BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

# MOBİL HABERLEŞME SEKTÖRÜ İÇİN ÖRNEK BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS) MODELİ

Hakan AYDOĞAN

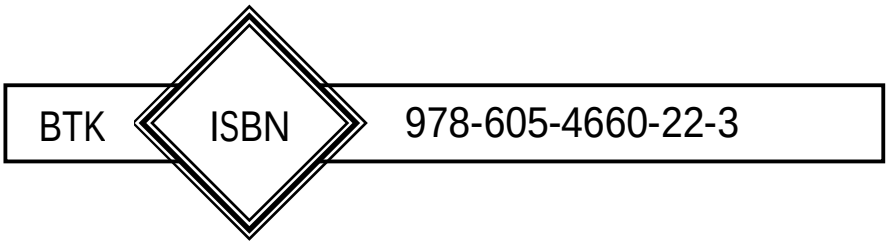
Bilişim Uzmanlığı Tezi

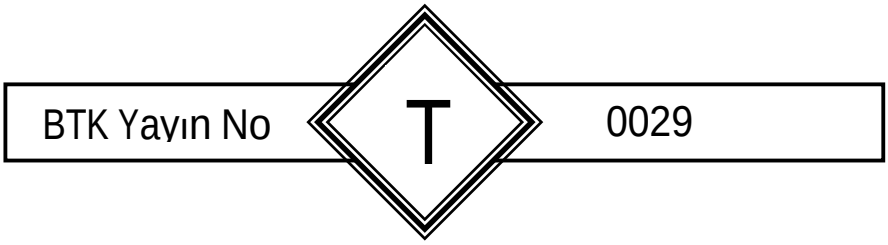
Ekim 2011

Ankara


Bu yayında öne sürülen fikirler eserin yazarına aittir;

Bilgi Teknolojileri ve İletişim Kurumunun görüşlerini yansıtmaz.



BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

# MOBİL HABERLEŞME SEKTÖRÜ İÇİN ÖRNEK BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS) MODELİ

Hakan AYDOĞAN

Bilişim Uzmanlığı Tezi

Ekim 2011

Ankara

Hakan AYDOĞAN tarafından hazırlanan "Mobil Haberleşme Sektörü İçin Örnek Bilgi Güvenliği Yönetim Sistemi (BGYS) Modeli" adlı bu tezin Uzmanlık tezi olarak uygun olduğunu onaylarım.

Prof. Dr. İnan GÜLER
Tez Yöneticisi

Bu çalışma, tez savunma komisyonumuz tarafından Bilişim Uzmanlığı tezi olarak kabul edilmiştir.

Başkan : _____
Kurul Üyesi M. Selçuk NURSOY

Üye : _____
Daire Bşk. Atilla ARSLAN

Üye : _____
Daire Bşk. Yasin BAKIRCI

Üye : _____
Daire Bşk. V. Elif ÖZDEMİR

Üye : _____
Bilişim Uzmanı N. Bengü KARABACAK

Üye : _____
Bilişim Uzmanı Mustafa ÖZDEMİR

Üye : _____
Prof. Dr. İnan GÜLER

Bu tez, Bilgi Teknolojileri ve İletişim Kurumu tez yazım kurallarına uygundur.

## İÇİNDEKİLER

# ÖZET


| BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU | |
|---|---|
| Tezin Adı | Mobil Haberleşme Sektörü İçin Örnek Bilgi Güvenliği Yönetim Sistemi (BGYS) Modeli |
| Türü | Bilişim Uzmanlığı Tezi |
| Yazar | Hakan AYDOĞAN |
| Teslim Tarihi | 08.07.2011 |
| Anahtar Kelimeler | Bilgi Güvenliği, Bilgi Güvenliği Yönetim Sistemi, Mobil Haberleşme, Mobil işletmeci |
| Tez danışmanı | Prof. Dr. İnan GÜLER |
| Sayfa Adedi | viii+122 |

Özet

Bu çalışmada, gelişen teknoloji ile hayatımızın vazgeçilmez parçası haline gelmiş olan 2N ve 3N mobil haberleşme sistemlerine sahip mobil işletmecilerin kendi mobil haberleşme alanlarına özel Bilgi Güvenliği Yönetim Sistemi (BGYS) ihtiyaçlarını karşılayacak ve bu konudaki uluslar arası standartları sağlayacak bir modelin geliştirilmesi amaçlanmıştır. Çalışmada öncelikle bilgi güvenliği ile ilgili genel bilgilere yer verilmiştir. BGYS modelinin kurulumunda yönetim tavrı ve sorumlu icracı birime duyulan ihtiyaçtan bahsedilmiştir. Daha sonra mobil işletmecilere özel örnek BGYS modelinin kurulumu sırasında; politikanın oluşturulması, risklerin değerlendirilmesi, varlıkların ve tehditlerin belirlenmesi gibi konular işlenmiş ve bazı örnek kayıtlar oluşturulmuştur. Kurulum sonrası modelin gerçekleştirilmesi ve işletilmesi, izlenmesi ve gözden geçirilmesi, sürekliliğinin sağlanması ve iyileştirilmesi ile ilgili yapılması gerekenler ele alınmıştır. Daha sonra model içerisinde yer alan; yönetimin rolü, icraci birim, politika dokümanı, varlık envanteri listesi, risk belirleme, risk derecelendirmesi, risk işleme, kontrol maddeleri seçimi, kabul edilebilir risk düzeyi, ayrılacak bütçe, alınanacak eğitimler, iç ve dış denetimlere ilişkin önerilere yer verilmiştir.

## ABSTRACT

| INFORMATION TECHNOLOGIES AND COMMUNICATIONS AUTHORITY | |
|---|---|
| Thesis | Proposal Of An Information Security Management System Model For Mobile Communication Market |
| Type | Informatics Expert Thesis |
| Author | Hakan AYDOĞAN |
| Submission Date | 08.07.2011 |
| Key Words | Information Security, Information Security Management System for Mobile Communications, Mobile Operator |
| Advisor | Prof. Dr. İnan GÜLER |
| Total Page | viii+122 |

Abstract

In this study, it is aimed to develop a model that provides not only conformity to international information security standards but also the needs of Information Security Management System (ISMS) in their special areas of mobile communication operators which have 2G and 3G mobile communication systems that has become an indispensable part of our lives. Firstly general information about information security had been mentioned. The need of management manner and executive unit for installation of ISMS model are described. Later, some sample records are prepared about the issues of policy creation, evaluation of risks, assets andthreats during the installation of specific ISMS model for mobile operators. After the installation; needs to be done about the implementing and operating, monitoring and review, continuity and improvement of the model are discussed. Then, within the model advice on the role of management, the executive unit, the policy document, asset inventory, risk assessment, risk rating, risk processing, selection of control substances, acceptable risk level, allocated budget, training, internal and external audits are given.

# TEŞEKKÜR

Çalışmam boyunca değerli yardım ve katkılarıyla beni yönlendiren danışmanım Prof. Dr. İnan GÜLER'e, bilgi ve tecrübesiyle beni destekleyen Daire Başkanı Sayın Ejder ORUÇ ve B.Uzmanı Ö.Faruk. AKTOP'a, ayrıca anlayış ve yardımını esirgemeyen eşime ve destekleriyle beni hiçbir zaman yalnız bırakmayan tüm çalışma arkadaşlarıma teşekkürü bir borç bilirim.

Hakan AYDOĞAN

Mayıs 2011

# TABLOLAR LİSTESİ

# ŞEKİLLER LİSTESİ

## KISALTMALAR LİSTESİ

Bu çalışmada kullanılan bazı simgeler ve kısaltmalar açıklamaları ile birlikte aşağıda sunulmuştur.

| | |
|---|---|
| BGY | Bilgi Güvenliği Yönetimi |
| BGYS | Bilgi Güvenliği Yönetim Sistemi |
| BS | İngiliz Standartları (British Standards) |
| BSC | Baz İstasyonu Denetleyicisi (Base Station Controller) |
| BSI | İngiliz Standartları Enstitüsü (British Standards Enstitution) |
| BTK | Bilgi Teknolojileri ve İletişim Kurumu |
| BTS | Baz Alıcı-Verici İstasyonu (Base Transceiver Station) |
| CEO | Genel Müdür (Chief of Executive Officer) |
| CFO | Finanstan Sorumlu Müdür (Chief Financial Officer) |
| CIO | Bilgiden Sorumlu Müdür (Chief Information Officer) |
| ÇM | Çağrı Merkezi |
| DWDM | Yoğun Dalga Bölmeli Çoğullama (Dense Wavelength Division Multiplexing) |
| GPRS | Genel Paket Radyo Hizmeti (General Packet Radio Service) |
| GSM | Mobil Haberleşme için Global Sistem (Global System for Mobile Communications) |

| | |
|---|---|
| GWMSC | Mobil Anahtarlama Merkezi Geçişi (Gateway Mobile Switching Center) |
| HLR | Abone Bilgileri Merkezi Veri Sistemi (Home Location Register) |
| IEC | Uluslararası Elektroteknik Komisyon (International Electrotechnical Commission) |
| IP | İnternet Protokolü |
| ISO | Uluslararası Standardizasyon Organizasyonu (International Organization for Standardization) |
| IT | Bilgi Teknolojileri (Information Technologies) |
| KERD | Kabul Edilebilir Risk Düzeyi |
| MSC | Mobil Anahtarlama Merkezi (Mobil Switching Center) |
| NSS | Ağ Anahtarlama Alt Sistemi (Network Switching Subsystem) |
| PBX | Özel Birim Santralı (Private Branch Exchange) |
| PUKÖ | Planla-Uygula-Kontrol et-Önlem Al |
| RAN | Radyo Erişim Şebekesi (Radio Access Network) |
| RNC | Telsiz Şebeke Denetleyicisi (Radio Network Controller) |
| SDH | Eş Zamanlı Sayısal Sıradüzeni (Synchronous Digital Hiyerarchy) |
| TS | Türk Standartları |
| TSE | Türk Standartları Enstitüsü |
| VAS | Katma Değerli Hizmetler (Value Added Services) |

| | |
|---|---|
| VLR | Abone Bilgileri Geçici Veri Sistemi (Visitor Location Register) |
| VOIP | İnternet Protokol Adresi Üzerinden Ses İletimi (Voice Over Internet Protocol) |
| YGG | Yönetimin Gözden Geçirmesi |
| 2N | İkinci Nesil Mobil Haberleşme Sistemleri (Second Generation) |
| 3N | Üçüncü Nesil Mobil Haberleşme Sistemleri (Third Generation) |

# GİRİŞ

Yönetim sistemi tetkikleri; 1991'den önce ön koşulları tanımlanmış olan, büyük oranda savunma ve nükleer başta olmak üzere birçok endüstride yaşanan pratiklerin sonucu olarak kararlaştırılmış ve geliştirilmiş bir dizi gereksinimden ibarettir. Bu gereksinimlerin çoğu o yıllar itibari ile henüz uluslararası kabul görmüş standartlar arasında yer almamaktadır.

Denetim programı ve denetçinin asgari gerekliliklerini içeren bir standart, ilk defa 1991'de Uluslararası Standardizasyon Organizasyonu (ISO) 10011 (İngiltere'de İngiliz Standardı (BS) BS 7229) olarak yayımlanmıştır (BSI, ISM04101TRTR). Bu standardı takiben İngiltere'de İngiliz Standarları Enstitüsü (BSI) tarafından, elektronik ofis sistemlerinin kullanımındaki artış, bu sistemlerin olası problemleri ve bu sistemler üzerindeki kontrol mekanizmaları ile ilgili kaygılar nedeniyle bilgi güvenliğine özel uygulama prensipleri ve standartlar geliştirilmiştir. Daha sonra ISO1779, ISO 27001 ve ISO 27002 gibi dünya çapında bilgi güvenliği standartları oluşturulmuştur.

Günümüzde üreticiler, şirketler ve devlet kurumları işlerini yürütürken yoğun şekilde bilgi kullanımı gerçekleştirmektedirler. Her geçen gün bilginin, önemi arttığı gibi güvenli bir şekilde saklanması, depolanması ve bir yerden bir yere nakil edilmesi hususları çeşitli problemleri beraberinde getirmiştir. Tüm bu problemler, bilgiye olan bağımlılık nedeniyle çözüme kavuşturulmaya çalışılmış ve dolayısıyla bilginin korunması ihtiyacı doğmuştur. Olası saldırılarda bilginin; tahrip edilmesi, silinmesi, bütünlüğünün ve/veya gizliliğinin zarar görmesi, bilgi altyapısının bozulmasına ve beraberinde işlerin aksamasına neden olmaktadır.

Bilgi güvenliği; kuruluştaki işlerin sürekliliğinin sağlanması, meydana gelebilecek aksaklıkların azaltılması ve beklenen faydanın artırılması için bilginin, geniş anlamda tüm tehditlerden korunmasını sağlamaktadır. Kuruluşlar, bilgi güvenliğini tesis edebilmek için kendi bünyelerinde Bilgi

Güvenliği Yönetim Sistemi (BGYS) kurarlar. Bu sistemler, isteğe bağlı olmakla beraber çoğu zaman bilgi güvenliği ile ilgili standartlara dayanmaktadır ve standartların gerekliliklerini yerine getirmektedir.

Bu bağlamda, gelişen teknolojinin sağladığı kolaylık ile hayatımızın vazgeçilmez parçası haline gelmiş olan ikinci nesil mobil haberleşme sistemleri (2N) ve üçüncü nesil mobil haberleşme sistemleri (3N) nedeniyle mobil haberleşme sistemlerini işleten işletmecilerin de bu alandaki uluslararası standartlara dayanarak kendi alanlarına özel BGYS' sini kurması beklenmektedir. Toplumun ve ekonominin kalkınması için önemli faktörlerden olan 2N ve 3N mobil haberleşme sistemleri, bilgi güvenliği açısından değerlendirildiğinde büyük kitleleri ilgilendirdiğinden dolayı kritik ve hassas varlıklar olarak tanımlanabilir.

Mobil haberleşme şebekelerinin; kanuni olmayan dinleme, yanıltıcı sinyal gönderme, hizmet sunumunun reddi, mesaj ile kandırma gibi kötü niyetli erişimlere ve sahteciliğe karşı korunması gerekir. Koruma aynı zamanda güvenlik ihlallerine karşı önlem, ihlalleri tespit ve onarma ile güvenliğe ilişkin bilgilerin yönetimini de kapsamalıdır. Bunun yanında doğal afetler veya terörist saldırılar nedeniyle hizmetin aksamasına karşın önlemleri de içermelidir.(BTK, 2007,Haberleşmenin Güvenliği)

Haberleşme araçları ve yöntemlerinde meydana gelen sürekli değişim ve gelişmeler, internet ve genişbant teknolojilerini ön plana çıkarmıştır. Bu teknolojilerin de mobil haberleşme sistemlerinde kullanılması ile beraber daha etkili bilgi güvenliği sağlanması adına çözüm yolları aranmaya başlanmıştır. Eğer bu sahada etkin BGYS'ler kurulup işletilmez ise bahsedilen teknolojiler gün geçtikçe daha fazla haberleşme riskinin oluşmasına sebep olabilecektir.

Bu nedenle ülkemizde elektronik haberleşme sektöründe faaliyet gösteren işletmeciler, 20 Temmuz 2008 tarih ve 26942 sayılı Resmi Gazete'de

yayımlanarak yürürlüğe giren "Elektronik Haberleşme Güvenliği Yönetmeliği" ile haberleşme güvenliği gereksinimlerini yerine getirmekle yükümlü kılınmıştır (BTK, 2008). Söz konusu yönetmelik ve devamındaki tebliğler ile kişişel ses ve/veya veri hizmeti taşıyan işletmecilerden belli ölçeğin[1] üstündeki işletmecilere, ISO/IEC (Uluslararası Elektroteknik Komisyon) 27001 Bilgi Güvenliği Standardı uygunluk belgesi alma yükümlülüğü getirilirken diğer işletmecilere belge almaksızın uyumluluk sağlama yükümlülüğü getirilmiştir (BTK, 2011).

Bu tezde ISO 27000 bilgi güvenliği ailesinin genel gereksinimlerinden yola çıkılarak mobil haberleşme sektöründe faaliyet gösteren işletmeciler için özelleştirilmiş bir BGYS önerisi yapılmaktadır. BGYS modeli oluşturulurken ele alınan ölçek, 20 milyon abonesi ve yıllık 5 milyar dolar net satışı olduğu varsayılan orta büyüklükte ulusal çaptaki bir mobil işletmeci ölçeğidir.

Önerilen BGYS modeli uygulaması ile temelde ISO/IEC 27001:2005 bilgi güvenliği standardına uygunluk sağlanabilecek ve istenirse sertifikasyon gerçekleştirilebilecektir. Ancak model önerisi, tamamen ISO/IEC 27001:2005 standardı teoriği ile sınırlı kalmamış ve faaliyet alanına has pratikler, kayıtlar, örneklemeler ve ilaveler içermektedir. Kısacası model önerisi, ISO/IEC 27001:2005 standardını da kapsayan bir üst uygulamadır.

Dolayısıyla tez içerisinde, genel kabul görmüş ISO/IEC 27001:2005 bilgi güvenliği standardının (ISO, 2005) bilinir olduğu kabul edilerek ISO/IEC 27001:2005 standardı kapsamı, gereksinimleri, kontrol amaçları ve kontrolleri üzerinde ayrıntılı bir şekilde durulmamıştır. Bunun yerine BGYS'nin; ne olduğu, neden ihtiyaç duyulduğu ve kurulum aşamaları hakkında genel bilgi

[1]Bu ölçek,23 Mart 2011 tarihli ve 27883 tarihli Resmi Gazete' de yayımlanarak yürürlüğe giren "Elektronik Haberleşme Güvenliği Kapsamında TS ISO/IEC 27001 Standardı Uygulamasına İlişkin Tebliğ'de Değişiklik Yapılmasına Dair Tebliğ" ile bu sınır Yıllık net satış tutarı üzerinden belirlenmiştir: Bir milyon (1.000.000) Türk Lirası

verildikten sonra mobil haberleşme hizmeti veren bir işletmeci için örnek BGYS modelinin:

- Kurulumu,
- Gerçekleştirilmesi ve İşletilmesi,
- İzlenmesi ve Gözden Geçirilmesi,
- Sürekliliğinin Sağlanması ve İyileştirilmesi,

aşamalarına değinilmiştir.

Bu kapsamda giriş bölümünü takiben ilk bölümde; bilgi güvenliği standartlarının tarihi gelişimi, BGYS'nin ne demek olduğu ve BGYS'ye neden ihtiyaç duyulduğu ile ilgili açıklamalar yapılmıştır.

Daha sonra ikinci bölümde BGYS kurulumu ve kurulum sonrasında BGYS'nin gerçekleştirilmesi ve işletilmesi, izlenmesi ve gözden geçirilmesi, sürekliliğinin sağlanması ve iyileştirilmesi aşamaları tek tek ele alınarak bu aşamalarda nelerin yapıldığı açıklanmıştır.

Üçüncü bölümde, 2N ve 3N mobil haberleşme sistemleri için örnek BGYS modelinin kurulumunda yönetim kararlılığına ve sorumlu icracı birime duyulan ihtiyaçtan bahsedilmiştir. Model içerisinde, yönetimin rolü üzerinde durulmuştur. Daha sonra mobil işletmecilere özel olan örnek BGYS modeli kurulum aşamalarında neler yapılacağı; politikanın oluşturulması, risklerin değerlendirilmesi, varlıkların ve tehditlerin belirlenmesi gibi konular işlenmiş ve bazı örnek kayıtlar oluşturulmuştur.

Dördüncü bölümde ise örnek BGYS modelinin kurulduktan sonra; gerçekleştirilmesi ve işletilmesi, izlenmesi ve gözden geçirilmesi, sürekliliğinin sağlanması ve iyileştirilmesi ile ilgili yapılması gerekenler ele alınmıştır.

Sonuç ve öneriler kısmında, örnek BGYS modelinin klasik anlamdaki BGYS'lere göre önerdiği farklılıklar ve getireceği faydalar sıralanarak çalışma sonlandırılmıştır.

# 1. BİLGİ GÜVENLİĞİ STANDARTLARI VE BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

## 1.1 Bilgi Güvenliği Standartları

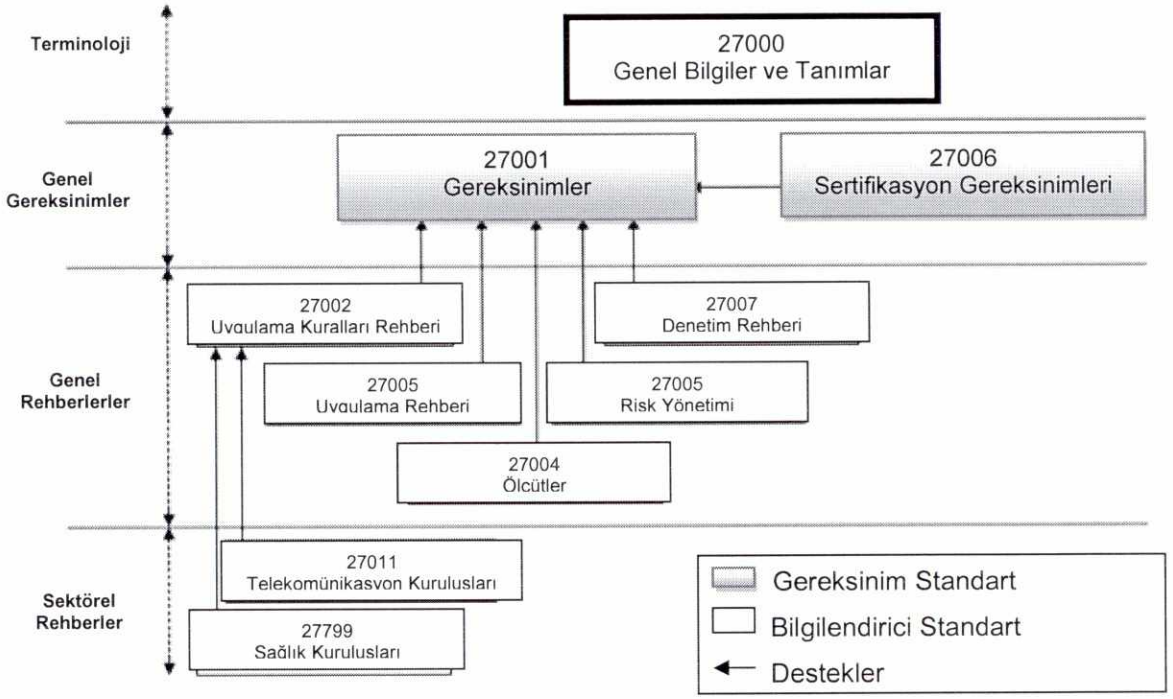
Bilgi Güvenliği Yönetim Sistemi ifadesi, ilk olarak 1998 yılında BSI tarafından yayımlanan BS 7799-2 standardında kullanılmıştır. Daha sonra bu standart ISO tarafından kabul edilerek ISO/IEC 27001:2005 olarak yayınlanmıştır. BSI tarafından daha önce yayımlanan diğer bir standart BS 7799-1 ise bilgi güvenliğinin sağlanmasında kullanılacak kontrolleri içermektedir (IT Governance Ltd.s.1-5, 2006).

BS 7799-1 standardı, ISO tarafından kabul edilmiş ve ISO 17799:2000 olarak yeniden numaralandırılarak uluslararası bir standart haline gelmiştir. Daha sonra ise revize edilerek ISO/IEC 27002:2005 adıyla yayımlanmıştır. Temmuz 2007 tarihine kadar ISO/IEC 17799:2005 olarak bilinen standart, bu tarihten itibaren ISO/IEC 27002:2005 olarak adlandırılmıştır. Bu standartları ISO/IEC 27000 ailesindeki:

- ISO/IEC 27000:2009 - Genel Bilgiler ve Tanımlar
- ISO/IEC 27003:2010 - Uygulama
- ISO/IEC 27004:2009 – Ölçütler
- ISO/IEC 27005:2008 - Risk Yönetimi
- ISO/IEC 27006:2007 - Sertifikasyon Gereksinimleri
- ISO/IEC 27007:2011 - Denetim Rehberi
- ISO/IEC 27011:2008 - Telekomünikasyon Kuruluşları için

rehber dokümanlar takip etmiştir (ISO 27001-BGYS Bilgi Güvenliği Portalı).

Şekil 1.1. ISO/IEC 27000 standartları ve dokümanları arasındaki ilişki




Kaynak: ISO 27001-BGYS Bilgi Güvenliği Portalı

Bilgi güvenliği yönetimi (BGY) konusunda en yaygın olarak kullanılan standart, "ISO/IEC 27002:2005 Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri" standardıdır. Bu standart, işletmeler içerisinde bilgi güvenliği yönetimini başlatmak, gerçekleştirmek, sürdürmek ve iyileştirmek için genel prensipleri ve yönlendirici bilgileri içermektedir. Şekil 1.1.'de görüldüğü gibi ISO/IEC 27002:2005 rehber edinilerek kurulan BGYS'nin belgelendirmesi için "ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler" standardı kullanılmaktadır. Bu standartta, bir BGYS kurulması, uygulanması, işletilmesi, izlenmesi, sürdürülmesi ve iyileştirilmesi için gereksinimler yer almaktadır (ISO, 2005). Yönetim sistemi, organizasyonu, yapıyı ve politikaları, planlama faaliyetlerini, sorumlulukları, uygulamaları, süreçleri ve kaynakları içerir. İş risklerini karşılamak amacıyla ISO/IEC 27002:2005'te ortaya konan kontrol hedeflerinin kurum içerisinde nasıl uygulanacağı ve denetleneceği ISO/IEC 27001:2005'te belirlenmektedir.

Her iki standardın Türkçe'ye tercüme edilmiş hali Türk Standartları Enstitüsü (TSE) tarafından sırasıyla Türk Standartları (TS) ISO/IEC 17799:2005 ve TS ISO/IEC 27001:2005 (TSE, 2005) isimleri ile 2006 yılında yayınlanmıştır.

ISO/IEC 27001 ve ISO/IEC 27002 standartları BGYS konusunda en temel başvuru kaynaklarıdır. Bu iki standart da doğrudan bilgi güvenliği konusunu ele almaktadır (ALPAR, 2011). Ayrıca bu standartlar, Önel ve Dinçkan (2007)'a göre teknik ve teknoloji bağımlı standartlar değildirler. Belli bir ürün veya bilgi teknolojisi ile ilgilenmezler. Tek ilgi alanı vardır, o da bilgi güvenliğidir.

Bilgi Güvenliği Standartları, temel olarak neyin nasıl yapılması gerektiğini tavsiye etse de tüm endüstri dalları için özelleştirilmemiştir. Ancak haberleşme sektörünün önemine binanen ISO/IEC 27002 standardı baz alınarak haberleşme sektörüne özel bir BGYS kurmak, gerçekleştirmek, sürdürmek ve geliştirmek için oluşturulmuş bir uygulama rehberi olan ISO/IEC 27011:2008 standardı yayımlanmıştır (ISO 27001-BGYS Bilgi Güvenliği Portalı).

Yayımlanan ISO/IEC 27011:2008 (ISO, 2008) standardı her ne kadar haberleşme sektörüne yönelik hazırlanmış ISO/IEC 27001:2005 standardının rehber dokümanı olsa da sektör içerisinde sabit, mobil, internet servis sağlayıcılığı, uydu haberleşme v.b. birçok haberleşme türü bulunmakta olup, bilgi güvenliğinin daha etkin bir şekilde sağlanması için, söz konusu heberleşme türleri için özelleştirilmiş BGYS'lere ihtiyaç duyulmaktadır.

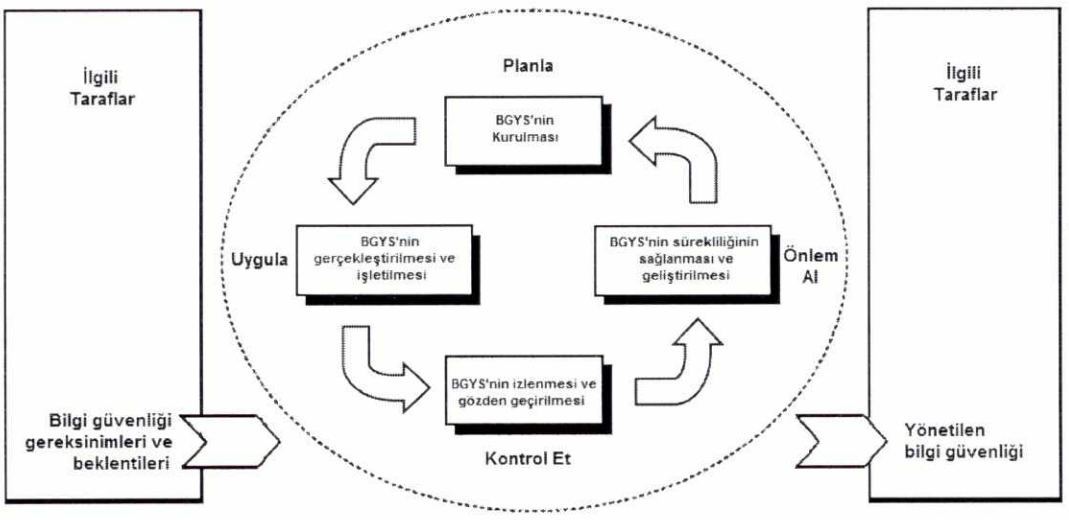
## 1.2 BGYS Nedir?

BGYS, hassas bilgileri yönetebilmek amacıyla benimsenen sistematik bir yaklaşımdır. Bu sistemin temel amacı hassas bilginin korunmasıdır. Bu sistem etmenleri, iş süreçlerini ve bilgi teknolojileri (BT) sistemlerini kapsar.

BGYS'nin faydalı olması için etkin olması gerekir. Bilgi güvenliği, kuruluşun işletme kültürünün etkin bir parçası olmalıdır. Bilgi güvenliği, sadece BT kullanım alanlarında geçerli teknik bir konu olmaktan çok bir yönetim konusudur. İyi uygulanmış bir BGYS, uzun dönemde kuruluşun sadece maliyetlerini düşürmekle kalmaz ayrıca başarısını arttırır. Bilgi güvenliği konusunda zaaf gösteren ve tedbir almayan kuruluşlar için en büyük kayıp, itibar kaybı olmaktadır.

BGYS'nin kurulumu, gerçeklenmesi, işletilmesi, izlenmesi, gözden geçirilmesi, sürdürülmesi ve tekrar gözden geçirilmesi için PUKÖ (Planla – Uygula – Kontrol et – Önlem al) modeli kullanılmaktadır. PUKÖ modelini görsel olarak anlatan Şekil 1.2, bir BGYS'nin bilgi güvenliği gereksinimlerini ve ilgili tarafların beklentilerini girdi olarak nasıl aldığını ve gerekli eylem ve süreçler aracılığıyla, bu gereksinimleri ve beklentileri karşılayacak bilgi güvenliği sonuçlarını nasıl ürettiğini göstermektedir.

