

# VII.BİLGİ TEKNOLOJİLERİ YÖNETİŞİM VE DENETİM KONFERANSI

**3-4 MART 2016**

## Suistimali Önlemenin ve İncelemenin Metodları

Çiğdem GÜRER, CFE, SMMM

GRR Danışmanlık – İç Sistemler ve Risk Yönetim Hizmetleri

# Çiğdem GÜRER – 16 yılın özeti



1999: Marmara Üniversitesi İngilizce İktisat

1999-2002: Deloitte Vergi

**Deloitte.**

2002-2007: Cognis Finansal Kontrolör



2003: SMMM

2007 – 2015 KPMG & EY Risk Danışmanlığı & Suistimal Önleme ve İnceleme



2011: SPK Denetim Lisansı



2008: CFE



2015: KGK Denetim Lisansı



2015: GRR & Nazalı



VII.BİLGİ TEKNOLOJİLERİ YÖNETİŞİM VE DENETİM KONFERANSI

3-4 MART 2016, İSTANBUL

# İki İyi Dost

BT Uzmanı



Suistimal İnceleme  
Uzmanı (CFE)



# Suistimal Nedir?

Yasal bir tanımı yok.

**SUISTİMAL:** Farsça *sūʿ-i istiʿmāl* " kötüye kullanma" deyiminden alıntıdır. Farsça deyim Arapça *sūʿ* " kötülük, fenalık" ve Arapça *istiʿmāl* " kullanma" sözcüklerinin bileşiğidir.

**SUISTİMAL:** *ACFE (Uluslararası Suistimal Soruşturmacıları Derneği)*'ye göre bir kişinin mesleki görevini, şirketinin varlıklarını ve kaynaklarını amacı dışında ve yanlış kullanmak suretiyle kişisel çıkar sağlamak ve zenginleşmek.

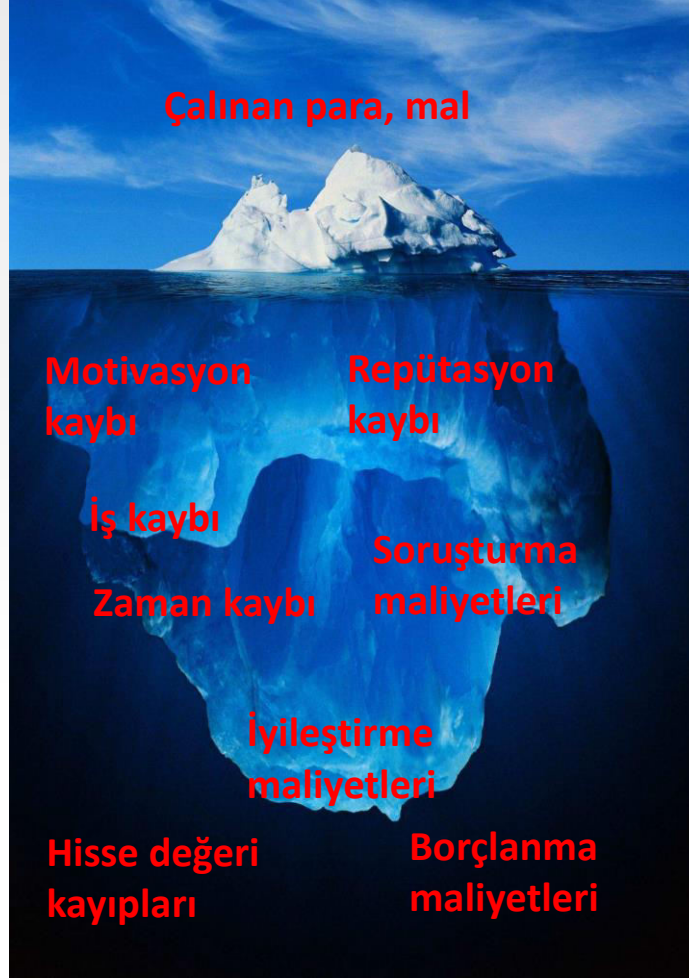
**SUISTİMAL:** *Uluslararası Denetim Standartlarına* göre; işletmenin yöneticileri, çalışanları veya işletme ile ilgili üçüncü kişilerin bir veya daha fazlası tarafından kendilerine adil olmayan ve illegal bir avantaj sağlamak üzere giriştikleri kasıtlı ve aldatıcı davranışlar hile olarak tanımlamaktadır.

