

Doküman Kodu: BGYS-0002

# BGYS KAPSAMI BELİRLEME KILAVUZU

SÜRÜM 1.00

21 03 2008

Hazırlayan: Ünal Perendi

## ÖNSÖZ

Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)'nin misyonu, "bilgi güvenliği, haberleşme ve ileri elektronik alanlarında Türkiye'nin teknolojik bağımsızlığını sağlamak ve sürdürmek için nitelikli insan gücü ve uluslararası düzeyde kabul görmüş altyapısı ile, bilimsel ve teknolojik çözümler üretmek ve uygulamaktır". Bu ana hedef göz önünde bulundurularak belirlenen "bilgi güvenliği, haberleşme ve ileri elektronik alanlarında yeni teknolojilerin geliştirilmesine öncülük eden uluslararası bilim, teknoloji ve üretim merkezi olmak" vizyonuna ulaşılabilmesi ve ülkenin ihtiyacı olan teknolojilerin geliştirilmesi için Enstitü'nün akredite test ortam ve laboratuvarlarında temel ve uygulamalı araştırmalar yapılmakta ve ihtiyaç sahiplerine teknik destek sağlanmaktadır.

Bu doküman, BGYS (Bilgi Güvenliği Yönetim Sistemi) kurmak isteyen kurumlar için yardımcı kaynak olarak hazırlanmıştır. Tüm kurum ve kuruluşlar bu dokümandan faydalanabilir.

Bu dokümanda anlatılanlar tamamen tavsiye niteliğindedir. UEKAE, yapılan uygulamalardan doğabilecek zararlardan sorumlu değildir. Bu doküman UEKAE'nin izni olmadan değiştirilemez.

## **BİLGİLENDİRME**

Bu dokümanın oluşturulmasında emeđi geen Ađ Güvenliđi personeline ve dokümanı gözden geirip fikirlerini öne sürerek dokümanın olgunlaşmasına katkıda bulunan Ali Dinkan'a ve Burak Bayođlu'na teřekkürü bor biliriz.

## İÇİNDEKİLER

<b>1. GİRİŞ .....</b>	<b>5</b>
1.1 Amaç ve Kapsam.....	5
1.2 Hedeflenen Kitle.....	5
1.3 Kısaltmalar.....	5
<b>2. BGYS KAPSAMI .....</b>	<b>6</b>
<b>3. BGYS KAPSAM TANIMLAMA.....</b>	<b>6</b>
3.1 BGYS Kapsam Dokümanı Örnekleri .....	7
3.1.1 BGYS Kapsamı Örneği 1.....	7
3.1.2 BGYS Kapsamı Örneği 2.....	9
<b>KAYNAKÇA .....</b>	<b>11</b>

## 1. GİRİŞ

Bu doküman ISO/IEC 27001:2005 standardında *BGYS Kurulumu* başlığı altındaki maddelerinin ilk sırasında olan BGYS Kapsamının tanımlanması maddesi için rehber niteliğindedir. ISO/IEC 27001:2005 standardına uygun olarak Bilgi Güvenliği Yönetim Sistemi (BGYS) kurma çalışması planlayan kurumlara BGYS kapsamının belirlenmesi konusunda yol gösteren bilgilere yer verilmiştir.

### 1.1 Amaç ve Kapsam

ISO/IEC 27001:2005 standardına uygun olarak Bilgi Güvenliği Yönetim Sistemi (BGYS) kurma çalışması planlayan kurumlara BGYS kapsamının belirlenmesi konusunda yol gösteren bilgilere yer verilmiştir.

Bu dokümanda ISO/IEC 27001 standardına uygun olarak Bilgi Güvenliği Yönetim Sistemi (BGYS) kurma çalışması sırasında BGYS kapsamının nasıl belirlenmesi gerektiği anlatılmıştır. BGYS Kapsam dokümanı örnekleri verilerek de kapsamın neleri içermesi gerektiği belirtilmiştir.

