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

İç Denetimde Bilgi Sistemleri Denetiminin Yeri

Dr. Eren GEGİN

İç Denetim Nedir?

Genel Kabul Görmüş Olan Tanım*

İç denetim, bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden bağımsız ve objektif bir güvence ve danışmanlık faaliyetidir. İç denetim, kurumun risk yönetim, kontrol ve yönetişim süreçlerinin etkililiğini değerlendirmek ve geliştirmek amacına yönelik sistemli ve disiplinli bir yaklaşım getirerek kurumun amaçlarına ulaşmasına yardımcı olur.

** TİDE Kırmızı Kitap, sy.2*

Uluslararası İç Denetim Standartları

Performans Standartları: 2120.A1

İç denetim faaliyeti, aşağıdakileri dikkate alarak, kurumun yönetişim süreçlerinin, faaliyetlerinin ve **bilgi sistemlerinin maruz kaldığı riskleri** değerlendirmek zorundadır:

- • Mali ve operasyonel bilgilerin güvenilirliği ve doğruluğu,
- • Faaliyetlerin etkililik ve verimliliği,
- • Varlıkların korunması,
- • Kanun, düzenleme ve sözleşmelere uyum.

Uluslararası İç Denetim Standartları

Performans Standartları: 2130.A1

İç denetim faaliyeti, kurumun yönetişim, faaliyet ve **bilgi sistemlerinin içinde bulunan risklere cevap olarak, kontrollerin yeterliliğini ve etkililiğini** aşağıdaki konularla ilgili olarak değerlendirmek zorundadır:

- • mali ve operasyonel bilgilerin güvenilirliği ve doğruluğu,
- • faaliyetlerin etkililik ve verimliliği,
- • varlıkların korunması,
- • kanunlara, düzenlemelere ve sözleşmelere uyum.

Bilgi Sistemleri (ya da Teknolojileri) Denetimi

- **Genel kabul görmüş bir tanımı yok !**
- **Genel tanımlardan bir tanesi:** İşin genel kontrol amaçlarının desteklenmesi amacıyla bilgi sistemleri ya da bilgi teknolojileri kontrollerinin kalitesinin ve etkililiğinin resmi bir şekilde doğrulanması ve onaylanması

IIA'e Göre Bilgi Teknolojilerinin Tanımı

- Bilgi işlemek ve iletişim sağlamak üzere kullanılan her türlü bilgisayar donanımı ve yazılımı,
- Teknolojinin uygulanması ve muhafaza edilmesine dönük süreçlerin tamamı,
- Söz konusu teknolojinin kullanımı ile ilişkili her türlü insan kaynağı…

Orijinali:

All the computer hardware and software used to process information and provide communications, the processes for administering and maintaining the technology, and the human resources associated with the use of technology.

Kaynak: GTAG – 1, sy. 46

Bilgi Sistemleri Denetimi Tanım

- Kurum tarafından kullanılan tüm yazılım, donanım ve bilgi sistem ve teknolojilerinin*;
  - Kurumun amaçları ile uyumlu olup olmadığının
  - yeterli, etkin ve verimli bir şekilde kullanılıp kullanılmadığının,
  - bilgi işlem sistemlerinde yer alan tüm kayıtların ve bilginin gizliliği ile izinsiz erişimlere karşı güvenilirliğinin sağlanıp sağlanmadığının

  sistematik bir yaklaşımla değerlendirilmesidir.

* Control Objectives For Information and Related Technology (COBIT), Framework Control Objectives Management Guidelines Maturity Models, Version: 4.1., sy.9-11

Bilgi Sistemleri Denetimi (2)

- **ISACA'nın tanımı *:** Bilgi sistemlerinin ve ilgili diğer kaynakların;
  - yeterli bir şekilde şirket varlıklarını koruduğu,
  - veri ve sistem bütünlüğünü sağladığı,
  - ilgili ve güvenilir bilgi sağladığı,
  - organizasyonel amaçlara etkili bir şekilde ulaşılması, kaynakların etkin bir şekilde kullanılması, operasyonel amaçların ve kontrol amaçlarının elde edilmesi amacıyla gereken iç kontrollerin var olup olmadığı konularında makul bir güvence sağlamak üzere gerekli bulguların toplanması ve analiz edilmesidir.