**SUISTİMAL:** *Bizim ilgilendiğimiz şekliyle;* kişisel bir çıkar için çalışanın sorumluluk ve yetkilerini kötüye kullanması; kanunları, düzenlemeleri, şirket politika ve prosedürlerini ve ahlaki gereklilikleri ihlal etmesi.

# Suistimalin Maliyeti

Doğası gereği GİZLİ

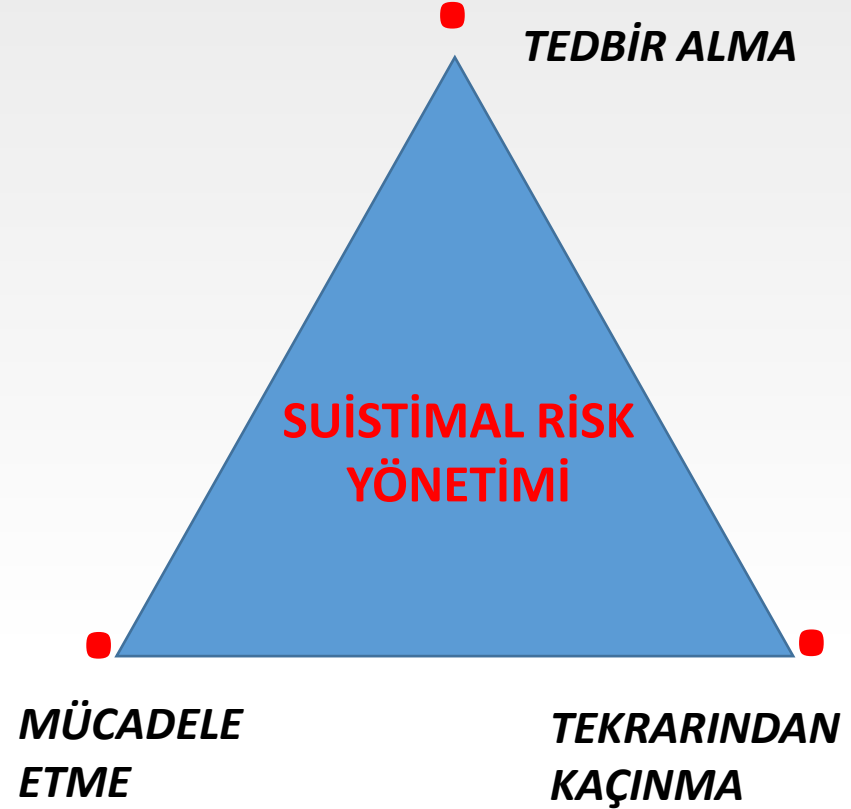
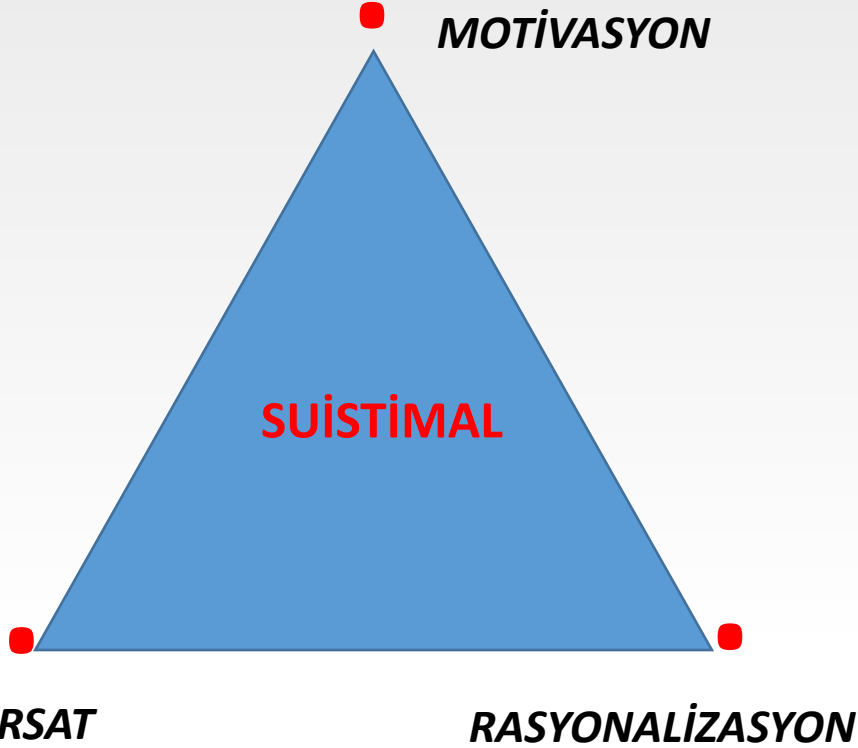
2013 Gayrisafi  
Küresel Hasıla'ya  
göre 3.7 trilyon \$



