Bağımsız Denetimde Bilgi Sistemleri Denetiminin Rolü

Sinem Cantürk
Şirket Ortağı,
Bilgi Sistemleri Risk Yönetimi Bölüm Başkanı,
KPMG Türkiye

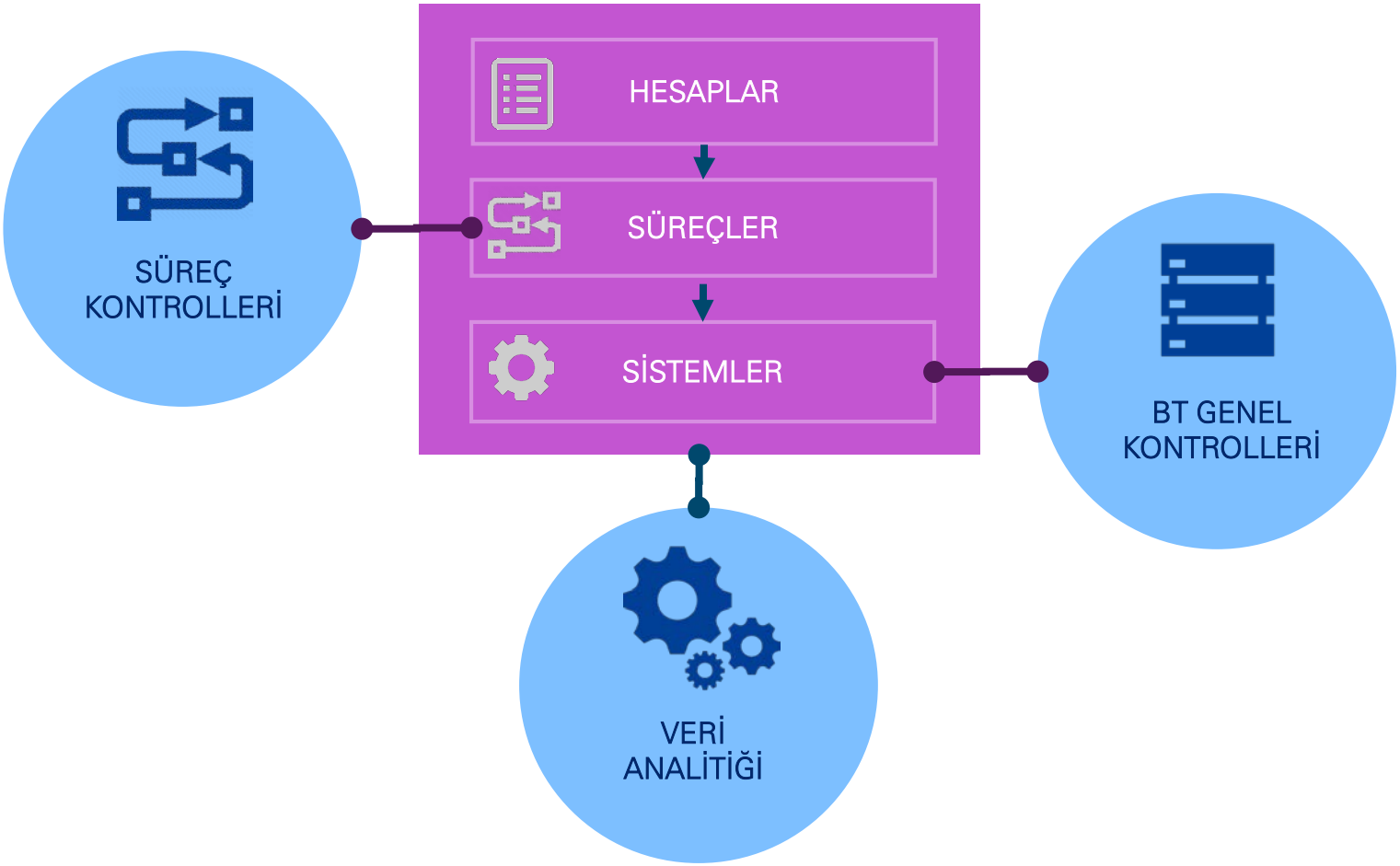
Eylül 2018

GÜNDEM

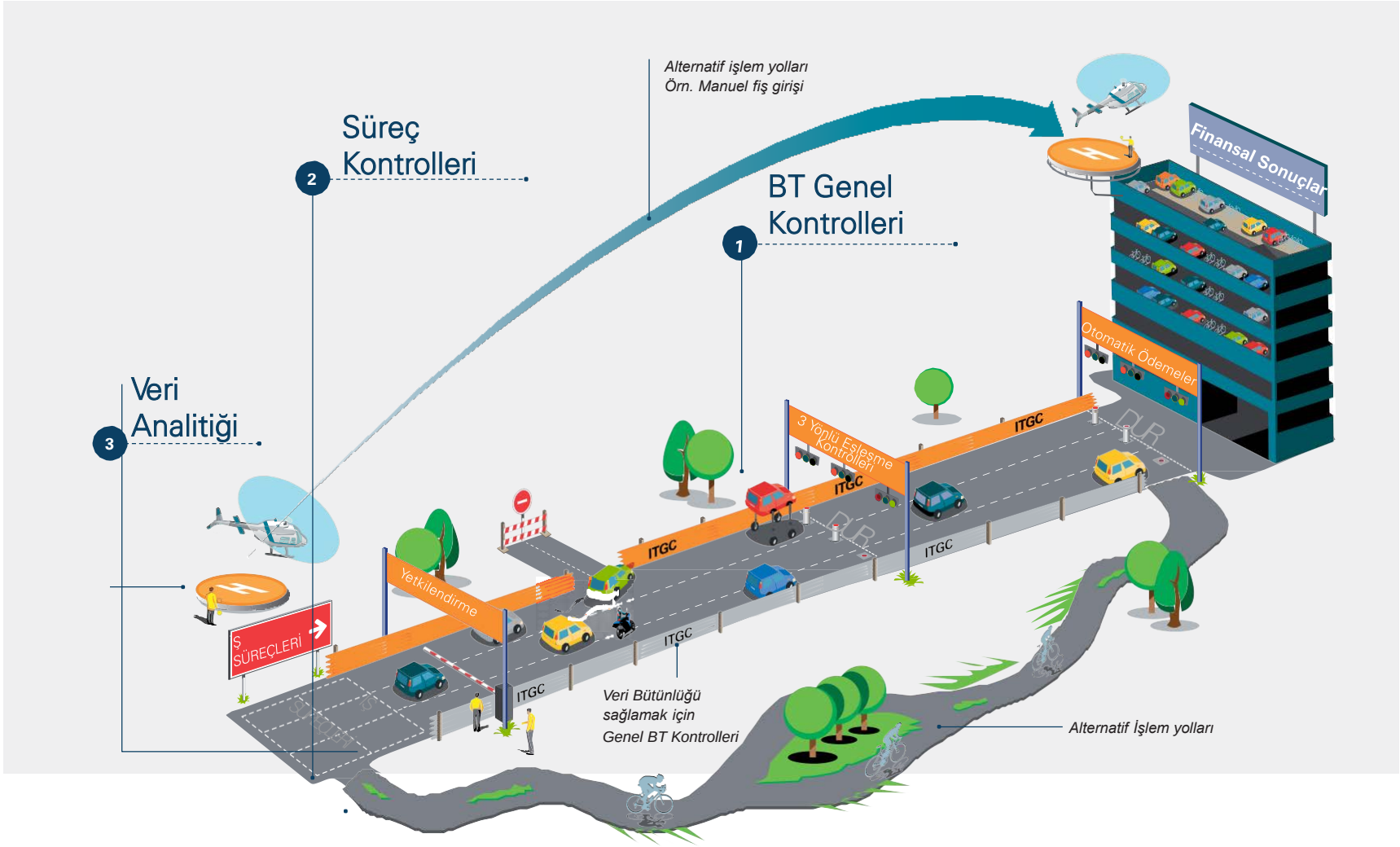
- Bilgi Sistemleri Denetimi Kavramı
- Bilgi Sistemleri Denetiminin Katma Değeri
- Dünya'da ve Türkiye'de Bilgi Sistemleri Denetimi
- Uluslararası Bilgi Sistemleri Denetim Uygulamaları
- Bilgi Sistemleri Yönetişim Çerçeveleri
- Genel Değerlendirme

