



# **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



# FİNANS SEKTÖRÜNDE İLK ISO27001 SERTİFİKASYONU, DENEYİMLERİN PAYLAŞILMASI

Ercüment BÜYÜKŞUMNULU Teknoloji Hizmetleri Direktörü BKM A.Ş.

# GÜNDEM

3

- **Bankalararası Kart Merkezi A.Ş. (BKM A.Ş.)**
- **ISO27001 Standardı Kısa Bakış**
- **BKM A.Ş. ISO27001 Sertifikasyon Süreci**
- **ISO27001 Sertifikasyonu İçin İpuçları**

# BANKALARARASI KART MERKEZİ A.Ş. (BKM A.Ş.)

## Türkiye'de Kartlı Ödeme Sistemleri (Mart 2009)

5

- POS Sayısı : 1.630.000
- ATM Sayısı : 22.320
- Kredi Kartı Sayısı : 43.500.000
- Banka kartı Sayısı : 56.300.000

## Bankalararası Kart Merkezi A.Ş. (BKM A.Ş.)

6

- Ağustos 1990 da 13 özel ve devlet bankası tarafından kuruldu
- Sermaye: 4 Milyon TL
- Non issuer – Non acquirer, sadece servis sağlayıcı
- Kar etmeyen kuruluş
- 28 üyesine servis veriyor (25 acquirers, 28 issuers)
- Personel sayısı : 41
- Ulusal kanun, kural ve yönetmeliklere uymak zorunda
- BDDK Üyesi

# BKM A.Ş. Organizasyonu

7

- **Yönetim Kurulu**
  - 8 KKM Yöneticisi
  - 2 Denetçi
- **Personel**
  - Genel Müdür
  - Bölümler
    - **Bilgi Teknolojileri**
      - Teknoloji Servisleri
      - Uygulama Geliştirme
    - **İş geliştirme, Pazarlama ve Kurallar**
      - Kurumsal İletişim, Risk ve Güvenlik
      - İş Geliştirme, Kurallar ve Yönetmelikler
    - **Mali ve İdari İşler**
  - BKM Polis ve Jandarma Görevlileri
- **Mali ve Yasa Danışmanları**

## BKM Hizmetleri - BT

8

- BKM Switch Sistemi
- Yurtiçi Kredi Kartı Takası ve Hesaplaşma – YTH
- Yurtiçi Banka Kartı Hesaplaşması ve Ücretlendirme – SIU
- Ulusal Kayıp/çalıntı Listesi Güncelleme - BUL
- Aylık ve 3 aylık Üye İstatistikleri
- Ulusal Veri Ambarı – BVA
- BKM Online Sistemi
- Merkezi İşyeri Veritabanı – MİV
- 3D Secure Sistemi
- Marka Paylaşım Takası – MTH
- BKM Helpdesk
- Chargeback Doküman Yönetim Sistemi – CDYS
- Test ve Sertifikasyon Hizmetleri