### 1.2 Hedeflenen Kitle

Bu doküman Bilgi Güvenliği Yönetim Sistemi (BGYS) kurma çalışması planlayan, kurulu BGYS sistemlerinin denetimini gerçekleştiren kurum yöneticilerine, güvenlik uzmanlarına, denetimcilere ve genel bilgi sistemleri güvenliğiyle ilgilenenler içindir.

### 1.3 Kısaltmalar

**BGYS** : Bilgi Güvenliği Yönetim Sistemi

**UEKAE** : Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

## 2. BGYS KAPSAMI

İş (aktiviteler), organizasyon (yönetimsel birimler), işin mekânı, varlıklar ve teknoloji karakteristikleri belirtilerek ve kapsam dışında kalacak olan her ayrıntının sebepleri açıklanarak BGYS'nin sınırları ve kapsamı tanımlanır. Hangi yönetimsel birimlerin ve aktivitelerin bilgi güvenliği yönetim kapsamı içerisinde yer alacağı belirtilmelidir. [1]

Kapsam dokümanı çok sık değişime uğraması gerekmez de yaşayan bir dokümandır. Gerektiğinde kapsamın içeriği değiştirilebilir. Fakat kapsamın ilk aşamada belirlenirken yönetilebilir boyutta tutulması önemlidir. Bu yüzden organizasyonun fiziksel yapısı ve süreçleri göz önüne alınmalıdır. Örneğin; az görülmesine rağmen yönetilebilirlik adına çok büyük bazı organizasyonlarda Finans bölümü ve Yazılım geliştirme bölümü için iki ayrı BGYS oluşturulduğu gibi örnekler mevcuttur. [2]

## 3. BGYS KAPSAM TANIMLAMA

BGYS Kapsamı tanımlanırken aşağıdakilerin belirtilmesi gereklidir:

**Kurum/Şirket/Organizasyon:**Kurum/Şirket/Organizasyon'un adı net şekilde belirtilmelidir.

**Hedef:** ISO/IEC 27001:2005 sertifikasyonunu elde etmek için standarda uyumluluk sağlanması amacıyla olduğu gibi bir amaç net bir şekilde belirtilmelidir.

**Kapsam:** Hangi yönetimsel birimlerin ve aktivitelerin bilgi güvenliği yönetim yapısı içerisinde yer alacağı belirtilmelidir.

**Sınırlar / Limitler:** BGYS kapsamının belirtmesi gereken limitler:

- Organizasyonun özellikleri (büyüklük, çalışma alanları vb.)
- Organizasyonun mekânı;
- Varlıklar
- Teknoloji

**Arayüzler:** Organizasyonun diğer sistem, organizasyon veya tedarikçiler ile olan arayüzleri hesaba katılmalıdır. Tüm Hizmetler ve Aktiviteler BGYS tanımı içerisinde yer almak zorunda değildir. Organizasyonun bilgi güvenliği risk analizinde yer alacak bilgisayar veya iletişim ortamı paylaşımı yaptığı veya organizasyon için önemli olan her türlü arayüz belirtilmelidir. [3]

**Bağımlılıklar:** Kurulacak BGYS belirli yasal ve ticari zorunluluklara tabi olabilir. Örneğin; bankacılık sektöründeki bir organizasyonun Bankacılık Düzenleme ve Denetleme Kanunları ile belirtilen yasalara uygunluk sağlaması gerektiği kapsam dokümanında belirtilmelidir.

**Hariç Tutma / Savunma:** BGYS tarafından tanımlanan ama herhangi bir güvenlik politikası veya güvenlik ölçütü tarafından kapsanmayan her bölümün veya elementin neden içerilmediği açıklamasıyla beraber belirtilmelidir.

