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

SERMAYE PİYASALARINDA BİLGİ TEKNOLOJİLERİ

Dr. İzzet Gökhan ÖZBİLGİN, SPK,
İş Geliştirme ve Analiz Grup Başkanı

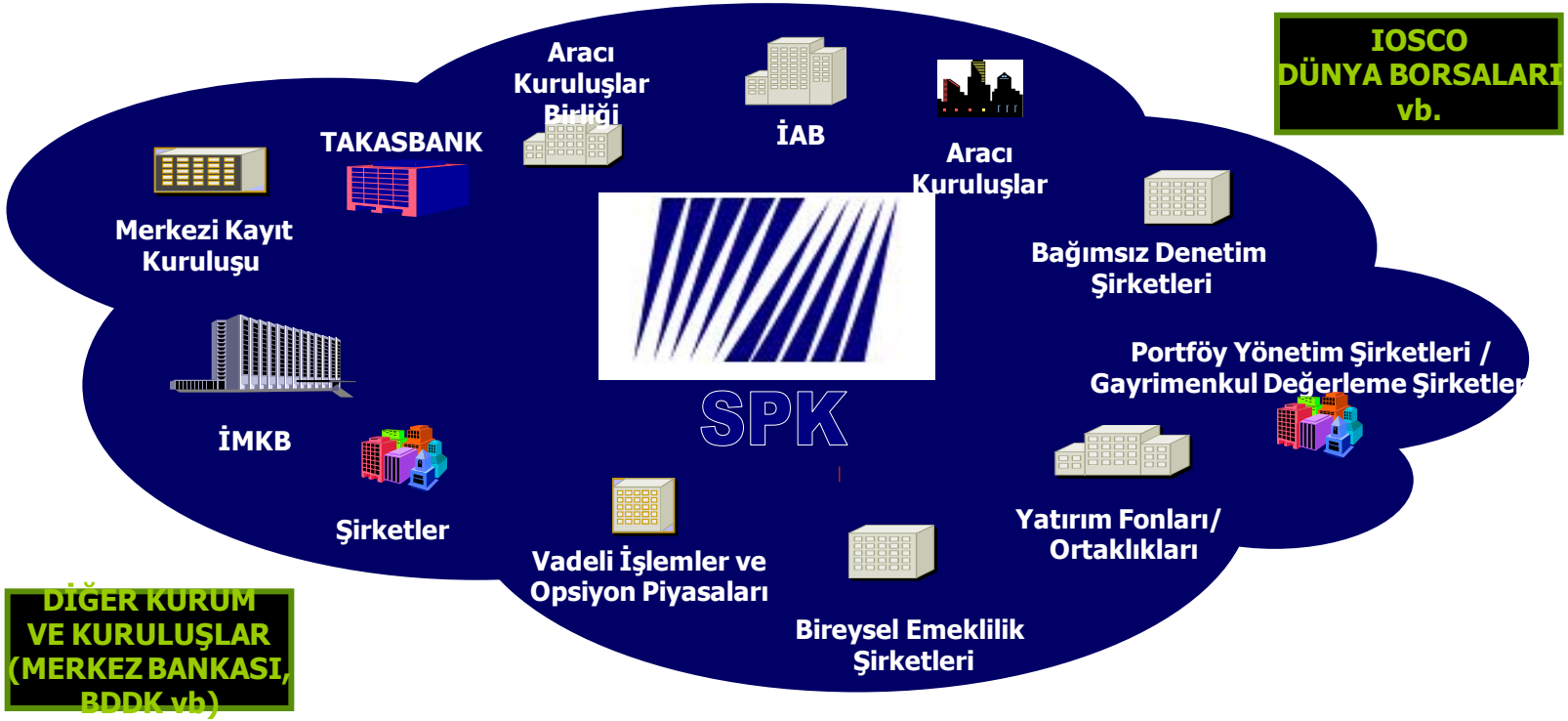
Sunum Planı

- Sermaye Piyasası Kurulu (SPK)
- Sermaye Piyasaları ve Bilgi Sistemleri
- SPK ve Bilgi Sistemleri İncelemesi
  - Neden ihtiyaç duyuldu?
  - Neler yapıldı?
  - Nasıl yapıldı?
  - Neler planlanıyor?
- Genel Değerlendirme

Sermaye Piyasası Kurulu

- Düzenleyici ve denetleyici bir kamu kurumu
- Kurul'un temel görevi:
  - Sermaye piyasasının güven, açıklık ve kararlılık içinde çalışmasını,
  - Tasarruf sahiplerinin yani yatırımcıların hak ve yararlarının korunmasını sağlamaktır.
- Kurul bu hedeflere
  - Kanun, yönetmelik ve tebliğlerle düzenlemeler yaparak,
  - piyasaların gözetim ve denetimini sağlayarak ulaşmaya çalışmaktadır.