BİLGİ SİSTEMLERİ DENETİMİ KAVRAMI

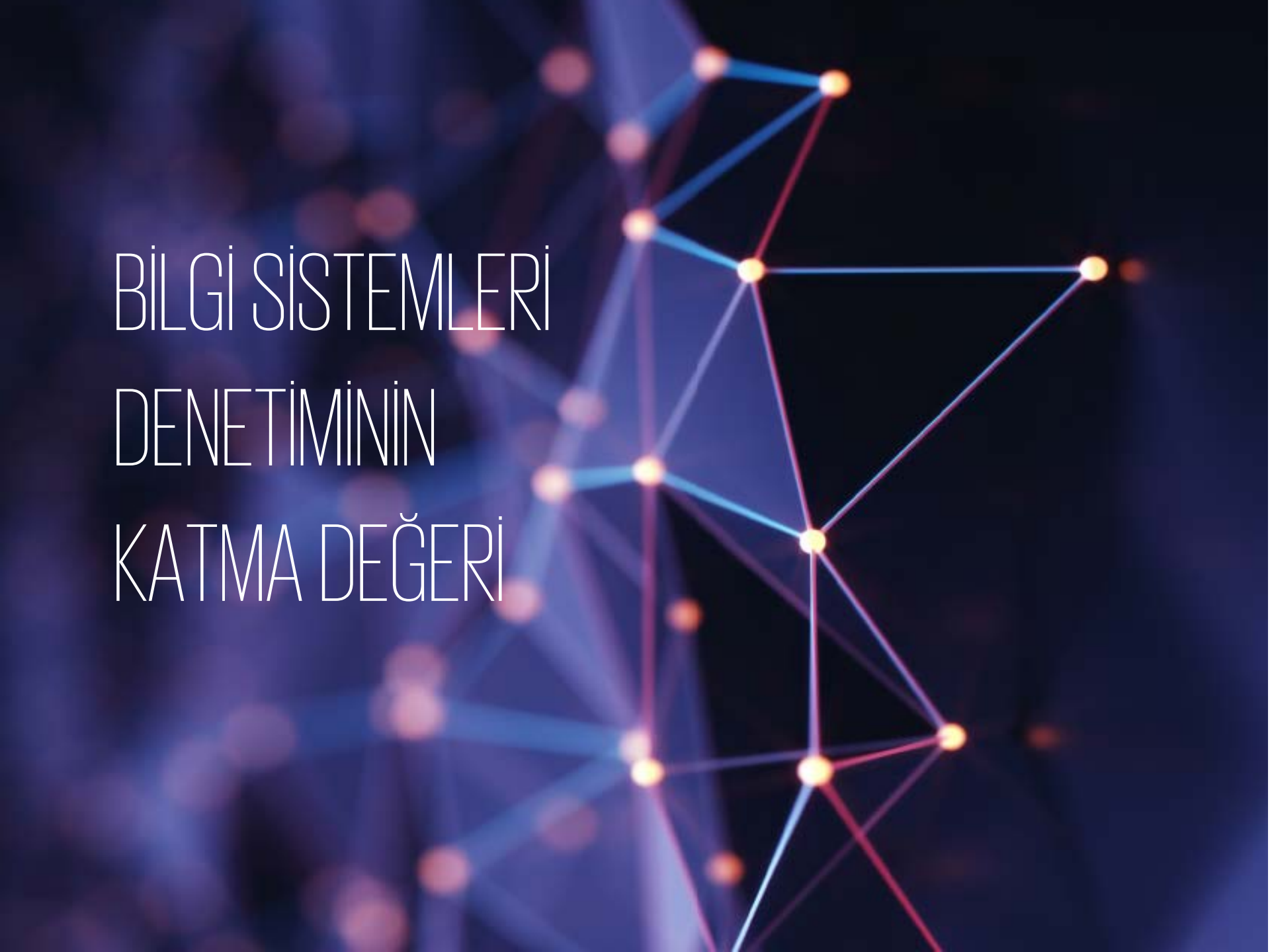
Bilgi Sistemleri Denetimine Giriş



Bilgi Sistemleri Denetimine Giriş



BİLGİ SİSTEMLERİ DENETİMİNİN KATMA DEĞERİ



Bilgi Sistemleri Denetiminin Katma Değeri

ARTAN GÜVENCE

Süreçlere ve kontrollere daha yaygın ve geniş örneklem ışığında bakarak güvence kapsamının artırılmasını sağlar. Denetimde teknoloji kullanımı ve veri analitiği yöntemleriyle daha etkili ve faydalı sonuçlar elde edilir.

