Siber Güvenlik ve Denetim

Servet Gözel, CISA

Direktör, Bilgi Sistemleri Risk Yönetimi

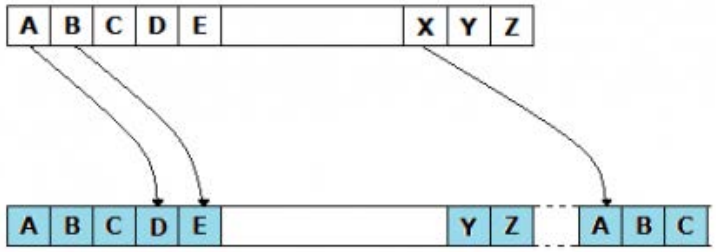
Ekim 2018

KPMG

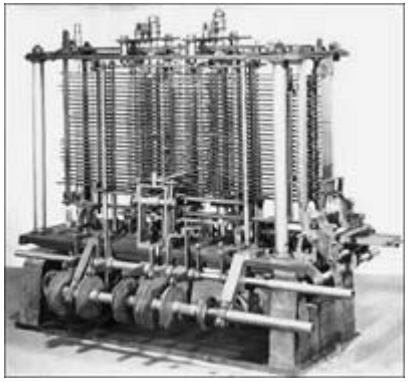
Kısa Bir Tarihçe

Kısa Bir Tarihçe

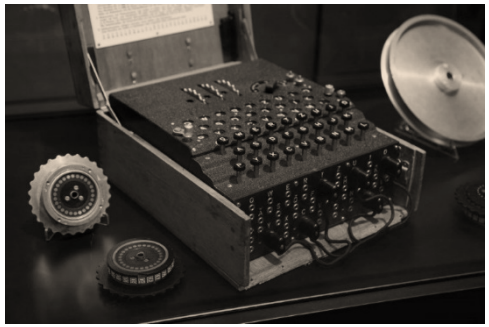
M.Ö. 200, Sezar'ın Şifresi



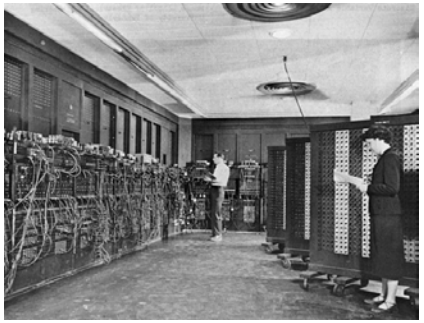
1837, Charles Babbage, Analytical Engine



1920'ler, Enigma



1946, ENIAC

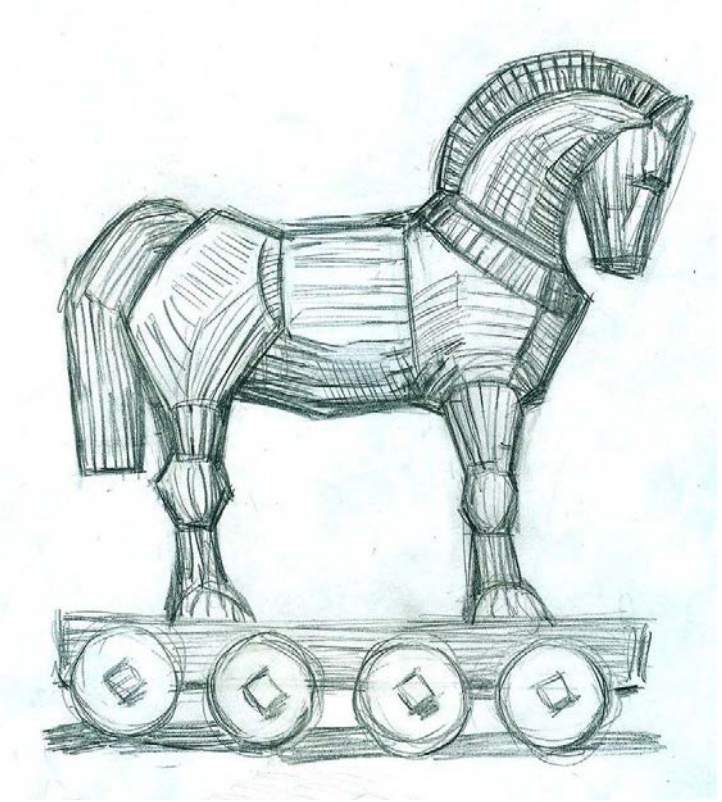


© 2018 KPMG Bağımsız Denetim ve SMMM A.Ş., bir İsviçre kuruluşu olan KPMG International Cooperative'e bağlı bağımsız üye firmalardan oluşan KPMG ağının üyesi bir Türk şirketidir. Tüm hakları saklıdır.

