T.C.
SAKARYA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ'NİN BİLGİ İŞLEM MERKEZLERİNDE UYGULANMASI

YÜKSEK LİSANS TEZİ

Hakan METE

Enstitü Anabilim Dalı: Çalışma Ekonomisi ve Endüstriyel İlişkiler
Enstitü Bilim Dalı : İnsan Kaynakları Yönetimi ve Endüstriyel İlişkiler

Tez Danışmanı: Prof.Dr. Yılmaz ÖZKAN

TEMMUZ-2010

T.C.
SAKARYA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ'NİN BİLGİ İŞLEM MERKEZLERİNDE UYGULANMASI

YÜKSEK LİSANS TEZİ

Hakan METE

Enstitü Anabilim Dalı: Çalışma Ekonomisi ve Endüstriyel İlişkiler
Enstitü Bilim Dal : İnsan Kaynakları Yönetimi ve Endüstriyel İlişkiler

Bu tez 09/06/2010 tarihinde aşağıdaki jüri tarafından oybirliği ile kabul edilmiştir.

Prof.Dr. Yılmaz ÖZKAN	**Doç.Dr.Erman COŞKUN**	**Yard.Doç.Dr.Tuncay YILMAZ**
Jüri Başkanı	**Jüri Üyesi**	**Jüri Üyesi**
☐ Kabul	☐ Kabul	☐ Kabul
☐ Red	☐ Red	☐ Red
☐ Düzeltme	☐ Düzeltme	☐ Düzeltme

BEYAN

Bu tezin yazılmasında bilimsel ahlak kurallarına uyulduğunu, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, tezin herhangi bir kısmının bu üniversite veya başka bir üniversitedeki başka bir tez çalışması olarak sunulmadığını beyan ederim.

Hakan METE

05.07.2010

ÖNSÖZ

Kurum ve kuruluşların bünyelerinde bilgi güvenliği kültürünü oluşturma ve bu kültürün gerekliliklerini yerine getirme çalışmalarının uluslararası düzeyde kabul görmüş kaynağı olan ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'nin, bu amaca yönelik gerçekleştirilen tüm adımlarının, kurum ve şirketler için kritik öneme sahip olan bilgilerin depolandığı, işlendiği ve saklandığı ortamları kuran ve yöneten kuruluşlar olan Bilgi İşlem Merkezleri kapsamında anlatılması, üzerinde durulmaya değer bulunmuştur.Bu çalışmanın hazırlanmasında yardım ve desteğini hiçbir zaman esirgemeyen danışman hocam Prof.Dr.Yılmaz ÖZKAN'a ve yorucu çalışmam sırasında büyük destek gördüğüm fedakar eşim Pınar METE'ye sonsuz teşekkürler eder, şükranlarımı sunarım.

İÇİNDEKİLER

KISALTMALAR ..... **iv**
TABLO LİSTESİ ..... **v**
ŞEKİL LİSTESİ ..... **vi**
ÖZET ..... **vii**
SUMMARY ..... **viii**

GİRİŞ **1**
BÖLÜM 1: BİLGİ GÜVENLİĞİ **4**
1.1.Ülkemizde Bilgi Güvenliği Kavramı ve İlgili Kanunlar 6
1.1.1.5651 Sayılı Kanun 8
1.1.2.Elektronik Haberleşme Kanunu ve Elektronik Haberleşme Güvenliği Yönetmeliği 10
BÖLÜM 2: ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ'NİN BİLGİ İŞLEM MERKEZLERİ'NDE UYGULANMASI **13**
2.1.Proses Yaklaşımı 14
2.2.BGYS'nin Kurulması ve Yönetilmesi 15
2.2.1.Bilgi Güvenliği Koordinasyonu 16
2.2.2.Boşluk (Gap) Analizi 19
2.2.3.Kapsamın Belirlenmesi 26
2.2.4.Bilgi Güvenliği Politikasının Hazırlanması 28
2.2.5.Risk Yönetim Süreci 32
2.2.6.BGYS'yi Gerçekleştirmek ve İşletmek İçin Yönetim Onayı İstemek 55
2.2.7.Uygulanabilirlik Bildirgesinin Hazırlanması 56
2.3.BGYS'nin Gerçekleştirilmesi ve İşletilmesi 58
2.3.1.Risk Yönetim Süreci-Risk İşleme Planının Hazırlanması 59
2.3.2.Risk İşleme Planının Gerçekleştirilmesi 61
2.3.3.Kontrollerin Uygulanması 63
2.3.4.Kontrol Etkinliğinin Nasıl Ölçüleceğini Tanımlama 64
2.3.5.Eğitim ve Farkındalık Programının Gerçekleştirilmesi 66

2.3.6.BGYS'nin İşletilmesinin İdaresi 67
2.3.7.BGYS İçin Kaynakların İdaresi 67
2.3.8.Güvenlik İhlal Olayları Prosedürlerini ve Diğer Kontrolleri Gerçekleştirme 67
2.4.BGYS'nin İzlenmesi ve Gözden Geçirilmesi 69
2.4.1.İzleme ve Gözden Geçirme Prosedürlerini Gerçekleştirme 70
2.4.2.BGYS'nin Dikkatle Gözden Geçirilmesini Sağlama 72
2.4.3.Risk Yönetimini Belli Aralıklarla Gözden Geçirme 72
2.4.4.Planlanan Aralıklarla İç BGYS Denetimlerini Gerçekleştirme 73
2.4.5.BGYS'nin Yönetim Tarafından Gözden Geçirilmesini Üstlenme 73
2.4.6.Güvenlik Planlarını Güncelleştirme 74
2.4.7.BGYS Etkinlik ve Performansını Etkileyecek Olayları Kaydetme 75
2.5.BGYS'nin Sürekliliğinin Sağlanması ve İyileştirilmesi 76
2.5.1.Tanımlanan İyileştirmelerin Gerçekleştirilmesi 77
2.5.2.Eylemler ve İyileştirmeleri 3. Taraflara Aktarma ve Onlarla Mutabık Kalma 78
2.5.3.İyileştirmelerin Amaçlara Uygunluğunu Sağlama 80
2.6.Dokümantasyon Gereksinimi 80
2.6.1.Dokümantasyon ve Kayıtları Kontrolü 86
2.7.Yönetimin Sorumluluğu 88
2.7.1.Yönetimin Bağlılığı 89
2.7.2.Kaynak Yönetimi 89
2.8.BGYS İç Denetimleri 99
2.9.BGYS'nin Yönetim Tarafından Gözden Geçirilmesi 101
2.10.BGYS İyileştirmeleri 104
2.11.Bilgi İşlem Merkezlerinde BGYS Kapsamında Uygulanan Ek-A Kontroller 106
2.11.1.İnsan Kaynakları Güvenliği 107
2.11.2.Fiziksel ve Çevresel Güvenlik 108
2.11.3.Haberleşme ve İşletim Yönetimi Güvenliği 110
2.11.4.Erişim Kontrolü 114
2.11.5.Bilgi Sistemleri Edinme, Geliştirme ve Bakımı 117
2.11.6.Bilgi Güvenliği İhlal Olayı Yönetimi 119
2.11.7.İş Sürekliliği Yönetimi 121
2.11.8.Uyum 123

2.12.BGYS Belgelendirme Süreci 124
2.12.1.Belgelendirme Kontrolleri 126
2.12.2.Belgelendirme 127

SONUÇ VE ÖNERİLER 130
KAYNAKLAR 134
ÖZGEÇMİŞ 142

KISALTMALAR

BGYS :Bilgi Güvenliği Yönetim Sistemi

BS :Bilgi Sistemleri

BT :Bilgi Teknolojileri

DOK :Doküman

EA :European Accreditation (Avrupa Akreditasyon Kurumu)

FTP :File Transfer Protokol (Dosya Transfer Protokolü)

GPRS :General Packet Radio Service (Genel Paket Radyo Servisi)

HTTP :Hyper Text Transfer Protokol (Hiper Metin Transfer Protokolü)

IEC :International Electrotechnical Commission (Uluslararası Elektroteknik Komisyonu)

IP **:**Internet Protokol (İnternet Protokolü)

ISMS :Information Security Management System (Bilgi Güvenliği Yönetim Sistemi)

ISO :International Standart Organization (Uluslararası Standart Organizasyonu)

İK :İnsan Kaynakları

LTD.ŞTİ :Limited Şirketi

OECD :Organisation for Economic Co-operation and Development (İktisadi İşbirliği ve Gelişme Teşkilatı)

PUKÖ :Planla-Uygula-Kontrol Et-Önlem Al

STS :Saldırı Tespit Sistemi

TC :Türkiye Cumhuriyeti

TSE :Türk Standartları Enstitüsü

TÜBİTAK :Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

TÜRKAK :Türk Akreditasyon Kurumu

UEKAE :Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

VER :Versiyon

WAP :Wireless Application Protokol (Kablosuz Uygulama Protokolü)

TABLOLAR

Tablo-1 Elektronik Haberleşme Güvenliği Yönetmeliğine Göre Bazı Tehdit ve Zafiyetler 11
Tablo-2 Örnek BGYS Ekibi Organizasyonu 17
Tablo-3 Boşluk (Gap) Analizi Kontrol Listesi 21
Tablo-4 Risk Skor (Derecelendirme) Tablosu 35
Tablo-5 Varlık Envanteri Tablosu 39
Tablo-6 Tehdit ve Açık Tablosu 43
Tablo-7 Olasılık Seviyeleri ve Açıklamaları 46
Tablo-8 Etki Analizi Dereceleri ve Açıklamaları 46
Tablo-9 Risk Dereceleri ve Açıklamaları 47
Tablo-10 Risk Değerlendirme/Derecelendirme Tablosu 49
Tablo-11 Kontrol ve Amaçlarını Belirleme Tablosu 53
Tablo-12 Uygulanabilirlik Bildirgesi 58
Tablo-13 Risk İşleme Planı 60
Tablo-14 Kontrol Etkinliğinin Ölçülmesi Tablosu 65
Tablo-15 BGYS Etkinlik ve Performansını Etkileyecek Olayları Kaydetme Formu ... 76
Tablo-16 Zorunlu Politika ve Prosedürler 86
Tablo-17 Bilinçlendirme Konuları 96
Tablo-18 Eğitim Konuları 98
Tablo-19 Örnek İç Denetim Raporu 101
Tablo-20 Örnek Yönetim Gözden Geçirmesi Raporu 103
Tablo-21 TÜRKAK'A Akredite ISO/IEC 27001 Belgelendirme/Tescil Kuruluşları ..125
Tablo-22 TSE Yönetim Sistemi Belgelendirme Ücretleri 125

ŞEKİLLER

Şekil-1 BGYS PUKÖ Yaklaşımı 15
Şekil-2 Sembolik Bilişim LTD.ŞTİ. BGYS Kapsamı 27
Şekil-3 Risk İşleme Yöntemi Belirleme Süreci 62
Şekil-4 Proses Bazlı Bilgi Güvenliği Yönetim Sistemi 83
Şekil-5 ISO/IEC 27001 BGYS Sertifikasyon Örneği 128

SAÜ, Sosyal Bilimler Enstitüsü **Yüksek Lisans Tez Özeti**

Tezin Başlığı : "ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'nin Bilgi İşlem Merkezlerinde Uygulanması"			
Tezin Yazarı	**:** Hakan METE	**Danışman**	**:** Prof. Dr. Yılmaz ÖZKAN
Kabul Tarihi	**:** Haziran 2010	**Sayfa Sayısı**	**:** viii (ön kısım) + 142 (tez)
Anabilim Dalı	**:** Çalışma Ekonomisi ve Endüstriyel İlişkiler	**Bilim Dalı**	**:** İnsan Kaynakları Yönetimi Endüstriyel İlişkiler

Bilgi iletişim teknolojilerinde internetin kullanımının artarak, verilen tüm hizmetlerin dünyaya açık sistemler haline gelmesi, gün geçtikçe bilgi güvenliğinin önemini arttırmış, kötü niyetli uygulamaların da bu paralelde çoğalması ile kurum ve kuruluşların kendi bilgi güvenliklerine daha fazla önem vermelerine neden olmuştur.

Bilgi güvenliği bilincini oluşturma ihtiyacı duyan tüm kurum ve kuruluşlar için temelleri 1995 yılından itibaren atılan ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi ile alınacak yönetimsel ve teknik önlemler standartlaştırılmıştır. Bu standart daha sonra devletler bazında da kabul görmüş ve kanunlara eklenerek bazı piyasalarda etkinlik göstermek isteyen firma ve kuruluşlara zorunluluk haline getirilmiştir.

Bilgi Güvenliği Yönetim Sistemi öncelikle kurumların bünyelerindeki tüm bilgilerin işlendiği, depolandığı ve saklandığı ortamları barındıran ve bunların yönetimini üstlenen Bilgi İşlem Merkezleri'nde uygulama alanı bulmaktadır.

Bu çalışmanın araştırma problemi; kuruluşları bünyesinde bilgi güvenliği kültürünü oluşturacak ISO/IEC 27001 BGYS Standardını, kurmak ve yönetmek isteyen Bilgi İşlem Merkezi Yöneticileri'ne Türkçe bir rehber hazırlamak olarak ifade edilebilir. Bu faaliyetlerin tüm aşamalarını ulaşılabilir manada tek bir belge üzerinden Türkçe olarak anlatan kaynağın yok denecek kadar az olması ve ilgili bilgilerin sadece danışmanlık şirketleri tarafından ödenecek ücretler karşılığında verildiği günümüzde, kuruluşların BGYS kurmak ve işletmek için zaman ve kaynak ihtiyaçlarını düşüreceği amaçlanan çalışmada sistemi kurup yönetirken yapılması gereken tüm adımlar sırasıyla anlatılmıştır.

Yukarıdaki ihtiyaçlara cevap ararken literatür taramasına ek olarak konu ile ilgili çeşitli seminer ve eğitimlere katılım sağlanmış, konu ile ilgili danışmanlık şirketleri ziyaret edilerek gerekli veriler toplanmıştır.

Anahtar Kelimeler: ISO/IEC 27001, BGYS, Bilgi Güvenliği, Bilgi İşlem Merkezleri

Title of the Thesis: "Implementation of ISO/IEC 27001 Information Security Management System in IT Department"

Author : Hakan METE **Supervisor :** Prof. Dr. Yılmaz ÖZKAN

Date : June 2010 **Nu. Of pages:** viii (pre text) + 142 (main body)

Department: Labour Economics and Industrial Relations **Subfield:** Human Resource Management and Industrial Relations

In Information Technologies, parallel to increase of internet usage, all services are started to offer online. It made information security more important and caused organizations to take precautions in their IT security.

All managerial and technical precautions are standardized for organizations needed an information security conscious with ISO/IEC 27001 Information Security Management System started in early 1995's. Later, this standart also has been accepted by goverments as a prerequisite for some IT organizations.

Primarily, Information Security Management System is applied to IT departments where all data processed, stored and managed .

The purpose of this study can be expressed as to prepare a Turkish guideline for IT managers who eager to establish a standart based on ISO/IEC 27001. Nowadays, resources in that field are scarce in turkish language and related information can only be reached via consulting companies by paying. With this study, it is aimed to decrease time and resource requirements and all steps needs to be taken for establishing and managing an Information Security Management System is explained in order.

While searching for an answer to all aforementioned problems in addition to literature survey, participated in various trainings and workshops, and visited related consulting companies for collecting necessary data.

Keywords: ISO/IEC 27001, ISMS, Information Security, IT Department

GİRİŞ

Bilginin; organizasyonlara değer katan ve bu vasfından dolayı uygun şekilde kullanılıp, korunması gereken bir işletme varlığı olarak algılanması, hayatımıza internetin girdiği 90'lı yıllar ile başlamış, günümüze kadar inanılmaz derecede artarak üzerinde daha da fazla durulan önemli konulardan biri halini almıştır. Bu dönemden önce sadece fiziksel alanların kontrolü, iç ağın kontrolü ya da evrakların kontrolü gibi daha çok birimsel/çevresel faktörlerin güvenliğinin alınmasıyla gereklilikler sağlanırken, verilen hizmetlerin internet vasıtasıyla tüm dünyaya açılması, getirilen kolaylıkların yanında güvenlik gereksinimlerini de aynı hızda değiştirmiştir. Daha önce sadece fiziksel güvenliğin yeterli olacağını düşünen kurum/işletmeler şu an itibariyle kendileri için hayati öneme sahip ve neredeyse bulundukları pazar içinde konumlarını koruyacak ve yükseltecek unsur olan bilginin güvenliğine diğer faktörlerden daha fazla önem göstermektedir.

Gerek bilişim sistemlerinin akıl almaz bir hızla gelişerek bu sistemleri kullanacak, işletecek ve yönetecek insan faktörünün zor yetişmesi, gerekse de kurumların işleyişlerinin ve verdikleri hizmetlerin bilgi sistemleri bağımlılığının artması ile bilgi güvenliği konusunun artık sadece profesyonel kişiler tarafından yapılması zarureti doğmuştur. Bu bağlamda kurumlar, kendi devletlerinin de konuya kayıtsız kalamayarak kanunlar yayınlamaları ile bilişim suçlarının önüne geçmeye çalıştığı şu dönemde kendi profesyonel bilgi güvenliği ekibini kurmak ve bu ekibe her türlü desteği sağlamak zorundadırlar. Bu şekilde kanunların emrettiklerini uygulamalarının yanında, kendi işleyişlerinin de daha güvenli hale getirilmesi ve uygulayacakları standartlar ve alacakları belgeler ile diğer firmalara göre bir adım önde olmalarını sağlamak için bilgi güvenliğine önem vermeli ve konuya sistematik bir şekilde yaklaşmalıdırlar. Bu bağlamda bilgi güvenliğinin uygulanması, kurum/şirketlerin rekabet gücünü arttırıcı bir unsur olarak karşımıza çıkmaktadır.

Bilgi güvenliği bir karar, bir strateji meselesidir. Firma ve kurumlar süreçlerinin güvenilirliğini sağlayarak, kontrolün ellerinde olduğunu öncelikle kendilerine, daha sonra müşterilerine kanıtlamak ya da diğer seçenek olan kontrolün kendi ellerinde olamayacağı, sonucu belli olmayan süreçlerle devam etmenin kararını vermelidir. Bu karara, organizasyonun yapısı, işleyişi, kurum kültürü, verilen hizmetlerin içeriği ve

yönetimin bilgi güvenliğine bakış açısı gibi birçok faktör etki etmektedir. İşte bu noktada yönetimin kararlılığı ve güvenlik sistemlerini oluşturacak profesyonel ekibin işlevselliği önem kazanmaktadır.

Çalışmanın Amacı

Tezin amacı bünyesinde bilgi güvenliği oluşturmak ya da zorunlulukları sağlamak isteyen kuruluşların, tüm süreçlerindeki kritik derecede bulunan bilgilerinin işlendiği, depolandığı ve saklandığı Bilgi İşlem Merkezleri'nde ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'ni nasıl kurup, işletecekleri hakkında bilgi vermektir. Sistemin sırasıyla hangi adımlar izlenerek kurulacağı anlatılmakta ve belgelendirmenin ne şekilde oluşturulacağı açıklanmaktadır. Bu çalışma standardın Türkçe kaynağının yok denecek kadar az olması, kurulum ve yönetim aşamalarındaki yönlendirici bilginin sadece danışmanlık şirketlerinden yüksek sayılabilecek ücretler ödenerek alındığı seminerler aracılığıyla sağlandığı düşünüldüğünde Bilgi İşlem Merkezleri'nde ve buradan hareketle başka sektörlerdeki kurum ve kuruluşlarda standardı oluşturup işletmek isteyen yönetici ve diğer kişilere kaynak doküman olacağı düşüncesiyle hazırlanmıştır.

Çalışmanın Önemi

Bu tez çalışması, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'nin Bilgi İşlem Merkezleri'nden hareketle tüm kurum kuruluşlarda uygulanmasının adım adım anlatımının yapıldığı ortak erişilebilir manada az sayıdaki Türkçe kaynaktan biri olması nedeniyle önem arz etmektedir.

Kurumlarında bilgi güvenliği konularıyla ilgili ve tüm dünya çapında kabul görmüş bir standardı uygulamak isteyen Bilgi İşlem Merkezi Personeli ya da departman yöneticileri, bu çalışmayı baz alarak kendi kurumuna özgün bir sistemi kurup yönetebilir niteliğe sahip olabilecekleri değerlendirilmektedir.

Çalışmanın Yöntemi

Bu tez çalışması ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'nin kurulması, gerçekleştirilmesi, kontrol edilmesi ve iyileştirilmesi aşamalarının birçok yabancı ve yerli kaynaktan edinilen bilgiler, katılınan seminerler ve danışmanlık şirketleri

ziyaretleri ışığında Bilgi İşlem Merkezleri'nde uygulanması konusunu ihtiva etmektedir. Örnek olarak Sembolik Bilişim LTD.ŞTİ. adında sanal bir bilişim şirketi üzerinden Bilgi İşlem Merkezleri yapıları ve buralarda Bilgi Güvenliği Yönetim Sistemi uygulamaları incelenerek, standardın tüm aşamalarında hangi adımları izlendiği aktarılmıştır.

Çalışmanın İçeriği

Bu tez çalışmasında, öncelikle bilgi güvenliğinin anlamı ve ilkelerinden bahsedilerek konunun ilk etapta daha iyi anlaşılması amaçlanmıştır. Daha sonra ülkemizde bilgi güvenliği kavramı ve ilgili yasalardan yola çıkılarak konunun yasal dayanakları açıklanmıştır. Bilgi güvenliği konusunda uluslararası manada kabul gören ISO/IEC 27001 BGYS Standardı'nın kurulumu ve işletilmesi adımlarının, kurum ve şirketlerin tüm bilgi iletişim teknolojileri hizmetlerinin sağlandığı kuruluşlar olan Bilgi İşlem Merkezleri'nde ne şekilde uygulanılacağı anlatılmıştır.

Kurulum adımları anlatılırken öncelikle Bilgi İşlem Merkezleri'nin yapılarından bahsedilerek, bu şirket/departmanlardaki personelin tüm BGYS süreçlerini yönetecek BGYS ekibindeki görevleri açıklanmıştır. Daha sonra Risk Yönetim Süreci'nden başlanılarak iyileştirme çalışmalarına kadar tüm adımlar detaylı bir şekilde anlatılmıştır. Burada ISO/IEC 27001 BGYS Standardı'nın PUKÖ çerçevesi içinde sürekli gelişen sonsuz yaşam döngüsü ile bir kez yapılıp bırakılamayacak bir çalışma olduğu ve yine sürekli yönetim desteği ihtiyacı vurgulanacaktır. Oluşturulacak belgeler üzerinden örnekler verilerek çalışmayı kaynak alıp, bünyelerinde BGYS oluşturacak kişilere yol gösterilmesi amaçlanmıştır.

Bilgi İşlem Merkezlerinin değişen yapısı ve Bilgi Güvenliği Yönetim Sistemi kültürünün kurum/merkeze kazandırdıklarından bahsedileceği sonuç kısmı ile çalışma tamamlanacaktır.

BÖLÜM 1: BİLGİ GÜVENLİĞİ

Bilgi; kişi, kurum ve kuruluşların günlük hayatlarındaki işlemlerinin, kayıtlarının ve tecrübelerinin sonucu elde edilmiş ve karar verme aşamasında kaynak olarak kullanılan işlenmiş veri, güvenlik ise; sahip olunan tüm varlıkların her türlü tehdit ve tehlikelerden korunması anlamına gelmektedir. Buradan hareketle bilgi güvenliği kişi ve kuruluşların karar aşamalarında kaynak olarak kullandıkları ve çeşitli ortamlarda saklanan işlenmiş verilerinin her türlü tehdit ve tehlikelere karşı korunması anlamına gelmektedir[1].

Bilginin her türlü tehdit ve tehlikelere karşı korunması işlemi ancak bilgi güvenliği ilkeleri olan gizlilik, bütünlük ve erişebilirliklerinin sağlanması ile mümkün olacaktır. Bilgi güvenliği, bu üç ilke üzerine inşa edilmektedir.

Gizlilik

Oluşturulan, işlenen ve saklanan bilginin sadece yetki verilen kişiler tarafından erişilebilmesi anlamına gelen gizlilik, güvenliğin en temel ilkesidir[2]. Örnek olarak bir odaya sadece elinde anahtarı olan ya da giriş kartında yetkisi olan kişinin girmesinin sağlanması verilebilir.

Bütünlük

Bilginin; yetkisiz kişilerce değiştirilmesi, silinmesi ve kasıtlı ya da kazara tahrip edilmesinin önlenmesidir. Bütünlük bilginin doğru ve eksiksiz olmasıdır. Bilginin olması gereken yerde olması gereken şekilde işlenip, saklanmasıdır. Buna bir örnek vermek gerekirse; veritabanlarında saklanan bilginin doğru ve eksiksiz olmasıdır. İnsan Kaynakları Bölümü bir personeli sisteme kayıt ederken T.C. kimlik numarasını girmeyi unuttuğu senaryoda veritabanı kendisini uyaracak ve numarayı girmesini sağlayacaktır. Numarayı girmediği durumlarda sistem kaydı tamamlamayacaktır. Böylece o personelin bilgileri eksik girilemeyecektir. Ya da kötü niyetli olarak bilgilerin silinmesi olasılığına karşı veritabanından önem arz edecek bilgi silindiğinde kullanıcıya işleminin izlendiğini hatırlatılacak ve sistem yöneticisine bilgilendirme yapılacaktır. Ayrıca yedekleme sistemleri ile silinen bilgilerin geri dönülmesi sağlanacaktır.

---

[1] Bilişim Sistemleri Güvenliği El Kitabı (Ankara: Türkiye Bilişim Derneği,Mayıs 2006)

[2] Sunay KAHRAMAN Yönetimde Bilgi Güvenliği Sistemi'nin Yapısı,İşleyişi ve Aselsan A.Ş.'de Uygulanması (Yayımlanmış Yüksek Lisans Tezi,Anadolu Üniversitesi Sosyal Bilimler Enstitüsü,2006)

Kullanılabilirlik

Bilginin, yetkili kişiler tarafından ihtiyaç duyulduğu anda hazır durumda olmasıdır. Örnek olarak bir banka müşterisinin internet üzerinden hesabına ulaşması gerektiği anda hesabına bağlanarak işlem yapabilme imkanını bulmasıdır. Bir hatanın oluşması ya da bilgilerinin yanlış olması durumunda kullanılabilirlik ilkesi zedelenecek ve hesabı erişilebilir duruma gelene kadar kaybedeceklerini bankadan talep edebilecektir. İşte bu gibi olayların yaşanmaması için sistemlerin yedekli yapıda kurulması, acil durum planları yapılması gibi birçok uygulama gerçekleştirilmektedir.

Bilgi güvenliğinin bu üç ilkesine ek olarak yine bu ilkeleri destekleyen bir çok unsur bulunmaktadır. Bunlara da kısa değinecek olursak;

Kimlik Doğrulama: Bilginin ulaşılması, işlenmesi ve depolanması aşamalarında bilgiye erişen kişilerin, gerçekten öne sürdüğü kişi olduğunun doğrulanmasıdır. Örnek olarak, bir kişi çalışma ofisine girerken manyetik kart okuyucusuna kartını göstermekte, sistem bu karta sahip olan kişinin o kapıdan girmeye yetkili olup olmadığını kontrol etmekte ve yetkisi varsa kilidi açmaktadır. Kilidi açarken de veritabanına saat yazılarak erişim kayıt altına alınmaktadır. Elinde kartı olmayan en üst düzey yetkili dahi olsa giriş yapamamaktadır. Aynı şekilde bilgisayarlara erişim de alınan bir kullanıcı adı ve şifresi ile yapılabilmektedir. Böylece sistem karşısındakinin yetkili/doğru insan olduğunu varsaymaktadır.

Erişim Denetimi: Bilginin gizliliğinin alt unsuru olan erişim denetimi kullanıcıların bilgiye erişim yetkilerini düzenlemektir. Örnek verecek olursak, dosya sunumcu üzerinde hassasiyeti olan bir klasörde sadece üst düzey yetkilinin değiştirme hakkının olması ve diğer kullanıcıların sadece okuma hakkı olmasıdır.

Kaydedilebilirlik: Bilgiye erişip, işleyen ve depolayan her kullanıcının bilgi varlığı üzerinde yaptığı tüm hareketlerinin izlenebilir nitelikte olmasıdır. Örnek olarak; kurum içerisindeki bilgisayar ağını kullanarak internete çıkan her kullanıcının girdiği web siteleri kanunların, standartların ve bilgi güvenliğinin bir gereği olarak kayıt altına alınmaktadır. Gönderilip alınan tüm elektronik postalar gereği duyulduğunda ya da hukuki bir işlem gerektirdiğinde kontrol edilmek üzere kayıt altına alınmaktadır.

İnkar Edilemezlik: Bilgi erişim ve kullanım kayıtlarının değiştirilmesini ya da silinmesini engelleyerek bu kayıtların doğruluğunun ve kesinliğinin kanıtlanmasıdır. Bilginin inkar edilemezliği kanunlar tarafından da aranan bir özelliktir. Örneğin, kullanıcının dosya sunumcu üzerindeki hareketlerinin kayıt edildiği sunumcuda ilgili kayıtlar üzerine zaman damgası vurularak o elektronik bilginin hangi zamanda değiştirildiği öğrenilecek ve kötü niyetli hareketler engellenecektir.

Bilginin bu unsurlarının oluşturulmasıyla güvenliğinin sağlanması, bilgi iletişim teknolojilerinin önemini arttırmıştır. Bilgi iletişim teknolojilerinin kullanımının olmadığı ya da yaygınlaşmadığı dönemlerde bilgiler, kağıtlara ya da bu gibi materyallere yazılarak fiziksel ortamlarda saklanmışlardır. Fiziksel ortamların da güvenliğine önem verilmiş fakat koruma yeterli olamayarak bilgilerin çalınması ya da başka kişilerin eline geçmesi engellenememiştir. Bilgi güvenliğinin sadece fiziksel korumanın yapılarak bile gerçekleştirilemediği dönemlerden, iletişim teknolojilerinin artmasıyla, bilgilerin bilgisayar ortamlarında saklandığı, dünyanın farklı birçok bölgesinden erişilerek işlem yapıldığı dönemlere gelinmiştir.

1.1.Ülkemizde Bilgi Güvenliği Kavramı ve İlgili Kanunlar

Ülkemizde bilgi güvenliği kavramının oluşması ve gerekliliklerin sağlanması çalışmaları, T.C. Başbakanlık Personel ve Prensipler Genel Müdürlüğü'nün 2003 yılında B.02.0.PPG.0.12-320-2789 sayılı ve "Bilgi Sistem ve Ağları İçin Güvenlik Kültürü" konulu genelgesini yayımlayarak başta tüm kamu kurum ve kuruluşları olmak üzere, bilgi sistem ve ağlarının korunması için yürütülen çalışmalarda, genelgede yayımlanan ilkelerin göz önünde bulundurması gerekliliğinin vurgulanması ile başlatılmıştır. Bu genelge OECD tarafından yayımlanan "Bilgi Güvenliği Rehber İlkeler" çalışmasının Türkçe çevirisinin yapılması ile ortaya çıkmıştır. Sayılan ilkeler ile tüm organizasyonlarda bilgi güvenliği kültürünün oluşturularak, gerekliliklerinin sağlanması amaçlanmıştır. Bu ilkeler;

-Bilinç

-Sorumluluk

-Tepki

-Etik

-Demokrasi

-Risk Değerlendirmesi

-Güvenlik Tasarımı ve Uygulama

-Güvenlik Yönetimi

-Yeniden Değerlendirme olarak ifade edilmiş ve istenilenler özetlenmiştir. Bu genelge ile bilgi güvenliği çalışmalarına başlanmış ve gün geçtikçe uluslararası düzeyde yayımlanan kanun ve standartlar takip edilerek literatüre eklenmiştir.

Ülkemizde bilgi güvenliği farkındalığının artmasına neden olan bir diğer olay Türk Standartları Enstitüsü'nün 2006 yılında "TS ISO/IEC 27001 Bilgi Teknolojisi-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler" adlı standardını yayımlaması olmuştur. Bu standarda göre o ana kadar kurumlarında bilgi güvenliği kültürünü ne şekilde oluşturacağını bilmeyen yöneticiler için kaynak olarak alınabilecek uluslararası düzeyde kabul görmüş Bilgi Güvenliği Yönetim Sistemi'nin ne şekilde kurulup yönetileceği anlatılmıştır.

Süreçlerinde bilgi sistemleri kullanım oranının yüksek derecede olduğu büyük şirketler, konuya ilgi göstermiş ve kurumlarına Bilgi Güvenliği Yönetim Sistemi'nin uygulanmasını sağlamışlardır. Bu kuruluşlara örnek olarak Sabancı Holding ve Oyak Teknoloji sayılabilir. Gün geçtikçe kamu kurum ve kuruluşlarının da standarda ilgisi artmıştır. BGYS ile belgelendirilmiş ilk kamu kuruluşu Antalya Büyükşehir Belediyesi'nin şirketi olan Aldaş'ın 2010 yılı itibariyle işlemleri tamamlanmasıyla Türkiye'de ISO/IEC 27001 Standardı ile belgelendirilmiş kurum sayısı 18'e yükselmiştir. Standart yayımlanan yönetmeliklerle bazı piyasalarda faaliyet gösterebilmek için zorunluluk haline getirilerek yaygınlaştırılmaya çalışılmaktadır.

Gerek OECD ülkelerinin aldığı güvenlik kültürünün oluşturulması kararları gerekse de ülkelerde işlenen suçların evrim geçirerek sanal ortama taşınması ve bilişim suçlarının artması sonucunda tüm dünyanın erişimine açık olan bu sistemlerin işleyişlerinin yasalar ile düzenlenmesi gereği ortaya çıkmıştır. Böylece bilişim teknolojilerini kullanan kurum ve kuruluşlarda bilgi güvenliği kapsamında yapılması gerekenler en alt

düzeyde zorunluluk şeklinde düzenlenme imkanı bulunulacaktır. Bu yasalar bir bakıma uygulanan kurallar bakımından standart getirecek ve hukuki bir olayın gerçekleşmesi durumunda kurum bilişim hareketlerinin kanıtlanmasının gereğini ortaya çıkaracaktır. Kanıtların geçerlilik kazanabilmesi için gereklilikler ortaya konulacak, suçların önlenmesi ya da sorumlularının tespit edilmesi sağlanacaktır.

Bilişim ve bilişim suçlarının Türk Ceza Kanunu'na ilk girişi 1991 yılında Resmi Gazete'de yayımlanan 3756 sayılı kanuna yapılan düzenleme işlemi ile gerçekleşmiştir. Burada ilgili kanuna "Bilişim Alanındaki Suçlar" başlığı eklenerek ilk kez bilişimden bahsedilmiştir[3]. Bilişim suçları hakkında düzenlenen en kapsamlı gelişme ise 2004 tarihli 5237 sayılı yeni Türk Ceza Kanunu'nda "Bilişim Alanındaki Suçlar" başlığı altında belirtilen suçların bilişim sistemleri aracılığıyla işlenmesinin ağırlaştırıcı neden olarak hükme bağlanmasıdır. (Bilişim sistemlerine girme, sistemi engelleme, bozma, banka ve kredi kartlarının kötüye kullanılması vs.) Ayrıca Türk Ceza Kanunu'ndaki birçok maddede münferit olarak bilişim suçlarından bahsedilmektedir.

5237 sayılı kanuna ek olarak günümüzde kullanımı hızlı bir şekilde artan elektronik imzanın ıslak imza yerine geçeceğinin vurgulandığı 5070 sayılı Elektronik İmza Kanunu'nda; imzayı sağlayan "Elektronik Sertifika Hizmet Sağlayıcısı" kurum ve kuruluşların yükümlülükleri belirtilerek, imzanın ne şekilde kullanılacağı ve hangi özelliklere sahip olması gerektiği anlatılmıştır.

1.1.1.5651 Sayılı Kanun

Türkiye Cumhuriyeti Devleti bilişim teknolojileri güvenliği ile ilgili en kapsamlı çalışmasını 04.05.2007 ve 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"u ve bu kanun ile ilgili yönetmelikleri çıkararak gerçekleştirmiştir. Burada yapılması gerekenleri sıralamış ve interneti kullanan kurum/kuruluşların işleyişlerini düzenlemiştir. Bu kanun ve ilgili yönetmeliklerde, internet üzerinden işlem yapan kişi, kurum ve kuruluşları beş bölüme ayırmaktadır.

[3] Ayla Altun,5651 sayılı Kanun:Internet Kanunu,2009
http://cisn.odtu.edu.tr/2009-16/5651.php

Abone: Herhangi bir sözleşme ile erişim sağlayıcılardan internet ortamına bağlanma hizmeti alan gerçek veya tüzel kişilerdir. Örnek verecek olursak evlerinden ya da kurumlarından bir servis sağlayıcı vasıtasıyla internete bağlanan kişi ve kuruluşlardır.

Erişim Sağlayıcı:İnternet toplu kullanım sağlayıcılarına ve abone olan kullanıcılarına internete erişim olanağı sağlayan işletmeciler ile gerçek veya tüzel kişilerdir. Örnek olarak ev ve kurumlara servis sağlayıcı olarak hizmet veren ve internet erişimi için başvurulan ilk kuruluşlardır. (Türk Telekom-Smile Adsl-Ulaknet vs.)

İçerik Sağlayıcı:İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişilerdir. Bunlar ise kurumların bilgi ve hizmetlerini internet üzerinden web ya da başka servisler vasıtasıyla oluşturan ve bunları paylaşan kişi, kuruluşlardır. Örnek olarak web sayfası olan ve bunun üzerinden işlem yapılmasını sağlayan kurumlar verilebilir.

Ticari Amaçla İnternet Toplu Kullanım Sağlayıcı:İnternet salonu ve benzeri umuma açık yerlerde ücret karşılığı, internet toplu kullanım sağlayıcılığı hizmeti veren veya bununla beraber bilgisayarda bilgi ve beceri arttırıcı veya zeka geliştirici nitelikteki oyunların oynatılmasına imkan sağlayan gerçek veya tüzel kişilerdir. Bunların örnekleri ise ülkemizde son yıllarda yaygınlığı artan internet kafelerdir. Kanunda bu gibi yerlerin açılması mülki idare amirlikleri iznine tabidir. Kamera kayıt sistemi kurmaları ve yedi gün süre ile bu kayıtları saklamaları istenmiştir.

Yer Sağlayıcı:İnternet ortamında hizmet ve içerikleri barındıran sistemleri sağlayan ve işleten gerçek veya tüzel kişilerdir. Bu gibi kişi, kurumlar ise bünyesinde bilgi sistemleri barındırmayan ve internet üzerinden hizmetlerini sunmak isteyen kurumlara donanım ve yazılım desteği sağlayan aracılardır. Bu kuruluşların verdikleri hizmetler arasında alan adı, web sayfası hizmetleri bulunmaktadır.

İlgili kanun bu beş farklı kişi ve kuruluşu, insan onuru ve temel hak, özgürlükleri, genç ve çocukların fiziksel, zihinsel ve ahlaki gelişimlerini ve ailenin huzur ve refahını zedeleyecek yayın yapmamak konusunda uyarmış ve bunları önleyici donanım ve yazılımları temin etmelerini istemiştir. Ayrıca kanuna göre bu yayınlar kötü alışkanlıkları teşvik etmemeli ve kişilerin kendilerine yönelik haklarını ihlal eden yayınlara karşı bir cevap verme ve düzeltme hakkı olduğu hatırlatılmaktadır.

Kanun bu zorunlulukların yanında kuruluşlara, bilişim hareketlerini izleme görevleri de vermiştir. Örneğin yer sağlayıcılar, üzerlerinden geçen ve hizmet verdikleri kuruluşların veri trafiklerini (kaynak-hedef IP, bağlantı tarih-saat, sayfa adresi, işlem bilgisi) en az altı ay saklamalıdır. Bu bilgilerin doğruluğunu, bütünlüğünü, oluşan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte saklamak ve gizliliğini temin etmekle yükümlüdürler. Aynı şekilde erişim sağlayıcılar trafik bilgilerini (abone adı, soyadı, kimlik bilgileri, adresi, telefon numarası, sisteme bağlantı/çıkış tarih saati, IP adresi ve bağlantı noktaları bilgisi) ve veriliyorsa vekil sunumcu hizmeti bilgilerini bir yıl saklamakla yükümlüdürler.

Ayrıca Yer Sağlayıcı ve Erişim Sağlayıcı kuruluşların faaliyet gösterebilmelerini Telekomünikasyon Kurumu iznine bağlamış ve faaliyetlerini bitirme aşamasına geldiklerinde de üç ay önceden bir yıllık trafik bilgileri ile kuruma başvurmalarını istemiştir.