Şekil 2.2. BGYS süreçlerine uygulanan PUKÖ modeli




Kaynak: Önel ve Dinçkan, 2007

- **Planla (BGYS'nin kurulması):** BGYS politikası, amaçlar, hedefler, süreçler ve prosedürlerin geliştirilmesi,
- **Uygula (BGYS'nin gerçekleştirilmesi ve işletilmesi):** BGYS politikası, kontroller, süreçler ve prosedürlerin gerçekleştirilip işletilmesi,
- **Kontrol Et (BGYS'nin izlenmesi ve gözden geçirilmesi):** BGYS politikası, amaçlar ve süreç performansının değerlendirilmesi, uygulanabilen yerlerde ölçülmesi ve sonuçların rapor edilmesi,
- **Önlem al (BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi):** Yönetimin gözden geçirme (YGG) sonuçlarına dayalı olarak, düzeltici ve önleyici faaliyetlerin gerçekleştirilmesi.

Önel ve Dinçkan (2007)'a göre bilgi güvenliği yönetimi, başlangıç ve bitiş tarihleri olan bir proje gibi görülmemelidir. Sürekli devam eden bir gelişim süreci olarak düşünülmelidir. PUKÖ modelinde gösterildiği gibi (Planla – Uygula – Kontrol et – Önlem al) faaliyetleri bir döngü içinde durmaksızın sürekli devam etmelidir. PUKÖ modeli özet olarak ne yapılacağına karar verilmesi, kararların gerçekleştirilmesi, çalıştığının kontrol edilmesi ve hedefine uygun çalışmayan kontroller için önlemlerin alınmasıdır.

## 1.3 BGYS İhtiyacı

Bilgi, kuruluşun en değerli varlıklarından biridir. Gerekli koruma olmazsa bilgi:

- Yetki sahibi olmayan kişilere verilebilir, sızdırılabilir veya ifşa edilebilir,
- Habersizce değiştirilerek daha az değerli ya da zarar verici hale getirilebilir,
- Geri kazanım ihtimali bırakılmadan kaybolabilir,
- İhtiyaç halinde ulaşılamaz hale getirilebilir (BSI, ISM04101TRTR).

Bilginin, karşı karşıya kalabileceği tehditlerden uygun şekilde korunmasının temin edilmesi; genel olarak yöneticilerin, bilgi sistemi sahiplerinin veya

koruyucularının ve kullanıcıların sorumluluğu altında olmalıdır. Bilginin, tüm diğer önemli iş varlıkları gibi önleyici tedbirler ile korunması ve uygun biçimde yönetilmesi gerekir.

Burada bahsedilen amaçlar bilgi güvenliğinin esası olan; bilginin gizlilik, bütünlük ve kullanılabilirliğinin korunması gerekliliği olarak özetlenebilir. BGYS; büyük, orta veya küçük tüm kuruluşların yararlanması için geliştirilen, yerinde düşünülen ve uygulanması gereken ortak pratiklerin bir özetidir.

BGYS; değişen ihtiyaçlara, özel hedeflere, kuruluşun büyüklüğüne ve sunulan hizmetlere göre kısmi değişiklik gösterebilir. Ancak her şekilde müşteri memnuniyetini artırmaya yardımcı olduğu muhakkaktır.

Kuruluşların amacı, müşterilerinin ihtiyaçlarını ve beklentilerini tespit etmek ve karşılamak; rekabet avantajı elde etmek; bunları etkili ve verimli şekilde başarmak; kurumsal performansını ve gücünü kazanmak, sürdürmek, iyileştirmektir. BGYS bu uygulamalara doğrudan fayda sağlamaktadır.

BGYS; kuruluşun kendisi, müşterileri ve diğer ilgili taraflar için önemli olan fayda ve masraf yönetimi hesapları ile beraber aşağıda yer verilen hususlar üzerinde de pozitif etkilere sahiptir.

- Bilginin; gizliliği, bütünlüğü ve kullanılabilirliği,
- İşin devamlılığı,
- Gelir ve pazar payı,
- Müşteri memnuniyeti ve sadakati,
- Kaynakların etkili ve verimli kullanılması,
- Artan kurumsal gücün getireceği rekabet avantajı,
- Tehditler ve zayıflıkların düzenli olarak gözden geçirilmesi,
- İstenilen sonuçlara ulaşabilmek için süreçlerin sıralanması,

- İnsanların, kurumsal hedef ve amaçlar doğrultusunda anlayış ve motivasyonları,
- Finansal ve sosyal faydalardan ötürü tüm tarafların kuruluşun etkinliği ve verimliliğine olan güveni,
- Piyasaya ayak uydurmadaki esneklik ve hız kadar, masraf ve kaynakları en uygun boyutlara çekebilme kabiliyeti (BSI, ISM04101TRTR).

Kısacası, bir kuruluş için hayati etmenler olan yukarıdaki hususlarda istenilen sonuçlara ulaşabilmek açısından BGYS, kaçınılmaz bir ihtiyaç sayılmaktadır.

# 2. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ KURULUMU VE DİĞER SAFHALARI

## 2.1 BGYS Kurulumu ve Kurulum Adımları

Kurulum adımlarına geçmeden önce BGYS ile ilgili bilinmesi gerekenlerden bahsetmek gerekir. Öncelikle sağlıklı işleyiş ve yarar sağlaması açısından BGYS'nin kurulması, en üst düzey yöneticilerin vermesi gereken stratejik bir karardır. Üst yönetimin desteği olmadan BGYS'nin başarıya ulaşması düşünülemez. Öncelikli şart; üst yönetimin, BGYS'nin gerekliliğine ve faydasına inanmasıdır.

BGYS kurulumu, bir bilgi teknolojileri ürünü veya sistemi kurulumuyla karıştırılmamalıdır. BGYS kuruluşun iş yapma tarzını tümüyle etkileyen bir sistemdir. Tüm kademelerdeki çalışanların işlerini bilgi güvenliği prensiplerine uygun hareket ederek yapmalarını gerekli kılmaktadır.

En yaygın yanlış kanılardan biri BGYS'nin sadece kurumun BT bölümüne ait bir iş olduğunun düşünülmesidir. BGYS, teknolojik veya teknik bir iş değildir. Kuruluşun tüm süreçlerinin aktif halde katılımıyla hedefine ulaşabilecek bir sistemdir. Üst kademe yöneticiden alt seviye çalışana kadar geniş katılım ve destek şarttır. Aksi halde BGYS'den beklenen fayda elde edilemez.

BGYS kurulumunda ilk yapılması gereken işlerden bir diğeri de kurum içinde bir Bilgi Güvenliği Grubu oluşturulmasıdır. Bu gruba bilgi güvenliği komisyonu ya da bilgi güvenliği yönetimi birimi adı da verilebilir. Bilgi güvenliği grubu, kuruluş içindeki her bir bölümden katılan temsilcilerden oluşur. Kuruluş bünyesinde yer alan bilgi işlem, pazarlama, satış, depo, muhasebe, insan kaynakları, güvenlik v.b. diğer tüm bölümlerden temsilciler, bu gruba katılmalıdırlar. Grup çalışanları, kendi bölümlerini temsil edebilme yetkisine sahip kişiler olmalıdır. Bilgi güvenliği konusunda yeterli bilgi seviyesine sahip olmayan grup üyeleri, mutlaka temel BGYS eğitimlerini almalıdırlar. Tüm

bölümlerden temsilci katılımı BGYS'nin başarı şansını arttırır ve gerekli güvenlik ihtiyaçlarının daha etkin biçimde farkında olunmasını sağlar. Bu durum BGYS'nin doğru planlanması ve sağlıklı işlemesi açısından çok büyük öneme sahiptir. Her bölümden bir temsilcinin katılımı, yönetim ve çalışanlar arasındaki iletişimi de güçlendirir. Problemleri yerinde yaşayan ve ihtiyaçları bilen kişiler, bu konularda yönetimin daha kolay ikna edilmesini sağlar. Bilgi güvenliği grubu sayesinde sadece bir birimin işi olmayan BGYS ile ilgili görev ve sorumluluklar kuruluşun tüm bölümlerine dağıtılmış olur (The Importance of Setting up an Information Security Management Committee in Organization).

BGYS kurulurken sistemin; yazılı hale getirilmesi, uygulanması, işletilmesi, sürdürülmesi ve sürekli iyileştirilmesi gereksinimleri tanımlanmalıdır. Kurulum, sistem için gerekli süreçleri tanımlamak demektir. Bu süreçlerin sıralanışının ve birbirleri ile etkileşiminin yanı sıra, süreçlerin etkili biçimde işletilmesi ve kontrolü için gereken kriterler ve yöntemler tespit edilmelidir. Süreçlerin işletilmesini ve izlenmesini destekleyecek gerekli bilgi, tüm çalışanlar için ulaşılabilir ve kullanılabilir hale getirilmelidir. Tüm bu süreçler ölçülmeli, izlenmeli, çözümlenmeli ve planlanan sonuçları başarmak için gerekli faaliyetler gerçekleştirilmelidir.

### 2.1.1 Kapsam belirleme

BGYS'nin kapsamı ve sınırları belirlenmelidir. BGYS'nin kapsamı, kuruluşun bütünü olabileceği gibi belli bir kısmı da olabilir. Kapsam belirleme işlemi, işin özelliklerine, kuruluşa, kuruluşun yerine, varlıklarına ve teknolojisine göre yapılmalıdır. Kapsamın diğer sistemler, kuruluşlar, üçüncü taraf tedarikçiler ile olan etkileşimi göz önünde bulundurulmalı ve varsa bağımlılıkları da dikkate alınmalıdır. Kuruluşun, kapsam dışında bırakılanların hangi sebeplerle dışarıda bırakıldıklarını sağlam gerekçelerle açıklayabilmesi

gerekmektedir. Ancak, her durumda, BGYS kapsamı ve sınırları eksiksiz ve doğru bir biçimde tanımlamalıdır.

BGYS kapsamı, üst yönetimin niyeti ve kurumun bilgi güvenliği hedefleri dikkate alınarak belirlenir. ISO/IEC 27001 ve ISO/IEC 27002 standartlarının bu konuda belli bir yönlendirmesi veya zorlaması söz konusu değildir. Bu adımın sonunda bir kapsam dokümanı yayınlanmalı ve üst yönetim tarafından onaylanmalıdır (Önel ve Dinçkan, 2007).

### 2.1.2 BGYS politikası tanımlama

Politika; kuruluş, yapılan işler, kuruluşun yeri, varlıklar, kullanılan teknoloji, yasal gereksinimler, sözleşmeye bağlı üçüncü taraflardan kaynaklanan zorunluluklar dikkate alınarak belirlenir. Bu politika, hedefleri ortaya koyan, yönetime yön veren ve harekete geçiren, hangi riskin değerlendirmeye alınacağına ilişkin risk yönetim kapsamı ve kriterini belirleyen bir çerçeve sunmalıdır. BGYS politikasının; gereksinimleri karşılaması, standartlara bağlılığını ifade etmesi ve BGYS'yi sürekli iyileştiriyor olması önemlidir.

Yönetim, ister yazılı ortamda isterse elektronik ortamda doküman haline getirilmiş BGYS politikası içeriğindeki maddelerin uygulamaya geçirileceğine ilişkin kararlarlığını çalışanlara hissettirmeli ve ilgili farkındalık faaliyetlerinde bulunmalıdır.

### 2.1.3 Risk değerlendirme yaklaşımı

Risk değerlendirme yaklaşımı, bilgi güvenliği politikası temel alınarak belirlenir. Kuruluşun riskleri kabul etme kriterleri ve kabul edilebilir risk seviyesinin neler olduğu risk değerlendirme yaklaşımı ile netleştirilir. Bu konuda kuruluş, kendine uygun bir metodoloji seçmekte serbest olsa da ISO 27001:2005 standardında yer alan tüm kontrol alanlarını (yönetim organizasyonu, personel kontrolleri, iş süreçleri, işletme ve bakım süreçleri,

düzenleme ve sözleşmelere tabii konuları, bilgi işleme imkanları) yaklaşımı içerisine katmalıdır (BSI, ISM04101TRTR).

Bağcı (2008)'ya göre seçilen risk değerlendirme metodolojisi kıyaslanabilir ve tekrarlanabilir sonuçlar üretebilmelidir. Bu adımda organizasyonun hedefleri ve faaliyetleri üzerinde herhangi bir potansiyel etkinin oluşturacağı beklenmedik olaylar önceden belirlenir, analiz edilir ve değerlendirilir. Geri kalan riskleri kabul edilebilir bir seviyeye ulaştırmak için risk karşılama stratejileri uygulanır.

Risk değerlendirmede, risklerin yeniden değerlendirilmesi, tehditlerin, zayıflıkların ve varlıkların güncellenmesi gereken birçok durumda, bir yazılım aracının kullanılmasında faydalar olabilir. Çünkü geniş ölçekli kuruluşlarda güncellemelerin otomatik bir sistem olmaksızın zamanında ve doğru şekilde yapılması zor olabilmektedir. Ancak yine de herhangi bir otomatik yazılım aracının kullanılması zorunlu değildir.

### 2.1.4 Risk belirleme (tanımlama)

Risk belirleme işlemi; kuruluşu, yapılan işleri, varlıkları, kullanılan teknolojiyi etkileyecek (bilinen ve potansiyel) tehditlerin, yükümlülüklerin ve saldırılara açık olma durumunun değerlendirilmesidir.

Önel (2007)'e göre BGYS içerisindeki tüm varlıkların tanımlanması, yani varlık envanterinin çıkarılması risk değerlendirme işinin esasını oluşturur. Bunlar; saygınlık, fikri mülkiyetler, ticari sırlar gibi konuları da içerebilir. Kuruluş, BGYS kapsamına dahil edeceği tüm varlıkların sahiplerini, türünü ve önem derecesini bir envanter listesi şeklinde belgelemelidir. Bir varlığın önem derecesini belirlemek için bu varlığın gizliliğine, bütünlüğüne ve kullanılabilirliğine gelecek zararın kuruluşa yapacağı etkinin derecesini baştan ortaya koymak gerekmektedir. Varlıkların gizlilik, bütünlük ve kullanılabilirlik özelliğine gelecek zararlar farklı etki derecelerine sahip

olabilirler. Örneğin çok gizli seviyede bir bilginin açığa çıkması kuruma büyük zararlar verebilecekken aynı gizli bilginin kullanılamaz hale gelmesi o kadar büyük zarar oluşturmayabilir.

Bağcı (2008), risk belirleme çalışmaları sonucunda risk kayıtları oluşturulması gerektiğini ifade eder. Risk kayıtları, bir risk numarasını, riskin sahibini, riskin sınıfını, riskin açık ifadesini ve riskin değerini (yüksek, orta, düşük vb.) içermelidir. Risk belirleme çalışmaları sırasında kullanılabilecek teknikler arasında olay analizi, tehdit modelleme, saldırıya açık olma analizi, senaryolar ve beyin fırtınaları sayılabilir.

### 2.1.5 Risk analizi

Bu adım bir önceki adımda tespit edilen risklerin, iş kolu hakkında detaylı bilgiye sahip, iş kolunun devamlılığı için sorumlulukları olan orta seviye yöneticilerle ve çalışanlarla birlikte detaylı incelenmesidir. Muhtemel katılımcılar; bilgi güvenliği grubu üyeleri, iş sürekliliği sorumluları, birim sorumluları, iş yöneticileri ile proje yöneticileri ve teknik uzmanlar olabilir. Risk analizi yaparken riske neden olan tehdit ve açıklıklardan yola çıkılmalıdır.

Risk, açıklığın bir tehdit tarafından kullanılmasıyla oluşur. Örneğin ahşap bir ev düşünelim. Evin ahşap oluşu, açıklığı temsil eder. Olası bir kıvılcım ise burada tehdidi oluşturur. Bu ikisinin bir araya gelmesiyle risk oluşur ki bu örnekte risk evin tutuşması ile evdeki insanların veya eşyaların zarar görmesidir. Bir tehdit, bir sisteme veya kuruluşa ve onun varlıklarına zarar verebilecek güvenlik ihlal olaylarına sebep olma potansiyeli taşır. Bu zarar, kuruluşun bilgisine doğrudan veya dolaylı bir atak olarak ortaya çıkabilir. Tehditler, kaza eseri veya kasti kökenlerden veya olaylardan kaynaklanıyor olabilir (BSI, ISM04101TRTR).

Tehditler organizasyon dışından gelebileceği gibi içinden de gelebilmektedir. Herhangi bir zayıflık olmadığı durumda tehdidin kaynağı bir risk oluşturmamaktadır. Bu adımda potansiyel tehdit kaynakları belirlenmeli ve bilgi sistemleri için tehdit olabilecek durumlara ait ifadeler listelenmelidir. En belirgin tehdit kaynakları şunlardır:

- Çevresel kaynaklar (sel, yıldırım, fırtına, deprem, yıldırım vb.)
- Organizasyonel eksiklikler (kadro eksikliği, aşırı trafik/işlem yükü, tam tanımlanmamış sorumluluklar vb.)
- İnsan hataları (şifreleri kâğıt üzerine yazma, yanlışlıkla dosya silme, sırlara ilişkin bilinçsiz konuşmalar vb.)
- Teknik hatalar (donanım arızaları, kısa devre, sabit disk arızalanması vb.)
- Planlanmış eylemler (hırsızlık, hack'leme, e-dolandırıcılık, zararlı kod kullanımı vb.)

Bağcı (2008)'ya göre risk analizleri yapılırken, sadece temel ve kalıcı (inherent risks) riskler değerlendirilmez aynı zamanda uzatmalı (prolonged risks) veya artakalan (residual risks) riskler de (konfigürasyon ve değişiklik kontrolleri veya süreçlerin kullanılmaması vb.) incelenir.

### 2.1.6 Risk derecelendirmesi

Riskin derecelendirilmesi veya değerinin belirlenebilmesi için öncelikle tehdidin veya güvenlik hatasının işe ve kuruluşa vereceği zarar ve böyle bir olayın oluşma ihtimali hesaplanmalıdır. Risk değerlendirmesi esnasında göz önüne alınan kriterler, iş öncelikleri, kuruluşa olan etkinin büyüklüğü, önemlilik, maliyet ve faydalar, paydaş endişeler ve yasal gereksinimler olabilmektedir.

Kuruluş gerçekleşme olasılığı ile etki derecesini dikkate alarak riskin seviyesini hesaplamak ve riskin kabul edilebilir mi, yoksa kendi iş bağlamında ele alınması gereken bir risk mi olduğuna karar vermelidir. Bu hesaplamalar yapılırken sayısal değerler kullanılabileceği gibi rakamlarla ifadenin zor olduğu durumlarda düşük, orta, yüksek gibi nitel değerler de kullanılabilir. Tüm bu hesaplama ve değerlemeler, uygulanan mevcut kontroller dikkate alınarak yapılmalıdır. Kontroller risk değerini azaltabilir. Risk değerlendirmesi bitiminde bir risk değerlendirme sonuç raporu yayınlanmalıdır.

### 2.1.7 Risk işleme

Bu adımda risk değerlendirme sonuç raporundan yola çıkılarak uygun risk davranış yöntemleri belirlenir. Risk değerlendirme sonuç raporu ile kuruluş risklerin işine olan etkisini belirlemiş ve değerlendirmiş olduğundan riskleri, uygun şekilde yönetmek ve işletmek için çeşitli önlemler alabilir. Önel (2007), belli bir risk karşısında dört farklı önlem saymıştır:

1. Uygun kontroller uygulanarak riskin ortadan kaldırılması veya kabul edilebilir seviyeye düşürülmesi,
2. Riskin oluşmasına neden olan faktörleri ortadan kaldırarak riskten kaçınılması,
3. Riskin sigorta şirketleri veya tedarikçiler gibi kurum dışındaki taraflara aktarılması,
4. Kurum politikalarına ve risk kabul ölçütlerine uyması şartıyla riskin objektif bir biçimde ve bilerek kabul edilmesi.

### 2.1.8 Kontrollerin seçimi

Risk yönetmek ve işlemek için kontroller uygulanmaya karar verildikten sonra bu amaca uygun kontrol ve kontrol hedeflerinin seçilmesi gerekir. Kontrol seçiminin gayesi, riskleri kuruluş için kabul edilebilir seviyeye indirmektir. Bu

kontroller, ISO/IEC 27001:2005 Ek-A'da yer almaktadır ve yol gösterici olması amacıyla verilmiştir.

ISO 27001 standardı BGYS kurmak isteyen kuruluşun risk analizi çalışmasının ardından çeşitli kontrolleri devreye sokarak mevcut riskleri tedavi etmesini ve kabul edilebilir risk seviyesinin altına indirmesini şart koşmaktadır. Bu kontroller 27001 standardı içerisinde "vazgeçilemez doküman" olarak gösterilen ISO 27002 standardında detaylı olarak açıklanmaktadır (Ottekine, 2008).

Diğer taraftan BGYS'yi kurmak için gerekli önlemler havuzu olarak sayılabilecek ISO/IEC 27002; Bilgi Güvenliği Yönetimi Sistemi (BGYS) oluşturmak için gereken 11 ana başlık altında yapılandırılmış, 133 adet güvenlik kontrolünü tanımlayan bir uygulama kılavuzu olarak kullanılabilir.

ISO/IEC 27001, ISO/IEC 27002'de ayrıntılı olarak verilen tüm bu kontrollerin bir özetini ek olarak sunar. (EZBER, 2010a).

**Ana Kontrol Alanları:**

1. **Güvenlik politikası:** Bilgi güvenliği konusunda yönetimin bakış açısını, onayını ve desteğini iletmek amacıyla, bir bilgi güvenliği politika dokümanı oluşturulmalı ve bu doküman yöneticiler tarafından onaylandıktan sonra yayınlanmalıdır.

   Bilgi güvenliği süreklilik gerektiren bir süreçtir. Aynı şekilde bilgi güvenliği politikalarının da sürekli uygunluğunu ve etkinliğini sağlamak için, dokümanlar düzenli aralıklarla veya önemli değişiklikler olduğu durumlarda tekrar gözden geçirilmelidir.

2. **Bilgi güvenliği organizasyonu:** Bilgi güvenliği organizasyonel altyapısının oluşturulması ve gerekli rollerin, sorumlulukların tanımlanması, iş süreçlerinin belirlenmesi gereklidir.

3. **Varlık yönetimi:** Kurum için kritik önem taşıyan her türlü bilgi varlıkları belirlenmeli ve değerleri, kiritiklik seviyeleri ve yasal gereksinimlerine göre sınıflandırılmalıdır. Varlıkların sahiplikleri ve sorumlulukları kurum içindeki belirli kişilere veya bölümlere verilmelidir.

4. **Personel güvenliği:** Kurumun bilgi güvenliği politikasına uygun olacak şekilde, çalışanların güvenlik rolleri ve sorumlulukları tanımlanmalıdır. Personel işe alımlarında gerekli kontroller yapılmalı ve ihtiyaç duyulduğu durumlarda gizlilik anlaşmaları imzalanmalıdır.

   Kullanıcıların güvenlik bilincini ve farkındalığını arttırmak amacıyla düzenli aralıklarla kurum içi eğitimler düzenlenmelidir.

5. **Fiziksel ve çevresel güvenlik:** Kart kontrollü giriş kapıları, görevli bulunan resepsiyon masaları gibi çok çeşitli fiziksel ve çevresel güvenlik önlemleri ile bilgiye erişimin sağlanabileceği ortamlara, kontrolsüz fiziksel erişim engellenmelidir.

   Bina içlerindeki güvenlik seviyeleri farklı olan alanlar, fiziksel olarak birbirinden izole hale getirilmelidir. Hassas alanlara erişimler kayıt altına altına alınmalı ve bu kayıtlar düzenli olarak kontrol edilmelidir.

6. **İletişim ve işletme yöntemi:** Bu kapsamda, işletim prosedürleri dokümante edilmeli, güncel tutulmalı ve ihtiyacı olan çalışanların kullanımına sunulmalıdır.

   Geliştirme, test ve operasyon ortamları birbirinden ayrılmış olmalı ve etkili bir değişim yönetim sistemi uygulanıyor olmalıdır. Sistemlerin, yazılımların, verilerin yedeklerinin düzenli olarak alınıyor ve test ediliyor olması gereklidir. Ayrıca çalışanlar için görev ayrılığı prensibi uygulanmalıdır. Hiçbir kullanıcı bir süreci başından sonuna kadar tek başına yürütebiliyor olmamalıdır. Örneğin, bir erişim yetkisine ihtiyaç duyulduğunda, aynı kişinin hem o erişim talebine onay verip, hem de erişim tanımını yapması uygun değildir.

7. **Erişim denetimi:** Her kurum, kendi yapısında bir erişim yönetim ve denetim sistemi işletiyor olmalıdır. Her türlü bilgiye veya sisteme erişim kontrol altında tutulmalıdır. Sadece gerekli olan personele, gerektiği kadar erişim yetkisi verilmesi prensip olarak kabul edilerek, uygulanmalıdır.

   Kurumun güvenlik politikalarına uygun olacak şekilde bir erişim kontrol politikası oluşturulmalı ve dokümante edilmelidir. Kullanıcılar kendi erişim hakları ve yükümlülükleri konusunda bilgilendirilmelidir.

8. **Bilgi sistemi tedariği, geliştirilmesi ve bakımı:** Kurum içinde geliştirilen veya dışarıdan alınan uygulamalar ve sistemler, kurumun güvenlik politikalarını destekleyecek şekilde planlanmalı ve tasarlanmalıdır. Kullanılan sistemlerin teknik açıklıkları bilinmeli ve varsa bu riskler değerlendirilerek uygun önlemler alınmış olmalıdır.

   İçeride geliştirilen uygulamaların kaynak kodları güvenli şekilde saklanmalıdır.

9. **Bilgi güvenliği olayları yönetimi:** Güvenlik olay ekipleri ve yöntemleri belirlenmelidir. Güvenlik ihlal durumunda, hızla gerekli yönetim birimlerine haber verilmesi için yöntem ve akışlar tanımlanmalıdır.

10. **İş sürekliliği yönetimi:** İş sürekliliğinin sağlanması bir süreç olarak tanımlanmalı ve felaket senaryoları planlanmalıdır. Bu senaryolara bağlı olarak iş devamlılık ve etki analizleri yapılarak kritik ve öncelikli iş süreçleri belirlenmelidir.

    Büyük çaplı sistem arıza ve çökme durumlarında, doğal afetlerde, kritik işlerin devamlılığını sağlayabilmek için gerekli önlemler alınmalıdır. İş sürekliliği planları oluşturulmalı ve güncel tutularak, düzenli olarak test edilmelidir.

11. **Uyum:** Kurumun uymakla yükümlü olduğu yasal düzenlemeler ve sözleşmelerden doğan gereksinimler belirlenmeli, dokümante edilmeli ve gerekli koşullar sağlanmalıdır (Bilgi Güvenliğinde ISO 27000 Standartlarının Yeri ve Öncelikli ISO 27002 Kontrolleri, 2009)

Kuruluş, kendi BGYS'sine göre ek kontroller de seçebilir. Standartta bulunan kontroller, standart etki alanlarında olabildiğince geniş kapsamlı olarak belirlenmiş olsa da dış kaynaklı kontrollere ihtiyaç duyulabilmektedir. Standartların dışında, herhangi bir bilgi güvenliği kaynağından uygun kontroller seçilebileceği gibi kuruluşun kendine özel geliştirebileceği kontroller de olabilmektedir.

Kontrollerin seçiminde, kabul edilebilir maliyetlerde olmaları göz önünde bulundurulmalıdır. Kontrollerin uygulanma maliyeti indirgenmek istenen risklerin finansal etkilerini aşmamalıdır. Aksi takdirde anlamını yitirir. Ayrıca bu etkilerin emniyet, kişisel bilgi, yasal zorunluluklar, imaj ve itibar ile de ilgisi dikkate alınmalıdır.

Kontroller seçilirken aşağıdaki bir dizi faktör dikkate alınmalıdır:

- Kontrollerin kullanım kolaylığı,
- Kullanıcı için saydamlık,
- Kullanıcılara işlevlerini yerine getirmeleri için sağlanan yardım,
- Kontrollerin göreli gücü,
- Yürütülen işlevlerin türleri-önleme, caydırma, saptama, geri alma, düzeltme, izleme ve farkında olma (BSI, ISM04101TRTR).

Genellikle, bir kontrol bu işlevlerin birden çoğunu yerine getirir ve ne kadar çok işlev yerine getirebiliyorsa o kadar iyidir. Toplam güvenlik açısından tüm işlevleri karşılayacak bir denge gözetilmelidir (BSI, ISM04101TRTR).

### 2.1.9 Kabul edilebilir risk onayı (KERD)

Kuruluş için tüm risk kontorlleri ve iyileştirmeleri sonrasında her zaman arta kalan bir risk olacaktır. Bunun nedeni kuruluş içerisinde hiçbir zaman yüzde yüz güvenliğin sağlanamaycak olmasıdır.

Bir riskin kabul edilebilir seviyeye indirgenmesi için belirlenmiş uygun kontroller sonrasında bu riskin daha ne kadar indirgenebileceği değerlendirilir ve kalan risk, artık risk olarak adlandırılır. Bu artık riskin değerlendirimesi zordur, ama yeterli korumanın başarıldığından emin olmak için kontroller sayesinde yapılan iyileşmenin riski ne kadar düşürdüğüne bakılabilir. Artık riskin, kabul edilebilir seviyede olduğuna kanaat getirilirse bu seviyedeki risk kabul edilebilir risk olarak belirlenir. Eğer risk düzeyinin halen yüksek olduğu ve kabul edilemez olduğu düşünülürse ilave kontrollerin seçilmesi gerekir.

Yukarıda bahsedilen kabul edilebilir risk düzeyi, bilgi güvenliği yönetimi birimince üst yönetime sunulur ve üst yönetim kuruluş için bu seviyedeki risklerin kabul edilebilir olduğuna kanaat ederse bu risk düzeyini onaylar. Onaylanan bu risk düzeyi, kabul edilebilir risktir ve tüm risklerin bu seviyeye indirilmesi BGYS'nin amacıdır.