Kısa Bir Tarihçe

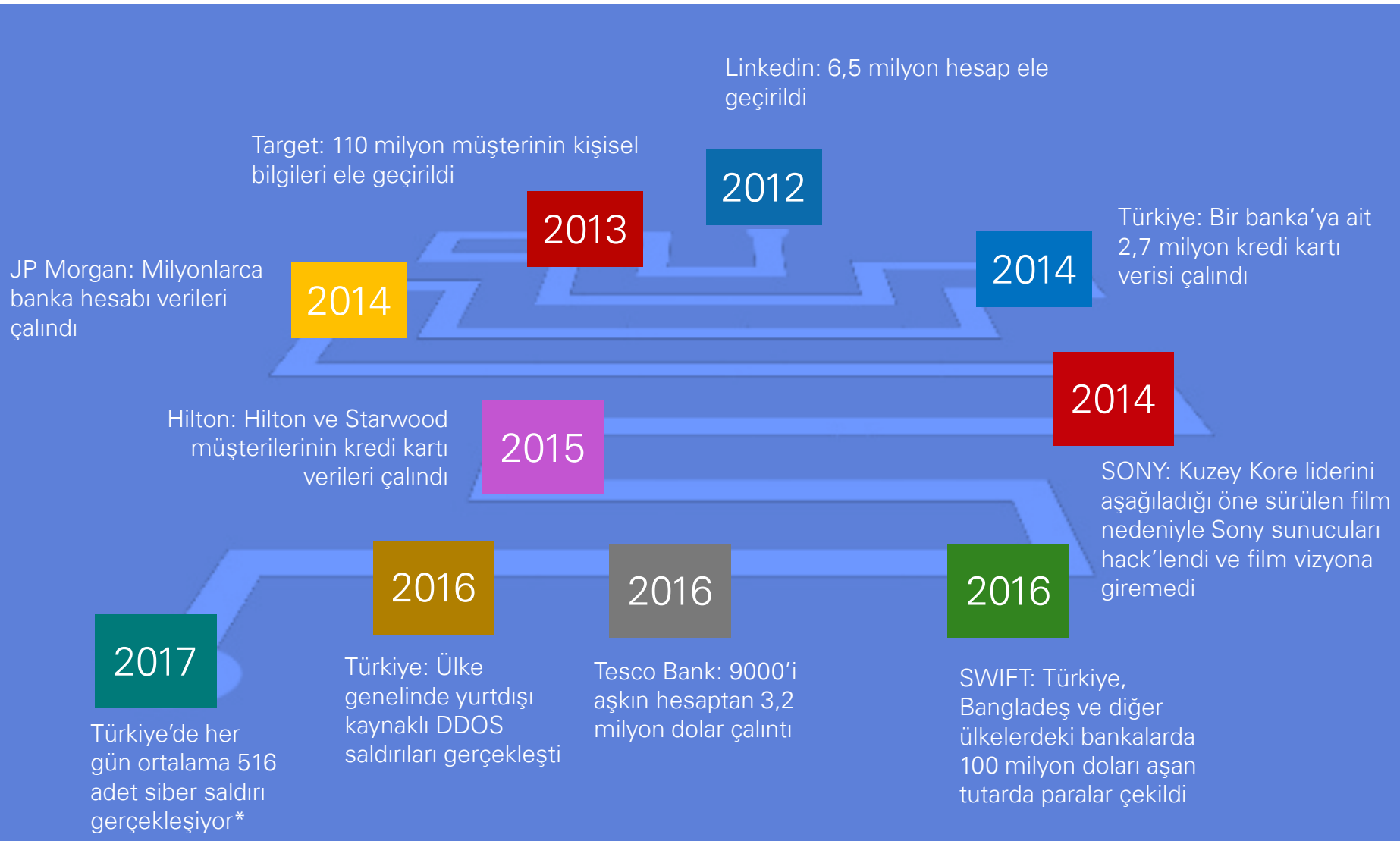
İlk Virüs ve Anti-Virüs

- 1971'de BBN adlı bir şirkette yayıldı
- Tenex OS işletim sistemi koşan sistemlere bulaştı
- Arpanet üzerinden ağdaki bilgisayarlara yayıldı
- Creeper'ın ortaya çıkması Reaper'ın ortaya çıkmasına sebep oldu



© 2018 KPMG Bağımsız Denetim ve SMMM A.Ş., bir İsviçre kuruluşu olan KPMG International Cooperative'e bağlı bağımsız üye firmalardan oluşan KPMG ağının üyesi bir Türk şirketidir. Tüm hakları saklıdır.