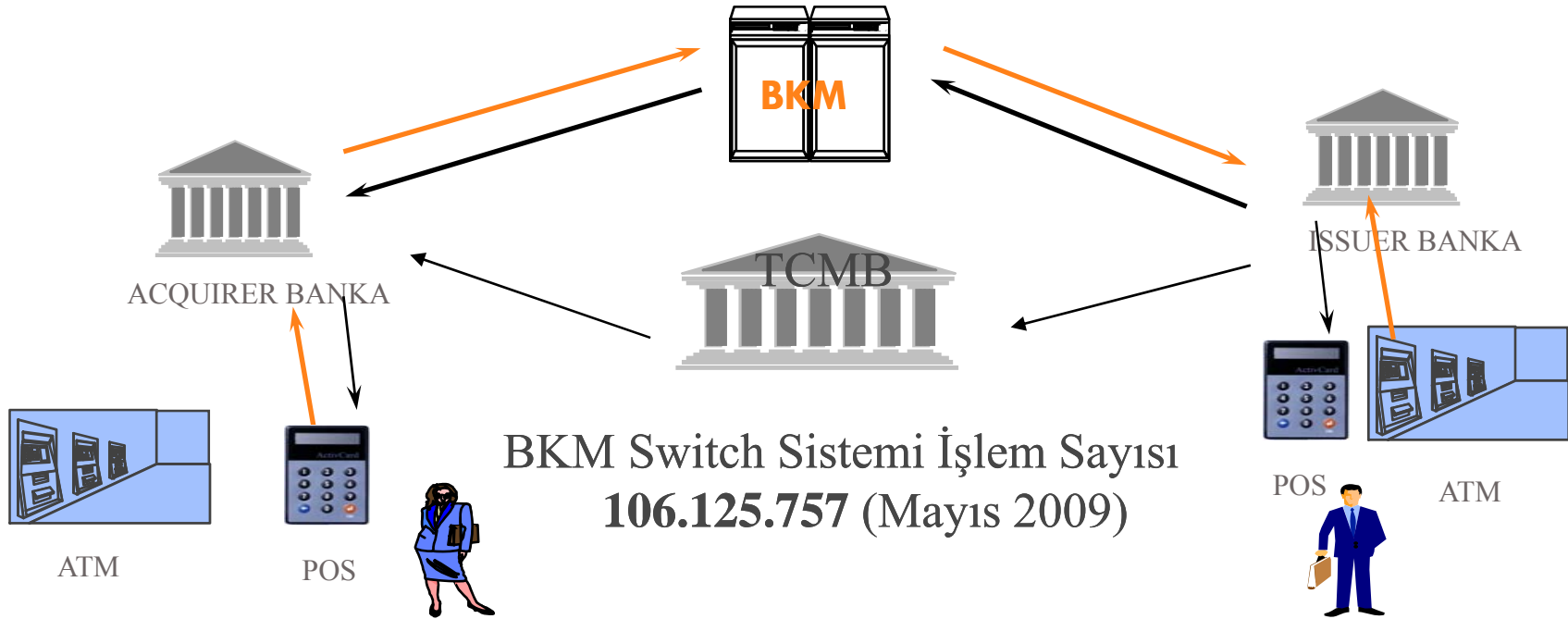
## BKM Hizmetleri - Genel

9

- Ulusal Kartlı Ödeme Sistemleri Yasa, Kural ve Yönetmelik Geliştirme
- Pazar Geliştirme ve Strateji Yönetimi
- Güvenlik Servisleri
- Eğitim Hizmetleri
- Hakem Görevi
- Bankalar Arası Koordinasyon
- Bilirkişi Hizmetleri

# BKM Switch ve Yurtiçi Takas

10



BKM Switch Sistemi İşlem Sayısı  
**106.125.757** (Mayıs 2009)

BKM A.Ş. 19.06.2009

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

# BKM A.Ş.'nin Yükümlülükleri

## (Ulusal/Uluslararası Yasa, Standart ve Yönetmelikler)

11

- 5464 Sayılı Banka Kartları ve Kredi Kartları Kanunu
- BDDK İlgili Yönetmelikleri
- Payment Card Industry Data Security Standards (PCI DSS) (\*)
- Visa/MasterCard/Amex PIN Security Management Regulations
- E-Commerce 3D Secure Regulations (\*)
- NFC (Near Field Communications) Payments Regulations (\*)

## ISO/IEC 27001 Standardı

(Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliđi Yönetimi  
Sistemleri - Gereksinimler)

# Bilgi Güvenliđi Yönetim Kontrolleri

13

1. Güvenlik Politikası
2. Bilgi Güvenliđinin Organizasyonu
3. Varlık Yönetimi
4. İnsan Kaynakları Güvenliđi
5. Fiziksel ve Çevresel Güvenlik
6. İletişim ve İşletim Yönetimi
7. Erişim Kontrolü
8. Bilgi Güvenliđi Edinimi, Geliştirme ve Bakımı
9. Bilgi Güvenliđi İhlal Olayı Yönetimi
10. İş Sürekliliđi Yönetimi
11. Uyumluluk