### 3.1 BGYS Kapsam Dokümanı Örnekleri

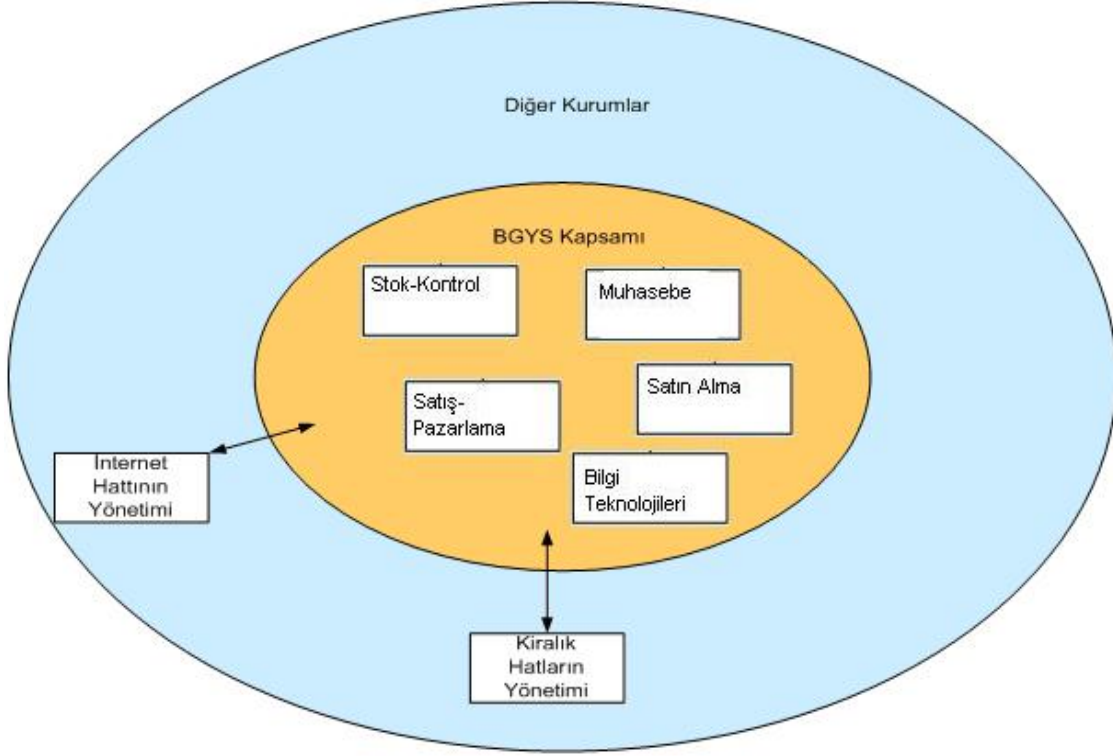
#### 3.1.1 BGYS Kapsamı Örneği 1

#### **ELAR Ltd. Şti. BGYS KAPSAMI**

**AMAC ve KAPSAM:**

1995 yılında Şişli’de kurulan ELAR Elektronik Ltd. Şti. Şirketi kendine ve müşterilerine ait bilgileri korumak amacıyla ISO/IEC 27001 standardına uygun olarak bir Bilgi Güvenliği Yönetim Sisteminin kurulmasına karar vermiştir. Bu BGYS uygulaması tüm ELAR şirketi birimlerine uygulanmaktadır.

BGYS kapsamı şeklen ifade edilmiştir. Yukarıda kapsamda belirtilen ‘bilgi’ ifadesi yazılı, sözlü ve elektronik ortamdaki tüm bilgi çeşitlerini kapsamaktadır.



Şekil 1 - ELAR şirketi BGYS Kapsamı

## ORGANİZASYON

ELAR şirketi 5 bölümden oluşmaktadır.

- Stok-Kontrol
- Satış-Pazarlama
- Satın Alma
- Muhasebe
- Bilgi Teknolojileri

## YERLEŞKE:

ELAR şirketinin iş operasyonlarını yürüttüğü yerler:

### Merkez:

ELAR Elektronik Ltd. Şti. Merkezi Etfal Sok. No:27 Şişli / ISTANBUL

### Şube:

Atatürk cad. No: 12 Kozyatağı /ISTANBUL

### Depo:

İnönü cad. No: 19 Ümraniye /ISTANBUL

**VARLIKLAR VE TEKNOLOJİ**

ELAR yerleşkeleri birbirlerine bağlayan kiralık hatlar ile internet hattının yönetimi dışındaki hizmetlerini kendisi yerine getirmektedir.