** CISA Review Manual, 2009, sy.34*

Bilgi Sistemleri Denetiminin Unsurları

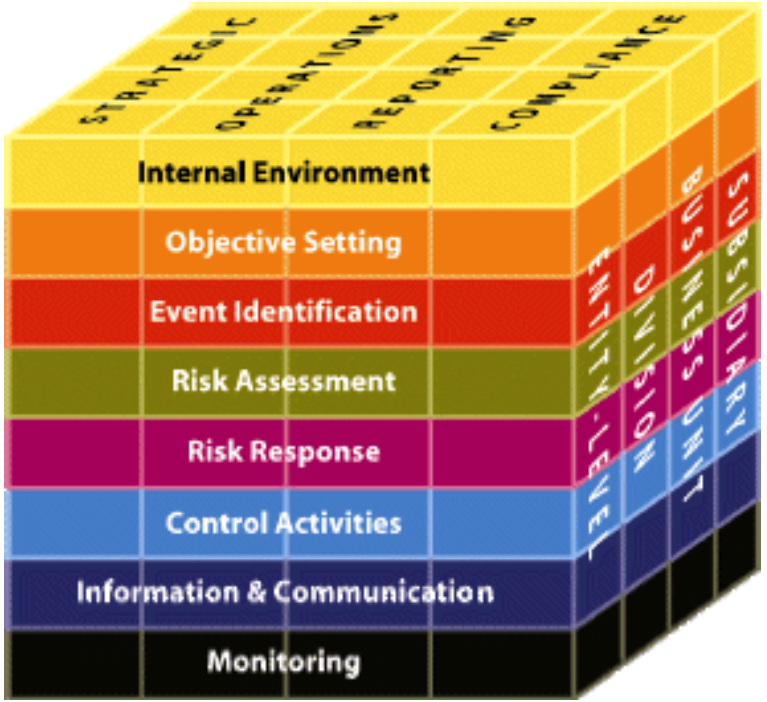
- **Fiziksel ve Çevresel Faktörlerin Kontrolü** *— Sistemlerin fiziksel güvenliği, güç merkezi, havalandırma, nem ve diğer çevresel faktörlerin kontrolünü kapsar.
- **Sistem Yönetiminin Kontrolü**—İşlemekte olan sistemler, veri tabanı yönetim sistemleri, tüm sistem yönetim prosedürleri ve bunlara uyumun kontrolü.
- **Uygulama Yazılımlarının Kontrolü**—Ücretlerin ödenmesi, faturalandırma, web tabanlı müşteri sipariş kabul sistemi, işletme kaynak planlama sistemi gibi işletmenin faaliyetlerini sürdürmesi amacıyla kullandığı yazılımların kontrolünü içerir. Bu sistemlerin kontrolü ve gözden geçirilmesi, erişim kontrolleri ve onayları, doğrulamalar, hata ve istisnai işlemlerin yönetimi, manuel süreçlerin kontrolü vs. içerir. Bunlara ilave olarak sistem geliştirme döngüsünün (lifecycle) de mutlaka bu gözden geçirmeye dahil edilmesi gerekir.
- **Ağ Güvenliğinin Kontrolü**—Sisteme dahili ve harici erişimlerin kontrolü, güvenlik duvarı, izinsiz girişlerin kontrolü gibi tipik kontrolleri kapsar.
- **İş Sürekliliğinin Kontrolü** —Yedekleme ve veri stoklama prosedürleri, planlanarak dokümante edilmiş ve bizzat test edilmiş acil durum ya da iş sürekliliği planlarının kontrolü.
- **Veri Bütünlüğünün Gözden Geçirilmesi**—Bilgisayar Destekli Denetim Teknikleri (CAAT) de kullanılmak suretiyle canlı verinin yeterliliğinin kontrol edilmesi.

** S. Anantha Sayana, IT Audit Basics, ISACA Journal, Vol I, 2002.*

Bilgi Sistemleri Denetimi (3)

Herkesin Üzerinde Mutabık Olduğu Şey!