1.1.2.Elektronik Haberleşme Kanunu ve Elektronik Haberleşme Güvenliği Yönetmeliği

Bu kanun ve ilgili yönetmeliklerine ek olarak bilgi güvenliği kapsamında sayılabilecek ve ilk adımları 1995 yılında Elektronik Haberleşme Kanunu ile atılan, içerisinde her türlü elektronik haberleşme cihaz, sistem ve şebekelerinin kurulması ve işletilmesinin esaslarını anlatan haberleşme güvenliği çalışmaları bulunmaktadır. Burada tüm haberleşme sistemlerinin işleyişlerinin ne şekilde gerçekleşeceği üzerinde durulmuş ve “kişisel verilerin işlenmesi ve gizliliğin korunması” bölümünde kısaca güvenlik gereklilikleri sayılmıştır.

2008’de Resmi Gazete’de yayımlanan Elektronik Haberleşme Güvenliği Yönetmeliği ile Telekomünikasyon Kurumu’nun yetkisiyle elektronik haberleşme hizmeti sunan, elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten sermaye şirketlerinin bilgi güvenliği ile ilgili uyması gereken tüm kurallar sıralanmıştır. Bu kurumların ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi sertifikasını almaları gerektiği emredilmiştir. Bu yönetmeliğe göre elektronik haberleşmeye ilişkin başlıca tehdit ve zafiyetler sıralanmıştır.

Tablo 1. Elektronik Haberleşme Güvenliği Yönetmeliğine Göre Bazı Tehdit ve Zafiyetler

Tehditler	Zafiyetler
Yetkisiz olarak veya yetki aşımıyla güvenlik hassasiyetli alana girilmesi	Gelecekte gerçekleşmesi muhtemel tehditlerin öngörülememesi
Yetkisiz olarak veya yetki aşımıyla silme, ekleme, değiştirme, geciktirme, başka bir ortama kaydetme veya ifşa etme yoluyla veri gizliliğinin, bütünlüğünün ve/veya devamlılığının bozulması	Bir sistem veya protokolün kurulumu sırasında oluşan problemler
Donanım-yazılım bileşenlerinin ulusal düzenleme ile ulusal ve/veya uluslararası standartlar uyarınca belirlenen gereklilikleri yerine getirmesinin kısmen veya tamamen engellenmesi	Geliştiricilerin hataları
Deprem, sel, su baskını, yangın gibi doğal afetler ile grev ve lokavt hali	Uygulayıcıların hataları
Kullanıcıyı yanıltarak doğru tarafla elektronik haberleşmede bulunduğu izleniminin verilmesi,	Sistemin işletimi sırasında oluşan uygunsuzluklar veya yetersizliklerdir

Kaynak: Elektronik Haberleşme Güvenliği Yönetmeliği (2008)

Daha sonra genel olarak alınacak güvenlik tedbirleri fiziksel güvenlik, personel güvenilirliği, veri güvenliği ve donanım-yazılım güvenliği başlıkları altında sıralanmıştır. Bu kurumlarda ISO/IEC 27001 BGYS standardını zorunlu kılarak yılda en az 1 kez risk analizi yapılması ya da tarafsız kuruluşlara yaptırılması öngörülmüştür. Yine bu yönetmeliğe göre ilgili kurumlar her yıl şubat ayına kadar hazırlanacak elektronik haberleşme güvenliği raporlarını Telekomünikasyon Kurumu'na göndermek zorundadırlar.

Bu kanunlar ile ilk etapta bilişim suçlarının önüne geçilmesi istenmiş ve faaliyetlerini bilişim teknolojileri üzerinden yapan firmalara güvenlik kültürü oluşturulma amacı güdülmüştür. Her geçen dönem teknolojinin geldiği noktaya göre güncellenecek olan kanunun zamanla oluşabilecek açıkları kapatacak niteliğe gelmesi hedeflendiği

görülmektedir. Kanun ve yönetmeliklerde süreçlerinde bilişim teknolojilerinin kullanım oranının yüksek olduğu kurum/kuruluşlarda ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'nin uygulanmasının bir zorunluluk olarak aranmasının bilgi güvenliği kültürünün tüm kurumlarda oluşturulması amacına uygun olduğu düşünülmektedir. Böylece kişi, kurum ve kuruluşlara yasa düzeyinde konunun önemi aktarılmış olacak, yaptırımlar açık ve net bir şekilde ortaya konacaktır.

BÖLÜM 2: ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ'NİN BİLGİ İŞLEM MERKEZLERİNDE UYGULANMASI

Literatürde BGYS olarak kısaltılan Bilgi Güvenliği Yönetim Sistemi, tüm kuruluş türlerini kapsayan ve ilgili kurumun bilgi varlıklarını yöneterek koruyan, sistematik bir yaklaşımdır. Temel amacı bilginin iyi yönetilerek korunmasının sağlanmasıdır[4]. BGYS etkili bir bilgi güvenliği elde edebilmek için süreçlerin oluşturulması, gerçekleştirilmesi ve sürdürülmesidir.

BGYS tüm çalışanları, süreçleri ve bilgi sistem teknolojilerini içine alan geniş ve kapsamlı bir çalışmadır. Bu yüzden sadece teknik önlemlerle başarılı olunamaz. Bilgi Güvenliği Yönetim Sistemi bir kültürdür ve yalnızca bu kültürün kurum kültürüne entegre edildiği durumlarda başarılı olunabilmektedir.

Kurumlar açısından hassas bilgilerin ve bilgi sistemlerinin korunabilmesi, risklerin en aza indirilerek sürekliliğinin sağlanması, BGYS'nin hayata geçirilmesiyle mümkün olabilmektedir. BGYS kurum/kuruluştaki tüm bilgi varlıklarının değerlendirilerek ve bu varlıkların sahip oldukları zayıflıkları ve karşı karşıya oldukları tehlikeleri dikkate alarak risk analizi yapılması ve bu risk analizine göre kontroller oluşturularak risklerin giderilmeye çalışılması işlemidir[5].

Bu işlemlerin yapılması öncelikle üst yönetimin daha sonra da bilgi varlıklarını kullanan tüm departmanların desteği ile olabilmektedir. Ayrıca BGYS bir kere yapılıp bitirilebilen bir sistem olmayıp sonsuz döngü içerisinde sürekli yaşayan bir sistemdir.

Bunlara ek olarak bilişim teknolojilerinde tam güvenlik diye bir olgu yoktur. Burada verilen her hizmet bir açık ve tehdit içermekte ve göze alınabilir riskler ortaya koyabilmektedir. Aynı şekilde bünyesinde BGYS sistemini kullanan firmalar da yüzde yüz güvenli değillerdir. Fakat burada bilgi güvenliği risklerinden haberdar olunduğu, risklere karşı ilgili kontrollerin gerçekleştirildiği ve göze alınabilecek arta kalan risklerin de kabul edildiği tüm 3. taraflara beyan edilmektedir.

ISO/IEC 27001 ise yukarıda sayılan Bilgi Güvenliği Yönetim Sistemi içeriklerinin sağlandığı uluslararası düzeyde tüm kuruluşların yararlanıp, sertifikalandırılabildiği bir

[4] Yılmaz Vural,Şeref Sağıroğlu,Kurumlarda Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme,Ankara,2008
[5] Dinçer Önel,Ali Dinçkan,Bilgi Güvenliği Yönetim Sistemi Kurulumu,TUBİTAK-UEKAE,Kocaeli,2007

standarttır. Bu belge ile bilgi güvenliği kurallarını en alt seviyede oluşturarak yapılması gerekenler sıralanmıştır. Bu standardı uygulayan kurumlar yapılarını düzenlerken bu belgeyi kaynak olarak alacak ve üzerine kendi işleyişlerini ekleyeceklerdir.

Kuruluşların elektronik veri ve bilgilerinin depolandığı, işlendiği, ayrıştırıldığı ve kullanıldığı birim/kurum olan Bilgi İşlem Merkezleri'nin bu standardın uygulanmasında -tüm kurumu kapsasın ya da sadece kendi bünyesinde oluşturulsun- odak noktası olması kaçınılmazdır. Örnek olarak Bilgi Güvenliği Yönetim Sistemi'nin pratiği olan EK-A Kontroller bölümü incelendiğinde birçok kural ve olgunun Bilgi İşlem Merkezleri tarafından ya işin tamamının yapıldığı ya da bir bölümünün yapılmasında yardımcı olunduğu görülmektedir. Ayrıca sadece bu bölümle kalınmayıp, Gap raporunun oluşturulmasından başlayarak en son önleyici faaliyetlere kadar alınan tüm karar ve yerine getirilmesi gereken kurallarda Bilgi İşlem Merkezleri'nin katkısı bulunmaktadır.

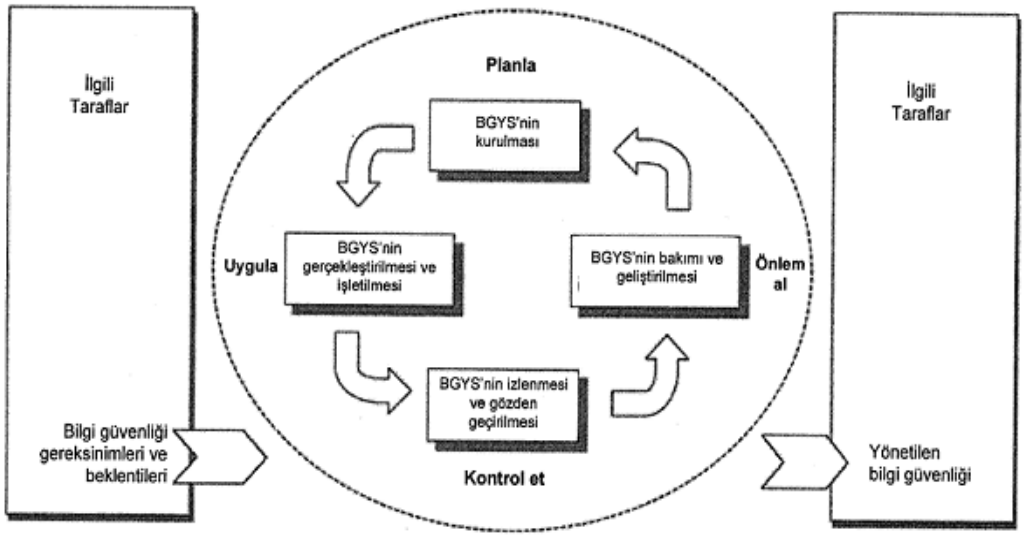
2.1.Proses Yaklaşımı

BGYS'nin bir kez tamamlanıp sona erdirildiği bir sistem olmadığını ve bir sürekli gelişim faaliyeti olduğunu belirtmiştik. İşte bu sürekli gelişim faaliyetleri, Planla/Uygula/Kontrol Et/Önlem Al süreçlerini kapsayan PUKÖ modeline dayanmaktadır. Bu modelde her bir sürecin çıktısı diğer sürecin girdisi olarak alınmakta ve buna göre işlem yapılmaktadır. Öncelikle süreçler planlanacak ve daha sonra bu planlara göre uygulanacaktır. Bu işlemler esnasında süreçler uygulanırken etkinlikleri de ölçülerek amaca ulaşılıp ulaşılmadığı kontrol edilecektir. Süreçte yapılan kontrollere göre önlemler alınarak yine planlama safhasına geri dönülecektir. PUKÖ modelinin ISO/IEC 27001 standardındaki karşılıkları BGYS'nin kurulması, gerçekleştirilmesi ve işlenmesi, izlenilmesi ve gözden geçirilmesi, iyileştirilmesi işlemlerine tekamül etmektedir.

Planlama bölümünde risk yönetimi aşamalarını oluşturacak BGYS politikasının, hedeflerin, proseslerin ve prosedürlerin oluşturulması, Uygula bölümünde planlanan politika, kontrol, süreç ve prosedürlerin gerçekleştirilip işletilmesi, Kontrol Et bölümünde genellikle tecrübeler ve daha önceden belirlenen kontrollere göre proses performansının değerlendirilmesi ve uygulanabilen yerlerde ölçülerek sonuçların gözden geçirilmek üzere yönetime rapor edilmesi, Önlem Al bölümünde ise sürekli

gelişimi sağlayabilmek için oluşturulan kaynaklar kullanılarak düzeltici ve koruyucu önlemlerin alınması işlemleri yapılmaktadır.

Şekil 1. BGYS PUKÖ Yaklaşımı



Kaynak:Önel ve Dinçkan (2007:8)

2.2.BGYS'nin Kurulması ve Yönetilmesi

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi, tüm süreçlerin güvenliğini sağlamayı amaçlayan bir bilgi güvenliği standardıdır[6]. Bu standardı sağlamak için sadece bilgisayarlar ve diğer bilişim sistemlerinin güvenliğinin oluşturulması yetmeyecek, içinde kağıt ve benzeri dokümanların güvenliği, insan kaynakları güvenliği, fiziksel güvenlik gibi her tür sürecin güvenliği kapsanacaktır. BGYS standardı ile bir Bilgi Güvenliği Yönetim Sistemi'ni kurmak, işletmek, gözden geçirmek ve iyileştirmek için bir konsept sağlamak üzere hazırlanan süreçler uygulanacaktır.

Bilgi Güvenliği Yönetim Sistemi kurulması işlemi tüm standartlarda olduğu gibi burada da Bilgi İşlem Merkezi ya da bağlı olduğu kurumun yönetim kurulu kararı ile başlayacaktır. Yönetim kurulu kararından sonra yine kurul içinden bir üye bu sistemin kurulması ile görevlendirilecektir. Bu görevlendirmenin yapılması ile tatbiki olarak başlayacak olan BGYS, sadece bir başkanlık ya da şubenin işi değildir. Buna ek olarak bir defa kurulup daha sonra bırakılacak bir iş olmadığı için tüm kurum tarafından

[6] Mehtap Çetinkaya,Kurumlarda Bilgi Güvenliği Yönetim Sistemi'nin Uygulanması,Çanakkale,2007

benimsenmesi ve arkasında durulması gerekmektedir. Bu yüzden Bilgi İşlem Merkezleri'nde de tüm personelin konu hakkında bilgisi ve değişime hazır olması gerekmektedir.

BGYS'nin kurulması tüm sistemin başlangıç safhası olarak tecrübelerin yapılacak hata/eksiklerle edinileceği ve sistemin yavaş yavaş kurum kültürüne entegresi ile kurumun bilgi güvenliğine bakışını değiştireceği göz önüne alındığında, değişimin ilk kez hissedileceği bölümdür. Bu işlemlerin ne kadar hatasız/eksiksiz olması gelecek için yön verecek ve sağlam temeller üzerine inşaa edilmesini sağlayacaktır.

2.2.1.Bilgi Güvenliği Koordinasyonu

Kurumda Bilgi Güvenliği Yönetim Sistemi'nin kurulup yönetilmesi de bir proje çalışması olacağından, bu projeyi gerçekleştirip idame ettirecek bir ekibin oluşturulması ve iş bölümünün yapılması gerekmektedir. Bilgi Güvenliği Yönetim Sistemi; tüm BGYS süreçlerinin kurulabilmesi için öncelikle yönetim kademesinin atayacağı bir yöneticinin önderliğinde BGYS ekibi ya da takımı olarak isimlendirilebilecek ve bilgi güvenliği yönetimi konusunda iyi eğitimli bir grubun oluşturulması ile başlamaktadır. Burada BGYS, tüm kurumu ve personeli kapsamasına karşın karar verici ve uygulayıcı pozisyonda tüm şubelerden belli sayıda personelin katılımıyla bir ekibin kurulmasını gerektirir. Bu ekip, risk yönetimi, politika oluşturma, güvenlik prosedürlerinin hazırlanması ve uygun kontrollerin seçilerek uygulanması aşamalarında, o bilgi varlığı ile ilgili kurum personelinden, yine bilgi güvenliği yönetimi konularında uzman ve danışmanlardan destek alacak ve böylece kuruma özgün BGYS'nin en iyi nasıl oluşturulup uygulanacağı ortaya çıkacaktır. Ayrıca olabildiğince yetkili kişiler ile oluşturulması, kararların gerektiği hızda alınması ve o hızda uygulanması işlemlerine yardımcı olacaktır. Bunun yanında bilgi güvenliğine bakış açıları aldıkları/alacakları eğitim, seminerlerle geliştirilecek ve herkesin bu konuda aynı dili konuşabilir hale getirilmesi sağlanacaktır.

Ekip, Bilgi İşlem Merkezleri yönetim şemasındaki tüm birimlerden yetkili ve bilgili personelin seçilmesinden sonra diğer bölümlerden de bilgiyi işleyen ve yönetici düzeyindeki kişilerin eğitim alarak katılmaları sağlanarak tamamlanacaktır.

Tablo 2.Örnek BGYS Ekibi Organizasyonu

BİLGİ GÜVENLİĞİ KOORDİNASYONU	
BGYS EKİP LİDERİ (YÖNETİM KURULU ÜYESİ)	
Sekreterlik	
Bilgi İşlem Müdürü	Bilgi İşlem Güvenlik Sorumlusu
Bilgi İşlem Veritabanı Sorumlusu	Bilgi İşlem Sistem Sorumlusu
Bilgi İşlem Ağ Sorumlusu	Bilgi İşlem Teknik Hizmetler Sorumlusu
Kalite Kontrol Şube Müdürü	Finans Şube Yetkilisi
Pazarlama Şube Yetkilisi	İKY Şube Yetkilisi

Bilgi güvenliği koordinasyonu oluşturulduktan sonra yapılacak ilk toplantıda sorumluluklar dağıtılarak sistemin kurulup işlenmesine başlanacaktır.

BGYS Ekip Lideri (Yönetim Kurulu Üyesi)

BGYS'nin kurulması ve işletilmesinden, gözden geçirilmesi ve iyileştirilmesinden sorumludur. BGYS ekibi ve yönetim kurulu arasındaki bağlantıyı sağlamaktadır. Yapılacak tüm toplantılara başkanlık edecek ya da vekalet bırakacaktır.

Sekreterlik

BGYS ekip lideri yönetim kurulu üyesinin sekreterliği aynı zamanda BGYS sekreterliği olarak da görev alacak olup yapılacak tüm yazışmalar bu birim üzerinden gerçekleşecektir. Kararların dağıtılması ve uygulamaların tüm personele tebliğini yapacak/yaptıracaktır.

Bilgi İşlem Müdürü

BGYS ekip lideri olmadığı zamanlarda BGYS ekibinin lideridir. Toplantılara da başkanlık edecek olan Bilgi İşlem Müdürü, teknik güvenlik konularının ve uygulanacak kontrollerin sorumlusudur.

Bilgi İşlem Güvenlik Sorumlusu

Bilgi güvenliği teknik konularındaki sorumludur. Güvenlik duvarı-içerik kontrol sunumcuları-elektronik posta güvenlik sunumcusu gibi güvenlik konularında alınacak kararların uygulayıcısı ve sahibidir.

Bilgi İşlem Veritabanı Sorumlusu

Kurum/merkeze ait tüm bilgilerin tutulduğu veritabanlarının güvenliğinden sorumludur. Toplantılarda üzerinde durulacak veritabanlarının yapısı ve işleyişi konularının açıklanmasını üstlenecektir. Veritabanları üzerinde risk işleme planı sonrasında uygulanacak kontrollerden ve bunların amaçlarına ulaşmasından sorumludur.

Bilgi İşlem Sistem Sorumlusu

Kurum/merkeze ait tüm sunumcuların güvenliğinden sorumludur. Toplantılarda bahsedilecek birçok hizmetin (elektronik posta, erişim denetimi) verildiği sunumcu ve sistemlerin kurulumu ve işleyişi konularının açıklanmasından sorumludur. Sunumcu sistemleri üzerinde risk işleme planı sonrasında uygulanacak kontrollerden ve bunların amaçlarına ulaşmasından sorumludur.

Bilgi İşlem Ağ Sorumlusu

Kurum/merkeze ait tüm iç ve dış ağların güvenliğinden sorumludur. Toplantılarda üzerinde durulacak ağ yapılarının açıklanmasından sorumludur. İç ve Dış ağlar üzerinde risk işleme sonrası uygulanacak kontrollerden ve bunların amaçlarına ulaşmasından sorumludur.

Bilgi İşlem Teknik Hizmetler Sorumlusu

Kurum/merkeze ait tüm donanım ve yazılımların bakım/tutumlarının yapılması işlemleri esnasında bilgi güvenliğinin sağlanmasından sorumludur. Tüm bakım/tutum hizmetlerinde risk işleme sonrası uygulanacak kontrollerden ve bunların amaçlarına ulaşmasında sorumludur.

İdari İşler Yetkilisi

Kurumun tüm birimlerinin işleyişine hakim ve kurum yerleşkelerinden sorumlu olan idari işler yetkilisi Bilgi Güvenliği Yönetim Sistemi’nde fiziksel ve çevresel güvenlik bölümlerinin planlanması ve uygulanmasından sorumludur. Fiziksel ve çevresel

güvenlik konularında mevcut durumun aktarılması ve yeni kontrollerin oluşturulmasında tecrübelerini aktararak istenilen duruma gelinmesine yardımcı olacaktır.

Kalite Kontrol Şube Sorumlusu

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardının dokümante edilmesinden ve standarta uygun maddelerin tamamlandığını kontrol etmekten sorumludur.

Finans Şube Yetkilisi

Bilgi Güvenliği Yönetim Sistemi'nde kurumun Finans Şubesi olarak kullandıkları bilgi kaynaklarının daha güvenli hale getirilmesi için uygulanacak kontrol ve uygulamalara işleyiş hakkında katkı sağlanmasından ve personelinin bilgi güvenliği kontrollerini uygulamasından sorumludur.

Pazarlama Şube Yetkilisi

Bilgi Güvenliği Yönetim Sistemi'nde kurumun Pazarlama Şubesi olarak kullanılan bilgi kaynaklarının daha güvenilir hale getirilmesi için uygulanacak kontrol ve uygulamalara işleyiş hakkında katkı sağlanmasından ve personelinin bilgi güvenliği kontrollerinin uygulanmasından sorumludur.

İnsan Kaynakları Yönetimi Yetkilisi

Tüm işe alma, iş sırasında ve işe son verme işlemlerinde bilgi güvenliğinin sağlanması konusunda işleyiş hakkında katkı sağlamak ve personelinin bilgi güvenliği kontrollerini uygulamasından sorumludur.

2.2.2.Boşluk (Gap) Analizi

Boşluk Analizi; şimdiki durumun, gelinmesi istenen durumla karşılaştırılarak amaç ve bu amaca yönelik olarak ihtiyaçların belirlenerek bir yol haritası çıkarılması işlemidir[7]. Bilgi İşlem Merkezleri'nde güvenlik açısından boşluk analizi uygulandığında uygulamaların mevcut durumunun incelenmesi ile eksikliklerin ortaya koyularak arzulanan durum için gerekli adımların belirlenmesidir.

[7] Stephen Coppola,Gap Analysis,ABD,2009

Kurumun alt yapısının (insan-sistem-süreç) risk yönetimine geçmek için ne kadar yeterli olduğu ve kurumsal risk yönetimi uygulamalarının oluşturulması için katedilecek aşamaların neler olduğunu gösteren bir çalışmadır. Bu analiz sonucu oluşturulan Boşluk (Gap) Raporu'nda, ulaşılmak istenen yapının gerektirdiği şartlar ile elde var olan imkan ve yapının sağlayabildiklerinin bir değerlendirmesi yapılacaktır. Bu değerlendirmeye bağlı olarak sürece başlamadan, süreç sırasında ve sürecin sonunda alınması gereken önlemler veya yapılması gereken öncül nitelikli çalışmalar ortaya konabilecektir.

Bu çalışma sonuçlarından yola çıkılarak, yapılacak işlerin zaman ve maliyet olarak daha doğru şekilde planlanması ve böylece başarı şansının büyük oranda artması söz konusu olacaktır.Bu raporda ;

a) Teknolojik alt yapı ile kurumun mevcut alt yapısının karşılaştırılması

b) Gerekli veri alt yapısı ile kurumun mevcut veri yapısının karşılaştırılması

c) Oluşturulması gerekli işlevsellik ile kurum beklentilerinin karşılaştırılması

d) Kurum personel yetkinliğinin gerçekleştirilmesi;

konuları irdelenecek ve açıklamalar getirilecektir.

Bilgi Güvenliği ile ilgili çalışmalara başlamadan veya çalışmaya devam etmeden önce yapılan fark analizi 'Nereden yola çıkıldığını', 'Nereye gidileceğini' ve 'Nasıl yol alınacağını' belirlemektir. Sırası ile;

a) Uyum sağlanması istenen standartlar belirlenir.

b) Kurumsal hedefler tanımlanır.

c) Mülakat, anket, doküman araştırması, süreç yapısı ve teknolojik yapının incelenmesi ile mevcut durum hakkında bilgi toplanır.

d) Mevcut durum raporu çıkarılır.

e) Mevcut durum ve hedeflenen durum arası farklar belirlenir.

f) İzlenecek yol belirlenir.Yapılacak işler, proje planı, kilometretaşları, takım iş gücü, iş maliyeti ve süreler tespit edilir, rapor oluşturulur. Bu rapor Bilgi Güvenliği Yönetim Sistemi'nin yol haritası olacaktır.

Boşluk analizi önce genel sorulardan başlamakta, daha sonra teknik sorularla devam etmektedir. ISO/IEC 27001'in ilk kez kurulacağı şirket, kurum ya da departmanlarda Bilgi Güvenliği Yönetim Sistemi'nin kurulması, uygulanması, kontrol edilmesi ve iyileştirilmesi aşamalarında birçok eksiğin olduğu görülecektir. Bu soruların cevaplarıyla birlikte bir yol haritası ve görev dağılımı çıkarılarak işlemlere başlanacaktır. Şirketin diğer bölümleri ile Bilgi İşlem Merkezleri'nin bilgi güvenliği açısından ayrımı ise buradan başlamaktadır. Sistem yöneticisi, mühendisi ve teknisyen kadrolarına sahip Bilgi İşlem Merkezleri en üst düzeyde bilgiye erişim imkanı bulduklarından, hem bilgi güvenliği ve risk yönetimi konularında daha fazla risk taşıyan niteliğe hem de bu konularda diğer çalışanlardan daha bilgili ve tecrübeli personele sahiptirler. Güvenlik sistemini tasarlama aşamasında görev alan ve bizzat uygulayan kişiler olması bakımından ise bilgi güvenliğine bakış açıları üst düzeyde olup, farkındalık açısından diğer bölüm ve departmanlara göre daha duyarlıdırlar.

İnsan kaynakları güvenliğinin yanında fiziki güvenlik, teçhizat güvenliği, erişim kontrolü gibi konularda da şimdiki durum ve olması gereken durumlar karşılaştırılarak yol haritaları çıkarılmalıdır. Örneğin fiziksel güvenlik açısından Bilgi İşlem Merkezleri'ne giriş kontrolleri, sistem ve ağ odalarına giriş kontrolleri, malzeme değişimleri ve tutulacak kayıtlarda istenen durum ve yapılacaklar listelenmelidir. Bundan sonra oluşturulacak tüm kontrollerin boşluk analizi baz alınarak düzenleneceği göz önüne alındığında tüm çalışma ve sonuçların açık ve net bir şekilde dokümante edilmesi, ilk yapılan kontroller ile gelinen durum arasında bağlantı kurulabilmesi için düzgün şekilde saklanması önemli bir zorunluluktur.

Tablo 3. Boşluk (Gap) Analizi Kontrol Listesi

BGYS BÖLÜMÜ	YAPILACAK KONTROL
4.BGYS'NİN KURULMASI	
4.1 GENEL BGYS GEREKLILIKLERININ PLANLANMASI	BGYS'nin Tanımlanması BGYS'nin İşletmeye Uygulanması BGYS'nin İşletmede Yönetimi

Tablo 3'ün devamıdır.

	BGYS'nin İşletmede İzlenmesi BGYS'nin İşletmede Gözden Geçirilmesi BGYS'nin İşletmede Sürdürülmesi BGYS'nin İşletmede Geliştirilmesi İşletmenin BGYS Belgelendirilmesi
4.2 BGYS'NİN KURULMASI VE YÖNETİLMESİ	**4.2.1.BGYS Kurulması** BGYS'nin Kapsam ve Sınırlarının Tanımlanması BGYS Politikasının Belirlenmesi Risk Değerlendirmesi Yaklaşımının Belirlenmesi Risklerin Analiz Edilmesi Risk İyileştirme Seçeneklerinin ve Eylemlerinin Tanımlanması Kontrol Amaçları ve Kontrollerin Seçilmesi Yönetimden Artık Risk Onayı Yönetimden Yetki Alınması Uygulanabilirlik Bildirgesinin Hazırlanması **4.2.2. BGYS'nin Gerçekleştirilmesi ve İşletilmesi** Risk İşleme Planının Hazırlanması Risk İşleme Planının Uygulanması Kontrollerin Uygulanması Eğitim Programlarının Uygulanması BGYS'nin Yönetimi BGYS Kaynak Yönetimi İşletmenin Güvenlik Prosedürlerinin İşlenmesi **4.2.3. BGYS'nin İzlenmesi ve Gözden Geçirilmesi** Prosedür ve Kontrolleri Kullanarak BGYS'nin Gözden Geçirilmesi BGYS'nin Düzenli Olarak Gözden Geçirilmesi Güvenlik Önlemlerinin Yeterliliğinin Kontrolü

Tablo 3'ün devamıdır.

	Risk Yönetim Sistemi'nin Gözden Geçirilmesi Artık Risklerin Gözden Geçirilmesi İç Denetim BGYS Yönetimi'nin Gözden Geçirilmesi BGYS Olaylarının Kaydı ve Kontrolü **4.2.4. BGYS'nin Sürekliliğinin Sağlanması ve İyileştirilmesi** BGYS Geliştirme Uygulamaları Uygun Düzeltici Eylemler Uygun Düzeltici Önlemler Alınan Dersleri Uygulama Tüm İlgili Taraflarla İletişim
4.3 DOKÜMAN GEREKSİNİMİ	**4.3.1. BGYS Belge ve Kayıtların Oluşturulması** Kayıtların Belgelendirilmesi Sistemi BGYS'nin Belgelendirilmesi **4.3.2.BGYS Belgelerinin Kontrolü** BGYS'nin Belgelerinin Kontrolü ve Korunması BGYS'nin Belgelerinin Kontrolü ve Korunması Prosedürü **4.3.3. BGYS'nin Kayıtlarının Kontrolü** BGYS Kayıtlarının Kontrolü ve Korunması Prosedürü BGYS Kayıtlarının Kontrolü ve Korunması
5. YÖNETİM SORUMLULUĞU	**5.1.Yönetimin Bağlılığı** Yönetimin BGYS Kurulumunu Desteklediğinin Belirtilmesi Yönetimin BGYS Uygulanmasını Desteklediğinin Belirtilmesi Yönetimin BGYS İşletilmesini Desteklediğinin Belirtilmesi Yönetimin BGYS İzlemelerini Desteklediğinin Belirtilmesi Yönetimin BGYS Gözden Geçirmelerini Desteklediğinin Belirtilmesi

Tablo 3'ün devamıdır.

	Yönetimin BGYS Korunmasını Desteklediğinin Belirtilmesi Yönetimin BGYS Geliştirilmesini Desteklediğinin Belirtilmesi **5.2.Kaynak Yönetimi** 5.2.1.BGYS Kaynak Sağlanması Kaynak İhtiyaçlarının Tanımlanması İhtiyaçların Karşılanması 5.2.1.Eğitim ve Farkında Olma Çalışmaları Personel Yeterliliklerinin Belirlenmesi Eğitim Faaliyetlerinin Gerçekleştirilmesi Eğitimlerin Etkinliğinin Değerlendirilmesi İlgili Kayıtların Tutulması
6. İÇ DENETİM	**6.1.İç Denetim Prosedürünün Oluşturulması** İç Tetkik Prosedürü Oluşturulması Prosedürün Belgelenmesi **6.2.İç Tetkiklerin Planlanması** Dahili BGYS Denetim Projeleri ve Faaliyetlerinin Planlanması İç Denetimlerin Ne Sıklıkla Yapılacağının Belirlenmesi Planlı Aralıklarla İç Denetimler Tüm İç Denetim Kapsamının Netleştirilmesi İç Denetim İçin Kriter Belirleme İç Denetim Metodunun Belirlenmesi İç Denetçilerin Seçimi **6.3.Düzeltici Önlemlerin Alınması** Uygunsuzlukların Ortadan Kaldırılması Düzeltici Önlemlerin Alındığının Kontrolü Doğrulama Sonuçlarının Raporlanması

Tablo 3'ün devamıdır.

7. YÖNETİM GÖZDEN GEÇİRMESİ	**7.1.Yönetimin İzlemesi** BGYS Performansının İzlenmesi BGYS Uygunluğunun İzlenmesi BGYS Yeterliliğinin İzlenmesi BGYS Etkinliğinin İzlenmesi BGYS Geliştirilip Geliştirilmemesi Kararının Değerlendirilmesi BGYS Yönetiminin Gözden Geçirilmesi Kayıtları BGYS Yönetiminin Gözden Geçirilmesi Sonuçları Kayıtları **7.2.BGYS Yönetiminin Gözden Geçirilmesi Girdileri** BGYS Girdileri Hakkındaki Bilgilerin Kontrolü Öncelikli Yönetim Gözden Geçirme Sonuçlarının Kontrolü Önceki İzleme Sonuçlarının Kontrolü Önceki BGYS Ölçme Sonuçlarının Kontrolü Daha Önceki Düzeltici Önlemlerin Durumlarının Kontrolü Önceki Risk Değerlendirmesindeki Yetersiz Açıklanan Güvenlik Olayları BGYS Geliştirme Fırsatlarının Kontrolü BGYS'yi Etkileyecek Değişikliklerin Kontrolü **7.3.Yönetimin Gözden Geçirilmesinin Çıktıları** Genel Karar ve Eylemler BGYS Geliştirmeye Yönelik Kararların Üretimi Yönetimin Kararları Neticesinden BGYS'nin Güncellenmesi BGYS Kaynak İhtiyaçlarını Belirten Yönetim Kararlarının Üretilmesi
8. BGYS İYİLEŞTİRMELERİ	**8.1.BGYS'nin Sürekli Gelişimi** BGYS'nin Etkinliğinin Arttırılması BGYS Etkinliği İçin Güvenlik Politikasının Kullanılması BGYS Etkinliği İçin Güvenlik Amaçlarının Kullanılması

Tablo 3'ün devamıdır.

	BGYS Etkinliği İçin Güvenlik İzlemelerinin Kullanılması BGYS Etkinliği İçin Güvenlik Yönetiminin Gözden Geçirilmesinin Kullanılması BGYS Etkinliği İçin Düzeltici ve Engelleyici Önlemlerin Kullanılması **8.2.BGYS Uygunsuzluklarının Düzenlenmesi** Uygunsuzlukların Tekrarına Karşılık Düzeltici Eylem Prosedürü Düzeltici Eylem Prosedürü Uygunsuzlukları Tanıma Özelliği

Kaynak: Standarts Gap Analysis (http://elsmar.com/Forums/showthread.php?t=26387)

2.2.3.Kapsamın Belirlenmesi

Proje ekibinin oluşturulmasından sonra ekibin yapacağı çalışmaların sınırları çizilmelidir. Burada kapsamın oluşturulması işlemi, proje ekibi tavsiyesine göre yönetim kurulu kararları çerçevesinde gerçekleştirilecektir. Kapsam her an değişikliğe uğrayabilecek bir olgu olmamasına rağmen genellikle yapılacak ilk çalışmaların neticesinde sınırlarının genişleyebildiği ya da azaltılabildiği görülmektedir[8]. Buna BGYS ekibinin tecrübesi, yönetim kurulu kararları ve organizasyonun mevcut süreçleri etki etmektedir.

Bilgi Güvenliği Yönetim Sistemi'nin genelde tüm süreçleri kapsaması ve güvenlik kültürünün tüm kurum çalışanlarına aktarılması istendiğinden genellikle kapsamın kuruluş departmanlarının hepsini içine aldığı görülmektedir. Çok büyük ölçekli kuruluşlarda bazı bölümleri kapsadığı örnekleri az da olsa bulunmaktadır.

Yapılacak ilk iş olarak amaç ve kapsam net bir şekilde belirlenmekte ve kapsam dokümanının ilk maddesi olarak yazılmaktadır. Daha sonra organizasyonun yapısı görsel şekilde oluşturulan çizimler üzerinden anlatılmaktadır. Burada merkez, şube ve depoların açık adresleri ile birlikte belirtilmesi daha uygun olacaktır.

[8] Ünal Perendi,BGYS Kapsamı Belirleme Klavuzu,TUBITAK-UEKAE,Kocaeli,2008

Daha sonra kısaca varlıklar ve teknolojilerden bahsedilecektir. Mevcut varlıklar madde madde sayılmayacak, genel hatlarıyla belirtilecektir. Şirketin tüm ticari bilgileri, çalışan ve müşterilere ait kişisel bilgiler, bu bilgileri içeren BT sistemleri gibi. Örnek BGYS Kapsam Dokümanı;

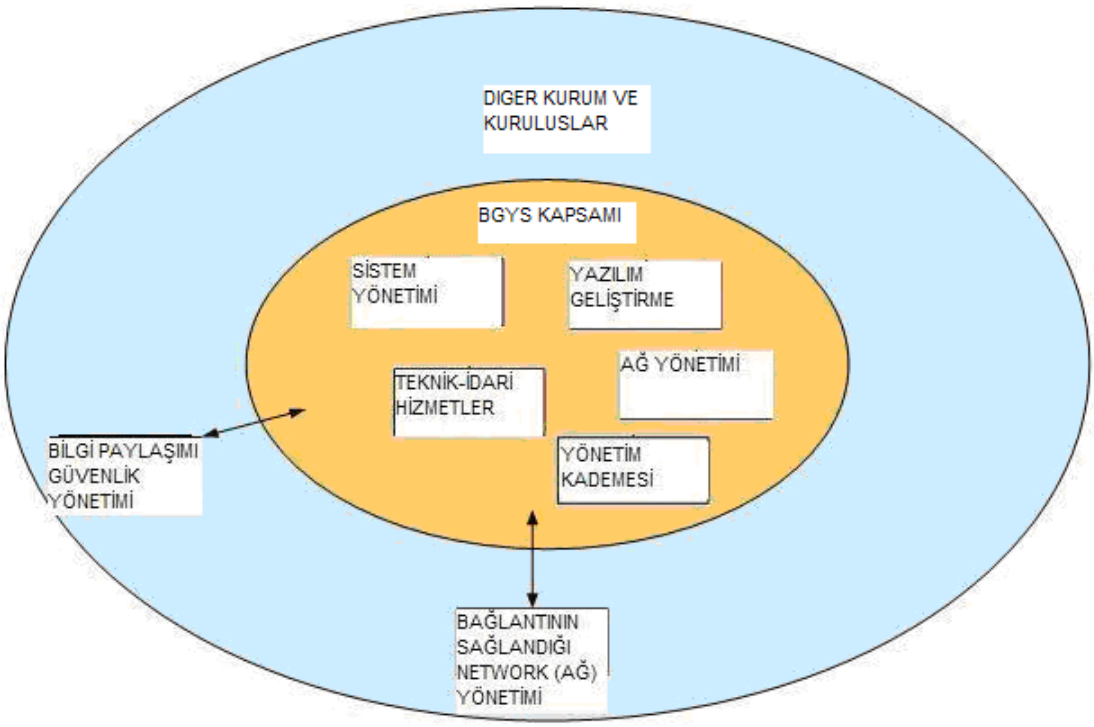
	SEMBOLİK BILISIM LTD.ŞTİ.BGYS KAPSAM DOKUMANI	
YAYIN NO: 27001-KPS-01	DOKUMAN ADI:DOK-KPS-V1	VER:0.1

SEMBOLİK BILISIM LTD.ŞTİ. BGYS KAPSAMI

Amaç ve Kapsam

2000 yılında Pendik'te kurulan Sembolik Bilişim LTD.ŞTİ. kendi personeli, müşterileri ve tedarikçilerinin kullandığı bilgi varlıklarının risk yönetimi çerçevesinde korunması amacıyla ISO/IEC 27001 BGYS'nin kurulmasına karar vermiştir. Uygulanacak sistem Sembolik Bilişim Şirketi'nin tüm bölümlerini kapsayacaktır.

Şekil 2. Sembolik Bilişim Şirketi BGYS Kapsamı



Kaynak: Perendi (2008:8)

Organizasyon

Sembolik Bilişim Şirketi 4 bölümden oluşmaktadır.

-Sistem Yönetim

-Yazılım Geliştirme

-Teknik ve İdari Hizmetler

-Ağ Yönetimi

Yerleşke

Ankara Cad.Doğu Mah.No:290 Kat:5 Pendik/İstanbul

Şube ve Depo bulunmamaktadır.