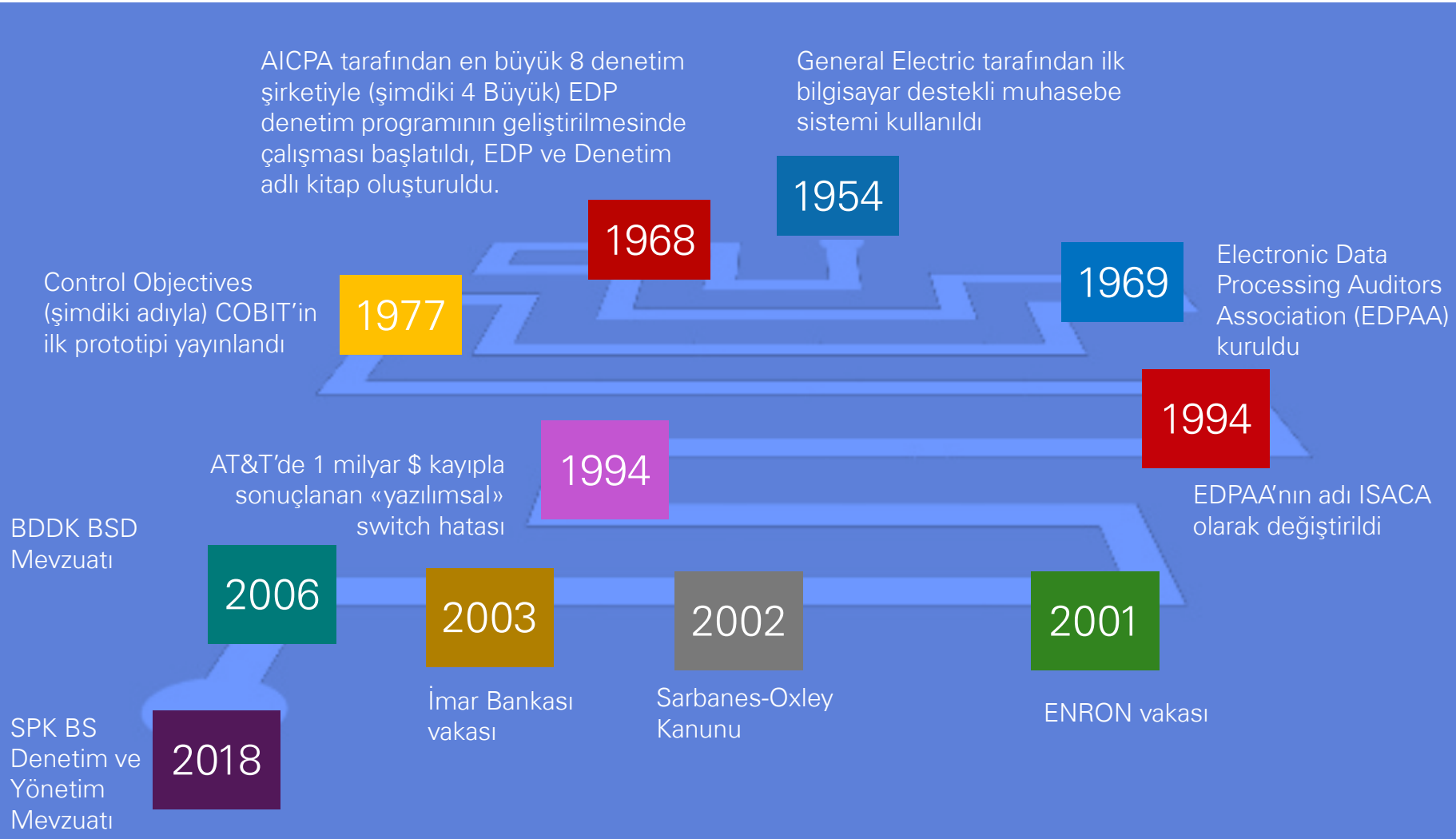
Yakın Dönem Siber Saldırılar



Kaynak: Fortune Türkiye

* Kaynak: Arbor Atlas

Denetimde Bilgi Sistemlerinin 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	Gümrük ve Ticaret Bakanlığı	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

© 2018 KPMG Bağımsız Denetim ve SMMM A.Ş., bir İsviçre kuruluşu olan KPMG International Cooperative'e bağlı bağımsız üye firmalardan oluşan KPMG ağının üyesi bir Türk şirketidir. Tüm hakları saklıdır.