Brüt gelirlerin %5'i

Brüt gelirlerinizi %5  
artıracak bir yol  
biliyoruz desek?

# İki Suistimal Üçgeni\*



\* Donald Cressey – Other People's Money (1973)

# Suistimal Risk Yönetimi

## SUISTİMAL RİSK YÖNETİMİ

### Tedbir Alma

- suistimal karşıtı kültür oluşturulması
- **suistimal risklerinin belirlenmesi**
- uygun kontrollerin konulması
- **kontrollerin etkinliğinin düzenli gözden geçirilmesi**
- Davranış Kuralları
- eğitimler
- politika ve prosedürler
- üçüncü şahıs gözden geçirmeleri
- müşterilerin, tedarikçilerin de ilgili kurallardan haberdar olması

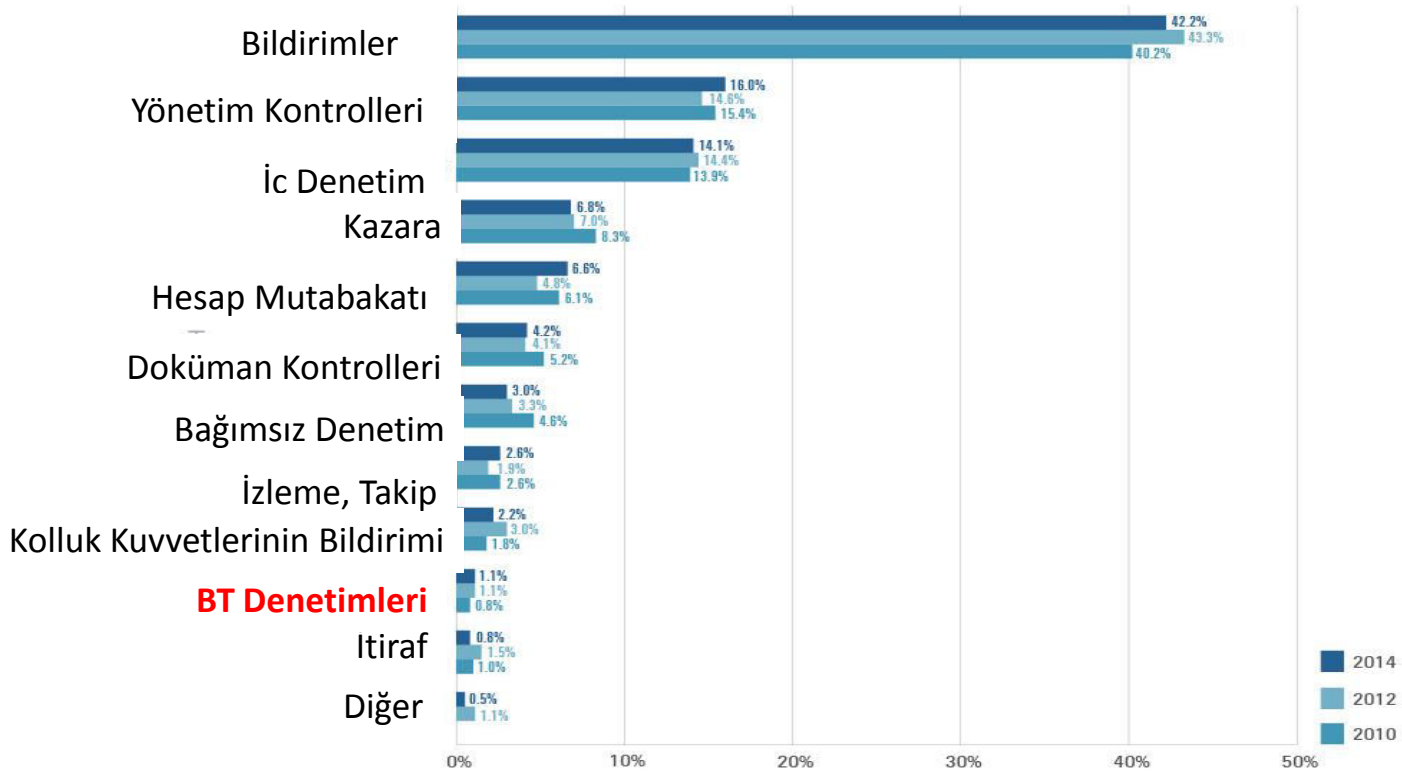
### Ortaya Çıkarma

- bildirim mekanizması
- **düzenli veri analizleri**
- sürpriz denetimler / sayımlar
- bildirim protokolleri
- iletişim planı
- **soruşturma**

### Tekrarından Kaçınma

- **kontrollerin gözden geçirilmesi**
- politika prosedürlerin güncellenmesi
- eğitimlerin tekrarlanması
- ilgili iletişim

# Ortaya Çıkarma Yöntemleri\*



\* ACFE 2014 Report to the Nations on Occupational Fraud and Abuse



# Suistimale Savaşta Teknolojiyi Kullanmak

## Kaynaklar:

- Bilgisayarlar
- E-postalar
- Sunucular
- Akıllı telefonlar
- Tabletler
- Bulut bellekleri
- Dış bellekler

