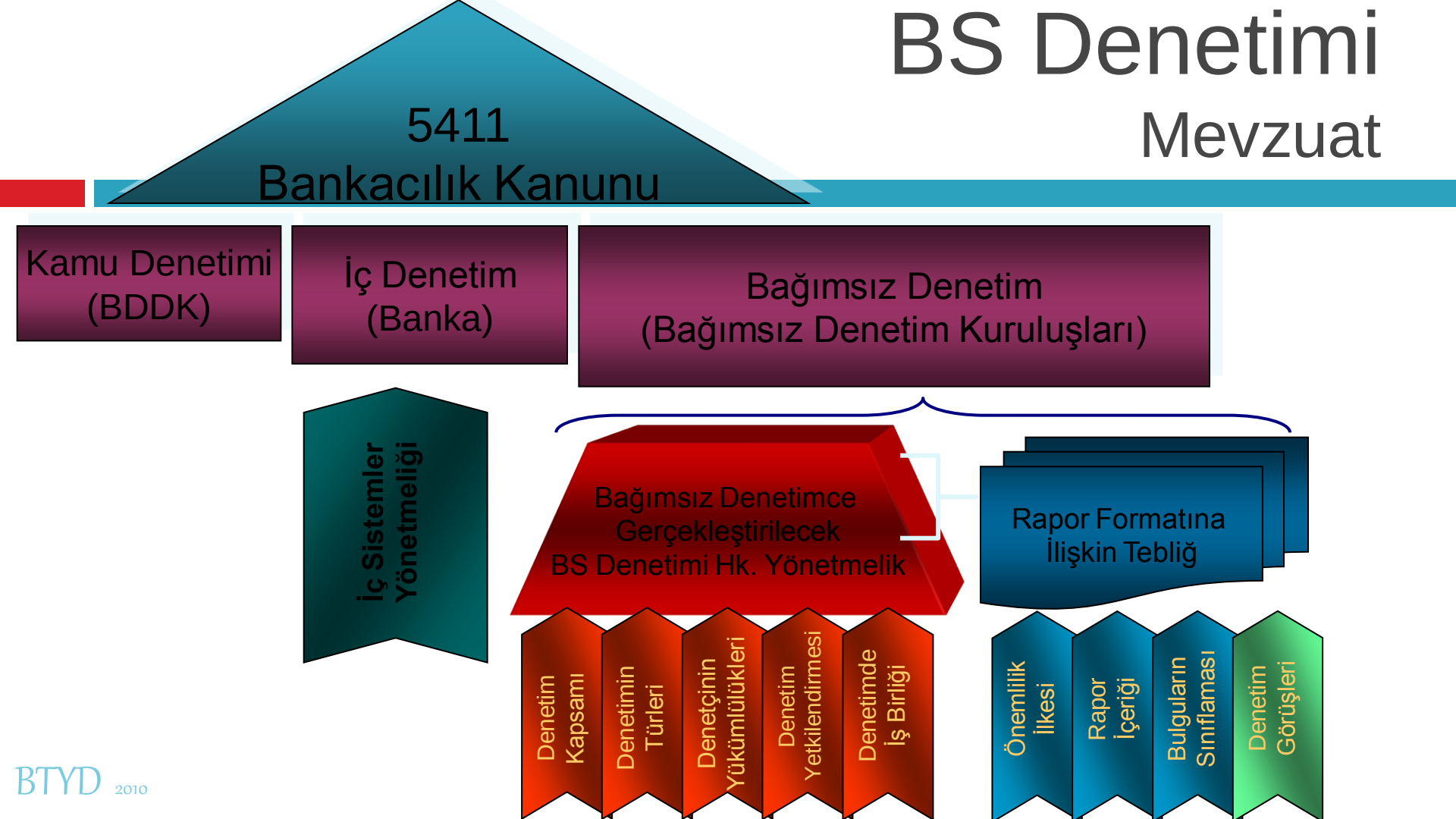
- Üç sac ayağı
  - İç denetim
  - Bağımsız Denetim
  - Kamu Denetimi
- Finansal ve bilgi sistemleri denetçileri arasında işbirliği
- Tek başlılık
  - Denetim alanlarının bütünselliği (Finansal + BS Denetimi)
  - Sorumlulukların Tespiti