Varlıklar ve Teknoloji

Sembolik Bilişim Şirketi'nde kullanılan internet altyapısının binaya gelene kadarki hattın yönetimi dışında tüm hizmetler kendi bünyesinden sağlanmaktadır. BGYS aşağıda belirtilen tüm varlıkları kapsamaktadır.

a) Ticari Bilgiler

b) Personel Kişisel Bilgileri

c) Müşteri Özel Bilgileri

d) Tüm BT Sistemleri

e) Tüm Dokümantasyon Bilgileri

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

2.2.4.Bilgi Güvenliği Politikasının Oluşturulması

Bilgi Güvenliği Politikası, Bilgi Güvenliği Yönetim Sistemi kurularak elde edilmeye çalışılan bilgi güvenliği kavramını, bu amaca yönelik olarak ortaya çıkan ihtiyaçları ve uyulması istenen kuralları anlatan, çalışanların genel olarak sistem hakkında bilgi sahibi olmalarını sağlamak için hazırlanan, yönetimin kurumda bilgi güvenliği kültürünü oluşturma sözünü ve desteğini içeren genel kurallar ve uygulamalar bütünüdür.

Kurum BGYS'ni, yönetim kurulu kararıyla kendi ihtiyaçları neticesinde kurabileceği gibi yasal zorunluluk nedeniyle de kurabilmektedir. Hazırlanacak politikada sistemin kurulma nedenleri gerekçeleri ile birlikte açık ve net bir şekilde ortaya koyulmalıdır.

Kurum tüm süreçlerini kapsayan genel bir bilgi güvenliği politikası oluşturabileceği gibi elektronik posta kullanım politikası, internet kullanım politikası gibi farklı süreçleri farklı politikalarda da belirtebilir. Bu durumda en üst seviyede bilgi güvenliği ilkelerini ihtiva eden genel güvenlik politikasını oluşturması ve diğer politikalara atıfta bulunması gerekmektedir.

Bilgi Güvenliği Politikası dokümanı, kurumun bilgi iletişim teknolojilerini kullanma derecesi ve bilgi güvenliğine bakış açısına göre değişebilecek nitelikte olarak, BGYS'nin bilgi güvenliğinden ne kastettiği, kurumun bu sisteme neden ihtiyaç duyduğu, risk değerlendirme altyapısı, bilgi güvenliği sorumluları ve bu politikanın ekleri olan diğer politikalara yapılan atıfları belirtmelidir.

Bilgi Güvenliği Politikası kurumda bilgi güvenliğinin oluşturulmasının ve personele bilgi güvenliği çalışmalarının yansıtılmasının temel aracı olması ve tüm personel ve iletişime geçilen diğer kurum ve kuruluşlar tarafından okunması isteneceği nedenlerinden dolayı mümkün olduğu kadar kısa ve kolay anlaşılabilir yapıda olmalıdır. Politikanın gereğinden fazla içerik ve teknik bilgiler ihtiva etmesi okuyan kişi tarafından bilgi güvenliği anlamında yaratması gereken etkiyi yaratamayacak ve sıkıcı bir doküman halini alacaktır. Bu yüzden doküman olabildiğince okuyan profiline hitap etmeli ve tüm güvenlik politika ve prosedürlerine kısaca değinilerek sistemin geneli hakkında görüş uyandırmalıdır.

Bilgi Güvenliği Politikası gereği olarak, bir kullanıcıya elektronik bilgiye erişim izni verilmeden önce, bu kullanıcının bilgi güvenliğine ilişkin sorumluluklarını okuyup anladığını onaylaması istenebilir. Bu belgenin ayrıca kurumdaki bilgi varlıklarının korunmasındaki sorumluluklarını anımsatmak amacıyla kullanıcılar tarafından her dönem tekrar okuması ve imzalanması sağlanabilir.Örnek Bilgi Güvenliği Politikası;

	SEMBOLİK BILISIM LTD.ŞTİ. BİLGİ GÜVENLİĞİ POLİTİKASI	
YAYIN NO: 27001-BGP-01	DOKUMAN ADI:POL-BGP-V1	VER:0.1

Amaç

Çalışanları kurum bünyesinde kurulan ISO/IEC 27001 BGYS Standardı hakkında bilgilendirmek ve bilgi güvenliği gerekliliklerini belirlemek.

Kapsam

Tüm çalışanları kapsamaktadır.

Bilgi Güvenliği Politikası

Kurumumuzca kullanılan tüm bilişim hizmetleri ve teknolojilerileri her geçen gün gelişmekte ve yenilenmektedir. Bunun bir sonucu olarak birçok ağ yapıları, sistem işletimi ve fazla sayıda iş uygulamaları ortaya çıkmaktadır. Bu aşırı çeşitlilik içerisinde kurumumuz, sistemlerini organize ederken, bilginin gizliliği, bütünlüğü ve erişebilirliği konularında hassasiyet ile durmaktadır. Verinin ve dolayısıyla bilginin elektronik ortamda saklanması, işlenmesi ve paylaşımı bu üç unsuru barındıran bilgi güvenliği açısından önem arz etmektedir. Ayrıca bilginin taraflarca iletişimi ve internete açık olması mevcut riski arttırmaktadır.

Doküman, tüm kurumumuzca üzerinde önemle durulan ve tüm departmanlarca hassasiyet gösterilmesi beklenen bilgi sistemlerinin güvenliği konusunda uyulması gereken minimum standartları belirlemekte, tüm güvenlik sistemi için temel teşkil etmektedir.

Kurumumuzun bilgi güvenliği kavramından anladığı ve tüm kullanıcı ve yöneticilerinden talep ettiği, bilgi varlıklarının şu üç temel ilkesinin sağlanmasıdır.

Gizlilik: Bilginin sadece yetkili kişiler tarafından erişilebilir olması,

Bütünlük: Bilginin yetkisiz değiştirmelerden korunması ve değiştirildiğinde farkına varılması,

Kullanılabilirlik: Bilginin yetkili kullanıcılar tarafından gerek duyulduğu an kullanılabilir olması.

Bu politika, bilgi işlem altyapı, sistem ve programlarını kullanmakta olan tüm kurum çalışanlarını, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcıları olarak sıralanan dış tarafları kapsamaktadır. Bu taraflar bilgi güvenliği çerçevesinde oluşturulan tüm politika, prosedür ve talimatlara uymakla yükümlüdürler. Birimlerin bilgi güvenliği sorumlularından oluşan BGYS ekibi, BGYS altyapısını desteklemek ve işleyişini devam ettirmekle sorumludur.Kurum yönetimi:

-Kurumun güvenilirliğini ve müşterilerine büyük emeklerle sağladığı imajını korumak,

-Üçüncü taraflarla icra edilecek sözleşme ve yapılacak tüm işlemlerde belirlenmiş uygunluğu sağlamak,

-İş faaliyetlerinin en az kesinti ile devam etmesini sağlamak amacıyla kurum bilişim hizmetlerinin gerçekleştirilmesinde kullanılan tüm fiziksel ve elektronik bilgi

varlıklarının bilgi güvenliğini sağlamayı hedefler.

Kurum bilgi işlem altyapısını, sistem ve uygulamalarını kullanan herkes:

-Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde kuruma ait bilginin gizliliğini sağlamalı,

-Kritiklik düzeylerine göre işlediği bilgiyi yedeklemeli,

-Risk düzeylerine göre belirlenen güvenlik önlemlerini almalı,

-Bilgi güvenliği ihlal olaylarını raporlamalı ve Bilgi Güvenliği Birimi'ne bildirmeli, bu ihlalleri engelleyecek önlemleri almalı,

-Kurum bilişim kaynaklarını, T.C. yasalarına ve bunlara bağlı yönetmeliklere aykırı faaliyetler amacıyla kullanmamalıdır.

Bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması halinde, kurum Personel Yönetmeliği gereğince aşağıdaki yaptırımlardan bir ya da birden fazla maddesini uygulayabilir:

-Uyarma

-Kınama

-Para cezası

-Sözleşme feshi

E-Posta, Şifre, İnternet Erişim ve Kullanım Politikaları, İş Sürekliliği ve Acil Durum Planları, Veri Yedekleme Prosedürleri, Virüs ve Saldırganlardan Korunma Politikası, Sistemlere Erişim Kontrolü, Bilgi Güvenliği Olayları Prosedürleri bu politikayı destekler. Bu alanlarla ilgili işleyiş, özel olarak dokümante edilmiş politika ve prosedürlerle tanımlanır.

Kurum yönetimi olarak, "Kurum Bilgi Güvenliği Politikası"nın uygulanmasının ve kontrolünün yapılmasının, güvenlik ihlallerinde de gerekli yaptırımın icra edilmesinin yönetim tarafından desteklendiğini beyan ederim.

GENEL MD. Levent BAĞLAR

Alt Politika Örneği;

TSE	SEMBOLİK BILISIM LTD.ŞTİ. ELEKTRONİK POSTA POLİTİKASI	SBS
YAYIN NO: 27001-EPP-01	DOKUMAN ADI:POL-EPP-V1	VER:0.1

Amaç

Kurum ile dış dünyanın iletişiminde büyük pay sahibi olan elektronik posta hizmetinin kullanım kurallarını açıklamak.

Kapsam

E-posta adresine sahip tüm personeli kapsamaktadır.

Politika

Bilindiği üzere kurumda oluşturulan ve personelimiz tarafından kullanılan elektronik posta adresleri resmi bir kimlik taşımakta ve iletişim açısından en önemli araçlardan biri olarak sayılmaktadır. Bu kapsamda önemi üzerinde durulması gereken ve güvenlik bakımından internete ve dış dünyaya açık olduğundan hassas bir konu olan elektronik postaların işletim kuralları;

Kurum elektronik postası kişisel amaçlar için kullanılmayacaktır.

Kullanıcılar taciz, suistimal, alıcının haklarına zarar verme, uygun olmayan içerikler gibi kötü niyetli muhteviyatı olan elektronik posta göndermeyecektir.

Gizli ve hassas bilgi içeren elektronik postalar kriptolanarak gönderilecektir.

Spam, sahte elektronik posta vb. zararlı e-postalara cevap verilmeyecektir.

Kaynağı bilinmeyen elektronik posta iletileri açılmayacak ve derhal silinecektir.

Elektronik postalar sık sık gözden geçirilecek, mesajlar uzun süre sunumcu üzerinde bulundurulmayacak ve bilgisayar üzerlerindeki kişisel klasörlere kopyalanacaktır.

Kurum dışından iç elektronik posta sunumcusuna bağlanma ihtiyacı duyulduğunda, güvenliğinden emin olunmayan bilgisayarlar ya da internet kafelerden web posta sistemi kullanılmayacaktır.

Kurum çalışanları kurumsal e-postalarının yetkisiz kişiler tarafından görülmesini ve okunmasını engellemekten sorumludurlar.

Yasadışı ve istenmeyen durumlar oluştuğunda sistem yöneticileri önceden haber vermeden e-posta mesajlarını denetleyecek ve o kişi hakkında yasal ve idari işlem başlatacaktır.

Kullanıcılar kendi e-posta adreslerinin şifre güvenliklerinden sorumludurlar. Şifrelerinin kırıldığını ya da kendilerinden habersiz bir değişiklik yapıldığını farkettikleri anda BGYS ekibiyle temasa geçeceklerdir.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

2.2.5.Risk Yönetim Süreci

Teknolojik imkanların gelişmesi ile bilgi işlem yapıları ve sistemleri de aynı oranda büyümekte ve kurumlar tüm süreçlerini sayısal ortamlara taşımaktadırlar. Gün geçtikçe artan sistemlerin sayısal ortama aktarılması beraberinde çıkabilecek sorunların da artmasını sağlamıştır. Bu sorunları önceden tahmin etmek ya da olasılıklarını azaltarak sorunların önüne geçecek önlemleri almak ve bu amaçlar doğrultusundaki, Bilgi İşlem Merkezleri'nde kullanılan yazılım ve donanım ürünlerini değerlendirmek için Risk Yönetim Süreci uygulanmaktadır.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'nin üzerine inşaa edileceği ve sistemin bel kemiği olarak nitelendirilen risk yönetim süreci, bir kuruluşu mevcut riskleri ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetlerdir[9].

BGYS Risk Yönetim Süreci, bilgi varlıkları üzerinde, gelecekte oluşabilecek tehlike ve tehditlerin, belirli bir zaman aralığında kurumun işlevini yapmasını sekteye uğratma olasılıklarının, nedenleri ile birlikte belirlenmesi, bunların ölçeklendirilerek sona erdirilmesi ya da en alt düzeye indirilmesi işlemidir. Bu işlemler üç safhada gerçekleştirilmektedir. Bunlar risk analizi, risk işleme ve değerlendirme, risklerin takip edilmesi aşamalarıdır.

Risk Yönetim Süreci'nde tüm risklerin tamamen ortadan kaldırılması mümkün olamayacağı gibi konu bilgi iletişim teknolojileri olunca bu husus imkansız hali almaktadır. Risklerin dünyaya açık olan BT sistemlerinde tamamen ortadan kaldırılması demek kurumun amacı olan bir hizmet ya da mal üretiminin yapılmaması demektir. Bu nedenle risklerin olumsuz yanlarından etkilenmemek için onları önceden belirleyerek önlemler almanın, ve mümkün olduğunca mevcut risklerden yarar sağlamanın gerçekleştirildiği risk yönetim süreci doğmuştur. Bu sürecin başarıya ulaşmasının tek yolu bilgi varlıklarına yönelik risklerin sistematik ve tutarlı bir şekilde belirlenmesi ve konu üzerinde detaylı bir şekilde çalışılarak denetim altında tutulmalarıdır. İkinci aşama olarak ise risklerin gerçekleştiği anda vereceği hasarları önceden tahmin edip oluşma anlarındaki hareket tarzlarının belirlenerek zararlarını en aza indirmektir.

[9] TSE ISO/IEC 27001 Bilgi Teknolojisi-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler Standardı,2006

Risk Yönetim Sürecinin oluşturulmasından sonra gerçekleşen her kontrolün sorumlularıyla birlikte dokümante edilmesi önemli bir gerekliliktir. Ayrıca kurum içi haberleşme kanallarının oluşturulmasıyla üst yönetim ile BGYS ekibi ve aynı şekilde BGYS ekibi ile diğer departmanlar arası iletişim arttırılmalıdır.

Öncelikle kuruluşun uzun vadedeki hedefleri göz önüne alarak bu hedefleri sekteye uğratacak risklerin üzerinde çalışılmalıdır. Burada üst yönetimin desteği, oluşturulan risk yönetiminin mevcut kurum süreçlerine birebir örtüşür yapıda olması, süreçleri daha karmaşık hale getirmeden gerçekleştirilmesi sistemin başarıya ulaşmasına yardımcı olacaktır.

Risklerin meydana geldiği anlarda gerekli işlemlerin yapılması, iş sürekliliğinin sağlanması ve felaket kurtarım yönetimleriyle ilgili kontrollerin oluşturulması risk yönetiminin araçlarıdır. Bu araçları önceden meydana getirip olası senaryoların uygulanmasıyla, hareket tarzlarını sorumlularına öğreterek, sistemin eksikliklerinin görülmesi Risk Yönetim Süreci'ni sürekli gelişim çerçevesinde olması gereken noktaya getirecektir.

2.2.5.1.Risk Değerlendirme Yaklaşımını Tanımlama

BGYS standardının gerekliliklerinden biri olan Risk Değerlendirme Yaklaşımı'nın tanımı ile kurum/kuruluşlar, tanımlanmış bilgi güvenliğine uygun bir risk değerlendirme metodolojisi oluşturmalıdırlar. Tanımlanacak metodolojide riskleri kabul etmek için hangi kriterlerin aranacağı ve kabul edilebilir risk seviyeleri belirtilmelidir[10]. Bu metodun seçilip uygulanması tamamıyla kurumun dolayısıyla BGYS ekibinin kararı ve yönetim onayı ile gerçekleşmektedir. Metodun tüm kontrol alanlarını kapsaması gerekmektedir.

Risk değerlendirme metodunun tanımlanması zorunlu bir gereksinim olmasından dolayı otomasyona dayalı yazılım araçlarının ortaya çıkmasına neden olmuştur. Otomasyon yazılımları risklerin yeniden değerlendirilmesi, varlıklara yönelik risklerin güncellenmesi gibi durumlarda kolaylık sağlamakta ve bir süre sonra karmaşıklaşmaya başlayan dokümante gereksinimlerinde yardımcı olmaktadır. Burada BGYS ekibi varlıkları ve riskleri programın içinde seçebileceği gibi kriterleri de otomatik

[10] ATSEC Information Security Corporation,ISMS Implementation Guide 2007

oluşturabilmektedir. Aynı zamanda kurumların kendi yapılarına göre değişiklik yapılabilmekte ve alınacak çıktılarla sistemin daha kolay anlaşılabilir niteliği kazanması sağlanabilmektedirler.

Örnek Risk Değerlendirme Yöntemi Dokümanı;

	SEMBOLİK BILISIM LTD.ŞTİ. RİSK DEĞERLENDİRME YÖNTEMİ DOKÜMANI	
YAYIN NO: 27001-RDY-01	DOKUMAN ADI:DOK-RDY-V1	VER:0.1

Amaç

Risk Yönetim Süreci'nde risklerin ne şekilde değerlendirileceği, hangi kriterlere göre kontrol uygulanıp uygulanmayacağı, hangi kritere göre artık risk olarak kabullenileceğini belirleyen Risk Değerlendirme Yöntemi'nin belirlenmesi ve ne şekilde çalışacağının düzenlenmesi.

Kapsam

Tüm BGYS süreçlerini kapsar.

Risk Değerlendirme Yöntemi

Tablo 4.Risk Skor (Derecelendirme) Matrisi

Tarih : Proses/Sistem : Takım :	**RİSK DERECELENDİRME MATRİSİ**		Düzenleyen : Revizyon No : Revizyon Tarihi :
	OLASILIK		
ETKİ	1 (DÜŞÜK)	2 (ORTA)	3 (YÜKSEK)
1 (DÜŞÜK)	1	2	3
2 (ORTA)	2	4	6
3 (YÜKSEK)	3	6	9

Şirketimizin BGYS süreçlerinde, Risk Değerlendirme Yöntemi olarak, gerek sebep-sonuç ilişkilerinin değerlendirilmesindeki genel kullanım alanı gerek öncelik

belirlemesindeki hızlı cevap verme yeteneği nedeniyle "Risk Değerlendirme Karar Matrisi Yöntemi" kullanılacaktır.

Öncelikle bilgi varlığının üzerinde mevcut ya da muhtemel riskin olasılık ve etki analiz değerleri çarpılarak toplam risk derecelendirme skoruna ulaşılacaktır.

Olasılık ve etki analizinde 3 seviyeli derecelendirme kullanılacak ve toplam risk skoru 3 ve aşağısında olanların riski "Düşük", toplam risk skoru 4 ile 6 arasında olanların riski "Orta" ve son olarak 9 olanların riski "Yüksek" olarak nitelendirilecektir. Riskin toplam skorunun 1 olması, teknolojinin yüzde yüz güvenliğe imkan sağlayamadığı durumların var olması, verilen hizmetin kritiklik durumu ve yönetim kurulu kararı ile gerekçeleri belirtilen risklerin kabul edilmesi sağlanacaktır.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

2.2.5.2.Riskleri Tanımlama

Risk değerlendirmesi veya analizi; kaynakları belirlemek ve riski tahmin etmek amacıyla bilginin sistematik kullanımı olarak tanımlanmaktadır[11]. Risk yönetim sürecinin risk değerlendirme bölümü, riskleri tanımlama ile başlamaktadır. Burada öncelikle risk değerlendirmesinin yapılacağı sınırları belirten kapsam belirleme çalışması yapılacak daha sonra varlıklar ve sorumluları belirlenecek, bu varlıkların mevcut tehdit ve açıkları üzerinde durulacaktır. En son işlem olarak ise bu tehdit ve açıklara göre olasılık ve etki analizleri yapılarak risk seviyeleri derecelendirilecektir.

2.2.5.2.1.Kapsam Belirlenmesi

Riskleri tanımlama işleminin ilk adımı kapsam belirlenmesidir. Burada kapsamın bilgi güvenliği amacına yönelik olarak en başta olması gereken şekilde yapılması, öncelikle sistemin doğru yönde gerçekleştirilmesini sağlayacak ve gereksiz çalışmaların önüne geçecektir[12].

"Bu risk analizi Sembolik Bilişim LTD. Şirketi'ndeki Sistem Yönetimi, Ağ Yönetimi, Yazılım ve Teknik Hizmetleri işlemlerinde kullanılan tüm donanım, yazılım ve personeli kapsar" ifadesi Risk Yönetim Süreci'nin kapsamını oluşturacaktır.

[11] TSE ISO/IEC 27001 Bilgi Teknolojisi-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler Standardı,2006
[12] Doğan Eskiyürek,BGYS Risk Yönetim Süreci Klavuzu,TUBITAK-UEKAE,Kocaeli,2007

2.2.5.2.2. Varlıkların Belirlenmesi

Kapsam belirleme işleminin tamamlanmasından sonra üzerinde risk değerlendirmesinin yapılacağı bilgi varlıklarının belirlenmesi işlemi gerçekleştirilecektir. Varlık, kuruluş işin değeri olan herşeydir[13]. Kuruluş için değer taşıyan her olgunun güvenliğinin sağlanması gerekliliği yapılacak çalışmanın amacını oluşturmakta ve tüm varlıkların koruma altına alınması hedeflenmektedir. Bunun için öncelikle varlıkları envanter dahilinde açıklayıcı bir şekilde sıralamak ve sınıflandırmak gerekmektedir.

Varlık envanteri çıkarılırken öncelikle bilgi ve süreç değerlendirilmeleri yapılmalı daha sonra bunları taşıyan ya da barındıran yazılım ve donanımların güvenlik açısından değerlendirilmeleri ve sınıflandırılmaları işlemi gerçekleştirilmelidir. Burada tek bir envanterden söz edilebileceği gibi yazılım-donanım-bilgi ve süreç gibi ayrı ayrı tablolarda da tutulması sağlanabilir. Varlık envanteri oluşturulurken azami ölçüde bahsedilmesi gereken maddeler;

Varlık

Kuruluş için değeri olan ve korunması gereken herşeydir. En somut varlık donanımdan en soyut varlık bilgiye kadar tüm unsurlar belirtilmelidir.

Varlık Grubu

Varlık envanterinin kolayca tasnif edilebilmesi, listede aranan varlığa kolay erişim sağlanabilmesi, düzenli yapının oluşturulması gibi amaçlarla varlıkların gruplandırılması işlemine gidilmektedir. Burada aynı süreç için kullanılan varlıklar gruplandırılabileceği gibi(yedekleme, sistem yönetimi, insan kaynakları) varlığın kendi yapısına göre de gruplandırma yapılabilir.(donanım, yazılım, doküman)

Varlık Sahibi

Varlığın sahibi, onu kullanan ve aynı zamanda bilgi güvenliğini sağlamakla sorumlu olan kişi ve kişilerdir. Burada sorumluluk anlamında kullanılan varlık sahibi örnek vermek gerekirse İnsan Kaynakları Yönetimi Departmanı ile ilgili bilgilerin sahibi İKY Departman Müdürü'dür. Varlık değerlerinin belirlenmesi ve risk tanımlamalarında

[13] TSE ISO/IEC 27001 Bilgi Teknolojisi-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler Standardı,2006

BGYS ekibine yardımcı olmak ya da çalışmalarda bizzat görev almak sorumluluğundadır.

Emanetçi

Varlığın sahibi olmamasına rağmen, varlığın sağlıklı bir şekilde sürekliliğinin idamesini sağlayan rolündeki kişi veya kişilerdir[14]. Örnek vermek gerekirse web üzerinden satış yapan bir firmada malzemelerin satış bilgileri pazarlama bölümü sahipliğinde iken emanetçisi kurum web sayfası yöneticisidir.

Bulunduğu Yer

Hem envanteri yeni okuyan bir yönetici için varlıkların yerlerinin öğrenilmesi, hem de felaket durumlarında ve sonralarında hareket tarzlarının varlıklarının yerlerine göre oluşturulduğu göz önüne alındığında envanterde fiziksel mevkilerin belirtilmesi uygun olacaktır.

Gizlilik Değeri

Varlığın erişimine izin verilmeyen kişiler tarafından erişilip, açığa çıkması ve kötü niyetle kullanılması sonucunda doğacak zararın değerini belirtir. Açığa çıkacak bilginin kurum açısından kritikliğine, kurumun bu bilginin öğrenilmesiyle göreceği etki derecesine göre Düşük, Orta ya da Yüksek olarak sınıflandırılabilmektedir.

Bütünlük Değeri

Varlığın bütünlüğünün silinerek ya da değiştirilerek bozulması sonucu doğacak zararın değerini belirtir. Kontrol dışı değişen bilginin kritikliği ve değişmesi ya da silinmesi durumunda kurumun göreceği etki derecesine göre Düşük,Orta ya da Yüksek olarak sınıflandırılabilmektedir.

Erişilebilirlik Değeri

Varlığın istenilen anda ve durumda erişilebilirliğinin sekteye uğraması durumunda doğacak zararın değerini belirtir. Varlığa zarar gelmesi durumunda bilginin erişilebilirliği ve bu erişememe durumunda kurumun göreceği etki derecesine göre Düşük,Orta ve Yüksek olarak sınıflandırılabilmektedir.

[14] Fatih Koç,BGYS Varlık Envanteri Oluşturma ve Sınıflandırma Klavuzu,TUBITAK-UEKAE,Kocaeli,2008

Değer

Gizlilik, bütünlük ve erişilebilirlik değerleri kullanılarak bunların matematiksel değerlerinin toplanması ya da çarpılması ile belirlenebilecek bir değerdir.

Varlığın Eklenme Tarihi

Varlığın daha sonraki tarihsel gelişiminin takip edilmesi ya da risk değerlendirilmesinin yapılıp yapılmadığını kontrol edilebilmesi için envantere eklendiği tarihin belirtilmesi uygun olacaktır.

Açıklama

BGYS ekibine varlık hakkında kısaca bilgiler verecek, varlığın kısa tanımı ve ilgili açıklamalar eklenmelidir. Örnek varlık envanteri tablosu;

	SEMBOLİK BILISIM LTD.ŞTİ.VARLIK ENVANTERİ	
YAYIN NO: 27001-VE-01	DOKUMAN ADI:DOK-VE-V1	VER:0.1

Amaç

Kurumda risk yönetim sürecinin uygulanacağı mevcut tüm bilgi varlıklarının listesini çıkarmaktır.

Kapsam

Yazılım, donanım, fiziksel güvenlik dahil tüm bilgi varlıklarını kapsamaktadır.

Tablo 5. Varlık Envanteri Tablosu

Tarih : Proses/Sistem : Takım :				**BGYS VARLIK ENVANTERİ**				Düzenleyen : Revizyon No : Revizyon Tarihi :			
Sıra No	Varlık Grubu	Varlık	Sahibi	Emanetçisi	BY	GD	BD	ED	Toplam Değer	ET	A

Kaynak: Koç (2008:10)

Burada BY Bulunduğu Yer GD Gizlilik Değeri, BD Bütünlük Değeri, ED Erişebilirlik Değeri, ET Eklenme Tarihi, A Açıklama olarak kısaltılmıştır.

Sıra No:5

Varlık Grubu:Veritabanları

Varlık:Personel Veritabanı

Sahibi:İnsan Kaynakları Şube Müdürü Ömer PARLAK

Emanetçisi:Sistem Yöneticisi Seyit SEVER

Bulunduğu Yer: Veritabanı Sunumcusu

Gizlilik Değeri:2

Bütünlük Değeri:2

Erişebilirlik Değeri:3

Toplam Değer:12

Eklenme Tarihi:24 Ocak 2010

Açıklama:IK Sunumcusunda tutulan personel veritabanı tüm personelin bilgilerinin tutulduğu bilgi varlığıdır.

Burada tüm bilgi varlıkları sıralanacaktır.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

2.2.5.2.3.Varlıkların Kabul Edilebilir Kullanımı

BGYS ekibi tarafından varlıkların ve güvenlik derecelendirmelerinin yapılmasından sonra bu belirlemelere uygun olarak hangi varlığın ne şekilde kullanılması gerektiği, hangi bilginin ne şekilde depolanıp, işlenebileceği ve ne şekilde kurum dışına çıkarılabileceği gibi konularda personeline bilgilendirme konusunda gerekli prosedür ve talimatları oluşturmalıdır.

Örnek olarak dizüstü bilgisayar sahibi olan tüm personele dizüstü bilgisayar kullanım prosedürü hazırlanarak bilgisayarın ne şekilde kullanılacağı ve bilgilerin nerelerde depolanacağını bildirmelidir.

Örnek Dizüstü Bilgisayar Kullanım Politikası'nda, diğer belgelendirmelerde olduğu gibi amaç ve kapsam belirlenecek ve daha sonra dokümanın uygulama bölümünde kullanım ve bilgi depolama kuralları anlatılacaktır.

	SEMBOLİK BILISIM LTD.ŞTİ. DİZÜSTÜ BİLGİSAYAR KULLANIM POLİTİKASI	
YAYIN NO: 27001-DBK-01	DOKUMAN ADI:POL-DBK-V1	VER:0.1

Amaç

Kurum içerisindeki dizüstü bilgisayarların kullanım şartlarını belirlemek.

Kapsam

Kurum içerisinde kullanılan tüm dizüstü bilgisayarları kapsar.

Uygulama

Genel Konular:

Dizüstü bilgisayar kullanıcıları hazırlanan dizüstü bilgisayar kullanım politikasını okuduğuna dair tebliğ formu imzalayacaklardır.

Dizüstü bilgisayarların kullanımı konusunda Teknik ve İdari Hizmetler bölümü tarafından tüm personele kısa bir brifing verilecek ve katılan kişi ve tarih listeleri dokümana eklenecektir.

Dizüstü bilgisayar kullanıcıları bilgisayarlarını Teknik ve İdari Hizmetler Departmanı'dan zimmet belgesi imzalayarak alacaktır. Geri iade edilirken zimmet belgesinde belirtilen tüm aksesuarları ile birlikte teslim edilecektir. (Çanta-Fare vs.)

Dizüstü Bilgisayar üzerlerine kurum numarası ve işlenilen bilginin derecesini gösterir etiket basılacaktır.

Güvenlik Konuları;

Kurum bilgi işlem ağına sadece izin verilmiş dizüstü bilgisayarlar bağlanacak, şahsi bilgisayarlar kesinlikle bağlanmayacaktır.

Kuruma ait taşınabilir bilgisayarlarda sadece yapılan işe yönelik doküman/dosyalar işlenebilecektir.

Taşınabilir bilgisayarlar gözetimsiz bırakıldıklarında fiziksel olarak emniyete alınacak, işletim sistemi erişimi kitlenecektir.

Ağa bağlı dizüstü bilgisayarlarda işlenilen bilgi kendi harddisklerinde depolanmayacaktır. Üzerinde işlem yapılacak doküman merkezi dosya sunumcusundan bilgisayar harddiskine alınarak düzenlemeler yapıldıktan sonra tekrar sunumcuya kopyalanacaktır.

Dizüstü bilgisayarların virus programı ve işletim sistemleri güncellemelerinin yapılabilmesi için ağa bağlı olmasa dahi teknik hizmetlerden destek alınarak işlemlerin tamamlanması sağlanacaktır.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

Bu şekilde hazırlanacak dokümanlar ile tüm personele kullanım politikaları oluşturulması gereken varlıklar konusunda bilgilendirme yapılmalıdır.

2.2.5.2.4.Bilgi Etiketleme ve İşleme

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'ne göre kurumda etiketlenmemiş ve kontrol altına alınmamış hiçbir bilgi varlığı bulunmamalıdır. Buna göre üzerinde bilgi işlenen/depolanan tüm bilgi varlıkları ihtiva ettikleri bilginin güvenlik derecesine göre etiketlenmeli ve kontrol altına alınmalıdır. Burada bilgi varlıklarının gizlilik dereceleri Gizli-Hizmet İçi Kullanım-Genel Kullanım olarak etiketlenecektir.

Örnek olarak; üzerinde kurum için hayati önem taşıyan projelerin ve yazışmaların işlendiği dosya sunumcusu gizli olarak belirlenmeli ve etiketlenmelidir.

2.2.5.2.5. Tehdit ve Açıkların Belirlenmesi

Tehdit, herhangi bir bilgi varlığının bilerek ya da kazayla zarar görmesine neden olabilecek olay ya da durumlardır. Tehditlere örnek olarak deprem, sel gibi doğal tehditler, elektrik kesintisi gibi çevresel tehditler, ağ saldırısı,yetkisiz erişim gibi insan kaynaklı tehditler sayılabilir.

Burada önemli olan her bir varlık üzerinde oluşabilecek tüm tehditlerin detaylı bir şekilde incelenerek göz ardı edilmemesidir. Bununla ilgili olarak daha önce yaşanmış tecrübeler, bilgi teknolojilerinin ve güvenlik konularının yakından takibi, mevcut tehdit tabloları kaynak olarak kullanılmalıdır.

Açık ise, bilgi güvenliğini zedeleyebilecek zayıflık, hata ve kusurlardır. Bir tehditin var olduğu durumlarda tehlike arz etmektedir. Örnek olarak web sunumcunun yazılım port açığı, bu açığı kullanarak kötü niyetli bir kişinin sisteme sızmaya çalışması ile tehlike arz edecektir.

Tablo 6. Tehdit ve Açık Tablosu

Sıra No	Olayın Cinsi	Tehdit / Açık	Kaynağı
1	Tehdit	Deprem/Sel/Fırtına/Yıldırım	Doğal Kaynaklı (Hizmet Verememe)
2	Tehdit	Bombalama/Silahlı Saldırı	İnsan Kaynaklı Bilerek (Hizmet Verememe)
3	Tehdit	Donanım Arızaları	İnsan Kaynaklı Kazayla (Hizmet Verememe)
4	Tehdit	Güç Dalgalanmaları	İnsan ve Çevre Kaynaklı (Hizmet Verememe)
5	Tehdit	Personel Hataları	İnsan Kaynaklı (Hizmet Verememe-Yetkisiz Erişim)
6	Tehdit	Lisansız Yazılım Kullanımı	İnsan Kaynaklı Bilerek (Yetkisiz Erişim-Hırsızlık-Hizmet Verememe)
7	Tehdit	Kullanıcı Kimliklerinin Çalınması	İnsan Kaynaklı (Hırsızlık-Yetkisiz Erişim)
8	Tehdit	Ağ Cihazlarının Arızalanması	İnsan ve Çevre Kaynaklı (Hizmet Verememe)
9	Açık	Binada Yeterli Güvenliğin Bulunmaması	İnsan ve Çevre Kaynaklı (Yetkisiz Erişim-Hırsızlık)
10	Açık	Eski Güç Kaynakları	İnsan Kaynaklı (Hizmet Verememe)
11	Açık	Periyodik Yenilemenin Yapılmaması	İnsan Kaynaklı (Hizmet Verememe)
12	Açık	Yama ve Kayıt Yönetimi Eksiklikleri	İnsan Kaynaklı (Yetkisiz Erişim-Hassas Bilginin Açığa Çıkması)
13	Açık	Erişim İzinlerinin Yanlış Verilmesi	İnsan Kaynaklı Yetkisiz Erişimi (Yetkisiz Erişim)

Tablo 6'nın devamıdır.

14	Açık	Saklama Ortamlarının Doğru Silinmemesi ve İmha Edilmemesi	İnsan Kaynaklı (Hassas Verinin Ortaya Çıkması,Yetkisiz Erişim)
15	Açık	Korunmayan Haberleşme Hatları	İnsan Kaynaklı (Haberleşmenin Dinlenmesi)
16	Açık	Dokümanın Güvensiz Saklanması	Hırsızlık
17	Açık	Eğitim Eksikliği	İnsan Kaynaklı (Personel Hataları
18	Açık	Donanım ve Yazılımların Yanlış Kullanılması	İnsan Kaynaklı (Personel Hataları)

Kaynak: Eskiyörük (2007:10)

Açıkların belirlenerek dokümante edilmesinde, teknik olarak yazılım tarama araçları, yüzyüze görüşme ya da dokümantasyonun kontrolü gibi araçlar kullanılmaktadır. Ayrıca bilgi güvenliği açık liste ve veritabanlarının yayımlandığı web siteleri ve e-posta grupları, üretici uyarıları ve denetim/test raporları da mevcut açıkları ortaya koyabilmektedir.

Tehdit ve açıkların sadece daha önce yaşanılan tecrübeler, bilişim teknolojilerinin yakından takibi ile belirlenebileceği unutulmamalı ve bu konular üzerinde görevlendirme/sorumluluklar dikkatlice belirlenmelidir. Bilişim teknolojilerinin yakından takibinin, genellikle yeni çıkan açıkların belirlenmesi ile sürekli devam ederek yaşayan bir süreç olduğu görülmektedir. Bu tehdit ve açıklara en kısa sürede müdahale edilerek kayıtlara eklenmesi ve gerekli kontrollerin oluşturulması işlemleri BGYS'nin atar damarıdır.

Tehdit ve açıkların oluşturulmasında Boşluk (Gap) analizi karşımıza çıkmaktadır. O ana kadar kurumun karşısına çıkan tehdit ve açıklara hangi kontrollerin yapıldığı ve yapılmaya devam edildiği incelenmeli ve ona göre kayıtlar oluşturulmalıdır.

Tablo 6’da sayılanlar gibi birçok tehdit ve açık mevcut olmakta olup, yapılacak boşluk analizinden sonra kendi kurum ve bilgi işlem merkezlerine göre uyarlanmalıdır. Gözden en ufak noktayı kaçırmamak, önemle üzerinde durulması gereken bir konudur.

2.2.5.3.Risk Çözümleme ve Değerlendirme

Risk çözümleme; kuruluş varlık envanterine göre gerçekleştirilen tehdit ve açık belirleme işlemlerinden sonra, varlık, tehdit ve açıkların BGYS ekibi tarafından topluca göz önünde bulundurularak potansiyel risklerin üzerinde detaylı bir şekilde çalışılmasıdır.

Yapılacak çalışma sırasında kuruluşun yapısı, personeli, iş süreçleri, süreklilik yaklaşımının yanısıra, yasal ve sözleşmeden doğan sorumluluklar da dikkate alınmalıdır.

2.2.5.3.1. Risk Derecelendirme

Risk derecelendirme, risk çözümleme işleminde BGYS ekibi tarafından kuruluş bilgi varlıkları üzerindeki risklerin nicel ya da nitel olarak ifade edilmesidir. Buradan çıkacak sonuca göre risklere müdahale, önceliklendirilecektir. Tehdit ve açıkların meydana gelme olasılıkları ve etkilerinin çarpımı olarak ifade edilir.

2.2.5.3.1.1. Olasılık Değerlendirme ve Etki Analizi

BGYS ekibi, risk derecelendirme işleminde, öncelikle bir açığın mevcut tehditler çerçevesinde meydana gelme olasılığının belirlenmesi için varlığı kullanan diğer departman personeli yardımıyla bir olasılık değerlendirme çalışması yapar. Bu çalışmada açığın cinsi ve önemi, mevcut kontrollerin durumu ve etkinliği, tehditin genel yapısı faktörleri dikkate alınmalıdır.

Olasılık değerlendirmede ilk yapılacak işlem BGYS ekibi tarafından kaç kademeli bir değerlendirme yapılacağı ve bu değerlendirmelerin ne şekilde standartlaştırılacağının belirlenmesidir. Burada düşük, orta, yüksek gibi niteleyici ifadeler kullanılabileceği gibi bu ifadelerin rakamsal olarak karşılıkları da kullanılabilmektedir.

Tablo 7. Olasılık Seviyeleri ve Açıklamaları

Olasılık Seviyesi	Açıklama
Düşük (1)	Tehdit kaynağının açıklığı öğrenip, kullanma olanağı düşük ve açıklığın gerçekleşmesini önleyecek kontroller mevcut
Orta (2)	Tehdit kaynağının açıklığı öğrenip, kullanma olanağı yüksek fakat açıklığın gerçekleşmesini önleyecek kontroller mevcut
Yüksek (3)	Tehdit kaynağının açıklığı öğrenip, kullanma olanağı yüksek ve alınan önlemler bulunmamakta ya da etkisiz kalmaktadır.

Kaynak: Eskiyörük (2007:13)

Etki analizi ise mevcut açıkların meydana gelmesi durumunda kurumun yaşayacağı etkinin nicel ya da nitel ifadesidir. Analizde dikkat edilen hususlar varlığın görevi, kritikliği, varlığın etkilediği verinin hassasiyeti ve varlığın mali değeri gibi bilgilerdir. Bu bilgiler önceden oluşturulmuş iş etki analizlerinden temin edinilebileceği gibi ilgili varlığın gizlilik, bütünlük ve erişilebilirlik katsayılarının gözönüne alınarak açığın meydana gelmesi durumunda yaşanılacak etkilerin değerlendirilmesi ile de oluşturulabilir. BGYS ekibi, olasılık değerlendirmesinde olduğu gibi kaç dereceli değerlendirme yapacağının ve hangi koşullarda hangi dereceleri atayacağının standartlaştırılması kararlarını vermelidir.