## Avantajları:

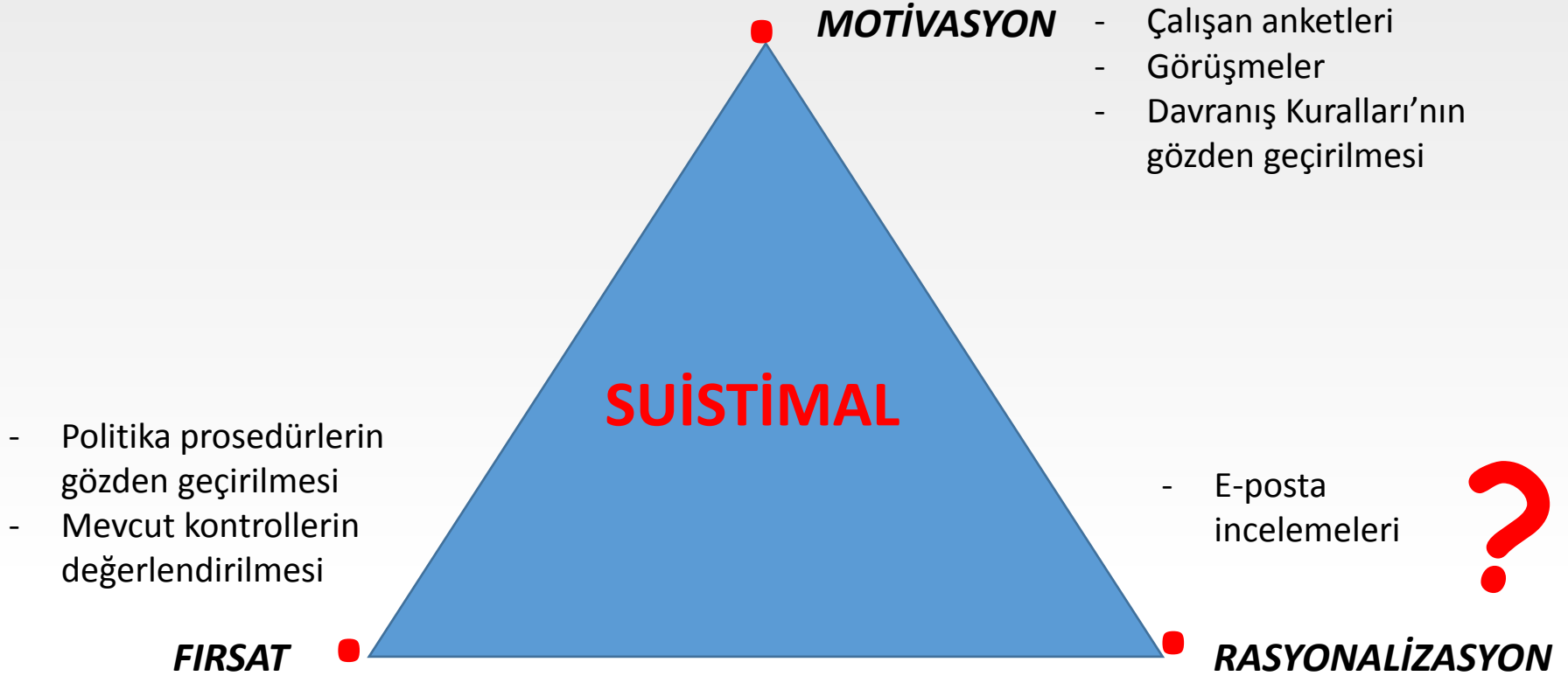
- Çok fazla verinin işlenebilmesi
- Hızlı veri işleme
- Silinmiş verilerin geri getirebilmesi (e-postalar ve Office dokümanları)
- Kullanıcıların isteyerek saklamadığı verilere ulaşılabilmesi (bilgisayarın hafızasında)

## Son yıllarda daha çok kullanılan yeni yöntemler:

- Anahtar kelime aramaları
- İnternet geçmişi
- Chat / mesajlaşma servisleri
- Akıllı telefon backup'ları
- Akıllı telefonların hafızasındaki fotoğraflardan GPS koordinatları
- Arama geçmişlerinden kullanıcının yerinin belirlenmesi
- Trend ve ilişki haritaları
- İşlem logları



# Suistimal Üçgeni Analitiği



# Veri Analizi – Düzensiz Veri

Şirket verilerinin %80'i (e-postalar, prezentasyonlar, internet belgeleri, sosyal medya, videolar) düzensiz (unstructured)

→ Kullanılan mevcut veri analizi teknikleri %20'lik düzenli (structured) veri üzerinde çalışıyor.

**OYSA**

E-postalarda Benford Yasası uygulanabilir mi?