### 2.1.10 Uygulanabilirlik bildirgesi

Uygulanabilirlik bildirgesi, riskler işlenirken seçilmiş kontrollerin neler olduğu ve bunların hangi gerekçelerle seçildiğini anlatan bildirgedir. Eğer kuruluş TS ISO/IEC 27001:2005 standardına uygunluk belgesi almak istiyorsa seçilen kontroller ve bunların seçilme nedenlerini açıklamalıdır. Standardın Ek-A'sındaki kontrollerden herhangi birinin dışarıda bırakılması ve bunların dışarıda bırakılma nedenlerine ilişkin açıklamalar, uygulanabilirlik bildirgesinde ele alınır. (Yönetimonline, 2009). Diğer bir ifadeyle seçilmemiş olan TS ISO/IEC 27001 standardın EK-A'sında yer alan 133 adet kontrol

maddelerinin de neden seçilmediğine dair geçerli gerekçelerin uygulanabilirlik bildirgesinde yer alması gerekir.

## 2.2 BGYS'nin Gerçekleştirilmesi Ve İşletilmesi

Kuruluşların, BGYS'yi kurduktan sonra uygulama aşamasında yapmaları gerekenler aşağıdaki gibi sıralanabilir:

- Risklerin giderilmesi adına risk planı hazırlanmalı ve bu plan uygulanmalı,
- Kontroller gerçekleştirilmeli,
- Eğitimler verilmeli ve farkındalık oluşturulmalı,
- Prosedürlere uygun hareket edilmelidir (BTK, 2007,Haberleşmenin Güvenliği).

## 2.3 BGYS'nin İzlenmesi Ve Gözden Geçirilmesi

Kuruluşların etkin bir BGYS'ye sahip olmaları için, sistemin detaylarını sürekli gözden geçirmeleri gereklidir. Eğer sistemde aksak yönler varsa bunlar derhal ele alınmalı ve en kısa zamanda giderilerek, eksiklerini gidermiş bir sisteme sahip olunması hedeflenmelidir. Bunun için aşağıdaki tavsiyeler önem arz etmektedir:

- Denetleme prosedürleri uygulanmalı,
- Düzenli gözden geçirmeler yapılmalı,
- Risklerin tehdit düzeyleri gözden geçirilmeli,
- İç BGYS denetçileri görevlendirilmeli,
- Dış denetimler alınmalı,
- BGYS'nin performansını ve etkinliğini etkileyecek olaylar ve faaliyetler kaydedilmelidir (BTK, 2007,Haberleşmenin Güvenliği).

## 2.4 BGYS'nin Sürekliliğinin Sağlanması Ve İyileştirilmesi

BGYS'nin mevcut etkinliğinin korunması ya da gelişen teknoloji ve yenilikler ile birlikte daha üst etkinlik sınırlarına ulaştırılabilmesi için aşağıdaki önlemlerin alınması gerekecektir.

- BGYS teknolojilerine ait yenilikler sisteme eklenmeli,
- Belirlenen düzenleyici ve önleyici faaliyetler uygulanmalı,
- İlgili birimlerle kordinasyon halinde olunmalı,
- Sistemde yapılan yenilemelerin istenen sonuçları verip vermediği kontrol edilmelidir(BTK, 2007,Haberleşmenin Güvenliği).

# 3. 2N VE 3N MOBİL HABERLEŞME SİSTEMLERİ İÇİN ÖRNEK BGYS MODELİNİN KURULUMU

Mobil haberleşme sistemlerine sahip olan mobil işletmecilerin model olarak kullanabileceği BGYS sisteminin kurulması ve işletilmesinde önerilen adımlar, aşağıdaki alt başlıklar altında verilmektedir.

## 3.1 Yönetimin Kararlılığı

Bilgi güvenliği söz konusu olduğunda çoğu kişi için bilgi teknolojilerinden kaynaklanan riskler akla gelmektedir. Ancak doğru olan, bilgi teknolojilerinin risk çeşidini arttırdığıdır. Bilgi güvenliğinin sınırlı bir bölümü teknoloji ile ilgiliyken, çok daha büyük kısmı personel ve süreçler ile ilgilidir. Teknoloji ile ilgili riskler genellikle bilgi teknolojileri yönetimi çerçevesine ihtiyaç duymadan seviyesi düşürebilecek risklerden oluşurken, personel ve süreçler ile ilgili riskler ise genellikle Bilgi Güvenliği Yönetimi (BGY) çerçevesinde seviyeleri düşürülebilecek risklerden oluşmaktadır. Bu nedenle, birçok işletmede standart güvenlik önlemleri (güvenlik duvarı, antivirüs vb.) tedarik edilip kullanılırken, bu karşı önlemlerin etkinliği (kuralların düzgün girilmesi, sistem günlüklerine bakılması, sistemlerin prosedürlere göre işletilmesi, sistemler üzerinde iç denetim yapılması vb.) konusunda sıkıntılar yaşanmaktadır. Daha ayrıntılı açıklamak gerekirse: işletmenin bilgi sistemlerini dış saldırılardan korumak için kurulan bir güvenlik duvarı bilgi güvenliğinin teknolojik yönünü yansıtmaktadır. Ancak, işletmenler tarafından güvenlik duvarına gerekli olan kuralların girilmemesi veya bilgisayar kullanıcıların modem gibi cihazlar yoluyla internete çıkmaları bu teknolojik önlemden beklenen faydayı sıfıra indirebilmektedir.

Haberleşme şebekelerinin de bilgi teknolojileri, personel ve iş süreçleri ile bütün olduğu düşünülürse, mobil işletmecilerin iş süreçlerinin hemen hemen hepsinin gerçekleşmesinde teknolojiden ve diğer nedenlerden kaynaklanan risklerin büyük pay sahibi olduğu ve iş süreçlerini kötü yönde etkileyebileceği değerlendirilebilir. Bu nedenle işletmelerde artan risklerin iyi yönetilebilmesi

ve düşürülmesi -olayın sadece bir bilgi işlem faaliyeti olarak anlaşılmasının da önüne geçmek açısından- en önce yönetimin görevi olarak kabul edilmelidir.

Bilgi güvenliğini sağlamak için sadece teknolojik karşı önlemler değil, insanları ve iş süreçlerini ilgilendiren karşı önlemler de uygulanmalıdır. Bilgi güvenliğinin sadece teknolojik karşı önlemler ile sağlanabilmesinin mümkün olduğu varsayıldığında, bilgi işlem yöneticisinin sorumlu olmasının yeterli olduğu söylenebilecektir. Ancak, bilgi güvenliğinin sağlanması için, işletmedeki personeli ve süreçleri de içine alan karşı önlemlerin gerekli olması nedeniyle, yönetimin bilgi güvenliğinden sorumlu olması gerekmektedir. Gerekli prosedürlerin oluşturulması ve takip edilmesi, iç denetimlerin yapılması, çalışanların uyması gereken prensiplerin yer aldığı politika dokümanlarının oluşturulması, disiplin sürecinin işlemesi gibi teknolojik olmayan gerekli birçok önlem ancak yönetimin sağlayacağı destek ile gerçekleştirilebilmektedir (Karabacak, 2008).

Bu nedenle model olarak önerilen BGYS'de bilgi güvenliği yönetiminin en önemli unsuru üst düzey yönetimin bizzat bilgi güvenliğinden sorumlu olmasıdır. İşletme yönetiminin, işletmede bilgi güvenliğini sağlama niyeti, politikada bulunması gereken en önemli ifadedir. Bu ifade olmadan, bilgi güvenliği personelinin yapmaya teşebbüs ettiği herhangi bir faaliyet etkin şekilde gerçekleşemeyecek ve işletme içinde ciddiye alınmayacaktır. Yönetim, vereceği bu sözle, bilgi güvenliği amaçlarına ulaşma konusunda kararlılığını ve bu iş için gereken desteği sağlayacağını ifade ederken, işletme çalışanlarının bilgi güvenliğine önem vermesini de sağlamaktadır.

Öztürk (2008)'e göre kuruluş içindeki en yüksek makam tarafından atılan onay imzası, kuruluşta bilgi güvenliğinin sağlanmasının yönetim tarafından desteklendiğini gösterir. Mobil işletmecilerde en üst düzey yöneticinin İcra Kurulu Başkanı (Chief Executive Officer- CEO), olduğunu varsayarsak bu konudaki iradenin CEO seviyesinde olması gerekir.

Bu konuda alınacak aşağıdaki gibi yazılı bir karar yönetimin bilgi güvenliği konusundaki kararlılığını gösterecektir.

| |
|---|
| "Kurum Bilgi Güvenliği Politikası"nın uygulamasının sağlanmasının ve kontrolünün yapılmasının, güvenlik ihlallerinde de gerekli yaptırımın icra edilmesinin yönetim tarafından desteklendiğini beyan ederim.<br><br>CEO (Chief Executive Officer) İcra Kurulu Başkanı |

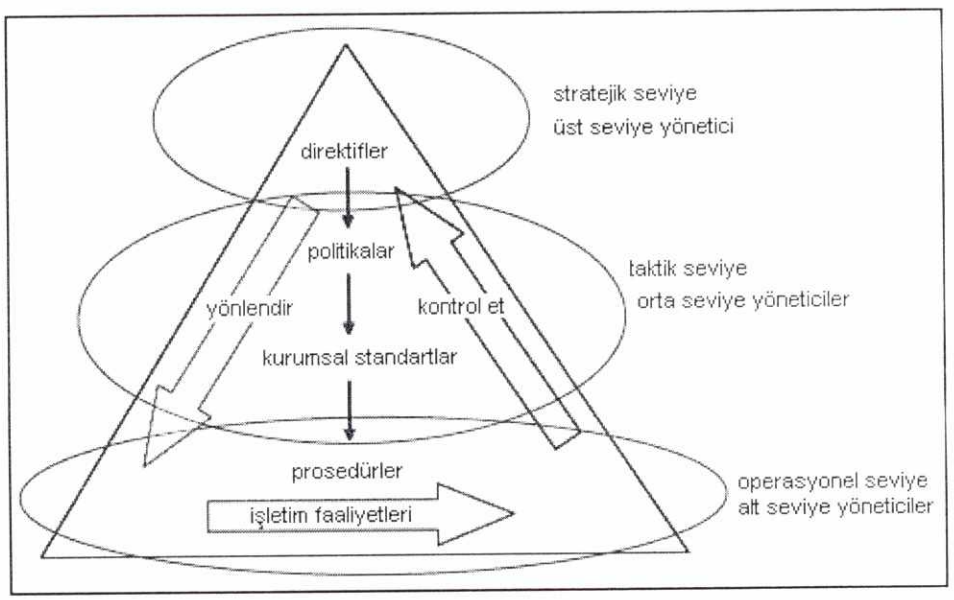
Yönetimin kararlılığı ve desteğinin yanında üstlenmesi gereken başka görevleri de bulunmaktadır. En üst düzey yönetici olan CEO'nun BGYS'nin kurulması ve diğer aşamalarına ait görevleri aşağıdaki gibidir.

1. Kaynakları (BGYS bütçesini onaylamak) sağlamak,
2. Bilgi güvenliği yönetimi biriminin sunduğu kontrol seçimlerine onay vermek,
3. Yatırım ve değişimler için onay vermek,
4. Düzenli BGYS- yönetimin gözden geçirmesi (YGG ) toplantılarına başkanlık etmek,
5. İşletme çalışanlarının katılımı için teşvik edici faaliyetlerde bulunmak,
6. BGYS proje koordinatörünü, yöneticisini, liderlerini ve takım üyelerini atamak ve yetkilendirmek,
7. BGYS risk kabul kriterlerini belirlemek, kabul edilebilir risk düzeyini onaylamak (Taşkın,2011).

Bilgi güvenliği yönetiminin, üst yönetimce desteklendiği ve uygulandığı işletmelerde, BGYS kurmak ve işletmek oldukça kolay olmaktayken, üst yönetim desteğinin olmadığı işletmelerde ise BGYS bir bilgi işlem faaliyeti gibi algılandığından BGYS'den beklenen başarı, verim ve güvenlik sağlanamamaktadır.

Model önerisinde, BGYS yönetimi için temelinde "yönlendir" ve "kontrol et" aktivitelerinin yer aldığı Solms tarafından tanımlanan ve Şekil-3.1'de gösterilen yönetim şekli önerilmektedir (Solm ve Solms, 2006, s.408-413).

Şekil 3.1. Yönlendirme ve kontrol etme döngüsünün kullanıldığı bilgi güvenliği yönetim şekli




Kaynak: Karabacak,2008

Solms'un bu çalışmasında, işletme içerisindeki yönetim seviyeleri stratejik, taktik ve operasyonel seviyeler olmak üzere üç seviyede ele alınmıştır. Stratejik seviyede kuruluşun üst düzey yöneticisi, taktik seviyede orta seviye yöneticiler ve operasyonel seviyede ise alt seviye yöneticiler yer almaktadır. Bu yönetim kademelerinde "yönlendir" ve "kontrol et" aktiviteleri aşağıdaki şekilde işler:

En üst seviyede yönlendir aşamasında, bilgi güvenliği ile ilgili direktifler (stratejiler) belirlenir, söz konusu stratejiler bir alt seviyedeki yönetim tabakasına girdi olarak verilir. Taktik seviyede söz konusu direktifler politika

ve kurumsal standart haline getirilir. Alt seviyedeki yöneticiler ise bu politika ve standartlara göre prosedürleri hazırlarlar. Bilgi güvenliği faaliyetleri hazırlanmış olan prosedürlere göre gerçekleştirilir.

Kontrol etme aşamasında ise operasyonel seviyede işlemlerin prosedürlere göre yapılıp yapılmadığı alt seviye yöneticiler tarafından kontrol edilir. Taktik seviyede, bir alt seviyedeki prosedürlerin politika ve standartlara uyumluluğu orta seviye yönetim tarafından kontrol edilir. Stratejik seviyede ise ilgili direktiflerin ne derece yerine getirildiği ve politikaların stratejilerle uyumu üst düzey yönetici tarafından kontrol edilir (Karabacak, 2008).

Zamanla bilgi güvenliği konusunda daha hassas hale gelecek olan üst yönetim, konu ile ilgili etkinliğini artıracaktır. Bu durumda Posthumusa ve Solms (2005)'a göre CEO, sorumluluğundaki riskler hakkında gerekli direktifleri verebilmek için alt seviyedeki bir birimin kendisine bilgilendirme yapmasına ihyiyaç duyacak ve muhtemelen bu birim, bilgi güvenliği konusunda denetim yapan denetçilerden oluşacaktır.

## 3.2 Bilgi Güvenliği Yönetimi Birimi Oluşturulması

Üst yönetimin bilgi güvenliği konusundaki kararlığı bu alanda faaliyet gösterecek bir birimle desteklenmelidir. İlgili bilgi güvenliği faaliyetlerini yürütmek üzere bizzat üst yönetim tarafından oluşturulmasına karar verilen ve bu konuda yetkilendirilen, BGYS'nin kurulması ve yönetilmesini üstlenecek bir birim oluşturulmalıdır. Birim yöneticisi ve üyeleri, BGY konusunda eğitimli/deneyimli olmalıdır. Çünkü bu birim, risk yönetimi, politika oluşturma, güvenlik prosedürlerinin hazırlanması ve uygun kontrollerin seçilerek uygulanması gibi çalışmaları yapacaktır. Gerektiğinde bu birimin, konusunda uzman danışmanlardan görüş ve öneri alması sağlanmalıdır (TBD Kamu, 2008, Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin Uygulanmasında ISO/IEC 27001:2005).

Kurulacak Bilgi Güvenliği Yönetimi (BGY) birimi içerisinde; birim yöneticisi, grup yöneticileri ve uzmanların yer almasının yerinde olacağı değerlendirilmiştir.

Söz konusu uzmanlar farklı birimlerden seçilmiş ve gerekli eğitimleri almış tam zamanlı BGY birimi çalışanı olabileceği gibi, başka bir birimde çalışarak yarı zamanlı olarak BGY birimine katkıda bulunan personelden oluşabilecektir. Ancak BGY birimi içerisinde belli sayıda tam zamanlı çalışan olması bir zorunluluktur.

BGYS'nin etkin ve verimli bir şekilde sürdürülebilmesi için BGY biriminde görev tanımlarının yapılması önem arz etmektedir. Bu kapsamda BGY birimi yöneticisinin görevlerini aşağıdaki gibi sıralamak mümkündür:

1. BGYS hazırlık, işletme, süreklilik ve iyileştirme faaliyetlerinin yönetimi,
2. BGYS politikası ve prosedürlerinin incelenmesi ve onaylanması,
3. Kayıt sisteminin kurulması ve BGYS'nin gerektirdiği kayıtların incelenmesi ve onaylanması,
4. Değişim ve konfigürasyon yönetimi faaliyetlerinin onaylanmması,
5. Risk yönetimi faaliyetlerinin sürekli ve düzgün yapılmasının sağlanması,
6. Kontrollerin etkinliğinin ölçülmesi,
7. BGYS-YGG toplantılarına katılım sağlanması,
8. Gerektiğinde seçilen kontroller ve kabul edilecek risklerle ilgili olarak yönetimin onayının alınması.

BGY grup liderlerinin görevleri ise aşağıdaki hususlardan oluşmaktadır:

1. BGYS politikası ve prosedürlerinin hazırlanması, revizyonları,
2. Kayıt sisteminin kurularak BGYS'nin gerektirdiği kayıtların tutulması,

3. Risk yönetimi faaliyetlerinin sürekli ve düzgün yapılmasını sağlamak için takım üyelerinin görevlendirilmesi ve BGY birim yöneticisine onaylatılması,
4. Tehdit ve zayıflık veritabanının güncelliği sağlanarak, değişen riskin yönetilmesi,
5. Denetimlerin planlanması ve uygulamalarının yönetilmesi,
6. Değişim ve konfigürasyon yönetimi faaliyetlerinin sağlanması,
7. Acil durum müdahale ekibine liderlik edilmesi,
8. BGYS-YGG toplantılarının organize edilmesi.

Son olarak, BGY uzmanlarının görevlerini aşağıdaki gibi sayabiliriz:

1. BGY birimi yöneticisi ve BGY grup liderinin vereceği görevlerin yerine getirilmesi,
2. BGYS iç tetkiklerinde görev alınması,
3. BGYS kontrol uygulamalarının hayata geçirilmesi ve izlenmesi,
4. Acil durum ekibine katılım sağlanması,
5. Planlama ve raporlama için BGY birimi grup liderlerine ve yöneticisine yardımcı olunması. (Taşkın, 2011)

### 3.3 BGYS Politikası

Model BGYS'de bilgi güvenliği politikasının, genel bir Bilgi Güvenliği Politikası ve belirli alanlara ait maksadı içeren kısa alt politikalardan (sorumluluk politikası, erişim kontrol politikası, risk yönetimi politikası, elektronik veri transferi politikası, kullanıcı politikası, e-posta kullanım politikası vb.) oluşması ve uygulamaları tanımlayan prosedür ve talimatlarla tamamlanması önerilmektedir.

Scott (2001)'e göre Bilgi Güvenliği Politikası, temel ilkeleri barındıran en üst düzey doküman olduğundan her seviyedeki ayrıntılı politikalara değinmek yerine onlara atıfta bulunabilir.

Bilgi Güvenliği Politikası işletmede bilgi güvenliğine yön veren temel dokümandır. Bu nedenle işletmenin tüm çalışanlarınca ve hatta üçüncü taraf iş ortaklarınca erişilebilen ve bilinen bir doküman olmalıdır. Bu amaçla elektronik ortamda kurumsal internet sayfasında ve dokümante edilmiş olarak her birim içerisinde erişilebilir olmalıdır.

Politikanın, çok uzun olması halinde okunmasında ihmaller yaşanabileceğinden kısa olmasında fayda vardır.

Ayrıca politika, tüm kullanıcılar tarafından anlaşılır ve net olmalıdır; teknolojik terimlerin kullanılmasından da mümkün olduğunca kaçınılmalıdır. Bilgi güvenliği politikasının işletme çalışanları tarafından uygulanması beklendiğinden gerçekçi olması önemlidir. Uygulanması zor veya imkânsız ifadelere yer verilmemelidir.

Model önerimizde, politika oluştururken ISO/IEC 27001 standardı A.5.1 maddesinde yer alan Bilgi Güvenliği Politikası ile ilgili BGYS Kontrolleri Gerçekleştirilmesi ve Denetlenmesi Kılavuzu'nda belirtilen aşağıdaki hususların yer alması gerektiği değerlendirilmekte ve mobil işletmeciler için örnekler oluşturulmaktadır:

- Bilgi güvenliğinin tanımı, genel kapsamı ve amacı olmalıdır.

Tanım, kapsam ve amaç önerileri:

| |
|---|
| Bu politikada yer alan bilgi güvenliği,<br><br>bilgi varlıklarını ve ilgili IT sistemlerini içerden ve dışarıdan gelebilecek kasıtlı veya kasıtsız tüm tehditlere karşı koruyarak bilgilerin gizlilik, bütünlük ve kullanılabilirliğini devam ettirmektir. |

Kapsam:

Bilgi işlem altyapısını kullanmakta olan tüm birim çalışanları, iş ortakları, üçüncü taraflar, hizmet-ekipman sağlayıcıları ve belirli durumlarda müşteriler bilgi güvenliği politikasına uymakla sorumludur.

Amaç:

Kurumun temel ve destekleyici iş faaliyetlerinin zarar görmemesi için yaşanması muhtemel bilgi güvenliği olaylarını önlemek veya etkilerini en aza indirmek, ilgili mevzuat ve sözleşme gereklerine uymak, elektronik haberleşme hizmetlerini iş sürekliliği çerçevesinde yönetmek ve bilgi güvenliği ile ilgili güvenlik hedeflerini tanımlamaktır.

- Yönetim desteğini politikada belirtmelidir. Bu konuya Bölüm 3.1.'de değinilmiştir.
- Görev ve sorumluluklar belirtilmelidir. Örnek olarak:

Politika ve değişiklikler CEO tarafından imzalanarak sahiplenilir ve geçerli kılınır.

BGY birim görevlisi, politikayı sürdürmek ve uygulanmasında rehberlik yapmakla yükümlüdür.

Tüm birim sorumluları politikanın kendi birimlerinde uygulanmasından sorumludur.

Tüm çalışanlar, politikaya uymakla ve bilgi güvenliği olaylarını raporlamakla yükümlüdür.

Bilgi güvenliği gözden geçirme komitesi politikayı periyodik olarak (3 ya da 6 ay) gözden geçirmek, onaylamak, BGYS ile ilgili stratejik kararları almakla yükümlüdür.

- Kontrol hedefleri ve kontrollerin seçimi için risk değerlendirmesi ve risk yönetimini de içeren bir çerçevenin ortaya konulması gereklidir. Örnek risk yönetim çerçevesi:

Risk Yönetim Çerçevesi:

Bilgi güvenliği riskleri, tehdidin yapabileceği etkiler ve olasılığı ile birlikte tanımlanır. Risk yönetim çerçevesi, bilgi güvenliği risklerinin tanımlanmasını, değerlendirilmesini, işlenmesini kapsar. Risk değerlendirmesi, uygulanabilirlik bildirgesi ve risk işleme planı, bilgi güvenliği risklerinin nasıl kontrol edildiğini tanımlar.

Uygun kontroller uygulanarak risk düzeyleri iyileştirilmeli ve bilginin gizliliği, bütünlüğü ve erişimi yeterli kontroller ile devam ettirilmelidir.

- Güvenlik politikaları, ilkeleri, standartları ve uyum gereksinimlerinden bahsedilmelidir. Örnek olarak:

- Her bilgi varlığı gizlilik derecesine göre sınıflandırılmalıdır. (Ör: G,G1,G2,G3)
- Kritiklik düzeylerine göre işlenen her bilgi yedeklemelidir.
- Hassas bilgiler kişisel bilgisayarlar yerine merkezi sunucuda tutulmalıdır.
- Kuruluş veritabanlarının uyumluluğu ve devamlılığı devam ettirilmelidir.
- Yetkisiz erişimi önlemek için tüm bilgi işlem cihazlarında ve ofislerde kullanıcılar belirlenmeli ve bu varlıklar korunmalıdır.
- Gizlilik derecesi yüksek bilgiler, şifreleme veya kriptolama yapılmadan dışarı çıkarılmamalıdır.
- Bilgi işleme süreçleri dokümante edilmiş prosedürlere göre yürütülmelidir.
- Bilgi güvenliği ihlal olayları raporlanmalı ve Bilgi Güvenliği Birimi'ne bildirilmeli, bu ihlalleri engelleyecek önlemleri alınmalıdır.

- Bilgi güvenliği ile ilgili tüm görev ve sorumlulukların tanımı:

> Çalışanlar kuruluş bilgi değerlerini sadece iş amaçlı olarak kullanırlar. Tüm çalışanlar ve BGYS de tanımlanan dış taraflar, bu politikaya ve bu politikayı uygulayan BGYS politika, prosedür ve talimatlarına uymakla yükümlüdür.
>
> Birimlerin güvenlik sorumlularından oluşan Bilgi Güvenliği Koordinasyon Grubu, BGYS altyapısını desteklemek ve işleyişini devam ettirmekle sorumludur.

- Politikanın ihlali durumunda yapılacak işlemler ve yaptırımlar belirtilmelidir. Örnek olarak:

> Bu politikada yer alan hususların ihlal edildiği durumlar, hemen yetkili bilgi güvenliği personeline haber verilmelidir.
>
> Bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması halinde, ihlalin niteliği ve ciddiyeti nispetinde yönetim, yaptırım uygulama hakkına sahiptir.

- Diğer ayrıntılı politikalar ve belirli bilgi sistemleri için prosedürler veya kullanıcıların uyması gereken kurallar gibi politikayı destekleyen dokümanlara atıflar yapılmalıdır.

Bilgi güvenliği politikası tek başına bir doküman değildir. Bilgi güvenliği amaçlarının gerçekleşmesi için hazırlanan başka ilgili politikalarla, standartlarla, prosedür ve talimatlarla desteklenecektir. Okuyucunun zihninde tam bir bilgi güvenliği resmi oluşturabilmesini sağlamak için bu dokümanlara da işaret edilmelidir. Ayrıca, kanun, mevzuat vb. ile belirtilmiş, kurumun uygulaması gereken belirli kontrol ve önlemler varsa, bu kontrol ve önlemlere politikada referans verilir (Öztürk, 2008). Örnek olarak:

Bilgi Güvenliği Olay Yönetimi Prosedürleri, İş Sürekliliği ve Acil Durum Planları, Veri Yedekleme Prosedürleri, Doğal Afet Durumu Prosedürleri, Güvenlik TehditleriniKarşılama Prosedürü, Sistemlere Erişim Kontrolü, İhbar Değerlendirme Prosedürü, Şebeke Güvenliği İzleme Prosedürleri, Soruşturma ve İzleme Prosedürü, Acil Durum Tahliye Prosedürü bu politikayı destekler. Bu alanlarla ilgili işleyiş özel olarak dokümante edilmiş politika ve prosedürlerle tanımlanır.

Bilgi güvenliği politikasında revizyon bilgileri de yer almalıdır. Onay kısmında ise kimin tarafından hazırlandığı, kimin tarafından onaylandığı isimleri ile belirtilmeli ve imzalanmalıdır. CEO'nun imzasının olmadığı doküman geçerlilik kazanamaz. Bu nedenle doküman üzerinde CEO imza ve yetki/izini (authorisation) olmalıdır.

### 3.4 Risk Değerlendirme

İşletmenin riskleri kabul etme kriterleri ve kabul edilebilir risk seviyesinin neler olduğu risk değerlendirme yaklaşımı ile netleştirilir. Ancak riskleri değerlendirmeden önce varlıkların neler olduğu iyi bilinmelidir. Çünkü aslında riskler; bilgi varlıklarının gizlilik, bütünlük ve kullanılabilirliğine olan tehditler ile ortaya çıkmaktadır.

**Gizlilik:** Bilginin içeriğinin görüntülenmesinin, sadece bilgiyi/veriyi görüntülemeye izin verilen kişilerin erişimi ile kısıtlanmasıdır. (Ör: Şifreli e-posta gönderimi ile e-postanın ele geçmesi halinde dahi yetkisiz kişilerin e-postaları okuması engellenebilir)

**Bütünlük:** Bilginin yetkisiz veya yanlışlıkla değiştirilmesinin, silinmesinin veya eklemeler çıkarmalar yapılmasının tespit edilebilmesi ve tespit edilebilirliğin garanti altına alınmasıdır. (Ör: Veri tabanında saklanan verilerin özet bilgileri ile birlikte saklanması, dijital imza)

**Erişilebilirlik/Kullanılabilirlik:** Varlığın ihtiyaç duyulduğu her an kullanıma hazır olmasıdır. Diğer bir ifade ile, sistemlerin sürekli hizmet verebilir halde bulunması ve sistemlerdeki bilginin kaybolmaması ve sürekli erişilebilir olmasıdır. (Ör: Sunucuların güç hattı dalgalanmalarından ve güç kesintilerinden etkilenmemesi için kesintisiz güç kaynağı ve şasilerinde yedekli güç kaynağı kullanımı) (Koç, 2008).

Hangi tehditlerin ne gibi riskler taşıdığını analiz edebilmek için bilgi varlıklarını da içeren tüm varlıkların envanterinin çıkarılması ve sınıflandırılarak değerlendirilmesi gerekmektedir. Mobil işletmeciler için önerilen envanter tablosu aşağıda verilmiştir.

Tablo 3.1. Mobil işletmeci varlık envanteri tablosu

| Varlık Kodu | Varlık Grubu | Varlık | Varlık Tanımı | Varlık Türü | Varlık Pozisyonu | Varlık Sorumlusu | Gizlilik Değeri | Bütünlük Değeri | Erişilebilirlik Değeri | Varlık Değeri | Açıklamalar |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| ... | | | | | | | | | | | |

Tablo 3.1.'de yer alan ifadelere ilişkin açıklamalar aşağıda verilmiştir:

**Varlık Kodu:** Her varlık sıraya göre numaralandırılır. Böylece varlıklar özelleşerek birbirinden ayırt edilebilir.

**Varlık grubu:** Varlık envanterinin anlaşılabilmesini kolaylaştırmak için benzer işler için kullanılan varlıklar, aynı grupta yer alacak şekilde gruplandırılabilir. (Ör: personel, doküman, son kullanıcı cihazları, çağrı merkezi sunucusu vb.)