Tablo 8. Etki Analizi Dereceleri ve Açıklamaları

Etki Derecesi	Açıklama
Düşük (1)	Açığın gerçekleşmesi durumunda kurumun kritik bilgileri az etkilenir, Kurumun misyonu ve prestiji etkilenmez.Maddi hasar az olur.
Orta (2)	Açığın gerçekleşmesi durumunda kurumun hassas bilgileri etkilenir ve kurum zarara uğrayabilir,misyon ve prestij etkilenebilir
Yüksek (3)	Açığın gerçekleşmesi durumunda kurumun en hassas bilgileri etkilenir ya da kaybedilir,maddi zarar büyük olur.İnsan hayat kaybı ya da yaralanmalar yaşanabilir,misyon ve kurum çıkarları büyük zarar görebilir.

Kaynak: Eskiyörük (2007:14)

2.2.5.3.1.2.Risk Derecelendirme İşleminin Yapılması

BGYS ekibi olasılık ve etki analizi işlemlerini tanımladıktan sonra tüm Risk Yönetim Süreci'ne kaynak sağlayacak risk derecelendirme işlemini gerçekleştirecektir. Burada risklerin, ekibin vereceği karara göre nicel ya da nitel şekilde değerlendirmeleri yapılarak ifade edilecek ve böylece risklere değer atanacaktır. Bu değer riskin önem derecesini belirtecektir. Yüksek çıkan değerlere daha fazla önem ve öncelik verilecektir.

BGYS ekibi tavsiyesi sonrası yönetim kurulu tarafından hangi derecedeki risklerin hangi bölümde değerlendirileceğine karar verilecek ve Risk Değerlendirme Yaklaşımına göre hangi derecedeki risklerin kabul edileceği belirlenecektir.

Risk derecesi ölçülürken kurumun alacağı karara göre öncelikle varlığın gizlilik, bütünlük ve erişilebilirlik değerleri göz önüne alınacak, bunlara göre verilecek etki analizi değeri ile olasılık değeri çarpılarak risk skoruna ulaşılacaktır.

Bu çalışma ile tehdit ve açıklara değerler atayıp onları kurum yapısına göre derecelendirme yaparak, oluşturulacak kontrollerin seçilmesi ve önceliklendirmesi işlemine veri sağlanmaktadır. Riskler öncelikle varlık envanterinden sağlanan gizlilik, bütünlük ve erişebilirlik değerleri ve daha sonra olasılık ve etki analizi değerleri ile ölçülebilmekte ve derecelendirilmektedir.

Tablo 9. Risk Dereceleri ve Açıklamaları

Risk Derecesi	Açıklama
Düşük (0-3)	Riske karşı önlem alınıp alınmayacağı sorumlusu tarafından karar verilebilir ve önlem alınmayacaksa risk kabul edilebilir.
Orta (4-6)	Riske karşı önlem alınması gerekmektedir.Alınacak önlemler uygun bir sürede planlanmalı ve uygulanmalıdır.
Yüksek (9)	Riske karşı en yakın zamanda önlem almak gerekmektedir. Sistemin güvenli bir şekilde çalışmasına devam etmesi alınacak önleme bağlıdır.

Alınacak karara göre olasılık ve etki analizinde nicel ya da nitel derecelendirme yapılabilir. Burada sonuçların daha göze çarpıcı şekilde belirtilebilmesi ve daha sonra

yapılacak risk işleme yöntemlerine kolay entegre olması açısından nicel yöntemler kullanılacaktır. Örnek Risk Derecelendirmesi Tablosu;

	SEMBOLİK BILISIM SIRKETİ RİSK DEĞERLENDİRME/DERECELENDİRME TABLOSU	
YAYIN NO: 27001-RDT-01	DOKUMAN ADI:DOK-RDT-V1	VER:0.1

Amaç

İcra edilen tüm risk derecelendirme işlemlerinin dokümante edilerek kayıt altına alınmasıdır.

Kapsam

Kurum bilgi varlıkları çerçevesinde mevcut ve potansiyel tüm riskleri kapsamaktadır.

Risk Değerlendirme/Derecelendirme

1-Varlık:Dizüstü Bilgisayar

Varlık Değeri (GizlilikXBütünlükXErişebilirlik) : 2 x 2 x 2 =8

Tehdit/Açık: Ağa bağlı dizüstü bilgisayarın kurum dışında kullanımında çalınması ve içerisindeki önemli bilginin yanlış ellere geçirilmesi

Olasılık: Tehdidin ortaya çıkma olasılığı orta olarak belirlenmiştir. “2”

Etki:Varlık değerleri göz önünde bulundurularak kurum ağı içerisinde kullanılan dizüstü bilgisayarın önemli bilgi ihtiva etmesi ve bu bilginin çalınarak yanlış ellere geçmesi etkisinin fazla olacağını göstermektedir. “3”

Risk Değeri olarak ise 2 x 3 = 6 olarak belirlenerek dokümante edilecektir. Kurum, Bilgi İşlem Merkezi’nin belirleyeceği Risk İşleme Planı’na göre risk işlenecek ve buna göre işlem yapılacaktır. Risk derecelendirmesi de bu işleme göre yapılacaktır. Kurumun ortaya koyduğu kriterlere göre 6 değeri hangi bölümde incelenecek ise (Düşük-Orta-Yüksek) buna göre işlem yapılacaktır. Risk değeri 6 olan bir tehdit eğer kurumun göze alamayacağı değerde ise karşı kontroller oluşturulacak, eğer bu kontrollerin maliyeti fazla ve karar o yönde alınacaksa aktarılacak, ya da 6 değeri göze alınabilirse artık risk olarak yönetim onayı istenecektir.

2-Varlık:Elektronik Posta Sunumcusu

Varlık Değeri: 2 x 2 x 3 = 12

Burada kurumumuzun tüm yazışma ve işlemlerini elektronik posta üzerinden yaptığı gözönüne alınarak gizlilik, bütünlük ve erişebilirlik değerlendirmeleri bu senaryoya göre yapılmıştır.

Tehdit/Açık:Elektronik Posta Sunumcusuna aynı anda çok sayıda istek yapılmasıyla

hizmetin gerekli cevabı veremeyerek durdurulması.(Servis Durdurma Atağı)

Olasılık: Burada olasılık değeri olarak “3” seçilmiştir.

Etki: Saldırının meydana gelmesi durumunda yukarıda belirtilen senaryoda önemli işlemlerin sekteye uğrayacağı, hizmetin geri getirilene kadar kaybedilecek maddi değerlerin fazla olacağı değerlendirilmektedir. “3”

Risk Değeri: 3 x 3 =”9” olarak çıkmış ve yukarıdaki örneğe göre daha fazla öneme

sahip olunduğu gösterilmektedir.

Tablo 10. Risk Değerlendirme/Derecelendirme Tablosu

Tarih : Proses/Sistem : Takım :			**RİSK DEĞERLENDİRME/ DERECELENDİRME TABLOSU**		Düzenleyen : Revizyon No : Revizyon Tarihi :	
Sıra No	Varlık	Varlık Değeri	Tehdit / Açıklık	Olasılık	Etki	Risk Değeri (Olasılık X Etki)

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

Bunun gibi her tehdit ve açıklığa göre tek tek işlem yapılmalı ve çıkacak kapsamlı tablo/listeye göre kontroller, prosedürler ve talimatlar belirlenmelidir.

Kurum yapısına göre daha hassas derecelendirme yapmak isteyen BGYS yöneticileri oluşabilecek nicel değerlendirmeyi daha da arttırabilirler.

2.2.5.4.Risk İşleme Seçeneklerinin Tanımlanması

Kuruluş mevcut bilgi varlıklarına göre risk ve buna bağlı unsurları belirledikten sonra ilgili risklere karşı hareket tarzı seçeneklerini ortaya koymalıdır. Alınacak bu karar ileri ki bölümlerde gerçekleştirilecek risklerin işlenmesi ve kontrollerin uygulanması aşamalarında izlenecek yolları belirleyecek olup, BGYS ekibine bu aşamada dokümante edilen risk işleme yöntemlerine göre hareket etme olanağı sağlayacaktır. Kuruluşun kullanacağı yöntem örnekleri olarak,

a) Riskleri azaltmak ya da ortadan kaldırmak için kontrol önlemlerinin uygulanması,

b) Riskin göz ardı edilerek riskten kaçınılması,

c) Riskin sigorta ya da onarım kuruluşu gibi üçüncü taraflara aktarılması,

d) Risk ve sonuçlarının bilinerek geçerli sebepler dahilinde kabul edilmesi

seçenekleri sayılabilir. Bu seçeneklerinin hangi durumda, hangilerinin kullanılacağı tamamen kurum kararı olduğu gibi, farklı durumlarda aynı riske farklı seçenekler de uygulanabilir. Tüm seçenek ve anlamlarının dokümante edilmesi ve alınan tüm kararların açıklamalarının belirtilmesi hem standardın gerekliliği hem de ileri ki çalışmalara veri sağlaması açısından önemlidir.

2.2.5.5.Kontrol ve Amaçlarını Belirleme

Kuruluşlar, mevcut risklere karşı ne gibi seçenekleri olduklarını belirledikten sonra riski işleyerek ortadan kaldıracak ya da azaltacak bir kontrol tedbiri almaya karar vermeleri durumunda riskin giderilmesi amacına uygun bir kontrol mekanizması geliştirmelidirler. Bu çalışma yasal kurallar, sözleşme ve standartlara dayalı gereksinimler göz önüne alınarak yapılmalıdır. Kontrol seçimi işlemlerinde riskin ne kadar azaldığı ve risk kabul ölçütü dikkate alınmalıdır.

Riskleri istenilen düzeye çekmek ve oluşması mühtemel riskleri önlemekte kullanılacak kontroller teknik, yönetimsel ve operasyonel olarak 3 gruba ayrılmaktadır. İlk gruptaki teknik kontroller, güvenlik yazılım ve donanımları gibi bilgi güvenliğini teknik olarak sağlayıp idame ettirecek kontrollerdir. Bunlara güvenlik duvarı, saldırı tespit sisteminin kurulması, kriptolama örnekleri verilebilir. İkinci gruptaki yönetimsel kontroller ise, mevcut politika ve prosedürlerin uygulanmasını sağlayacak kontrollerdir. Bunlara örnek olarak, kişilere sorumluluklar atanması, eğitim ve farkındalık çalışmaları verilebilir. Operasyonel kontroller, bilgi varlıklarının doğru bir şekilde kullanılmasını sağlamak için oluşturulacak kontrollerdir. Bunlara erişim kontrolü ve acil durum kontrolleri örnek sayılabilir. Herhangi bir riski ortadan kaldırmak için birden fazla kontrol çeşidi birlikte kullanılabilir.

Kontrol önerileri BGYS ekibi ve onlara yardımcı departman personeli tarafından gerçekleştirilen risk derecelendirmeleri sonucunda risklerin ortadan kaldırılması ya da

azaltılmasını sağlayacak yapıda belirlenecektir. Uygulanacak kontroller ve bu kontrollerin amaçları oluşturulurken ISO/IEC 27001 EK-A ve ISO/IEC 27002 gibi belgeler kaynak olarak alınacak, kuruluşa özgü farklı kurallar eklenebilecektir. Hangi kaynaktan alınırsa alınsın ilgili kontrol ve amaçları açıklamaları ile birlikte dokümante edilmelidir.

Daha önceki aşamalarda yapılan boşluk ve zafiyet analizlerinden sonra hali hazırda kullanılan kontrollerin belirlenmesi işlemi tamamlanmıştı. Bu aşamada ise mevcut kontrollerden, açıklanan risk derecelendirmesine göre geliştirilecek olanların ya da yeni kontrollerin ne şekilde uygulanacağı belirlenecektir.

Burada kapsamlıca oluşturulan risk yapılarına göre uygulanacak kontrollerin belirlenmesi işlemi tüm BGYS ekibi ve ilgili sistem/donanımı kullanan kişilerce tamamlanarak uygulamaya sokulacaktır. Bu noktada varlık envanterinin oluşturulması gibi tüm kurum/merkeze iş düşmekte ve bu sistemin sadece BGYS ekibinin işi olmadığı bilincinin tüm personele aktarılması sağlanmaktadır. Uygulama ve donanımı bir fiil kullanan personelin konuya göstereceği katkı ile bilgi güvenliği istenilen düzeye getirilmeye çalışılacaktır.

Dokümanda kontrollerin ve ne şekilde uygulanacaklarının belirlenmesine ek olarak, mevcut ya da olası riskler üzerinde gerçekleşmesi beklenen etkilerin de belirtilmesi gerekmektedir. Burada belirlenen kriterlere göre oluşturulan kontrol ile riskin hangi düzeye indirilmesi amaçlandığı dokümante edilerek, daha sonra kontrol et aşamasına veri olması sağlanacaktır. Örnek olarak istenmeyen ya da reklam amaçlı gönderilen (spam) elektronik postaların filtrelenmesi kontrolünde bir günde alınan bu yapıdaki postaların yüzde kaçının bloklanması gerektiği burada belirtilecektir.

BGYS kontrollerinin, amaçlarının, sorumlularının ve nasıl gerçekleştirileceğinin belirleneceği bu bölüm, risk yönetim sürecinin yol haritası anlamına gelmekte ve risk işleme planlarına da kaynak teşkil etmektedir. Uygulanacak kontrollerin seçilmesi işlemleri risk yönetim süreci içerisinde dikkate alındığında kontrollerin uygulanmasının yol haritası, ISO/IEC 27001 BGYS Standardı'nın genel süreci dikkate alındığında ise risk işleme planlarının kaynağı olduğu görülmektedir. Bu işlemlerin neticesinde ise uygulanabilirlik bildirgesi ve yönetim onayının alınmasına müteakip kontrollerin uygulanması sağlanacaktır.

Kontrollerin seçildiği ve dokümante edildiği belge de olması muhtemel bilgiler aşağıda belirtilmiştir.

Varlık: Varlık envanterinden, üzerinde tehdit ve açık olduğu tahmin edilen ve ona göre risk değerlendirmesi yapılan varlığın kendisi.

Tehdit/Açık: Risk değerlendirmesinin yapıldığı ve varlığın güvenlik kriterlerine göre zarar vermesi muhtemel olay.

Risk Değeri: Olasılık ve etki analizi sonuçlarının çarpıldığı değer ya da bu değere karşılık gelen risk önemidir.(“6” ya da “Orta” gibi) Bu değer kontrollerin uygulanmasındaki önceliklerin belirlenmesinde önemli bir kriterdir.

Uygulanacak Kontrol: Risklerin giderilmesi ya da makul bir seviyeye çekilmesinde kullanılacak kontrolün açıklandığı bölümdür. BGYS’nin pratiği olarak görülen kontrollerin uygulanması bu bölümler kullanılarak yapılacağından açıklamaların eksiksiz ve istenilen durumu tam yansıtır şekilde olması kritik öneme sahiptir.

Sorumlular: Kontrolleri uygulayacak kişilerin listelendiği bu bölümde ilgili kontrollerin hangi departmanda ve kimler aracılığıyla uygulanacağı belirtilecektir. Sorumlular belirtilirken yardım alacağı kişilerin de belirtilmesi ile açıklık kazanmış olacaktır. Örneğin Personel Şube ile ilgili bir kontrol gerçekleştirilecekse bu şube personelinin de sorumlu bölümünde belirtilmesi uygun olacaktır.

Atıfta Bulunulan Doküman:Eğer uygulanacak kontrol, oluşturulan/oluşturulacak politika ya da prosedürler ile desteklenecekse burada dokümanın adı ve numarası belirlenecektir. Bu durumda kontrol üzerinde kısa açıklama yapılarak dokümanın okunmasına işaret edilecektir.

Örnek vermek gerekirse;

TSE	SEMBOLİK BILISIM LTD.ŞTİ. KONTROL VE AMAÇLARINI BELİRLEME TABLOSU	SBS
YAYIN NO: 27001-KT-01	DOKUMAN ADI:DOK-KT-V1	VER:0.1

Amaç

Tüm bilgi varlıkları çerçevesinde mevcut risklerin işlenmesi için uygulanacak kontrollerin belirlenmesidir.

Kapsam

Tüm bilgi varlıklarını, mevcut ve potansiyel tüm riskleri kapsamaktadır.

Kontrol Tablosu

Tablo 11. Uygulanacak Kontroller

Tarih : Proses/Sistem : Takım :		**KONTROL VE AMAÇLARINI BELİRLEME TABLOSU**			Düzenleyen : Revizyon No : Revizyon Tarihi :	
Sıra No	Varlık	Tehdit / Açıklık	Risk Değeri	Uygulanacak Kontrol	Sorumlular	Atıfta Bulunulan Dokümanlar

1-Varlık:Dizüstü Bilgisayar

Tehdit/Açık: Ağa bağlı dizüstü bilgisayarın kurum dışında kullanımında çalınması ve içerisindeki önemli bilginin yanlış ellere geçirilmesi

Risk Değeri: 6 ya da “Orta”

Uygulanacak Kontrol: Öncelikle dizüstü bilgisayarlara Bios seviyesinde giriş şifresi tanımlanacaktır. Daha sonra bir dosya sunumcusu oluşturulacak, dizüstü bilgisayar kullanıcıları tarafından işlenen önemli bilgi ve belgeler bu dosya sunumcusuna taşınarak güvenlik arttırılacaktır.

Sorumlular:Dizüstü bilgisayarlara gerekli ayarların yapılması Teknik Hizmetler Şube Sorumlusu:Sebahattin YILMAZ, dosya sunumcusu oluşturulması Sistem Yönetim Sorumlusu Oğuzhan BAL, konu üzerinde hassasiyetle durmak ve kurum dışına çok önemli dokümanları çıkarmamak konusunda ise dizüstü bilgisayar kullanan herkes sorumludur.

Atıfta Bulunulan Dokümanlar: Bilgi Güvenlik Politikası Dokümanı , Dizüstü Bilgisayarı Kullanım Politikası , Bilgisayarla Uygulanacak Güvenlik İşlemleri Süreci

2-Varlık Elektronik Posta Sunumcusu

Tehdit/Açık: Elektronik Posta Sunumcusuna aynı anda çok sayıda istek yapılmasıyla

hizmetin gerekli cevabı veremeyerek durdurulması. (Servis Durdurma Atağı)

Risk Değeri: 9 ya da “Yüksek”

Uygulanacak Kontrol:Servis Durdurma Atağı olarak nitelendirilen bu atağa karşı, “Saldırı Tespit Sistemi”ve “Saldırı Önleme Sistemi” kurulacak ve sayısal imza güncellemeleri sürekli takip edilerek yeni imzalara karşı önlemler alınacaktır. Bilgi İşlem tarafından personel konu ile ilgili uyarılacak gönderileni belli olmayan elektronik posta ve içeriklerindeki dosyalar açılmayacaktır.

Sorumlular: Sistemlerin kurulması ve güncelleştirmelerin yapılması Güvenlik Sorumlusu İsa KARA, konunun personele bilgilendirilmesi Bilgi İşlem Şube Müdürü Alpay KOR ve kötü niyetli olabileceği düşünülen elektronik posta konusunda dikkatli olunması tüm personel sorumluluğundadır.

Atıfta Bulunulan Dokümanlar:Elektronik Posta Kullanımı Politikası, Saldırı Tespit veya Önleme Sistemi Uygulanması Süreci

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

2.2.5.6.Artık Risklere Yönetim Onayı İsteme

Esas amacı ilgili riski tamamen ortadan kaldırmak olan kontrol uygulamalarının yüzde yüz oranında başarılı olamadığı riskler de meydana gelebilmektedir. Bu durumda kurum BGYS ekibi önerisi ve yönetim kurulu kararıyla daha önce belirlenen kabul edilebilir risk seviyelerine göre işlem yapılacaktır. Eğer risk bu seviye üzerindeyse tekrar analiz ve azaltma işlemi gerçekleştirilecek, eğer bu seviye altında ise artık risk kabul edilerek nedenleri ile birlikte dokümante edilecektir. Böylece kuruluş yönetim kurulu, dış dünya ve kendi çalışanlarına bazı risklerin var olduğu ve bunlara karşı şu çalışmaları yaparak önlem almaya çalıştıklarını anlatmış olacaktır.

Bunların en temel nedenlerinden biri bilişim teknolojilerinde yüzde yüz güvenliğin sağlanamayacak nitelikte olmasıdır. Bilişim teknolojileri üzerinden bir hizmet verilmek isteniyorsa önüne geçilemeyecek riskleri de bulunmaktadır. İkinci örneği olarak ise maliyetlerin riskin gerçekleşmesi halinde getireceği zarardan daha fazla olduğunda karşılaşılandır. Üçüncü ve esas olması gerekeni ise bir riskin uygun kontrol ve işlemlerden geçirilerek tamamen bitmemesine rağmen düşük risk değerine sahip olmasıdır. Risk işleme yapıldıktan sonra göze alanılabilecek ufak risk değeri nedenleri

ile dokümante edilerek artık risk olarak yönetim onayı alınmalıdır. Bir örnek vermek gerekirse;

Kurumumuzda web sayfası sunumcusu bulunuyorsa verilen hizmet HTTP 80 portu üzerinden sağlanacaktır. Bu portun güvenlik nedeniyle kapatılması bu hizmetin verilmemesi anlamına gelmektedir. Bu yüzden HTTP 80 portu tüm isteklere açılır. Bunun karşılığında ise kötü niyetli kişiler bu açık portu kullanarak sisteminizin içerisine girebilmekte ve ağınıza sızma yapabilmektedir. İşte burada yüksek maliyetli çözümler de olsa yüzde yüz güvenlik sağlanamamakta ve artık risk olarak yönetim onayı istenmektedir.

İkinci örneğimiz ise dizüstü bilgisayarlardaki önemli bir bilgi ihtiva eden bilgisayarın çalınması durumudur. Personele bilgi güvenliği ile ilgili farkındalığı yaratmak için eğitim verilmiş ve dizüstü bilgisayar kullanım politikası oluşturularak kuralların belirlenmiş olmasına rağmen bilgisayarın kurum dışında kullanım için de izin veriliyorsa bazı riskler göze alınmış demektir. Burada personelin farkındalığına ve güvenine inanılmış ve karşılaşılacak tehlikeler göze alınmış demektir. Amaç, güvenlik ve verilen hizmetin dengede yürütülmesi, ilgili süreç yönetiminin başarı ile uygulanmasını temin edecek kontrollerin uygulanması ve bunların sonucunda ortaya çıkabilecek artık risklerin göze alındığını belirten yönetim onayının alınmasıdır.

2.2.6.BGYS'yi Gerçekleştirmek ve İşletmek İçin Yönetimin Yetki Vermesi.

İcra edilen tüm çalışmaların çerçevesi olan planla aşamasının sonuna gelindiğinde BGYS ekibinin, planlanan tüm kontrol ve hedeflerin uygulanabilmesi için yönetim kurulundan yetki alması gerekmektedir. Alınacak bu yetki bir nevi meşruluk olarak kabul edilmekte ve yapılacak tüm işlemlerin yönetim kurulu kararı olduğunun çalışanlara aktarılması sağlanmaktadır.

Bilgi Güvenliği Yönetim Sistemi'nden bahsederken bu standardın her bölümünde yönetimin desteğinin zarureti ve bunu kurum/merkezde bilişim teknolojilerini kullanan herkesin bilmesi gerektiğinden bahsetmiştik. İşte burada BGYS ekibinin yönetimin desteğini her noktada arkalarına almasının kanıtı olacak ve planlanan tüm işlemlerin bir özetini belirtecek yönetim onayı oluşturulacaktır.

Gerçekleştirilecek tüm politika ve prosedürlerin yönetim isteği olduğunu ve tüm personelin bunun yönetim kurulu başkanı/merkez müdürünün ricası/emri olduğunu bilmesi gerektiği vurgulanacaktır. Burada yönetim onayı alınırken tüm kontrollerin ve artık risklerin yönetim tarafından bilindiği ve onların izni ile bu standardın uygulanmasına yönelik işlemlerin yapılacağı duyurulmuş olacaktır.

2.2.7.Uygulanabilirlik Bildirgesinin Hazırlanması.

Birçok proje ve uygulamada kullanılan Uygulanabilirlik Bildirgesi (Statement of Applicability SoA) oluşturulacak ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'nde tüm resimin gözönüne getirilmesi ile tanımlanabilir. Standartta geçen tüm maddeler için daha önce nelerin yapıldığı, oluşturulan risk yönetim sürecine göre neler yapılacağı ve atıfta bulunulan dokümanlar belirtilerek sistemi uygulamaya geçirmeden önce tüm işlemlerin eylem planı şeklinde sistematik olarak görülmesini sağlar[15]. Tüm ISO/IEC 27001 bölümleri standartta geçtiği şekliyle sıralanarak karşılarına ise konularla ilgili hangi dokümana göre neler yapıldığı belirtilmektedir. Uygulanabilirlik Bildirgesinin bölümleri şu şekildedir.

Madde:ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi içeriğine göre uygulanması gereken maddeler.

Madde Numarası:İlgili madde numarası.(ISO/IEC 27001 ya da kurumun belirleyeceği başka bir numaralandırma)

Kontrol:ISO/IEC 27001 EK-A'sında, ISO/IEC 27002 standardında ve oluşturulan Risk Yönetim Süreci'nde belirtilen gerekliliklerin şirketin Bilgi Güvenliği Yönetim Sistemi'ne entegrasyonunun sağlanacağı adımlar olan kontroller.

Hali Hazırdaki Kontrol:İlgili maddeye göre şu ana kadar yapılan kontrol ve işlemlerdir. Bu maddeye daha önce kaynak alınan bir doküman varsa eklenebilir. İlk defa uygulanacak BGYS'de idari birçok maddenin olmadığı görülmektedir. Fakat teknik olarak birçok konu zaten güvenlik yapısı tarafından oluşturulmuş olacağından teknik konularda yapılanların varsa prosedür/talimatlarıyla birlikte bu bölümde dokümanta edilmesi karşılaştırma yapılabilmesi açısından önemlidir.

15 http://www.praxiom.com/iso-27001-definitions.htm

Artık Risk Açıklaması: Risk Yönetim Süreci'ne göre ilgili madde/kontrol artık risk olarak belirlenmişse bunun nedeninin açıklandığı bölüm.

Kontrolün Seçilme Kaynağı: Burada uygulanacak kontrolün hangi kaynaktan seçildiği belirtilir. Kaynaklara örnek olarak Kanuni Zorunluluklar, Sözleşme Zorunlulukları, İşletmenin Kendi Zorunlulukları, Karşılaşılan ya da Örnek Alınan Olaylar, Risk Yönetim Sonuçları verilebilir. Bu kaynaklar Bilgi İşlem Merkezlerinin yapılarına göre düzenlenecektir.

Açıklama:İşlem görmesi için onay alınan kontrolün açıklanması. İlgili kontrol kısaca ve açıkça burada belirtilmelidir.

	SEMBOLİK BILISIM LTD.ŞTİ. UYGULANABİLİRLİK BİLDİRGESİ	
YAYIN NO: 27001-UB-01	DOKUMAN ADI:DOK-UB-V1	VER:0.1

Amaç

Kurum ISO/IEC 27001 BGYS Sistemi'nin tüm unsurlarıyla bir dokümanda toplanıp, uygulanabilirliğinin yönetim tarafından onayının düzenlenmesi.

Kapsam

Tüm BGYS süreçlerini ve kuruluşun tüm personelini kapsar.

Uygulanabilirlik Bildirgesi

Madde:Fiziksel ve Çevresel Güvenlik

Madde Numarası:9.1.2.

Kontrol:Sistem ve Ağ Odalarına Fiziksel Giriş Kontrolleri

Mevcut Kontrol:"Giriş Yetkileri" sürecine göre sistem ve ağ odalarına giriş kontrolleri belirlenmiş ve sadece sorumlularına giriş anahtarları verilmiştir.

Artık Risk Açıklaması:

Kontrolün Seçilme Kaynağı:Burada İşletmenin Kendi Zorunlulukları (IZ), Karşılaşılan ve Örnek Alınan Olaylar (O) ve Risk Yönetimi Sonuçları (RY) seçilecektir.

Açıklama:Giriş Yetkileri Süreci geliştirilecektir. Buna göre sistem ve ağ odalarına giriş ve çıkış kayıtlarını tutacak manyetik kartlı giriş kontrolü, kamera kontrol sistemi ve ziyaretçiler için ziyaretçi formu oluşturulacaktır. Giriş çıkışlar saat ve kişi bazlı kontrol edilecek, konunun hassasiyeti bakımından verilecek farkındalık eğitimine ekleme

yapılacaktır.

Tablo 12. Uygulanabilirlik Bildirgesi

Tarih : Proses/Sistem : Takım :	**UYGULANABİLİRLİK BİLDİRGESİ**	Düzenleyen : Revizyon No : Revizyon Tarihi :

BGYS KONTROLLERİ			MEVCUT KONTROL	ARTIK RİSK VE AÇIKLAMASI	KAYNAK ÇEŞİDİ					KONTROL VE AÇIKLAMASI
					KZ	SZ	IZ	O	RY	
Madde	Madde No	Kontrol								

Kaynak: www.iso27001security.com/ISO27k_SOA_sample.xls

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

Bu şekilde tüm maddeler sıralanacak ve uygulanabilirlik bildirgesi tamamlanarak dokümanlar bölümünde muhafaza edilecektir. BGYS'nin yeni kurulumunda ve iyileştirme süreçlerinde kaynak doküman olarak kullanılacağından tüm maddeler dikkatlice değerlendirilmeli ve açıklayıcı olmalıdır. Burada kontrollerin neden seçildiğinin açıklanacağı gibi standardın EK-A Kontroller bölümündeki seçilmeyen kontroller için de neden çalışmaya dahil edilmediğinden de bahsedilecektir. Ayrıca artık risk açıklamaları yapılacak ve boşluk analizi çalışmasında belirlenen konuyla ilgili mevcut kontroller belirtilecektir.

2.3.BGYS'nin Gerçekleştirilmesi ve İşletilmesi

ISO/IEC 27001 Bilgi Güvenliği Yönetimi Sistemi'nin daha önce belirtilen PUKÖ süreçleri kapsamında "Uygulanabilirlik Bildirgesi"nin hazırlanarak yayımlanması ile "planla" bölümü tamamlanmış ve ikinci bölüm olan "uygula" aşamasına geçilmiştir.

Burada ilk bölümde planlanan ve politika/prosedürler haline getirilen gereklilikler yerine getirilecek ve teori aşamasında eksik kalan işlemler sisteme entegre edilecektir.

2.3.1.Risk Yönetim Süreci-Risk İşleme Planı'nın Hazırlanması

Risk yönetim sürecinde esas amaç olan risklerin yönetilmesiyle ilgili olarak planlama işlemi yapılıp, bu planların yönetim kurulu tarafından onaylanmasından sonra risk işleme planı hazırlanarak eylem aşamasına geçilecektir. Bu aşamada daha önce seçenekleri belirtilen risk işleme yöntemleri kuruluşun mevcut tüm riskleri üzerine uygulanarak o riske yönelik en uygun yöntemin seçilmesi ve dokümante edilmesi işlemi gerçekleştirilecektir[16].

Tüm sistemin esas amacı olan risklerin tamamen ortadan kaldırılması bazen teknik bazen de maddi imkansızlıklar nedeniyle gerçekleşememektedir. İşte bu çalışma ile bu gibi olayların gerçekleşmesi durumunda diğer risk işleme eylemlerinin belirlenmesi yapılacaktır. Bunun için de yönetim en düşük maliyetli ve en uygun kontrolün nasıl seçileceği üzerinde duracaktır. Risk işleme planının bölümleri şu şekildedir.

Risk: Bu bölümde üzerinde işlem yapılacak riskler sıralanacaktır.

Risk İşleme Yöntemi: Risk işleme yöntemlerinden hangisinin kullanılacağı açıklanacaktır. Bunlar riski gidermek veya azaltmak için kontrol uygulanması, riskin tamamının veya bir kısmının sigorta ya da başka kurumlara aktarılması ve riskin önemsizliği ya da teknolojik imkanların el vermemesi gibi nedenlerle kabul edilmesidir.

Risk İşleme Yönteminin Açıklanması: Burada seçilen risk işleme yönteminin neye göre ve nasıl seçildiğinden kısaca bahsedilecek ve referans dokümana atıfta bulunulacaktır.

Öncelik: Burada Risk Yönetim Süreci'nde belirlenen risk değerine göre öncelikler belirtilecek ve bunlara göre müdahale yapılacağı beyan edilecektir.

Zaman: Riske uygulanacak kontrolün planlanan başlangıç ve işlenme tarihleri belirtilerek bu tarihler arasında yapılması amaçlanacaktır.

[16] Joel Brenner,Risk Management,ABD,2007 http://www.allbusiness.com/finance/business-insurance-risk-management/4060499-1.html

Sorumlu: Riskin işlenmesi ve sonuçlarının dokümante edilmesi ile ilgili kimlerin görev aldığı burada belirtilecektir.

	SEMBOLİK BILISIM SIRKETİ RİSK İŞLEME PLANI	
YAYIN NO: 27001-RİP-01	DOKUMAN ADI:DOK-RİP-01-V1	VER:0.1

Amaç

Risklerin giderme yöntemlerinin, önceliklerinin, planlanan tarihlerin ve sorumluların belirlenmesi.

Kapsam

Mevcut ve potansiyel tüm riskleri kapsamaktadır.

Risk İşleme Planı

Tablo 13. Risk İşleme Planı

Tarih : Proses/Sistem : Takım :		**RİSK İŞLEME PLANI**		Düzenleyen : Revizyon No : Revizyon Tarihi :	
Risk	Risk İşleme Yöntemi	Açıklama	Öncelik	Zaman (Başlangıç-Bitiş)	Sorumlu

Risk:Dosya Sunumcusundaki Proje Dosyalarının Fiziksel Arıza Sonucunda Kaybolması

Risk İşleme Yöntemi:Kontrollerin Uygulanarak Riski Azaltma/Giderme

Açıklama:Dosya sunumcularında Windows 2003 Sunumcu işletim sisteminin günlük-haftalık ve aylık yedekleme imkanlarından faydalanarak dosyalar yedeklenecektir. Yedekleme işlemleri ve Yedekleme Planı hakkında yapılacak tüm işlemler Yedekleme Süreci'nde belirtilecektir.

Öncelik:Yüksek

Zaman:Başlangıç;12 Mayıs 2010-Bitiş 20 Mayıs 2010

Sorumlu:Sistem Yönetim Kısmı Sorumlusu Sistem Mühendisi Oğuzhan BAL

Risk:Sistem Odasına Sel Basması Sonucu Tüm Sunumcu ve Cihazların Kullanılamaz Hale Gelmesi

Risk İşleme Yöntemi:Uygulanacak Kontrollerle Riskin Azaltılması/Giderilmesi ve Riskin Yapılacak Onarım Anlaşmasına Göre 3.Şirkete Aktarılması

Açıklama:Bu duruma karşın Acil Durum Planı ile geriye dönüş sağlanacak ve donanımların onarılıp yenilenmesi konusunda Donanım Bakım Tutum Sözleşmesi Süreci'ne göre imzalanılacak sözleşme gereğince firma tarafından aynı gün içerisinde donanımın onarılması ya da yerine yenilerinin konulması sağlanacaktır.

Öncelik:Yüksek

Zaman:Başlangıç;Acil Durum Planı 10 Mayıs 2010-14 Mayıs 2010,Donanım Bakım Tutum Sözleşmesinin Oluşturulması;24 Mayıs 2010-28 Mayıs 2010

Sorumlular

Bilgi İşlem Merkezi Müdürü Alpay KOR

Acil Durum Planı'nın hazırlanması Sistem Yönetim Kısmı Sorumlusu Oğuzhan BAL,

Donanım Bakım Tutum Sözleşmesinin Oluşturulması Teknik Hizmetler Kısım

Sorumlusu Sebahattin YILMAZ

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

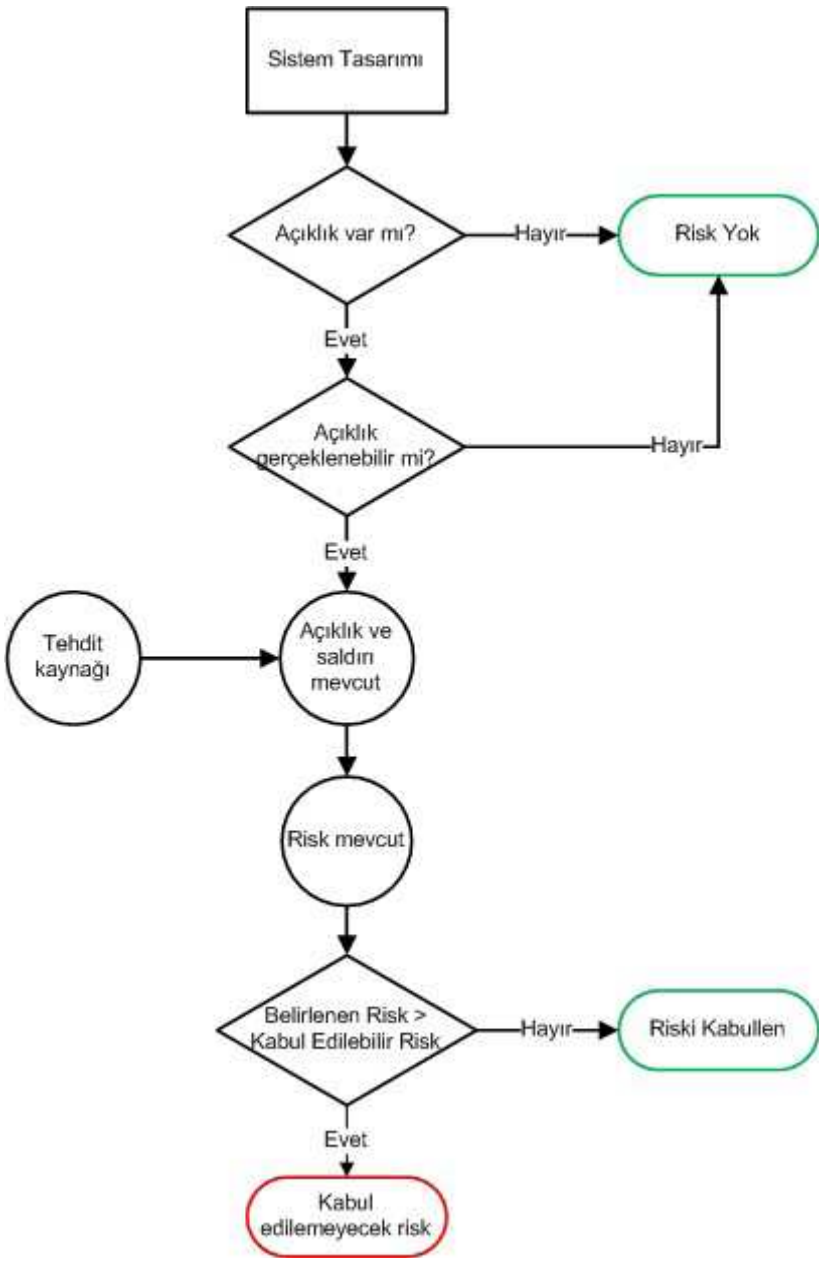
Bu şekilde tüm riskler ve eylem planları dokümante edilerek belgenin risk giderme işlemlerine kaynak olması sağlanacaktır. Tüm detayları belli olan planda yeni eklemeler ve değişiklik yapıldığında PUKÖ döngüsü içerisinde değerlendirilecektir.

2.3.2.Risk İşleme Planının Gerçekleştirilmesi

Kurum ya da kuruluş, Risk İşleme Planında dokümante ettiği seçenekleri, bu seçenekleri gerçekleştirecek sorumlular ve rollerini, gerekli kaynakları göz önüne alarak süreçler belirlemelidir. Bu süreçlerde kontrol uygulanacaklar, sigorta ya da 3.taraf şirketlere devredilecekler ve artık risk olarak kabul edilecekler ayrılarak risklere karşı gerekli işlemler gerçekleştirilmelidir. Burada dikkat edilmesi gereken nokta ise planın gerçekleştiği sırada öngörülememiş, uygulama bölümünde karşılaşılan durumların planlara dahil edilmesi ve dokümanların güncelleştirilmesidir. Böylece işin başında yapılan değişiklikler ile en başa dönülerek zaman kaybedilmemiş olacaktır.Bu konu

özellikle Bilgi İşlem Merkezlerinde önem kazanmaktadır. Plan yapılırken ortaya koyulan hedeflerin, teknolojinin ve tecrübenin her geçen gün arttığı bilgi iletişim teknolojilerinde, Risk İşleme Planları'nın güncellenmesine her an gerek duyulabilmekte ve böylece işin başında yapılan değişikliklerin zaman kaybının önlemesi amaçlanmaktadır.