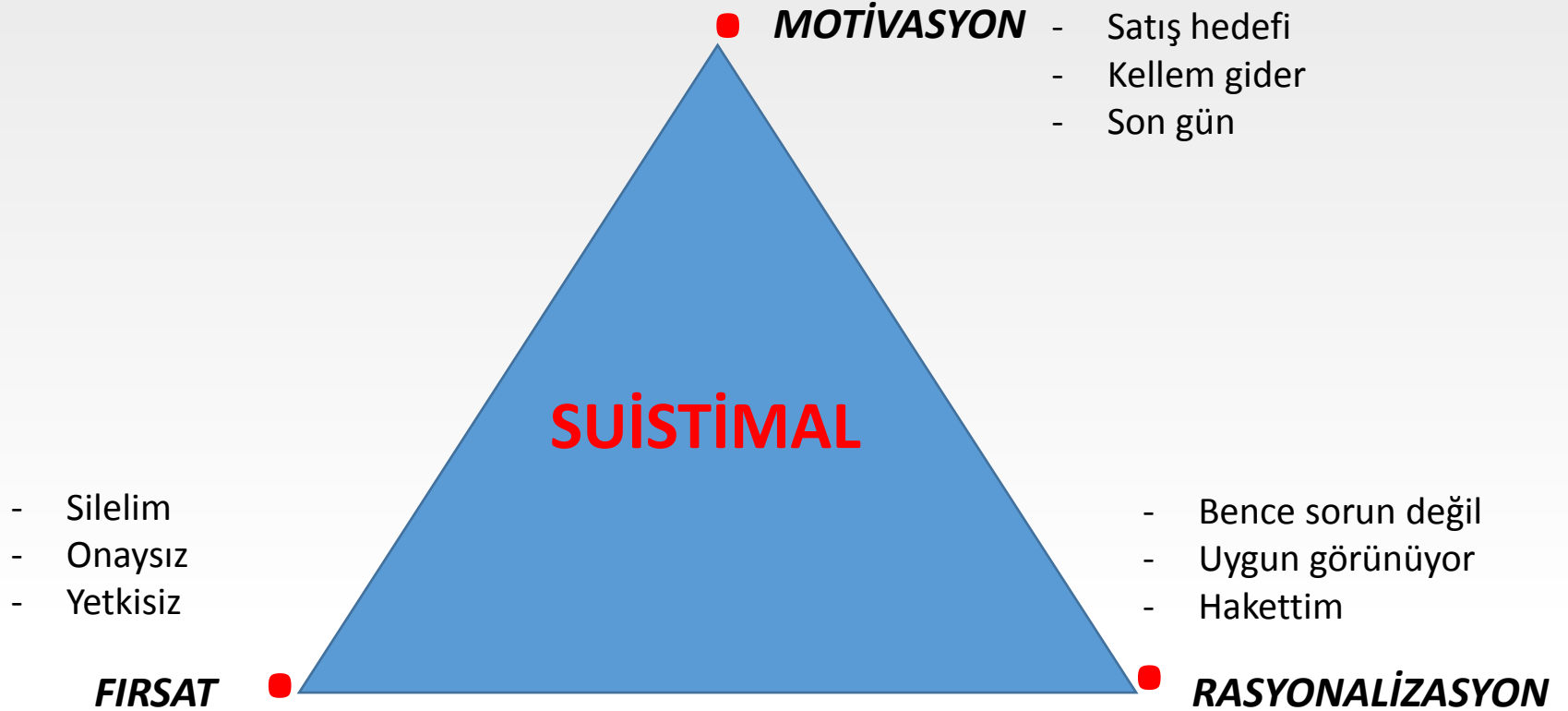
Metin bazlı bilgiler analiz edilirse, suistimalin:

- Kim
  - Ne
  - Ne zaman
- soruları yanıtlanabilir.



**Kişisel verilerin korunması?**

# E-posta Analizi



*Her bir suistimal çeşidi (finansal tablo suistimalleri, yolsuzluk, şirket kaynaklarının kötüye kullanımı gibi) için, her bir suistimal üçgeni elementini kapsayan **3.000'den fazla** anahtar kelime (key word) bir araya getirilmiş.*

# Veri Analizi – Kolay Yoldan Sürekli Denetim Sürekli Gözetim

## Uygulama Adımları:

- 1) Yönetimi ikna etmek / BT desteği sağlamak / Verilerin nerede depolandığını ve nasıl elde edilebileceğini öğrenmek
- 2) Süreci, riskleri, kontrolleri anlamak / Planlama safhası / Gerekli verilerin belirlenmesi
- 3) Verinin elde edilmesi (en zaman alan bölüm)
- 4) Verinin arındırılması (gereksiz verinin, yanlış pozitiflerin temizlenmesi)
- 5) Verinin incelenmesi / İncelemenin sonuçlandırılması
- 6) SDSG haline getirilmesi  
/ Periyodik olarak tekrarlanması