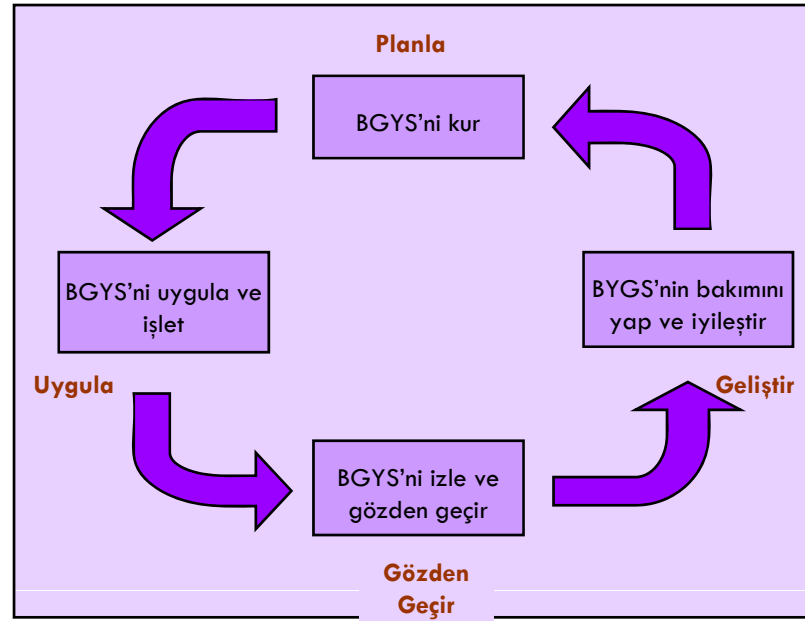
## **KONTROL AMAÇLARI ve KONTROLLER**

(11 Temel Alan ve 133 Alt Kontrol) 19.06.2009

# Genel Yönetim Sistemi Yaklaşımı

14

- Planla
- Uygula
- Gözden Geçir
- Geliştir



## MAYIS 2009 İTİBARI İLE ISO 27001 SERTİFİKALARI - DÜNYA

|                |      |                    |    |             |      |
|----------------|------|--------------------|----|-------------|------|
| Japan          | 3191 | Iceland            | 12 | Peru        | 3    |
| India          | 451  | Netherlands        | 12 | Vietnam     | 3    |
| UK             | 400  | Pakistan           | 11 | Belgium     | 2    |
| Taiwan         | 321  | Singapore          | 11 | Isle of Man | 2    |
| China          | 190  | Norway             | 10 | Kazakhstan  | 2    |
| Germany        | 119  | Russian Federation | 10 | Morocco     | 2    |
| USA            | 91   | Saudi Arabia       | 10 | Portugal    | 2    |
| Korea          | 88   | Slovenia           | 9  | Ukraine     | 2    |
| Czech Republic | 68   | Sweden             | 9  | Argentina   | 1    |
| Hungary        | 65   | Bahrain            | 6  | Armenia     | 1    |
| Italy          | 54   | Kuwait             | 6  | Bangladesh  | 1    |
| Poland         | 39   | Slovakia           | 6  | Belarus     | 1    |
| Spain          | 35   | Switzerland        | 6  | Denmark     | 1    |
| Hong Kong      | 30   | Colombia           | 5  | Kyrgyzstan  | 1    |
| Australia      | 29   | Croatia            | 5  | Lebanon     | 1    |
| Austria        | 29   | Indonesia          | 5  | Lithuania   | 1    |
| Ireland        | 29   | South Africa       | 5  | Luxembourg  | 1    |
| Mexico         | 27   | Qatar              | 4  | Macedonia   | 1    |
| Malaysia       | 26   | Sri Lanka          | 4  | Mauritius   | 1    |
| Brazil         | 22   | Bulgaria           | 3  | Moldova     | 1    |
| Greece         | 22   | Canada             | 3  | New Zealand | 1    |
| Turkey         | 20   | Chile              | 3  | Sudan       | 1    |
| UAE            | 18   | Egypt              | 3  | Uruguay     | 1    |
| Thailand       | 16   | Gibraltar          | 3  | Yemen       | 1    |
| Philippines    | 15   | Iran               | 3  |             |      |
| Romania        | 15   | Macau              | 3  |             |      |
| France         | 12   | Oman               | 3  |             |      |
|                |      |                    |    | Total       | 5626 |