**Varlık:** Varlık adıdır.(Ör: BTS, Bayblon 6, masaüstü bilgisayar )

**Varlık Tanımı:** Varlığın varsa marka modelinin yoksa amacının yazıldığı kısımdır. (Ör: Alcatel134, Nokia45, personel yönetimi )

**Varlık Türü:** Varlığın niteliğini gösterir. (Ör: Bilgi, yazılım, donanım, hizmet, personel, fiziksel ortam)

**Varlık Pozisyonu:** Varlığın bulunduğu fiziksel yeri belirtir.(Ör: Kartal/İstanbul, Samsun satış ofisi)

**Varlık Sorumlusu:** Varlık sahibi, tanımlanan rol ve sorumluluklara göre belirlenir. Bölüm/birim sorumlusu ya da doğrudan isim olarak belirlenebilir. (Ör: Şebeke planlama başkanı, Şebeke gözetim müdürü, Haluk KOÇ)

**Gizlilik Değeri:** Varlığın yetkisiz kişilerce erişilmesi sonucu olabilecek zararı belirtir. (Ör: 0/1/2/3, düşük/orta/yüksek, s/se/sec/secr/secre/secret)

**Bütünlük Değeri:**Varlığın bütünlüğünün bozulması sonucunda doğacak zararı belirtir. (Ör: 1/2/3,düşük/orta/yüksek,)

**Erişilebilirlik Değeri:** Varlığın erişilebilirlik açısından önemini belirtir. (Ör: 1/2/3,düşük/orta/yüksek,)

**Varlık değeri:** Varlığa değer atama kriterleri belirlendikten sonra varlıkların değerlerinin atanması gereklidir. Bilgi varlıkları için güvenliğin üç temel ilkesinin (gizlilik, bütünlük, erişilebilirlik) uygulanması çok büyük bir sorun teşkil etmemektedir. Fakat envanterde bulunan bir donanım varlığının gizliliği veya bütünlüğünü değerlendirmek çok daha zor bir eylemdir. Bu zorluğun önüne geçmek maksadıyla varlık değerlendirmesine (derecelendirmesine) bilgi ve süreç varlıklarından başlamakta fayda vardır.

İşletmenin varlıklarına değer biçilmesi risk analizi için temel bir adımdır. Tüm varlıklar belirlendikten sonra ikinci adım olarak, bir varlık için değer atama kriterinin belirlenmesi gerekir. Varlık çeşitleri düşünülecek olursa, derecelendirme için tipik örnek olarak şunlar verilebilir: İhmal Edilebilir, Çok Düşük, Düşük, Orta, Yüksek, Çok Yüksek, Kritik. Kaç derecelendirme

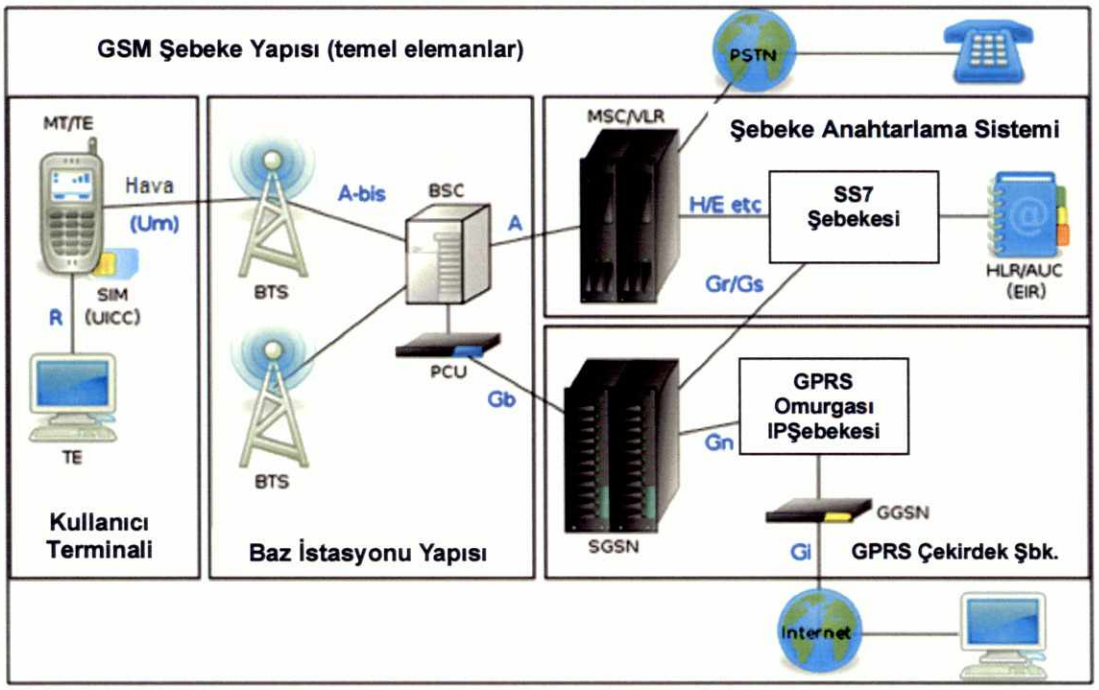
seviyesi kullanılacağı organizasyonun güvenlik ihtiyaçlarına bağlıdır. Çok fazla derecelendirme ihtiyacı olan bir mobil işletmeci için 4-5 derecelendirme kullanılabilir. (Ör: 0/1/2/3,A1/A2/A3/A4, Aleni / Şirket içi / Sınırlı / Gizli / Hayati) Önemli olan nokta bir varlığa atanacak derecenin kriterinin belli belirsiz ifadeler kullanılmadan yazılabilmesidir. Yani bir varlık değeri için "düşük" denildiğinde bu tanımın ne anlama geldiği net olarak anlaşılmalıdır.

**Açıklamalar:** İlave edilmesinde fayda görülen bilgiler bu kısma yazılabilir.

Bu genel bilgilerden sonra, risk değerlendirmesine konu olan ve genel şebeke yapısı Şekil 3.2'de verilen mobil haberleşme şebekesi içerisinde yer alan varlıklar genel hatları ile ele alınacaktır.

Bir mobil işletmecinin tüm varlıklarını bu çalışma içerisinde listelemek ve anlatmak mümkün olamayacağından sadece önemli bazı varlıklara değinilecek ve bu varlıklar için örnek envanter tablosu doldurulacaktır.

Şekil 3.2. Mobil haberleşme şebeke yapısı




Kaynak:wapedia.mobi

Şekil 3.2'de basit olarak temsil edilen mobil haberleşme şebekesinin, varlık envanteri oluştururken dört bölüm altında ele alınması gerektiği düşünülmektedir:

- Radyo Erişim Şebekesi (Radio Access Network-RAN)
- Transmisyon Şebekesi
- Ağ Anahtarlama Alt Sistemi (Network Switching Subsystem-NSS)
- Operasyon ve Destek Sistemleri

Bir mobil işletmecinin şebeke dışında da varlıkları vardır. Model önerisinde şebeke dışı varlıklar da yine dört bölüm altında ele alınmaktadır:

- Bilgi Teknolojileri (Information Technologies-IT) Varlıkları
- Katma Değerli Servisler (Value Added Services-VAS)
- Çağrı Merkezleri
- Kişiye Tahsisli Varlıklar

İşletmecinin sahip olduğu insan kaynağı varlığı ise her bölüm için kendi altında değerlendirilmekte olup ayrı bir varlık grubu olarak sayılmamıştır.

Burada üzerinde durulması gereken bir diğer önemli husus da farklı varlık grupları için farklı riskler söz konusu olduğundan alınacak tedbirlerde de farklılıklar olabileceğidir. Örneğin şebeke ile doğrudan ilgili varlıklardan olan radyo erişim şebekesi ile transmisyon şebekesi sahaya yaygın olduğundan fiziksel erişimi önleyici tedbirler, yeterli çözüm olamamaktadır. Bu nedenle bu varlıklar için alınacak tedbirler içerisinde kriptolama, algoritma kulanımı gibi yetkisiz fiziksel erişim olsa bile bilgiyi koruyucu tedbirler ön plana çıkmaktadır. Şebeke dışı diğer varlıklar için ise daha çok şifre kullanımı ve yönetimi ile fiziksel güvenlik önlemleri öne çıkmaktadır.

### 3.4.1 Radyo Erişim Şebekesi (RAN)

Radyo erişim şebekesi baz istasyonu alt sistemleri olarak da bilinmekte olup bu şebekede yer alan bazı önemli varlıklar aşağıda açıklanmıştır

**Baz Alıcı-Verici İstasyonu (Base Transceiver Station-BTS):** Mobil telefonların GSM şebekesi ile kablosuz bağlantısını kuran, halk deyimi ile baz istasyonu diye tabir edilen ekipmanlardır. Radyo sinyallerini gönderme ve almaya yarayan antenler ihtiva eder.

**Baz İstasyonu Denetleyicisi (Base Station Controller-BSC):** BTS'lerin arkasındaki akıllı ekipmandır. 10 ile 100 arası BTS'yi kontrol edebilir. Cep telefonlarından alınan sinyalleri ölçerek ve takip ederek hangi BTS'nin devreye girmesi gerektiğine karar verir.

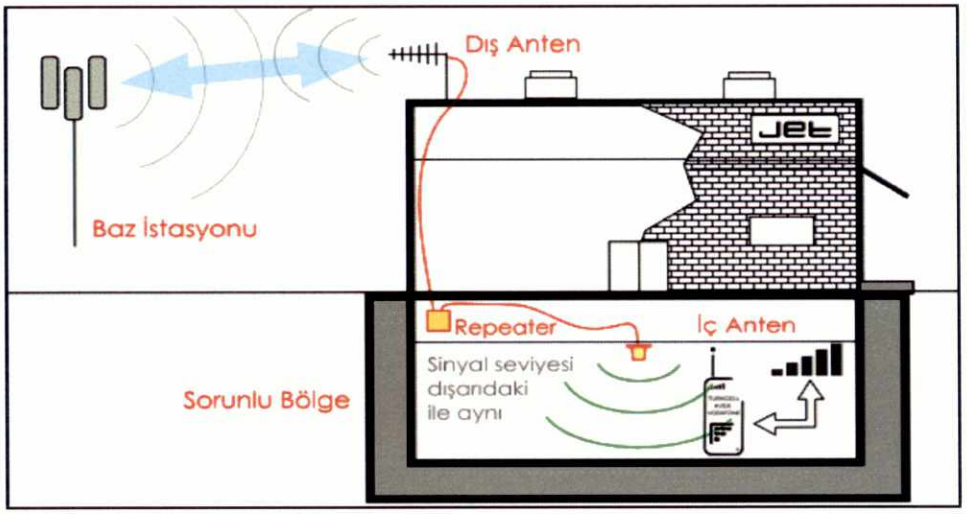
**Node-B:** GSM şebekesindeki BTS'lerin 3N şebekesindeki muadilidir.

**Telsiz Şebeke Denetleyicisi (Radio Network Controller-RNC) :** Bir anlamda GSM şebekesindeki BSC'lerin 3N şebekesindeki karşılığıdır. Kendine bağlı Node-B'lerin idaresi RNC'dedir.

**Personel:** RAN planlama müdürü, mühendisi v.b.

**Tekrarlayıcı (repeater):** Bu sistemin amacı, uygun bir bölgeden bulunduğunuz bölgeye ihtiyacınız olan frekansı aktarmaktır. Örnek olarak bu sistem, cep telefonu şebekesinin kuvvetli olduğu bir bölgeye sistemin dış antenini yerleştirmek suretiyle buradaki ortamı, şebekenin zayıf olduğu bir binanın bodrum katına aktarabilir. Şekil 3.3'te temsili gösterimi ve işleyişi yer almaktadır.

Şekil 3.3. Frekans tekrarlayıcı, repeater




Kaynak:Jet, 2010

Yukarıda açıklamaları yer alan RAN varlıkları, Tablo 3.1.'deki örnek varlık envanterine Tablo 3.2.'deki[1] gibi işlenebilir.

[1] Tabloda verilen markalara ait modeller, kişiler ve pozisyonlar farazidir.

Tablo 3.2. Radyo erişim şebekesi varlıklarının örnek varlık envanter tablosuna işlenmesi

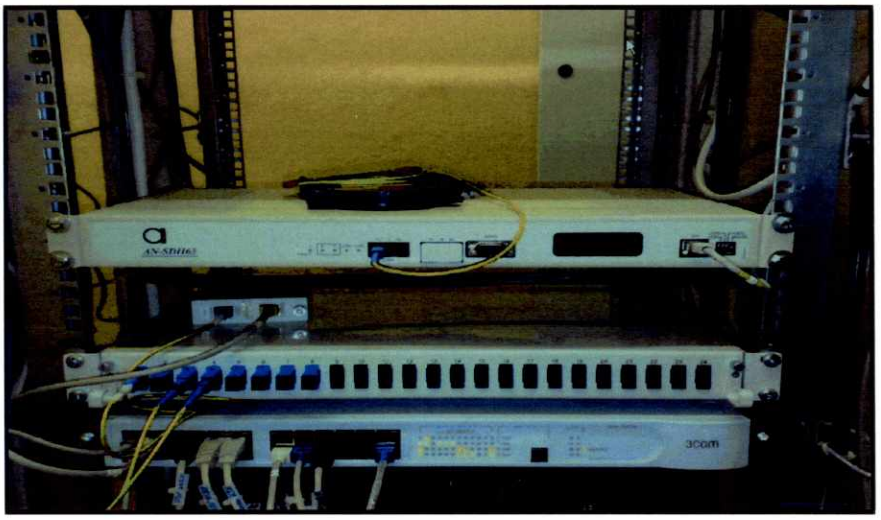
| Varlık Kodu | Varlık Grubu | Varlık | Varlık Tanımı | Varlık Türü (Bilgi, yazılım, donanım, hizmet, personel) | Varlık Pozisyonu | Varlık Sorumlusu | Gizlilik Değeri (Düşük, Orta, Yüksek) | Bütünlük Değeri (Düşük, Orta, Yüksek) | Erişilebilirlik Değeri (Düşük, Orta, Yüksek) | Varlık Değeri (1,2,3,4,5) |
|---|---|---|---|---|---|---|---|---|---|---|
| R1041 | RAN | 1041 nolu BSC | Huawei N50-34 | Donanım | Pazar/Rize | Samsun Bölge Şebeke Yönetim Amiri | Yüksek | Yüksek | Orta | 4 |
| R33 | RAN | 33 nolu BTS | Siemens C2300 | Donanım | Merkez/ Rize | Samsun Bölge Şebeke Yönetim Amiri | Yüksek | Yüksek | Yüksek | 5 |
| R554 | RAN | 554 nolu Node-B | Huawei K33-25 | Donanım | Beştepe/ Trabzon | Samsun Bölge Şebeke Yönetim Amiri | Yüksek | Yüksek | Orta | 4 |
| R25 | RAN | 25 nolu RNC | Siemens C3500 | Donanım | Merkez / Trabzon | Samsun Bölge Şebeke Yönetim Amiri | Yüksek | Yüksek | Yüksek | 5 |
| R63 | RAN | 63 nolu Repeaters | Alcatel R3 | Donanım | Matbaacılar Sitesi/ Topkapı | İstanbul Bölge Şebeke Yönetim Amiri | Yüksek | Yüksek | Orta | 4 |
| R501 | RAN | Şebeke Planlama Mühendisi | Şebeke Planlama | Personel | Kartal/İST. | Şebeke Planlama Müdürü | Orta | Orta | Orta | 3 |

### 3.4.2 Transmisyon Şebekesi

Optik ve radyolink transmisyon ağırlıklı taşıyıcı ağlardan oluşan bu şebekede yer alan bazı önemli varlıklar şunlardır:

**Eş Zamanlı Sayısal Sıradüzeni (Synchronous Digital Hiyerarchy-SDH):** Farklı kapasitelerde sayısal sinyaller taşıyabilen, yüksek hızlı uluslararası bir transmisyon sistemidir. SDH, fiber optik ortamının yüksek band genişliği ve güvenilirlik avantajlarından yararlanmak için fiber optik transmisyon linkleri ve radyolinkler kullanır. SDH ekipmanı örneği Şekil 3.4'te verilmiştir.

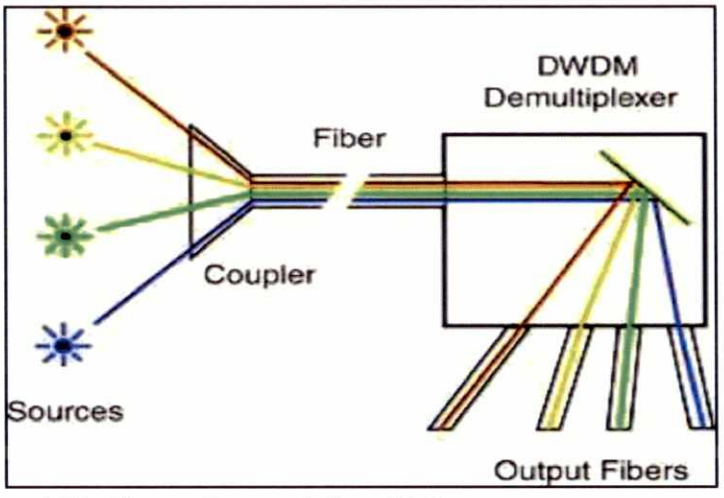
Şekil 3.4. AN-SDH63 bağlantı ekipmanı



Kaynak: Ad-Net technology, 2005

**Yoğun Dalga Bölmeli Çoğullama (Dense Wavelength Division Multiplexing-DWDM):** Tek bir fiber üzerinde farklı dalga boylarında birden fazla yüksek hızlı devre taşıyabilen optik transmisyon teçhizatlarıdır (netmon.com.tr, 2008). Farklı dalga boylarında aldığı dataları algılayıp ayırt eden DWDM optik data iletim mantığı Şekil 3.5'te görülmektedir. Buradaki fayda tek fiber hattı ile farklı data kanalları oluşturulabilmesidir.

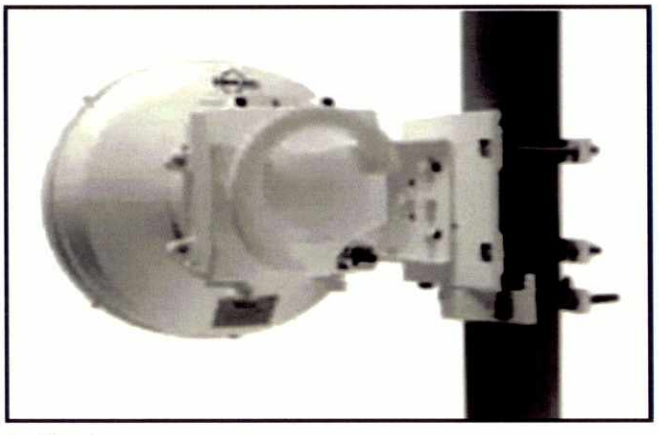
Şekil 3.5. DWDM çalışma prensibi




Kaynak:The fiber optic association, 2003

**Radyolink:** İki baz istasyonu sahası arasında karasal kablo bağlantısı kurmaksızın radyo dalgalarıyla hava arayüzünün belli frekanslarda kullanılması sayesinde gerçekleştirilen iletişimde kullanılan bağlantı sistemi elemanlarıdır. Şekil 3.6'da bir radyolink cihazı örneği verilmiştir.

Şekil 3.6. 18 GHz Radyolink teçhizatı



Kaynak: Karel

Yukarıda açıklamaları yer alan transmisyon varlıkları, Tablo 3.1. deki örnek varlık envanterine Tablo 3.3'teki gibi işlenebilir.

Tablo 3.3.Transmisyon şebekesi varlıklarının örnek varlık envanter tablosuna işlenmesi

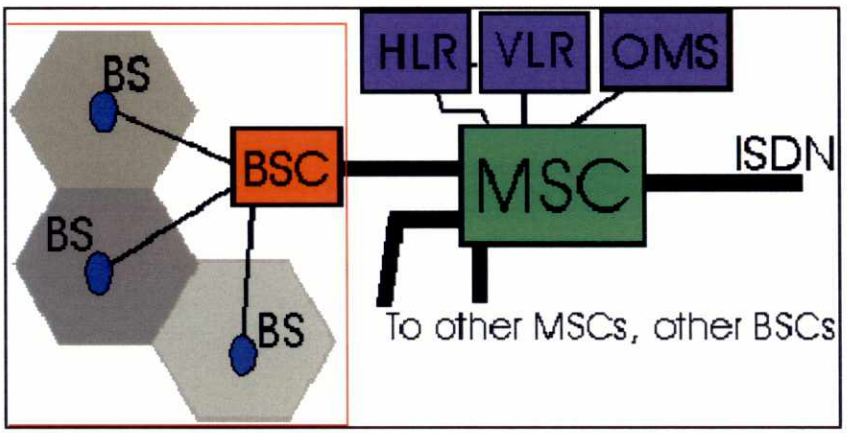
| Varlık Kodu | Varlık Grubu | Varlık | Varlık Tanımı | Varlık Türü (Bilgi, yazılım, donanım, hizmet, personel) | Varlık Pozisyonu | Varlık Sorumlusu | Gizlilik Değeri (Düşük, Orta, Yüksek) | Bütünlük Değeri (Düşük, Orta, Yüksek) | Erişilebilirlik Değeri (Düşük, Orta, Yüksek) | Varlık Değeri (1,2,3,4,5) |
|---|---|---|---|---|---|---|---|---|---|---|
| T122 | Transmisyon | SDH | ALCATEL 1662 | Donanım | Kartal/İst. | Cem KARA | Yüksek | Orta | Yüksek | 5 |
| T433 | Transmisyon | Radyolink | NEC-RL45 | Donanım | Harput/ Elazığ | Akif Uyar | Yüksek | Orta | Yüksek | 5 |
| T67 | Transmisyon | DWDM | HUAWEi OPTiX OSN 6800 | Donanım | Elazığ | Akif UYAR | Yüksek | Orta | Yüksek | 5 |

### 3.4.3 Ağ Anahtarlama Alt Sistemi (NSS)

GSM şebekesinin anahtarlama fonksiyonlarını yerine getirir. Abonenin şebeke içinde veya diğer şebekelerle (PSTN ya da diğer GSM şebekeleri) olan bağlantısı NSS üzerinden anahtarlanır. Ayrıca abonelik işlemleri ve abonenin hareketliliği için gerekli veriler NSS'te bulunmaktadır.

**Mobil Anahtarlama Merkezi (Mobil Switching Center-MSC):** "Santral" olarak da tabir edilen bu ekipman şebeke içinde ve diğer şebekelerle olan tüm anahtarlama fonksiyonlarını yerine getirir. BSC'ler MSC'ye bağlıdır. Şekil 3.7'de şebeke anahtarlama sistemi elemanları arasındaki ilişki gösterilmiştir (Atasoy, 2006).

Şekil 3.7 Şebeke anahtarlama sistemi elemanları arasındaki ilişki




Kaynak:Jean-Poul Linnartz, 2009

**Mobil Anahtarlama Merkezi Geçişi (Gateway Mobile Switching Center-GWMSC):** "Geçiş Santralı" olarak da tabir edilen bu ekipman MSC'de abone bilgilerinin tutulduğu veri tabanından gerekli abone bilgilerini sağlar. Diğer şebekelerden gelen çağrılar önce GWMSC'ye oradan MSC'ye bağlanır (Atasoy, 2006).

**Abone Bilgileri Merkezi Veri Sistemi (Home Location Register-HLR):** Abone kayıtlarının yapıldığı ve saklandığı kütük dosyalarıdır. Abonelere verilen telefon numaraları HLR'a kaydedilen numaralardır. Bu numaralar tahsis edildiğinde aboneye ait kimlik bilgisi, ücret tarifeleri, kısıtlamalar ve kullanılacak servisler hakkında bilgiler bu dosyalara kaydedilir. Böylece abone şebekede tanımlanmış olmaktadır. Bu özelliğiyle HLR şebekenin ana ekipmanı gibidir.

**Abone Bilgileri Geçici Veri Sistemi (Visitor Location Register-VLR):** VLR aboneye ait aktif işlemleri gerçekleştirmede kullanılan geçici kütüklerdir. Yapı olarak HLR'nin kopyalarıdır. Konuşmalar esnasında abone kayıtlarının sabit dosyalar halinde tutulduğu HLR yerine VLR'ler kullanılarak şebeke sinyalleşme yükü dengede tutulur ve şebekenin performansının yüksek olması sağlanır (Wifi-Turk.com, 2009)

Yukarıda açıklamaları yer alan şebeke anahtarlama sistemi varlıkları, Tablo 3.1. deki örnek varlık envanterine Tablo 3.4. deki gibi işlenebilir.

Tablo 3.4.Şebeke anahtarlama sistemi varlıklarının örnek varlık envanter tablosunaişlenmesi

| Varlık Kodu | Varlık Grubu | Varlık | Varlık Tanımı | Varlık Türü | Varlık Pozisyonu | Varlık Sorumlusu | Gizlilik Değeri | Bütünlük Değeri | Erişilebilirlik Değeri | Varlık Değeri (1,2,3,4,5) |
|---|---|---|---|---|---|---|---|---|---|---|
| A35 | Anahtarlama | MSC | Alcatel-Lucent 5600 | Donanım | Ankara | Musa KOÇ | Orta | Orta | Yüksek | 4 |
| A21 | Anahtarlama | GWMSC | Alcatel-Lucent 7270 | Donanım | Ankara | Musa KOÇ | Orta | Orta | Yüksek | 4 |
| A3 | Anahtarlama | HLR | Siemens R13 | Donanım | Ankara | Ahmet BİR | Yüksek | Yüksek | Yüksek | 5 |
| A67 | Anahtarlama | VLR | Siemens D900 | Donanım | Kartal/İST. | Can ATAK | Yüksek | Yüksek | Orta | 5 |

### 3.4.4 IT Varlıkları

Yedekleme sistemleri, izleme sistemleri, finansal bilgisayar programlarından, alan adı sistemi, elektronik posta sunucuları, işletim sistemleri, program lisansları, internet üzerinden satış sistemlerine kadar birçok sistem ve bunların birbirleriyle olan dolaylı veya dolaysız bağlantılarının tümü bilgi alışverişi sağlayan IT varlıkları arasında sayılabilir.

Zamanımızda, her ne alanda faaliyet gösterirse göstersin her kuruluş, IT varlıklarına sahiptir. Ancak haberleşme sektöründeki işletmecilerin faaliyetlerinin büyük bir bölümü IT varlıklarını içermektedir. Bu nedenle mobil işletmeciler için IT varlıkları daha da önemlidir.

Şekil 3.8.IT varlıkları

Kaynak: Wikipedia

Bazı IT varlıkları,Tablo 3.1. deki örnek varlık envanterine Tablo 3.5'teki gibi işlenebilir.

Tablo 3.5. IT varlıklarının örnek varlık envanter tablosuna işlenmesi

| Varlık Kodu | Varlık Türü | Varlık | Varlık Tanımı | Varlık Türü | Varlık Pozisyonu | Varlık Sorumlusu | Gizlilik Değeri | Bütünlük Değeri | Erişilebilirlik Değeri | Varlık Değeri (1,2,3,4,5) |
|---|---|---|---|---|---|---|---|---|---|---|
| IT29 | IT | Backup Tape/mail01, app01 | Mail Services | Donanım | ADANA | Ali KOÇ | Orta | Düşük | Orta | 2 |
| IT33 | IT | Cisco Fabric Manager Server License | Anahtarlama performansı | Yazılım | Kartal/İST. | Cenk KARA | Orta | Orta | Yüksek | 3 |
| IT111 | IT | crdbp2/MNP Applications | Web satışları sunucusu | Yazılım | Kartal/İST. | Metin AL | Yüksek | Yüksek | Orta | 3 |
| IT65 | IT | e-faturalama uygulayıcısı | Ebilling System | Donanım | Kartal/İST. | Metin AL | Yüksek | Yüksek | Yüksek | 5 |
| IT21 | IT | HP tester | IT-System Support - HP Test Server | Donanım | İzmir | Sami PEK | Düşük | Düşük | Düşük | 1 |
| IT78 | IT | Billingquality2 | Fatura Kontrol Sistemi | Donanım | Kartal/İST. | Metin AL | Düşük | Düşük | Düşük | 3 |
| IT135 | IT | DNS | HP Sunucu | Donanım | Ankara | Ali KARA | Yüksek | Yüksek | Yüksek | 5 |
| IT90 | IT | risk1p1/RA | Billing Control System | Yazılım | Kartal/İST. | Metin AL | Düşük | Düşük | Düşük | 3 |
| IT89 | IT | Senior Unix Administrator | IT Systems&Storage Management Personnel | Personel | İzmir | Sami PEK | Düşük | Düşük | Düşük | 2 |
| IT123 | IT | SqlTest | SQL Server | Donanım | Kartal/İST. | Anıl ÖZ | Düşük | Düşük | Düşük | 3 |
| IT55 | IT | BTK-STS | BTK Subscriber tracking System | Donanım | Kartal/İST. | Anıl ÖZ | Yüksek | Yüksek | Yüksek | 4 |

### 3.4.5 Katma Değerli Servisler (VAS)

Mobil işletmeciler tarafından abonelere sunulan temel iletişim servislerinin dışında kalan her türlü içeriği kapsayan çağrı, data servisleri ve uygulamaları mobil VAS olarak anılır. İşletmecilerin temel gelir kaynağı olarak hala ses hizmetleri ön plana çıksa da VAS, giderek azalmakta olan ses gelirlerinin yerini dolduran ve operatörlere kendilerini farklılaştırma şansı veren teknolojiler olarak ortaya çıkmaktadır.

Bu kapsamda, oyun, yarışma, oylama, bilgi, eğlence, müzik içerik servisleri, sohbet servisleri, indirilip yüklenebilir servisler (Java, Symbian benzeri araçlarla geliştirilen ve mobil cihazlara indirilebilen servisler), mobil pazarlama servisleri, interaktif medya servisleri (televizyon, radyo kanalları gibi medya kanalları üzerinden sunulan oylama, yarışma vb. servisler) gibi servisler sunulmaktadır

Çoğunlukla sunucular üzerinden çalışan VAS kısaca birer uygulamadır. Bu uygulamaları mümkün kılan unsurlar yazılım ve donanımdır. Bunları sunabilmek için konuşmayı gerçekleştiren teknolojiye ek olarak ayrı bir teknoloji geliştirmek ve kullanıcının ihtiyacı olan içerikler sunmak gerekmektedir. (mobilsad, 2011)

Bazı VAS varlıkları, Tablo 3.1.'deki örnek varlık envanterine Tablo 3.6.'daki gibi işlenebilir.