COSO Çerçevesi



- Kurum faaliyetlerinin etkin ve verimli bir şekilde gerçekleştirilmesi,
- Üretilen finansal veri ve raporların güvenilir olması,
- Kurum varlıklarının (aktiflerinin) korunması ya da
- Faaliyetler sırasında mevzuata uygunluğun sağlanması

amacıyla aldıkları her türlü karar, önlem ya da yaptıkları uygulamaların toplamı

İç Denetim Yaklaşımı

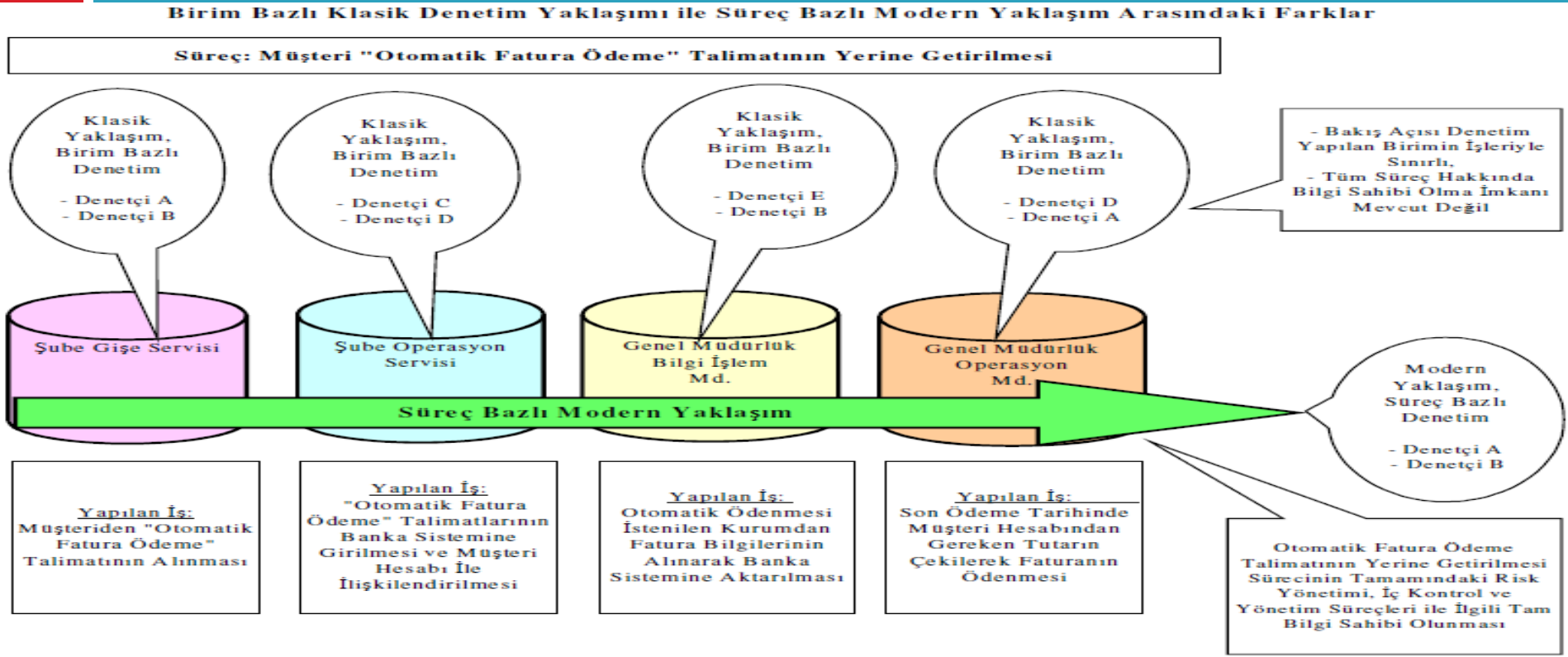
Birim Bazlı

- Geleneksel Yaklaşım

Süreç Bazlı

- Modern Yaklaşım

İç Denetim Yaklaşımındaki Farklılıklar



İç Denetim Yaklaşımındaki Farklılıklar (2)

Temel Karar Noktaları

- Bilgi Sistemleri Denetimi Hangi Yaklaşıma Göre Yapılacak? Avantajları, Dezavantajları…

- Hangi Metodoloji, Yöntem Kullanılacak?
  - COBIT,
  - ITIL,
  - ISO\IEC 27002-ISO\IEC 27001
  - NIST SP800-53-Recommended Security Controls for Federal Information Systems
  - CMMI

  ….