Kiralık hattının ve internet hattının yönetimi dışı kaynak kullanımı yolu ile gerçekleştirilmektedir. Dış kaynak kullanımı ile ilgili sözleşmeler, hazırlanmış dış kaynak kullanım sözleşme taslağı temel alınarak yapılmaktadır.

BGYS, aşağıdakilerin hepsini kapsar:

- Şirketin tüm ticari bilgileri
- Şirket çalışanlarına ait kişisel bilgiler
- Müşterilerin tüm kişiye özel bilgileri
- Yukarıdaki bilgileri içeren BT(Bilgi Teknolojileri) Sistemleri
- Dış kaynak kullanım faaliyeti
- Sistem Dokümantasyonu

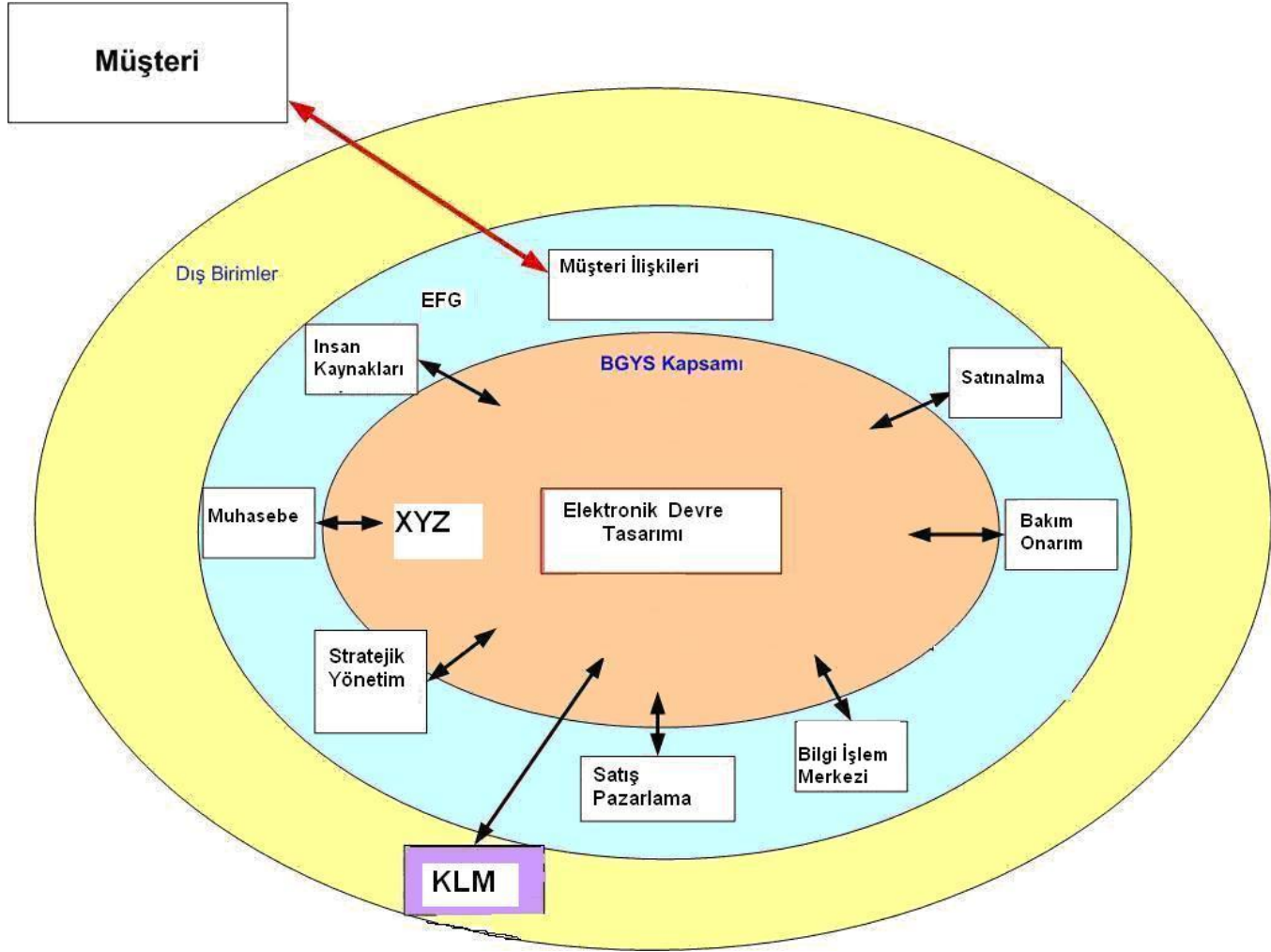
**3.1.2 BGYS Kapsamı Örneği 2****XYZ A.Ş. BGYS Kapsam Dokümanı****BGYS KAPSAMI**

