SACIS EXPO 2006

IT AUDIT UYGULAMA BAŞARISI

NİLHAN FİDAN

Ernst & Young, Müdür

Teknoloji ve Güvenlik Risk Hizmetleri

5 Mayıs 2006, İstanbul

IT Denetimi

- Risk Değerlendirmesi
- Kontrollerin tespiti
- İyileştirme noktaları

? Çalışanlarınızdan biri bir güvenlik vakası ile karşılaşsa bunu görmezden mi gelir? Kime nasıl raporlar?
? Şirketinizde toplam kaç adet bilgisayar bulunuyor? Bir tanesi ortadan kaybolsa bunu nasıl fark edersiniz?
? Kurum bilgi sistemlerini kullanan kaç kişi var? Bu kişilerin gerçekten yetkili kişiler olup olmadığını ve erişimlerini kimse takip ediyor mu?
? En son virüs saldırısından etkilendiniz mi? Bu yıl kaç virüs saldırısı yaşadınız?
? Kurumun en kritik bilgi varlıkları nelerdir? Bu varlıkların korunması için neler yapılmaktadır?
? Gizli şirket bilgilerinin dışarıya sızması nasıl engellenmektedir?
? Şirket bilgisayar ağının güvenliği test edilmiş midir?
? IT güvenliği yönetim toplantılarında gündeme gelen bir konu mudur?

IT Denetimi

- NEDEN ? **IT Riskleri**

IT Denetim Standartları

+ En iyi uygulamalar, uzmanlık, bilgi & beceri
+ Zaman & maliyetten tasarruf
+ Başarısızlık riskini azaltma

- Standartların yeterince ayrıntılı olmaması
- Statik yaklaşım & karşılaşılabilecek problemler
- Her zaman tek bir doğrunun olmaması

Kritik Başarı Faktörleri ve Zorluklar

- Sınav psikolojisi
- Hedef…sonuç…süreç
- Yönetim desteği
- Kurum kültürü
- Tepkiler, itirazlar… ve kabullenme
- IT ve güvenlik konularındaki bilinç

IT Denetimi'nin Geri Dönüşü

- Güvenlik risklerine karşı önlem alınmadığı takdirde şirket itibarının zedelenmesi, müşteri ve gelir kaybı olasıdır.
- Ancak bu olasılığa göre bir maliyet çıkarmak ve IT Denetimi'nin geri dönüşünü sayısal olarak ifade etmek oldukça zordur. Çünkü:
  - Gerçekleşen tüm IT problemleri fark edilmemektedir.
  - Fark edilen tüm IT problemleri raporlanmamaktadır.
  - Raporlanan IT problemleri merkezi bir veritabanında saklanmamaktadır.
  - IT problemlerinin gerçekleşme sıklığını öngörmeye yetecek düzeyde bilgi mevcut değildir.

IT Denetimi Başarısı

- Bağımsız ve objektif değerlendirme
- Bilgi kaynaklarına yönelik muhtemel tehditler ve açıkların, potansiyel ya da mevcut risklerin anlaşılması
- Bu risklerin kapatılması için gerekli bilgi ve en iyi uygulamalar hakkında bilgi edinilmesi
- Operasyonel risklerin kontrol altına alınarak yasal uyumluluğunun sağlanması
- Yatırımcıların finansal raporlamada şeffaflık beklentisine cevap verilmesi
- Risk yönetimi uygulamalarının güçlendirilmesi
- Üst yönetim gündemine IT konularının dahil edilmesi
- Donanım ve yazılımların daha etkin bir şekilde kullanılarak maliyette tasarruf edilmesi ve teknoloji varlıklarının daha iyi değerlendirilmesi