COBIT

- 4 ana grup (Planlama ve Organizasyon, Tedarik ve Uygulama, Teslim ve Destekleme, İzleme) altında düzenler,
- 34 üst düzey, 300 detaylı kontrol amacı belirler,
- 36 genel kabul görmüş BT standardı ve uygulamasını referans alır

Bilgi Sistemleri Denetimi

Herkesin Üzerinde Mutabık Olduğu Bir Başka Konu

Risk Bazlı Denetim

Uluslararası İç Denetçiler Enstitüsü IIA'nin Konuya Bakışı

Zorunlu Değil, Kuvvetle Tavsiye Edilen Rehber İçerisinde !

Uluslararası Meslekî Uygulama Çerçevesi		
	Zorunlu	Kuvvetle Tavsiye Edilen
Tanım	✓	
Etik Kuralları	✓	
Standartlar ve Yorumlar	✓	
Pozisyon Raporları		✓
Uygulama Önerileri		✓
Uygulama Rehberi		✓

Uluslararası İç Denetçiler Enstitüsü IIA'nin Konuya Bakışı

Uygulama Rehberleri

İç denetim faaliyetinin yönetiminde ayrıntılı rehberlik sağlar.
Araç ve teknikler, programlar, adım adım uygulamalar ve uygulama örnekleri gibi ayrıntılı süreç ve prosedürler bulunmaktadır*.