IŞIK TUTMA

Kuruluşların teknolojideki yenilikler ve mevzuattaki gelişmeler ışığında güncel bilgiye sahip olmasını, öngörü kazanmasını ve zamanında harekete geçmesini sağlar.

ÇOK YÖNLÜLÜK

Teknik ve yönetimsel anlamda karma bir disiplinden gelen denetçiler; hem iş süreçleri, hem de BT süreçlerini anlayarak; iş birimleri ve teknik birimler arasında bir nevi köprü görevi görür.

REGÜLASYON

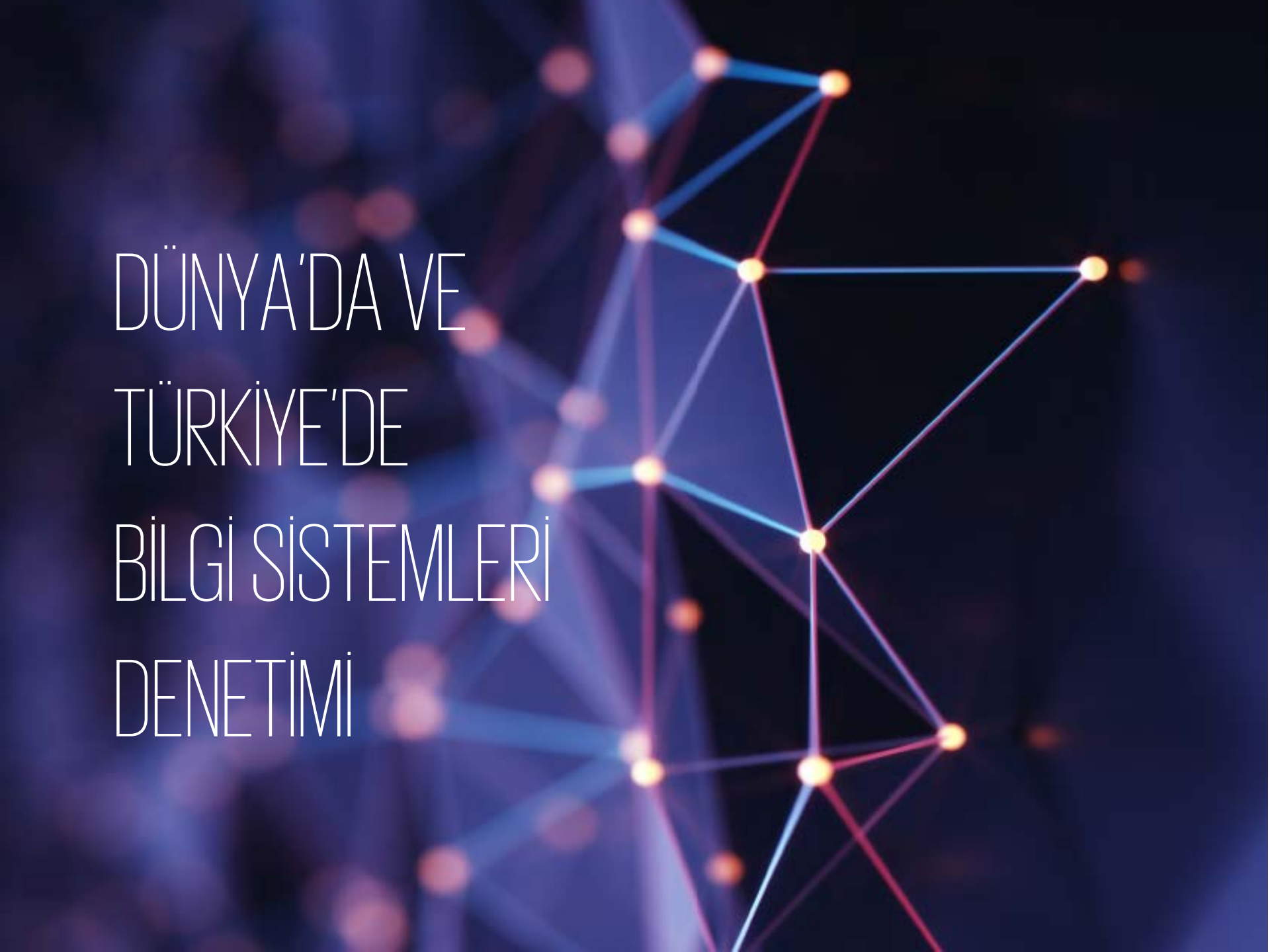
Düzenleyici otoritelerin taleplerine karşılık olarak kuruluşların mevzuata uyumu hakkında etkin güvence sağlar.