Şekil 3. Risk İşleme Yöntemi Belirleme Süreci



Kaynak: Eskiyörük (2007:23)

Buradaki seçenekler üzerinden, risklerin kontrol uygulanarak giderilmesi ya da kabul edilebilir düzeye çekilmesi amaçlanmaktadır. Sigorta ya da diğer şirketlere devredilecek riskler için de yine devir işlemlerinin ne şekilde yapılacağı, sorumlulukların hangi durumlarda hangi tarafta olacağını belirleyen politika/prosedürler hazırlanarak bu işlemin de kurallar dahilinde yapılması sağlanacaktır. Artık risk olarak kabul edilenler ise hangi karara dayanılarak gözardı edildikleri dokümante edilecek, daha sonra meydana gelebilecek değişiklikler için saklanacaklardır.

2.3.3. Kontrollerin Uygulanması

Risk İşleme Planı'nın gerçekleştirilmesinde temel araç olan kontrollerin uygulanması konusu Bilgi Güvenliği Yönetim Sistemi'nin pratiğini oluşturmaktadır. Bu plana göre kontrol uygulanarak azaltılacak ya da ortadan kaldırılacak riskler için planlama aşamasında hazırlanan prosedür ve talimatlara göre işlem yapılacaktır[17]. Risk Yönetim Süreci boyunca planlanan işlemler sorumlulukları tarafından yönetimin sağladığı kaynaklar kullanılarak gerçekleştirilecektir. Ayrıca gerekiyorsa kontrolün gerçekleştirilmesi konusunda farklı kullanıcı ya da yöneticilerin sürecin içine dahil edilmesi sağlanacaktır. Sistemleri kullanan ve yönetenlerin diğer departman personeli olduğu göz önüne alındığında bu kişilerin süreçlerin bizzat içlerinde olmaları sistemin benimsenmesi ve gereğiyle yapılması konularına katkı sağlayacaklardır.

Kuruluş, amaca uygun kontrolleri bir plan dahilinde, yönetim kademesi tarafından kaynakların sağlanması ile gerçekleştirecektir. Burada oluşturulan ana politika ve bunu destekleyici prosedür ve talimatlardan yararlanılacaktır. Yapılan her işlem ince ayrıntısına kadar dokümante edilecek ve ileriki çalışmalara kaynak olması amacıyla saklanacaktır. Kontroller uygulanırken de karşılaşılaşılan ve daha önceden öngörülememiş olaylar kaydedilerek ilgili dokümanlar güncellenecektir. Böylece süreklilik sağlanacak, daha sonraki müdahalelerde kolaylık getirecektir.Örnek olarak;

"Dosya Sunumcusundaki Proje Dosyalarının Fiziksel Arıza Sonucunda Kaybolması" riskine karşılık olarak oluşturulacak yedekleme sisteminde öncelikle donanım temin edilecektir. Donanım temini konusunda Satın Alma Müdürlüğü'ne istek yapılmıştır. 19 Mayıs 2010 tarihinde gelen donanım üzerine Yedekleme Sistemi'nin Kurulması Süreci

[17] http://www.isoqar.com/uk/standards/iso27001/iso-27001-about.aspx

doğrultusunda sistemin kurularak dosya sunumcusunda Zamanlanmış Görevler Süreci'nde belirtilmiş görevler oluşturulmuş, günlük, haftalık ve aylık yedekler alınmaktadır. Ayrıca Satın Alma Müdürlüğü'ne 12.04.2010 tarihinde teslim edilen Yıllık Donanım Bakım Sözleşmesi Şartnamesi ile 20.04.2010 tarihinde "Talamus LTD.ŞTİ." firması ile yıllık bakım anlaşması imzalanmıştır. Buna gore sistem ve ağ cihazlarının onarım ve değişim günleri 1 gün olarak belirlenmiş olup, sistem bu zaman içerisinde çalışır hale getirilecektir.

Tüm riskler için ayrı ayrı hangi kontrollerin uygulandığı bu şekilde tamamlanacak ve dokümante edilecektir.

2.3.4.Kontrollerin Etkinliğinin Nasıl Ölçüleceğini Tanımlama

Kontrollerin uygulanması aşamasını tamamladıktan sonra daha sonraki "Kontrol Et" aşamasına kaynak olacak, kontrollerin etkinliğinin nasıl ölçüleceğinin tanımlanması işlemine gelinecektir. Burada kontrollerin sonuçları ile amaçlanan durumun nasıl karşılaştırılacağı ortaya koyulacak ve standardın belgelendirme gereksinimine dayanılarak dokümante edilecektir.

Kontrollerin etkinliğinin ölçülmesi risk yönetiminin sürekli iyileşen sonsuz döngüsünün bir gereğidir[18]. Bu etkinliği ölçmek için de önceden planlanacak unsurlara göre hareket edilmesi hem sistemin meşruluğu hem de standardın gerekliliği ile doğru orantılıdır. Planlanmamış bir ölçüm sistemi tüm yanlarıyla bilgi güvenliğinin sağlanmasına engel olabilir. Etkinlik ölçümlerinin kötü ya da iyi niyetli olarak anın gerekliliklerine göre değiştirilebilme olasılığı ölçümlerin daha önceden planlanıp dokümante edilerek gerçekleştirilmesi gerekliliğini zorunlu kılmaktadır.

Planlamanın bu özelliği onun hiçbir zaman değişmeyeceği anlamına gelmez. Aksine tüm risk yönetimi, zamanın ve özellikle bilişim teknolojilerinin çok hızlı değiştiği göz önüne alındığında ileriye dönük olarak gelişen bir süreç olduğundan etkinlik ölçüm kriterlerinin de değişmesi kaçınılmazdır. İstenen durum ise kriterlerin planlamanın içine dahil edilmesi ve bu planlama dahilinde değişikliğe uğramasıdır.

[18] Karen Worstell,Achieving Effectiveness in Information Protection,ABD,2006 http://www.wec-llc.com/achieving-effectiveness.pdf

Burada bir doküman hazırlanarak tüm kontrollerin etkinliğinin ne şekilde ölçüleceğini belirtmek en doğru yaklaşım olacaktır. Bilgi İşlem Merkezleri tarafından yapılacak kontrol etkinliği ölçümü oluşturulacak kontrollerde yapılacak bir hata ya da eksiklikten dolayı oluşacak güvenlik zaafiyetlerinin önüne geçecek ve büyük sıkıntılar yaşanmadan önlem alınmasını kolaylaştıracaktır.

Uygulanacak kontrol etkinliğini ölçme yöntemleri bir tabloda toplanacak ve tüm kontrollere ayrı ayrı belirtilecektir.

	SEMBOLİK BILISIM SIRKETİ KONTROL ETKİNLİKLERİ ÖLÇÜLMESİ DOKÜMANI	
YAYIN NO: 27001-KEÖ-01	DOKUMAN ADI:DOK-KEÖ-V1	VER:0.1

Amaç

Riskleri ortadan kaldırmak ya da işlemek için uygulanan kontrollerin etkinliğinin ne şekilde ölçüleceğini belirlemek.

Kapsam

Uygulanacak tüm yönetimsel-teknik kontrolleri kapsamaktadır.

Kontrol Etkinliği Ölçme Yöntemleri

Tablo 14. Kontrol Etkinliğinin Ölçülmesi Tablosu

Tarih : Proses/Sistem : Takım :		**KONTROL ETKİNLİĞİ ÖLÇÜLMESİ TABLOSU**	Düzenleyen : Revizyon No : Revizyon Tarihi :
Risk	Kontrol	Etkinlik Yöntemi	Açıklama ve Atıfta Bulunulan Doküman

Bu tabloya göre;

Risk:Web Sunumcusunun Devre Dışı Kalması Sonucu Müşteriler ve Tedarikçilerin Sisteme Girememesi

Kontrol:Yedek Web Sunumcunun Devreye Alınması ve Birlikte Çalışabilirliklerinin

Sağlanması

Etkinlik Yöntemi:İletişimin fazla yoğun olmadığı gece saatlerinde ilk web sunumcu devreden çıkarılarak kurulan yedek web sunumcusunun %0 hata ve zaman kaybı olmaksızın devreye girip girmediğinin ve o ana kadar yapılan değişiklikleri üzerinde tutup tuttmadığının kontrolü yapılacaktır.

Açıklama ve Atıfta Bulunulan Doküman:Yedek Web Sunumcusu Kurulumu

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

Şeklinde tüm riskler için bir veya daha fazla etkinlik ölçüm yöntemi belirlenecektir. Yöntemler gereğine göre uygulanarak öncelikle kontrolün ve daha sonra Bilgi Güvenliği Yönetim Sistemi'nin etkinliği ölçülecektir.

2.3.5.Eğitim Ve Farkındalık Programının Gerçekleştirilmesi

Bünyesinde BGYS Standardı'nı uygulamak isteyen her kurum ve kuruluş, bu standardın gereklililiği olan bilgi güvenliğinin oluşturulması ve idamesi konularında genelden özele doğru her düzeydeki personelin eğitim ve farkındalık programları çerçevesinde eğitimlerini asgari düzeyde gerçekleştirmesini ve bu sistemi bizzat kuracak BGYS ekibi personelinin de konu hakkında üst düzey bilgiye sahip olmalarını sağlamalıdır[19].

Bu program bilgi güvenliğinin kurum için gereği ve öneminden başlayarak öncelikle personelin konuya önyargılarını azaltacak farkındalık çalışmalarına ağırlık vermelidir. Oluşan fakındalık teknik bilgilerle pekiştirilerek kazaran ya da bilgisizlikten kaynaklanan bilgi güvenliği olaylarının önüne geçilmelidir. BGYS sorumluluğu bulunan personelin verilen görevleri yerine getirme konusunda yeterli olmalarını sağlamak için uygun bir farkındalık ve eğitim programı uygulanmalıdır. Program gerekli yeterlikleri belirlemeli, bu gereksinimleri karşılamak için gerekli olan eğitimi sunmalı, eğitimin etkinliğini değerlendirmeli ve kazanılan yetkilerin ve niteliklerin kaydını tutmalıdır.

Eğitim ve fakındalık çalışmaları da diğer çalışmalar gibi bir plan dahilinde gerçekleştirilmelidir. Bu planda ulaşılması gereken bilgi güvenliği amacına yönelik

[19] Ted Humphreys ve Angelika Plate,Guidelines on Requirements and Preparation for ISMS Certification based on ISO/IEC 27001,British Standarts Institute,2005

olarak bilgi ve beceri düzeyi belirlenmeli ve bu hedef doğrultusunda gerekli eğitim içeriği ve materyaller sağlanmalıdır. Kurum ve kuruluş bazında yönetim tarafından tam destek sağlanması gereken eğitim ve farkındalık çalışmaları oluşturulacak profesyonel eğitim birimi ya da dışarıdan alınacak destek ile özel önem verilerek hazırlanmalıdır. İnsan faktörünü ön planan çıkaracak eğitimlerle bilgi güvenliği konusundaki en çok karşılaşılan durum olan personel hatalarının giderilmesi amaçlanmalıdır.

2.3.6.BGYS'nin İşletilmesinin İdaresi

Kurum ve kuruluşlar, bilgi güvenliğinin istenilen duruma gelmesi için BGYS standardının bir gereği olarak atacağı her adımı, tanımlanan kontroller, politikalar ve prosedürlere uygun olarak gerçekleştirmelidir. "Dokümana Göre İdare" yöntemi ile, her kontrol için öncelikle ilgili dokümanın düzeltilip, akabinde kuralın iyileştirmesinin tamamlanması aranmaktadır[20]. Böylece "Kontrol Et" aşamasında gerçekleştirilecek incelemelerin sisteme entegresinin yapılarak bilgi güvenliğinin istenilen duruma getirilmesi sağlanacaktır. Bu amaç doğrultusunda her türlü inceleme ve yaşanılan olay kayıt altına alınacak ve ileriki çalışmalara kaynak olacaktır.

2.3.7. BGYS İçin Kaynakların İdaresi

Risk İşleme Planı'nın oluşturulması sırasında mevcut risklere uygulanan kontrollerin hayata geçirilmesi, BGYS'nin planlama, uygulama, kontrol etme ve iyileştirme aşamalarının gerçekleştirilmesi, hem yönetimsel hem de teknik olarak gereksinimlerin yerine getirilebilmesi için kaynak yaratma ve bu kaynakların yönetimini sağlama ihtiyacı ortaya çıkmaktadır. BGYS ekibinin önerisi ve yönetim kurulu kararları sonrası ortaya çıkan bu kaynak ihtiyaçlarının yönetimi, detayları standardın 5.2. nolu Kaynakların İdaresi maddesinde de belirtildiği üzere üst yönetimin sorumluluklarından biridir.

2.3.8.Güvenlik İhlal Olayları Prosedürlerini ve Diğer Kontrolleri Gerçekleştirme

Bilgi Güvenliği Yönetim Sistemi'nin gereklilikleri yerine getirilerek mevcut bilgi güvenliği düzeyi arttırılmaya çalışılsa da günlük hayatta önleyici kontrollerin yeterli olamadığı durumlar meydana gelebilmektedir. İşte bu noktada bilgi güvenliğinin bir

[20] Inger Nordin,Implementation of an ISMS,Litvanya,2003
http://www.ivpk.lt/dokumentai/prezentacijos/09%20Information%20Security%20Management%20System%20-%20Implementatio.ppt

gereği olarak bu kötü senaryolara da hazırlıklı olunması ve senaryonun gerçekleştiği anda hareket tarzlarının önceden belirlenerek uygulanması sağlanmalıdır.

Bunun için ilk yapılacak iş ihlal olayı meydana geldiğinde süratle iletişimin sağlanacağı haberleşme kanalları oluşturarak gerekli tüm personele bilgilendirmenin yapılmasıdır. Bundan sonra en alt düzey kullanıcıdan en üst düzey yöneticiye kadar yapılması gerekenler anlatılmalı ve olaydan en az seviyede zararla kurtulmanın yolları dokümante edilmelidir. Doküman yapısında sistematik bir şekilde politikadan talimata kadar tüm seçenekler kullanılmalı ve gerçekleşen her olayın haritası çıkarılarak dokümana eklenmelidir. Her ihlal olayı Bilgi Güvenliği Yönetim Sistemi'ni ileriye götürecek şekilde kullanılmalıdır. Ayrıca kontrollerin bu durumları tekrar yaşatmaması amacıyla güncellenmelidir.

Günümüzde teknolojinin ilerlemesi ile güvenlik olay ve ihlallerini anında saptayabilme seçenekleri çok fazla bulunmaktadır. Bunlara örnek olarak, fiziksel kontrolün sağlandığı kamera kontrol ve giriş kartı kontrol sistemleri, bilgi işlem altyapısı saldırı tespit sistemleri sayılabilir. Önemli olan nokta bu sistemlerle ilgili görevlendirmenin iyi yapılması ve yapılacak rutin kontroller ile sistemin bu olaylar karşısında otomatik olarak haber vermesi özelliklerinin kazandırılmasıdır. Bu işlemleri de sağlayacak olan yönetim onayı ile çıkmış süreç ve talimatlardır.

Bilgi İşlem Merkezleri'nin güvenlik olaylarını anında saptayabilme ve bu olaylara karşılık verebilme yeteneğine sahip olmasının en büyük araçlarından biri saldırı tespit ve önleme sistemleridir. Bu sistemlerin saldırıları saptama ve önleme olarak iki ayrı bölümü bulunmakta ve verilecek karara göre kurulumu bir prosedür dahilinde yapılmaktadır. Örnek olarak, Saldırı Tespit Sisteminin Kurulumu Süreci incelenirse;

TSE	SEMBOLİK BILISIM LTD.STI. SALDIRI TESPİT SİSTEMİ KURULUMU SÜRECİ	SBS
YAYIN NO: 27001-STS-01	DOKUMAN ADI:SÜR-STS-V1	VER:0.1
Amaç Kurum bünyesinde bilgi işlem ağlarına yapılacak muhtemel saldırıları tespit edip sistem yöneticilerine otomatik mesajlar gönderen STS sistemlerinin kurulması		

Kapsam

İlgili sistemi kuracak Bilgi İşlem Merkezi Personelini kapsamaktadır.

Uygulama

Kurum bünyesine bir adet açık kaynak kodlu Saldırı Tespit Sistemi kurulacak ve bu sistem ile yapılan saldırılar anında tespit edilerek sistem güvenlik altına alınacaktır.

Saldırı Tespit Sistemi kurulumu konusunda Sistem ve Ağ Yönetimi Şube'sinden bir kişi detaylı eğitim alacak ve sistemin kurulumunu aldığı eğitimi paylaşarak yapacak/yaptıracaktır.

Saldırı Tespit Sistemi kurulumu sistemin daha az kullanıldığı gece saatlerinde gerçekleştirilecek ve ağ kesintilerine yol açmayacaktır.

Saldırı tespit sistemi yönlendirici ile güvenlik duvarı arasına kurularak kurum içerisine yapılmak istenen tüm saldırılar tespit edilecektir. STS, köprü modunda çalışarak tüm trafiği üzerinden geçirecek ve paketleri inceleme imkanı bulacaktır.

Uygulanacak STS sistem ve imza güncellemeleri sorumlu personel tarafından her gün kontrol edilecek ve değişiklikler anında uygulanacaktır.

Saldırı Tespit Sistemi'nin üzerinden geçen bilgileri ve istekleri görsel olarak raporlayacak ve bir saldırı tespit ettiğinde güvenlik sorumlusu ve sistem yönetim sorumlusuna otomatik e-posta ile bilgilendirme yapması sağlanacaktır. E-posta tüm sistem yöneticilerine gönderilecektir. Güvenlik Olaylarına Müdahale Süreci ile olaya müdahale edilecek ve saldırının etkileri kısa sürede giderilecektir.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

Bunlar ile birlikte kurulacak sistemin tüm detayları belirlenecek, dokümante edilerek ilgili kısımlar güncellenmesi ile süreç işleyecek ve devamlı idamesi sağlanacaktır.

2.4.BGYS'nin İzlenmesi Ve Gözden Geçirilmesi

Bilgi Güvenliği Yönetim Sistemi'nin Uygula aşaması tamamlandıktan sonra gelinen Kontrol et aşaması ile planlanan ve uygulanan tüm kontrol ve işlemlerin daha önceden kararlaştırılan prosedür ve talimatlara göre kontrol edilmesi işlemleri gerçekleştirilecektir. Bu şekilde sistemin sağlamasının yapılması ile bir sonraki bölüm olan İyileştirme'de yapılacaklar hakkında kaynak bilgiler oluşturulacaktır. Burada yapılacak tüm işlemlerin bilgi güvenliğini istenilen duruma getirecek olması göz önüne alınarak tarafsız bir anlayışla gerçekleştirilmesi ve dokümante edilmesi gerekmektedir.

Kurumda bilgi güvenliği adına yapılan tüm çabalar bu aşamada kontrol edilecek ve gözden kaçırılabilecek bir nokta nedeniyle tüm sistemin zedelenmesi ve çalışmaz hale gelmesi önlenmeye çalışılacaktır.

2.4.1.İzleme ve Gözden Geçirme Prosedürlerini Gerçekleştirme

BGYS'nin temel araçları olan yönetimsel ve teknik kontroller oluşturulurken bunların bilgi güvenliğini sağlama işlevlerini ne ölçüde gerçekleştireceklerini sınayacak izleme ve gözden geçirme prosedürlerinin de oluşturulması gerekmektedir. Bu prosedür ve diğer kontrollerin, BGYS'nin uygulanması sırasında ortaya çıkan hataları anında tespit edecek, başarısız ve başarılı olan güvenlik açıklarını tanımlayacak, bilgi güvenliği olaylarını ortaya koyacak, bilgi güvenliği ihlal olaylarını önleyecek ve alınan önlemlerin güvenlik açıklarını giderip gidermediğini ya da işe yarayıp yaramadığını tespit edecek yapıda olmaları sağlanmalıdır. Bu prosedürler ile kontrol sorumlularının risk giderme planında tasarlandığı gibi görevini yerine getirdiği de kontrol edilecektir.

Standardın gereği olarak tüm izleme kayıt ve dosyaları, yapılan kontroller sonucunda iyileştirilen sistem hareketleri, kayıt altına alınarak dokümante edilmelidir[21]. Böylece geriye dönük bir bilgi deposu oluşacak ve yapılan tüm eylemler kayıt altına alınarak tecrübelerin aktarılması sağlanacaktır.

Örnek olarak, Bilgi İşlem Merkezleri'nde kurumun internet ağı çıkışları tek makine üzerinden sağlanarak bu makine üzerinde izleme gerçekleştirilmektedir. Vekil sunumcu olarak adlandırılan bu sunumcu üzerinde sistem günlükleri kontrol edilerek çalışanların internet hareketleri kontrol edilmektedir. Yapılan bu kontrolle ilgili prosedürün içeriği aşağıdaki gibi olacaktır.

[21] Tammy Clark ve William Monahan,Developing a Risk Based Information Security Program,ABD,2007 http://net.educause.edu/ir/library/powerpoint/SER07059.pps

Amaç

İnternet Kullanım Politikası'nda belirtilen kurum vekil sunumcusunun sistem günlükleri takip edilerek, sistemin etkinliğinin gözden geçirilmesinin sağlanması

Kapsam

Bilgi İşlem Merkezi bünyesinde bulunan Vekil (Proxy) Sunumcusunu yöneten Sistem Yönetim Kısım personelini kapsar.

Uygulama

Genel Konular

İnternet Kullanım Politikası gereğince Vekil (Proxy) Sunumcusu Kurulum Prosedürü'ne göre kurulumu tamamlanan kurum internet vekil sunumcusunun kayıtlarının izlenmesi gerçekleştirilecektir.

Yönetim kurulu üyeleri dahil tüm kullanıcıların internet erişimleri vekil sunumcu üzerinden verilecektir. Böylece tüm şirketin internet altyapısı kontrollü şekilde sağlanacaktır.

Sistem yöneticileri günlük, haftalık, aylık ve yıllık kayıtları kontrol ederek, sistemin düzgün çalıştığını onaylayacak, ayrıca kullanıcıların girdiği web adreslerinden güvenlik, ahlak ve ruhsal sağlık açısından sıkıntı yaratacak olanların erişim yetkilerini kısıtlayacaklardır. Sistem yöneticileri yaptıkları tüm işlemleri haftalık olarak Sistem Yönetimi Şube Müdürü vasıtasıyla Bilgi İşlem Şube Müdürü'ne sunacaktır.

5651 nolu "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" yasası gereğince 6 ay boyunca kullanıcıların girdikleri siteler, indirdikleri dokümanlar, sitede kalma süreleri saklanacak olup, bu tarihten sonra yeni gelecek bilgiler üzerlerine yazmak suretiyle otomatikman silinecektir.

Teknik Konular

Tüm kullanıcıların vekil sunumcu üzerinden internete çıkması için güvenlik duvarına kayıtlar eklenecek ve bu bilgisayar harici başka hiçbir bilgisayardan gelen internete çıkış istekleri kabul edilmeyecektir.

Kullanıcıların internet ağına dahil olduklarında "Internet Explorer Ağ Ayarları" bölümüne vekil sunumcu IP adresi ve port bilgisi merkezi bilgisayar yönetimi vasıtasıyla girilerek bu ayarların değiştirilmesi engellenecektir.

Vekil sunumcuda içerik tarama ve Web sitesi yetkilendirmeleri açık kaynak kodlu bir program vasıtasıyla yapılacaktır.

Vekil sunumcu üzerine kurulacak ve sistemin günlük kayıtlarının görsel olarak kontrol edilmesini sağlayan açık kaynak kodlu program vasıtasıyla farklı tarihler arasında kayıt incelenmesi yeteneği kazandırılacaktır.

Günlük kayıtlar aylık olarak depolanacak ve bu aylık kayıtlar oluşturulacak zamanlanmış görev ile başka bir klasöre kaydedilerek yedekleri alınmış olacaktır. 6 ay

tutulan kayıtlar otomatik olarak üzerine yenilerinin kaydolmasıyla silinecektir.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

Bu gibi prosedürler tüm kontrol ve sistemler için yazılarak düzenli kontrol edilmesi ve buna göre yaşanılan aksaklıkların giderilmesi sağlanacaktır. Bu prosedürlerin planlanması ile birlikte kontrollerin amacına uygun olarak çalıştığı görülecek ve bir sıkıntı durumunda müdahale edilerek arızanın giderilmesi sağlanacaktır.

2.4.2.BGYS'nin Dikkatle Gözden Geçirilmesini Sağlama

BGYS'nin gözden geçirilmesi işlemine veri sağlayacak olan eylemler, periyodik olarak BGYS ekibi tarafından gerçekleştirilen güvenlik denetimleri, daha önce yaşanmış ihlal olayları, bunların sisteme verdiği zararlar, personel ve etkileşimde bulunulan 3. taraf kurum kuruluşlarca yapılan geri bildirimler, sektör ve dünya bazında meydana gelen bilgi güvenliği olayları, bu konu hakkında eğitim ve devlet kurumları gibi kaynaklardan edinilen önerilerdir. Bu öneriler öncelikle dokümante edilecek ve yapılacak çalışmalar ile ilişkilendirilecektir. Bu kaynaklardan gelen verilere göre BGYS'nin güvenlik, politika ve hedeflerinin tutturulması amacıyla kontrollerin etkinliği gözden geçirilecektir.

Geçen zaman içerisinde yaşanılan tüm olaylar ve geri bildirimleri ışığında Bilgi Güvenliği Yönetimi Ekibi, yapacağı yıllık toplantılarda sistemin tamamını yeniden gözden geçirmeli ve yapılacak iyileştirmeleri planlamalıdır. Yapılacak güncelleştirme ve iyileştirmeler dokümante edilmeli, sisteme geriye dönük olarak geçmişteki durum ile gelinen nokta arasında ilişki kurulabilme niteliği kazandırılmalıdır.

Örneğin daha önce oluşturulmuş olan Güvenlik Duvarı Süreci'nde yaşanan saldırı nedeniyle açık olan bazı portların belli aralıklarla kontrol edilmesi ve gerekirse kapanması kararı verildiğinde yapılacak değişiklik yeni maddeler olarak eklenmelidir.

2.4.3.Risk Yönetimini Belli Aralıklarla Gözden Geçirme

Kontrollerin etkinliğinin gözden geçirilerek iyileştirilmesi, teknolojinin ilerlemesi, verilen hizmetlerin değişmesi, yeni iş ve hizmetlerin oluşması, değişen müşteriler, farklı pazarlara açılma, üçüncü şahıs ve dış kaynaklarla yapılan sözleşmelerin değişmesi,

kanunların değişmesi, kuruluş yapısı, işgücü ve çalışma ortamlarının değişmesi ve nihayetinde gerçekleştirilen kontrollerin etkinliklerinin ölçülmesi sonuçları gibi nedenlerle risklerin yapısı değişebilmektedir. Bu yapı değişikliği kurum bazında risk yönetim sürecinde de değişikliğe gidilmesi ihtiyacını doğurmaktadır.

Daha önce risk olarak kabul edilen bir olgunun gelinen durumla birlikte "artık risk" olarak kabul edilebilmesi, mevcut artık riskin ortadan kaldırılması, yapılan çalışmalar ile riskin 3. taraf şirketlere aktarılması gibi değişikliklere yapılacak rutin BGYS toplantıları ile reaksiyon gösterilmelidir. Bu gözden geçirmeler tehditlerde, hassasiyetlerde ve etkilerde meydana gelen değişiklikleri tanımlamalı ve dokümante etmelidir. Bu işlemler BGYS'nin bir kez yapılıp kenara bırakılmadığı ve yaşayan bir sistem olduğununun gereği olarak karşımıza çıkmaktadır.

2.4.4.Planlanan Aralıklarla İç BGYS Denetimlerini Gerçekleştirme

Kurum ve kuruluşlar detayları standardın 6. maddesinde değinilmiş olan İç BGYS Denetimi'ni planlı aralıklarla gerçekleştirerek sistemi genel çerçevede hedef, kontrol, politika ve prosedürler bazında tanımlanan gereksinimlere uygunluğunu sağlamak amacıyla denetlemelidir.

İç BGYS Denetimleri tüm yönetimsel ve teknik kontrollerin bağımsız kuruluş ya da ilgili uygulamalarla alakalı olmayan bu konuda eğitimli firma personeli tarafından denetlenerek raporlanması işlemidir. Yönetim kurulu kararıyla yılda 1 ya da 2 kez uygulanabilir. Uygulamada her dokümante kontrol edilerek, oluşturulan prosedür ve talimatların gereğine uygun olduğu teyit edilmeli, eksikler BGYS ekibinin sistemi iyileştirme çalışmalarına kaynak olması nedeniyle dokümante edilmelidir.

2.4.5.BGYS'nin Yönetim Tarafından Düzenli Olarak Gözden Geçirilmesini Üstlenme

Tüm ISO/IEC standartlarında olduğu gibi Bilgi Güvenliği Yönetim Sistemi'nde de planlı aralıklarla yönetim tarafından gözden geçirme işlemi standardın gereklilikleri çerçevesinde uygulanmaktadır. Burada sistemin BGYS ekibinin oluşturulması ve kapsamın geçerliliğinden başlanarak son aşama olan iyileştirmelere kadar tüm gereklilikleri sağladığının kontrolü yapılmaktadır. Böylece 3 yılda 1 yapılan yenileme çalışmalarının yıllık bazda gerçekleştirilmesi yapılmış ve standarta uygunluk kontrol edilmiş olacaktır.

İçerik olarak prosedürlerin geçerliliği, rol ve sorumlulukların geçerliliği kontrolü, ihlal olaylarına işlem süreçlerinin doğruluğu, iş süreklilik planlarının geçerlililiği konuları gözden geçirilerek yeniden değerlendirilmesi sağlanacaktır. Yapılan tüm kontroller dokümante edilecek ve bu değerlendirmeler uygulanacak iyileştirme süreçlerinin başlıca kaynağı olacaktır.

2.4.6.Güvenlik Planlarını Güncelleştirme

Kuruluş planlayıp gerçekleştirdiği izleme ve gözden geçirme prosedürlerinden sonra bu işlemlerin sonuçlarını dikkate alarak sistemi üzerine inşaa ettiği genel güvenlik planlarını güncelleştirme ihtiyacı duyacaktır. İşte bu güncelleştirme işlemleri de daha önceden planlanmış olmalı ve sonuçların ne şekilde kullanılıp planların ne şekilde güncelleneceği belirlenmelidir. Güncelleştirmelerin genel hatları hazırlanacak güvenlik planlanları güncelleştirme prosedürleri ile anlatılmalıdır. Burada sonuçların ne şekilde değerlendirileceği konusu ve güvenlik planlarının etkileyeceği hususlar detaylı bir şekilde açıklanmalıdır. Örnek Acil Durum Planı Güncelleştirme Prosedürü;

	SEMBOLİK BILISIM LTD.ŞTİ. ACİL DURUM PLANI GÜNCELLEŞTİRME SÜRECİ	
YAYIN NO: 27001-ADPG-01	DOKUMAN ADI:SÜR-ADPG-V1	VER:0.1

Amaç

Uygulanan izleme ve gözden geçirme prosedürlerinin sonuçları, geri bildirim ve ihlal olaylarının sonuçları ve güvenlik denetim ihlal olaylarının sonuçlarına göre Acil Durum Planı'nın ne şekilde güncelleneceğinin açıklanması.

Kapsam

Felaket ya da acil bir durumun oluşması karşısında uygulanacak kontrolleri belirleyen Acil Durum Planı'nı kapsar.

Uygulama

İlk sürümü BGYS'nin kurulması ile 20 Mart 2010 tarihinden oluşturulan Acil Durum Planı'nın düzenli aralıklarla her yıl amaç kısmındaki nedenlerden dolayı güncellenmesi bu prosedüre göre yapılacaktır.

Tüm sene boyunca kaydedilen bilgi güvenliği olayları, BGYS ekibi ve Sistem Yönetim-Güvenlik kısmı personelleri tarafından incelenerek edinilen tecrübeler ve yeni teknolojiler ışığında planın değişimi sağlanacaktır.

Kurum için hayati öneme sahip Acil Durum Planı'nın güncelliğine azami önem

gösterilecek yapılacak tüm değişiklikler dokümante edilerek gelinen durum ortaya koyulacaktır.

Varlık Envanteri Dokümanı'na eklenen her bilgi varlığı ya da hizmeti için yönetiminden sorumlu Bilgi İşlem Merkezi personeli tarafından, BGYS ekibi ivedi şekilde bilgilendirilerek varlığın Acil Durum Planı'na eklenmesi isteği yapılacaktır. BGYS ekibinin haftalık toplantılarında bu istek karara bağlanarak işlem başlatılacaktır. Acil Durum Planı'nın oluşturulmasıyla görevli güvenlik kısım personeli ile o varlık ya da hizmetten sorumlu personel tarafından taslak değişiklik çalışması ortaya koyularak BGYS ekibi onayına sunulacaktır. Taslak çalışmada varlık değeri, olasılık ve etki analizi, kabul edilebilir kesinti süreleri ve kabul edilebilir veri kaybı bilgileri bulunacaktır. Bir doğal afet ya da acil durumda ilgili hizmet ya da varlığın ne şekilde tekrar hizmet verebilir hale getirileceği, yedek donanım ve bilgilerin ne şekilde kurulacağı detaylı bir şekilde belirtilecektir. Varlık ya da hizmet yedekleme prosedürü içine dahil edilerek, belli aralıklarla yedeklerinin alınması sağlanacaktır.

BGYS ekibi onayı alındıktan sonra, dokümanın ön kapağında yapılan her değişikliğin kısa açıklaması, tarih ve belgenin orjinal hali farklı numara ile saklanacaktır. Her sene yapılan değişiklikler farklı punto ve renklerle belirtilerek kontrol aşamasında kolay göze çarpacak ve müdahaleyi yapacak personele özel durumları aktaracak nitelikte olacaktır.

Her sene yapılan değişiklikten sonra Acil Durum Planı tatbik edilerek değişikliğin etkinlik kontrolü yapılacaktır. Bu kontrolde karşılaşılanlar da değişikliğe dahil edilecek ve nihai gelinen durum dokümante edilecektir.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

Bu ve bunu gibi maddeler her kurum için oluşturularak plan değişikliklerinin de ne şekilde yapılacağının prosedürlere bağlanması sağlanacaktır.

2.4.7.BGYS Etkinlik ve Performansını Etkileyecek Olayları Kaydetme

Bilgi Güvenliği Yönetim Sistemi'nin kurulup işletilmesinde ideal yaklaşım meydana gelen tüm bilgi işlem faaliyet ve olaylarının kaydedilmesidir. Bu bilgilerin yazılım üzerinden ya da kağıt ortamında tutulması, sistemin işleyişinin gözler önüne serilmesi, nereden nereye gelindiğinin bir göstergesi olması gibi yönetimsel nedenlerinin yanında, daha önceki olaylara karşı müdahale yöntemleri, bir daha oluşmaması için alınması gereken önlemler gibi teknik nedenlerden dolayı kritik öneme sahiptir.

Bu gibi olaylara örnek olarak yönetimin gözden geçirme sonuçları, BGYS kuruluş içi denetim sonuçları, güvenlik ihlal raporları, izleme faaliyetleri sonuçları, geri beslemeler ve öneriler sayılabilmektedir. BGYS ekibi tarafından sistemin bu gibi etkinlik ve performansını etkileyebilecek olaylarının uygun şekil ve depolama ortamlarında en kısa

sürede kayıt altına alınmaları standart gerekliliği ile de zorunlu hale getirilmiştir. Kaydetme işlemlerinin ne şekilde yapılacağı bir prosedür şeklinde belirlenmeli ve tüm olayların kaydedilmesinin bu prosedür aracılığıyla uygun yerlere yapılması sağlanmalıdır.

Tablo 15. BGYS Etkinlik ve Performansını Etkileyecek Olayları Kaydetme Formu

Tarih : Proses/Sistem : Takım :		**BGYS OLAYLARI KAYDETME FORMU**			Düzenleyen : Revizyon No : Revizyon Tarihi :
Sıra No	Varlık	Olay	Tarih	Yapılan İşlem – Kontrol	Açıklama (Doküman)

2.5.BGYS'nin Sürekliliğinin Sağlanması ve İyileştirilmesi

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'nin Kontrol Et aşamasının tamamlanmasıyla bu sonuçları dikkate alarak sistemin geliştirilmesi işleminin gerçekleştirileceği Önlem Al aşamasına gelinmiş ve bu aşamanın tamamlanmasına müteakip PUKÖ döngüsünün başına dönülerek sistemin sonsuz yaşam döngüsü sağlanılacaktır. Burada da diğer bölümlerde olduğu gibi sistematik bir anlayışın benimsenmesi ve standartta geçen adıyla sürekliliğin sağlanması ve iyileştirme adımlarının gerçekleştirilmesi sağlanacaktır.

BGYS'nin kontrol et aşamasında karşılaştığı olaylarla edindiği tecrübelere göre harekete geçip, bunların sonucu olarak sistemi daha ileriye götürecek ve güvenliğin derecesini arttıracak adımları atması gerekmektedir. İşte bu adımlar sadece sürekliliğin sağlanması ve sistemin iyileştirilmesi prosedür ve talimatları ile olabilmektedir. Edinilen tecrübeleri açık bir şekilde sisteme entegre edecek prosedürler oluşturularak her geçen dönem içerisinde bilgi güvenliği, olması gereken seviyeye çıkarılacak ve durmadan daha ileriye doğru götürülecektir. Süreçlerin bilgi iletişim teknolojilerindeki gelişimi göz önüne alındığında durması imkansız ve her geçen gün daha içinden çıkılmaz bir hal alması ile BGYS'nin sürekli gelişme göstermesi zorunluluğu

kaçınılmazdır. Bilgi güvenliği konusunda kontrolü en başından itibaren ele almak doğru yaklaşım olacaktır. Aksi durumda tekrar yakalamak imkansız denebilecek kadar zordur.

2.5.1.Tanımlanan İyileştirmelerin Gerçekleştirilmesi.

Kontrol aşamasında izlenilen prosedürler kapsamında sistemin eksikleri ya da güncelleştirilmesi gereken yerleri tespit edilmiş olup, bunların yine bir prosedür vasıtası ile iyileştirmelerinin yapılması ile döngünün tamamlanması sağlanacaktır. Bu iyileştirmeler, mevcut risklerin doğru şekilde yönetilmesinin temini olmakta ve yapılan hatalardan dersler çıkarılarak bilgi güvenliği amacına ulaşma çabasını ihtiva etmektedir.

Örnek olarak kontrol et aşamasının bir bölümü olan Elektronik Posta Sunumcusu kontrol edilmiş ve “Spam” olarak adlandırılan ticari ya da reklam amaçlı istenmeyen elektronik postaların kabul edilmemesi konusunda istenilen duruma gelinemediği tespit edilmiştir. Bu konuda araştırmalar yapılıp ayrıca bir spam filtreleme sunumcusu kurulma ihtiyacının olduğu kanaatine varılmıştır. Tanımlanan bu iyileştirmenin gerçekleştirilmesi yani bu sunumcunun kurulması işlemi ise bu bölümde gerçekleştirilecektir. Oluşturulacak prosedür ile sistemin kurulumu ve kullanımı anlatılacaktır.

TSE	SEMBOLİK BILISIM LTD.ŞTİ. ELEKTRONİK POSTA SUNUMCU İYİLEŞTİRME SÜRECİ	SBS
YAYIN NO: 27001-EPSI-01	DOKUMAN ADI:SÜR-EPSI-V1	VER:0.1

Amaç

Ticari ya da reklam amaçlı istenmeyen elektronik posta olarak adlandırılan “Spam”lerin sistemde oluşturulacak bir filtreleme sunumcusu ile reddedilmesinin sağlanması.

Kapsam

Filtreleme sunumcusunu kuracak Sistem Yönetimi ve Güvenlik personelini kapsar.

Uygulama

Elektronik Posta Sistemi’nin kontrol edilmesi prosedürüne göre yapılan kontrollerde sistemin spam filtreleme özelliğinin yeterli sonuçları vermediği ve sistemden fazla sayıda istenmeyen spam’in geçtiği görülmüştür.

Yapılan istişareler ve alınan öneriler sonucunda Elektronik Posta Sunumcu önüne bir adet spam filtreleme sunumcusu kurularak gelen e-postaların öncelikle bu sunumcuda

kontrol edilmesine karar verilmiştir.