1. GTAG'lar (Global Technology Audit Guides)

Global Teknoloji Denetim Rehberleri

2. GAİT'ler (Guide to the Assesment of IT Risk)

Bilişim Risklerinin Değerlendirme Rehberi

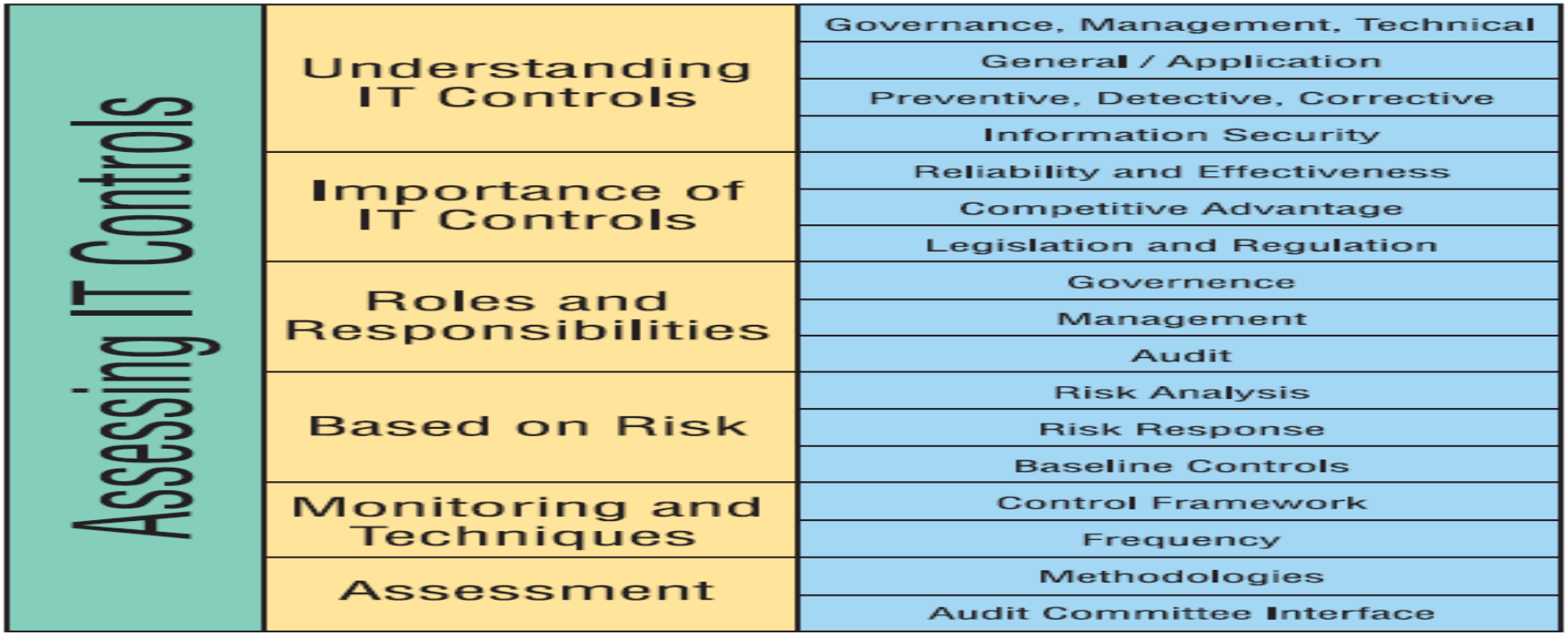
** TİDE Kırmızı Kitap, sy. xix*

Uluslararası İç Denetçiler Enstitüsü IIA'nin Konuya Bakışı

GTAG'lar

PG GTAG-15: Bilgi Güvenliği Yönetimi (Information Security Governance)
PG GTAG-14: Kullanıcı Bazlı Geliştirilen Uygulamaların Denetimi (Auditing User-developed Applications)
PG GTAG-13: Otomasyonda Yolsuzlukların Tespiti ve Önlenmesi (Fraud Prevention and Detection in an Automated World)
PG GTAG-12: BS Projelerinin Denetimi (Auditing IT Projects)
PG GTAG-11: BS Denetim Planının Geliştirilmesi (Developing the IT Audit Plan)
PG GTAG-10: İş Sürekliliği Yönetimi (Business Continuity Management)
PG GTAG-9: Kimlik ve Erişim Yönetimi (Identity and Access Management)
PG GTAG-8: Uygulama Kontrollerinin Denetimi (Auditing Application Controls)
PG GTAG-7: Bilgi Sistemlerinin Dış Kaynaklardan Tedariki (Information Technology Outsourcing)
PG GTAG-6: Bilgi Sistemlerinin Zayıf Noktalarının Denetim ve Yönetimi (Managing and Auditing IT Vulnerabilities)
PG GTAG-5: Gizlilik Risklerinin Yönetim ve Denetimi (Managing and Auditing Privacy Risks)
PG GTAG-4: Bilgi Sistemleri Denetiminin Yönetimi (Management of IT Auditing)
PG GTAG-3: Sürekli Denetim: Güvence, İzleme ve Risk Değerlemeye Dönük Sonuçlar (Continuous Auditing)
PG GTAG-2: Değişim ve Onarım Yönetimi Kontrolleri (Change and Patch Management Controls:Critical for Organizational Success)
PG GTAG-1: Bilgi Teknolojileri Kontrolleri (Information Technology Controls)

Bilgi Sistemleri Denetiminin Yapısı



GTAG-1: Bilgi Teknolojileri Kontrolleri, Sy. 2-3

Bilgi Teknolojileri Riski

Genel Yanlış Görüş:
BT Riski, Bilgi Güvenliği Riskinden İbarettir

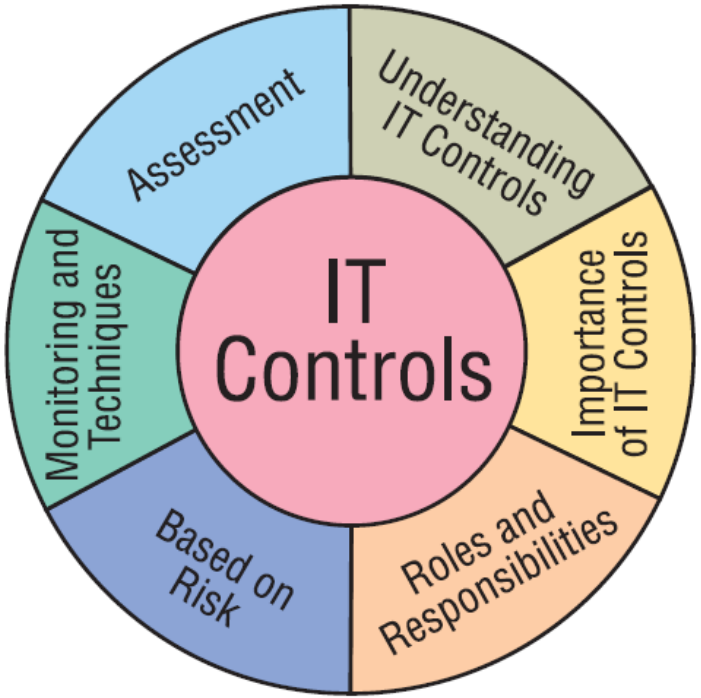
Doğrusu:
İş ve organizasyon ile ilgili çok sayıda farklı riski de içerir,
farklı risk gruplarıyla **içiçe** geçmiştir