ANLAŞILIR SONUÇLAR

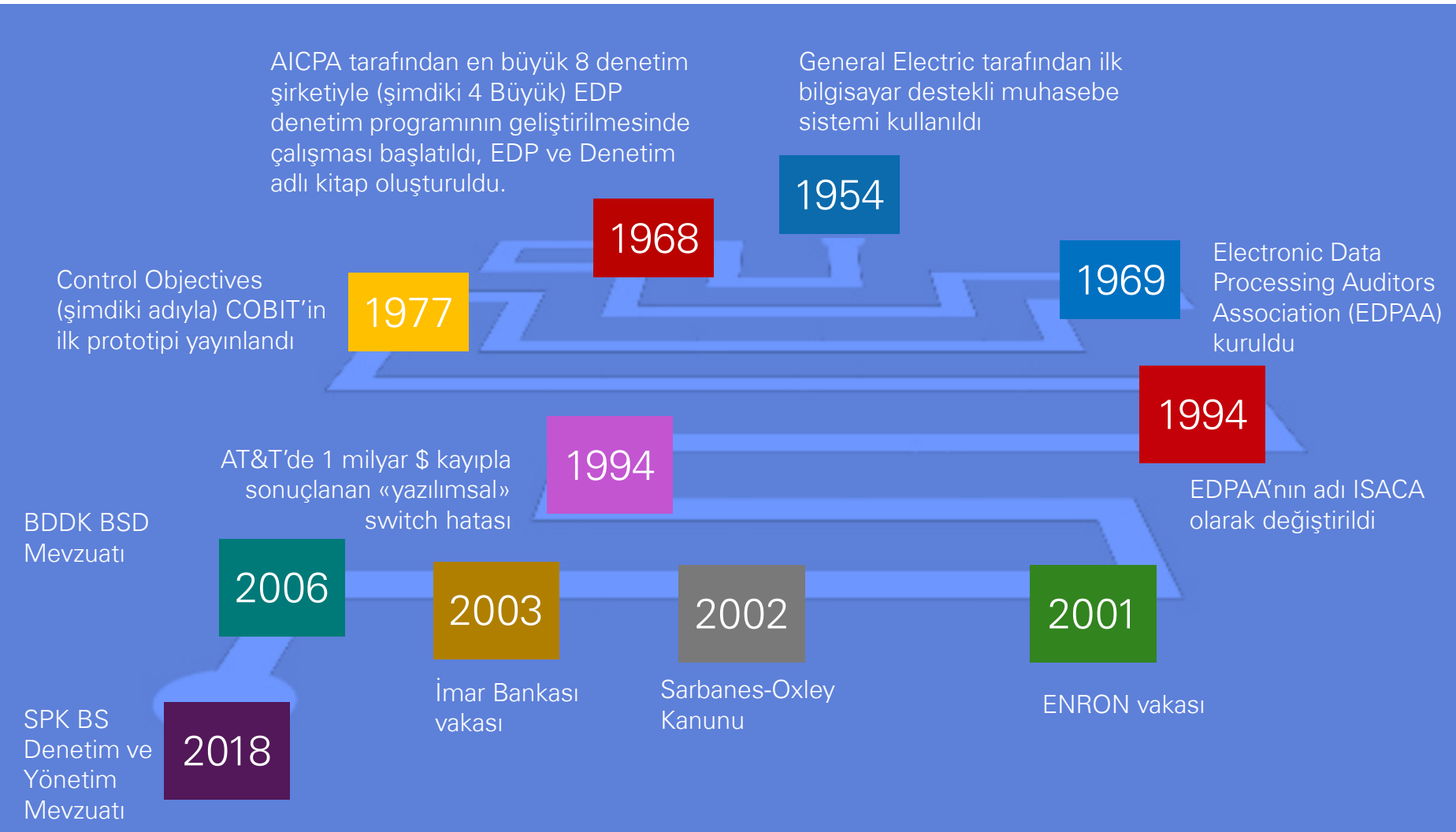
BT ve süreç denetimine ait çalışmalar, kuruluşa özel bir yaklaşımla raporlanır ve somut aksiyon planlarıyla birlikte üst yönetime sunulur.

VERİMLİLİK VE KALİTE

Denetim çalışmalarında manüel iş yükünü azaltarak verimliliği ve kaliteyi artırır.