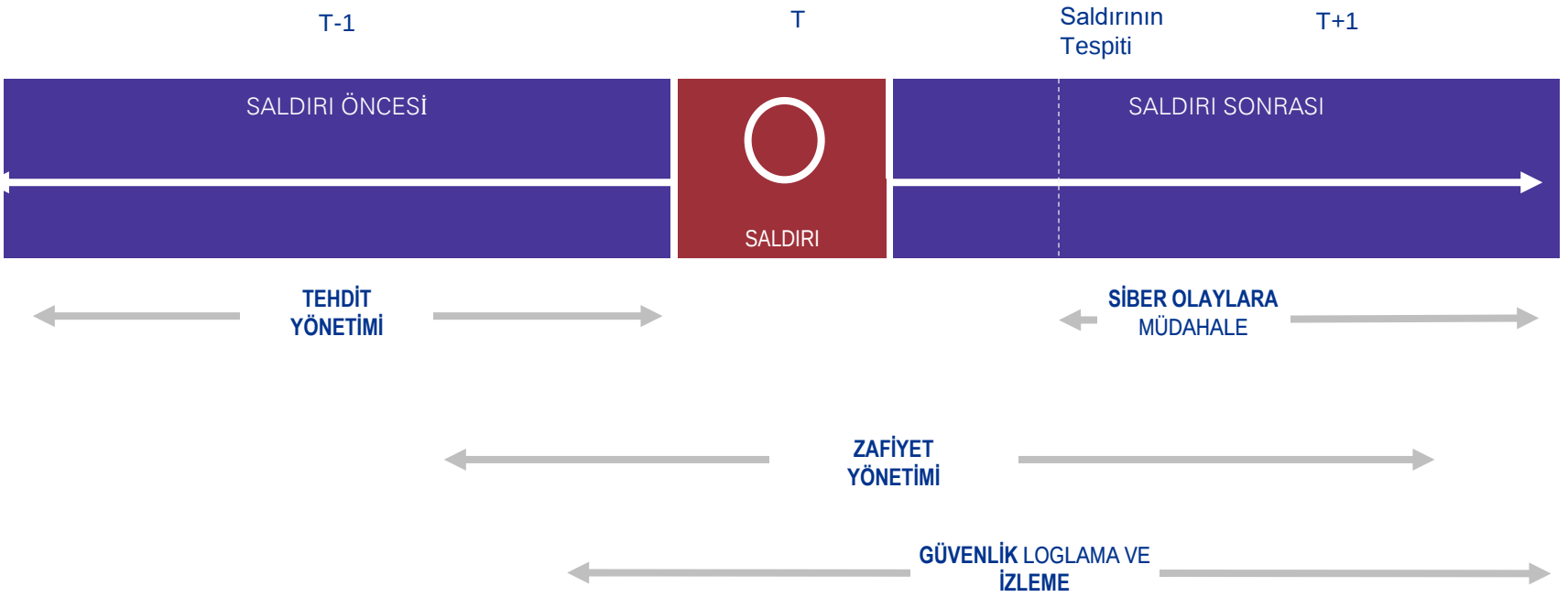
KPMG

Siber Güvenlik Çerçevesi

Siber Güvenlik Çerçevesi

Bir Saldırının Anatomisi

Etkin bir siber güvenlik çerçevesi, saldırı öncesi tehditlerin ve zafiyetlerin farkında olunmasını ve yönetilmesini, olası saldırıların tespit edilebilmesi için güvenlik olaylarının izlenmesini ve saldırı sonrasında etkin bir siber olaylara müdahale sürecine sahip olunmasını gerektirir.



© 2018 KPMG Bağımsız Denetim ve SMMM A.Ş., bir İsviçre kuruluşu olan KPMG International Cooperative'e bağlı bağımsız üye firmalardan oluşan KPMG ağının üyesi bir Türk şirketidir. Tüm hakları saklıdır.

Siber Güvenlik Çerçevesi

Uçtan Uca Siber Güvenlik Çerçevesi

STRATEJİ VE YÖNETİŞİM

- Siber Güvenlik Stratejisi
- Üçüncü Parti Güvenlik Risk Yönetimi
- Siber Olgunluk Değerlendirmesi
- Uyum/Yapı Değerlendirme
- Gizlilik / KVKK

DÖNÜŞÜM

- Kimlik ve Erişim Yönetimi
- Güvenlik Denetimi, Risk ve Uyum
- Loglama, İzleme ve Analiz Etme
- Varlık Koruması

SİBER SAVUNMA

- Sızma Testleri
- Uygulama Güvenliği
- Sosyal Mühendislik Testi
- Hizmet Dışı Bırakma Testi (DDOS)
- Fiziksel Güvenlik
- Kaynak Kodu Analizi
- Güvenlik Operasyonları Danışmanlığı
- Yeni Jenerasyon SOC
- SAP Güvenliği
- Endüstriyel Kontrol Sistemleri Güvenliği (SCADA)

SİBER OLAYLARA MÜDAHALE

- Siber Olaylara Müdahale
- İhlal Sonrası Hizmetler
- Siber Tehdit Simülasyonları

© 2018 KPMG Bağımsız Denetim ve SMMM A.Ş., bir İsviçre kuruluşu olan KPMG International Cooperative'e bağlı bağımsız üye firmalardan oluşan KPMG ağının üyesi bir Türk şirketidir. Tüm hakları saklıdır.