Yapılan fizibilite araştırmaları ve merkezin açık kaynak kodlu yazılım kullanma politikasına uygun olarak bu tipte bir yazılımın kullanılmasına karar verilmiştir. Seçenekler üzerinde çalışma yapılarak en uygun uygulamanın "Kontangle" yazılımının spam filtreleme modülü olduğu tespit edilmiştir.

Bir adet sunumcu donanımı sadece bu iş için ayrılacak ve üzerine Kontangle yazılımı kurularak gerekli ayarlamalar yapılacaktır. Sistemin bir bacağı ağın girişine bir bacağı da çıkışına bağlanarak köprü (bridge) modda çalışması sağlanacaktır.

Sistemin güncellemeleri haftalık olarak kontrol edilecek ve kara listeye girmiş e-posta sunumcuları ile kullanıcıları otomatik olarak sisteme entegre edilecektir.

Sistem, engellediği e-postaları günlük olarak kullanıcılara bildirecek ve kullanıcıların spam olmadığını bildikleri halde sistemin blokladığı e-postalarına erişme imkanı sağlayabilecektir.

Sistem engellediği e-postaları haftalık olarak Sistem Yönetim ve Güvenlik bölümlerindeki sorumlu sistem yöneticilerine bildirecektir.

Sistemin doğru çalıştığı hergün kontrol edilecek olup, gözden kaçan e-posta sunumcuları ve kullanıcılar veritabanına elle yüklenecektir.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

Bu ve bunun gibi işleyişle ilgili yapılan iyileştirmeler, prosedür ve talimat halinde dokümante edildikten sonra gerçekleştirilecektir.

2.5.2.Eylemler ve İyileştirmeleri 3.Taraflara Aktarma ve Onlarla Mütabık Kalma

İstenen bilgi güvenliğini sağlamak ve BGYS standardını uygulamak için sadece kendi bünyesinde BGYS'yi gerçekleştirmek günümüz global dünyasında yeterli olmamaktadır. Bu dönemde, içinde bulunulan sektör içinde bilgi varlıklarının yüksek etkileşim oranına sahip olduğu ve uygulanılan güvenlik tedbirlerinin de iletişimde bulunulan kurum kuruluşlara haberdar edilmesi, bu eylem ve iyileştirmeler hakkında işleyiş üzerinde mütabık kalınması ihtiyacını doğurmaktadır.

Bu işlem düzeltici ve engelleyici tüm eylemlerin kaydedilip, uygun iletişim kanallarıyla doğru kişilere aktarılması ile gerçekleşmektedir. Bu iletişim sonucunda gerçekleşen eylemlerin çalışma ortamı ve süreçlerini nasıl etkileyeceği konusunda mütabık kalınması sağlanmalıdır. 3. taraf olarak adlandırılan kurum dışı çalışan ortak ya da tedarikçilerle iletişim kanallarının doğru kurulması, oluşabilecek değişime karşı

direncin daha kolay kırılmasını sağlayacaktır. Bunun için prosedür ve talimatlarla dokümante edilmiş ve her değişiklikte uygun olarak güncellenen bir iletişim kanalı kurulması en uygun durum olacaktır. Örnek süreç;

	SEMBOLİK BILISIM LTD.ŞTİ. 3. TARAF HABERLEŞMELERİ SÜRECİ	
YAYIN NO: 27001-3TH-01	DOKUMAN ADI:SÜR-3TH-V1	VER:0.1

Amaç

Bilişim Teknolojileri güvenliği konusunda alınan karar ve uygulanan kontrollerin 3. taraflara aktarılması konusunda oluşturulacak iletişim kanallarının işleyişini belirlemek.

Kapsam

Kurum/merkez ve 3. taraf kurum/kişileri ve bunlar tarafından atanacak bilişim güvenliği konularında yetkili kişileri kapsar.

Uygulama

Her geçen gün artan bilişim teknolojileri kullanımı ve bu teknolojilerin hızla gelişmesi karşısında artan güvenlik ihtiyaçları ile ilgili olarak oluşturulacak kontrol ve alınacak önlemlerin de o denli hızlı olması gerektiği aşikardır. Bu hızlı ihtiyaçlar nedeniyle oluşturulacak kontrol ve önlemlerin uygulanması neticesinden işleyişi etkilenecek 3. taraflar etkileşimleri için hızlı çalışacak bir iletişim kanalı kurma ihtiyacı doğmuştur. Bu nedenle kurulacak tüm iletişim kanalları her an erişilebilir olmalı ve alınacak kararlarda yetkili kişilere bilgilendirilme yapılmalıdır.

Esas amaç olan güvenliğin etkili bir şekilde sağlanması ve işleyişin olabildiğince kısıtlanmamasıdır. Bu ancak hızlı ve karara olumlu katkılar sağlayabilecek iletişim ile gerçekleşebilecektir.

Bu esaslar çerçevesinde tüm 3. taraflarla yapılan anlaşma ve sözleşmelerde bilgi güvenliğinden bahsedilecek ve sorumlular açıkça belirlenecektir. Bilgi İşlem Merkezi tarafından da yetkili bir kişi ek görev olarak iletişim sağlamakla yükümlü olacaktır. Şu anki sorumlu Sistem Yöneticisi Fatih Durusoy olacaktır. Tüm tedarikçilerin bilgi güvenliği yöneticileri listesi bu prosedüre ek yapılacaktır.

Her an erişilebilir olma ilkesi geçerli olacak ve yapılan işlemlerin habersiz ve mütabık kalınmadan gerçekleşmesi maksimum seviyede engellenecektir.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

2.5.3.İyileştirmelerin Amaçlara Uygunluğunu Sağlama

Kuruluş, gerçekleştirilen tüm iyileştirmelerin, en genel manadaki bilgi güvenliğini sağlama ve geliştirmekten, en özel manadaki oluşturulan sistemin gerekliliklerini yerine getirmesine kadar düşünülen tüm hedeflere ulaşmasını temin etmelidir. Bu uygunluk, alınan düzeltici ve engelleyici önlemlerin gözden geçirilmesi ile kontrol edilecektir. Sistemin ya da kontrolün yapısına göre oluşturulacak ölçü birimleri başarının belirlenmesinde ve gelişmenin kaydedilmesinde önemli rol oynamaktadır.

Bir önceki Spam filtreleme örneğinden yola çıkarsak; bu sunumcunun kurulması ile istenmeyen elektronik postaların engellenmesi amaçlanmış ve kullanıcılardan gelen bu tip isteklerin önüne geçilmesi istenmiştir. Bu yapılan iyileştirmenin tam olarak isteneni karşılaşıp karşılamadığı sonsuz iyileştirme döngüsü içerisinde bu bölümde kontrol edilecektir. Yapılan kontroller sonucu isterleri karşılamaması durumunda sistemin iyileştirmesi seçeneği düşünülerek ya ticari yazılım ve lisansı temin edilecek ya da ilgili yazılımın bilinmeyen yönleri araştırılarak/eğitim alınarak isterleri karşılaması sağlanacaktır. Görüldüğü gibi sistemin bir açığının kapatılması için sadece oluşturulan bir kontrol ve uygulamanın tatbiki ile yetinilmemekte, bunun da kontrolü yapılarak, amaca uygunluğu kontrol edilerek aksi durumlarda tekrar iyileştirme yapılmaktadır.

2.6.Dokümantasyon Gereksinimi

Bilgi Güvenliği Yönetim Sistemi belgesine hak kazanmak isteyen kuruluşlar diğer ISO standartlarında olduğu gibi standardın dokümantasyon bölümünde belirtilen gereksinimlere uyumlu, belgelenmiş bir yönetim sistemi kurmak zorundadırlar. Bu bölümde bahsedilen gereksinimler;

a) BGYS Politikası ve kontrol amaçlarının dokümante edilmiş ifadeleri

b) BGYS Kapsamı

c) BGYS'yi destekleyici prosedürler ve kontroller

d) Risk değerlendirme metodolojisinin tanımı

e) Risk değerlendirme Raporu

f) Risk İşleme Planı

g) Bilgi güvenliği proseslerinin etkin planlanması, işletilmesi ve kontrolünü sağlamak için ihtiyaç duyulan prosedürler ve kontrollerin etkinliğinin nasıl ölçüleceği

h) Gerek duyulan kayıtlar

i) Uygulanabilirlik Bildirgesi

Dokümantasyonun kapsamını, kuruluşun büyüklüğü, faliyet türü, güvenlik gereksinimlerinin ve yönetilen sistemin kapsamı ve karışıklığı belirler. Bu yüzden dokümantasyonlar küçük bazda da olsa farklılık gösterebilmektedir.

BGYS standardının yukarıda sayılan zaruri belgelendirme ihtiyaçlarına ek olarak yine bu belgelerle alakalı, yönetim kurulu toplantı ve karar tutanaklarının da kayıt altına alınması gerekmektedir. Böylece oluşturulan politika ve prosedürün hangi kararın sonucu olduğunun görünmesi ve geriye doğru sorgulanabilir yapısının muhafazası sağlanmalıdır.

Dokümantasyona el kitabı ile başlamak gerekir. Kurumun bilgi güvenliği yönetim sistemine bakış açısı ve ilkeleri bu kitapta toplanacaktır. Tüm BGYS'nin okunması yerine personelin bu el kitaplarını okuyarak konu hakkında açıklayıcı bilgi edinmeleri ve kısaca BGYS'nin içeriğini öğrenmeleri uygun olacaktır.

El kitabına "Giriş" bölümünde bilgi ve bilgi güvenliğinin anlamı, bunların kurum/merkez için önemi açıkça belirtilerek sistemin amacı açıklanmaktadır. İkinci bölümde "Bilgi Güvenliği Yönetim Sistemi Politikası"ndaki Risk Yönetimi'nden bahsedilmekte ve kurumun bilgi güvenliği genel politikalarından söz edilmektedir. Üçüncü bölüm "Bilgi Güvenliği'nin Kapsamı ve Genel Kullanımı"nda bilgi güvenliği kültürüne vurgu yapılarak süreç yaklaşımının anlatımı yapılmaktadır. Kişisel güvenlik, ağ güvenliği, sistem güvenliği konularına değinilerek sistemin işleyişi hakkında kısa bilgiler verilmektedir. Daha sonra BGYS standardının bölümleri olan BGYS'nin gerçekleştirilmesi ve iyileştirilmesi, dokümantasyon gereksinimleri, yönetimin sorumluluğu, iç denetimler, gözden geçirmeler ve BGYS iyileştirmeleri adımlarından kısaca bahsedilecektir.

Bu kitap konunun en başından öğrenilmesi ve getireceği avantajların açıklanması ile sistemin uygulayıcısı olan Bilgi İşlem Merkezi personelinin ve daha sonra diğer

departman personelinin değişime direnç göstermelerini engelleyecektir. Örnek El Kitabı;

	SEMBOLİK BILISIM LTD.ŞTİ. BGYS EL KİTABI	
YAYIN NO: 27001-EK-01	DOKUMAN ADI:DOK-EK-V1	VER:0.1

Giriş

Bilgi İletişim Teknolojilerinin kullanımının hayatın her döneminde arttığı 21.YY ile kişisel ve kurumsal bilgi güvenliğinin hassasiyeti de bir o kadar artmıştır. Hayatımızı kolaylaştıran bu otomasyon sistemlerinin en büyük sorunu ise bilgi güvenliğidir.

Kişisel ve kurumsal bilgi erişimlerinin dünyaya açılmasıyla hem içerden hem de dışarıdan her türlü tehditle karşı karşıya kalınması, bunları organize ederken gizlilik, bütünlük ve erişebilirliklerinin önemini artmıştır.

Bilgi güvenliğinin bu üç ilkesini sağlamak adına oluşturulan yapının ilk bölümü sisteme kendini tanıtmadır. Bunun sağlanması için şifreler, giriş anahtarları vb. sistemler kullanılmaktadır. İkinci bölüm ise ağ güvenliğidir. Burada kullanılan işletim sisteminin güvenliği, yetkilendirme, ağ cihaz güvenliği gibi araçlar kullanılmaktadır. Üçüncü bölüm, hizmetlerin büyük bir bölümünün verildiği web güvenliğidir. Açık anahtar yapısı, dijital sertifikalar, dijital imza, saldırı tespit ve engelleme sistemleri gibi araçları bulunan web güvenliği üzerinde en fazla durulan konu olarak karşımıza çıkmaktadır. Son bölüm ise bilgi güvenliğinin etkinliğinin ölçüldüğü kontrollerdir. Burada sistem kontrolünden bakım kontrolüne kadar bir çok araç bulunmakta ve bilgi güvenliğinin doğru ve etkin bir şekilde oluşturulduğunun sağlaması yapılmaktadır.

Bilgi Güvenliği Yönetim Sisteminin Tanımı

Bilgi Güvenliği Yönetim Sistemi, tüm bilgi varlıklarının belirlenip üzerlerinde risk değerlendirmesi yapılarak bu değerlendirmeye göre eldeki tüm bilgileri korumaya yönelik olarak kontrollerin oluşturulup işlenmesi, bu kontrollerin etkinliğinin ölçülmesiyle her geçen gün iyileştirilerek sonsuz bir döngü içerisinde bilgi güvenliğinin sağlanması işlemlerinin yapıldığı ve tüm personelin bu konuda bilgilendirilerek bilginin öneminin vurgulandığı organize bir sistemdir.

BGYS, bilişim sistemlerini tasarlayıp işletirken bilgi güvenliği konusunda uyulması gereken kuralları anlatmakta, en üst düzey yöneticiden en alt düzey çalışana kadar herkesi ilgilendirmektedir. Bütün personel “Bilgi Güvenliği Yönetim Sistemi El Kitabı”nı okuduğunu imzalayarak tebliğ etmekten ve kendisi ile ilgili bölümleri uygulamaktan sorumludur.

Bilgi Sistemlerinin Genel Kullanımı

Bilişim ile ilgili tüm sistem, cihaz ve ekipmanlar sadece kuruma hizmet için kullanılmalıdır. Kuruma hizmet için kullanılırken de ahlak ve adalet sistemini zedeleyecek uygulamalardan sakınılmalıdır. Tüm çalışanlar günlük aktivitelerini yerine

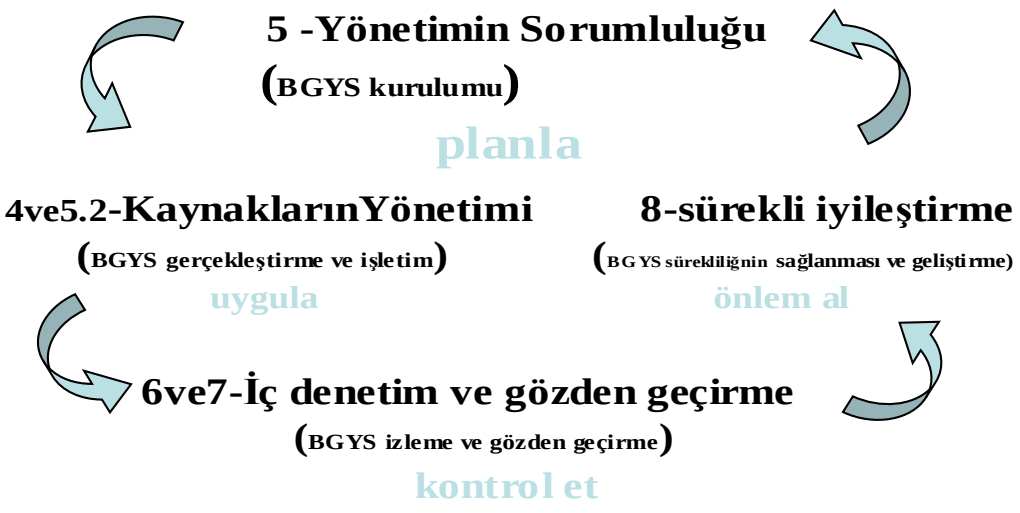
getirirken bu sistemin kurallarını bilmenin ve uygulamanın sorumluluğunu taşımaktadırlar.

Uygunsuz ve kötü amaçlı kullanım sonunda meydana gelecek zararların oluşması, kurum içinde ceza yaptırımıyla karşılaşabileceği gibi yasal yaptırımlara da dönüşebilmektedir.

BGYS İçin Genel Gereksinimler

Bilgi Güvenliği Yönetim Sistemi kurumun tüm ticari faaliyetleri ve karşılaşabileceği riskleri bağlamında kurulmuştur. Yönetim bu standardın gereği olarak sistemi kurmaya, işletmeye, kontrol etmeye ve iyileştirmeye yönelik süreçleri belirlemiştir.

Şekil 4. Proses Bazlı Bilgi Güvenliği Sistemi Modeli



Proses Bazlı Bilgi Güvenliği Sistemi Modeli

Kaynak: Humphreys (2006:5)

BGYS'nin Kurulması

Bilgi ve dolayısıyla bilgi güvenliği için şifreleme hayati öneme sahiptir. Bunun sağlanmasında ilk halka kullanıcı şifresidir. Kullanıcı şifreleri kesinlikle zayıf güvenliğe sahip olmayacak ve kırılması zor, karmaşık yapıda olacaktır. Bütün sistemlerdeki seviyeli şifreler (Kullanıcı,teknik,yönetici) en az ayda bir kez değiştirilecektir. Sistem yöneticileri ise her sistem için ayrı şifreler kullanacaktır. Şifreler kağıt ya da elektronik ortamlara yazılmayacak, ayrıca elektronik posta ya da forma eklenmeyecektir. 3.taraflardan da sisteme girecek kullanıcılar var ise onların da şifreleri karmaşık ve kırılması zor yapıda olacaktır.

Kurumdaki bütün sunumcuların yönetiminden BGYS sistem yöneticileri sorumludur. Konfigürasyon, ayarlama ve değişiklikleri sadece bu grup personeli tarafından yapılacaktır. Tüm sunumcu ve yazılımları yönetim sistemine kayıtlıdır. Üzerinde koşan

yazılımlar, donanım özellikleri, işletim sistemi versiyonları ve görevleri bir merkezi sunumcuda güncel olarak tutulmaktadır.

Kurum veritabanı sistemlerinin güvenli ve kesintisiz bir şekilde işletilmesine yönelik standartlar oluşturulmuştur.

Tüm personelin hassas kurum bilgilerinin tutulduğu sistem odasına, kurum binası ve tüm çalışma alanlarına ise yetkisiz girişlerin önlenmesini sağlayacak sistemler kurulmuştur.

Risk analizi süreci içerideki ya da dışarıdaki herhangi bir donanım üzerinden, uygulama programları, sunucular ve ağ sistemleri üzerinden yapılacaktır. Buna göre oluşturulan raporlar çevresel ve fiziksel güvenlik önlemleri alınmış bir ortamda saklanacaktır.

Tüm çalışanların bilgi güvenliği ile alakalı herhangi bir acil durum meydana geldiğinde ne şekilde davranacağına ve kimlere bilgilendirme yapacağına yönelik prosedürler belirlenmiştir. Acil durumlar oluşmadan önce de uygulanacak acil durum senaryolarının bir plan dahilinde yapılması sağlanmalıdır.

Kurumun tüm bilgisayar ağlarının güvenlik açıklarının taranması konusunda prosedür ve politika belirlenmiştir. Bu sistemin temel gerekliliklerinden biri de güvenlik politikalarına uyumun kontrolü için güvenlik açıklarını tespit etmek ve kullanıcıların ve sistemin tüm hareketlerini kontrol etmektir.

BGYS'nin Gerçekleştirilmesi ve İşletilmesi

Bilgi varlıklarının risklerini yönetmek için gerekli yöntem, kaynaklar, öncelikler ve sorumlular tanımlanarak bir risk işleme planı hazırlanmıştır. Bu planda ayrıca karşılaştırılabilir, yeniden üretilebilir sonuçlar sağlamak için ölçümlerin nasıl yapılacağı da tanımlanmıştır.

Alınan önlemler ve etkinlikler, öneriler, geri bildirimler, ihlal olayları ve güvenlik denetimlerini dikkate alınarak yılda en az 1 kez BGYS'nin gözden geçirme işlemi yapılır. Bu işlem için toplanacak BGYS ekibi ve üst yönetim alınan kararları tüm personele tebliğ edecektir. Ayrıca personele, BGYS'nin işleyişi ve güvenlik ihlallerini hemen tespit ederek BGYS ekibine haber vermesi konularında eğitimler verilerek bunların kayıt altına alınmalarını sağlayacaktır.

BGYS Dokümantasyon Sistemi

BGYS dokümantasyon sistemi, tüm kayıtlardaki eylemlerin yürütülmesi ve izlenebilirliği işlemlerinin bir geri dönüşümünü ihtiva eder. Dokümantasyon hazırlığında Bilgi İşlem Müdürlüğü ve Kalite Müdürlüğü birlikte çalışmış, temel politika olan sistem bütünlüğü korunmuştur. BGYS dokümanlarının hazırlanması ve dağıtım mekanizması Kalite Müdürlüğü'nce yürütülmektedir.

Yönetimin Sorumluluğu

Kurum yönetimi, BGYS'nin kurulumu, gerçekleştirilmesi, izlenilmesi ve iyileştirilmesi konularında BGYS politikalarına bağlı olarak çalışacağını taahüt etmiştir. BGYS'nin bu safhalarını gerçekleştirmek için tüm kaynağı sağlamış, belirlenen risk ve kabul edilebilirlik seviyelerini tespit etmiş ve yapılan iç denetimleri ile tüm sistemi kontrol

etmiş/etmektedir. Ayrıca yönetim tüm personelin bilgi güvenliği konularına gerekli önemi vererek üstüne düşen görevleri yapmasından sorumludur.

İç Denetimler

Kurumumuzdaki BGYS, ISO/IEC 27001 Standardı'nın gerekleri, bilgi güvenliği yasalarıyla uyumu, tanımlanan bilgi güvenliği gereksinimlerine uyumu ve kontrollerin etkin şekilde gerçekleşmesi konularında yılda en az 1 kez genel kontrolden geçirilir.

Görülen uygunsuzluklar ve nedenlerinin giderilmesi için önlemlerin alınması sağlanacaktır. İzleme faaliyetleri ise, önlemlerin doğrulanmasının ve doğrulama sonuçlarının raporlanmasıdır.

Gözden Geçirmeler

Kurulan sistemin uygunluğu, doğruluğu ve etkinliğini ölçmek için yılda en az 1 kez BGYS gözden geçirme toplantısı yapılır. Yapılacak çalışmanın iç denetimden farkı burada sadece BGYS verilerinin, BGYS'de saptanan uygunsuzlukların, BGYS performansının ve bu performansı etkileyen sebeplerin, BGYS prosedürlerinin, BGYS ile ilgili iyileştirmelerin konuşulmasıdır.

Toplantı tutanağında risk değerlendirmesi ve risk işleme planlarındaki değişiklikler, eklenmesi gereken prosedürler, güvenlik gereksinimleri ve kaynak ihtiyaçları yazılmalıdır.

BGYS İyileştirme ve Önleyici Faaliyetler

Kurumumuzda BGYS iyileştirme faaliyetlerine; BGYS politika ve hedefleri, gözden geçirme ve iç denetimler, risk değerlendirme, üçüncü taraf kontrolleri, yasal denetimler, rapor edilen uygunsuzluklar kaynak olmaktadır. Bu faaliyetlerin sonucu olarak düzeltici ve önleyici faaliyetler belirlenmekte, uygulamaları yapılmakta ve bunların da sonsuz döngü içerisinde etkinlikleri izlenmektedir.

BGYS'nin her anı ve her aşamasında tespit edilen uygunsuzluklar takip edilmektedir. Karşılaşılan problemin çözümünde nedenlerinin kaynağına inilmek amacıyla tüm hareketler kayıt edilerek analiz yapılmaktadır. Esas amaç olan problemin çözülmesi değil bir daha oluşmaması için gerekli önlemlerin alınmasıdır. Tüm yapılanlar daha sonra risk değerlendirme ve iç denetimler ile gözden geçirilerek etkinlikleri kontrol edilmekte, öncelikleri yine risk değerlendirme işleminde belirtilerek uygulamaya geçilmektedir.

Olması muhtemel uygunsuzlukların giderilmesi amacıyla bunların nedenlerini ortadan kaldırmak için iç denetimler, periyodik kontroller, sürekli geliştirme faaliyetleri, BGYS gözden geçirme toplantıları ve haftalık kontroller yapılmaktadır. Bu çalışmanın amacı ise varsa değişen risklerin tanımlanmasını ve önemli ölçüde değişen risklerin üzerinde durularak önleyici faaliyetleri gerçekleştirmektir. Yine risk değerlendirme yapılarak yeni oluşan ya da önemi artan risklere kontroller oluşturulacak, belirlenen önceliğe göre bunların uygulanması ile risklerin istenilen duruma getirilmesi ya da tamamen ortadan kaldırılması sağlanacaktır.

GENEL MD. LEVENT BAĞLAR

Tablo 16. Zorunlu Politika ve Prosedürler

POLİTİKALAR		PROSEDÜRLER	
Sıra No	Politika Adı	Sıra No	Prosedür Adı
1	Kurumsal ISO/IEC 27001 Genel Politikası	1	Bilişim Sistem Yönetim Güvenliği Prosedürleri
2	E-Posta Alt Politikası	2	Ağ Yönetim Güvenliği Prosedürleri
3	İnternet Erişim Alt Politikası	3	Teknik Servis Hizmetleri Güvenliği Prosedürleri
4	Erişim Denetimi Alt Politikası	4	Güvenlik Donanım ve Yazılımları Prosedürleri
5	İş Sürekliliği Alt Politikası	5	Kontrol Etkinliklerinin Ölçülmesi Prosedürü
6	Problem Yönetimi ve Güvenlik Olayı Takip Alt Politikası	6	Eğitim ve Farkında Olma Çalışmaları Prosedürü
7	İnsan Kaynakları Güvenliği Alt Politikası	7	Kaynakların Sağlanması Prosedürü
8	Fiziksel ve Çevresel Güvenlik Alt Politikası	8	İzleme ve Gözden Geçirme Prosedürleri
9	Taşınabilir Bilgisayar Alt Politikası	9	BGYS İç Denetim ve Yönetim Gözden Geçirmeleri Prosedürleri
10	Bilgi Sistemleri Edinim, Geliştirme ve Bakımı Alt Politikası	10	Dokümantasyon ve Kayıtların Oluşturulması ve Korunması Prosedürü
11	Haberleşme ve İşletim Yönetimi Politikası	11	Yedekleme Prosedürü

2.6.1.Dokümantasyonun ve Kayıtların Kontrolü

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi, kayıt ve dokümanların sadece uygun yerlerde depolanmasını yeterli bulmamaktadır. Buna göre BGYS ekibi dokümanların yeterince korunup, kontrol edilmeleri konularında bazı gereksinimler tanımlamaktadır.

Bu gereksinimlerin yerine getirilmesi için süreçler oluşturulmalı ve bunlar dikkatlice uygulanmalıdır.

Buna göre BGYS'nin işletilip etkin bir şekilde çalıştığını göstermek için gerekli tüm doküman ve kayıtlar sürekli kullanılabilir, güncel ve olaylarla ilişkilendirilmiş yapıda olmalıdır. Bunlara ek olarak kayıtların gizliliğinin ve bütünlüğünün de sağlanması gereklidir.

Kayıt ve dokümanların saklanıp, işlenmesinin bir diğer nedeni de adli bir olayın meydana gelmesi durumunda bunların kanıt yerine geçip olayın açığa çıkarılmasında yardımcı olma gerekliliklerdir. Bu gibi durumlarda sayılan gereksinimlere ek olarak yasal mevzuatlar devreye girmekte ve bunların BGYS doküman gereksinimlerine entegre edilmesi ihtiyacı ortaya çıkmaktadır. Örneğin 5651 sayılı kanuna göre kullanıcıların web sayfası erişimlerinin kayıtlarının kanıt olarak kullanılabilmesi için, ilgili kayıtların zaman damgası (hash) kodlarıyla birlikte depolanması gerekmektedir. Buna göre kurulacak web sayfası kayıt sisteminde bu özelliğin olması aranmalıdır.

Örnek Dokümantasyon ve Kayıtların Oluşturulması ve Korunması Prosedürü;

	SEMBOLİK BILISIM LTD.ŞTİ. DOKÜMANTASYON VE KAYITLARIN OLUŞTURULMASI VE KORUNMASI SÜRECİ	
YAYIN NO: 27001-KS-01	DOKUMAN ADI:SÜR-KS-V1	VER:0.1

Amaç

BGYS Dokümantasyon Sistemi'nde tutulacak tüm belge ve kayıtların ne şekilde oluşturulup, korunması işlemlerini düzenlemektir.

Kapsam

Tüm BGYS süreçlerini kapsamaktadır.

Uygulama

Dokümantasyonun Oluşturulması

Standart gereğince oluşturulması zorunlu olan ya da ek olarak hazırlanan tüm doküman ve kayıtlar ISO/IEC 27001 BGYS Dokümantasyon Sistemi'ne eklenerek, bilgisayar ortamında ve çıktı şeklinde iki farklı ortamda kayıt edilecektir.

Her dokümanın isimlendirilmesi ve numaralandırılması işlemi Kalite Kontrol Şube

tarafından yapılacaktır. Politika/prosedür/kayıtların isim ve numaları birbirine ilişkilendirilebilir yapıda olacaktır.

Doküman ve kayıtlarda tarih, oluşturan kişi, sürüm bilgileri belirtilecek, değişiklikler kapak sayfasında yine tarih bilgisi ile kayıt edilecektir.

Dokümantasyon içeriğinde amaç ve kapsam açıkça belirtilecek ve süreçlerde sorumlular açıklanacaktır. Son sayfasında hazırlayan, kontrol eden ve onaylayan bölümlerinde ilgili personel bilgileri belirtilecektir. Türkçe Dilbilgisi kurallarına dikkat edilecek, azami şekilde Türkçe kelime kullanılacaktır.

Yeni oluşturulan her dokümanın çalışanlara tebliği ivedi şekilde yapılacak, gerçekleştirilerek eğitim ve farkındalık çalışmalarında dokümantasyon işlemlerinin anlatımına önem verilecektir.

Dokümantasyonun Korunması

Dokümantasyon ve kayıtların BS ve kağıt ortamlarına erişimi sınırlandırılacaktır. Bilgisayar ortamında kayıt edilen dokümanlarda işletim sistemi erişim kontrolü yapılacak, kağıt dokümanların saklandığı odaya giriş izinleri kontrollü yapılacak, giriş çıkış kayıt edilecektir.

Dokümantasyon değişiklikleri tarih bilgileri ile kayıt edilerek, eski sürümlerin kayıtları silinmeyecektir. Geçerliliğini yitirmiş dokümanların imha edilmesi BGYS önerisi ve yönetim kurulu kararı ile gerçekleşecektir.

Yasal gereklilikler ve sözleşmelerden doğan doküman ve kayıtların doğruluğunun sağlanması işlemi özel yazılımlar sayesinde gerçekleştirilecektir. İlgili yazılımda, tüm doküman ve kayıt değişikliklikliklerinin BGYS ekibine otomatik bilgilendirme yapabilme kabiliyeti aranacaktır.

Yasalar gereği zaman damgası ile işaretlenen tüm kayıtlar ayrı bir sunumcuda toplu olarak depolanacak ve buradan istenildiği anda sorgulama yapabilme yeterliliği kazandırılacaktır.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

Bu şekilde tüm dokümantasyon ve kayıt gereksinimleri belirtilecek olup, kuruluşların kendilerine özgü dokümante gereksinimleri sürece eklenecektir.

2.7.Yönetimin Sorumluluğu

Bilgi Güvenliği Yönetim Sistemi diğer standart sistemlerinde olduğu gibi yönetim kararı ve desteği ile gerçekleşmektedir. Ayrıca bilgi güvenliği araçlarının ilk kez yönetim üzerinde uygulanmasıyla sistemin kritikliğinin tüm taraflara aktarıldığı bir standarttır.

2.7.1.Yönetimin Bağlılığı

BGYS standardında yönetimin standarda bağlılığı konusunda yapması gereken tüm işlemler belirtilmiştir. Bilgi güvenliği politikasını kurma, BGYS rol ve sorumlularını atama, BGYS aşamaları için yeterli kaynağı sağlama, yönetimin gözden geçirmesini gerçekleştirme, bu gerekliliklerden bazılarıdır. Burada yönetim kademesi BGYS'nin kurulması, gerçekleştirilmesi, işletilmesi, izlenmesi ve gözden geçirilmesi, sürekliliğinin sağlanması ve iyileştirmesi faaliyetlerinde üstlendiği tüm işlem ve faaliyetler için bizzat kural koyucu ve uygulatıcı mevkide olduğunu beyan etmesi ve kanıtlaması gerekmektedir.

Müstakil ya da herhangi bir kurumdaki Bilgi İşlem Merkezi'nde uygulanan Bilgi Güvenliği Yönetim Sistemi Standardında tüm standartlarda olduğu gibi başarının en önemli faktörlerinden biri yönetimin bağlılığıdır. Kurumda oluşacak tüm değişim ve yenilemelerin kararları, personele örnek olmak ve motivasyon kazanmalarını sağlamak amacıyla yönetim kademesinden çıkar ve bu düzeyde uygulanmaya başlanır. Yönetimin bağlılığı sadece politika, prosedür imzalamak ve bunların uygulanmasını sağlamak ile sınırlı kalmayarak sistemin kurulması, idamesi ve iyileştirmesi konularında ihtiyaç duyulan kaynakların sağlanması ve eğitim ihtiyaçlarının giderilmesi ile tamamlanmaktadır. Bu konuda Bilgi İşlem Merkezleri'ne düşen en büyük görev yönetim kademesine yapacakları doğru ve zamanında bilgilendirme ile oluşacak sıkıntı ve istenmeyen durumların önüne geçilmesidir. Çünkü yönetim BGYS'nin oluşturulması ve eksiklerinin giderilmesi konularındaki gelişmelerden Bilgi İşlem Merkezleri'nin yapacağı bilgilendirme ile haberdar olacaktır. Yapılacak yıllık kontrol ve gözden geçirmeler ile de harekete geçecektir.

2.7.2.Kaynak Yönetimi

Kurum ve kuruluşlarda BGYS'nin kurulması ve işletilmesi yönetim kurulu kararı ile alındığından, maddi ve manevi anlamda gereken tüm ihtiyaçların karşılanması ve bu ihtiyaçları karşılamak için kullanılan kurum kaynaklarının yönetimi yine yönetim kurulu tarafından gerçekleştirilecektir.

2.7.2.1.Kaynakların Sağlanması

Kuruluş BGYS standardında tanımlanan ve uygulanmasını istediği tüm gereksinim ve işlemlerin gerçekleştirilebilmesi için yeterli kaynağa sahip olduğundan emin olmalı ve bunları olması gereken şekilde yönettiğini doğrulamalıdır. Burada örnek olarak Risk Yönetim Sürecinde kullanılacak kaynaklar, planlanan kontrolleri gerçekleştirmek için kullanılan kaynaklar, BGYS'yi sürekli yapıda güncel olarak tutmak için gerekli kaynaklar sayılabilir. Bunların gerekli zamanlarda gerekli şekilde tahsis edilmesini sağlayacak politika ve prosedürler BGYS ekibinin yönetim kurulu ile yapacağı koordine sonucu oluşturulmalıdır.

Kurumda BGYS'nin kurulması, işletilmesi, iyileştirilmesi ve etkinliğinin sağlanması gibi işlemlerde tüm ihtiyaçların belirlenmesi, BGYS ekibi tarafından bunların giderilmesi kararının verilmesi ve maddi desteğin sağlanması yönetim tarafından gerçekleştirilecektir. Kararların direk yönetim tarafından verilmesi ve ne gerekiyorsa maddi desteğin sağlanması personelin gözünde yönetimin bilgi güvenliğine ne kadar önem verdiği olgusunu pekiştirmektedir. Bu konuda Bilgi İşlem Merkezleri'ne düşen görev ise BGYS ekibine olabildiğince destek vermek ve BGYS kurulumu, idamesi, iyileştirilmesi ve etkinliğinin sağlanması işlemlerinde tüm birimlerle birlikte sistemi oluşturmaktır. BGYS'nin Bilgi İşlem Merkezlerinde oluşturulmasının avantajı olarak tüm sistem ve ağ altyapıları hakkında bilgi sahibi olan personelin bu konularda daha önce çalışmış ve nispeten tecrübeli olmasıdır

Kaynakların sağlanması işlemine BGYS ekibi tarafından yapılan haftalık ve yıllık toplantı ve gözden geçirmeler, oluşan anlık bilgi güvenliği olayları ve kapasite yönetimi veri sağlamaktadır. Toplantı ve gözden geçirmelerde alınan kararların uygulanmasında ve bilgi güvenliği olaylarına müdahalede hızlı hareket etmek önemlidir. Bu işlemler düzeltici faaliyetler olmasına karşın kapasite yönetiminin planlanması önleyici bir faaliyet olarak karşımıza çıkmaktadır. Bu üç işlemin uygulanması BGYS ekibi ve nihayet yönetim tarafından oluşturulan politika ve prosedürlerle desteklenmelidir. Politika ve prosedür içeriklerinde istek ve ihtiyaçların yönetime bilgilendirme şekil ve zamanları açıkça belirtilmeli kapasite yönetimine özellikle önem verilmelir. Örnek Kaynakların Sağlanması Prosedürü;

	SEMBOLİK BILISIM LTD.ŞTİ. KAYNAKLARIN SAĞLANMASI SÜRECİ	
YAYIN NO: 27001-KS-01	DOKUMAN ADI:SÜR-KS-V1	VER:0.1

Amaç

Bilgi Güvenliği Yönetim Sisteminin kurulması, işletilmesi, iyileştirilmesi ve etkinliğinin sağlanması aşamalarında ihtiyaç duyulacak tüm kaynakların sağlanması işlemini düzenlemektir.

Kapsam

Kararların alınması ve tüm kaynakların sağlanması konusunda Yönetim Kurulu'nu, İhtiyaç ve isteklerin belirlenmesi konusunda yönetime rapor oluşturulması konusunda BGYS ekibini ve tüm Bilgi İşlem Merkezi personelini kapsar.

Uygulama

Bilgi Güvenliği Yönetim Sistemi'nin kurulması ve idamesi konularında oluşacak tüm ihtiyaçlar yıl sonlarındaki Yönetim Kurulu toplantılarında Bilgi Güvenliği konusuna eklenerek görüşülecektir.

BGYS ekibi tarafından, gerçekleşen bilgi güvenliği ihlal olayları sonucunda gerek duyulan ihtiyaçlar ve öncelikleri belirten aylık rapor Yönetim Kurulu'na sunulacaktır.

BGYS aylık ihtiyaç raporlarından hariç olarak yıllık icra edilecek gözden geçirmeler, iç denetimler ve kapasite yönetimi çalışmalarının sonucu olarak genel manada ayrıntılı yıllık BGYS ihtiyaç raporu sunulacaktır.

BGYS ekibi tarafından çıkarılan ve gereklilikleri sağlayacak ihtiyaç listesinin, finans bölümü tarafından maliyet fizibilite çalışmaları yapılarak rapora eklenecektir. Yönetim Kurulu kararından sonra sistemin önce denemeleri yapılacak, isterleri karşılaması halinde yine yönetim onayı alımı sağlanacaktır.

Fiziki güvenlik ve insan kaynakları güvenliği konularında oluşacak zaafiyetlere anında tepki verilerek yönetim kuruluna rapor edilmesi ivedi işlem yapılması sağlanacaktır.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

Bu şekilde bir prosedür detaylandırılarak hazırlanacak ve tüm taraflara tebliğ edilecektir. Böylece ihtiyaçların giderilmesi konusunda süreç oluşmuş ve acil durumlarda hal ve hareket tarzları belirlenmiş olacağından işlemler kolaylaşacaktır.

2.7.2.2.Eğitim ve Farkında Olma Çalışmaları , Yeterlilik

Bilgi Güvenliği Yönetim Sistemi'nin başarıya ulaşabilmesi için, sadece yönetim kurulu ya da BGYS ekibinin tek başına yapacaklarının yetmeyeceği ve bir kez tamamlanıp, bitirilecek bir sistem olmadığının bilinciyle, kurumda bilgi güvenliğini oluşturacak ve idame ettirecek tüm tarafların katılımını gerektiren eğitim ve farkındalık çalışmalarının yürütülmesi en önemli faktörlerden biridir.

Kurumda Bilgi Güvenliği Yönetim Sistemi'nin oluşturulmaya başlandığı ilk andan itibaren öncelikle bu sistemin insanların yaptıkları işi engellemek için kurulmadığı bilincinin en üst düzey yöneticiden en alt çalışana kadar oluşturulması gerekmektedir. Bu bilincin oluşması sistemin tam anlamıyla sağlıklı bir şekilde kurulup, işletilebilmesi açısından hayati önem taşımaktadır. Kullanıcılara bu bilinci veremeyen, onları süreçlerin içine kendi istekleri dahilinde çekemeyen kurumlar son teknolojiyi kullanarak diğer tüm istekleri karşılamaları durumunda bile başarıyı sağlayamazlar.

