



# ISO/IEC 27001

**BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ  
& BELGELENDİRMESİ SEMİNERİ**

**18 Haziran 2009, İstanbul**

**ITMS DAYS**

[www.itmsdays.com](http://www.itmsdays.com)

Information Technologies Management Systems Days

# Kařitest

## FİNANS PİYASALARINDA BİLGİ GÜVENLİĞİ VE ISO 27001

Dr. İzzet Gökhan ÖZBİLGİN

Biliřim Uzmanı, SPK

# Finansal Piyasalar



# Finansal Piyasalar

- İnternet bankacılığı
- Elektronik ortamda emir iletimi
- Portföy yöneticiliği
- Hesap bilgileri
- Kredi kartları
- Elektronik imza
- ...

# Finansal Piyasalar

**GÜVEN**



Sistemik Risk

Bilgi Güvenliđi  
(ISO 27001)

## Dünyadan...

- **IMF**
- **Dünya Bankası**
- **Kreditkort-İzlanda**
- **Bank of Ghana**
- **OECD...."Securities Activity on the Internet"**
- **SOX**
- **COSO, COBIT...**
  - **"Mapping between COBIT, ITIL and ISO 27001"**
- **BASEL II**
  - **Piyasa riski, kredi riski ve OPERASYONEL RISK**

## Türkiye'den...

- **SPK**
  - MKK
  - Borsalar
  - Aracı Kurumlar
  - Yatırım Fonları
- **BDDK**
  - Bankalar
- **Uygulamalar: e-imza, KAP, internet bankacılığı...**
- **Mevzuata uyum, Bilişim suçları...**

## BGYS'nin Getirdikleri

- Uluslararası kabul görmüş yapısal bir metodoloji
- Sertifika,
  - kurumun güvenlik seviyesiyle ilgili bir gösterge
  - güvenliğe ciddi yaklaşımın bir göstergesi
  - bir imaj konusu

## BGYS'nin Getirdikleri

- Yaşayan bir yönetim sistemi (portal, aylık toplantılar, yönetim desteği, eğitim vb.)
- Kuruma uygun politikalar, prosedür ve talimatlar oluşturmaya yol göstermesi
- Güvence standardı

## SPK

- Sermaye piyasasının güven, açıklık ve kararlılık içinde çalışmasını sağlamak için SPK'nın **bilgi** varlıklarına **zamanında, eksiksiz, doğru ve kesintisiz** biçimde ulaşması büyük önem taşımaktadır.
- Bu kapsamda, SPK'nın bilgi varlıklarını **bilinçli ve sistematik** olarak **koruması ve yönetmesi** çok önemlidir.

## SPK ve BGYS

- “...Kurulumuz yönetimi bilgi güvenliğinin sahip olduğu yaşamsal önemin bilincinde olarak Bilgi İşlem, İstatistik ve Enformasyon Dairesi **Bilgi Teknolojileri Hizmetleri** kapsamında BGYS kurulmasına karar vermiştir...”

***Bilgi Güvenliği Politikası***

## BGYS ve Sertifikasyon Süreci

- Yönetimin desteđi
- Gerekli eğitim ve danışmanlık hizmetleri
- Bilgi Güvenliđi Forumunun oluşturulması
- Varlıkların tespiti
- Risk analizi
- Dokümantasyon (politika, yönerge vb. )
- Başvuru ve ön dokümanların gönderilmesi
- Denetimleri gerçekleştirilmesi
- ISO / IEC 27001 sertifikası (01.06.2006)

## Kritik Başarı Faktörleri

- Yönetim desteği ve bilgilendirme
  - Yönetim tarafından onaylanan ve yayınlanan bir **Bilgi Güvenliği politikası** hayata geçirildi.
  - Bu politika, “**İç Genelge**”yle kurum personeline ve “**WEB sayfamız**” yoluyla da ilgili dış taraflara duyuruldu.

# Kritik Başarı Faktörleri

- Yasa ve düzenlemelere uyum
  - BGYS yasa ve düzenlemelere uygun olarak hazırlandı.
  - Yasa ve düzenlemeler?
    - 657 sayılı Devlet Memurları Kanunu
    - Türk Ceza Kanunu
    - Fikir ve Sanat Eserleri Kanunu
    - Sermaye Piyasası Kanunu
    - SPK Yönetmelikleri (Personel, Teşkilat, Muhasebe)

# Kritik Başarı Faktörleri

## ➤ Eğitim

- Bilgi güvenliği kapsamında üst yönetim dahil eğitimler alındı.
- Farkındalık ve bilinç düzeyi artırıldı.

# Kritik Başarı Faktörleri

## ➤ Risk Analizi

- **Varlıkların Belirlenmesi:** Varlıklar belirlendi ve 0(önemsiz)- 4(çok önemli) arasında değerler atandı. (96 adet varlık)
- **Açıklıklar ve Tehditlerin Belirlenmesi:** Varlıklara ait açıklıklar ve varlıklara yönelik tehditler belirlendi.