Siber Güvenlik Çerçevesi

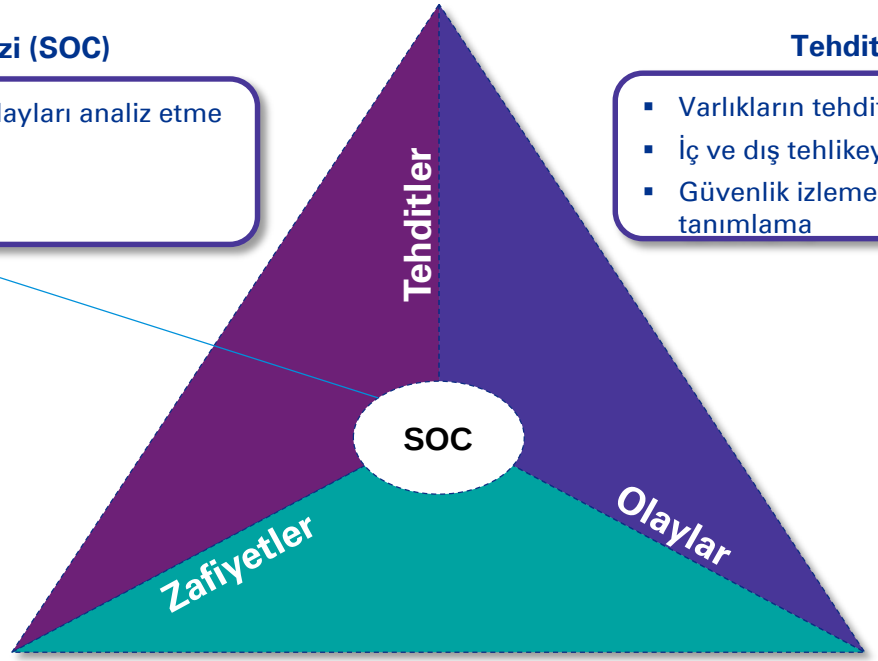
SOC (Güvenlik Operasyonları Merkezi)

Güvenlik Operasyon Merkezi (SOC)

- İzleme aracı (SIEM) kullanarak olayları analiz etme
- İzleme kurallarını koruma
- Kritik olayların eşkâle edilmesi

Tehdit Yönetimi

- Varlıkların tehdit düzeyini belirleme
- İç ve dış tehlikeye karşı bilgi akışlarını analiz etme
- Güvenlik izleme için kullanım durumlarını tanımlama



Zafiyet Yönetimi

- BT varlıklarının ve güvenlik açıklarının denetimi
- Güvenlik testlerinin koordinasyonu
- Zayıf noktalar hakkında izleme koordinasyonu

Olay Yönetimi

- Rapor edilen olayların önceliklendirilmesi
- Olay tepkisinde destek verilmesi
- Olayların kök-neden analizi

KPMG

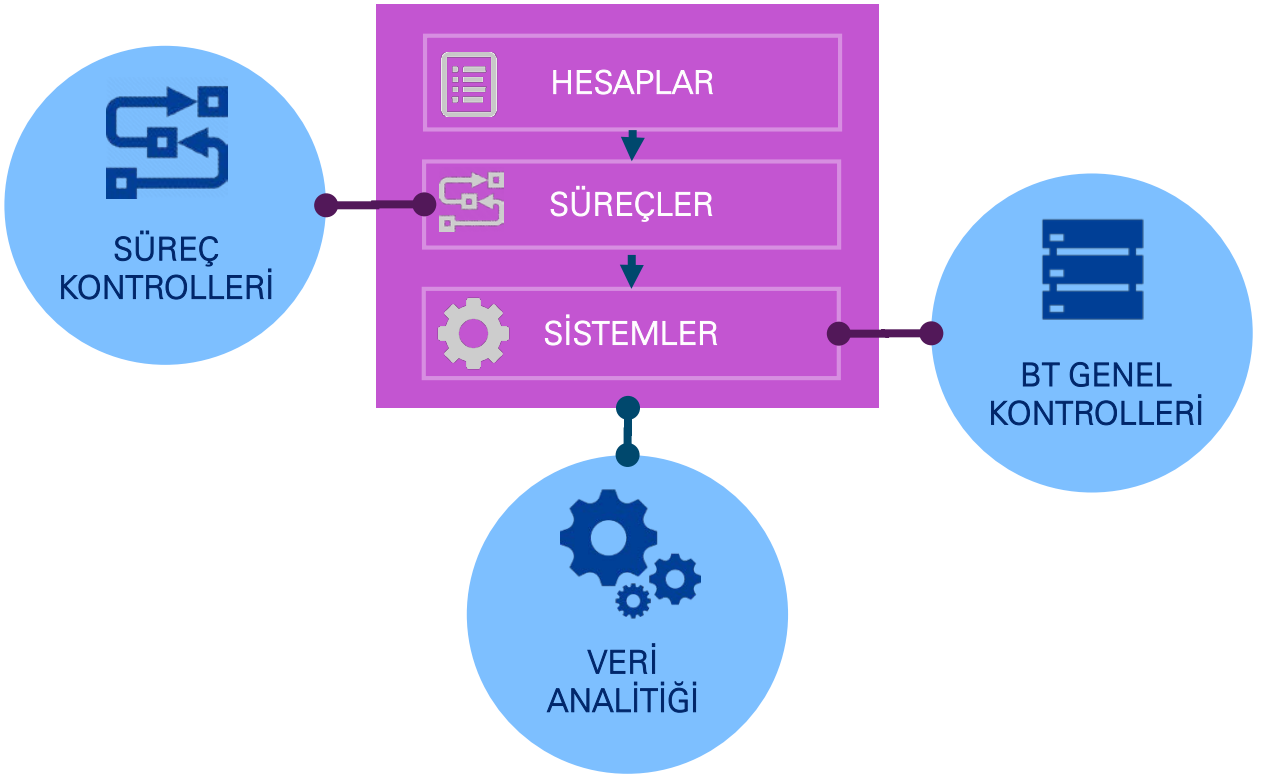
© 2018 KPMG Bağımsız Denetim ve SMMM A.Ş., bir İsviçre kuruluşu olan KPMG International Cooperative'e bağlı bağımsız üye firmalardan oluşan KPMG ağının üyesi bir Türk şirketidir. Tüm hakları saklıdır.