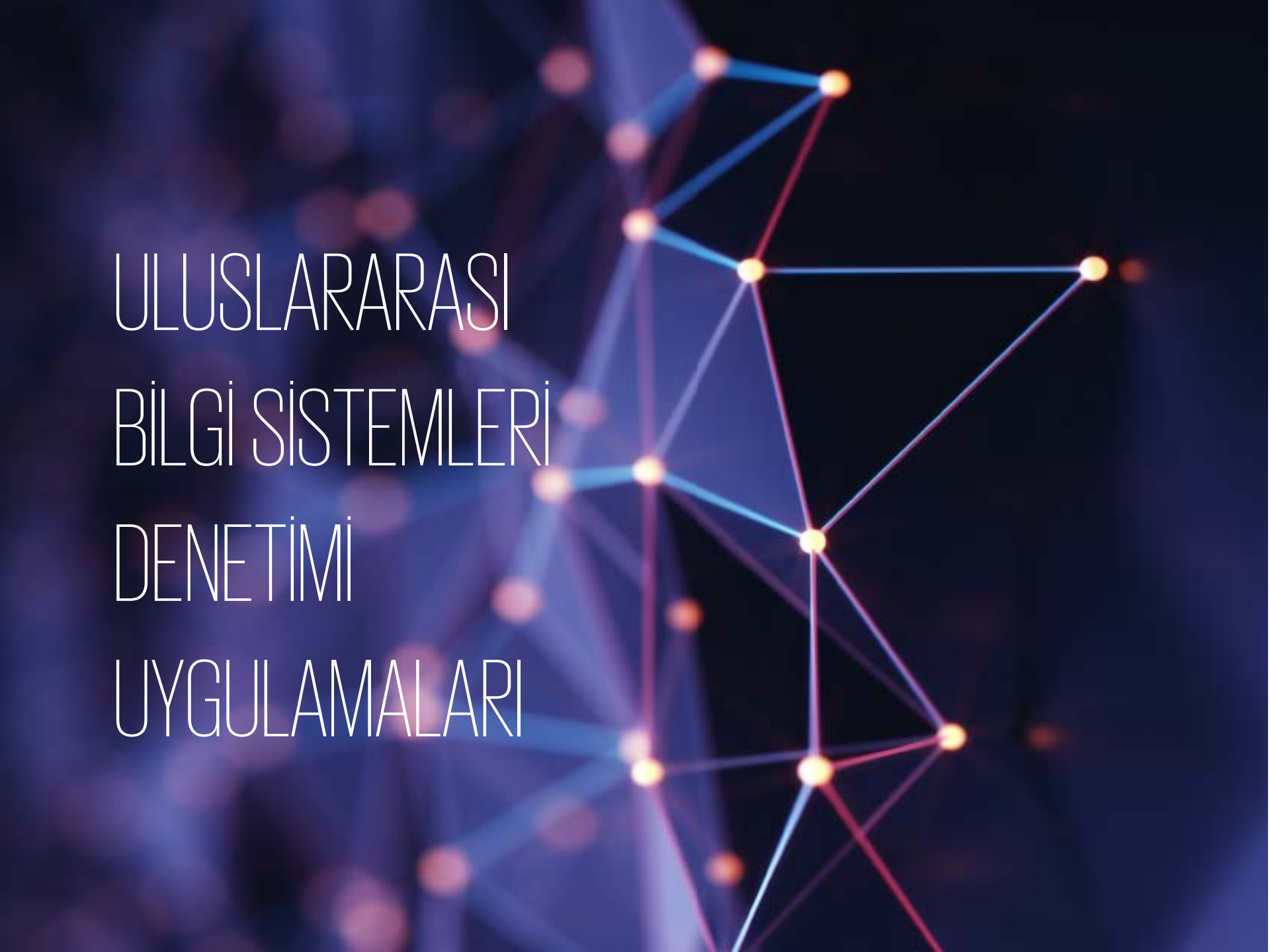

DÜNYA'DA VE
TÜRKİYE'DE
BİLGİ SİSTEMLERİ
DENETİMİ

Bilgi Sistemleri Denetiminin Kısa Tarihçesi



Türkiye'de Bilgi Sistemleri Denetimi

2006	BDDK	Bankacılık Süreçleri ve Bilgi Sistemleri Denetimi Mevzuatı
2013	T.C. Sayıştay	Bilgi Sistemleri Denetim Rehberi
2013		Yetkili Yükümlü Statüsü ISO27001 Zorunluluğu
2013	Sermaye Piyasası Kurulu	Aracı Kurumlar İç Denetim Sistemine İlişkin Esaslar
2014	BDDK	Ödeme ve Elektronik Para Kuruluşları Bilgi Sistemleri Denetimi Mevzuatı
2015		Yeni Nesil ÖKC'lere Ait TSM Merkezlerinin Bilgi Sistemleri Denetimi Mevzuatı
2016	Türkiye Bankalar Birliği	Risk Merkezi Üye Denetim Genelgesi
2016	EPDK T.C. Enerji Piyasası Düzenleme Kurumu	ISO27001 Belge Zorunluluğu
2018	Sermaye Piyasası Kurulu	Bilgi Sistemleri Denetim ve Yönetim Mevzuatı


ULUSLARARASI
BİLGİ SİSTEMLERİ
DENETİMİ
UYGULAMALARI

Uluslararası Bilgi Sistemleri Denetim Uygulamaları

BaFin: Alman Federal Gözetim Kurumu	MaRisk: Erişim Hakları, Veri Bütünlüğü, Erişilebilirliği, Gizliliği
BSI: Federal Bilgi Güvenliği Ofisi	Bilgi Teknolojilerinin Güvenlik Yönetim Sistemi ve Risk Yönetimi Standartları
IDW: Alman Denetçileri Enstitüsü	IDW PS 330: BT ortamı, BT stratejisi, BT altyapısı, uygulamaları, izleme sistemleri ve dış kaynak kullanımı

Uluslararası Bilgi Sistemleri Denetim Uygulamaları

PCAOB: Halka Açık Şirketler için Muhasebe Gözetim Kurulu

NIST: Ulusal Standartlar ve Teknoloji Enstitüsü

GAO: A.B.D. Sayıştayı

SOX: Finansal Raporlama Süreçleri Üzerindeki İç Kontrol Ortamı, Yönetim Beyanı, SOX404 BT ve Süreç Denetimleri

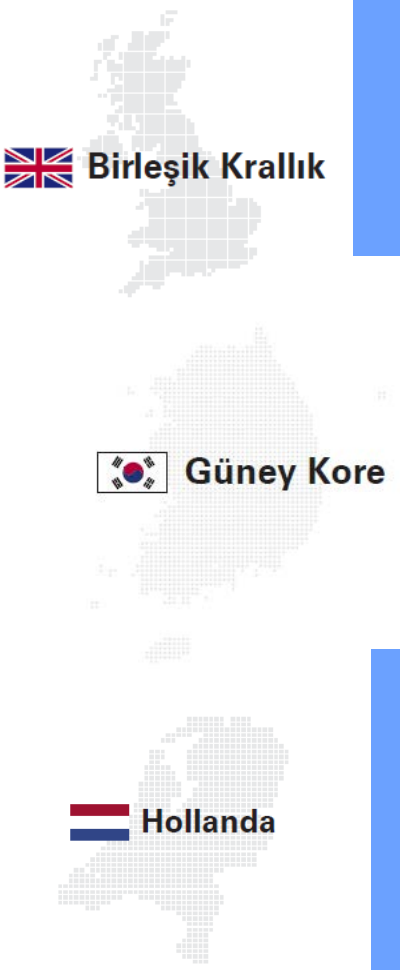
GAPP: Genel Kabul Görmüş Güvenlik Prensip ve Uygulamaları

SSAG: Güvenlik Öz-Değerlendirme Rehberi

GAGAS: Kamu Denetimi Standartları, Güvenlik Yönetimi, Erişim Yönetimi, Konfigürasyon Yönetimi, Görevler Ayrılığı, Acil Durum Planlaması

FISCAM: Federal BT Denetim Kılavuzu

Uluslararası Bilgi Sistemleri Denetim Uygulamaları



Birleşik Krallık

FSA: Finansal Hizmetleri Otoritesi

Senior Management Arrangements, Systems and Controls (SYSC13): Teknoloji stratejileri, gereksinimler, sistem edinimi, geliştirme, ISO27002

Güney Kore

KICPA: Kore Mali Müşavirler Enstitüsü

Bilgi Sistemleri Ortamlarında Denetim: Risk değerlendirme ve denetim prosedürleri alt başlıkları içerisinde BT denetimine ilişkin düzenlemeler yer almaktadır.

Log kayıtları, görevler ayrılığı, bilgisayar destekli denetim teknikleri, verinin erişilebilirliği, bütünlüğü vb.

Hollanda

NOREA: BT Denetçileri Birliği

Registered EDP-Auditor: Ulusal düzeyde kayıtlı BT denetçisi sertifikasının bulunduğu tek ülkedir.