Tablo 3.6.Katma değerli servis varlıklarının örnek varlık envanter tablosuna işlenmesi

| Varlık Kodu | Varlık Grubu | Varlık | Varlık Tanımı | Varlık Türü (Bilgi, yazılım, donanım, hizmet, personel) | Varlık Pozisyonu | Varlık Sorumlusu | Gizlilik Değeri (Düşük, Orta, Yüksek) | Bütünlük Değeri (Düşük, Orta, Yüksek) | Erişilebilirlik Değeri (Düşük, Orta, Yüksek) | Varlık Değeri (1,2,3,4,5) |
|---|---|---|---|---|---|---|---|---|---|---|
| KDS24 | KDS | CAGS | Cep telefonlarına ayar gönderen sistem | Donanım | Kartal/İst. | Cem KARA | Yüksek | Yüksek | Orta | 4 |
| KDS125 | KDS | Huawei IVR Sistemi | Prepaid aboneler kredi yükleme/dinleme sistemleri | Donanım | Adana | Akif UYAR | Yüksek | Yüksek | Yüksek | 4 |
| KDS206 | KDS | smsas1 | Kısa mesaj adresleme sistemi | Donanım | Kartal/İst. | Akif UYAR | Yüksek | Yüksek | Orta | 4 |
| KDS227 | KDS | bulksms | Toplu sms sistemi | Donanım | Kartal/İst. | Akif UYAR | Yüksek | Yüksek | Yüksek | 4 |
| KDS208 | KDS | mmscapp1 | mms sistemi | Donanım | Kartal/İst. | Akif UYAR | Yüksek | Yüksek | Yüksek | 4 |
| KDS129 | KDS | websim2 | Proxy gateway | Donanım | Kartal/İst. | Akif UYAR | Yüksek | Yüksek | Orta | 4 |
| KDS30 | KDS | CBC Sistemi | Hücre Bilgi yayın sistemi | Hizmet | Kartal/İst. | Akif UYAR | Yüksek | Yüksek | Orta | 4 |
| KDS311 | KDS | Location software application | Lokasyon bulma sistemi | Hizmet | Kartal/İst. | Akif UYAR | Yüksek | Yüksek | Yüksek | 4 |
| KDS132 | KDS | ussd notify | Arama sonrası bilgilendirme sistemi | Donanım | Kartal/İst. | Akif UYAR | Yüksek | Yüksek | Orta | 4 |

### 3.4.6 Operasyon Destek Sistemleri (ODS)

Operasyon destek sistemleri, şebeke operasyonunun güvenliğini artıran sistemlerdir. Operasyon sırasında yaşanabilecek herhangi bir olumsuz durumda veya acil müdahale gerektiren durumlarda haberleşmenin kesintisiz devam edebilmesi için kullanılan bu sistemler operasyonun ayrılmaz bir parçası sayılırlar. Mobil şebekeler, kesintinin olmaması ve operasyonların doğru gerçekleştirilebilmesi için sürekli izlenir ve test edilir.

Destek sistemleri ile farklı şebekelerin ortak çalışması, hataların uçtan uca tek bir merkezden kontrol edilmesi, arızaların temel sebebinin bulunması, servis seviyesi yönetimi, şebeke içi iş emri yönetimi, performans yönetimi ve raporlama sağlanmaktadır (IŞIK, ÇETİN, 2007).

Çoğunlukla izleme ve test cihazlarından oluşan operasyon destek sistemi varlıklarından bazıları, Tablo 3.1'deki örnek varlık envanterine Tablo 3.7'deki gibi işlenebilir.

Tablo 3.7.Operasyon destek sistemi varlıklarının örnek varlık envanter tablosunaişlenmesi

| Varlık Kodu | Varlık Grubu | Varlık | Varlık Tanımı | Varlık Türü (Bilgi, yazılım, donanım, hizmet, personel) | Varlık Pozisyonu | Varlık Sorumlusu | Gizlilik Değeri (Düşük, Orta, Yüksek) | Bütünlük Değeri (Düşük, Orta, Yüksek) | Erişilebilirlik Değeri (Düşük, Orta, Yüksek) | Varlık Değeri (1,2,3,4,5) |
|---|---|---|---|---|---|---|---|---|---|---|
| ODS13 | ODS | TEMS Automatic SYSTEM | Şebeke yoğunluğuna göre performans ölçer | Donanım | Kartal/İst. | Ref:Sistem Cihazları Yön&İzl | Orta | Orta | Orta | 3 |
| ODS104 | ODS | OSS İzmir gui2 server | NSN Core Network Management System | Donanım | İzmir Bölge Santral Salonu | CN Kalite Ali PEK | Orta | Orta | Orta | 3 |
| ODS215 | ODS | OSS İstanbul omniback server | NSN Core Network Management System | Donanım | Kartal/İst. | Ref:Sistem Cihazları Yön&İzl | Orta | Orta | Orta | 3 |
| ODS116 | ODS | TEKTRONiX Geoprobe 14U | Core network pasif probe | Donanım | Kartal/İst. | Ref:Sistem Cihazları Yön&İzl | Yüksek | Orta | Düşük | 4 |
| ODS170 | ODS | Syserz1 | Motorola OMC-R Server - | Donanım | İzmir Bolge Santral Salonu | CN Kalite Ali PEK | Orta | Orta | Orta | 3 |
| ODS138 | ODS | OracleUfm | Umbrella Fault Management Server-2 | Donanım | Kartal/İst. | Ref:Sistem Cihazları Yön&İzl | Yüksek | Yüksek | Orta | 4 |
| ODS19 | ODS | Core Network/Nmc Monitoring Engineer | İzleme Teknik personeli | Personel | İzmir | Mehmet OK | Orta | Orta | Yüksek | 4 |
| ODS201 | ODS | Netas-trans-12 | Netas Transmission DXX | Donanım | Kartal/İst. | Ref:Sistem Cihazları Yön&İzl | Orta | Orta | Orta | 3 |

### 3.4.7 Çağrı Merkezleri (ÇM)

Çağrı Merkezi (Call Center-ÇM), GSM işletmecilerinin müşterileri ile olan iletişimlerini yürüttükleri; yazılım, donanım, insan kaynakları ve iş akışlarından oluşan etkileşim ve bilgi merkezleridir.

Yoğun şekilde gelen ve giden telefon çağrıların gerçekleştirildiği bu merkezlerde işletmecilerin ve müşterilerin gizli bilgilerine erişmek mümkündür. Çünkü arayan müşterinin taleplerinin karşılanabilmesi için hem müşterinin kimlik ve abone bilgilerine (doğrulamak amaçlı) hem de işletmeci sistemlerine erişebilmek gerekmektedir. Erişilebilen bilgi ve sistemler göz önüne alındığında çağrı merkezlerinde BGYS'nin işletilmesi daha da önem kazanmaktadır.

Çağrı merkezlerinde Özel Birim Santralı (Private Branch Exchange-PBX) olarak bilinen santral sistemleri ve sunucuları bulunabileceği gibi internet protokolü IP PBX olarak da bilinen, İnternet Protokolu üzerinden aramaları aktaran, internet protokol adresi üzerinden ses taşıma VOIP PBX ve IP sunucular da bulunabilmektedir.

Çağrı merkezi varlıklarından bazıları, Tablo 3.1'deki örnek varlık envanterine Tablo 3.8'deki gibi işlenebilir.

Tablo 3.8.Çağrı merkezi varlıklarının örnek varlık envanter tablosuna işlenmesi

| Varlık Kodu | Varlık Grubu | Varlık | Varlık Tanımı | Varlık Türü (Bilgi, yazılım, donanım, hizmet, personel) | Varlık Pozisyonu | Varlık Sorumlusu | Gizlilik Değeri (Düşük, Orta, Yüksek) | Bütünlük Değeri (Düşük, Orta, Yüksek) | Erişilebilirlik Değeri (Düşük, Orta, Yüksek) | Varlık Değeri (1,2,3,4,5) |
|---|---|---|---|---|---|---|---|---|---|---|
| ÇM12 | ÇM | MCCIC41 | CIC Sunucu (IP PBX, IVR, Ses Kayit) | Donanım | Kartal/İst. | SEMA UÇAR | Orta | Orta | Düşük | 4 |
| ÇM113 | ÇM | MCCICR13 | CIC ses ve ekran kayıtları göndericisi/ Depolama sunucusu | Donanım | Kartal/İst. | Sema UÇAR | Orta | Orta | Düşük | 4 |
| ÇM144 | ÇM | Or-Client-10G | Oracle Client Uygulaması | Yazılım | Kartal/İst. | Sema UÇAR | Orta | Orta | Düşük | 4 |
| ÇM215 | ÇM | GMSCCNTR | IVN test Sunucusu | Donanım | Kartal/İst. | Sema UÇAR | Düşük | Düşük | Düşük | 3 |
| ÇM167 | ÇM | CCSQLSRV | Çağrı merkezi SQL Sunucusu | Donanım | Kartal/İst. | Sema UÇAR | Orta | Orta | Düşük | 4 |
| ÇM107 | ÇM | ANTCS1000E | BackOffice PBX Santral Sistemi | Donanım | Adana | Erol TOK | Yüksek | Yüksek | Orta | 5 |
| ÇM158 | ÇM | Call Center Core Sistem Uzmanı | Call Center Core Sistem Uzmanı | Personel | Kartal/İst. | Sema UÇAR | Orta | Orta | Düşük | 4 |
| ÇM196 | ÇM | VCS Sunucu | Video Konferans Sunucusu | Yazılım | Kartal/İst. | Sema UÇAR | Orta | Orta | Yüksek | 4 |

### 3.4.8 Kişiye Tahsisli Varlıklar

Kişiye tahsisli varlıklar, işletme çalışanlarının kullanımına tahsis edilmiş olan dizüstü bilgisayarlar, masaüstü bilgisayarlar, çeşitli bilgisayar programları, cep telefonları, e-posta hesapları, flash bellekler, evrak klasörleri v.b. ofiste ve mobil kullanılabilen varlıklar olarak sayılabilirler.

Kişiye tahsisli varlıklardan bazıları, Tablo 3.1'deki örnek varlık envanterine Tablo 3.9'daki gibi işlenebilir.

Tablo 3.9.Kişiye tahsisli varlıkların örnek varlık envanter tablosuna işlenmesi

| Varlık Kodu | Varlık Grubu | Varlık | Varlık Tanımı | Varlık Türü (Bilgi, yazılım, donanım, hizmet, personel) | Varlık Pozisyonu | Varlık Sorumlusu | Gizlilik Değeri (Düşük, Orta, Yüksek) | Bütünlük Değeri (Düşük, Orta, Yüksek) | Erişilebilirlik Değeri (Düşük, Orta, Yüksek) | Varlık Değeri (1,2,3,4,5) |
|---|---|---|---|---|---|---|---|---|---|---|
| KT47 | KT | ADOBE ACROBAT 9 PRO | Pdf görüntüleyici | Yazılım | İşletme çalışanları | Cem KARA | Orta | Düşük | Düşük | 2 |
| KT561 | KT | Blackberry | Smart telefon | Donanım | İşletme çalışanları | Akif UYAR | Yüksek | Düşük | Düşük | 3 |
| KT253 | KT | GSX Monitoring Tool | Monitör Programı | Yazılım | İşletme çalışanları | Elif KOÇ | Düşük | Düşük | Düşük | 1 |
| KT479 | KT | LotusMP01 | Mail Sistem | Yazılım | Kartal/İst. | Sema UR | Yüksek | Orta | Yüksek | 4 |
| KT444 | KT | Microsoft Office Project Professional | Proje Tasarım Prog. | Yazılım | İşletme çalışanları | Cem PAK | Düşük | Düşük | Düşük | 1 |

## 3.5 Risk Belirleme

Risk belirleme işlemi, birim sorumlularının, mobil haberleşme işleyişini etkileyecek (bilinen ve potansiyel) tehditlerin, yükümlülüklerin ve zayıflık durumunun değerlendirilmesidir.

Risk belirleme çalışmalarına birim/bölüm yöneticileri, Bilgiden Sorumlu Müdür (Chief İnformation Officer – CIO), Finanstan Sorumlu Müdür (Chief Financial Officer-CFO), Bilgi Sistemleri Yöneticisi, İnsan Kaynakları Yöneticisi, Bilgi Güvenliği Sistem Yöneticisi gibi yönetici grubun katılmasında fayda vardır. Çünkü herhangi bir tehdidin gerçekleşmesi durumunda birinci derecede sorumlular yöneticiler olacaktır. Riskleri yönetebilmek için önceliklerin ve risklerin neler olduğunun bilinmesi gerekmektedir.

Şebeke, insan kaynakları, finans, IT ve diğer önemli varlıklar işe yaptıkları etkiye göre belirlenmeli ve sınıflandırılmalıdır. Böylece, tüm bilgi kaynaklarının bilinmesi ve uygun şekilde önceliklendirilmesi ile sadece risk yönetimine değil aynı zamanda felaket kurtarma planına da hazırlık yapılmış olur.

Risk belirlemesi yapılırken risk alanlarının çok fazla olduğu görülecektir. Ancak model BGYS için bazı risk alanları aşağıdaki gibi ifade edilebilir;

- Tespit edilemeyen hassas veri sızması veya değiştirilmesi (çalışanlar, tedarikçiler, üçüncü taraf hizmet sağlayıcılar),
- Silme, ekleme, değiştirme, kopyalama ve ifşa nedeniyle hassas bilgilerin gizlilik, bütünlük veya erişilebilirliğinin zarar görmesi,
- Hacker saldırıları,
- İnternet sayfasında açıkların olması,
- Haberleşmenin yasadışı dinlenmesi,
- Onaylanmamış ve test edilmemiş değişikliklerin sisteme uygulanması,

- Şebeke cihazlarında yazılım ve donanım arızası,
- Hatalı veya kasıtlı bozulmuş yazılımlar,
- Çalışanların kasıtlı olmayarak sildiği ve değiştirdiği veriler,
- Çalışanların kasıtlı olarak bilgilerin gizlilik, bütünlük veya erişilebilirliğine zarar verme çabası,
- Yetkisiz kişilerin abonele bilgilerinin tutulduğu veritabanlarına erişmesi,
- Tedarikçilerin cihazlara istenmeyen erişimleri,
- Üçüncü tarafların sözleşme gereklerini yerine getirmemesi,
- Çağrı merkezlerinin çökmesi,
- Sel, deprem, yangın gibi doğal afetler,
- Aşırı yükleme nedeniyle sistemlerin çökmesi,
- Sistem soğutma cihazlarının bozulması,
- İşletme sırlarına vakıf çalışanın rakip işletmeye geçmesi,
- Gizli fiyat uygulamalarının ve tekliflerinin ifşa edilmesi.

Risk belirleme çalışmaları sonucunda belirlenen riskler, belli bir biçimde tablolaştırılarak risk kayıtları oluşturulur. Bu kayıtlar risk analizi, derecelendirmesi ve iyileştirilmesi sırasında kullanılır.

Mobil haberleşme sektörü için model olarak sunulan sistemde risk kayıtlarında;

- Tehdit altındaki varlık ve grubu,
- Risk numarası,
- Gerçekleşme ihtimali bulunan tehdidinaçık ifadesi,
- Tehdidin tahmini gerçekleşme ihtimali (mobil işletmeciler için 1'den 5'e düşük ve yüksek ihtimal olarak değer atanabilir),
- Tehdidin işletme işleyişinde oluşturacağı etki (mobil işletmeciler için 1'den 5'e düşük ve yüksek etki olarak değer atanabilir),
- Varlığın ya da sistemin zayıf tarafları/zaafları,
- Riskin açık ifadesi,

- Riskin sahibi (çoğu zaman varlık sorumlusu ya da birim yöneticisidir),
- Riskin değeri (1-25; yüksek, orta, düşük vb.)

yer almalıdır.

Belirlenen riskler Tablo 3.10.'da oluşturulmuş örnek risk kayıt tablosuna işlenir.

Tablo 3.10. Örnek risk kayıt tablosu

| Varlık Grubu | Varlık | Risk No | Tehdit | Tehdidin Gerçek Olma İhtimali (1,2,3,4,5) | İşleyişe Etkisi (1,2,3,4,5) | Zaafiyet/ Açıklık | Risk | Risk Sorumlusu | Risk Değeri (1-25) | Risk Değerlendirmesi (Düşük,Orta, Yüksek) |
|---|---|---|---|---|---|---|---|---|---|---|
| RAN | | R2 | Donanım çalışma hatası | | | | Kısmı haberleşme kesintisi | | | |
| Transmisyon | | R35 | Doğal afet sonucu SDH bağlantılarının zarar görmesi | | | | Bazı bölgeler için kısmen ya da tamamen haberleşme kesintisi | | | |
| ÇM | | R43 | Çağrı merkezi şebekesinin; arızalanması, aşırı ısınma, nem, toz, terör saldırıları | | | | Sistem ekipmanlarının zarar görmesi | | | |
| | | | | | | | | | | |

Tüm risk alanlarına ait birçok tehdit ve zayıflıktan bahsetmek mümkündür. Ancak tez içerisinde hepsine yer vermek mümkün olmadığından Tablo3.10.'a bazı riskleri işleyerek model BGYS sisteminin bu konudaki yaklaşımını biraz daha somutlaştırmak mümkündür.

### 3.6 Risk Analizi ve Derecelendirilmesi

Tespit edilen riskler, işletme ve mobil haberleşme şebekesi hakkında detaylı bilgiye sahip, faaliyetlerin devamlılığı için sorumlulukları olan orta seviye yöneticilerle ve çalışanlarla birlikte detaylı incelenerek analiz edilir.

Riskleri yönetebilmek için önceliklerin ve risklerin neler olduğunun bilinmesi gerekmektedir. Yapılan analizler sonrasında risklerin ve tehditlerin ciddiyetinin daha iyi anlaşılabilmesi için derecelendirme yapılır. Risk derecelendirmesi esnasında göz önüne alınan hususlar; iş öncelikleri, işletmeye ve operasyona olan etkinin büyüklüğü, önem, maliyet, faydalar ve yasal gereksinimler olabilmektedir.

Yukarıda bahsedilen hususlar göz önüne alınarak tehdidin tahmini gerçekleşme ihtimali 1' den 5' e düşük ve yüksek ihtimal, tehdidin işletme işleyişinde oluşturacağı muhtemel olumsuz etki 1' den 5' e düşük ve yüksek olumsuzluk olmak üzere derecelendirilir.

Bu kapsamda tehdidin oluşması ihtimali değeri ile tehdidin muhtemel etkisi çarpılarak risk değeri hesaplanır. Her iki değer de 1'den 5'e kadar değer aldığından çarpım sonucu da 1'den 25'e kadar değerler alır. Bu değerler Tablo 3.11.'de gösterilmiştir. Farklı mobil işletmeciler, risk değerlendirmesi yaparken değer aralıklarını risk iyileştirme kabiliyeti ve istekliliğe göre farklı değerlendirebilirler. Ancak BGYS'nin ana amaçlarından biri de risklerin en

aza indirilmesi olduğundan model BGYS'de risk değerlendirmesinde aralıkların aşağıdaki gibi;

[1,4] aralığı risk değeri: Düşük
[5,9] aralığı risk değeri: Orta
[10,25] aralığı risk değeri: Yüksek

olarak değerlendirilmesi önerilmektedir.

Tablo 3.11. Risk değerleri tablosu

| (Tehdidin gerçekleşme ihtimali) X (Tehdidin oluşturacağı muhtemel etki) | Risk Değeri | Risk Değerlendirmesi |
|---|---|---|
| 1x1 | 1 | Düşük |
| 1x2 | 2 | Düşük |
| 1x3 | 3 | Düşük |
| 1x4 | 4 | Düşük |
| 1x5 | 5 | Orta |
| 2x1 | 2 | Düşük |
| 2x2 | 4 | Düşük |
| 2x3 | 6 | Orta |
| 2x4 | 8 | Orta |
| 2x5 | 10 | Yüksek |
| 3x1 | 3 | Düşük |
| 3x2 | 6 | Orta |
| 3x3 | 9 | Orta |
| 3x4 | 12 | Yüksek |
| 3x5 | 15 | Yüksek |
| 4x1 | 4 | Düşük |
| 4x2 | 8 | Orta |
| 4x3 | 12 | Yüksek |
| 4x4 | 16 | Yüksek |
| 4x5 | 20 | Yüksek |
| 5x1 | 5 | Orta |
| 5x2 | 10 | Yüksek |
| 5x3 | 15 | Yüksek |
| 5x4 | 20 | Yüksek |
| 5x5 | 25 | Yüksek |

Tablo 3.12'de verilen risk kayıt tablosunda bazı tehditler ve bu tehditlerin oluşturduğu risklerin analiz ve derecelendirilmesi yapılmıştır.

Tablo 3.12. Risklerin risk kayıt tablosuna işlenmesi

| Varlık Grubu | Varlık | Risk No | Tehdit | Tehdidin Gerçek Olma İhtimali (1,2,3 4,5) | İşleyişe Etkisi (1,2,3,4,5) | Zaafiyet/ Açıklık | Risk | Risk Sorumlusu | Risk Değeri (1-25) | Risk Değrln. (Düşük, Orta, Yüksek) |
|---|---|---|---|---|---|---|---|---|---|---|
| IT | Probe | R5 | Şebeke izleme ekipmanları ile elektronik haberleşmenin içeriden ya da dışarıdan yetkisiz kişilerce dinlenilmesi | 2 | 5 | Veriler, şebeke cihazlarına ve probe' lere yüklü dağıtıcılara transfer sırasında ele geçirilebilir ya da kaydedilebilir. | Hassas veri sızması | Test ve İzleme Birim Amiri | 10 | Yüksek |
| ÇM | CTI (Computer Telephony Integration System) Bilgisayar-Telefon Entegrasyon sistemi | R8 | Çağrı merkezi şebekesinin; arızalanması, aşırı ısınma, nem, toz, terör saldırıları | 1 | 4 | Yedeği olmayan ekipmanların erişilebilirliği, çevresel tehditlere ve yetkisiz erişimlere karşı yeterli korumanın olmayışı, | Sistem ekipmanlarının zarar görmesi | Çağrı Merkezi IT Müdürü | 4 | Düşük |
| IT | Dolandırıcı İzleme Sistemi | R34 | Sistem tedarikçisinin yetkisiz erişimi | 3 | 5 | Tedarikçilere güvenlik duvarı geçişleri için süreli şifre veriliyor ama giriş kayıtları tutulmuyor. | Hassas veri sızması veya değiştirilmesi | Dolandırıcık İzleme Birim Amiri | 15 | Yüksek |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Genel | Personel | R12 | Çalışanların yetkisiz oldukları hassas bilgilere ulaşarak ifşa etmesi | 2 | 5 | Çalışanların Bilgi güvenliği politikası ve BGYS farkındalığının düşük olması, yetersiz izleme ve güvenlik ayarları | Arama kayıtlarının (CDR) kasıtlı olarak ifşa edilmesi | İlgili birim amiri | 10 | Yüksek |
| IT | Dolandırıcı İzleme Sistemi | R78 | Kasıtlı kullanıcı eylemleri | 3 | 5 | Şifrelerin kötü amaçlı kişilere verilmesi yada direkt kullanıcının verilere erişmesi | Veri tabanalarına yetkisiz erişimler,CDR kayıtlarının ifşası | Dolandırıcık İzleme Birim Amiri | 15 | Yüksek |
| Trans. | SDH | R51 | Doğal afet sonucu SDH bağlantılarının zarar görmesi | 1 | 5 | Bağlantıların zarar görmesi ihtimaline karşı boş portların bırakılmamış olması, | Bazı bölgeler için kısmen ya da tamamen haberleşme kesintisi | Transmisyon Hatları İzleme Amiri | 5 | Orta |
| KDS | MMSC(Multi media Messaging Service Center) | R15 | Yetkisiz sistem yönetici eylemeleri - Kayıtları silme ve değiştirme - Yetkisiz MMS izleme - Sistemi kapatma | 1 | 5 | Kullanıcı hesabı yönetimi kuralları net belirlenmemiş | MMSC servisinde bozulmalar | BGYS Amiri | 5 | Orta |
| RAN | BTS | R32 | Donanım çalışma hatası | 2 | 3 | Yeterli yedek parça stoku yok Tedarikçiler ile yapılan sözleşemeler yok ya da iyi yapılmamış. | Kısmı haberleşme kesintisi | RAN Şebekesi İzleme Birim Amiri | 6 | Orta |

## 3.7 Risk İşleme

Mobil işletmeci, riskler belirlendikten ve derecelendirildikten sonra risk değerlerini düşürmek için riskleri masaya yatırır ve risk iyileştirme kararları alır. Bu eyleme model içerisinde kısaca risk işleme eylemi denmektedir.

İşletmenin uygulayabileceği risk iyileştirme yöntemleri aşağıdaki gibi sınıflandırılabilir:

- Azaltma: Uygun kontroller uygulanarak riskin kabul edilebilir seviyeye düşürülmesi şeklinde olabilir. ISO/IEC 27001:2005 standardında yer alan kontroller bu amaca uygundur.
- Kaçınma: Riskin oluşmasına neden olan faktörleri ortadan kaldırarak riskten kurtulmaktır. Örneğin yedek şebeke anahtarlama sisteminin operasyonda kullanılan aktifler ile aynı binada olması sabotajda beraber zarar görme riski oluşturur. Bu durumda yedek sistemler kaldırılmalı ve farklı binalara hatta farklı şehirlere taşınmalıdır. Bir başka örnek olarak; internet üzerinden kontör ya da kredi yüklenebilmesi işletme için yeni riskler getirecektir. Bu risklerden kaçınmak isteyen işletmeci bu faaliyeti için interneti kullanmaktan vazgeçebilir.
- Transfer: Riskten kaçınmak, riski indirmek zor veya çok pahalı ise riskin transferi iyi bir seçenektir. Bu anlamda riskin sigorta şirketleri veya tedarikçiler gibi dış taraflara aktarılması riskin taşınması demek olacaktır. Örneğin doğal afetlere karşı şebekenin sigortalanması ile çok yüksek olan yeni şebeke cihazları temini maliyeti, sigorta şirketine transfer edilecektir.
- Tutma: İşletme politikalarına ve risk kabul ölçütlerine uyması şartıyla riskin objektif bir biçimde kabul edilmesidir.

- Bildirim: Risklerin ilgili taraflara (Otorite, abonelar, iş ortakları) önceden bildirilebilir

Risk işleme eyleminde kararlar; birim amirleri, orta seviye yönetici ve çalışanlarla birlikte yapılan bir çalışma ile alınır. Örneğin çağrı merkezi için; üst düzey bir yönetici (CEO ya da Genel Müdür yardımcısı gibi), ÇM yöneticisi, BGYS yöneticisi, sorumlu teknik personel, koordinatör müşteri hizmetleri temsilcisi ve bazı müşteri hizmetleri temsilcileri olarak düşünebilir.

Daha önceden hazırlanmış risk kayıtlarında yer alan numaralanmış ve sahibi belirlenmiş riskler için tedbirler belirlenir. Bu tedbirler içinde görevin kime atandığı ve tamamlanma zamanı gibi bilgiler de yer alabilir.

Örnek risk kayıtlama tablosu olan Tablo 3.10. üzerine işlenen ve Tablo 3.12'de yer alan risk örneklerini iyileştirerek risk değerlerini düşürmek için yapılabilecek tedbirler, risk iyileştirme tablosu Tablo 3.13.'de görülebilir.

Tablo 3.13.Risk iyileştirme tablosu

| Varlık Grubu | Varlık | Risk No | Tehdit | Tehdidin Gerçek Olma İhtimali (1,2,3,4, 5) | İşleyişe Etkisi (1,2,3,4, 5) | Zaafiyet/ Açıklık | .... | Risk Değeri (1-25) | Risk Değerlendirmesi (Düşük,Orta , Yüksek) | Risk iyileştirme eylemi | Kontrol maddeleri | Gerçekleşme İhtimalindeki İyileşme | Etkideki İyileşme | Yeni Risk değerlendirmesi |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| IT | Probe | R5 | Şebeke izleme ekipmanları ile elektronik haberleşmenin içeriden ya da dışarıdan yetkisiz kişilerce dinlenilmesi | 2 | 5 | Veriler, şebeke cihazlarına ve probe'lere yüklü dağıtıcılara transfer sırasında ele geçirilebilir ya da kaydedilebilir. | | 10 | Yüksek | Sunuculardan probe'lere veri transferlerinde kriptolamanın kullanılması | A.15.1.4 A.10.6 | -1 | 0 | Orta |
| ÇM | CTI (Computer Telephony Integration System) Bilgisayar-Telefon Entegrasyon sistemi | R8 | Çağrı merkezi şebekesinin; arızalanması, aşırı ısınma, nem, toz, terör saldırıları | 1 | 4 | Yedeği olmayan ekipmanların erişilebilirliği, çevresel tehditlere ve yetkisiz erişimlere karşı yeterli korumanın olmayışı, | | 4 | Düşük | 1-Acil durumlar için yedek ekipmanların sağlanması, 2- Çağrıların bir diğer çağrı merkezine yönlendirilebilmesi, | A.10.3.1 | 0 | -2 | Düşük |
| IT | Dolandırıcı İzleme Sistemi | R34 | Sistem tedarikçisinin yetkisiz erişimi | 3 | 5 | Tedarikçilere güvenlik duvarı geçişleri için süreli şifre veriliyor ama giriş kayıtları tutulmuyor. | | 15 | Yüksek | 1-Güvenlik duvarı ve veri tabanlarında giriş kayıtlarının tutulabilmesi için ayarların yapılması, gerekli izleme programların kurulması 2- Periyodik olarak kayıtların denetlenmesi | A.6.2.1 A.10.10.1 A.10.10.2 A.10.10.3 | -2 | -1 | Orta |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Genel | Personel | R12 | Çalışanların yetkisiz oldukları hassas bilgilere ulaşarak ifşa etmesi | 2 | 5 | Çalışanların Bilgi güvenliği politikası ve BGYS farkındalığının düşük olması, yetersiz izleme ve güvenlik ayarları | | 10 | Yüksek | 1- İzleme prosedürlerinin uygulanması, 2- Farkındalık eğitiminin ve faaliyetlerinin yapılması | A.10.10 A.8.2.2 | -1 | -1 | Orta |
| IT | Dolandırıcı İzleme Sistemi | R78 | Kasıtlı kullanıcı eylemleri | 3 | 5 | Şifrelerin kötü amaçlı kişilere verilmesi yada direkt kullanıcının verilere erişmesi | | 15 | Yüksek | 1- Verilen şifreler ile yapılan işlemlerin eşleştirilebilmesi, 2- Herhangi bir neden ve ihtiyaç oluşmadan erişim izni verilmemesi, 3- Şifrelerin kişliye özel ve tek kullanımlık olması | A.11.5 | -2 | -2 | Orta |
| Trans misyon | SDH | R51 | Doğal afet sonucu SDH bağlantılarının zarar görmesi | 1 | 5 | Bağlantıların zarar görmesi ihtimaline karşı boş portların bırakılmamış olması, | | 5 | Orta | 1- Alternatif yönlendirmelerin yapılması, 2- Boş portların olması, | A.11.4.7 A.14.1 | 0 | -2 | Düşük |
| KDS | MMSC(Multi media Messaging Service Center) | R15 | Yetkisiz sistem yönetici eylemeleri - Kayıtları silme ve değiştirme - Yetkisiz MMS izleme - Sistemi kapatma | 1 | 5 | Kullanıcı hesabı yönetimi kuralları net belirlenmemiş | | 5 | Orta | İzleme prosedürleri kapsamında kullanıcı hesaplarının izlemesi | A.10.10.4 A.10.10.3 | 0 | -2 | Düşük |
| RAN | BTS | R32 | Donanım çalışma hatası | 2 | 3 | Yeterli yedek parça stoku yok Tedarikçiler ile yapılan sözleşemeler yok yada iyi yapılmamış. | | 6 | Orta | 1- Yeterli yedek parça stoku oluşturulmalı, 2- Tedarikçler ile yapılan sözleşmelerin yenilenmesi, | A.14.1 A.10.2 | -1 | 0 | Düşük |

Uygun kontroller uygulanarak riskin kabul edilebilir seviyeye düşürülmesi mümkündür. Bu kontrol maddeleri ISO/IEC 27001:2005 standardında yer alan kontroller arasından seçilebilir ya da işletme kendine özel kontroller geliştirebilir. Tablo 3.13.'de görülen kontrol maddeleri sütunu o satırda yer alan riskin azaltılabilmesi için ISO/IEC 27001:2005 standardından belirlenmiş uygun kontrol maddeleridir.