Sermaye Piyasası ve İlgili Kurum/Kuruluşlar



Sermaye Piyasaları ve Bilgi Teknolojileri

- Borsalara uzaktan erişim imkanı
  - İşlem hızlarının artması
  - İşlem maliyetlerinin azalması
- İnternetin yaygınlaşması ve geniş bir yatırımcı kitlesi
- Aracısızlaşma, online işlemler
- Bilgiye hızlı ve rahat erişim
- e-imza uygulamaları, ispat ve geri bildirim şekilleri vb.
- Uzaktan gözetim ve denetim, iç kontrol, operayonel risk
- ....

Sermaye Piyasaları ve Bilgi Teknolojileri

- KAP
- SERYET
- OFDOS
- FONORT
- eCAS
- ASUR
- …

Bilgi Teknolojileri ile Gelen Riskler

- Yazılı ortamdan sanal ortama geçiş
- İşlemleri ve kurumları denetlemenin güçleşmesi
- Güvenlik riskleri
- Personel
- Sistem problemleri, ağ kesintileri
- …
    - OPERASYONEL RİSKLER

Yapılan Faaliyetler

1. Ön Hazırlıklar
2. Düzenlemeler ve standartlar
3. BGYS süreci: Önemli bir tecrübe
4. Yapılan İncelemeler

Yapılan Faaliyetler

1. Ön Hazırlıklar
    1. Eğitimler, seminerler
    2. Toplantılar (BDDK, Sayıştay vb.)
2. Düzenlemeler ve standartlar (SOX, COBIT, SEC, ITIL, ISO 27001 vb.)

2. Düzenlemeler ve Standartlar

Örnek bir düzenleme:SEC 17a-3/4

- Menkul kıymet işlemlerine yönelik kayıtlarla ilgili düzenleme
- Elektronik iletişim ve mesajlaşma (E-posta ve anlık mesajlaşma gibi kayıtlar) dahil
- Kayıtların, inceleme ve denetimlere uygun şekilde oluşturulması ve saklanması
- 17a-3: Kayıtların nasıl oluşturulacağı
- 17a-4: Kayıtların nasıl saklanacağı
- Benzer düzenleme: NASD 3010/3110

2. Düzenlemeler ve Standartlar

Örnek bir düzenleme:SEC 17a-3/4

- Yasaya uyum konusu çok sıkı ve cezalar çok ağır
- Yatırım bankalarının bazılarının istenilen bu gereklilikleri sağlamamasından dolayı aldığı ceza : 8 milyon $'dan daha fazla

2. Düzenlemeler ve Standartlar

Örnek bir düzenleme:SEC 17a-3/4

Company	Fine	Violation	Date
SG Cowen	$100,000	E-mails deleted before retention period expired.	May-03
Deutsche Bank Securities	$1.65 mil	Violated SEC 17a-4, NYSE 440 and NASD 3110.	Dec-02
Goldman Sachs	$1.65 mil	Violated SEC 17a-4, NYSE 440 and NASD 3110.	Dec-02
Morgan Stanley	$1.65 mil	Violated SEC 17a-4, NYSE 440 and NASD 3110.	Dec-02
Salomon Smith Barney	$1.65 mil	Violated SEC 17a-4, NYSE 440 and NASD 3110.	Dec-02
U.S. Bancorp Piper Jaffray	$1.65 mil	Violated SEC 17a-4, NYSE 440 and NASD 3110.	Dec-02

Source: Connor, Deni. "Confusion reigns over data archiving." Network World, 06/23/03.