Uluslararası Bilgi Sistemleri Denetim Uygulamaları

FSA: Finansal Hizmetler Kurumu

- BT Risklerinin Yönetimi için Kontrol Ortamı
- BT Risk Yönetimi Sistemi
- J-SOX: Finansal Araçlar ve Borsa Kanunu

CICA: Kanada Mali Müşavirler Odası

COCO: İç Kontrol Modeli
ITCG: BT Kontrol Rehberi

Özet: Ortak Temalar

YÖNETİŞİM

- BT Stratejisi ve Politikası
- Bilgi Sistemleri Risk Yönetimi
- Veri Bütünlüğü, Gizliliği ve Erişilebilirliği
- BT Dış Hizmet Yönetimi

GÜVENLİK

- Bilgi Güvenlik Farkındalık ve Eğitimi
- Erişim Yönetimi
- Görevler Ayrılığı
- Denetim İzleri
- Fiziksel ve Çevresel Güvenlik

GELİŞTİRME

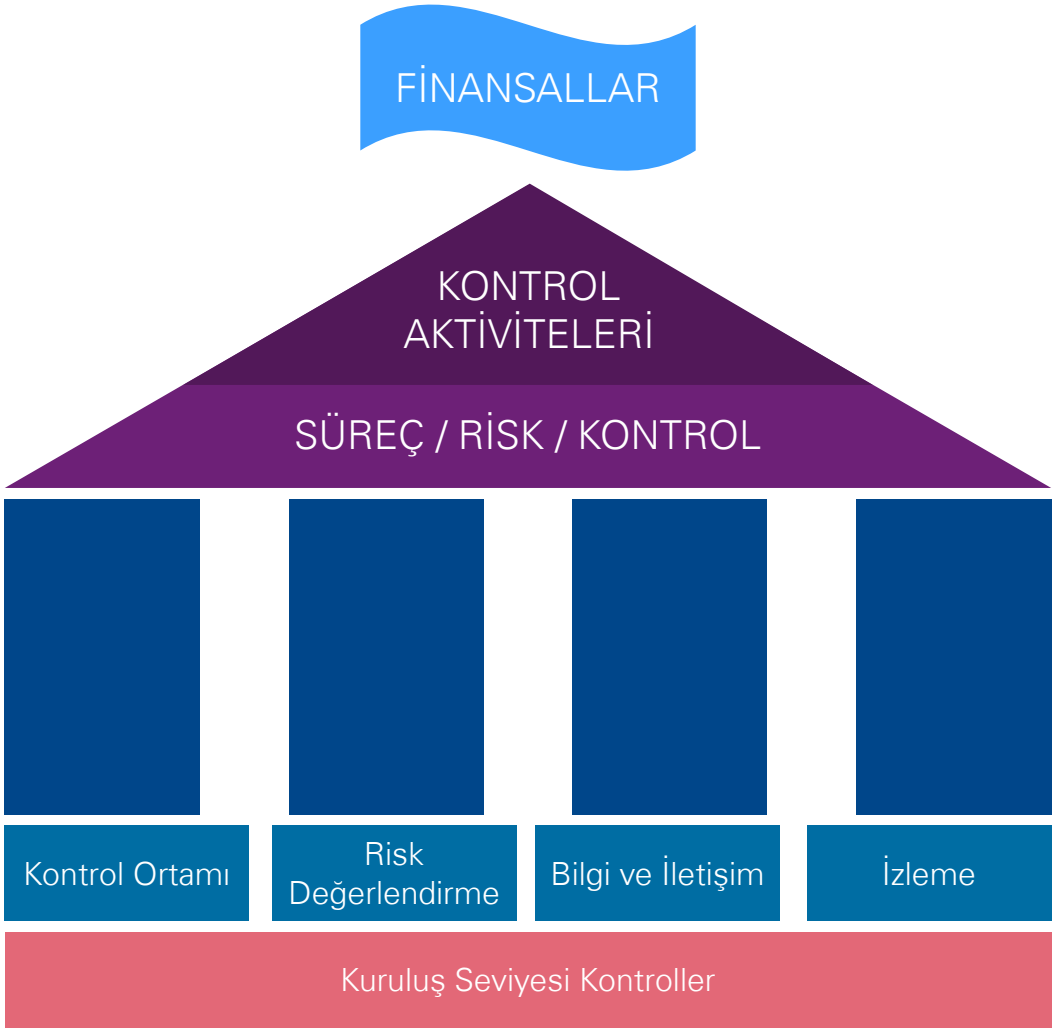
- Bilgi Sistemleri Edinimi, Geliştirilmesi ve Bakımı
- Değişiklik Yönetimi
- Konfigürasyon Yönetimi