BKM A.Ş. 19.06.2009

## MAYIS 2009 İTİBARI İLE ISO27001 SERTİFİKALARI - TÜRKİYE

| Name of the Organization                               | Country | Certificate Number | Standard BS 7799-2:2002 or ISO/IEC 27001:2005 |
|--|---------|--------------------|---|
| Anadolu Bilisim Hizmetleri A.S.                        | Turkey  | IS 548547          | ISO/IEC 27001:2005                            |
| Bankalarasi Kart Merkezi A.S., Istanbul                | Turkey  | 212748             | ISO/IEC 27001:2005                            |
| BEKO ELEKTRONİK A.Ş.                                   | Turkey  | GB05/64028         | ISO/IEC 27001:2005                            |
| Borcelik Celik Sanayii Ticaret A.S.                    | Turkey  | 29                 | ISO/IEC 27001:2005                            |
| Bursagaz Bursa Sehirici Dogalgaz Dagitim Ticaret       | Turkey  | GB07/72173         | ISO/IEC 27001:2005                            |
| Corbuss Kurumsal Telekom                               | Turkey  | IS 514424          | ISO/IEC 27001:2005                            |
| E-Kart Elektronik Kart Sistemleri San. Ve Tic. A.Ş     | Turkey  | 192589             | ISO/IEC 27001:2005                            |
| Global Bilgi Pazarlama, Danisma ve                     | Turkey  | IS 510931          | ISO/IEC 27001:2005                            |
| Haci Omer Sabanci Holding A.S.                         | Turkey  | IS 530644          | ISO/IEC 27001:2005                            |
| İGDAŞ İSTANBUL GAZ DAĞITIM SANAYİ VE                   | Turkey  | 218289             | ISO/IEC 27001:2005                            |
| KAYACI BİLGİSAYAR GÜVENLİK OTOMASYON                   | Turkey  | 47/0               | ISO/IEC 27001:2005                            |
| Koc.net Haberlesme Teknolojileri                       | Turkey  | IS 514232          | ISO/IEC 27001:2005                            |
| Merkezi Kayıt Kuruluşu A.Ş                             | Turkey  | GB09/77358         | ISO/IEC 27001:2005                            |
| National Ministry of Education, Education Technologies | Turkey  | 77/0               | ISO/IEC 27001:2005                            |
| PWC / BASARAN NAS BAGIMSIZ DENETİM                     | Turkey  | IND82112           | ISO/IEC 27001:2005                            |
| Siemens AG   | Turkey  | 302147 ISMS        | ISO/IEC 27001:2005                            |
| TEMSA SANAYI ve TICARET A.S.                           | Turkey  | GB07 / 73225       | ISO/IEC 27001:2005                            |
| Turk Traktor ve Ziraat Makineleri A.S                  | Turkey  | IS 96691           | ISO/IEC 27001:2005                            |
| TÜRKTRUST Bilgi, İletişim ve Bilişim Güvenliği         | Turkey  | GB05/65355         | ISO/IEC 27001:2005                            |
| Tusas Aerospace Industries, Inc., Ankara               | Turkey  | 203376             | ISO/IEC 27001:2005                            |

# BKM A.Ş. ISO27001 SERTİFİKASYON SÜRECİ

# BKM A.Ş. ISO27001 SERTİFİKASYON SÜRECİ

18

- **Ön Analiz Çalışmaları**
- **Danışmanlık Çalışması**
- **Varlık ve Risk Yönetimi Çalışmaları**
- **Dokümantasyon Çalışmaları**
- **BKM Yönetim Katılımı ve Toplantıları Çalışmaları**
- **Düzenleyici/Önleyici Faaliyetler Çalışmaları**
- **Denetim ve Sertifikasyon Çalışmaları**

# BKM A.Ş. ISO27001 SERTİFİKASYON SÜRECİ

19

- **Ön Analiz Çalışmaları**
  - Mevcut durum kontrolü (PCI DSS'e göre).
  - Oluşturulacak Bilgi Güvenliği Yönetim Sistemi (BGYS) kapsam belirlenmesi.
  - Süreç tespiti.
  - BGYS Yöneticisi ve ekiplerin belirlenmesi.

# BKM A.Ş. ISO27001 SERTİFİKASYON SÜRECİ

20

## • Danışmanlık Çalışmaları

- BGYS Politikası'nın hazırlanması.
- Varlıkların (asset) belirlenmesi, sınıflandırılması ve tanımlanması.
- Risklerin değerlendirilmesi, sınıflandırılması ve tanımlanması.
- BKM Bilgi sınıflandırılması oluşturulması ve etiketlenmesi.
- BT dokümantasyonunun, standart gereksinimlerine göre (politika, standart, prosedür, yönetmelik, vb.) sınıflandırılması.
- Ölçülebilir Hedeflerin tespiti ve İş Takviminin oluşturulması.
- BGYS eğitimlerinin organize edilmesi.
- Uygulanabilirlik (SOA) dokümanının hazırlanması.
- Güvenlik ihlallerine karşı aksiyon planı hazırlanması ve ilgili ekibin oluşturulması
- İç Denetim çalışmasına hazırlanması.