Kontrollerin riski azaltma mantığı oldukça basittir. Örneğin hassas veri tabanlarına yetkilendirilmiş ve sınırlı girişlerin kayıtlarının tutulup tutulmadığı, ilgili kontrol maddesi kapsamında iç ve dış denetimlerde izlenebilir.

İyileştirme eylemlerinin uygulanması sonrasında eylemlerin işleyişi BGYS sorumluları tarafından düzenli olarak takip edilmeli ve eylemlerin sonuçları değerlendirmelidir.

## 3.8 Kontrollerin Seçimi

Risk yönetmek ve işlemek için bu amaca uygun kontrol ve kontrol hedeflerinin seçilmesi gerekir. Kontrol seçiminin gayesi, riskleri işletme için kabul edilebilir seviyeye indirmektir. Bu kontroller, ISO/IEC 27001:2005 Ek-A' dan seçilirken burada yer alan 133 kontrol maddesine bir nevi kılavuzluk yapan ISO/IEC 27011:2008 rehber dokümanından faydalanılabilir.

Haberleşme sektörüne özel ISO/IEC 27011:2008 rehber kılavuz, ISO/IEC 27002 standardında tanımlanmış olan 11 ana kontrol alanından oluşmaktadır:

- Güvenlik Politikası
- Bilgi Güvenliği Organizasyonu
- Varlık Yönetimi
- Personel Güvenliği
- Fiziksel ve Çevresel Güvenlik

- İletişim ve İşletme Yönetimi
- Erişim Denetimi
- Bilgi Sistemi Tedariği, Geliştirilmesi ve Bakımı
- Bilgi Güvenliği Olayları Yönetimi
- İş Sürekliliği Yönetimi
- Uyum

Ayrıca özellikle ISO/IEC 27011:2008 standardı kapsamında ek olarak sunulan "Telekomünikasyon Sektörü İçin Genişletilmiş Kontroller" ve "Ek Uygulama Kılavuzu" kısımlarında, telekom altyapı ve servislerinde güvenliği sağlamaya yönelik yeni kontrollerin uygulanmasında da fayda vardır. Söz konusu ilave kontroller ve uygulama kılavuzları aşağıdaki gibi sıralanabilir.

Telekomünikasyon sektörü için genişletilmiş kontroller (Ezber, 2010b):

9 Fiziksel ve Çevresel Güvenlik
9.1 Güvenlik Alanı
9.1.7 İletişim merkezinin güvenliğinin sağlanması
9.1.8 Telekomünikasyon ekipman odasının güvenliğinin sağlanması
9.1.9 Fiziksel olarak izole edilmiş çalışma alanlarının güvenliğinin sağlanması

9.3 Diğer kurumların kontrolü altında güvenlik
9.3.1 Taşıyıcının lokasyonunda bulunan ekipman güvenliği
9.3.2 Kullanıcı lokasyonunda bulunan ekipman güvenliği
9.3.3 Bağlantılı telekomünikasyon hizmetleri

10 İletişim ve İşletme Yönetimi
10.6 Ağ Güvenliğinin Yönetilmesi
10.6.3 Sunulan Telekomünikasyon Hizmetlerinin Güvenlik Yönetimi
10.6.4 Spam Maillere Karşı Tepki
10.6.5 DoS/DDoS Saldırılarına Karşı Tepki

11 Erişim Denetimi

11.4 Ağ Erişim Denetimi

11.4.8 Kullanıcı tarafından taşıyıcı tespiti ve kimlik denetimi

15 Uyum

15.1 Yasal Gereklere Uyumluluk

15.1.7 İletişim Gizliliği

15.1.8 Temel İletişim

15.1.9 Acil Tedbirlerin Uyumluluğu

Ek uygulama kılavuzu:

B.1 Siber Saldırılara karşı ağ güvenlik önlemleri

B.1.a Ağ Araçlarının Korunması

B.1.b Kimlik Sahteciliğine karşı önlemler

B.1.c Telekomünikasyon Servis Kullanıcılarının Dikkatini Çekmek

B.2 Şebeke Tıkanmasına Yönelik Ağ Güvenlik Önlemleri

B.2a Şebeke Tıkanmasını tespit ve önlemeye yönelik mekanizmalar

B.2.b Şebeke Tıkanmasına sebep olabilecek bilginin önceden toplanması

B.2.c Geçici hız yükseltme tedbirleri

B.2.d Temel iletişimlerin tespiti ve önceliklendirilmesi

B.2.e Arıza tetikleyebilecek bilginin toplanması (Ezber, 2010b)

### 3.9 Kabul Edilebilir Risk Onayı

İşletmeci, risk kayıt tablosundaki iyileştirilebilir risklere müdahale ettikten sonra kalan riskleri artakalan risk (residual risk) olarak kabul edebilir. Örneğin veri kriptolama ile dizüstü bilgisayarların çalınması sonucu oluşan veri gizliliğine ilişkin risk azaltılabilir. Ancak veri kriptolama için kullanılan yöntemin kırılması riski her zaman mevcuttur ve artakalan bir risktir. Bununla birlikte kriptolama kullanılmaması öncesine göre daha az bir riskten

bahsetmek mümkündür. Artakalan risklerin yönetim tarafından kabul edilmesi gerekmektedir (Bağcı, 2008).

Üst düzey yönetimin bizzat bilgi güvenliğinden sorumlu olması nedeniyle kabul edilebilir risk onayını, ancak işletmenin üst düzey yönetimi verebilir.

Model önerimizde kabul edilebilir risk düzeyi (KERD),risk değerlerinin belirlendiği tabloda düşük risk aralığında değerlendirilen "[1,3]" olarak belirlenmiştir. "[1,3]" risk değerinden daha yüksek risk değerine sahip riskler, eğer;

- Düşük risk [3,4] düzeyinde ise, en az önlem alınarak ve zaman harcanarak KERD'e indirilir.
- Orta risk [5,9] düzeyinde ise, daha fazla önlem ve zaman harcanarak KERD'e indirilir.
- Yüksek risk [10,25] düzeyinde ise işletme kaynak ayırarak ve çözüm arayışına girerek KERD'e indirilir.
- Kabul edilebilir risk düzeyinde ise alınan önlemler sürdürülür.

### 3.10 Yönetim Onayı

Mobil haberleşme işletmecileri için düşünülen model BGYS kurulum aşamalarından sonra BGYS işletimi ve uygulamasını yapmak için üst yönetimden onay almak gerekmektedir.

Çünkü yönetim her ne kadar tüm aşamalarda doğrudan yada dolaylı olarak işin içinde olsa bile sistemin bütününü gördükten sonra bazı risklerin yersiz olup olmaması, bazılarının göz ardı edilmesi, risk iyileştirme eylemlerinin isabetliliği, kabul edilebilir risk düzeyinin yeterliliği v.b. konularda düzeltmeler isteyebilir. Dolayısıyla kurulmuş BGYS, üst yönetim onayı alındıktan sonra gerçekleştirilir ve işletilir.

### 3.11 Uygulanabilirlik Bildirgesi

En son olarak uygulanabilirlik bildirgesi hazırlanarak model BGYS kurulumu tamamlanır. Uygulanabilirlik bildirgesi, riskler işlenirken seçilmiş kontrollerin neler olduğu ve bunların hangi gerekçelerle seçildiğini anlatmalıdır. Kurulacak model BGYS önerimiz, TS ISO/IEC 27001 standardını uygulamayı da kapsadığından, standardın EK-A'sında yer alan 133 adet kontrol maddesinden seçilmemiş olanların neden seçilmediğine dair geçerli gerekçelerin de uygulanabilirlik bildirgesinde yer alması gerekir. Çünkü uygulanabilirlik bildirgesi TS ISO/IEC 27001:2005 belgesi almak isteyen işletmeler için bir zorunluluktur.

# 4. ÖRNEK BGYS MODELİNİN; GERÇEKLEŞTİRİLMESİ, İŞLETİLMESİ, İZLENMESİ, GÖZDEN GEÇİRİLMESİ, SÜREKLİLİĞİNİN SAĞLANMASI VE İYİLEŞTİRİLMESİ

BGYS süreçleri içerisinde en zor ve en çok zaman alan adım sistemin kurulmasıdır. Ancak sistemin kurulması işlemin bittiği anlamına gelmez. BGYS sürekli devam eden ve gelişen bir yönetim sistemidir. Klasik PUKÖ modeli anlayışında olduğu gibi BGYS için "Planla – Uygula – Kontrol et – Önlem al" faaliyetleri bir döngü içinde durmaksızın sürekli devam eder. Sisteminplanlama kısmına denk düşen kurulumundan sonra; gerçekleştirilmesi ve işletilmesi, izlenmesi ve gözden geçirilmesi, sürekliliğinin sağlanması ve geliştirilmesi gerekmektedir. Tüm bu faaliyetler Şekil1.2.'deki PUKÖ döngüsünün diğer adımlarına denk gelmektedir.

Mobil haberleşme sektöründe faaliyet gösteren işletmeciler adına başarılı bir BGYS'den bahsedebilmek için diğer tüm adımların da dikkatle uygulanması ve bunların bir döngü içinde kendini geliştirmesi gerekir.

## 4.1 Örnek BGYS Modelinin Gerçekleştirilmesi Ve İşletilmesi

Kurulan BGYS içerisinde temel olarak BGYS politikası ve prosedürlerinin sonrasında risklerin iyileştirilebilmesi için belirlenmiş kontrollerin uygulanarak gerçekleştirilmesi ve sistemin işletilmesi gereklidir.

Sistemin işletilebilmesi için mobil işletmeci, BGYS'nin kuruluşu aşamasında planladığı bazı hususları hayata geçirmelidir. Bu hususların başlıcaları:

- BGYS için bütçe sağlamak,
- Bir plan dâhilinde farkındalık ve ilgili diğer eğitimleri vermek,

- Farkındalığı artırıcı eylemler hazırlamak,
- Kaynakların yönetimi prosedürlerini hazırlamak ve uygulamak,
- Bilgi güvenliği risklerini yönetmek için risk işleme planı oluşturmak,
- Kontrol hedeflerini karşılaması için seçilen kontrolleri gerçekleştirmek,
- Vakalar ve ihlal olaylarını idare etmek için prosedürleri ve kontrollerigerçekleştirmek

şeklinde sayılabilir.

### 4.1.1 BGYS bütçesinin oluşturulması

Bir mobil işletmeci için BGYS sistemine ayrılacak bütçe ilk yıl için doğal olarak en yüksek seviyede olabilir. Çünkü gerek personel gerekse yazılım ve donanım ihtiyaçları en çok ilk BGYS yılında fark edilecektir. Ve bu ihtiyaçların temini ancak yeterli bir bütçe ile mümkün olabilir.

Risk belirlemede kullanılacak kaynaklar, kontrollerin gerçekleştirilmesi için gerekli olan kaynaklar, eğitim ve BGYS bir kez kurulduktan sonra onu güncel tutmak ve iş için her gün etkin olmasını sağlamak için gerekli olan kaynağın tahsis edilmesi gerekir.

İlk yıl BGYS bütçesi oluşturulurken dikkate alınacak başlıca kalemler; BGYS personeli istihdam maliyeti, eğitimler ve eğitim saatlerinin işletmeye dolaylı maliyeti, güvenlik yazılımları harcamaları, fiziksel güvenlik sistemleri harcamaları, dokümantasyon giderleri, sertifikasyon giderleri, yeni sigorta harcamaları ve varsa danışmanlık giderleri olarak sayılabilir.

Sonraki yıllarda ise bu giderler kısmen azalabileceği gibi yaşanan riskler ve risk iyileştirme kararları neticesinde ilk yıla yakın seyredebilir.

20 milyon abonesi ve yıllık 5 milyar dolar net satışı olduğu varsayılan orta büyüklükte ulusal çaptaki bir mobil işletmecinin ayırdığı BGYS bütçesi milyon dolarlar mertebesinde olmalıdır.Söz konusu BGYS bütçesi, bilgi güvenliği yönetimi birimi tarafından teklif edilir ve en üst düzeyde (CEO ya da Genel Müdür) onaylanır.

### 4.1.2 Eğitimler

İşletme, BGYS sorumlulukları olan personelin verilen görevleri yerine getirme konusunda yeterli olmalarını sağlamak için uygun bir farkındalık ve eğitim programı uygulamalıdır.

Bilgi güvenliği eğitimlerinin hedeflediği kitleler farklılıklar gösterir. Örneğin temel farkındalık eğitimini, tüm çalışanların alması gerekirken sadece yöneticiler için bilgi güvenliği eğitimleri de bulunmaktadır.

İşletme, eğitim ve farkındalık gereksinimlerini tanımlamalı ve BGYS'in etkin olduğunu, bilgi güvenliğinin uygun bir biçimde uygulanmasını temin etmek amacıyla tüm kullanıcılar, işletmenin idari personeli ve yöneticiler için uygun eğitimler seçmelidir.

Verilecek eğitim, bilgi güvenliği için rol ve işlev ile belli sorumluluklarla orantılı olmalıdır. Genel eğitim ve farkındalık programının bir parçası olarak, işletme bilgi güvenlik yönetimini içine almalı ve eğitilen kişilere doğru rollerin ve sorumlulukların verildiğinden ve rol ve sorumluluk verilen bu kişilerin bilgi güvenlik yönetimi konularıyla uğraşacak yeterlikte olduklarından emin olmalıdır. Burada geçen yeterlik düzeyi, herkesin sahip olması gereken basit anlama ve yeterlik düzeyinden (örneğin; parola kullanımı, fiziki güvenliğin temelleri, elektronik postanın doğru kullanımı, virüslerden korunma, vs.), tüm çalışanların sahip olması beklenmeyen daha karmaşık yeterlik düzeyine

(örneğin koruma duvarı oluşturulması, bilgi güvenlik ihlal olayı işlem sürecinin yönetilmesi, vb.) kadar olabilir.

Bazı eğitimlere katılımların bütün personel düzeyinde olduğu düşünüldüğünde, işletme işleyişinin etkilenmemesi için eğitim planlamasının iyi yapılması gerekir. Bu planlamayı insan kaynakları yapmalı ve çağrı merkezi çalışanlarından VAS çalışanlarına kadar herkesi dahil etmelidir. Hatta hizmet alınan üçüncü tarafların da bu eğitimlere katılmaları istenebilir.

Eğitimlerde verilmesi amaçlanan bilgi ya da farkındalığın, ne kadar kazanıldığı ölçücü testler ile ölçülmeli ve geçme barajı tayin edilmelidir. Program gerekli yeterlikleri belirlemeli, bu gereksinimleri karşılamak için gerekli olan eğitimi sunmalı, eğitimin etkinliğini değerlendirmeli ve kazanılan yetilerin ve niteliklerin kaydını tutmalıdır.

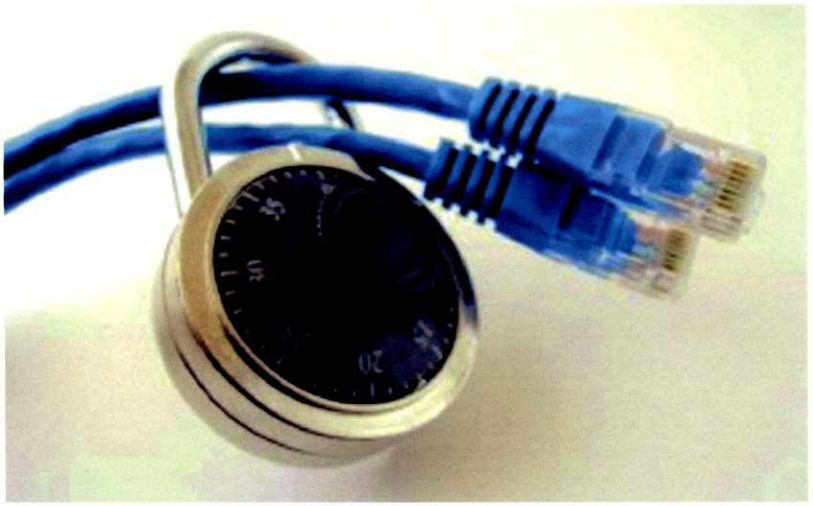
En azından tüm çalışanlar, Bilgi Güvenliği Farkındalık Eğitimi ve Bilgi Güvenliği Olay Müdahale Eğitimi almalıdırlar. Bilgi güvenliği yönetimi birimi içerisinde görev yapan ve bu konuda uzmanlık kazanması istenen kişilere ise; Bilgi Güvenliği Temelleri Eğitimi, Bilgi Güvenliği Risk Analizi Eğitimi, Saldırı Teknikleri ve Araçları Eğitimi, Windows Güvenliği Eğitimi ve İç Denetçi Eğitimi aldırılmasında fayda vardır.

Tüm bu eğitimlerin tek bir kez alınması yeterli olmayacaktır. Konuya ilişkin bilgilerin güncelliğinin sağlanması için tazeleme eğitimlerinin yapılması da gerekmektedir. Söz konusu tazeleme eğitimlerinin periyodu, 6 ay ya da 1 bir yıl olarak tercih edilebilir. Ancak daha uzun periyotların, BGYS açısından zayıflık oluşturması ihtimal dahilindedir.

### 4.1.3 Farkındalık artırıcı eylemler

Farkındalık eğitimleri sonrasında bilgi güvenliği bilincinin tazeliğini sürdürebilmesi için çalışanlara yönelik eylemler düşünülebilir. Örneğin her ay işletme iç ağı üzerinden yapılacak ödüllü bir test, periyodik bir BGYS bülteni, gizlilik derecelerinin üzerinde yazılı olduğu bir takvim ya da "Mouse pad", Şekil 4.1'deki gibi şifreli kullanımı tavsiye edici resimler, bilgi güvenliğinin karikatürize edildiği duvar afişleri v.b. farkındalığı artırıcı eylemler olarak sayılabilir.

Şekil1.1. Şifre kullanımı ile ilgili görsel



### 4.1.4 Kaynak yönetim prosedürlerinin hazırlanması ve uygulanması

İşletme, BGYS'yi işletmek, izlemek, gözden geçirmek, sürekli kılmak ve geliştirmek için gerekli olan kaynakları tanımlamalı ve sağlamalıdır. Bu kaynaklar bütçe ve iş gücü olarak ikiye ayrılır.

Bütçenin hazırlanması, onayının alınması ve düzeltici eylemlere pay edilmesi ile işgücünün planlanması ve kadrolanması, organizasyonu ve değerlendirilmesi, BGYS içerisinde tam zamanlı çalışan personelin sorumluluklarının belirlenmesi, yıllık denetim takvimlerinin hazırlanması kaynak yönetimi olarak sayılabilir.

Tüm bu kaynak yönetimlerini yapmak, geliştirmek, bilgi güvenliği ile kayıt işlemlerini sistematize etmek prosedürlerin hazırlanması ile mümkün olur.

### 4.1.5 Bilgi güvenliği risklerini yönetmek için risk işleme planının oluşturulması

Belirlenmiş riskleri yönetmek için hangi eylemlere başvurulması gerektiği, bu eylemlerin öncelikleri, sınırlayıcı faktörler ve gerekli kaynakların neler olduğunu ana hatları ile belirlenmelidir. Bunlar oluşturulmuş risk işleme tablolarında özet halini alır. Risk işleme başlıklı bölüm 3.7.'de bu konuya değinilmiş ve örnek Tablo 3.13 oluşturulmuştur.

### 4.1.6 Kontrol hedeflerini karşılaması için seçilen kontrollerin gerçekleştirilmesi

Risk iyileştirme planında yer alan tedbirler, öncelikler, kaynaklar, roller ve sorumluluklarla birlikte seçilen kontrollerin gerçekleştirilmesi için prosedürler ortaya koyulmalıdır. Kaynak israfını önlemek için gerçekleştirme derecesi (örneğin; ne kadar eğitim, kayıt veya raporlama),çok dikkatlice belirlenmelidir. Örneğin sık eğitime alınan personel asli görevlerini yerine getirmede zaman problemi yaşamaya başlar. Gereğinden fazla gerçekleştirme; tüm kontrol etkinliğinde bir gevşeme ve ihmalle sonuçlanabilir ve kontrolden etkilenen personel rahatsızlık duymaya başlayabilir.

Kontroller, seçildiği bilgi güvenliği risk(ler)inin yönetiminde işe yaramalıdır. Bu nedenle işletme, kontrollerin öngörülen hedefleri karşılmasının sağlanması için kontrollerin etkinliğini nasıl ölçmek istediğini belirlemelidir. Kontrol etkinliğinin belirlenmesinde kullanılan ölçütler, karşılaştırılabilir ve yeniden elde edilebilir sonuçlar vermelidir. Bu ölçütler, kontrollerin maliyet etkinliğini de ortaya koymalıdır.

### 4.1.7 Olay yönetim prosedürlerinin çalıştırılması

İşletme, olaylar (bilgi güvenliği olayı, yangın, doğal afetler v.b.) karşısında yapılacakları belirlemek, olayları tanımlamak ve rapor etmek, bu olayları değerlendirmek, olaylara etkili bir biçimde karşılık vermek, olayların vereceği zararı sınırlamak için gerekli olan prosedürleri ve kontrolleri belirler.

BGYS Politikası başlıklı Bölüm 3.3'te de yer verildiği gibi BGYS Politikası tek başına bir doküman değildir. Bilgi güvenliği amaçlarının gerçekleşmesi için mobil işletmeciler, BGYS Politikasını hazırladıkları prosedürler ve talimatlarla desteklemelidir.

İşletme çalışanları, aslında BGYS'yi bu prosedürler ve dolayısıyla süreçler ile yaşar ve hissederler. BGYS eğitimlerinde, sayısı ve konusu tam olarak kısıtlanamayacak bu prosedürlerin nasıl uygulanacağına ilişkin bilgiler verilir. Söz konusu prosedürler, süreçlere dönüştürülerek çalışanların daha kolay uygulayabileceği hale getirilir. Prosedürlerin, süreçlere dönüştürülmesi ve her zaman erişilebilecek yerlerde olması acil ve önemli olaylara karşı BGYS gerekliliklerinin yerine getirilebilmesi açısından çok önemlidir. Hızlı gelişen olaylar esnasında takip edilecek prosedür ve süreçlere erişilememesi durumlarında istenen netice alınamayacaktır.

BGYS kurulum aşamasında mobil işletmecilerin hazırlaması gereken başlıca prosedürler şunlardır:

- Bilgi Güvenliği Olay Yönetimi Prosedürü,
- İş Sürekliliği ve Acil Durum Planları,
- Veri Yedekleme Prosedürleri,
- Doğal Afet Durumu Prosedürleri,
- Güvenlik Tehditlerini Karşılama Prosedürü,
- Sistemlere Erişim Kontrol Prosedürü,
- İhbar Değerlendirme Prosedürü,
- Şebeke Güvenliği İzleme Prosedürleri,
- Soruşturma ve İzleme Prosedürü,
- Acil Durum Tahliye Prosedürü

Söz konusu yukarıda belirlenmiş prosedürlerin BGYS'nin gerçekleştirilmesi ve işletilmesi safhasında tatbik edilmesi gereklidir. Genel olarak bu prosedürlerin içeriğinde;

1. Dayanak
2. Amaç
3. Kapsam
4. Görev Ve Sorumluluklar
5. İlgili Porsedür Ya da Standart
6. Gözden Geçirme
7. Dokümanin Geçmişi
8. İlgili Dokümanlar
9. İlgili ISO/IEC 27001 Kontrolleri
10. Onay Ve Yetkilendirme
11. Dokümanın Geçmişi
12. Dokümanın Dağıtımı
13. Ekler

bölümleri bulunur.

Söz konusu prosedürler içerisinde en çok kullanılacak olan bilgi güvenliği olay yönetimi prosedürüdür. Bu prosedürün, bilgi güvenliği olaylarını müteakip düzgün olarak uygulanması ile elde edilen kayıtlar ve tecrübeler BGYS'nin işletilmesinde ve iyileştirilmesinde önemli role sahiptir. Bir bilgi güvenliği olayının yada zafiyetinin açtığı zararı en aza indirebilmek ve bu açığı kapatabilmek için bilgi güvenliği olay yönetimi prosedürünün gerektirdiği kayıtların düzgün tutulması gerekir.

Bilgi güvenliği olaylarına hızlı, etkili ve düzenli bir biçimde karşılık verebilmek için bilgi güvenliği olay yönetimi prosedürü içerisinde; yönetime ait sorumluluklara, bilgi güvenliği yönetimi birimi müdürü ve uzmanlarına ait sorumluklara, hızlı bir şekilde raporlama yapabilmek için resmi forma, raporlama prosedürü ve başvuru noktalarına, tüm personel ve üçüncü taraf çalışanlarına karşılaştıkları bilgi güvenliği olaylarını hızla bildirme konusunda yükümlü olduklarına değinilmelidir (Nazlı, 2009)

Bu prosedürlerin mobil işletmeci tarafından nasıl hazırlanacağına ilişkin bazı ipuçları taşıması adına ve model önerisinin sunduğu prosedür yaklaşımını göstermek için bu çalışmanın Ek-1'inde mobil işletmecilere yönelik örnek bir Bilgi Güvenliği Olay Yönetimi Prosedürü hazırlanmıştır. (Bkz Ek-1)

Yaşanan herhangi bir bilgi güvenliği olayı sonrasında tutulacak bilgi güvenliği olay kayıtlarda olayın;

- Tanımı,
- Yeri,
- Gerçekleşme tarihi,
- Raporlanma tarihi,
- Raporlayıcısı,
- Düzeltici eylemi,
- Yapılan işlem,
- Sınıfı,

- Bulguları,
- Öğrettikleri,
- Kök nedeni,
- Kalıcı çözümü.

Tablo haline getirilerek tutulur.

Tablo 4.1'deki bilgi güvenliği olay kayıtları bu konuda bir fikir verebilir.

Tablo 4.1 Örnek bilgi güvenliği olay kaydı

| OLAY | OLAY ZAMANI | RAPORLAMA ZAMANI | RAPOR EDEN | AÇIK/ KAPALI | AKSİYON | OLAY SINIFI | BULGU | ÖĞRETİ | OLAY YERİ | KÖK SEBEP | KALICI ÇÖZÜM |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Abonenin şifresinin alındığı iddiası | 3.12.2010 11:34 | 4.12.2010 15:00 | Hacı KAN | KAP. | Aile mensupları ve olası ilişkiler incelendi. Şikayet edilen Ali EFE ile görüşüldü. Log kayıtlarına ve e-postalara bakıldı. Simkart değişikliği itirazı nedeniyle hazırlanan Kayıp Sim Kart Talep Formu tekrar incelendi. Şifre şikayeti ve bilgi güvenliği şikayetleri abone Veli DEMİR tarafıdan değil, kızı olan ve aynı zamanda Ali EFE'nin eski nişanlısı olan Gizem DEMİR tarafından yapıldı. | Düşük | Abone şikâyeti | Bilgi güvenliği ile ilgili abone şikayetlerinde, aşağıda belirtilen süreç uygulanmasının çok daha hızlı ve obektif değerlendirme olduğu tespit edildi. 1 - Kayıtlarının incelenmesi 2 - Şahıslar arasındaki ilişkilerin incelenmesi 3 - Adli makamlara bu şahıslarla ve şikayetin sebei ilgili bu konularda intikal etmiş dosyaların inclelemesi. | Aziz Telekom Elazığ | Özel ilişkilerden kaynaklanan anlaşmazlıkların sürekli olarak var olbilme olasılığı nedeniyle, kök sebep tam net değil. | 1 - Log kayıtlarının incelenmesi 2 - Şahıslar arasındaki ailevi ilişkilerin incelenmesi 3 - Adli makamlara bu şahıslarla ve şikâyetin sebebi ile ilgili bu konularda intikal etmiş dosyaların inclelemesi. |
| Ağ altyapısı sunucu ağına 3G/GPRS üzerinden erişim sağlanabiliyor | 5.12.2010 16:12 | 9.12.2010 16:00 | Ali KÖK | KAP. | Güvenlik duvarı tercileri gözden geçirilecek ve kısıtlamalar getirilecek. | Orta | Operasyon denemeleri | Güvenlik duvarı erişimleri periyodik olarak kontrol edilmeli, | Şebeke İzleme Müdürlüğü | Yanlış güvenlik duvarı tercihleri | Güvenlik duvarı ayarları her şebeke için ayrılmalı. |
| Veritabanı Sunucusu Şifresi Bulunmayan kişilerin girişi veya tahmin edilebilir kullanıcı şifrelerini ele geçirmeleri. | 5.2.2011 16:05 | 25.2.2011 16:04 | Cem OK | KAP. | İlgili sunucular için mysql kullanıcılarına karışık-kompozit şifre verilmiştir. | Düşük | Giriş kayıtları | Komplex şifre verilmedigi durumlarda güvenlik açıklarına sebep olabilir. | Çekirdek şebeke | gerekli şifre güvenligi prosedürleri uygulanmamış. | Şifrelerin basit olmaması; sayı, harf ve noktalamalar dan oluşması. |

## 4.2 Örnek BGYS Modelinin İzlenmesi Ve Gözden Geçirilmesi

BGYS modelinin izlenmesi ve gözden geçirilmesi aşaması, kurulmuş olan BGYS'yi izlemek ve gözden geçirmek için hali hazırda uygun süreçler dizisine sahip olunup olunmadığının kontrol aşamasıdır. TS ISO/IEC 27001:2005 standardının Kontrol et aşaması Madde 4.2.3'deki kontroller; BGYS'nin izlenmesi ve gözden geçirilmesi için uygun süreçler dizisine sahip olup olmadığına yöneliktir.