OPERASYON

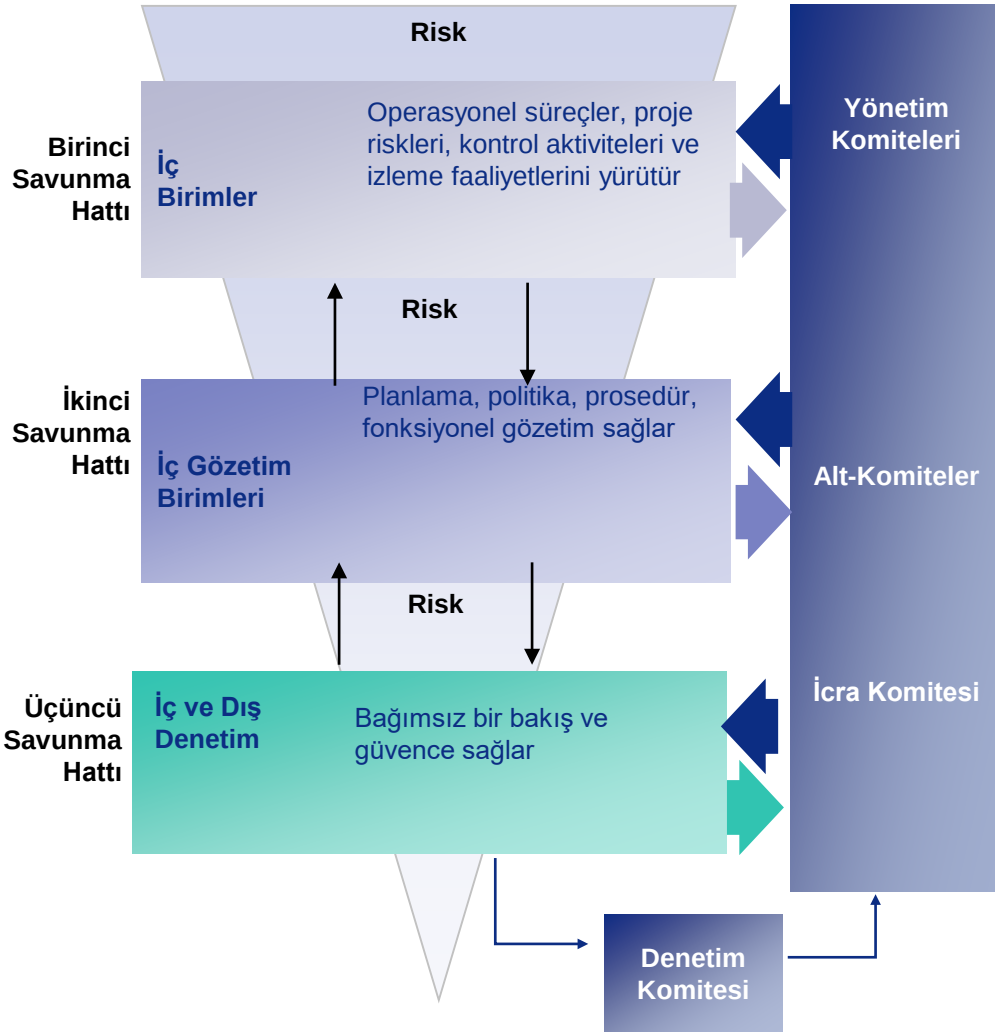
- Acil Durum Yönetimi
- İş Sürekliliği Planı
- Olay Yönetimi
- BT Operasyonları

BİLGİ SİSTEMLERİ YÖNETİŞİM ÇERÇEVELERİ

COSO: İç Kontrol Çerçevesi



SOX404: ICOFR- Bütünleşik Denetim Çerçevesi



Sarbanes-Oxley tarafından önerilen bütünleşik denetim yapısı; aynı anda hem yönetim tarafından hem de bağımsız denetim tarafından; kuruluş seviyesi kontroller, üst seviye kontroller, süreç kontrolleri ve BT kontrollerinin değerlendirmesini içeren bir «İç Kontrol Raporu» hazırlanmasını içerir.

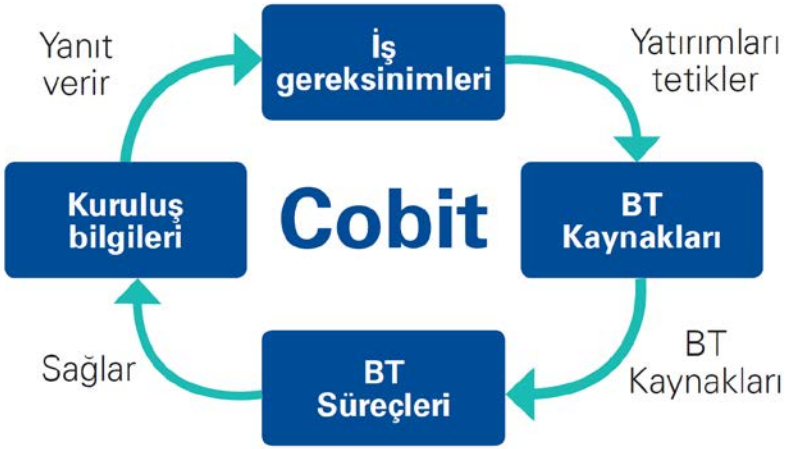
Bağımsız denetçi tarafından İç Kontrol Çalışması temel alınarak güvence çalışması gerçekleştirilir ve buna istinaden denetim görüşü oluşturulur.

IFAC: Uluslararası Denetim Standartları

ISA 300	Finansal Tabloların Denetiminin Planlanması	Denetim planlamasının temel adımları
ISA 315	Kuruluş ve Ortamının Anlaşılması Yoluyla Önemli Kontrol Eksikliği Risklerinin Belirlenmesi ve Değerlendirilmesi	Bilgi sistemleri ortamının anlaşılması, bilgi sistemleri iç kontrol ilişkisi, bilgi sistemleri riskleri
ISA 402	Hizmet Kuruluşu Kullanan bir Kuruluş için Denetim Hususları	Hizmet kuruluşları iç kontrol ortamının değerlendirilmesi