# BKM A.Ş. ISO27001 SERTİFİKASYON SÜRECİ

21

## • Varlık ve Risk Yönetimi Çalışmaları

- Varlıkların ve risklerin tespiti.
- Varlıkların ve risklerin kayıt edilmesi (RA2).
- Kabul edilebilir risk seviyesi tespit edilmesi.
- Riski azaltma, transfer etme ve yok etme yöntemlerinin belirlenmesi.
- Şirketin riske karşı tutumuna uygun olan kontrollerin seçimi.
- Kabul edilebilir risklerin belirlenmesi, yönetim onayı alınması yayınlanması ve dokümantasyonu.
- Risk iyileştirici sürecin oluşturulması ve dokümantasyonu.
- Varlıklara ait listelerinin oluşturulması.

# BKM A.Ş. ISO27001 SERTİFİKASYON SÜRECİ

22

- **Dokümantasyon Çalışmaları**

- BGYS için belirlenen doküman tiplerine göre (Politika, Prosedür, Standard, Yönetmelik, Liste, Form) mevcut dokümantasyonun gözden geçirilmesi, düzenlenmesi ve etiketlenmesi.
- BYGS için gereken eksik dokümanların (ISO27001 SOA, Risk Yönetimi, Kayıtlar, Ölçülebilir Hedefler, Planlar, İş Takvimi Kapsamı, Geçersiz Dokümanlar) hazırlanması.
- BKM BGYS dokümantasyon listesinin hazırlanması.
- BGYS dokümantasyonun dosyalanması.

# BKM A.Ş. ISO27001 SERTİFİKASYON SÜRECİ

23

- **BKM Yönetim Katılımı ve Toplantı Çalışmaları**
  - ISO27701 Kapsamı (Scope) belirlenmesi, onayı ve dokümantasyonu.
  - Uygulanabilirlik (Statement of Applicability) dokümanın kapsamının onayı.
  - Yıllık ölçüm hedeflerinin (Ölçülebilir Hedefler) için İş Takviminin onayı.
  - BKM Yönetimi'nin çalışmalardan düzenli olarak bilgilendirilmesi.
  - Yönetimin Gözden Geçirme Toplantı'sının Gündemi belirlenmesi ve toplantı organizasyonu.
  - Yönetimin Gözden Geçirme Toplantı'sının gerçekleştirilmesi, sonuçların yayınlanması ve onay alınması.
  - İç denetim ve Sertifikasyon süreçleri için onay alınması.

# BKM A.Ş. ISO27001 SERTİFİKASYON SÜRECİ

24

- **Düzenleyici/Önleyici Faaliyetler Çalışmaları**

- Düzenleyici/Önleyici Faaliyet (DÖF) yönetiminin şirket kapsamında anlaşılması ve uygulanmasının sağlanması.
- BGYS Etkinliğini ve performansının artırabilecek tekniklerin, yöntemlerin ürünlerin araştırılarak DÖF kapsamına alınması.
- BGYS Etkileyebilecek değişikliklerin belirlenmesi ve DÖF kapsamına alınması.
- Şirket bütçelenmiş projeleri kapsamında yapılacak ve BGYS kapsamına girecek çalışmaların DÖF kapsamına alınması.
- Değişiklik Yönetimi'nin DÖF ile uyumlu hale getirilmesi, sonuçlarının DÖF kapsamında izlenmesi ve dosyalanması.
- Yıllık DÖF listesinin takibi, sürekli güncel tutulması, dosyalanması ve raporlanması.

# BKM A.Ş. ISO27001 SERTİFİKASYON SÜRECİ

25

- **Denetim ve Sertifikasyon Çalışmaları**

- Yıllık İç Denetim çalışması için firma ve tarih belirlenmesi, şirket içi koordinasyonun sağlanması, gerçekleştirilmesi ve sonuçlarının paylaşılması.
- İç Denetim çalışması sonrasında tespit edilen eksikler için gerekli çalışmaların ve DÖF yönetiminin başlatılması, takibi ve sonuçlandırılarak, gözden geçirilmesi.
- ISO27001 Sertifikasyon için Ön Denetim ve Denetim süreçlerinin seçilen denetçi firma ile birlikte organize edilmesi ve şirket bilgilendirilmesi ve koordinasyonun sağlanması.
- ISO27001 Sertifikasyon için Ön Denetim çalışmasının yapılması, sonrasında tespit edilen uyumsuzluklar (non-conformities) için gerekli çalışmaların ve DÖF yönetiminin başlatılması, takibi ve sonuçlandırılması ve uyumsuzluklarla ilgili sonuçların raporlanması.
- ISO27001 Sertifikasyon için Denetim çalışmasının yapılması, denetimde tespit edilen eksikler ve yapılması istenen iyileştirmeler için projeleri kapsamında yapılacak ve BGYS kapsamına girecek çalışmaların DÖF kapsamına alınması ve denetim sonucunun paylaşılması.