Örnek:
BT uygulamalarının büyümeye uyum gösterememesi (stratejik risk),
Pazarın ihtiyaç duyduğu BT uygulamalarının geliştirilememesi (operasyonel risk),
Mevcut sistemin yavaş ve yetersiz performans göstermesi (stratejik risk)

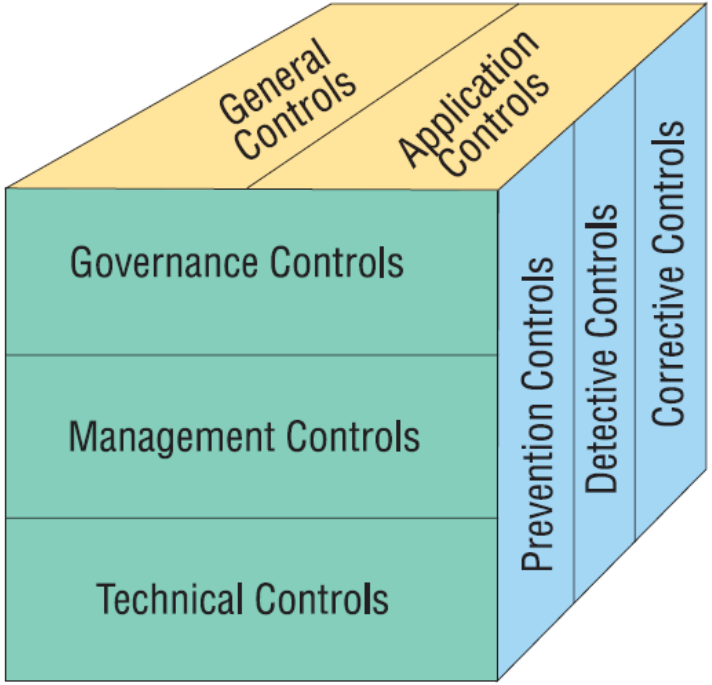
BT Risk Analizinde Sorulması Gereken 5 Temel Soru

- Risk altındaki bilgi varlıkları neler? Bunların gizliliği, bütünlüğü ve kullanılabilirliğinin değeri nedir?
- Söz konusu bilgi varlıkları hangi olaylardan olumsuz etkilenebilir? Bu soruya bağlı olarak yapılacak bir kırılganlık/zayıflık (vulnerability) testi sonucunda ortaya çıkan zayıflıklar nelerdir, olumsuz etkilenmesi muhtemel ve tehdit altındaki bilgi varlıkları hangileridir?
- Var olan bir tehdit varsa bunun etkisi ne kadar olacaktır?
- Bu tehdidin oluşma sıklığı nedir?
- Belirsizlik analizinin sonuçları (Bu sorulara aldığımız sonuçlar ne kadar doğru?)

GTAG-1 : Bilgi Teknolojileri Kontrolleri



GTAG-1 : Bilgi Teknolojileri Kontrolleri



Kontrollerin 3 Farklı Şekilde Sınıflandırılması

•Genel Kontroller
•Uygulama Kontrolleri

•Önleyici Kontroller
•Tespit Edici Kontroller
•Düzeltici Kontroller

•Yönetişim Kontrolleri
•Yönetim Kontrolleri
•Teknik Kontroller

GTAG-1 : Bilgi Teknolojileri Kontrolleri

• **Genel Kontroller**

Altyapı kontrolleri olarak da adlandırılır. Makro kontrollerdir. Tüm sistem bileşenleri, süreçler ve şirketin ya da sistemin verilerine dönüktür.