COBIT: BT için Kontrol Hedefleri

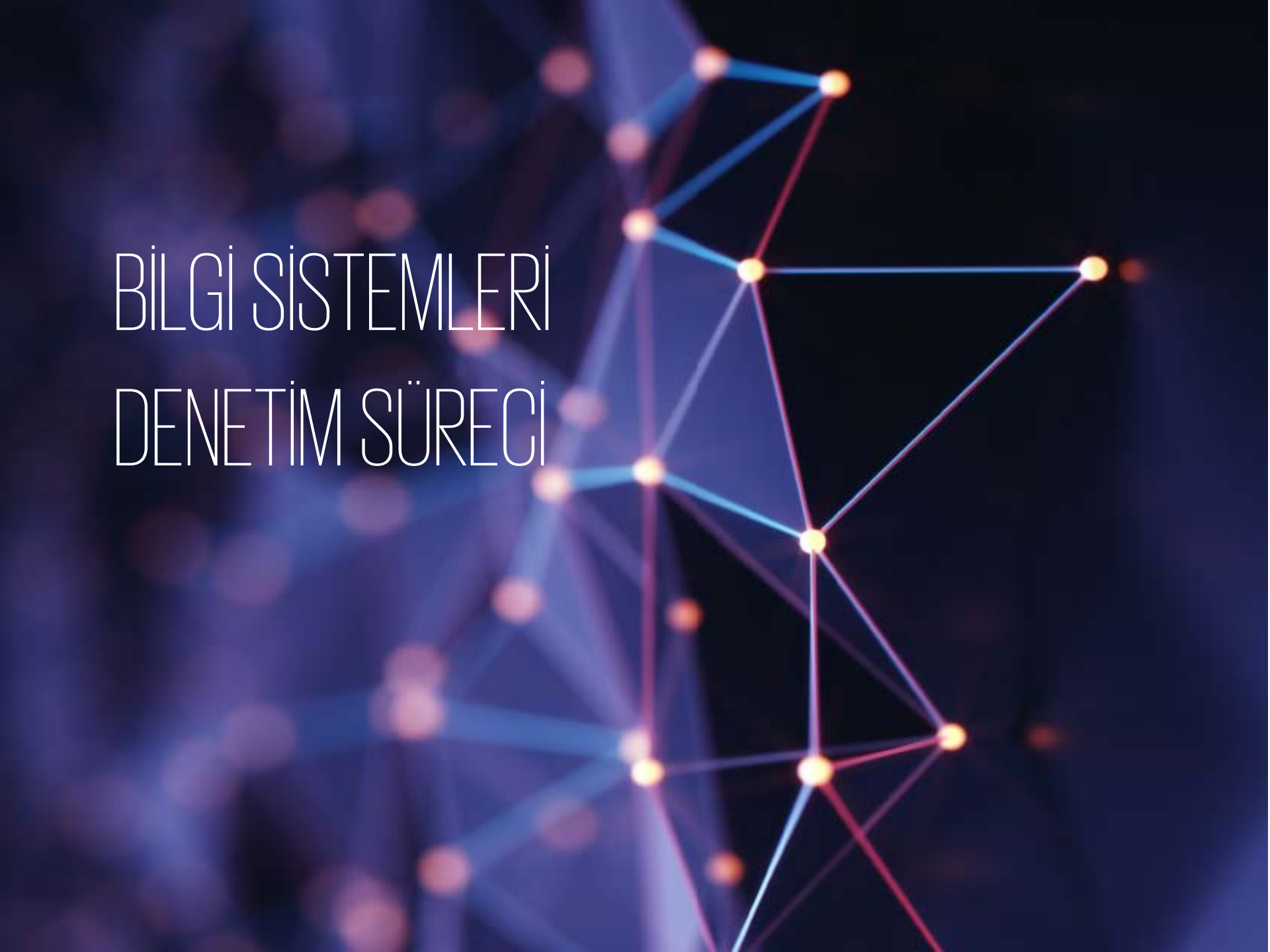
COBIT, bazı ülkelerde çeşitli sektörler için yasal düzenleme olarak da kullanılmakta olup, ülkemizdeki en somut örneği ise bankacılık sektörü için Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) tarafından regüle edilmiş olmasıdır.



COBIT, genel anlamda dört ana başlık altında öneriler getirir ve kontrol noktaları belirler:

Planlama ve Organizasyon (PO)
Tedarik ve Uygulama (AI)
Teslimat ve Destek (DS)
İzleme ve Değerlendirme (ME)

BİLGİ SİSTEMLERİ DENETİM SÜRECİ



Özet: Denetim Süreci

BT Denetimi Zorunluluğu Var mı?

Ayrı bir BT ve Süreç Denetim Raporu Var mı?

Bağımsız Denetim Şirketleri BT Denetimi için Yetkilendiriliyor mu?

Kişiler BT Denetçisi Olarak Yetkilendiriliyor mu?

Denetim Kapsamı

BT Denetim Zorunluluğu Var mı?

BDDK (Türkiye)	Bankalar özelinde her yıl süreç denetimi, iki yılda bir ise zorunlu BT denetimi gerçekleştirilmektedir.	BDDK düzenlemeleri ve COBIT 4.1 çerçevesi baz alınmaktadır.
PCAOB (ABD)	BS denetimi özelinde bir düzenleme bulunmamaktadır.	Standartlar içerisinde BS kontrollerine değinilmiştir.
IFAC (Global)	BS denetimi özelinde bir düzenleme bulunmamaktadır.	Standartlar içerisinde BS kontrollerine değinilmiştir.

Denetim Raporu ve Görüş

BT ve Süreç Denetimi İçin Ayrı Rapor Hazırlanıyor mu?

BDDK (Türkiye)	Evet
PCAOB (ABD)	Hayır
IFAC (Global)	Hayır

Denetçi Yetkilendirme

	Bağımsız denetim kuruluşları mali denetim için yetkilendiriliyor mu?	Bağımsız denetim kuruluşları BT denetimi için yetkilendiriliyor mu?
BDDK (Türkiye)	Evet	Evet
PCAOB (ABD)	Evet	Hayır
IFAC (Global)	Hayır (Kalite kontrol standartları ile uyum temel alınıyor, ülkeler nezdinde yetkilendirme söz konusu)	Hayır
Diğer Ülkeler	Evet	Hayır

Denetim Sertifikaları

Kişiler BT denetçisi olarak yetkilendiriliyor mu?

BDDK (Türkiye)	Evet (CISA sertifikası ve asgari 10 yıl tecrübe)
PCAOB (ABD)	Hayır
IFAC (Global)	Hayır
Hollanda	Hayır (RE sertifikası mevcut, fakat herhangi bir sektörde BT denetimi gerçekleştirmek için zorunlu tutulmuyor)

Genel Değerlendirme

Türkiye'de bankacılık sektörü dışında bir BT denetimi mevzuatına ihtiyaç vardır. Kritik BT ortamlarına sahip sektörlerdeki kuruluşların veya belirli bir boyutun üzerindeki kuruluşların BT denetimine tabi tutulması gerekli görülmektedir.

Bilgi teknolojileri denetim raporlarının özel ve gizli raporlar olarak hazırlanması önem arz etmektedir.

BT denetimi için Türkiye özelinde kişilerin ve kuruluşların yetkilendirilmesi gerekli ve faydalı görülmektedir.

Yetkilendirme ve sertifikasyon için mevcut uygulamaların denkliğinin kabul edilmesi mesleğin gelişimini destekleyecektir.

KPMG

İLETİŞİM

Sinem Cantürk
Şirket Ortağı,
Bilgi Sistemleri Risk Yönetimi
Bölüm Başkanı,
Finasal Hizmetler Sektör Lideri

T: +90 216 681 90 00 – 9037
M: +90 533 533 294 36 08
E: scanturk@kpmg.com
W: www.kpmg.com.tr