# ISO27001 SERTİFİKASYONU İÇİN İPUÇLARI

# ISO27001 SERTİFİKASYONU İÇİN İPUÇLARI

27

- **Mutlaka Kontrol Edilen Dokümanlar**
  - Bilgi Güvenliği Politikası
  - BGYS kapsamı (Scope Statement) ve Uygulanabilirlik ifadesi (SOA)
  - Kabul Edilebilir Kullanım Politikası
  - Personel Görev ve Sorumlulukları (görev tanımları ve matrisi)
  - Risk analiz metodolojisi, risk analiz raporu
  - Kabul edilebilir riskler listesi ve iyileştirme planı
  - Bilgi Sınıflandırması ve metodolojisi ile ilgili dokümanlar
  - BGYS izleme, gözden geçirme, iyileştirme ile ilgili dokümanlar
  - Personel eğitimi ile ilgili dokümanlar
  - Fiziki güvenlik ile ilgili dokümanlar

# ISO27001 SERTİFİKASYONU İÇİN İPUÇLARI

28

- **Mutlaka Kontrol Edilen Dokümanlar**
  - BGYS bünyesinde yer alan prosedür, politika ve standartlar
  - Güvenlik ihlali ve olayları ile ilgili dokümanlar
  - Felaket yedekleme / iş sürekliliği ile ilgili dokümanlar
  - İç Denetim Politikası
  - Dokümanların ve kayıtların kontrolü ile ilgili dokümanlar

# ISO27001 SERTİFİKASYONU İÇİN İPUÇLARI

29

- **Mutlaka Kontrol Edilen Kayıtlar**
  - BGYS ve ilgili dokümanların kabul edildiği ve okunduğuna dair kayıtlar
  - Değişim Yönetimi ile ilgili kayıtlar
  - Erişim hakları ve kontrolleri ile ilgili kayıtlar
  - Merkezi veri toplama (log) yönetimine ait kayıtlar
  - DÖF kayıtları
  - Eğitim Planı ve ilgili kayıtları
  - Güvenlik olayları ile ilgili kayıtları
  - Yönetimin Gözden Geçirme Toplantısı dokümanı
  - Ölçülebilir Hedefler ile ilgili kayıtlar
  - Personel dosyaları
  - Fiziki Güvenlik yönetimine ait kayıtlar

# ISO27001 SERTİFİKASYONU İÇİN İPUÇLARI

30

- **Sertifikasyon Devamlılığı İçin Yapılması Gerekenler**
  - Yeni varlıkların ve ilgili risklerin eklenmesi
  - Risklerin azaltılması için aksiyon planlaması, risk seviyelerinin güncellenmesi
  - Kabul edilebilir risklerin belirlenmesi ve risk tedavi planlarının yapılması
  - BGYS Yönetiminin sağlanması, kapsamının gözden geçirilmesi
  - BGYS kaynaklarının yönlendirilmesi ve etkinliğinin kontrol edilmesi
  - Bilgilendirme eğitimlerinin ve eğitim değerlendirmelerin yapılması
  - İç Denetim çalışmasının yapılması ve ilgili iyileştirme çalışmalarının yapılması
  - Yönetimin Gözden Geçirme Toplantısı'nın düzenli yapılması ve raporlanması
  - Ölçülebilir Hedeflerin geliştirilmesi ve ile ilgili kayıtların tutulması
  - Erişim yetkilerinin düzenli kontrolünün sağlanması
  - Belirlenen geliştirme ve değişikliklerin uygulanması ve değişim yönetimi altında kayıt edilmesi
  - Tespit edilen aksamalar ve yeni hizmetler için DÖF'lerin düzenli olarak takip edilmesi
  - BGYS Dokümantasyonun güncellenmesi



**Ercüment  
Büyükşumnulu**

**Teknoloji Hizmetleri Direktörü**

**Nispetiye Cad. Akmerkez E3 Blok Kat:3  
34337 Etiler İstanbul - TÜRKİYE  
(212) 350 79 00 Ext:931  
(212) 350 79 31 (D)  
[buyuksumnulu@bkm.com.tr](mailto:buyuksumnulu@bkm.com.tr)**