# Kritik Başarı Faktörleri

## ➤ Risk Analizi

- **Tehditlerin Mutlak Etkilerinin Belirlenmesi:** 0(önemsiz)-4(çok ciddi) arasında her tehdide gizlilik, bütünlük ve erişebilirlik açısından değerler atandı.
- **Tehditlerin Gerçek Etkilerinin Belirlenmesi:** Tehditlerin mutlak etkileri varlıkların değerleri ile ilişkilendirildi. Bu durumda bir varlık-tehdit ikilisi, gizlilik, bütünlük ve erişebilirlik açısından ayrı ayrı ele alınmış oldu. (Toplam 331 adet varlık-tehdit ikilisi)

# Kritik Başarı Faktörleri

## ➤ Risk Analizi

➤ **Tehditlerin Gerçekleşme Olasılığının Belirlenmesi:**0(gerçekleşemez)-4(çok yüksek) arasında her tehdide olma ihtimali atandı.

➤ **Varlıklara ait Risklerin Belirlenmesi:**Her varlık için gizlilik, bütünlük ve erişebilirlik açısından 3 farklı risk değeri hesaplandı.

➤  $Risk_g = \text{Tehdidin Olma İhtimali} * \text{Tehdidin Gerçek Etkisi}_g$

➤  $Risk_b = \text{Tehdidin Olma İhtimali} * \text{Tehdidin Gerçek Etkisi}_b$

➤  $Risk_e = \text{Tehdidin Olma İhtimali} * \text{Tehdidin Gerçek Etkisi}_e$

# Kritik Başarı Faktörleri

## ➤ Risk Analizi

- **Kabul Edilebilir Risk Düzeyinin Belirlenmesi:** İlk risk analiz çalışması olduğundan bu düzey “0” kabul edildi. Böylece tüm risklerin belirlenmesi sağlandı.
- **Artık Risk Düzeyinin Belirlenmesi:** Hesaplanan risk değerlerinden kabul edilebilir risk düzeyleri (=0) çıkartılarak kritik varlıklar belirlendi. Böylece kritiklik derecesine göre varlıklar sıralandı.

# Kritik Başarı Faktörleri

- Destek Politikalar(5 adet)
  - Ağ Yönetimi Politikası
  - Sistem Yönetimi Politikası
  - Erişim Denetimi Politikası
  - Uygulama Geliştirme Politikası
  - Uygun Kullanım Politikası

# Kritik Başarı Faktörleri

- Yönergeler (31 adet)
  - Ayrıcalık Yönetimi Yönergesi
  - Dış Kaynak Kullanımı Yönergesi
  - Doküman Yönetimi Yönergesi
  - Fiziksel ve Çevresel Güvenlik yönergesi
  - İç Tetkik Yönergesi

## Kritik Başarı Faktörleri

- Yönergeler (31 adet)
  - Yedekleme ve Kurtarma Yönergesi
  - Web Sitesi Yönetim Yönergesi
  - Personel Güvenliği ve Eğitim Yönergesi
  - Yardım Masası Yönergesi
  - Kullanıcı Parola Yönetim Yönergesi

# Kritik Başarı Faktörleri

## ➤ İzleme

- Risk Analizi çalışması periyodik olarak yılda en az bir(1) kere yapılmaktadır.
- Ayrıca
  - Yeni bir bilgi sistemi devreye alındığında,
  - Yeni bir uygulama başlatıldığında,
  - Yeni teknolojiler uyarlandığında,
  - Yeni bir görev tanımı yapıldığında vb.

riskler gözden geçirilmektedir.

# Kritik Başarı Faktörleri

## ➤ İzleme

- Ayrıca yapılan “Genel İç Tetkik” sonucunda tüm BGYS’nin genel bir değerlendirilmesi yapılır.
- “Uygulanabilirlik Bildirgesi” gözden geçirilir.

# Kritik Başarı Faktörleri

## ➤ Sertifikasyon

- TSE'ye başvuru
- TSE tetkiki
- ISO/IEC 27001 sertifikası (1/6/2006)

## BGYS'nin Getirdikleri

- Sermaye Piyasası Kurulu Bilgi Güvenliđi Yönetim Sistemi'ni Uluslararası Standarda (ISO/IEC 27001) uygun hale getiren ilk Kamu Kurumu olmuştur.( 01.06.2006)
- DPT Müsteşarlığı koordinasyonunda hazırlanan “E-Dönüşüm Türkiye Projesi Birlikte Çalışabilirlik Esaslar Rehberi”nde Bilgi Güvenliđi Yönetim Sistemini tamamlayan kurumların bunu belgelendirmeleri öngörülmüştür.



# TEŞEKKÜRLER