İşletme BGYS'nin gerçekleştirilmesinde ve işletilmesindeki uyumsuzlukları tanımlamalı, bu uyumsuzlukların nedenlerini tespit etmeli ve uyumsuzluklarla tekrar karşılaşılmaması için gereken düzeltici önlemleri almalıdır. Bu önlemlerin öngörülen hedefin elde edilmesini sağlaması için sonuçlar kayıt altına alınır ve gözden geçirilir.

Yukarıda sayılanlara ek olarak işletme, BGYS gereksinimleriyle ortaya çıkabilecek olası uyumsuzluklar ile bu uyumsuzlukların nedenlerini tanımlamak için gerekli olan önlemleri de tespit etmelidir. Bu önlemlerin alınması ihtiyacı değerlendirilmeli ve önlem alınacaksa, önce bu önlem tanımlanmalı ve sonra da tanımlanan bu önlem alınmalıdır. Bu tür önlemlerin sonuçları, önlemlerin uygun olup olmadığı ve öngörülen hedeflerin elde edilmesini sağlayıp sağlamadığının değerlendirilmesi için kayıt altına alınmalı ve sonradan gözden geçirilmelidir (BSI, ISM04101TRTR).

Yeni teknolojilere açık mobil elektronik haberleşme hizmeti veren işletmelerde, BGYS'nin bilgi güvenliği risklerini yönetmede etkin olabilmesi için BGYS'yi etkileyebilecek tüm değişiklikleri izlemek ve izini tutmak önemlidir. Organizasyon yapısının değişmesi, operasyon alanının genişlemesi/değişmesi, yeni şebeke cihazları, yeni IT ekipmanları, yazılım güncellemeleri v.b. birçok değişiklik artık olağanlık kazanmıştır. Bu

değişiklikler, direk olarak tehdit ve zayıflığa dönüşebileceği gibi dolaylı tehdit ve zayıflıklara da yol açabilirler.

Bu aşamada, değişiklikler sonrasında BGYS kapsamı, prosedürleri, ve sorumluluklarının hala uygun, yeterli ve geçerli olup olmadıklarının sorgulaması yapılır. Yaşanan bilgi güvenliği olaylarının ele alınışı, sonuçlara yansıması, risklerin yeniden değerlendirilmesi sorgulanır.

BGYS'nin izlenmesi ve gözden geçirilmesi aşamasında aşağıdaki faaliyetler yer alır.

### 4.2.1 Prosedürlerin izlenmesi ve gözden geçirilmesi işleminin yapılması

İzleme ve gözden geçirme prosedürleri ve diğer kontroller, BGYS işletilirken ortaya çıkan hataları tespit eder, başarısız ve başarılı olan güvenlik açıklarını tanımlar, bilgi güvenliği olaylarını ortaya koyar, bilgi güvenliği ihlal olaylarını önler ve alınan önlemlerin güvenlik açıklarını giderip gidermediğini ya da işe yarayıp yaramadığını tespit eder. Bunlara ek olarak, söz konusu izleme ve gözden geçirme prosedürleri, gerçekleştirilen kontrollerin etkin olarak çalışıp çalışmadığını ve sorumluluk verilen kişilerin risk giderme planında tasarlandığı şekilde görevlerini yerine getirip getirmediklerini yönetimin tespit etmesine imkân verir. Dolayısıyla prosedürlerin istenen amaçları sağladığının kontrolü önemlidir. Bu prosedürlerden bölüm 4.1.7'de bahsedilmişti.

### 4.2.2 BGYS'nin etkinliğinin düzenli aralıklarla gözden geçirilmesi

Bu aşamada işletme, BGYS'nin ne kadar etkin çalıştığını belirler. Bu işlem, güvenlik politikaları ve hedefleri ile güvenlik kontrollerinin gözden geçirilmesi bakımından ele alınarak BGYS'nin yeterliliğinin tespitidir. Söz konusu bu gözden geçirme faaliyetlerinde, BGYS'nin etkinliğinin tespit edilmesi

sırasında tüm faktörlerin göz önüne alındığından emin olunması için güvenlik gözden geçirmeleri ve denetimlerinin sonuçları mutlaka incelenir.

BGYS'nin etkinliği konusunda tespit edilen herhangi bir uyumsuzluk ya da yetersizlik; düzeltici önlemlerin alınması, BGYS'nin çalışmasının sürdürülmesi ve geliştirilmesini durdurmak yerine teşvik edici olur. Durumun gözden geçirilmesinden sonra, bazı ilke ve işlemlerin eklenmesi/değiştirilmesi/geliştirilmesi; ya da bazı teknik kontrol önlemlerinin eklenmesi/değiştirilmesi/geliştirilmesi gerekebilir anlamı çıkar.(BSI, ISM04101TRTR)

### 4.2.3 Kontrollerin etkinliğinin ölçülmesi

Gerçekleştirilen kontrollerin etkinliğinin belirlenmesi için ortaya konulan tanımlar, kontrollerin ne kadar etkin çalıştığının ve kontrollerin düşünülen hedeflere ulaşılıp ulaşılmadığı ile tanımlanan gereksinimleri karşılayıp karşılamadığının ölçülmesi için kullanılır.

### 4.2.4 Planlanan sürelerle risk belirlemelerin gözden geçirilmesi

Bilgi güvenliği risklerinin yönetiminde etkili olmak için BGYS'yi etkileyebilecek değişiklikleri izlemek ve kaydını tutmak BGYS için önemlidir. Söz konusu gözden geçirmeler;değiştirilen iş politikası ya da değişen hedefler, işletme yapısı, işgücü, çalışma ortamı, yeni iş ortakları, yeni ve farklı ikmal zincirleri, yeni, farklı veya özellikleri değişen abone tabanı, farklı teknolojilere geçiş, pazar koşulları, üçüncü şahıs düzenlemeleri, dış kaynaklı düzenlemeler, değişen mevzuatlar,değişecek iş süreçleri ve meydana gelen ihlal olayları, yeni sistemler ve uygulamalar, güncellemeler, genişleyen iş ağları gibi meydana gelen değişikliklerden dolayı oluşacak yeni tehditleri tanımlamalıdır.

Burada sayılan değişiklik örneklerinin hepsinin risklerin üzerinde etkisi ve işletmenin işi konusunda tesiri vardır. Risklerin yeniden değerlendirilmesi, artık risk düzeyi ve kabul edilebilir risk; BGYS'nin ne kadar etkili olacağını garanti etmesi adına gereklidir.

### 4.2.5 Kuruluş içi BGYS denetimlerinin yapılması

İşletme, BGYS'nin kontrol hedeflerinin, kontrollerinin, politikalarının ve prosedürlerinin tanımlanan gereksinimlere uygun şekilde işlemesini sağlamak için BGYS iç denetimleri planlar ve yapar.

BGYS denetimleri,iç ve dış tetkikler olarak gerçekleştirilir. İç tetkikler bilgi güvenliği yönetimi birimince işletme çalışanları arasından belirlenmiş ve gerekli denetçi eğitimlerini almış denetçiler tarafından yapılır. Dış tetkikler ise bilgi güvenliği konusunda profesyonel hizmet veren firmalar tarafından, tam bağımsız bir gözle yapılır. Ayrıca hizmet alınan üçüncü taraflar da sözleşme şartları bağlamında iç denetçiler tarafından işletme adına denetlebilir.

İç BGYS denetimlerinin yapılması ISO/IEC 27001:2005'in 6'ncı maddesi gereğince bir zorunluluktur. İşletme, kontrol hedeflerinin, kontrollerin, prosedürlerin ve süreçlerin tanımlanan güvenlik gereksinimlerini karşılayıp karşılamadığını ve yürürlükteki yasal mevzuatla uyumlu olup olmadığını tespit etmek için BGYS denetimleri yapar. BGYS denetimleri sonucunda kontrollerin etkin bir biçimde gerçekleştirilip gerçekleştirilmediğini; kontrol hedeflerinin, kontrollerin, prosedürlerin ve süreçlerin beklenildiği şekilde işe yarayıp yaramadığı da ortaya çıkar.

BGYS iç denetimlerinde denetçinin tarafsız olması, dokümantasyonun ve sonuçların iyi rapor edilmesi gibi tüm denetimlerde görülen gereklilikler uygulanmalıdır.

Mobil işletmeci denetim planını her birimde yıllık en az iki denetim gerçekleştirecek şekilde planlamalıdır. Bunların haricinde gerek görülmesi halinde plansız denetimler de düzenlebilir. Ayrıca bu denetimleri gerçekleştirebilecek yeterli sayıda gerekli yeterliliğe sahip iç denetçi belirlenmelidir.

### 4.2.6 BGYS'nin yönetim gözden geçirmesinin yapılması

Yönetimin, ISO/IEC 27001 standardındaki Madde 5 ile uyumlu olarak; BGYS'nin kurulması, gerçekleştirilmesi, işletilmesi, izlenmesi ve gözden geçirilmesi, sürekliliğinin sağlanması ve iyileştirilmesinde üstlendiği süreçlerin ve faaliyetler için var olduğunu kanıtlaması gerekir. Bilgi güvenliği politikasının tesisinden başlayarak, hedeflerin belirlenmesi, rollerin ve sorumlulukların verilmesi, kaynakların BGYS için tedarik edilmesi, risk kabul ölçütüne ve kabul edilebilir risk seviyesine karar verilmesi, yönetimin gözden geçirme sürecinin uygulanması gerçek, pozitif, şeffaf destek veren bir yönetim ile olabilir.

Yönetimin, ISO/IEC 27001 standardının 7'nci maddesine göre işletmenin BGYS'yi belirlenen bir plan ve gözden geçirme programına göre incelemesi gerekir. İşletme yönetimi; Kontrol et aşaması'nda, kendi BGYS'sinin kapsamının ve kontrol sisteminin hâlâ geçerli ve etkili olduğu, prosedürlerin hâlâ geçerli olduğu ve doğru bir biçimde mevcut iş kapsamında kullanıldığı, yapılan rol ve sorumluluk paylaşımının hâlâ geçerli olduğu ve verilen güvenlik faaliyetlerinin kendilerinden beklenildiği gibi yerine getirildiği, güvenlik ihlal olayı işlem süreçlerinin uygun olduğu ve güvenlik ihlal olayı işlem süreçlerinin sonuçlarının doğru biçimde kullanıldığı ve iş süreklilik planının hâlâ geçerli olduğu konusunun gözden geçirilmesinden ve yeniden değerlendirilmesinden sorumlu olduğundan periyodik olarak yönetim gözden geçirme toplantıları yapar. Mobil elektronik haberleşme hizmeti veren işletmeler için bu süre periyodik olarak 3 ya da 6 ay olmalıdır.

Yönetim gözden geçirmelerinin girdileri olarak aşağıdaki hususlar sayılabilir:

- Yönetim gözden geçirmeleri öncesi sonuçlar,
- Önceki BGYS denetim sonuçları,
- Önceki BGYS ölçüm sonuçları,
- Önceki düzeltici eylemlerin durumu,
- Önceki risk değerlendirmesi sırasında uygunsuz olarak adreslenen (belirlenen) güvenlik sorunları,
- BGYS'ni geliştirme fırsatları,
- BGYS'ni etkileyebilecek değişiklikler.

Yönetim gözden geçirmelerinin çıktıları olarak ise aşağıdaki hususlar sayılabilir:

- İşletmenin BGYS etkinliğini iyileştirme,
- İşletmenin BGYS'ni (risk değerlendirme ve risk işleme planını) güncelleme,
- BGYS'ni etkileyen olaylara karşılık vermek için bilgi güvenliğini etkileyen prosedür ve kontrol değişiklikleri,
- İşletmenin BGYS kaynak gereksinimlerinin tespiti (TBD Kamu, 2008, Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin Uygulanmasında ISO/IEC 27001:2005).

### 4.2.7 Güvenlik planlarının güncellenmesi

İşletme, bilgi güvenliği olaylarına karşılık vermek ve güvenlik planlarını en etkin hala getirebilmek amacıyla güvenlik planlarının güncellenmesi için izleme ve gözden geçirme faaliyetlerinin sonuçlarını iyi değerlendirmelidir. İzleme ve gözden geçirme faaliyetlerinin sonuçlarını güvenlik planlarına aktarmada kullanılabilecek bir prosedür dahi belirlenebilir.

### 4.2.8 Eylemlerin ve olayların kaydedilmesi

Yönetimin gözden geçirme sonuçları, güvenlik ve işletme içi denetimleri, sistem testleri, güvenlik ihlal olayları raporları, izleme faaliyetlerinin sonuçları, bilgi sistemi sahiplerinin, yöneticilerin, kullanıcıların geri beslemeleri ve önerileri gerekli olan tüm iyileştirmelerin tanımlanmasını temin etmek için kaydedilmelidir. Bu aynı zamanda etkin bir biçimde çalışan BGYS bölümlerini göstermeye de yardımcı olmaktadır. Kayıt etme işlemine BGYS'nin iyi işlemesini sürdürmek için doğru bir biçimde sürdürülmelidir.

## 4.3 Örnek BGYS Modelinin Sürekliliğinin Sağlanması Ve İyileştirilmesi

BGYS modelinin sürekliliğinin sağlanması ve iyileştirilmesi aşaması, kurulmuş olan BGYS' yi sürdürebilmek ve iyileştirmek için hali hazırda uygun süreçler dizisine sahip olunması amacıyla tasarlanmıştır. TS ISO/IEC 27001:2005 standardının "önlem al" aşamasında Madde 4.2.4' teki kontroller; BGYS'nin iyileştirilmesine yöneliktir.

### 4.3.1 Tanımlanan iyileştirmelerin gerçekleştirilmesi

"Kontrol aşaması"nda süreçlerin izlenmesi ve gözden geçirilmesi, bilgi güvenlik risklerinin doğru biçimde yönetilmesini temin etmek için BGYS'nin iyileştirilmesini gerektiren tanımlanmış değişiklikleri önerebilir. İşletme, bu iyileştirmeleri gerçekleştirmeli ve önceki kayıtlara ve "Kontrol et aşaması"ndan edinilen geri beslemeye dayanarak bu iyileştirmeleri hayata geçirmek için gerekli diğer adımları atmalıdır.

Süreçlerin izlenmesi ve gözden geçirilmesi aşamasında ihtiyaca binaen ortaya çıkan iyileştirmelerin gerçekleştirilmesi, kontroller ve prosedürler ilk defa gerçekleştirilirken alınması gereken önlemlerden gerçekte farklı değildir. Çünkü iyileştirmeler de aslında yeni ya da yenilenmiş kontrol ve prosedürlerdir.

### 4.3.2 Uygun düzeltici ve önleyici adımların atılması

İşletme, BGYS'in etkinliğinin sürekli geliştirilmesinin nasıl mümkün olacağına dair çeşitli prosedürler hazırlar. Bu prosedürler, olaylardan, denetimlerden ve kontrollerden yola çıkılarak iyileştirici adımlara ve bu adımları sisteme dahil edici kararların nasıl alınacağına dair rehber dokümanlardır. Bir başka deyişle, bu prosedürler kümesi, denetim ve gözden geçirmelerin sonuçlarının kullanılmasını, izleme faaliyetlerinin ve ihlal olaylarının analizini kapsayacaktır. Düzeltici ve koruyucu önlemler, BGYS'nin gerçekleştirilmesi ve işleyişindeki herhangi bir uyumsuzluğu ortadan kaldırmak ve uyumsuzlukların tekrar yaşanmaması için alınmalıdır.

İşletmenin, olup bitenden ders almaya ihtiyacı vardır. Ayrıca diğer kuruluşların deneyimlerinden, eğilim analizlerinden ya da işletmenin erişebileceği veya erişmek isteyebileceği başka bilgi kaynaklarından da faydalanılabilir(BSI, ISM04101TRTR).

Bilindiği gibi iç ve dış denetimlerde tespit edilen bulgular, bilgi güvenliği olay kayıtlarındaki olaylar ve diğer tüm bilgi güvenliğini ilgilendiren yaşanmış tecrübeler kayıt altına alınmaktadır. Bu kayıtların hemen yanı başına açılacak bir iyileştirme önerisi ve kök sebep çözümü sütunu iyileştirme süreçleri işletilebilir. Buradan hareketle denilebilir ki işleyen bir BGYS devamlı kendini geliştirir ve zamanla daha da güvenilir olur.

### 4.3.3 İlgili tüm tarafların eylemlerinden ve iyileştirmelerinden haberdar olunması

Buradaki önemli husus; düzeltici ve koruyucu tüm eylemlerin kaydedilmesi ve uygun iletişim kanalları ile, BGYS iyileştirme sonuçlarının işletmedeki doğru kişilere aktarıldığından ve gerçekleşen eylemlerin gerçekten bu sürecin bir sonucu olarak ortaya çıktığından emin olunmasıdır. Söz konusu olan yalnızca işletme çalışanları değildir, aynı zamanda üçüncü taraf yükleniciler veya bu iyileştirmelerden etkilenebilecek başka taraflar da olabilir ve

günümüzde, değişen politikalar, prosedürler ve denetimlerle de uyumlu olmasına ihtiyaç vardır.

İyileştirmelerin ardından yapılmasına ihtiyaç duyulan tüm değişiklikler, revize edilen dokümanlara yansır ve gerek duyulursa ayrı bir bildirim şeklinde ilgili kişilere duyrulur.

### 4.3.4 İyileştirmelerin tasarlanan hedefleri sağlayacağında emin olunması

İşletme, gerçekleştirilen geliştirmelerin istenilen gereksinimleri karşılamasını ve elde edilmesi düşünülen hedeflere ulaşılmasını temin etmelidir. Bu husus, alınan düzeltici ve koruyucu önlemlerin gözden geçirilmesini içerir.

BGYS süreçlerinin ve kontrollerinin etkinliğinin ölçülmesi için düşünülen metrik ölçü birimleri ile ölçümler iyileştirmelerin başarısının belirlenmesine yardımcı olabilir ve işletmenin sonraki dönemlerde risk yönetiminde kaydettiği gelişmenin belgelenmesinde de kullanılabilir (BSI, ISM04101TRTR).

## SONUÇ VE ÖNERİLER

Bu çalışmada, 2N ve 3N mobil haberleşme şebekelerini işleten işletmeciler için model bir BGYS kurulmuş ve işletilmiştir. Kurulacak sistemin, mobil işletmecinin sadece BT ya da IT ekipmanları veya bölümü için değil tüm faaliyet alanını kapsaması gerekmektedir.

Model oluşturulurken, BGYS için yönetimin kararlılığı ve sistemi kuracak BGY biriminin oluşturulmasının önemi anlaşılmıştır. BGYS'de varlık kayıtlarının oluşturulmasının esas olduğu ve bu kayıtlar üzerinden varlık sahiplerinin atanması gerektiği görülmüştür.

Mobil işletmecilerin varlık çeşitlerinin fazlalığı varlıkları sınıflandırma ihtiyacını doğurmuştur. Bu sınıflandırma, varlıkların haberleşme şebekesi ile doğrudan ve dolaylı olmasına göre gerçekleştirilmiştir. Sonrasında bu varlıkları bekleyen tehditler ve riskler örnekleme yoluyla tanımlanmış, gerekli düzeltici ve önleyici eylem önerileri geliştirilmiştir. Şebeke ile doğrudan ilgili varlıklar için alınacak tedbirler içerisinde kriptolama, algoritma kulanımı ile sanal erişimi önleme öne çıkarken diğer varlıklar için şifre kullanımı ve yönetimi ile fiziksel güvenlik tedbirlerinin öne çıktığı görülmüştür.

Tüm bunlar yapılırken dokümantasyon ve kayıtların BGYS içinde önemli bir yer tuttuğu anlaşılmış ve BGYS için ISO 27000 ailesi bilgi güvenliği standartlarından faydalanılabileceği görülmüştür.

İşletmecinin BGYS'yi kurmuş olmasının tek başına bir faydasının olmadığı, kurulan sistemin PUKÖ döngüsünde olduğu gibi işletilerek, gözden geçirilerek ve iyileştirilerek canlı tutulması gerektiği sonucuna varılmıştır.

Sonuç olarak bu çalışma kapsamında yapılan mobil haberleşme sektörü ve bilgi güvenliği standartları incelemeleri ile elde edilen sonuçlar dikkate alınarak, mobil işletmecilerde BGYS ile ilgili olarak geliştirilen öneriler aşağıda yer almaktadır.

**BGYS kurulum aşamasında:**

- *Yönetime düşen görev:* İşletme içerisindeki yönetim seviyeleri stratejik, taktik ve operasyonel seviyeler olmak üzere üç seviyede ele alındığında stratejik seviyede işletmenin üst düzey yöneticisi (CEO), taktik seviyede orta seviye yöneticileri (birim yöneticileri) ve operasyonel seviye de alt seviye yöneticileri (bilgi güvenliği yönetimi birimi) yer alır. Bu yönetim kademeleri, "yönlendir" ve "kontrol et" aktivitelerini yürütür.

  En üst seviyede yönlendirme yapılmalıdır. Bilgi güvenliği ile ilgili stratejileri CEO belirlemeli, söz konusu stratejileri bir alt seviyedeki birim yöneticilerine bildirmeli ve yerine getirilmesi için direktif vermelidir. Taktik seviyedeki bu yöneticiler, söz konusu direktifleri politika ve kurumsal standart haline getirmelidir. BGY birimi ise bu politika ve standartlara göre prosedürleri hazırlamalıdır.

  Kontrol etme aşamasında ise operasyonel seviyede işlemlerin prosedürlere göre yapılıp yapılmadığı BGY birimi tarafından, prosedürlerin politika ve standartlara uyumluluğu orta seviye yönetim tarafından kontrol edilmelidir. İlgili direktiflerin ne derece yerine getirildiği ve politikaların stratejilerle ne derece uyumlu olduğunun da üst düzey yönetici tarafından kontrol edilmesinin faydalı olacağı değerlendirilmektedir.

- *Bilgi Güvenliği Yönetimi Birimi Oluşturulması:* Bilgi güvenliği faaliyetlerini yürütmek üzere bizzat üst yönetim tarafından oluşturulmasına karar verilen ve bu konuda yetkilendirilen, BGYS'nin kurulmasını ve

yönetilmesini üstlenecek bir birim oluşturulmalıdır. Bu birim, risk yönetimi, politika oluşturma, güvenlik prosedürlerinin hazırlanması ve uygun kontrollerin seçilerek uygulanması gibi çalışmaları yapacağından birim yöneticisi ve üyeleri, bilgi güvenliği yönetimi konusunda eğitimli/deneyimli olmalıdır. Alınması tavsiye edilen eğitimlere her kademe için ayrı ayrı olarak Bölüm 4.1.2.' de değinilmiştir.

Çalışma içerisinde BGY birimi; yöneticisinin, grup liderlerinin ve uzmanlarının görev tanımları yapılmıştır. (Bkz Bölüm 3.2.)

Orta büyüklükte ulusal çaptaki bir mobil işletmecinin BGY biriminde; sistemin kurulumu ve sonrasında işletecek, iç ve dış denetimlerde görev yapacak, düzeltici eylemleri takip edecek, işletme personellerine farkındalık eğitimleri verecek, bilgi güvenliği kayıtlarını tutacak ve güncelleyecek yeterli sayıda tam zamanlı bilgi güvenliği uzmanı görev yapmalıdır.

- *BGYS Politikası:* BGYS için temel ilkeleri barındıran en üst düzey doküman olan BGYS politikası, elektronik ortamda kurumsal internet sayfasında ve dokümante edilmiş olarak her birim içersinde erişilebilir olmalıdır. Uzun olması halinde okunmasında ihmaller yaşanabileceğinden kısa olmasında fayda vardır. Mobil işletmeciler için tavsiye edilebilecek uzunluk 3-10 sayfa aralığıdır.

  Politika dokümanı içerisinde yer almasında fayda olduğu değerlendirilen temel ilkeler, bu çalışmanın "BGYS Politikası" başlıklı Bölüm 3.3.'te verilmiştir. Politika dokümanında diğer başka ilgili politikalara, standartlara, prosedürlere ve talimatlara atıflarda bulunularak bu dokümanlar desteklenmelidir.

  Bilgi güvenliği yönetim gözden geçirme komitesi, politikayı periyodik olarak (3 ya da 6 ay) gözden geçirmeli, onaylamalı, BGYS ile ilgili stratejik kararları almalıdır.

*Risk Değerlendirme:* Hangi tehditlerin ne gibi riskler taşıdığını analiz edebilmek için bilgi varlıkları dahil olmak üzere tüm varlıkların envanterinin çıkarılması ve sınıflandırılarak değerlendirilmesi gerekmektedir. Bu işlemin yapılmasında Tablo 3.1'in kullanılması önerilmektedir. Varlık envanteri oluşturulurken mobil işletme varlıkları:

- Radyo Erişim Şebekesi (RAN)
- Transmisyon Şebekesi
- Şebeke Anahtarlama Sistemi ( NSS )
- Operasyon ve Destek Sistemleri

şebeke ile ilgili varlıkları ve

- IT varlıkları
- Katma değerli Servisler (VAS)
- Çağrı Merkezleri
- Kişiye Tahsisli Varlıklar

şebeke dışı varlıklar olmak üzere gruplandırılabilir.

Radyo erişim şebekesi, transmisyon şebekesi, şebeke anahtarlama sistemi ve IT varlıkları haberleşmenin gizliliği, bütünlüğü, erişilebilirliği ve sürekliliği açısından mobil işletmeciler için kritik varlıklar olduğundan, bu varlıklardan başlıcalarının varlık değerleri yüksek (4-5 / 5) olarak tayin edilmelidir.

Risk değerlendirmede, risklerin yeniden değerlendirilmesi, tehditlerin, zayıflıkların ve varlıkların güncellenmesi gereken birçok durumda, bir yazılım aracının kullanılmasında faydalar olabilir.

- *Risk Belirleme:* Risk belirleme çalışmalarına birim/bölüm yöneticileri, CIO CFO, Bilgi Sistemleri Yöneticisi, İnsan Kaynakları Yöneticisi, Bilgi Güvenliği Yönetimi Birimi Yöneticisi gibi yönetici grubun katılmasında fayda vardır. Şebeke, insan kaynakları, finans, IT ve diğer önemli varlıklar işe yaptıkları etkiye göre belirlenmeli ve sınıflandırılmalıdır. Varlıkları bekleyen tehditler, gerçek olma ihtimali ve oluşturduğu risklerin belirlenmesi gerekir.

- *Risk Analizi ve Derecelendirilmesi:* Tespit edilen riskler, işletme ve mobil haberleşme şebekesi hakkında detaylı bilgiye sahip, faaliyetlerin devamlılığı için sorumlulukları olan orta seviye yöneticilerle ve çalışanlarla birlikte detaylı incelenerek analiz edilmelidir.

  Tehdidin tahmini gerçekleşme ihtimali 1'den 5'e düşük ve yüksek ihtimal, tehdidin işletme işleyişinde oluşturacağı muhtemel olumsuz etki 1'den 5'e düşük ve yüksek olumsuzluk olmak üzere derecelendirildiğinde bunların çarpılması ile hesaplanan risk değeri 1'den 25'e kadar olan değerler ile ifade edilmelidir.(Bkz Tablo 3.11.) BGYS modelinde risk değerlerinin:

  [1,4] aralığı risk değeri: Düşük
  [5,9] aralığı risk değeri: Orta
  [10,25] aralığı risk değeri: Yüksek

  olarak kabul edilmesi önerilmektedir.

- *Risk İşleme:* Daha önceden hazırlanmış risk kayıtlarında yer alan numaralanmış ve sahibi belirlenmiş riskler için tedbirler belirlenmelidir. Bu tedbir kararları; birim amirleri, orta seviye yönetici ve çalışanlarla birlikte yapılacak bir çalışma ile alınır. Örneğin çağrı merkezi için; üst düzey bir yönetici (CEO ya da Genel Müdür yardımcısı gibi), ÇM yöneticisi, BGYS

yöneticisi, sorumlu teknik personel, koordinatör müşteri hizmetleri temsilcisi ve bazı müşteri hizmetleri temsilcileri olabilir.

- *Kontrollerin Seçimi:* Kontrol maddelerinin seçiminde ISO/IEC 27001:2005 Ek-A'da yer alan 133 kontrol maddesinden uygulanabilir olanlar ve özellikle ISO 27011:2008 standardındaki elektronik haberleşme sektörüne altyapı ve servislerde güvenliği sağlamaya yönelik yeni kontroller tavsiye edilmiştir.

- *Kabul Edilebilir Risk Düzeyi:* Model önerimizde kabul edilebilir risk düzeyi (KERD), risk değerlerinin belirlendiği tabloda düşük risk aralığında değerlendirilen "[1,3]" olarak belirlenmiştir. "[1,3]" risk değerinden daha yüksek risk değerine sahip riskler, eğer;

  - Düşük risk [3,4] düzeyinde ise, en az önlem alınarak ve zaman harcanarak KERD'e indirilir.
  - Orta risk [5,9] düzeyinde ise, daha fazla önlem ve zaman harcanarak KERD'e indirilir.
  - Yüksek risk [10,25] düzeyinde ise işletme kaynak ayırarak ve çözüm arayışına girerek KERD'e indirilir.
  - Kabul edilebilir risk düzeyinde ise alınan önlemler sürdürülür.

**BGYS'nin gerçekleştirilmesi ve işletilmesi aşamasında:**

- *BGYS Bütçesi:* BGYS modeli oluşturulurken ele alınan ölçek, 20 milyon abonesi ve yıllık 5 milyar dolar net satışı olduğu varsayılan orta büyüklükte ulusal çaptaki bir mobil işletmeci ölçeğidir. Bu büyüklükteki bir işletmecinin ayırdığı BGYS bütçesi; tüm personele verilecek eğitimler, BGY birimi uzmanlarına aldırılacak eğitimler, iç ve dış denetimler ile düzeltici eylemleri gerçekleştirebilecek düzeyde olmalıdır. Söz konusu

BGYS bütçesi, BGY Birimi tarafından teklif edilmeli ve en üst düzey yönetim seviyesinde (CEO ya da Genel Müdür) onaylanmalıdır.

- *Eğitimler:* İşletmeci, BGYS sorumlulukları olan personelin verilen görevleri yerine getirme konusunda yeterli olmalarını sağlamak için farkındalık ve eğitim programı uygulamalıdır. Eğitimlerde verilmesi amaçlanan bilgi ya da farkındalığın, ne kadar kazanıldığı ölçücü testler ile ölçülmeli ve geçme barajı tayin edilmelidir.

  En azından tüm çalışanlar, Bilgi Güvenliği Farkındalık Eğitimi ve Bilgi Güvenliği Olay Müdahale Eğitimi almalıdırlar. BGY birimi içerisinde görev yapan ve bu konuda uzmanlık kazanması istenen kişilere ise; Bilgi Güvenliği Temelleri Eğitimi, Bilgi Güvenliği Risk Analizi Eğitimi, Saldırı Teknikleri ve Araçları Eğitimi, Windows (işletim sistemi) Güvenliği Eğitimi ve İç Denetçi Eğitimi aldırılmasında fayda vardır.