## Veri analizi ile cevaplanabilecek sorulara örnekler:

- Sahte tedarikçiler
- Tedarikçi ödemelerindeki anormallikler
- Hayalet çalışanlar
- Müşteri ödemelerinin saklandığı hesaplar
- Giderlerin politika ve prosedürlere uyumu (ilaç sektörü)
- Stok hareketlerindeki düzensizlikler
- Satın alımların mal kabulü ve faturalar ile incelenmesi

**Veri Analizi:** Şirketlerin günlük işleyişleri sırasında ürettiği farklı kaynaklardaki verilerin, çeşitli karşılaştırmalar, özetler, toplamalar yapılmak yoluyla muhtemel anormallikleri bulmak amacıyla incelenmesi.

# Soruşturmalar Sırasında BT - Dijital Kanıt Toplama

## İmaj Alma > Tek Atış hakkı

Şüpheli ve ilgililerin bilgisayarlarının / telefonlarının, tabletlerinin, **alet açılmadan**, tek bir bit'i değişmeden yalnızca okunabilir / incelenebilir / değiştirilemez kopyasını almak.



## “Bulut”taki Bilgilerin İncelenmesi

- Şirketin dokümanları ve proje yönetimi bir “bulut”ta, e-mailleri başka buluttaysa...
- Peki bulut nerede?
- Olduğu yerdeki kişisel bilgi yasaları ile soruşturmanın yapıldığı yerdeki yasalar uyuyor mu?
- Hangisi uygulanacak?
- Backuplar’da sadece bizim verilerimiz mi var?
- Nasıl ayrılacak?

# Vaka Yönetim (Case Management) Programları

## Soruşturmacının kabusu:

- Pek çok farklı formatta önemli veriye sahip olup, bunları anlamlı bir şekilde bir araya getirememek:
- e-postalar
- mesajlaşmalar
- telefon görüşmeleri
- tanık ifadeleri

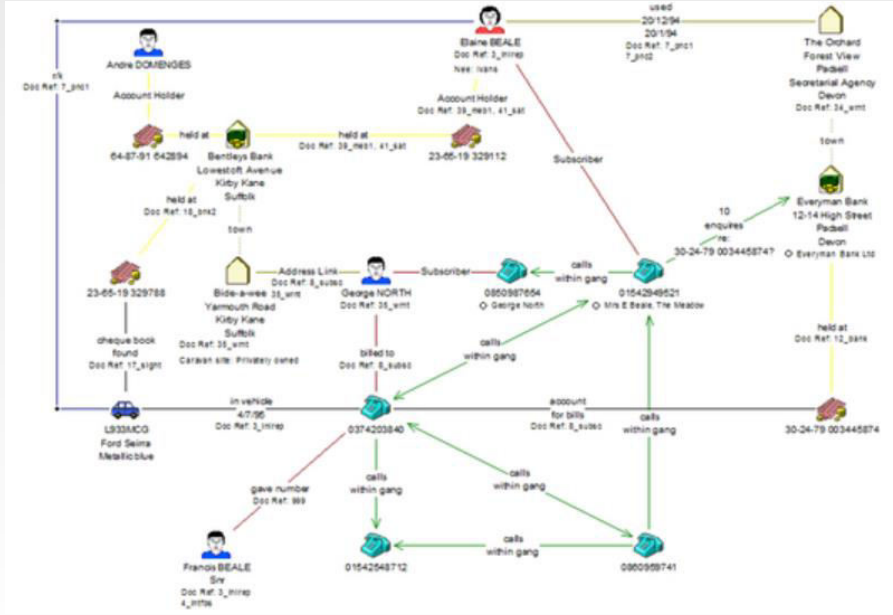


## Artık suistimal vakaları:

- Birden çok kişi
- Birden çok şirket
- Birden çok ERP
- Birden çok veri kaynağı
- Birden çok suistimal çeşidi
- Kişiler arasında karışık ilişkiler ve hatta
- Birden çok ülke içerebiliyor.

- Takımla anlık olarak paylaşamamak
- Soruşturmanın kalanında faydalı olacak şekilde saklayamamak
- İstenen hızda ve formatta raporlayamamak
- Dava sürecinde avukatlarla etkin paylaşımında bulunamamak ve dava dosyasına tüm detayları sağlayamamak.