KPMG

Siber Güvenlik ve Denetim

Geleneksel Bilgi Sistemleri Denetimi

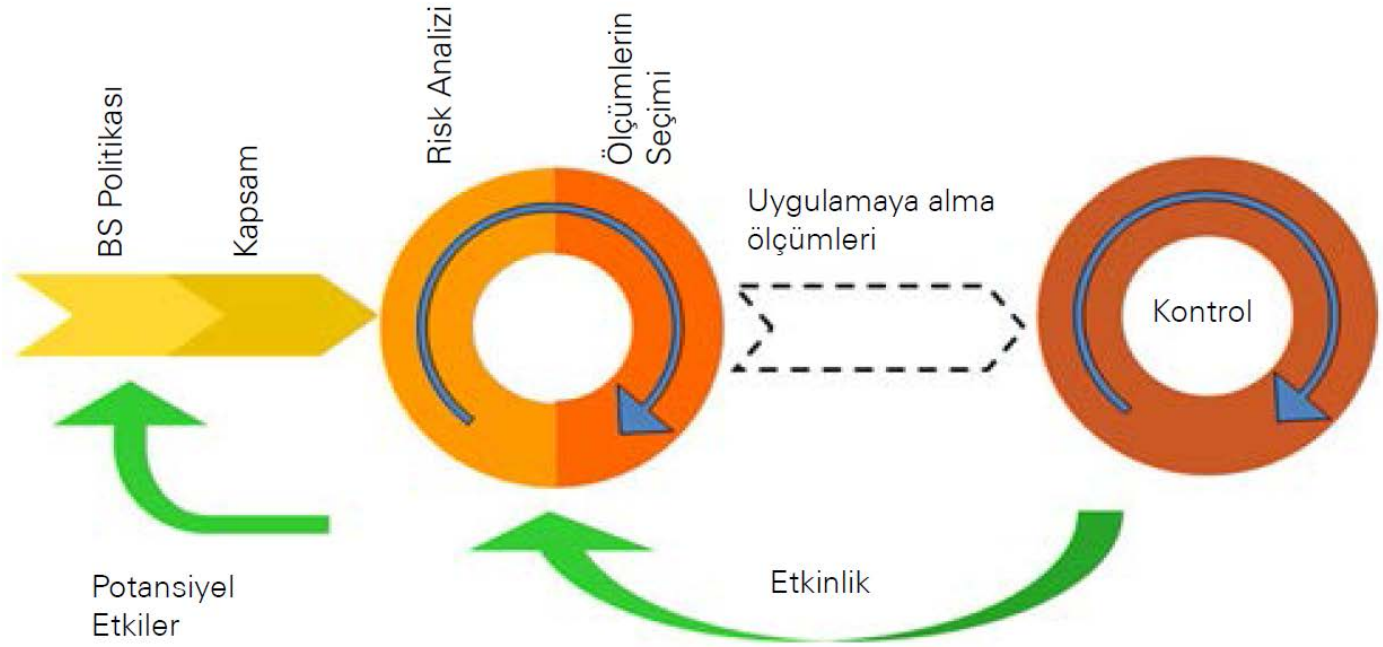
Alışılagelmiş bilgi sistemleri denetimi yaklaşımında, önemli finansal hesapları oluşturan süreçlerde yer alan otomatik kontrollerin test edilmesi, bu kontrollerin yürütüldüğü genel BT kontrollerinin test edilmesi ve sistemler üzerinde yer alan verilerin derinlemesine ve geniş popülasyonlarla veri analitiği prosedürlerine tabi tutulması yer almaktadır.



© 2018 KPMG Bağımsız Denetim ve SMMM A.Ş., bir İsviçre kuruluşu olan KPMG International Cooperative'e bağlı bağımsız üye firmalardan oluşan KPMG ağının üyesi bir Türk şirketidir. Tüm hakları saklıdır.