Bankacılıkta BS Denetimi
Kabul Edilen Temel Prensipler (II)

- Risk odaklı denetim
  - Üstlenilen Riskler
  - Oluşturulan Süreçler ve Politikaların Yeterliliği
- Süreç denetimi yaklaşımı

BS Denetimi

Mevzuat



BS Denetimi Yönetmeliği
Ana Başlıklar (I)

- Yetkilendirme ve Meslek Mensupları
- Tarafların Yükümlülükleri
- Bilgi Sistemleri Denetimine İlişkin Esaslar
- Genel İlkeler ve Sorumluluklar

BS Denetimi Yönetmeliği
Ana Başlıklar (II)

- Bankaların Destek Hizmeti Alması ve Destek Firmalarının Denetimi
- BS Denetiminde İşbirliği
- BS Denetiminde Dış Hizmet Alımı
- BS Denetimi Raporu ve Bildirimi

BS Denetimi Yönetmeliği
Öne Çıkan Noktalar (I)

- Finansal Denetim ile BS Denetiminde bütünsellik
- Bağımsız Denetim Şirketlerinin, BS denetimini destek hizmeti alabilmeleri
- BS Denetimi Türleri;
  - uygulama kontrollerinin denetimi,
  - genel kontrol alanlarının denetimi,
  - genel kontroller ile uygulama kontrollerinin birlikte gerçekleştirildiği geniş kapsamlı denetim
  - konsolide bilgi sistemleri denetimi

BS Denetimi Yönetmeliği
Öne Çıkan Noktalar (II)

- Etik kurallar
  - Ticari ilişkiler
  - Denetçilerin bankalarda görev alamaması
- Denetim Takvimi
  - Uygulama Kontrolleri her yıl ve Genel Kontroller iki yılda bir yapılır.
  - Kurul özelleştirilmiş denetim isteyebilir.
- Benimsenen Denetim Çerçevesi: CobiT®

Konular

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

Benimsenen Denetim Çerçevesi

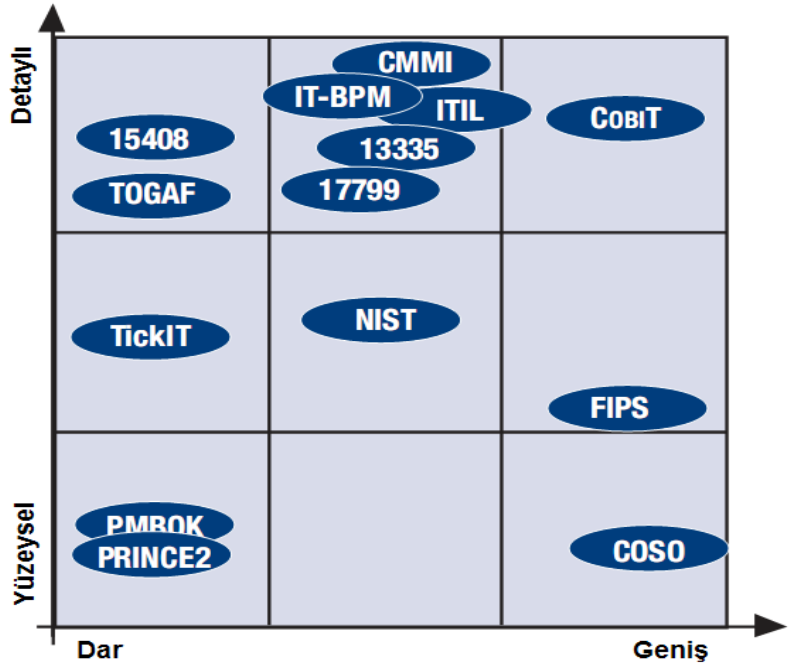
CobiT®

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

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

Teşekkürler

Mustafa TURAN

Bankacılık Uzmanı

BTYD 2010

www.btyd.org