# Vaka Yönetim (Case Management) Programları -2



## Doğru program seçilirken:

- Ne kadar yoğun veriyle aynı anda çalışmaya olanak sağlıyor?
- Hangi veri türlerini işleyebiliyor?
- Çeşitlenen ihtiyaçlara cevap verebilecek kadar esnek mi?
- Ne kadar alan kaplıyor?
- Aynı anda kaç kullanıcının kaç farklı işlem yapmasına olanak veriyor?
- Çeşitli yetkide kullanıcılar oluşturulmasına izin veriyor mu?
- Aynı anda kaç vakanın çalışılmasına izin veriyor?
- Mevcut sistemdeki verilerin aktarılması mümkün mü?
- Güvenlik konusunda BT ekibini ikna edebiliyor mu?

Elektronik olan ya da elektroniğe dönüştürülebilen verileri bir araya getirip anlamlı bir şekilde Suistimal Soruşturmacısı'na sunan programlar.



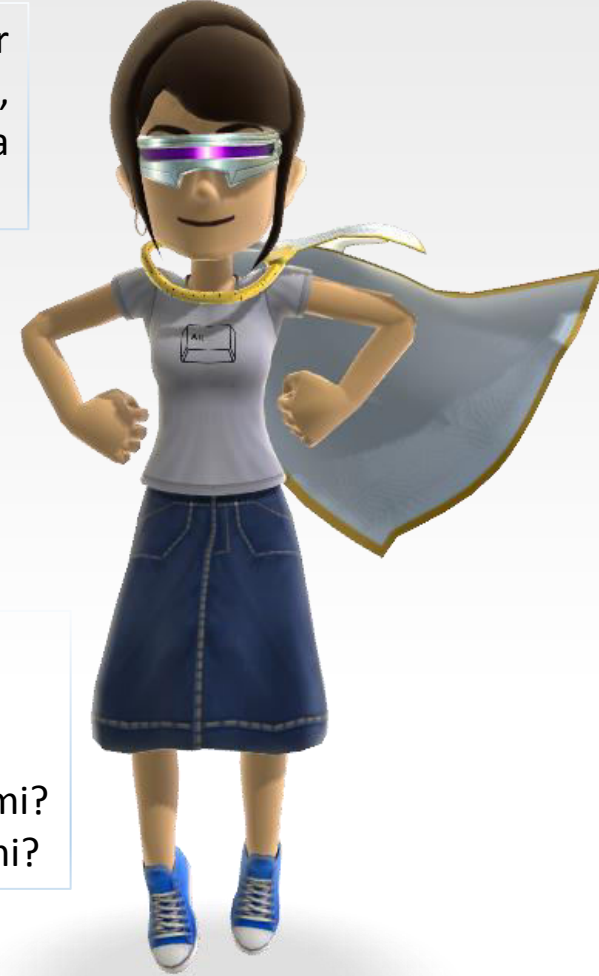
# Şimdilik son nokta: Avatar Görüşmeleri

Şimdilik sadece Arizona sınırında kullanılıyor. Gelenlere bazı sorular soruyor, hem cevaplarını, hem davranışlarını (mimik artışı, azalışı, nefes alıp verme hızı, vücut ısısı, tonlamalar) değerlendirip sonuca varıyor.

- Kullananlar rahat hissediyor mu?
- Gerçek bir insanla konuşur gibiler mi?
- Sonuçlar ne kadar güvenilir?
- Mahkemede kullanılabilir mi?
- Peki empati???

Elbette insanların görüşmeleri kadar esnek ya da başarılı değil.

- Ama bazı basit aşamalarda kullanılabilir mi?
- Görüşülen kişi sayısının artırılmasını sağlar mı?
- Ya da görüşme öncesi kullanılıp asıl görüşme için veri sağlayabilir mi?
- İnsanlar bazı konuları canlı olmayan birine daha rahat anlatabilir mi?



# Sonuç