3. BGYS süreci: Önemli bir deneyim

IQNet

THE INTERNATIONAL CERTIFICATION NETWORK

CERTIFICATE

IQNet and
TSE
hereby certify that the organization
SERMAYE PİYASASI KURULU BİLGİ İŞLEM İSTATİSTİK VE ENFORMASYON DAİRESİ

ESKİŞEHİR YOLU 5.KM NO:156 ANKARA / TÜRKİYE

has implemented and maintains a

which fulfils the requirements of the following standard

TS ISO / IEC 27001

Scope of the certificate is given in annex.
Date of Certificate: 31-07-2009
Valid Until: 31-07-2012
Registration Number : TR-BY-001/06

IQNet
René Wasmer
President of IQNet

Mukaddes İLHAN
Head of System and Personnel
Certification Department

TSE

4. Yapılan Denetimler

İSTANBUL MENKUL KIYMETLER BORSASI

VADELİ İŞLEM VE OPSİYON BORSASI
VOB

TAKASBANK

SPK

4. Yapılan Denetimler

Denetim alanları

- Kurumun BS süreçleri
- Bilgi güvenliği
- Kurum yönetimi ve personel yapısı
- Dışarıdan alınan hizmetler
  - Güvenlik Taraması Hizmeti
  - SLA
- Ağ, Sistem, Veritabanı, Uygulama Geliştirme

4. Yapılan Denetimler

- Yedeklilik ve yedekten dönme
- Dokümantasyon
- Risk analizi
- Acil Durum Planları
- Ayrıcalık Yönetimi
- İç denetim
- Uyum, Yasal yükümlülükler

Sermaye Piyasası Mevzuatından...

- **Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ**
  - “...bağımsız denetçinin risk değerlendirmesinde bilişim sistemlerini ne şekilde ele alacağı...” ve “...bilişim teknolojilerine ilişkin kontroller hakkında açıklamalar...”

Sermaye Piyasası Mevzuatından...

- **Aracılık Faaliyetinde Belge ve Kayıt Düzeni Hakkında Tebliği**
  - "...internet üzerinden alınan emirlerde tarih, zaman ve müşteri bazında olmak üzere emri ileten müşterilere ilişkin kayıtlarının …."
  - "… elektronik ortamda diğer şekillerde alınan emirlerde emri veren kaynağı gösterecek şekilde gerekli elektronik log kayıtlarının emri alan aracı kuruluşlarca tutulması zorunlu..."

Sermaye Piyasası Mevzuatından...

- **Aracı Kurumlarda Uygulanacak İç Denetim Sistemine İlişkin Esaslar Hakkkında Tebliğ**
  - "...Aracı kurumların bilgi sistemlerinin güvenliğine yönelik olarak aracı kurum personelinin görev tanımları dikkate alınarak yetkilendirmeler yapılır. Erişim ve yetkilendirme işlemleri ile sistemin sürekliliğini temin edecek yedekleme işlemleri dahil olmak üzere, bilgi sistemleri ile ilgili faaliyetlere ilişkin tüm hususlar belirlenir..."

Sermaye Piyasası Mevzuatından...

- **Aracılık Kurumlarda Uygulanacak İç Denetim Sistemine İlişkin Esaslar Hakkında Tebliğ**

- “...Aracı Kurumlar, Teftiş kurulunda görev yapacak müfettişlerde mesleki yeterlilik aramak zorundadırlar...lisans ve mesleki tecrübe...müfettişlerden bilgi teknolojileri denetimi icra edeceklerin bilgi teknolojileri ile bilgi teknolojilerine dayalı denetim teknikleri konularında.....”

Planlar ve Beklentiler

- Konsolide denetimler (finansal ve BS)
- Denetim raporlarının değerlendirilmesi
- Denetim raporlarına yönelik geri bildirimler
- Denetim alanın genişletilmesi
- Mevzuat çalışmaları
- Diğer ülke uygulamaları

Planlar ve Beklentiler

- Daha iyi bir kurumsal yönetim
- Daha iyi bir iç kontrol sistemi
- Sermaye Piyasalarında işlem şekilleri değişmektedir. Buna uygun denetim süreci geliştirilmelidir.
- BS Denetimi kanuni zorunluluk olmaktan çok profesyonel iş yapmanın gereğidir

Planlar ve Beklentiler

- Etkili bir bilgi teknolojileri denetimi için uygulayıcıların, kurumların ve yasa koyucuların bilgi teknolojileri denetim kavramını anlamaları ve kabul etmeleri gerekmektedir.
  - Kurumlararası işbirliği
- Denetim rehberi ve yol haritası

Teşekkürler...

İzzet Gökhan ÖZBİLGİN
gokhan@spk.gov.tr

BTYD 2010

www.btyd.org