Bazı örnekler: Bilgi sistemleri politikasının varlığı, erişim ve onaylama prosedürleri, temel BS fonksiyonlarının ayrıştırılması, değişim yönetimi, yedekleme, iş sürekliliği...

•**Uygulama Kontrolleri**

Her bir iş süreci ya da uygulamaya yönelik kontrollerdir. Veri girişi ve onaylama gibi fonksiyonların ayrıştırılması, çıktı toplamlarının karşılaştırılması, işlemlerin loglanması, hataların raporlanması

Önleyici, tespit edici ya da düzeltici olarak 3 alt başlıkta ele alınabilir

GTAG-1 : Bilgi Teknolojileri Kontrolleri

- **Önleyici Kontroller**

Hata, atlama ya da güvenlik ihlallerin oluşmasının engellenmesi

Örnek: Sadece rakam girilebilecek alanlara harf girişine izin verilmemesi, antivirüs ya da sızma engelleme yazılımları

- **Tespit Edici Belirleyici Kontroller**

Önleyici kontrolleri atlatmış, hata ya da atlamaların tespit edilmesine yönelik kontroller

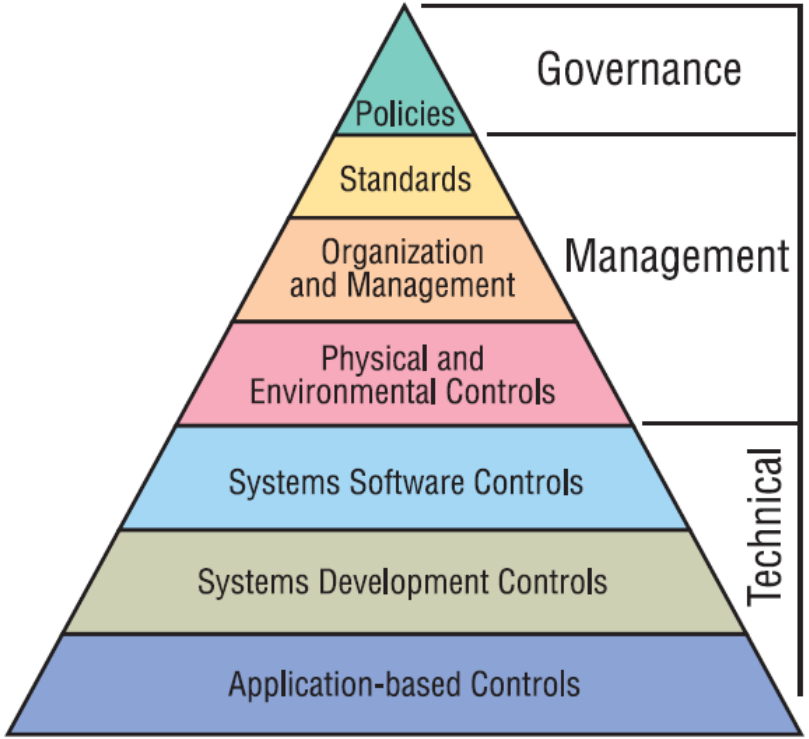
Örnek: şüpheli faaliyetler gerçekleştiren ya da aktif durumda bulunmayan hesapların tespit edilmesi, önceden belirlenmiş limitleri aşmış faaliyet ya da olayların tespit edilmesi vs...

- **Düzeltici Kontroller**

Tespit edilmiş kontrol eksikliklerinin düzeltilmesi amacıyla getirilen kontrol uygulamaları

Örnek olarak hatalı veri girişlerinin düzeltilmesine dönük getirilen yeni kontrol uygulamaları, yetkisiz kullanıcıların sistemden uzaklaştırılması

GTAG-1 : Bilgi Teknolojileri Kontrolleri



GTAG-1 : Bilgi Teknolojileri Kontrolleri

Neleri Ele Alıyor?

- BT Kontrolleri Nelerdir?
- BT Kontrollerinin Değerlendirilmesi ve Analizi
- BT Kontrollerinin Anlaşılması, Önemi ve Şirket İçindeki Rolü
- **Risklerin Analiz Edilmesi**
- Risklerin İzlenmesi
- BT'ye İlişkin Yasal Düzenlemelere Nasıl Uyum Gösterilebilir?
- COSO Kullanılarak BT Kontrollerinin Değerlendirilmesi
- COBIT Çerçevesi
- .....