İşte bu nokta eğitim ve farkındalık çalışmalarının başlangıç noktası olarak tanımlanmalı ve değişime direnci yok etmenin en büyük aracı olan eğitimin temeli bu bakış açısı ile atılmalıdır. Güvenliğin insanların işlerini zorlaştırmaktan ziyade onların işlerini kolaylaştıracağını, oluşturulan kontrollerle emeklerinin çıktılarını kaybetme ihtimalinin ortadan kaldırıldığını, kötü niyetli insanların aralarında barınmasının önlendiğini anlamalarının sağlanması ve bu amaç doğrultusunda oluşturulacak tüm süreçlerde onlardan da en üst düzeyde katkı beklendiğinin belirtilerek sisteme sahiplik hissiyatı kazandırılması ile başarı kendiliğinden gelecektir[22].

Verilecek eğitim, bilgi güvenliği için rol ve sorumluluklar bazında orantılı şekilde olmalıdır. Rol ve sorumluluk verilecek bu kişilerin istenilen süreçleri gerçekleştirebilecek yeterliliğe sahip olduklarından emin olana kadar eğitimler devam etmelidir.

Eğitim ile ilgili tüm kayıtlar tutulmalı ve bu faaliyetlerin kanıtlanması için muhafaza edilmelidir. Kayıtlar, eğitimin etkinliğinin ve hedeflere ulaşma düzeylerinin ortaya çıkmasında nihai veri olacaktır.

[22] Mohan Kamat,The User Awareness Training of ISMS,Yeni Zelanda,2010 www.iso27001security.com/ISO27k_Awareness_presentation.ppt

Bu bilincin yanında teknik olarak bilgiyi işleme ve kullanma faaliyetlerinin büyük kısmının bilgisayar ağları üzerinde gerçekleştiği günümüz dünyasında, kurumların sahip oldukları bilginin gizliğini, bütünlüğünü ve kullanılabilirliğini koruyabilmeleri için süreçlerinde bilişim teknolojilerini kullanan çalışanlar:

a) Görev ve sorumluluklarını en başta kurumun misyonu doğrultusunda anlamaları,

b) Kurumun bilgi güvenliği ile ilgili çıkardığı ve kendilerinden yüksek düzeyde itaat beklenen politika, prosedür ve uygulamaları anlamaları,

c) Sorumlu oldukları bilgi varlıklarını korumaya yönelik yönetimsel, operasyonel ve teknik açıdan gerekli asgari bilgi seviyesine sahip olmaları gerekmektedir[23].

Ne kadar üst düzeyde bilgi güvenliği teknolojileri kullanılırsa kullanılsın insan/personel faktörünü göze almayan kurumlar en büyük hatayı yaparak yüksek duvarlarla ördükleri sistemin kapısını açık bırakmış olacaklardır. Kurumda en çok hareket gören ve değişiklik gösteren varlık olan insanın istenilen bilgi güvenliği ilke ve talimatlarını uygulaması için en üst düzeyde bilgi ile donatılması gereklidir. İşte bu yüzden Bilgi İşlem Merkezleri'nde en kısa sürede eğitim ve farkındalık çalışmaları süreci oluşturulmalı ve bu sürece uyularak yine sonsuz döngü içerisinde eğitim sistemi geliştirilmelidir. Eğitim sistemi oluşturulurken gereklilikler, sorumluluklar, amaca ulaşma yöntemleri ve etkinlik ölçümleri açık sekilde belirterek sistemde açık bir nokta bırakılmadan üzerinde hassasiyetle durulmalıdır. Bunun en önemli sebeplerinden biri en başta yanlış öğrenilenlerin düzeltilmesinin daha da zor olmasıdır. Bunun tersi olarak ise en başta doğru şekilde öğrenilenlerin, bu temel üzerine yine istenilen şekilde devam etmesi olasılığını arttırdığıdır.

Bilgi güvenliğinin tam ve etkin bir şekilde oluşturulması konusunda en son teknolojinin kullanıldığı durumda dahi bunları bizzat kullanacak ve etkinliklerini sağlayacak olan insan faktörünün yapılan tüm araştırmalar ve yaşananlara bakıldığında sistemin en zayıf halkasını oluşturduğu ortaya çıkmaktadır. Bu nedenle bilişim teknolojileri kullansın ya da kullanmasın tüm personel istenen bilgi güvenliğinin sağlanması konusunda anahtar role sahiptir. Bir kurum varlığı olarak insan gerek beşeri gerek toplumsal özellikleri

[23] Dinçer Önel,Bilgi Güvenliği Bilinçlendirme Süreci Oluşturma Klavuzu,Kocaeli,2008

bakımından değişken bir varlık olması nedeniyle üzerinde daha büyük bir dikkatle durulması gerekmektedir. Burada BGYS'ni kuran tüm kurumlarda olduğu gibi Bilgi İşlem Merkezleri'nde de her seviyedeki kurum çalışanın bilgi güvenliği konusundaki sorumluluklarını kavramasını sağlayacak bir bilinçlendirme ve eğitim sürecinin oluşturulması gerekmektedir. Örnek Eğitim ve Farkındalık Oluşturma Süreci;

	SEMBOLİK BILISIM LTD.ŞTİ. EĞİTİM VE FARKINDALIK OLUŞTURMA SÜRECİ	
YAYIN NO: 27001-EF-01	DOKUMAN ADI:POL-EF-V1	VER:0.1

Amaç

BGYS kapsamında bilgi güvenliği eğitim ve farkındalık süreci oluşturma ve bu süreci yönetme işlemlerini düzenlemek.

Kapsam

Tüm personeli kapsar.

Uygulama

Genel

Eğitim ve farkındalık çalışmalarının oluşturulması ve yönetilmesi süreci tüm BGYS'de olduğu gibi tasarlama (planlama), geliştirme, uygulama ve iyileştirme adımlarından oluşan sonsuz bir yaşam döngüsü içinde oluşturulacaktır.

Sorumluluklar açık ve net bir şekilde belirlenerek, atamaları yapılacaktır. Üst yönetim bilgi güvenliği yöneticisi atayarak ve bu konudaki tüm kaynakları sağlayarak sürecin arkasında durduğunu ve bunun bir yönetim kurulu kararı olduğunu tüm personele hissettirecektir.

Sorumlu atamalarında üst yönetim ile süreç arasındaki iletişimi BGYS ekip lideri, sürecin planlarak uygulanmasını Bilgi Sistemleri Şube Müdürü, personellerinin süreçte belirlenen hususlar üzerinde hassasiyetle durmaları konusunda bölüm yöneticileri ve süreci tam olarak uygularak gerekli bilgi güvenliğinin sağlanmasında ve yöneticilere destek vermeleri konularında kullanıcılar sorumlu olacaklardır.

Sürecin Planlanması ve Tasarlanması

Bilgi güvenliği eğitim ve farkındalık çalışmaları tasarlanırken en başta, verilecek eğitimin kurumun misyonu ve vizyonu, iş gereksinimleri ve hedefleri dikkate alınacaktır. Sürecin kurum kültürü ve kurumun bilgi işlem altyapısına uygun olmasına önem verilecektir.

Öncelikle kurumun bilgi güvenliği eğitim ihtiyaçlarını ortaya koyacak ihtiyaç analizi yapılacaktır. Bu ihtiyaç analizi yöneticiler, güvenlik personeli, sistem yönetimi ve

teknik hizmetler personeli, yazılım personeli, işletmen ve kullanıcıları şeklinde ayrılarak tüm personeli kapsayacak şekilde genişletilecektir. Her grup farklı rol ve sorumluluk taşıdığından farklı eğitim programları hazırlanacaktır. İhtiyaç analizinde anketler, yüzyüze görüşmeler, bugüne kadar düzenlenmiş eğitim ve farkındalık faaliyetleri, geçmiş olay incelemeleri, mevcut kullanıcı hesap dökümleri ve erişim hareketleri, geçmiş denetimler, her türlü teknik ve altyapısal değişiklikler, akademik çevrelerde ve eğitim kurumlarında yaşanan son gelişmeler dikkatle takip edilecek ve bu bilgiler ışığında tüm merkezin ihtiyaç değerlendirilmesi yapılacaktır.

İhtiyaç analizinde; ihtiyaçlar, bugüne kadar ve hali hazırda yapılanlar, öncelikler belirlenerek bu belirlemelere göre başta teknik olmak üzere tüm gereksinimler dokümante edilecektir.

İhtiyaç analizine göre eğitim programının stratejisi ve planı belirlenecektir. Eğitim planında; genel güvenlik politikasındaki eğitim programını ilgilendiren maddeler, programın kapsamı, eğitimi alacak, sunacak personellerin görev ve sorumlulukları, hedef kitle, zorunlu ve isteğe bağlı materyaller, hali hazırdaki ve ulaşılmak istenen bilgi düzeyi, işlenecek konular, dokümantasyon yapısı, gözden geçirme ve güncellenme işlemleri, tekrarlanma sıklıkları konularına değinilecektir.

Plan hazırlandıktan sonra ise öncelikler belirlenerek bir uygulama takvimi oluşturulacaktır. Çalışmalarda takvimlere riayet edilecek olup, eğitimin zaman değişiklikleri yönetim kurulu kararı ile mümkün olacaktır.

Personelin kurumdaki konumu ve iletişim teknolojileri bilgisine göre eğitim materyalleri hazırlanacaktır. Grup tarafından anlaşılması mümkün olmayan karmaşık bilgilerin verilmesi ya da hali hazırda bilinen bilgilerin verilmesi engellenecektir. Bunun sağlanması için bilgi materyallerinin gruplandırılması işlemine gidilecek ve çalışma grubuna göre farklı materyaller kullanılacaktır.

Tasarlama aşamasının son maddesi olarak sürece yönelik kaynak gereksinimleri belirlenecek ve plana eklenecektir. BGYS Ekip lideri bu konudaki ihtiyaçları yönetime açık ve net bir şekilde sunacak, önceliklere göre kaynak aktarımının eğitimlere dağıtımını sağlayacaktır. Kaynak aktarımı işlemi, tüm eğitim bütçesinden ya da tüm bilgi işlem bütçesinden sağlanacaktır.

Sürecin Geliştirilmesi

Bu bölümde eğitim faaliyetleri ve materyalleri içerik detaylarıyla belirlenecek ve temini yapılacaktır. Temin işlemleri yönetim kurulu kararına binaen, kurum içerisinden, diğer kurum ve eğitim kurumları çalışmalarından uyarlanarak veya eğitim kuruluşlarından hazır satın alınarak gerçekleştirilecektir.

Burada süreç geliştirilirken bilinçlendirme ve eğitim faaliyetleri içerik ve bilgi düzeyi konusunda birbirinden ayrılacak, materyaller de bu ayırım çerçevesinde değerlendirilerek temini ve geliştirilmesi sağlanacaktır.

Eğitim ve materyaller doğrudan katılanların görev ve sorumluluklarıyla ilgili olacaktır. Ayrıca güncel konuları da inceleyerek eğitime iştirak edenlerin ilgisini çekecek bilgiler ihtiva edecektir.

sorusunun cevabı verilerek konular belirlenecektir. Kullanıcıların bilgi güvenliğinin önemini anlamaları ve bu ilkelere uygun işlem yapmaları sağlanacaktır. Buna ek olarak denetim ve iç kontrol çalışmaları, bilinçlendirmenin hangi konularda yapılacağına kaynak olarak alınacaktır. Bilinçlendirme konuları bir tablo halinde raporlanacaktır.

Tablo 17. Bilinçlendirme Konuları

Sıra No	Bilinçlendirme Konusu	Açıklama
1	Politikalar	Personele politikalar hakkında genel bilgiler verilecektir.
2	Bilgi Sistemlerinin Tanıtımı	Bilgi Sistemlerinin altyapısı ve işletiminin anlatılması.
3	Giriş Kontrolü ve Fiziksel Erişim Kuralları	Kartlı geçiş sisteminde kullanıcıların yetkileri ve oda yapıları
4	Parola Kullanımı ve Bilgi Kaynaklarına Erişim Kontrolleri	Parola kullanım kuralları ve sunumculara erişim kontrolleri hakkında genel bilgi
5	Virüs ve Kötü Niyetli Yazılımlardan Korunma	Virüs programı kullanımı ve otomatik güncelleştirme özelliği
6	Acil Durum Eylemleri	Acil durum senaryolarında kullanıcı sorumlulukları
7	Yedekleme Sistemleri	Kullanıcılara hangi bilgilerinin yedeklendiğinin anlatılması. Dosyaların yedeklenen sunuculara aktarılması.
8	Bilgisayar Güvenliği	Bilgisayarlarda ne tür güvenlik ilkelerinin uygulandığı hakkında kısa bilgi
9	E-Posta Güvenliği	E-posta güvenlik kuralları ve dikkat edilmesi gereken hususlar
10	Yazılım Lisans Konuları	Lisansız yazılım kullanılmaması ve yıllık temini yapılan yazılımların lisans işlemleri,kullanımı
11	Sosyal Mühendislik	Sosyal Mühendislik konularında genel bilgi,dikkatli olunmasının sağlanması,telefonla şifre sorulmayacağı

Tablo 7'nin devamıdır.

12	Web Sayfaları Kullanımı ve Güvenliği	Web sayfalarında ne gibi hizmetler verildiğinin,bu hizmetlerden hangi şekilde yararlanılacağının ve güvenlik konularının açıklanması
13	Dizüstü Bilgisayar Kullanımı ve Güvenliği	Dizüstü bilgisayarların ne şekilde kullanılacağı ve kullanıcı tarafından alınması ve kontrol edilmesi gereken güvenlik ilkeleri
14	Dosya Aktarım İlkeleri	Bir ağdan diğer bir ağa ne şekilde dosya aktarımlarının yapıldığının anlatılması
15	İnternet Altyapısı ve Kullanım İlkeleri	İnternet altyapısının anlatımı ve alınan güvenlik ilkeleri
16	Intranet Altyapısı ve Kullanım İlkeleri	İç ağ (Intranet) altyapısının genel anlatımı ve alınan güvenlik ilkeleri

Eğitim ise kullanıcı ya da yöneticilere belli konular hakkında güvenlik kabiliyetleri kazandırmak ya da mevcut kabiliyetlerini arttırmak amaçlı verilecektir. Eğitimde verilecek konular da tablo halinde raporlanacaktır.

Bilgi güvenliği eğitici personeli konu hakkında gerçekleştirilecek kurs ve seminerleri azami düzeyde takip edecektir. Kurumsal ya da ülke çapında bilgi güvenliği web siteleri ve e-posta gruplarına üye olunarak bu seviyedeki eğitime kaynak sağlanacaktır. Yıllık kurs planları BGYS ekibi önerisi sonrasında yönetim kurulu kararı ile hazırlanacak ve katılınan eğitimlerin ilgili personel grubuna toplu şekilde aktarılması sağlanacak, bölüm yöneticileri tarafından bu konu hassasiyetle takip edilecektir.

Her eğitim sonrası çalışmanın personel üzerinde bıraktığı etkiler, anlaşılma durumu, uygulamanın kullanıcıları tarafından doğru algılanması, pratiğe geçildiğinde yaşanılacak aksaklıklar üzerinde çalışılarak eğitimin hedefleri kontrol edilecek, ve bu hedeflerin sağlandığı görülecektir.

Sürecin Uygulanması

Sürecin uygulanması için gerekli kaynak temini ve sürecin ne şekilde uygulanacağına yönelik yönetim kurulu kararı alınarak sürece başlanacaktır.

Bilgi güvenliğinin önemi kısa kelime dizeleri ve cümlelerle göze çarpacak şekilde uyarıcı mesaj, uyarıcı ve bilgilendirici poster, ekran koruyucu ifadesi, bilgi güvenliğine yönelik yazı ve yaşanmış olayların tüm personelle paylaşılması, sunum, seminer ve aktiviteler gibi araçlarla her zaman personele hatırlatılacaktır.

Eğitim materyalleri video, bilgisayar ve web tabanlı eğitim, sınıf içi eğitmen gibi araçlarla sağlanacak, eğitimler sonunda çalışanların konuları anladığına dair ufak çaplı

Sürecin İyileştirilmesi

Tüm BGYS'de olduğu gibi edinilen tecrübeler, iç denetimler dokümante edilecek ve bu kaynaklar göz önüne alınarak eğitim sürecinin de sonsuz yaşam döngüsünde iyileştirmeleri yapılacaktır.

Çıkan iyileştirme ihtiyacına göre sürecin planlanması, geliştirilmesi tekrarlanacak, yönetim kurulu kararına göre uygulanması sağlanacaktır.

Yapılan iyileştirmeler kayıt altına alınacaktır.

Tablo 18. Eğitim Konuları

Sıra No	Eğitim Konusu	Açıklama
1	Güvenlik Duvarı-İçerik Filtreleyicisi	Güvenlik duvarı ve içerik filtreleyicisi programlarının kurulumu, işletilmesi
2	Kriptolama Programı Kullanımı	Kriptolama sunumcu ve istemci programlarının kurulumu, işletimi ve kullanımı
3	Vekil (Proxy) Sunumcusu Kurulumu / İşletimi	Vekil sunumcu kurulumu, ayarlamaları, işletilmesi, yedeklenmesi
4	Ağ Altyapısı ve Güvenliği	Ağ altyapısının sistem yöneticisi ve ağ yöneticisi düzeyinde anlatımı
5	İşletim Sistemi Güvenliği	İşletim sistemlerinin güvenlik personeli düzeyinde anlatımı, oluşturulan ilkelerin anlatılması
6	Kartlı Geçiş Sistemi'nin Kurulumu ve İşletimi	Kartlı Geçiş Sistemi'nin kurulumu, işletimi ve arıza giderimi
7	Kamera Kontrol Sistemi Kurulumu ve İşletimi	Kamera Kontrol Sistemi'nin kurulumu, işletimi ve arıza giderimi
8	Bilgi Varlıklarının Sınıflandırılması	Bilgi Varlıklarının ne şekilde sınıflandırılacağı, sınıflandırılan evrak ve bilgilerin ne şekilde saklanacağı ve imha edileceği

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

2.8.BGYS İç Denetimleri

PUKÖ süreç yaklaşımı çerçevesinde kurulup yönetilen Bilgi Güvenliği Yönetim Sistemi'nin kontrol et aşamasının araçlarından biri olan BGYS İç denetimleri ISO/IEC 27001 standardının 6. maddesi gereğince zorunlu kılınmıştır. Buna göre kuruluşlar, mevcut risklerine karşı uyguladıkları kontrollerin, bu kontrolleri uygularken oluşturduğu politika ve süreçlerin tanımlanan bilgi güvenliği hedefine ulaşmak için, ihtiyaçları karşılayıp karşılamadığını, yürürlükteki kanuni zorunluluklarla uyumlu olup olmadığını, etkin olarak gerçekleştirildiklerini ve beklendiği gibi işlenip işlenmediklerini kontrol etmek için BGYS denetimlerini yapmaktadır.

BGYS iç denetimlerine kaynak olacak veriler, geçen dönemlerdeki denetim raporları, kontrol etkinlik ölçümleri, yıl içinde meydana gelen bilgi güvenliği olayları, diğer kuruluşlarca edinilmiş bilgi güvenliği tecrübeleri ve tavsiyeleri gibi bilgilerdir.

Kuruluşun bu denetimleri ne zaman ve ne şekilde yapacağı hakkında bir prosedürü olmalıdır. Bu prosedürde tanımlanan tüm işlemler için sorumlular belirlenmeli ve denetimlerin yapılması esnasında sonuçların kayıt altına alınarak dokümante edilmesi gerekmektedir. Denetimin bir gereği olarak denetçi tarafsız olmalıdır.

Bilgi Güvenliği Yönetim Sistemi'nin Bilgi İşlem Merkezleri ve diğer kurum/kuruluşlarda uygulanmasının ve etkinliliğinin maksimum seviyede olmasının şartlarından biri olan iç denetim, bağımsız bir dış firma tarafından icra edilebileceği gibi kontrolü yapılacak prosedürlerle ilgisi olmayan ve aynı zamanda bilgi güvenliği iç denetimleri konusunda eğitim almış, tecrübeli bir kurum çalışanı tarafından da gerçekleştirilebilir. Fakat gerek işlemlerin karmaşıklaşabileceği gerekse de destek almanın her durumda profesyonellik açısından yararı olacağı düşünüldüğünde, imkan olması dahilinden dış firmadan destek alınması daha faydalı olacaktır.

Sistemin iç denetimi kurum çalışanı tarafından yapılması durumunda olması gereken durum, ilgili çalışanın iç denetim eğitimi alması ve bu konuya eğitim sonrasında sistematik olarak yaklaşabilme yeteneğinin kazandırılmış olması gerekmektedir. İç denetim eğitimi ülkemizde verilmekte, bu eğitimi alma imkanı olmayan kurumlarda ise daha önce bilgi güvenliği konusunda uzman olan birinin görevlendirilmesi

gerekmektedir. Kuruluş her iki seçenekte de bir İç Denetim Prosedürü oluşturulmalı ve genel manada yapılacaklar sıralanmalıdır.Örnek BGYS İç Denetim Prosedürü;

	SEMBOLİK BILISIM LTD.ŞTİ. İÇ DENETİM SÜRECİ	
YAYIN NO: 27001-İD-01	DOKUMAN ADI:SÜR-İD-V1	VER:0.1

Amaç

Yönetim Kurulu kararınca yılda bir yapılacak iç denetim adımlarını belirlemek.

Kapsam

Tüm BGYS'nin denetlenmesini konusunda iç denetim sorumlusunu ve BGYS taraflarını kapsamaktadır.

Uygulama

BGYS İç Denetimi bir önceki yıl olağan yönetim kurulu toplantısından alınacak karara gore yılda 1 kez tarafsız denetleme kurumu ya da kurum çalışanı tarafından yapılacaktır.

Denetmen tarafından oluşturulan sonuçlar BGYS ekibi ve yönetim kuruluna raporlar halinde sunulacaktır. Bu raporlar ve oluşacak kayıtlar 3 sene boyunca saklanacak ve gelecek yılki gözden geçirmeler için kaynak teşkil edecektir.

BGYS ekibi ve tüm personel tarafından denetmene bilgi güvenliği işleyişi hakkında yardımcı olunacak ve işlemlerin denetmen tarafından istendiği gibi kontrol edilmesine yönetim kurulu kararında bahsedilen kapsama göre izin verilecektir.

BGYS kim tarafından yapılırsa yapılsın amacı sistemin açığını bulmaya çalışmak ve eksikleri yönetime bildirmektir. Bulunan açığın giderilmesi hakkında hali hazırda bir planlama yapılmış olsa dahi açıklar yine de bildirilecek ve sistemin genel haritası çıkarılacaktır.

BGYS iç denetimi icracısı/icracıları, tüm politikaları ve prosedürleri inceleyerek daha önce aldıkları güvenlik eğitimleri kapsamında sistemin tüm açıklarını tarayacaklardır. Özellikle Acil Durum Planı incelenecek ve uygulanarak eksiklikler pratik üzerinde gözden geçirilecektir.

BGYS iç denetimi icracıları, kontrol ve uygulamalardan ayrı olarak dokümantasyon sistemini de inceleyecek, oluşturulması gereken dokümanları ve yapılması gereken güncellemeleri kontrol edecektir. Risk analiz raporlarını inceleyerek yıl içinde oluşan olayların risk planlarına dahil edilip edilmediğini kontrol edecektir. Ayrıca başka kurumlarda yaşanan bilgi güvenliği olaylarının işlenip işlenmediği de kontrol edilecektir.

BGYS iç denetim raporunda kontrolün yapılma tarihi, kontrolün içeriği, yapılan

kontrol sonrasında görülen açık/eksikler ve sorumlular belirtilecektir.

Bu gibi tüm işlemler prosedüre eklenerek iç denetimin yapılması ve eksikliklerin giderilmesi sağlanacaktır. Oluşacak rapor dokümante edilecek ve 3 yıl saklanacaktır. Rapor örneğinde;

Tablo 19. Örnek İç Denetim Raporu

Tarih : Proses/Sistem : Takım :		**İÇ DENETİM RAPORU**	Düzenleyen : Revizyon No : Revizyon Tarihi :	
Sıra No	Tarih	Yapılan Kontrol	Eksiklik / Açıklık	Sorumlu

Örnek olarak;

Tarih:25.10.2009

Yapılan Kontrol:Sebat İthalat firmasında 20.05.2009 tarihinde yaşanan ve 2594 sayılı evrakta dokümante edilen güvenlik olayında; güvenlik duvarının FTP Protokolü açığından yararlanarak sisteme girilmiş, aynı sistemi kullanan firmamızda güncellemenin yapılıp yapılmadığı kontrol edilmiştir.

Var Olan Eksiklik/Açık:Sistemimizde de aynı açıktan yararlanarak sisteme sızma, servisleri kullanılamaz hale getirme imkanı bulunmaktadır.

Sorumlu:Bilgi İşlem Merkezi Md., Bilgi İşlem Merkezi Güvenlik Kısım Sorumlusu

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

Bu şekilde tüm eksik ve açıklar tespit edilerek raporda belirtilecek ve yeniden yapılacak risk değerlendirmesi ile öncelikler belirlenerek eksikliklere işlem yapılacaktır.

2.9.BGYS'nin Yönetim Tarafından Gözden Geçirilmesi

BGYS'nin iyileştirme aşamasında asıl kaynak olarak kullanılacak olan sistemin yönetim tarafından gözden geçirilmesi ISO/IEC 27001 BGYS Standardı'nın 7. maddesine göre zorunlu kılınmıştır. Burada sistem tüm detaylarıyla kontrol edilecek ve

bir nevi üç yılda bir yapılan belgelendirme süreçlerinin tüm bölümlerinin uygulanmasıyla sistemin bu kontrole hazır hale getirilmesi sağlanacaktır.

Yönetim tarafından gözden geçirme, önceki yönetim gözden geçirmesi kayıt ve sonuçlarını, BGYS denetim ve sonuçlarını, edinilen geri bildirimleri, önleyici ve düzeltici faaliyetlerin durumunu, risk değerlendirme sürecinde meydana gelen değişiklikleri, etkinlik ölçüm sonuçlarını dikkate alarak bilgi güvenliğini oluşturup her zaman geliştirme hedefine yönelik, tüm sistemde yapılması gereken iyileştirme ihtiyaçlarını ortaya koyan bir çalışmadır. Yapılan denetimlerin sonucu olarak BGYS ve kontrollerinin etkinliklerinin iyileştirilmesi, bilgi güvenliğini etkileyen prosedür ve süreçlerin iyileştirilmesi ve kaynak ihtiyaçları kararları ortaya konmakta ve yapılacak düzenlemeler için çıkarılacak yönetim kurulu kararı ile bu çalışmalara dayanak oluşturulmaktadır[24].

İç denetimlerde olduğu gibi Yönetimin Gözden Geçirmesi işleminin de ne zaman ve ne şekilde yapılacağı politika ya da prosedür şeklinde ortaya konmalıdır. Ayrıca kontrol ve sonuç kayıtları dokümante edilmelidir. Örnek BGYS'nin Yönetim Tarafından Gözden Geçirilmesi Süreci;

	SEMBOLİK BILISIM LTD.ŞTİ. YÖNETİM GÖZDEN GEÇİRMESİ SÜRECİ	
YAYIN NO: 27001-YGG-01	DOKUMAN ADI:SÜR-YGG-V1	VER:0.1

Amaç

İyileştirme çalışmalarına nihai bilgi sağlayacak BGYS'nin yönetim tarafından gözden geçirilmesi işlemlerini düzenlemektir.

Kapsam

Bilgi İşlem Merkezi'nin tüm bilgi güvenliği uygulama, prosedür ve işlemlerini kapsamaktadır.

Uygulama

BGYS'nin Yönetim tarafından gözden geçirilmesi tüm sistemin detaylı bir şekilde kontrol edilerek sonuçlarının yönetim kuruluna rapor halinde sunulması işlemlerini ihtiva eder. Bu işlem en az yılda 1 kez yönetim kurulu olağan toplantısından önce

[23] Dr.Fredrick Björck,ISO 27001 Implementation Guide-Management Review,İsveç,2007 http://security.dj/wp-content/uploads/2009/03/iso-27001-implementation-guide-management-review.pdf

bitirilmelidir.

Yönetim Gözden Geçirmesi, PÜKO modeli çerçevesinde icra edilen ISO/IEC 27001 BGYS standardının sürekli iyileştirme amacını gerçekleşmesinde, yıl boyunca yapılan sürekli kontrol ve iyileştirmelerin genel bir raporunu ihtiva etmektedir. Bu nedenle yapılan 3 yıllık belgelendirme sürecinde icra edilen tüm süreçler burada da tekrarlanarak eksik hususlar ve ihtiyaçlar sonuç raporunda dokümante edilecektir.

Yönetim gözden geçirmesi, BGYS Yönetim Kurulu üyesi başkanlığındaki BGYS ekibi tarafından iç denetimleri kaynak alarak icra edilecek olup, çıkan raporun yönetimin bir kararı olduğu vurgulanacaktır.

BGYS'nin dokümante eksikleri kurum Kalite Kontrol Şubesi tarafından, teknik prosedür ve talimatların uygulanarak etkinliğinin ölçülmesi ise BGYS ekibi tarafından kontrol edilecektir. Tüm güvenlik olayları ve iş süreklilik planları kontrol edilecek olup eklenecek güncelleştirmeler rapora eklenecektir.

Başka kurum/merkez tecrübeleri, 3.taraflardan edinilerek dokümante edilen geri bildirimlerin BGYS'ye entegre edilip edilmediği kontrol edilerek iyileştirme gerekleri rapora eklenecektir.

Önleyici ve düzeltici faaliyetlerin durumu ve etkinlik ölçüm raporları, önceki yönetim gözden geçirme sonuçları, risk değerlendirme sürecinde ifade edilmeyen açıklar kontrol edilecektir.

Oluşturulan BGYS'nin Yönetim Tarafından Gözden Geçirilmesi Süreci yapılan toplantılardan sonra güncelleştirilmeli ve işlemlerin bu prosedüre göre icra edilmesi sağlanmalıdır

Yapılacak tüm kontrol ve uygulamalar sonunda açık/eksik raporu oluşturularak sistemin istenen duruma getirilmesi konusunda öneriler ve kaynak ihtiyaçları eklenecektir.

Tablo 20. Örnek Yönetim Gözden Geçirmesi Raporu

Tarih :			**YÖNETİM GÖZDEN GEÇİRMESİ RAPORU**		Düzenleyen :	
Proses/Sistem :					Revizyon No :	
Takım :					Revizyon Tarihi :	
Sıra No	Tarih	Kontrol	Açıklık	Yapılması Gerekenler/Öneriler	Sorumlular	Kaynak İhtiyaçları

Örnek Kayıt;

Sıra No:5

Tarih:28.01.2010

Uygulanan Kontrol:Oluşturulan Acil Durum Planları'nın uygulanabilir olduklarının kontrol edilmesi

Açık/Eksikler:Alınan yedeklemelerde donanım bağımlı kalındığı görülmüş olup, doğal afetten sonra sistemin geriye döndürülmesi konusunda sıkıntılar yaşanabileceği değerlendirilmiştir.

Yapılması Gerekenler/Öneriler:Yedekleme planı donanım bağımlı olmayan bir sistem üzerine kurularak güncellenecek ve Acil Durum Planları tekrar oluşturulacaktır. Acil durum senaryoları denenerek sistemin eksiksiz çalıştığı test edilecektir. Ayrıca yedekler ikinci bir merkeze daha gönderilerek bölgesel doğal afetlerde başka bir merkezdeki yedeklerden geriye dönme işlemi yapılacaktır.

Sorumlular:Bilgi İşlem Merkezi Müdürü;Sistem Yönetim Kısım Sorumlusu

Kaynak İhtiyaçları:Profesyonel yedekleme yazılımlarının toplam 40 sunumcu için temini ve kurulması konusunda maddi kaynak ihtiyacı

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

2.10.BGYS İyileştirmeleri

BGYS'nin genel yapısının bir defa yapılıp bırakılamayan, sürekli gelişerek yaşayan bir sistem olduğundan daha öncede bahsetmiştik. Burada yapılan tüm çalışmaların amacı kurumda eksiksiz bir bilgi güvenliği sağlayabilmek için sürekli iyileştirmelerin gerçekleştirilmesidir. Bunun en büyük nedeni ise risklerin durağan bir yapıda olmayıp birçok faktöre bağlı olarak değişiklilik göstermesidir. Risklerin bu değişiklik gösterebilir yapısı gerçekleştirilen tüm gözden geçirmeler ile ortaya çıkarılmakta ve risk yönetimini her geçen gün daha da karmaşıklaştırmaktadır. Bir yandan mevcut risklerin değişimleri bir yandan da her geçen gün yeni risklerin oluşması, iyileştirmelerin düzeltici ve önleyici önlemlerinin belirlenip derhal uygulanması ihtiyacını ortaya çıkarmıştır.

BGYS'nin tüm aşamalarındaki mevcut uyumsuzlukların sistematik bir yapıda tespit edilip giderillmesi, tekrar oluşma nedenlerinin ortadan kaldırılması ve gelişen bilgi güvenliği ihtiyaçlarını önceden tahmin ederek olaylarla karşılaşmadan önlemlerinin alınması iyileştirme işlemlerinin içeriğini oluşturmaktadır. Bunları yaparken kontrol et

aşamasındaki sonuçlar kaynak veri olarak alınmakta ve gerektiğinde bunlara girdi yapılarak sistemin eksikleri kapatılmaya çalışılmaktadır.

Gerçekleştirmesi planlanan tüm işlemler PUKÖ döngüsü içinde tekrar risk yönetimi sürecine dahil edilecek ve kontroller oluşturularak işlenmesi ve bunların gözden geçirilmesi ile tamamlanacaktır. Kontrollerde çıkacak uyumsuzluklar iyileştirilecek ve yapı bu şekilde devam edecektir.

Gerçekleştirilen tüm iyileştirme işlemleri hangi kontrole göre ne şekilde yapıldığı kayıt altına alınmalı ve sonraki çalışmalara kaynak olacak şekilde saklanmalıdır. Bu iyileştirmeler sistemin nereden nereye geldiğini kanıtlama konusunda yardımcı olacaktır.

Önleyici ve düzeltici iyileştirme olarak ayrılan konu tüm standartlarda ortak olarak vurgulanmaktadır. Bilgi İşlem Merkezleri'nde BGYS uygulanması hususunda özel olan nokta Yazılım/Donanım/Sistem/Personel maliyetlerinin daha fazla olması nedeniyle önleyici iyileştirmelerin üzerinde daha fazla durularak tüm personele bu konunun hassasiyetinin hissettirilmesi ihtiyacıdır. Güvenlik ihlal olaylarında anında müdahaleden daha önemli olan bu olayların gerçekleşmesine imkan verilmemesidir. İhlal olayı gerçekleştiğinde oluşacak maliyet bunları önlemenin maliyetinden çoğu kez daha fazla olmaktadır. Bu kararların verilmesinde Risk Yönetim Süreci'nin hayati önemi bulunmakta ve önceden görülebilecek bir riskin giderilmesi, BGYS iyileştirmeleri için en uygun durum olarak karşımıza çıkmaktadır. BGYS'nin önleyici ve düzeltici iyileştirmelerinin içeriği ve sorumluları tek bir prosedür/talimat/planda toplanacağı gibi ayrı ayrı da dokümante edilebilmektedir. Örnek BGYS İyileştirme Süreci;

TSE	SEMBOLİK BILISIM LTD.ŞTİ. BGYS İYİLEŞTİRME SÜRECİ	SBS
YAYIN NO: 27001-İYİ-01	DOKUMAN ADI:SÜR-İYİ-V1	VER:0.1
Amaç BGYS'nin Kontrol Et aşamasındaki eksikliklere göre iyileştirmelerin yapılması işlemlerinin düzenlenmesi **Kapsam**		

Tüm BGYS etkinliklerini kapsar.

Uygulama

İç denetim raporları, Yönetim Gözden Geçirmeleri raporları ve BGYS ekibinin olağan toplantılarında alınan kararlara göre sistemin iyileştirilmesi, güncelleştirilmesi işlemlerini yapmak, sürekli iyileştirme amacı güden ISO/IEC 27001 BGYS Standardının olmazsa olmaz kuralı olduğu unutulmamalıdır. Konuya bu hassasiyetle yaklaşarak sadece kurulup bırakılan bir sistemin yaşamını sürdüremeyeceğinin tüm personel tarafından bilinmesi gerektiği vurgulanacaktır. Düzeltici faaliyetler kapsamında kontrol et aşaması sonucunda çıkan raporlara göre, uygunsuzlukları tanımlama, uygunsuzlukların nedenlerini belirleme, bunların tekrar yaşanmamaları için uygun faaliyetleri belirleme, düzeltici faaliyetleri belirleme ve gerçekleştirme, bu faaliyetlerin sonuçlarını kaydetme ve gözden geçirme işlemleri yapılacaktır.

Önleyici faaliyetler kapsamında ise olması muhtemel uygunsuzlukları ve nedenlerini belirleme, önleyici faaliyet ihtiyacını değerlendirme, önleyici faaliyet belirleme ve gerçekleştirme, faaliyet sonuçlarını kaydetme ve bunları gözden geçirme işlemleri gerçekleştirilecektir.

Oluşturulan raporlara ve günlük olaylara karşı yapılan risk değerlendirmesine göre öncelik sıralarını göz önünde bulundurarak en hızlı şekilde tepki gösterilecektir.

İç Denetim ve Yönetim Gözden Geçirme Raporları'na göre gerçekleştirilecek iyileştirmeler genel manada sistemin gerekirse köklü değişiklere götüreceğinden yıllık olağan yönetim kurulu toplantısında alınacak karara göre icra edilecektir.

Oluşturulacak raporda, iyileştirmeler iş planı şeklinde detaylı bir şekilde belirtilecektir. Bunların hangi karara istinaden yapıldığı raporda açıklanacak, sorumlu ve öneriler eklenecektir. Öneri alınması konusunda sadece bilgi güvenliği personeli değil, o sistemi kullanan personel de karar mekanizmasına dahil edilecektir.

Yeni iyileştirmeler oluşturulacak prosedür ve talimatlara göre uygulanacaktır. Mevcut kontrolün güncellenmesi ya da yeni kontrollerin eklenmesi aşamasında tüm uygulamalar dokümante edilecektir.

İyileştirme yapıldıktan sonra kontrol etkinlikleri ölçülecek ve istenen duruma gelene kadar iyileştirme işlemine devam edilecektir.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

2.11.Bilgi İşlem Merkezlerinde BGYS Kapsamında Uygulanan EK-A Kontrolleri

Şu ana kadar ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı'nın Bilgi İşlem Merkezleri'nde kurulması ve işletilmesi, gözden geçirilmesi ve iyileştirmeleri konuları işlenmiştir. Buradan sonra ise standardın EK-A bölümünde bahsedilen ve

ISO/IEC 27002 ile desteklenen uygulamaya yönelik kontroller ve bunların uygulanış şekillleri anlatılacaktır.

2.11.1.İnsan Kaynakları Güvenliği

Bilgi İşlem Merkezleri'nde kurulacak Bilgi Güvenliği Yönetim Sistemi Standardı'nın EK-A'sında ve ISO/IEC 27002 önlemler klavuzunda üzerinde önemle durulan insan kaynakları güvenliği konusu, istihdam öncesi, istihdam sırasında ve sonrasindeki işlemlerin, yönetimin sorumluluğunun ve eğitim gibi genel konuların anlatıldığı bir politika ile netleştirilmelidir. Örnek insan kaynakları güvenliği politikası;

	SEMBOLİK BILISIM SIRKETİ INSAN KAYNAKLARI GÜVENLİĞİ POLİTİKASI	
YAYIN NO: 27001-İYİ-01	DOKUMAN ADI:POL-IKG-V1	VER:0.1

Amaç

İstihdam edilecek insan kaynakları ve 3. taraf kişi/kuruluşlar için uygulanacak bilgi güvenliği kontrollerinin düzenlenmesini sağlamak.

Kapsam

Kurum/merkezde istihdam edilecek personel 3. taraf kişi/kurumları kapsamaktadır.

Uygulama

İstihdam Öncesi

Yönetim kurulu tarafından ihtiyaç duyulacak pozisyonlar için gerçekleşecek personel alımlarında çalışanların, malzeme ya da hizmet alımlarında yüklenici ve üçüncü tarafların seçilmesinde güvenliğin baştan sona yaşanan bir süreç olduğu göz önüne alınarak istihdam öncesinden önem verilecektir.