Geleneksel Bilgi Güvenliği Yaklaşımı

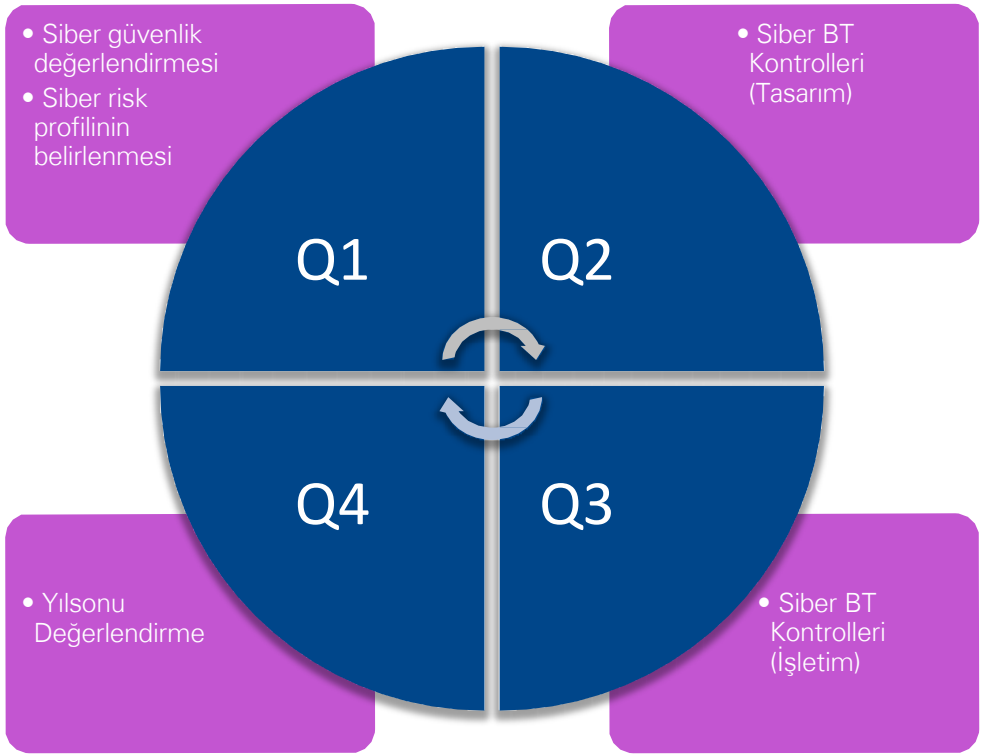
Geleneksel bilgi güvenliği yönetimi yaklaşımında, süreç ve varlıkların risk değerlendirmesinin gerçekleştirilmesi, risk iştahına göre önlemlerin uygulamaya alınması ve sürekli izleme faaliyetleri bulunmaktadır. Bu yaklaşım bilgi güvenliği politika ve prosedürleri esasına dayanmaktadır.



© 2018 KPMG Bağımsız Denetim ve SMMM A.Ş., bir İsviçre kuruluşu olan KPMG International Cooperative'e bağlı bağımsız üye firmalardan oluşan KPMG ağının üyesi bir Türk şirketidir. Tüm hakları saklıdır.

Önerilen Siber Denetim Yaklaşımı

KPMG'nin Siber BT Kontrolleri (CITC) yaklaşımına göre, BT genel kontrolleri ve süreç kontrollerinin yanı sıra, kuruluşun ilk çeyrekte siber ortamının anlaşılması ve risk profilinin belirlenmesi, ikinci çeyrekte, siber BT kontrollerinin tasarımının değerlendirilmesi, üçüncü çeyrekte işletim testlerinin yapılması, son çeyrekte ise yılsonu test çalışmaları ve değerlendirmelerin finalize edilmesi bulunmaktadır.



© 2018 KPMG Bağımsız Denetim ve SMMM A.Ş., bir İsviçre kuruluşu olan KPMG International Cooperative'e bağlı bağımsız üye firmalardan oluşan KPMG ağının üyesi bir Türk şirketidir. Tüm hakları saklıdır.