XYZ Şirketi'ne ait BGYS (Bilgi Güvenliği Yönetim Sistemi), EFG Şirketinin organizasyon yapısı altında kurulmuştur. XYZ organizasyonu içerisinde kredi kartı üretimi yapmaktadır.

XYZ, EFG'nin Düzce Yerleşkesindeki binasında bu iş için tahsis edilmiş özel olarak korumalı bölgenin içerisinde kurulmuştur. XYZ idari ve destek hizmetleri için EFG'nin altyapısını kullanmaktadır. XYZ kredi kartı üretimi ile ilgili süreçleri kendi altında yürütmektedir.

XYZ BGYS, Kredi kartı üretimi ile ilgili süreçlerinin altında Elektronik Devre Tasarımı, Damgalama hizmetleri, Bilişim Hizmetleri süreçleri yer almaktadır. Bu süreçlerden sadece Damgalama hizmetleri süreci KLM 'den dış kaynak olarak sağlanmaktadır. Elektronik Devre Tasarımı ve Bilişim Hizmetleri süreçleri XYZ tarafından yürütülmektedir.

XYZ, Müşteri İlişkileri, Satın alma, Stratejik Yönetim, Muhasebe, İnsan Kaynakları, Bakım Onarım, Satış ve Pazarlama, Bilgi İşlem Merkezi gibi hizmetleri EFG İdari ve Destek hizmetlerden sağlamaktadır. Bu kapsamdaki hizmetler XYZ ana iş amaçlarına yardımcı hizmetlerden oluşmaktadır. Bu kapsamdaki alınan hizmetlere ilişkin XYZ ile ilgili bölümler arasında 'Kurum İçi Hizmet Sözleşmesi' imzalanmıştır.



Şekil -2- XYZ Bölümü BGYS Kapsamı

*XYZ BGYS, Düzce'deki yerleşkesinde Kredi kartı yapımında kullanılan tüm ürünler ile ilgili işlenen, saklanan ve/veya taşınan tüm bilgileri ve tüm XYZ personelini kapsar.*

XYZ Hizmetleri, DÜZCE' de bulunan EFG binasında verilmektedir.

BGYS, aşağıdakilerin hepsini kapsar:

- Kredi kartı üretimiyle ilgili tüm özel ve tüzel bilgiler.
- XYZ çalışanlarına ait kişisel bilgiler.
- XYZ iç ve dış müşterilerine ait bilgiler.
- Tedarikçi sözleşmeleri.
- Dış kaynak kullanım sözleşmeleri.
- Kurum içi hizmet sözleşmeleri.
- Hizmet sunulan ofis, oda, binalarda bulunan tüm araç ve gereçler.
- Personel, BT(Bilgi Teknolojileri) Sistemleri ve Sistem Dokümantasyonu

### KAYNAKÇA

- [1] R.Saliba, “Callio Secura 17799 - A tool for implementing the ISO 17799 / BS 7799”, 1998, pp. 12 –14.
- [2] T.Humphreys, “ISMS Standarts The ISO 27000 Family and BS7799-2 ”, ISMS International User Group Seminar, pp. 32-35.
- [3] S. Lihuan Liang, “An ISMS Implementation Practice in Enviroments with limited Resources” APEC-OECD Workshop on Security of Information Systems and Networks, September ,2005.