  Tüm bu eğitimlerin tek bir kez alınması yeterli olmayacaktır. Konuya ilişkin tazeliğin korunması için tazeleme eğitimleri yapılması da şarttır. Söz konusu tazeleme eğitimlerinin periyodu, çok özel eğitimler dışında 6 ay ya da 1 bir yıl olarak tercih edilebilir.

- *Farkındalık Artırıcı Eylemler:* Bilgi güvenliği bilincinin tazeliğini sürdürebilmesi için çalışanlara yönelik eylemler düşünülmelidir. Örneğin her ay işletme iç ağı üzerinden yapılacak ödüllü bir test, periyodik bir BGYS bülteni, gizlilik derecelerinin üzerinde yazılı olduğu bir takvim ya da Mouse pad, şifreli kullanımı tavsiye edici resimler, bilgi güvenliğinin karikatürize edildiği duvar afişleri v.b. farkındalığı artırıcı eylemler olarak önerilmektedir.

- *Olay Yönetim Prosedürleri:* BGYS'nin gerçekleştirilmesi ve işletilmesi safhasında tatbik edilecek prosedürlerin neler olduğu ve içerikleri bölüm 4.1.7.'de verilmiştir.

Yine 4.1.7.'de bu prosedürlerin mobil işletmeci tarafından nasıl hazırlanacağına ilişkin bazı ipuçları taşıması adına ve model önerisinin sunduğu prosedür yaklaşımını göstermek için mobil işletmecilere yönelik örnek bir Bilgi Güvenliği Olay Yönetimi Prosedürü (Bkz Ek-1) hazırlanmıştır. Buna ilave olarak örnek bilgi güvenliği olay kayıtları (Bkz Tablo 4.1.) hazırlanmıştır. Prosedürlerin hazırlanmasında ve olayların kayıt altına alınmasında bu örneklerden faydalanılması önerilmektedir.

**BGYS'nin izlenmesi ve gözden geçirilmesi aşamasında:**

- *İşletmede BGYS Denetimlerinin Yapılması:* İç tetkikler BGY birimince işletme çalışanları arasından belirlenmiş ve gerekli denetçi eğitimlerini almış denetçiler tarafından yapılmalıdır. Dış tetkikler ise bilgi güvenliği konusunda profesyonel hizmet veren firmalara yaptırılmalıdır. Ayrıca hizmet alınan üçüncü taraflar da sözleşme şartları bağlamında iç denetçiler tarafından işletme adına denetlenmelidir.

  Mobil işletmeci denetim planını her birimde yıllık en az iki denetim gerçekleştirecek şekilde planlamalıdır. Bunların haricinde gerek görülmesi halinde plansız denetimler de düzenlebilir. Tabii ki bu denetimleri gerçekleştirebilecek yeterli sayıda iç denetçi belirlenmelidir.

- *BGYS'nin yönetim gözden geçirmesinin yapılması:* İşletme üst yönetiminin, BGYS'sinin gözden geçirilmesinden ve yeniden değerlendirilmesinden sorumlu olduğundan periyodik olarak yönetim gözden geçirme toplantılarını yapması gerekir. Mobil elektronik haberleşme hizmeti veren işletmeler için bu süre periyodik olarak 3 ya da 6 ay olmalıdır. Bu toplantılara asgaride CEO, birim yöneticileri ve BGY birimi yöneticisi mutlaka katılmalıdır.

**BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi aşamasında:**

- *Uygun düzeltici ve önleyici adımlar:* İşletmeci, BGYS'in etkinliğinin sürekli geliştirilmesinin nasıl mümkün olacağına dair çeşitli prosedürler hazırlamalıdır. Bu prosedürler kümesi; denetim ve gözden geçirmelerin sonuçlarının kullanılmasını, izleme faaliyetlerinin ve ihlal olaylarının analizini kapsamalıdır. BGYS'nin gerçekleştirilmesi ve işleyişindeki herhangi bir uyumsuzluğu ortadan kaldırmak ve uyumsuzlukların tekrar yaşanmaması için düzeltici ve koruyucu önlemlerin alınmasının faydalı olacağı değerlendirilmektedir.

- *İlgili tarafların eylemlerden ve iyileştirmelerden haberdar edilmesi:* Değişen politikalar, prosedürler ve denetimlerle de uyumlu olması açısından düzeltici ve koruyucu tüm eylemlerin kaydedilmesi ve uygun iletişim kanalları ile, yalnızca işletme çalışanlarına değil, aynı zamanda üçüncü taraf yüklenicilere veya varsa bu iyileştirmelerden etkilenebilecek başka taraflara da bildirilmesinin faydalı olacağı değerlendirilmektedir.

# KAYNAKLAR


Ad-net, 2005, http://www.ad-net.com.tw/index.php?id=402, (9.10.2010).

ALPAR Cengiz Idris, 2011, Bilgi Güvenligi Yönetim Sistemi ISO 27001, http://www.cio-club.net/Makaleler/PDF/Kalite_Yolculugu_Mart.pdf (21.3.2011).

ATASOY Kenan, 2006, GSM Sistemi ve Sağlık, Fen Edebiyat Falültesi Fizik Bölümü Araştırma Projesi, Gazi Üniversitesi, Ankara,s.5.

BAĞCI Barış, Bilgi Teknolojileri Risk Yönetimine Genel Bakış, Deloitte Touche Tohmatsu, 2008.

Bilgi Güvenliğinde ISO 27000 Standartlarının Yeri ve Öncelikli ISO 27002 Kontrolleri, 2009, http://fentanyl.wordpress.com/2009/01/15/bilgi-guvenliginde-iso-27000-standartlarinin-yeri-ve-oncelikli-iso-27002-kontrolleri/ (25.11.2010).

BSI, ISM04101TRTR, 24(3):2, s.1-41, 2010.

BTK, 2007,Haberleşmenin Güvenliği, Teknik Düzenleme Ve Standardizasyon Dairesi Başkanlığı, Ankara.

BTK, 2008, Elektronik Haberleşme Güvenliği Yönetmeliği, BTK Düzenlemeler/Yönetmelikler Sayfası, http://www.btk.gov.tr/Duzenlemeler/Hukuki/yonetmelikler/Yonetmelikler.htm,(11.09.2010).

BTK, 2011, Elektronik Haberleşme Güvenliği Kapsamında TS ISO/IEC 27001 Standardı Uygulamasına İlişkin Tebliğ'de Değişiklik Yapılmasına Dair Tebliğ, BTK Düzenlemeler/Tebliğler Sayfası, http://www.btk.gov.tr/Duzenlemeler/Hukuki/tebligler/Tebligler.htm,(24.4.2010).

EZBER Pelin, 2010a, ISO 27011 – ISO27001 Temelleri ve Ana Kontrol Alanları,http://www.adeosecurity.com/standardizasyon/iso27001-temelleri-ve-ana-kontrol-alanlari/ (21.4.2011).

EZBER Pelin, 2010b, ISO 27011 – Telekom Sektörüne Özel Güvenlik Standardı,http://www.adeosecurity.com/standardizasyon/iso-27011-telekom-sektorune-ozel-guvenlik-standardi/ (21.4.2011).

ISO 27001-BGYS Bilgi Güvenliği Portalı, ISO 27000 Ailesi, http://www.iso27001-bgys.com/iso-27000/iso-27000-ailesi.html(25.4.2011).

ISO, 2005, ISO/IEC 27001:2005, Information technology -- Security techniques -- Information security management systems – Requirements, International Organization for Standardization, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103, (17.9.2010).

ISO, 2008, ISO/IEC 27011:2008, Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002,http://www.iso.org/iso/search.htm?qt=27011%3A2008&searchSubmit=Search&sort=rel&type=simple&published=on, (17.9.2010).

IŞIK Ali Hakan, ÇETİN Gürcan, 2007, Yeni Nesil Operasyon Destek Sistemleri,Bilisim Enstitüsü Elektronik ve Bilgisayar Egitimi Anabilim Dalı, Gazi Üniversitesi, Ankara, s.2-4.

IT Governance Ltd, Information Security and ISO27001 – An Introduction, s.1-5, 2006.

Jean-Poul Linnartz, 2009,GSM Network Architecture http://www.wireless.per.nl/reference/chaptr01/telephon/gsm/gsmnetw.htm (11.2.2011).

KARABACAK Bilge, ISO/IEC 27001:2005 ve Bilgi Güvenliği Yönetişimi - Türkiye Analizi, TÜBİTAK-UEKAE, 2008.

Karel, 2005, Türk Telekom Projeleri, http://www.karel.com.tr/karel/karel_telecommunication.jsp, (10.10.2011).

KOÇ Fatih, BGYS - Varlık Envanteri Oluşturma Ve Sınıflandırma Kılavuzu, TÜBİTAK-UEKAE, 2008.

MOBİLSAD, 2011, Mobil Katma Değerli Servis Nedir, http://www.mobiltuketici.com/tuketici-rehberi/sss#,

(9.1.2011).

Netmon.com.tr, 2008, DWDM, http://www.netmon.com.tr/index.php/tr/coezuemler/telekomuenikasyon/dwdm.html, (15/2/2011)

NAZLI Mikail, 2009, Bilgi Güvenliği Olay Yönetimi http://www.mikailnazli.com, (8/9/2010).

OTTEKİN Fikret, TS ISO/IEC 27001 Denetim Listesi, TÜBİTAK-UEKAE, 2008.

ÖNEL Dinçel, DİNÇKAN Ali, Bilgi Güvenliği Yönetim Sistemi Kurulumu, TÜBİTAK-UEKAE, 2007.

ÖZTÜRK Günce, Bilgi Güvenliği Politikası Oluşturma Kılavuzu, TÜBİTAK-UEKAE, 2008.

POSTHUMUSA S., SOLMS R., 2005, IT Oversight: An Important Function of Corporate Governance, Computer Fraud & Security, s.11-17.

SCOTT B, Writing Information Security Policies, New Riders Publishing, 2001.

SOLM V. S., SOLMS B., Information Security Governance: A Model Based on the Direct-Control Cycle, s.408-413, 2006.

TAŞKIN Erman, 2011, ISO 27001 Projesi BGYS Takımı Oluşturma, http://educore.info/2011/02/05/iso-27001-projesi-bgys-takimi-olusturma/ (20.3.2011).

TBD Kamu, 2008, BİB Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin Uygulanmasında ISO/IEC 27001:2005, Kamu Bilişim Platformu X.

The Fiber Optic Association, 2003, http://www.thefoa.org/tech/dwdm.htm,(9.10.2010).

The Importance of Setting up an Information Security Management Committee in Organization http:// www.cybersecurity.my/data/content_files/11/29.pdf

TSE, 2006, TS ISO/IEC 27001 Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler, Ankara.

Wifi-Turk.com, 2009, GSM Şebeke Yapısı, http://www.wifi-

turk.com/forum/lofiversion/index.php?t2576.html, (14.1.2011).

Wiki GSM, 2011, Network structure,http://wapedia.mobi/en/GSM (12.2.2011).

Yönetimonline, 2009, Bilgi Güvenliği Yönetim Sistemi Kurmak , http://www.yonetimonline.com/iso-27001-bilgi-guvenligi/635-Bilgi-Guvenligi-Yonetim-Sistemi-Kurmak.html, (15.4.2011).

JET, 2010, Jet Repeater, http://www.jet.com.tr/repeater, (5.1.2011).

# EKLER

## Ek-1: Örnek Bilgi Güvenliği Olay Yönetimi Prosedürü

## BİLGİ GÜVENLİĞİ OLAY YÖNETİMİ PROSEDÜRÜ

### 1 DAYANAK

1.1. Bu prosedür Bilgi Güvenliği Politikası'na dayanılarak hazırlanmıştır.

### 2 AMAÇ

2.1 Bu prosedürün amacı, bilgi sistemleri ve diğer tüm iş bölümlerinde tespit edilen bilgi güvenliği olaylarının ve açıklıklarının bildirilmesi, tedbir alınması, incelenmesi ve kayıtlarının tutulması hususlarında işletmeci, çalışanlarına ve üçüncü taraf firma çalışanlarına düşen görev ve sorumlulukları tanımlamaktır.

### 3 KAPSAM

3.1 Bu prosedür, işletmeye ait bilgi sistemleri ve diğer tüm iş bölümleri ile ilgili veya bunları olumsuz etkileyebilecek bütün güvenlik olaylarını,kırılmları ve açıklıkları kapsar.

### 4 GÖREV VE SORUMLULUKLAR

4.1 Bilgi Güvenliği Yönetimi Üst Komitesi,

Bilgi güvenliği olayı raporlarının gözden geçirilmesinden ve ilgili koruyucu ve düzeltici eylemlere kaynak sağlamaktan sorumludur.

4.2 Bilgi Güvenliği Yönetimi Müdürü,
Bilgi Güvenliği Olay Yönetimi Prosedürü'nın güncellenmesinden sorumludur.

Rapor edilen tüm bilgi güvenliği olaylarının kayıtlanması, izlenmesi ve sonuçlandırılmasından sorumludur.

Bilgi güvenliği olaylarının değerlendirilmesi sonucunda elde edilen verilerin; güvenlik faaliyetlerinin beklenen biçimde çalışması, gerekli güvenlik önlemlerinin alınarak güvenlik ihlallerinin önlenmesi, bir güvenlik kırılmasını önlemek için alınan önlemlerin etkisini artırması için kullanılmasını temin eder.

Gerekli iş paylaşımını yapar, düzeltici eylem ve kontrolleri onaylar, koordine eder.
Bilgi güvenliği olayının kapatılmasında son karar vericidir.

4.3 BGYS Uzmanı,
Olayın bir bilgi güvenliği olayı olup olmadığını tespit eder
Olay, bir bilgi güvenliği olayı ise, Bilgi Güvenliği Yönetimi Müdürü'ne olayı ve etkilerini bildirir.
Bilgi Güvenliği Yönetimi Müdürü'nün onay vermesi halinde gerekli eylemleri başlatır ve takip eder.
Olayı ve sonrasındaki bütün eylemleri önce kayıt altına alır sonar analiz eder.

Bilgi güvenliği olayının neticelenmesini ve kapatılmasını izler.

Geçmiş bilgi güvenliği olaylarından sağlanan tecrübe ile olayların tekrarlanmaması veya büyük hasar meydana getirmemesi için koruyucu ve önleyici eylemler belirler.

4.4 Sistem/Şebeke Sorumluları ve Yöneticileri,
Yaşanan bilgi güvenliği olaylarını ve kendilerine bağlı çalışanlarca ulaştırılan formları rapor ederler.

Bilgi Güvenliği Yönetim Müdürü'nün görevlendirmesi halinde ilgili düzeltici eylemleri yürütürler.

Monitoring/İzleme Prosedürü gereğince sistemlerini herhangi bir bilgi güvenliği olayı ihtimaline karşı izlerler.

Olayla ilgili delilleri toplar, muhafaza edir, kayıt altına alır ve Bilgi Güvenliği Yönetim Müdürü'ne iletirler.

4.5 Bilgiye erişebilen çalışanlar,
Yaşanan bilgi güvenliği olaylarını rapor ederler. Olayı raporlayabilecekleri form işletme iç ağında yer almaktadır.

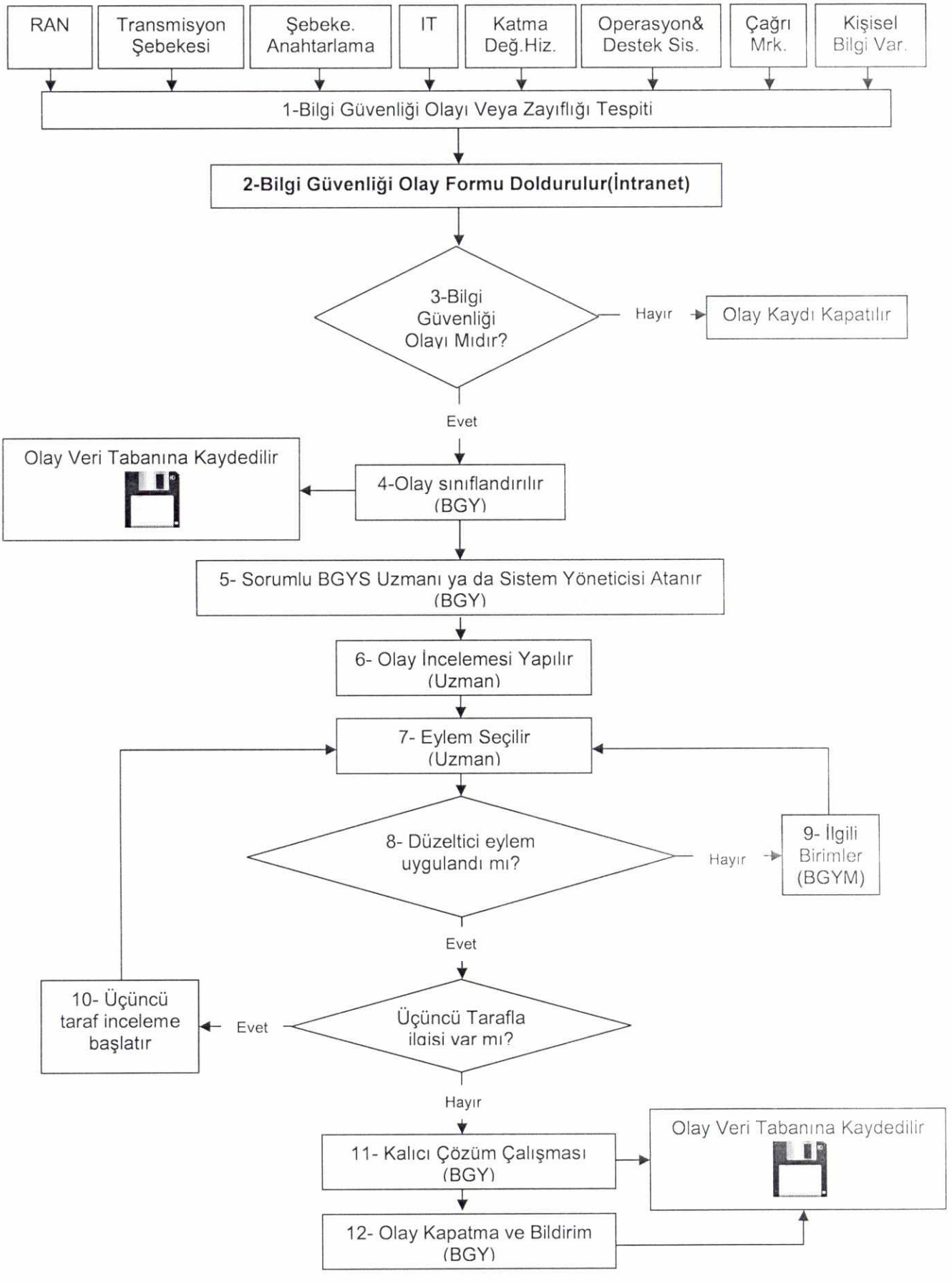
Herhangi bir bilgi güvenliği olayı yaşanması durumunda birimlerinde başvurabilecekleri yetkin kişileri bilmeleri gerekir. Bu kişiler, işletme intranettinde ve ilan panolarında ilan edilmiştir.

Rapor ettikleri bilgi güvenliği olayları ile ilgili düzeltici ve koruyucu eylemleri dışarıdan takip ederler.

## 5 BİLGİ GÜVENLİĞİ OLAY YÖNETİMİ PROSEDÜRÜ

5.1 Bilgi Güvenliği Olay Yönetimi Prosedürü aşağıdaki süreci takip eder:

5.2. Süreç Akışı


RAN
Transmisyon Şebekesi
Şebeke. Anahtarlama
IT
Katma Değ.Hiz.
Operasyon& Destek Sis.
Çağrı Mrk.
Kişisel Bilgi Var.
1-Bilgi Güvenliği Olayı Veya Zayıflığı Tespiti
2-Bilgi Güvenliği Olay Formu Doldurulur(İntranet)
3-Bilgi Güvenliği Olayı Mıdır?
Hayır
Olay Kaydı Kapatılır
Evet
Olay Veri Tabanına Kaydedilir
4-Olay sınıflandırılır (BGY)
5- Sorumlu BGYS Uzmanı ya da Sistem Yöneticisi Atanır (BGY)
6- Olay İncelemesi Yapılır (Uzman)
7- Eylem Seçilir (Uzman)
8- Düzeltici eylem uygulandı mı?
Hayır
9- İlgili Birimler (BGYM)
Evet
10- Üçüncü taraf inceleme başlatır
Evet
Üçüncü Tarafla ilgisi var mı?
Hayır
11- Kalıcı Çözüm Çalışması (BGY)
Olay Veri Tabanına Kaydedilir
12- Olay Kapatma ve Bildirim (BGY)

5.3. Süreç Adımları

1) Bilgi güvenliği olayı veya zayıflığı tespiti: Her departmanda, rutin izleme olaylarında yada beklenmedik şekillerde bilgi güvenliği olayları (Suiistimal, suç, uygunsuzluk, etik olmayan davranışlar ve firmalar arası fraud) ortaya çıkabilir.
2) Bilgi güvenliği olay formunun doldurulması: Tespit edilen bilgi güvenliği olayı, tespit eden kişice elektronik yada basılı ortamdaki bilgi güvenliği olayı formuna doldurularak rapor edilir.
3) Bilgi güvenliği olayı karar aşaması: Sorumlu bilgi güvenliği uzmanı yada şebeke/IT sorumlusu rapor edilen olayı değerlendirir ve bunun bir güvenlik olayı olup olmadığına karar verir. Eğer bir güvenlik olayı olduğuna karar verilirse, Bilgi Güvenliği Yönetimi Müdürü'ne iletilir.
4) Olayın sınıflandırılması: Sorumlu bilgi güvenliği uzmanı yada şebeke/IT sorumlusu güvenlik olaylarını DÜŞÜK, ORTA veya YÜKSEK olarak sınıflandırır. Bilgi Güvenliği Olaylarının sınıflandırılmasında aşağıda belirtilen kriterler dikkate alınmalıdır:

- Düşük: İşleyişi kesintiye uğratmayacak, abone veya üçüncü taraflarla ilişkilerin düşük seviyede etkilenebileceği veya hiç etkilenmeyeceği olaylardır.
  Müdahale Süresi: 1 İş günü
  Çözüm Süresi: 20 İş günü

- Orta: İşleyişi kesintiye uğratabilecek, abone veya üçüncü taraflarla ilişkilerin orta seviye de etkilenebileceği olaylardır.
  Müdahale Süresi: 1 İş günü
  Çözüm Süresi: 10 İş günü

- Yüksek: Verilen mobil elektronik haberleşme hizmetini, İşletme marka ve imajını, gelir/giderleri direk veya dolaylı olarak

etkileyecek olaylardır. Bu tür olaylar, en öncelikle incelenmeli ve en hızlı şekilde çözümlenmelidir.
Müdahale Süresi: 1 İş günü
Çözüm Süresi: 3 İş günü

5) Sorumlu BGYS Uzmanı ya da Sistem Yöneticisi Atanması:Bilgi güvenliği yönetimi müdürü tarafından güvenlik olaylarını araştırmak, koordine etmek ve çözmek üzere Sorumlu bilgi güvenliği uzmanı yada şebeke/IT sorumlusu atanır.
6) Olay İncelemesinin Yapılması: Görevlendirilmiş sorumlu bilgi güvenliği uzmanı yada şebeke/IT sorumlusu, olayla ilgili delilleri toplar, muhafaza edir, kayıt altına alır. Olayın meydana gelişindeki etkenleri hesaplamaya çalışır.
7) Düzeltivi Eylemin Seçilmesi: Görevli uzman olay incelemesi sonucunda bilgi güvenliği yönetim birimi ile koordineli olarak uygun bir eylem seçer.

8) Düzeltici Eylemin Uygulanması: Görevli uzman bazen uygun eyleme karar vemekte zorlanabilir. Bazen de eylemi uygulamada ihmalkar davranabilir. Bu durumlarda eylemi başlatamaz. Bu nedenle ilgili birimlerle bir araya gelinmesi ve eyleme geçilmesi gerekir.

9) İlgili birimler : Gerektiğinde ilgili birimler de sürece dahil olur ve olayın yeniden değerlendirilmesi yapılarak düzeltici eylem başlatılır.
Yeniden değerlendirme yapılırken:

- Yüksek bilgi güvenliği olayını inceleme görevlendirmesine rağmen, uzman tarafından uygun eylem belirlenememişse 1 saat sonra yeniden değerlendirme yapılır.

- Orta Bilgi güvenliği olayını inceleme görevlendirmesine rağmen, uzman tarafından uygun eylem belirlenememişse 24 saat sonra yeniden değerlendirme yapılır.

- Düşük: Bilgi güvenliği olayını inceleme görevlendirmesine rağmen, uzman tarafından uygun eylem belirlenememişse 48 saat sonra yeniden değerlendirme yapılır.

10) Üçüncü tarafın inceleme başlatması: Olaya göre üçüncü tarafların da sürece dahil olması gerektiğinde üçüncü taraflar üstlerine düşen incelemeyi yapar ve görevli Bilgi Güvenliği Uzmanına bilgi verirler.

11) Kalıcı Çözüm Çalışması: Görevli uzman, bilgi güvenliği olayına ilişkin iyileştirme faaliyetleri belirlerken "Olay Veri Tabanı"na girerek önceki olaylara ve iyileştirici faaliyetlere de bakarak söz konusu olaya kalıcı bir çözüm bulunur.

12) Olay Kapatma ve Bildirim: Yaşanan bilgi güvenliği olaylarında çıkarılan dersler "Olay Veri Tabanı"na işlenmeli, olayların için kök sebepleri belirlenerek analizi yapılmalıdır. Bu kök sebeplerin ortadan kaldırılması için Düzeltici-Önleyici faaliyetler başlatılır. Bu işlemlerden sonra Bilgi Güvenliği Yönetimi Müdürü olayı kapatır ve olay kaydı Olay Veri Tabanı"na işlenir. Son olarak görevli Uzman ilgili tarafları ve bilgi güvenliği olay formunu doldurarak süreci başlatan kişiyi kapatma konusunda bilgilendirir.

## 6 GÖZDEN GEÇİRME

6.1 Bu prosedür yıllık olarak veya gerek görüldüğünde gözden geçirilmelidir.

## 7 DOKÜMANIN GEÇMİŞİ

| Değişiklikler\Güncellemeler | | | |
|---|---|---|---|
| Değişiklik | Tarih | Açıklama | Yayın |
| Yeni Doküman | 02/08/2010 | Yeni Doküman | 1.0 |
| Değişiklik | 11/01/2011 | 1. Bilgi güvenliği olaylarında bilgi güvenliği uzmanlarından başka system yöneticileri ve şebeke operasyon uzmanlarının da sorumlu atanabileceği belirtildi. | 1.1 |

## 8 İLGİLİ DOKÜMANLAR

8.1Bilgi Güvenliği Politikası

8.2 Bilgi Güvenliği Olay Raporlama Prosedürü

8.3 Şebeke Güvenliği İzleme Prosedürü

## 9 İLGİLİ ISO/IEC 27001 KONTROLLERİ

9.1 A.13 Bilgi Güvenliği Olay Yönetimi

## 10 EKLER

## 11 DAĞITIM

Kurumsal intranete kısa yol ile erişim sağlanacak şekilde eklenmiştir.

Kağıt kopya dağıtımı ise tabloda belirtilmiştir.

| Dokümanın Adı | Yayın | Verildiği Birim |
|---|---|---|
| BGOYP | 1.1 | RAN İzleme Müdürlüğü |
| BGOYP | 1.1 | IT Müdürlüğü |
| BGOYP | 1.1 | CPN Şebeke Yönetimi |
| BGOYP | 1.1 | Ankara Çağrı Merkezi |

## 12 ONAY/YETKİLENDİRME

| Hazırlayan | İlgili Birim | Kontrol Eden | Onaylayan |
|---|---|---|---|
| Ali KOÇ (BGYS Müdürü) | Bilgi Güvenliği Yönetimi | Kenan OK BGYS Müdür Yrd. | Hakan MİR CEO |

## ÖZGÜNLÜK BİLDİRİMİ

Uzmanlık tezi olarak sunduğum bu çalışmayı, bilimsel ahlak ve geleneklere aykırı düşecek bir yol ve yardıma başvurmaksızın yazdığımı, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlardan her seferinde değinme yaparak yararlandığımı ve Bilgi Teknolojileri ve İletişim Kurumu Meslek Personeli Sınav, Görev, Çalışma Usul ve Esasları Hakkında Yönetmeliğe uygun olarak hazırladığımı belirtir, bunu onurumla doğrularım.

Bilgi Teknolojileri ve İletişim Kurumu tarafından belli bir zamana bağlı olmaksızın, tezimle ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara katlanacağımı bildiririm.

18.10.2011
(Tarih)

(İmza)

Hakan AYDOĞAN
(Adı Soyadı)

# ÖZGEÇMİŞ

1982 yılında Elazığ'da doğdu. İlköğrenimini, Elazığ Atatürk İlkokulunda tamamladı. Orta öğrenimi için Elazığ Anadolu Lisesine devam etti. 2006 yılında Boğaziçi Üniversitesi Elek- Elektronik Mühendisliği bölümünden mezun oldu.

Mezun olduktan sonra Ulaştırma Bakanlığı Sivil Havacılık Genel Müdürlüğünde Operasyon Denetçisi olarak görev yaptı. 2008 yılı Mayıs ayında Bilgi Teknolojileri ve İletişim Kurumu'nda Bilişim Uzman Yardımcısı olarak göreve başladı.

2009 yılında Anadolu Üniversitesi Açık Öğretim İşletme Fakültesini bitirdi. Gazi Üniversitesi, İleri Teknolojiler Anabilim Dalında yüksek lisans eğitimine devam etmektedir.

Teknik Düzenleme ve Standardizasyon Dairesi Başkanlığı'nda görev yaptığı süre içerisinde[1]; baz istasyonu kulelerinin güçlendirilmesi ve ortak kullanılması, kısa mesajlarda Türkçe karakter kullanımı ve sabit elektronik haberleşme hizmetlerinde hizmet kalitesi çalışmalarında yer aldı. Daha sonra Elektronik Haberleşme Güvenliği Yönetmeliği kapsamında Bilgi Güvenliği ve Haberleşmenin Güvenliği konularında çalıştı.

Halen[2] Yetkilendirme Dairesi Başkanlığı bünyesinde, mobil ve sabit elektronik haberleşme çalışma gupları içerisinde görev yapmaktadır.

---

[1] 2008-2010
[2] 2011