Siber Güvenlik Değerlendirmesi

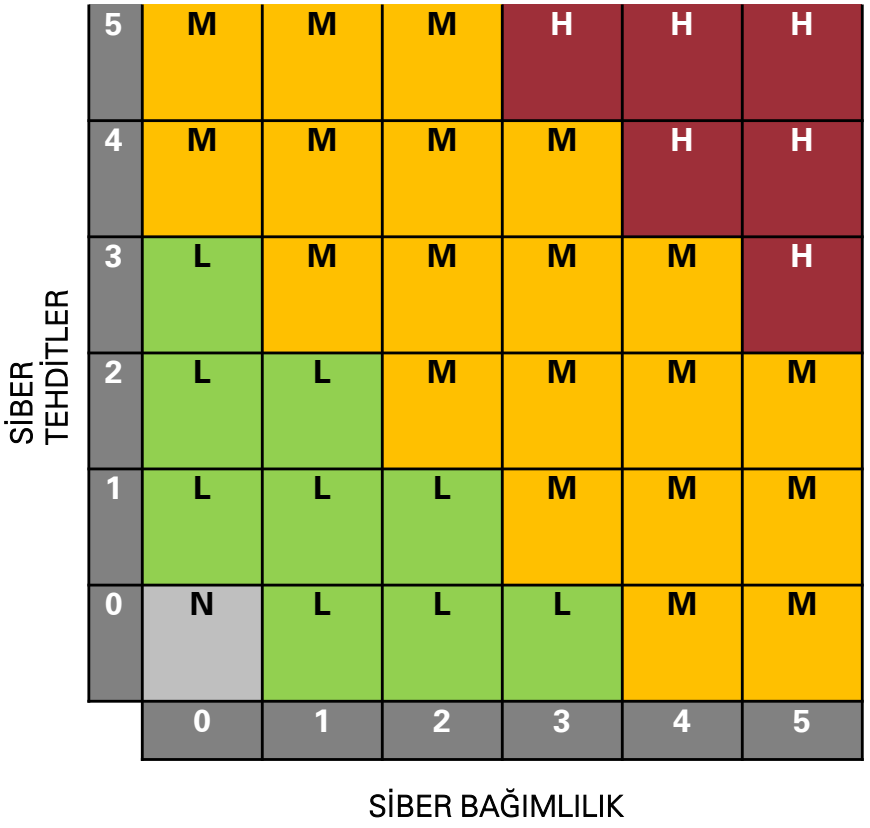
Siber güvenlik değerlendirmelerinin kuruluşların genel risk yönetim ilkelerine uygun olması için risk bazlı bir yaklaşım uygulanır. Bu sayede risklerin etkin bir şekilde devamlı olarak yönetilmesine yardımcı olunur. KPMG'nin Siber Güvenlik Olgunluk Modeli 6 ana alandan oluşur:

© 2018 KPMG Bağımsız Denetim ve SMMM A.Ş., bir İsviçre kuruluşu olan KPMG International Cooperative'e bağlı bağımsız üye firmalardan oluşan KPMG ağının üyesi bir Türk şirketidir. Tüm hakları saklıdır.

Siber Güvenlik ve Denetim

Siber Risk Profili Oluşturma

Uçtan uca siber olgunluk ve risk değerlendirme yaklaşımının yanında, kuruluşun kıymetli bilgi varlıklarına bağımlılık seviyesi ile dışarıda ve içeride maruz kalabileceği siber tehdit seviyesi belirlenir ve buna göre kuruluşun genel siber risk profili ortaya çıkar.



© 2018 KPMG Bağımsız Denetim ve SMMM A.Ş., bir İsviçre kuruluşu olan KPMG International Cooperative'e bağlı bağımsız üye firmalardan oluşan KPMG ağının üyesi bir Türk şirketidir. Tüm hakları saklıdır.

Siber Güvenlik ve Denetim

Siber BT Kontrolleri

Denetim esnasında değerlendirilmesi önerilen siber BT kontrolleri, üç ana başlıkta toplanabilir:

YÖNETİŞİM

- Siber güvenlik politikası
- Siber güvenlik farkındalığı
- Sistem ve veri sınıflandırması

OPERASYONLAR

- Zafiyet yönetimi
- Tehdit yönetimi
- Siber güvenlik olay izleme ve belirleme
- Siber güvenlik olaylarına müdahale

TEKNİK KONTROLLER

- BT güvenlik konfigürasyonu
- BT güvenlik önlemleri
- BT altyapı ve ağ güvenliği
- Son kullanıcı güvenliği
- Mantıksal erişim yöntemleri

KPMG

© 2018 KPMG Bağımsız Denetim ve SMMM A.Ş., bir İsviçre kuruluşu olan KPMG International Cooperative'e bağlı bağımsız üye firmalardan oluşan KPMG ağının üyesi bir Türk şirketidir.
Tüm hakları saklıdır.

Saldırıların Denetime Etkisi

Genel değerlendirmelerin dışında, kuruluşta gerçekten bir saldırı gerçeklemiş olabilir. Bu durumda, denetçi gerçekleşen vakayı detaylı irdelemeli, kök nedenini tespit etmeli, denetime ve finansallara etkisini değerlendirmeli ve tespit edilen zafiyetlerin kısa vadede ve uzun vadede çözümü için kuruluşla yakın çalışmalıdır.

© 2018 KPMG Bağımsız Denetim ve SMMM A.Ş., bir İsviçre kuruluşu olan KPMG International Cooperative'e bağlı bağımsız üye firmalardan oluşan KPMG ağının üyesi bir Türk şirketidir.
Tüm hakları saklıdır.

İletişim:

Servet Gözel
Direktör
Bilgi Sistemleri Risk Yönetimi

T: +90 212 316 61 76
E: servetgozel@kpmg.com

KPMG Türkiye
İstanbul, Levent
İş Kuleleri Kule 3, Kat 2-9
Levent/İstanbul