BT Risk Analizinde Sorulması Gereken 5 Temel Soru

- Risk altındaki bilgi varlıkları neler? Bunların gizliliği, bütünlüğü ve kullanılabilirliğinin değeri nedir?
- Söz konusu bilgi varlıkları hangi olaylardan olumsuz etkilenebilir? Bu soruya bağlı olarak yapılacak bir kırılganlık/zayıflık (vulnerability) testi sonucunda ortaya çıkan zayıflıklar nelerdir, olumsuz etkilenmesi muhtemel ve tehdit altındaki bilgi varlıkları hangileridir?
- Var olan bir tehdit varsa bunun etkisi ne kadar olacaktır?
- Bu tehdidin oluşma sıklığı nedir?
- Belirsizlik analizinin sonuçları (Bu sorulara aldığımız sonuçlar ne kadar doğru?)

GTAG-2 : Değişim ve Onarım Yönetimi Kontrolleri

Neleri Ele Alıyor?

- Şirket ya da Kurumumun Değişimi Nasıl Yönettiği Neden Önemlidir?
- BT Değişim Yönetimi, **En Riskli Alanlar**
- İç Denetçilerin Değişim ve Onarım Yönetiminin Kontrolündeki Rolü Nerede Başlar?
- Değişim ve Onarım Yönetimi Denetim Programının Hazırlanması
- Örnek Vakalar, Analizler
- Değişim Yönetiminin Kontrolüne Dönük Araç ve Yazılımlar, Tedarikçileri

....

GTAG-2 : Değişim ve Onarım Yönetimi Kontrolleri

Zayıf Bir Değişim Yönetimine Dair En Yüksek 5 Risk Göstergesi

- *Yetkisiz Gerçekleştirilen Değişiklikler (Sıfırdan büyük her rakam kabul edilebilir değil)*
- *Planlanmamış Duraksamalar, Kesintiler*
- *Düşük Değişim Başarı Oranı*
- *Olağanüstü Durum Değişiklik Sayısındaki Yükseklik*
- *Ertelenmiş Proje Uygulamaları, Teslimatları*

....

GTAG Dizini

GTAG'lar

PG GTAG-15: Bilgi Güvenliği Yönetimi (Information Security Governance)
PG GTAG-14: Kullanıcı Bazlı Geliştirilen Uygulamaların Denetimi (Auditing User-developed Applications)
PG GTAG-13: Otomasyonda Yolsuzlukların Tespiti ve Önlenmesi (Fraud Prevention and Detection in an Automated World)
PG GTAG-12: BS Projelerinin Denetimi (Auditing IT Projects)
PG GTAG-11: BS Denetim Planının Geliştirilmesi (Developing the IT Audit Plan)
PG GTAG-10: İş Sürekliliği Yönetimi (Business Continuity Management)
PG GTAG-9: Kimlik ve Erişim Yönetimi (Identity and Access Management)
PG GTAG-8: Uygulama Kontrollerinin Denetimi (Auditing Application Controls)
PG GTAG-7: Bilgi Sistemlerinin Dış Kaynaklardan Tedariki (Information Technology Outsourcing)
PG GTAG-6: Bilgi Sistemlerinin Zayıf Noktalarının Denetim ve Yönetimi (Managing and Auditing IT Vulnerabilities)
PG GTAG-5: Gizlilik Risklerinin Yönetim ve Denetimi (Managing and Auditing Privacy Risks)
PG GTAG-4: Bilgi Sistemleri Denetiminin Yönetimi (Management of IT Auditing)
PG GTAG-3: Sürekli Denetim: Güvence, İzleme ve Risk Değerlemeye Dönük Sonuçlar (Continuous Auditing)
PG GTAG-2: Değişim ve Onarım Yönetimi Kontrolleri (Change and Patch Management Controls:Critical for Organizational Success)
PG GTAG-1: Bilgi Teknolojileri Kontrolleri (Information Technology Controls)

Teşekkürler

Dr. Eren GEGİN

erengegin@yahoo.com

BTYD 2010

www.btyd.org