Güvenliğin kurum için önemi istihdam öncesinden personele, yüklenicilere ve üçüncü taraflara bildirilerek bilgi güvenliğinin kurum kültürü olduğu hissettirilecektir.

Tüm işe alım adayları, yükleniciler ve üçüncü taraflar için ilgili yasa, düzenleme ve etiğe göre iş gereksinimleri, erişilebilecek bilginin sınıflandırılması ve alınan risklerle orantılı olarak geçmiş doğrulama kontrolleri gerçekleştirilecektir.

Sözleşme yapılırken tüm tarafların rol ve sorumlulukları, bilgi güvenlik politikalarına göre tanımlanacak ve dokümante edilecektir. Üçüncü taraf kullanıcı sözleşmelerinde kurumun bilgi güvenliği politikalarından haberdar olmaları sağlanacak ve bilgi güvenliği hususları da dokümante edilerek imzalatılacaktır.

İstihdam Esnasında;

Kurum bünyesinde çalışanlar, yükleniciler ve üçüncü taraf kullanıcılarının bilgi güvenliği tehdit/kaygılarının ve kendi sorumluluklarının farkında olmaları sağlanacaktır. Bu kişilerin çalışmaları sırasında kişisel ve kurumsal güvenlik ilkelerini sağlayarak, insan hatası riskini en aza indirecek bilgi düzeyine erişmeleri temin edilecektir.

Yönetim olarak tüm taraflardan, oluşturulan politika/prosedürlere göre bilgi güvenliği gerekliliklerini yerine getirmeleri istenecektir. Bu uygulamaların bilgi güvenliği ilkeleri çerçevesinde yapılması gerektiği kontrol edilecektir.

Bilgi Güvenliği Yönetim Sistemi ilk kurulduğunda tüm taraflara detaylı bir şekilde gelinen ve amaçlanan durum açıklanarak prosedür/talimatlar hakkında bilgiler verilecektir. Uygulamalar başladıktan sonra ise yapılacak her türlü değişiklikte çalışanların eriştikleri bilginin derecesine göre bilgilendirme yapılacaktır. Bilgi güvenliği uygulamalarının herhangi bir değişikliğinden habersiz olan tarafın kalmaması amaçlanacak ve bununla ilgili gerekirse aylık toplantılar planlanacaktır. Verilecek eğitim sadece yetkililere değil tüm personeli kapsayacak şekilde tabana yayılacaktır.

Bilgi güvenliği ile ilgili olarak disiplin prosesi geliştirilerek tüm taraflar üzerinde caydırıcılık oluşturulacaktır. Kişilerin bilgi güvenliğini zedeleyecek hata ya da bilinçli davranışlarda başlarına gelecekler sıralanarak daha dikkatli olmaları sağlanacaktır.

İstihdamın Sonlandırılması veya Değiştirilmesi

İstihdamın sonlandırması işlemini yapacak birim istihdamın başlangıcında olduğu gibi İnsan Kaynakları Şubesi'dir. Bu bölümün mevcut olmadığı durumlarda birimin en üst düzey yöneticisi görevlendirilecektir. İstihdamın sonlandırılması kararı gerekçeleri ile açıklanacak, mümkün olduğunca çalışanların hakları ödenerek tarafların düşmanca tavır alması önlenecektir.

İstihdam sonrası yapılacak tüm varlık değişimleri ilk sözleşmede belirtilerek yapılacak değişikliklerin dokümante edilmesi sağlanacaktır. Bilgi güvenliğini zedeleyebilecek tüm varlıklar teslim alınacaktır.

Personel işten ayırımlarında merkez/kurumun tüm bilgi varlıkları teslim alınacak ve yeniden kullanılabilmeleri için gerekli ayarlamalar yapılacaktır. Personelin görev yerine göre yönetici parolaları kesinlikle değiştirilecektir. Yapılacak çalışmaya göre daha önce ayrılan personel tarafından erişilen tüm dosya ve klasörlerin erişim denetimleri kaldırılacak, şifreleri resetlenecektir.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

2.11.2.Fiziksel ve Çevresel Güvenlik

EK-A kontroller ve ISO/IEC 27002 Standardı'nın üzerinde durduğu bir diğer konu da fiziksel ve çevresel güvenliktir. Bilgi güvenliği işleminin ilk olarak en dışarıdan içeriye doğru oluşturulduğu göz önüne alındığında bina güvenliği ve çevresel güvenlik

konularının hayati öneme sahip olduğu anlaşılmaktadır. Fiziksel ve çevresel güvenliğin oluşturulması ile ilgili merkez/kurumun bir politikası olmalı ve bu politikaya göre işlemler yapılarak dokümante edilmelidir. Örnek olarak Fiziksel ve Çevresel Güvenlik Politikası;

	SEMBOLİK BILISIM SIRKETİ FİZİKSEL VE ÇEVRESEL GÜVENLİK POLİTİKASI	
YAYIN NO: 27001-FÇG-01	DOKUMAN ADI:POL-FÇG-V1	VER:0.1

Amaç

Kurum/merkezin fiziksel ve çevresel güvenlik ilkelerini belirlemek

Kapsam

Tüm firma çalışanları ve üçüncü şahısları kapsamaktadır.

Uygulama

Güvenli Alanlar

Bilginin işlendiği, depolandığı ve saklandığı tüm alanların en üst seviyede fiziksel güvenlikleri alınacaktır. Bilgi İşlem Merkezleri binanın alt katında konumlandırılacaktır. Genelden özele doğru tüm kapılar kontrol altında bulundurulacaktır.

Tüm odaların giriş çıkışları merkezi kontrol sistemi ile sağlanacak ve bu giriş çıkışlar bir program vasıtasıyla izlenecektir. Odaların anahtarları sadece oda sorumlusunda kontrollü şekilde bulundurulacak ve açılış kapanış zamanları oluşturulacak defterlere kayıt edilecektir.

Yangın, sel, deprem, patlama ve diğer doğal/insan kaynaklı felaketlere karşı kontrol sistemleri kurulacaktır. Tüm oda ve alanlarda yangın detektörlerini ihtiva eden yangın sistemi oluşturulacaktır. Bina depreme karşı kuvvetlendirilecektir. Patlama ve diğer insan kaynaklı felaketlere karşı uygun önlemler alınarak tatbikatları yapılacak ve bu felaketlerin meydana geldiği durumlarda herkesin yapması gerekenler öğretilecektir. Tüm sistemlerin kapı kontrol sistemi ile entegresi sağlanarak, olağanüstü durumlarda kapıların otomatik olarak açılması sağlanacaktır.

Turnike sistemi kurulacak, malzeme alımı ve yükleme alanlarında çalışacak yetkisiz kişilerin de girebildiği alanların bu turnike sisteminin dışında bırakılması sağlanacaktır. Böylece yetkisiz kişiler Bilgi İşlem Merkezlerinden uzak tutulacaktır.

Teçhizat Güvenliği

Kullanılan tüm bilgi varlık/teçhizatları çevresel tehditlerden ve tehlikelerden kaynaklanan riskleri, yetkisiz erişim fırsatlarını azaltmak amacıyla uygun şekilde

yerleştirilmeli ve korunmalıdır.

Bilgisayar monitörleri cama yakın ve dışarıya dönmüş şekilde konumlandırılmayacaklardır. Yazıcılar yetkisiz kişilerin de erişebileceği ortak alanlara konulmayacaklardır.

Bina elektrik kesilmelerine karşı jeneratör ile beslenecektir. Elektrik ihtiyacı duyan tüm bilgi varlıkları kesintisiz güç kaynaklarına bağlanacak ve uzun elektrik kesintilerinde kontrollü şekilde kapatılarak sistemin zarar görmesi ihtimali ortadan kaldırılacaktır.

Tüm bilgi transferlerinin yapıldığı data kabloları ile elektrik kabloları ayrı şekilde asma tavan üzerine yapılacak tavalar üzerinden götürülecektir. Duvar kenarlarından kablo geçmeyecektir. Yapılacak tüm işlemler kendi tavaları üzerinden gerçekleştirilecektir. Oda içerlerinde ise plastik kablo kanalları kullanılacak olabildiğince kablonun dışarıya çıkması engellenecektir. Kablolardan geçen datanın kayba uğramaması için elektrik ve data kablo tava ve kanallarının arasında mesafe bırakılacaktır.

Depolama ortamı olarak kullanılan cd, disket ve usb cihazların içerikleri arıza ya da transfer gibi nedenlerle elden çıkarılma durumlarında, hassas bilgi ya da lisanslı yazılımla gönderilmeleri ihtimaline karşı farklı silme programları ile silinecektir.

Tüm bilgi teçhizat/varlıklarının kurumdan dışarıya çıkarılmaları söz konusu olduğunda içerisinde hassas bilgi olmayacak şekilde, Bilgi İşlem Yetkilisi izni ile işlem yapılacaktır.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

2.11.3.Haberleşme ve İşletim Yönetimi Güvenliği

Buraya kadar oluşturulan ve daha çok kurumun altyapısına yönelik kontrollerden sonra Bilgi İşlem Merkezleri'nin daha çok üzerinde mesai harcadığı haberleşme ve işletim yönetimi güvenliği konusuna değinelecektir. Burada yapılacak tüm işlemler, bilgi varlıklarını yöneten Bilgi İşlem Merkezleri'nin bilgi güvenliği konusunda başlıca görevlerini sıralamakta ve oluşturulacak politika, prosedür ve talimatlarla haberleşme ve diğer sistemlerin güvenliği arttırılmaktadır. Yine yapılacak tüm işlemler dokümante edilmeli ve standarta eklenmelidir. Örnek Haberleşme ve İşletim Yönetimi Güvenliği Politikası;

	SEMBOLİK BILISIM SIRKETİ HABERLEŞME VE İŞLETİM YÖNETİMİ GÜVENLİĞİ POLİTİKASI	
YAYIN NO: 27001-HİY-01	DOKUMAN ADI:POL-HİY-V1	VER:0.1

Amaç

Haberleşme ve İşletim yönetimi safhalarında bilgi güvenliği gerekliliklerini yerine getirerek, güvenliğin sonsuz döngü içerisinde arttırılmasını sağlamaktır.

Kapsam

Tüm personeli ve üçüncü şahısları kapsamaktadır.

Uygulama

Operasyonel Prosedürler ve Sorumluluklar

Bilgi varlıklarının işlenmesi, depolanması işlemlerinde kullanılan tüm uygulamalar işletim prosedürü olarak dokümante edilecek,işlemler bu dokümanlar üzerinden sürdürülecek ve gereklilikleri tüm çalışanlar tarafından uygulanacaktır.

Tüm teknolojik gelişmeler ve bilgi işleme olanaklarındaki değişiklik ve yenilikler kontrol edilerek, bunların sisteme entegrasyonları sağlanacaktır.

Bilgi varlıklarının yetkisiz olarak veya farkında olmadan değiştirilme ve kötüye kullanma fırsatlarını azaltmak ya da ortadan kaldırmak için en ufak işten en kapsamlı işe kadar görev ve sorumluluklar detaylı bir şekilde anlatılacak ve dokümante edilecektir.

İdari sistemleri ile geliştirme ve test sistemleri yetkisiz erişim ve yetkisiz değiştirme risklerini azaltmak için tamamen ayrılacaktır.

Üçüncü Taraf Hizmet Sağlama Yönetimi

Üçüncü taraflara hizmet sağlama sözleşmeleri yapıldığında uygun bilgi güvenliği ve hizmet dağıtım seviyeleri gerçekleştirilecek ve sürüdürülecektir.

Uygulanan tüm bilgi güvenliği uygulamalarının hizmet tanımları ve servis seviyeleri yapılacak sözleşmede belirtilecek ve bunların üçüncü taraflarca gerçekleştirilmesi, işletilmesi ve sürdürülmesi sağlanacaktır.

Sağlanan tüm hizmetler, raporlar ve düzenli kayıtlarla izlenecek, gözden geçirilecek ve düzenli olarak denetlenecektir.

Tüm değişiklikler yönetilecek, riskler yeniden değerlendirilerek sisteme entegre edilecektir.

Sistem Kabulü

Yeni bilgi sistem alımları, sistem yükseltmeleri ve yeni sürümler için kabul kriterleri oluşturulacaktır. Bu kriterler her yıl/dönem güncellenecektir. Ayrıca teslim alınacak

sistemlerin alımı yapılmadan önce tüm testleri tamamlanacak, bundan sonra nihai alım gerçekleştirilecektir.

Kurum/merkezin tüm işlemlerini yapmasına kaynak olan donanım ve yazılımların kullanımı incelenerek, gelecekteki kapasite gereksinimleri için öngörüler oluşturulacaktır. Kapasite kullanımının %75'i geçmesi durumunda yeni dönemde kaynaklar gözden geçirilerek düzeltmeler, geliştirmeler yapılacaktır.

Oluşturulacak kapasite planlama prosedürüne göre tüm sistemler incelenecek, raporlanacaktır.

Kötü Niyetli ve Modil Koda Karşı Koruma

Sistemin kötü niyetli ve mobil koddan korunması için gerekli saptama, önleme ve kurtarma prosedürleri oluşturulacaktır. Bu sistemler kurulurken teknoloji takip edilecek ve açıklar kontrol edilecektir.

Hizmetlerin ihtiyacı olan bir mobil kod yetkilendirildiğinde, işletilmesi güvenlik kriterlerine göre devam edecek ve yetkilendirilmemiş kodun yürütülmesi engellenecektir.

Yedekleme

Acil Eylem Planları ve olağanüstü durumlarda sistemin yeniden çalışabilir hale getirilmesinde hayati öneme sahip olan yedekleme ayrı bir prosedür olarak dokümante edilecek ve tüm işlemler bu prosedür üzerinden gerçekleştirilecektir.

Yedekler alındıktan sonra çalışabilirliği test edilecektir. Her ay yapılacak düzenli kontrollerde yedeklerin sistemi geri döndürme kabiliyetleri sınanacaktır.

Yedekler farklı iki bölgede depolanacak ve aralarındaki iletişim de yedekli olacaktır.

Ağ Güvenliği Yönetimi

Tüm bilginin üzerinden aktığı ağ sistemlerinin kontrolü, hem cihaz hem de kablo üzerinde sağlanacaktır. Tüm ağ cihazları tek bir sunumcu üzerinden kontrol edilerek güvenliği sağlanacaktır. Sistemler bu sunumcu üzerinden verilen yetkilendirmeye göre ağa dahil olabileceklerdir.

Data kabloları güç kabloları ile aynı yerden çekilmeyecekler, aralarında mesafe bırakılacaktır. Kabloların cihazlara bağlı olduklarını kontrol eden ve değişiklikleri rapor edebilen yazılımlar sisteme entegre edilecektir. Oluşacak kablo kopuklukları ya da data kayıplarında sistem yöneticisine anında bilgi gönderilecektir.

Tüm ağların haritası çıkarılarak üzerlerinden geçen iletişimin band genişliği ve bilgi çeşitliliği incelenecektir.

Ortam İşleme

Usb, cd ve disket gibi taşınabilir ortamların değiştirilmesi, bina dışına çıkarılması ve yok edilmesi kontrollü yapılacak ve bilgi dahilinde olmayan işlemler gerçekleştirilmeyecektir.

Tüm sistemin haritası ve bilgileri sadece ilgilisi tarafından erişilebilir hale getirilecek

ve dışarıya bilgi sağlanmayacaktır. Ayrıca dokümante edilen tüm bilgi varlıkları yetkisiz erişime karşı korunacaktır.

Taşınabilir ortamlara bilgi işlenen yerler dağınık yapıda olmayacak ve merkezi halde tutulacaktır. Sadece izin verilmiş kişiler tarafından bilgi aktarılacak ve şahsi ortam ve bilgi kullanılmayacaktır.

Tüm taşınabilir ortamla bilgi işlenmesi hareketleri izlenebilir ve kontrol edilebilir nitelikte olacaktır. Bunun için sistemler kurulacak ve haftalık kontrolleri yapılacaktır.

Bilgi Değişimi

Tüm bilgi değişimi etkinlikleri prosedür ve talimatlar çerçevesinde kontrollü bir şekilde gerçekleştirilecektir.

Bilgi değişimi dış şahış ve kurumlarca yapılacaksa, nasıl yapılacağı oluşturulacak sözleşmelerde açıkça belirtilecektir.

Ortam, kuruluşun fiziksel sınırları dışarısına taşınacaksa, çalınma, kötüye kullanım ya da bozulmalara karşı korunacaktır. Tüm ortamlar kriptosuz şekilde bina dışına çıkarılmayacak ve sadece ulaşması gereken yerlerde uygun şifreleri ile açılacaktır. Dış etkenlerden zarar görmemesi için uygun şekilde paketlenecek, muhafazası alınacaktır.

Bilgi değişiminin en fazla yoğunluğa sahip çeşidi olan elektronik mesajlaşma ayrı bir prosedür şeklinde kontrollü olarak yapılacaktır. Burada da bilgi güvenliğine önem verilecek ve oluşturulacak kontrol sistemleri ile erişim ve iletişim güvenli olarak sağlanacaktır.

Verilen ya da alınan bir hizmete yönelik yazılım ve donanımların oluşturulduğu iş bilgi sistemlerinin birbirine bağlantısı ve ilgili bilgiyi korumak için geliştirilen prosedür ve talimatlar, o hizmetle ilgili oluşturulacak genel prosedür ve talimatlarda vurgulanacaktır. Burada da hizmet verilir ya da alınırken güvenliğin önemi vurgulanacaktır.

Elektronik Ticaret (Kurum elektronik ticaret hizmeti veriyorsa)

Alım satım hizmetlerini bir web sitesi üzerinden veren kurumumuz bu işlemlerin güvenliğini sağlamaktaki mevcut son teknolojileri kullanacaktır.

Kripto teknolojilerinin gelişmesi ile birlikte bunların takibini ve entegrasyonunu sağlayacak bir ekip kurulacak ve bu ekip, tüm müşterilerinin bilgilerinin tutulduğu veritabanlarından ticaretin yapıldığı banka hizmetlerine kadar baştan uca bilgi güvenliğinin sağlandığı sistemler oluşturacaktır. Konuyla ilgili çıkmış tüm kanun, tüzükler kontrol edilerek uygulanması gereken tüm hizmet kriterleri sağlanacaktır.

Yetkisiz erişim ve değiştirme üzerinde durularak yetkilendirme sistemlerinin çeşitlendirilmesi ile bir sistemdeki açığın diğer sistemle kapatılması sağlanacaktır. Oluşturulacak kripto teknolojileri vasıtasıyla müşteri ile şirket arasındaki özel ağ üzerinden işlem yapılacaktır.

İzleme

İzleme ile ilgili öncelikle kanun gereklilikleri sağlanacak, gerekirse alınan kararlar

doğrultusunda gerekliliklerden de fazla bilgiler izlenerek ileri de yaşanabilecek soruşturma ve erişim kontrolü izleme işlemlerine yardımcı olacak bir bilgi sistemi kurulacaktır.

Kurulacak izleme bilgi sisteminin tek yerden yönetilebilir ve merkezi yapıda olması sağlanacaktır. Mümkünse, yeterlilikleri sağlayacak tek bir sistemin oluşturulması amaçlanacaktır. İzleme birkaç sistem üzerinden yapılacaksa alınan kayıtlar çapraz incelenebilir yapıda olacaktır.

Öncelikle kullanıcı hareketleri izlenecektir. Daha sonra alınacak kayıtların yetkisiz erişimi ve değiştirilmesini önlemek için zaman damgası yapısı oluşturulacaktır. Bu işlemlerden sonra tüm sunumcu ve istemci bilgisayarların hata kayıtları toplanarak üzerlerinde hata incelemeleri yapılabilir hale getirilecektir.

Kayıtların incelenmesinde tüm sistem saatlerinin aynı olması önemlidir. Bu yüzden saat senkronizasyonu internetteki doğruluğu kabul görmüş bir sunumcudan yapılacaktır.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

2.11.4.Erişim Kontrolü

Bilgi güvenliği ilkelerinden biri olan erişim kontrolü Bilgi İşlem Merkezleri'nin bilgi güvenliği konusunda üzerinde durduğu ve pratik olarak en çok çalıştığı bölümdür. Erişim kontrolünün gereğiyle yapılmaması sonucunda bilginin gizliliği, bütünlüğü ve erişilebilirliği bozulabilmektedir. Karşılaşılan sorunların büyük bir kısmı erişimin yetkisiz kişilere de verilmesi sonucunda oluşmaktadır. Bu yüzden erişim kontrolü bilgi güvenliğini sağlamada kritik konumdadır. Bilgi işlem Merkezleri erişimin kontrollü bir şekilde yapılması konusunda birçok farklı sistem kullanmakta ve geliştirmektedir. Bu nedenlerden dolayı Bilgi İşlem Merkezi personelinin gerek dosya erişimi gerekse sistem erişimi konularında bilgi ve birikime sahip olması gerekmektedir. Erişim kontrolünün ne şekilde gerçekleştirileceği en üst düzeyde politikalardan en alt düzeydeki prosedür ve talimatlara kadar açık bir alan bırakmadan dokümante edilerek uygulanmalıdır. En üst düzeyde erişim kontrolü politikası oluşturulmalı ve alt düzeylere doğru her sunumcunun ve sistemin erişim kontrolleri prosedürler halinde yayımlanmalı ve uygulanmalıdır. Örnek Erişim Kontrolü Politikası;

	SEMBOLİK BILISIM LTD.ŞTİ. ERİŞİM KONTROLÜ POLİTİKASI	
YAYIN NO: 27001-EKP-01	DOKUMAN ADI:POL-EKP-V1	VER:0.1

Amaç

Merkez/kurum bünyesindeki mevcut sunumcu ve sistemlere erişim yetkilerinin ne şekilde gerçekleştirileceğini tanımlamaktır.

Kapsam

Bilgi erişimini kontrol eden tüm Bilgi İşlem merkezi personelini ve bu bilgilere erişip, işleyen diğer departman personellerini kapsamaktadır.

Uygulama

Erişim Kontrolü İçin İş Gereksinimi

Bilgi güvenliği ilkelerinden biri olan erişim kontrolü işlenen ve depolanan tüm bilgi varlıklarını kapsayarak bunların erişimlerinin kontrollü yapılmasını sağlayacaktır.

Tüm sistemler için ayrı ayrı erişim kontrolü prosedürleri belirlenecek ve gözden geçirilerek yapılan değişikliklerle güncellenecektir.

Kullanıcı Erişim Yönetimi

Tüm kullanıcıların bağlı bulunduğu departmana göre tüm işlemleri tek ve kendine özgü kimlik ile yapabilmeleri için kullanıcı adları oluşturulacaktır.

Verilecek tüm yetkiler bu kullanıcı adları üzerinden yapılacak olup, sistemlere kullanıcı adı ve parola kullanmadan erişim sağlanmayacaktır.

Kullanıcı adları personeli kuruma katılışı ile oluşturulacak ve bu kayıtlar merkezi olarak saklanacaktır. Mümkün olduğu takdirde ayrılan personelin kullanıcı adı yeni katılan personele verilmeyecektir. Mümkün olmaması takdirde ise ayrılan personelin kullanıcı adı 1 yıl süre ile saklanacaktır.

Sistemde Yönetici ve kullanıcı olmak üzere iki adet kullanıcı çeşidi bulunacaktır. Yönetici olacak kullanıcıların yetkileri ayrı ayrı tanımlanacak ve mümkün olduğunca yapılacak işin gerekliliklerinden fazla yetki verilmeyecektir. Verilen yetkiler dokümante edilecektir.

Kullanıcı parolaları ayrı bir prosedürle belirlenecektir. Burada parola en az 6 karakter olacak, rakam ve harf ihtiva edecektir. 15 gün süre ile değiştirmeleri istenecek ve en az önceki 3 şifreyi hatırlayacaktır.

Sistem yöneticileri kullanıcıların erişim yetkilerini özellikle dosya sunumcularındaki hakları bakımından aylık olarak kontrol ederek hataların önüne geçilecektir.

Kullanıcı Sorumlulukları

Kullanıcıların parola prosedürlerini tebliğ etmeleri sağlanacak ve bu prosedüre uygun şifre seçmeleri sistem tarafından zorlanacaklardır.

Ortak kullanım için oluşturulan ortak ve gözetimsiz teçhizatların kontrolünü sistem yöneticilerinin merkezi olarak yapmasının yanında kullanıcıların da bu konuda uyanık olmaları sağlanacaktır.

Bilgisayar ve çalışma masaları üzerinde gereksiz ve gizlilik ihtiva eden belge ve taşınabilir ortamlar bulundurulmayacaktır. Bu konuda temiz masa ve ekran politikası benimsenecektir.

Bilgi güvenliğinin sağlanmasında kullanıcı sorumlulukları prosedür ve talimatlarla belirlenecek ve kendilerine tebliğ ettirilerek oluşabilecek bir hukuki durumda sorumluluğun kendilerinde olduğu hissettirilecektir.

Ağ Erişim Kontrolü

Kullanıcılar sadece, kullanımlarına yetki verilen hizmetlere erişim sağlayacaklardır.

Kurum dışından erişim sağlayacak kullanıcıları da kontrol etmek için kripto güvenli erişim kontrolü sağlanacaktır. Uzaktan erişim için kullanıcı bilgisayarları ile merkez sunumcusu arasında özel ağ oluşturulacak ve bu özel ağa erişim için kullanıcılara kullanıcı adı ve şifresi verilecektir. Bu kullanıcı adı ve şifreler düz metin şeklinde değil kriptolanarak depolanacaktır. Kullanıcı genel anahtarını sunumcu ile paylaşacak ve alınan kriptolu şifreyi özel anahtarıyla açarak iletişimin sağlanması gerçekleştirilecektir.

Ağlardaki cihazların otomatik tanımlama özellikleri aktif hale getirilerek daha önce yapılan ayarlamalara göre hizmet vermeleri sağlanacak, böylece cihazlara bir kez ayar yapılarak daha sonraki işlemlerini bu ilk ayar üzerinden gerçekleştirilmesi sağlanacaktır.

Bilgisayar ve sunumculara uzaktan bağlanıp, onları kontrol etme hizmeti mümkün olduğu kadar az verilerek güvenlik arttırılacaktır. Bu hizmetin verilmesinin zaruri olduğu durumlarda genel bilinen port kullanılmayacak, değiştirilecektir. Bunun için de kullanıcı adı ve şifresi sağlanarak kontrollü erişim sağlanacaktır.

Tüm ağlar, bilgi hizmetleri, kullanıcılar ve bilgi sistemleri, üzerinde işlenen gizlilik derecesine göre ayrılacak ve erişime açık ağlardan diğer ağlara geçiş engellenecektir.

Tüm ağlarda iletişimi sağlayan yönlendirme protokolleri ve işlemleri erişim kontrol politikasını ihlal etmeyecek şekilde oluşturulacak ve aylık olarak kontrol edilecektir.

İşletim Sistemi Erişim Kontrolü

Bir kullanıcının kullandığı işletim sistemine göre kullanıcı kimliğini ispatlamak için uygun bir kimlik doğrulama metodu seçilecektir. Windows sistemlerde kerberos kimlik doğrulama, linux sistemlerde ise digest kimlik doğrulama metodu kullanılacaktır.

Kullanıcılar tarafından sistem dosyaları üzerinde değişiklik yapabilme yeteneği olan yardımcı sistem programları kullanılmayacaktır.

Sunumcu üzerinde işlem yapmadan bekleyen kullanıcıların oturumları yarım saat

içinde kapatılacak şekilde ayarlama yapılacaktır.

Yüksek riskli uygulamalar için üzerinde işlem yapılsa bile bağlantı süreleri 1 saat ile sınırlanacaktır. Bir saat sonunda oturumu düşen kullanıcının sisteme tekrar giriş yapması sağlanacaktır.

Uygulama ve Bilgi Erişim Kontrolü

Kullanıcılar ve destek personeli sadece yetkili oldukları bölüm ve sunumculara erişebilecek ve bu erişimleri kayıt altına alınacaktır. Verilen tüm erişimler aralıklarla kontrol edilecek, gözden kaçan yanlış yetkilendirmeler en kısa sürede geri alınacaktır.

Hassas/kritik uygulama ve bilgiler için erişim saat kısıtlaması getirilerek mesai saatleri dışında erişim sağlanamayacaktır. Olağanüstü durumlarda izin mekanizması kurularak personelin erişim yetkileri bu şekilde düzenlenecektir.

Hassas/kritik sistemler ortak sunumcularda konumlandırılmayacak, bunların yerine sadece onlar için adanmış sunumcular üzerinde çalışılacaktır.

Mobil Bilgi İşleme ve Uzaktan Çalışma

Mobil bilgi işleme olanakları sadece merkezin personele sağladığı cihazlar üzerinden gerçekleştirilecektir. WAP/GPRS/3G teknolojileri kullanımında diğer dışarıdan bağlantılar gibi güvenliği arttırılmış protokoller kullanılarak mobil cihaz ile merkez sunumcusu arasında özel ağ kurulması sağlanacaktır. Bunlar için bina içi kimlik doğrulasından daha güvenli bir kimlik doğrulama metodu kullanılacaktır.

Uzaktan erişim mümkün olduğunca kısıtlanacak olup, erişmesi gereken personel için güvenlik önlemleri arttırılacaktır. Hangi bilgisayarlardan bağlanacağı daha önceden kuruma bildirelecek ve üzerlerine güvenlik yazılımları kurularak yetkisiz erişim olasılığı azaltılacaktır.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

2.11.5.Bilgi Sistemleri Edinme, Geliştirme ve Bakımı

BGYS'nin Bilgi İşlem Merkezleri'nde uygulanmasının bir diğer ayırıcı yanı, temini yapılan tüm bilgi varlıklarının teknik altyapılarının Bilgi İşlem Merkezleri tarafından oluşturulması işleminde, bilgi güvenliği süreçlerinin en başından uygulanması ilkesi gereğince ihtiyaçların dokümante edilmesinde de güvenliğin ön planda olması gerçeğidir. Bu yüzden bilgi sistemleri edinimi, geliştirilmesi ve bakımı süreçlerinde bilgi güvenliği unsuru ön planda tutularak, en baştan kontrol altına alınması, daha sonraki safhalarda güvenlik gereksinimlerinin azaltılmasını amaçlamaktadır.

Bilgi İşlem Merkezleri'nin bilgi sistemleri edinme, geliştirme ve bakımları safhalarında bilgi güvenliğinin ne şekilde oluşturulması gerektiğini belirleyen bir politika ya da prosedüre ihtiyaç duyulmaktadır. Örnek Bilgi Sistemleri Edinme, Geliştirme ve Bakımı Politikası;

	SEMBOLİK BILISIM LTD.ŞTİ. BİLGİ SİSTEMLERİ EDİNME, GELİŞTİRME VE BAKIM POLİTİKASI	
YAYIN NO: 27001-BSE-01	DOKUMAN ADI:POL-BSE-V1	VER:0.1

Amaç

Bilgi İşlem Merkezleri tarafından bilgi sistemleri edinme, geliştirme ve bakımları safhalarında bilgi güvenliği ilkesinin ne şekilde oluşturulacağını düzenlemek.

Kapsam

BS ihtiyaçlarının teknik altyapısını belirleyen tüm Bilgi İşlem Merkezi personelini kapsar.

Uygulama

Bilgi Sistemlerinin Güvenlik Gereksinimleri

İhtiyaç duyulan tüm BS donanım ve yazılımları için teknik özelliklerin yanında ayrı ayrı güvenlik gereksinimleri belirlenerek dokümante edilecektir.

Her donanım ve yazılım için dokümante edilen güvenlik ihtiyaçları teknolojinin gelişmesi ve yenilikler ışığında gerekli görülürse hemen, görülmezse her yıl/dönem başında güncellenecektir.

Uygulamalarda Doğru İşleme

Güvenlik gereksinimleri, hali hazırda uygulanan ve yeni uygulanacak bilgi sistemleri için planlı aralıklarla kontrol edilerek düzeltilecek, geliştirilecektir.

Uygulamaların veri girişi esnalarında zorunlu alanlar ve bu alanlara ait veri formları oluşturularak bu verinin doğruluğu ve uygunluğu sağlanacaktır. Uygulamalar işlenirken ise hata veya kasıtlı eylemler nedeniyle bilginin bozulmasını saptamak amacıyla kimlik doğrulama ve otomatik doğrulama soruları ile bilgi geçerleme yapılacaktır.

Uygulamalardaki verinin doğruluğunu sağlama, mesaj bütünlüğü ve çıktı doğruluğunu ve uygunluğunu sağlama amacıyla yine veri geçerleme yapılacaktır.

Kriptografik Kontroller

Merkez/kurum hassas/krıtik bilgilerinin işlenmesi ve depolanması esnasında satın alacağı bir kriptoloji programıyla şifreli şekilde anahtarlı yapı kuracaktır. Hassas yazılım kullanacak personellerin bilgisayarlarına kriptografik yazılımın istemci yazılımı

kurularak sadece o bilgisayarı kullanan personele yetki verilecektir.

Seçilecek anahtar yapılarının şifreleyebileceği karakter sayısı her uygulama için ayrı ayrı belirlenerek ihtiyaca göre dokümante edilecektir. Sistemin önce testleri yapılarak şifrelemenin sağlıklı şekilde oluşturulduğu kontrol edilecek ve nihai alım yapılacaktır.

Sisem Dosyalarının Güvenliği

Tüm yazılımların kaynak kodlarına erişim sınırlandırılarak sadece yetkili kişilerin erişebilmesi sağlanacaktır.

Oluşturulacak sistemin test verileri dikkatlice seçilecek, korunacak ve bu bilgiler planlı aralıklarla kontrol edilecektir.

Geliştirme ve Destekleme Proseslerinde Güvenlik

Yazılım oluşturulduktan sonra değişim ihtiyacı duyulduğunda ilgili prosedürler oluşturulacak ve yapılan değişiklikler dokümante edilecektir. Ayrıca değişiklikler sadece gerek duyulan bölümler için yapılarak sıkı bir biçimde kontrol edilecektir. Yazılımın değiştirilmeden önceki sürümü de ayrı bir yerde yedeklenecektir.

Yazılımlar gibi işletim sistemlerininde de değişiklik kararı alındığında bunun güvenliğe kötü etkisi olmamasını sağlamak amacıyla tüm gözden geçirme ve test prosedürleri tekrarlanacaktır. Bu işlem yapılmadan önceki halinin tam kopyası yedeklenecektir.

Bilgi sızmasını önlemek maksadıyla dışarıdan alınan tüm yazılımların kaynak kodları istenerek denetlenecek ve dışarıya oluşan tüm trafik kontrol edilerek bilgi sızması önlenecektir.

Teknik Açıklık Kontrolü

Temini yapılacak yazılımlarda, mümkün olduğunca yayımlanmış teknik açık olmayanlar tercih edilecek, zaruret doğması durumunda bu açıkların takibine önem verilerek zararları zamanında müdahalelerle en aza indirilecektir.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

2.11.6.Bilgi Güvenliği İhlal Olayı Yönetimi

Şu ana kadar anlatılan konular önleyici kontroller olup, bilgi güvenliği ihlal olayı oluşmasını önlemeye yönelik işlemlerdir. Fakat günlük hayatta alınan tüm önlemlere rağmen güvenlik ihlal olayları gerçekleşmekte ve bu olayların yönetiminin ihtiyacı artmaktadır. Bilgi güvenliği ihlal olaylarının oluşma olasılıkları, bilişim teknolojilerinin gün geçtikçe büyük bir hızla gelişmesi, bilgi işlem faaliyetleriyle ilgilenen kişilerin artması, hizmetlerin internet gibi açık bir sistemde verilmesi ve kişilerin kötü niyetli

araçlara kolaylıkla sahip olabilmesi gibi birçok nedenden dolayı artmıştır. Bu gibi işlemlerin muhattabı olan Bilgi İşlem Merkezleri'nin ise iş yükü bu konuda yoğunlaşmıştır.

Tüm bu nedenlerden dolayı yaşanabilecek kötü senaryolara hazırlıklı olması gereken Bilgi İşlem Merkezleri'nin bilgi güvenliği ihlal olaylarını da uygun politika/prosedürler ile yönetebilme kabiliyetini kazanmaları gerekmektedir. Bunun için tüm senaryolar incelenerek politikanın oluşturulması ihtiyacı bulunmaktadır. Tek politika üzerinden genel hatları çizilecek sistemin prosedürler ile desteklenmesi ve tatbiki test edilerek tecrübe kazanılması gerekmektedir. Örnek Bilgi Güvenliği İhlal Olayı Yönetimi Politikası;

	SEMBOLİK BILISIM LTD.ŞTİ. BİLGİ GÜVENLİĞİ İHLAL OLAYI POLİTİKASI	
YAYIN NO: 27001-GİO-01	DOKUMAN ADI:POL-GİO-V1	VER:0.1

Amaç

Bilgi Güvenliği İhlal Olayı vuku bulduğunda yapılacak tüm işlemleri belirlemektir.

Kapsam

Bu olayın oluştuğu andan itibaren sistemi eski haline getirmekle görevli bilgi işlem merkezi ve diğer departman personelini kapsamaktadır.

Uygulama

Bilgi Güvenliği Olayları ve Zayıflıklarının Rapor Edilmesi

Bilgi güvenliği olaylarının en hızlı biçimde rapor edilmesi için uygun hiyerarşik kanal mekanizmaları oluşturulacaktır. Her personele bu mekanizmalar bildirilerek karşılaşılan durumun ne şekilde rapor edileceği öğretilecektir.

Yapılacak sözleşmelerde tüm çalışanların, yüklenici ve üçüncü tarafların, sistem ve hizmetlerdeki gözledikleri veya şüphelendikleri herhangi bir güvenlik zayıflığına dikkat ederek rapor etmeleri istenecektir.

Bilgi Güvenliği İhlal Olayları ve İyileştirmelerinin Yönetilmesi

Bilgi güvenlik ihlal olayı oluşması durumunda ne şekilde işlem yapılacağı tüm senaryolar üzerinden geçilerek sorumlularla birlikte dokümante edilecektir.

Öncelikle planlı bir şekilde çalışma yapılabilmesi için ihlal olaylarının türleri, miktarları ve kuruma maliyetlerini ölçüp, izlemeye yarayan mekanizma kurulacaktır. Bunun için olay meydana geldiğinde hızlı bir şekilde BGYS ekibi toplanacaktır.

Sistemin zararlarının giderilip eski haline dönmesi konusunda yapılan plan ve ihtiyaçlar rapor halinde yönetim kuruluna sunulacaktır. Alınan karara binaen sorumluları ile birlikte kontroller uygulanacak, bu durumun tekrar yaşanmaması amacıyla gerekli iyileştirmeler yapılacaktır.

Bilgi güvenliği ihlal olaylarında mevcut izleme programları sayesinde alınacak kanıtlar toplanacak ve ilgili makama sunulacaktır. Bunun kanun karşısında kanıt olarak sunulabilmesi için gereksinimleri sağlayacak şekilde sistem kurulacaktır.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

2.11.7.İş Sürekliliği Yönetimi

İş Sürekliliği BGYS'nin kurulması ve işletilmesi açısından büyük öneme sahiptir. Sistemin kurulmasının başlıca amaçlarından birini oluşturan iş sürekliliği, merkez/kurumun hassas iş süreçlerinin devamlılığını sağlamak ve aksi durumlarda daha önceden belirlenen kesinti süreleri içerisinde sistemin tekrar kullanılabilir hale getirilmesi işlemlerini gerçekleştirmektir. Hassas/kritik süreçlerin, istendiği her anda kullanılabilir olması gerekmekte, günlük yaşamda ise bunları kesintiye uğratan ufak ya da büyük olaylar gerçekleşebilmektedir. Burada ulaşılabilir amaçlar ortaya koyarak merkezin en az zararla çalışmalarını sürdürmesi amaçlanmalıdır. Bu amaç doğrultusunda gerekli sistemin planlı bir şekilde kurularak, olması muhtemel olaylara karşı kontrollerin oluşturulması ve tatbikinin yapılarak hazır duruma gelinmesi gerekmektedir.

İş Süreklilik Yönetimi dokümante edilerek sorumluların belirlenmesiyle planlı bir şekilde sistem eski haline getirilmelidir. Örnek İş Süreklilik Politikası;

	SEMBOLİK BILISIM SIRKETİ İŞ SÜREKLİLİK POLİTİKASI	
YAYIN NO: 27001-İSS-01	DOKUMAN ADI:POL-İS-V1	VER:0.1

Amaç

Merkez/kurumda İş Sürekliliği Yönetim Sistemi kurulması işlemlerini düzenlemektir.

Kapsam

Merkezde İş Sürekliliği Yönetim Sistemi kurulumu ve yaşatılması çalışmalarına

katılacak tüm Bilgi İşlem Merkezi ve diğer departman personelini kapsamaktadır.

Uygulama

Öncelikle BGYS ekip lideri başkanlığında ve BGYS ekibiyle birlikte tüm süreç sahiplerinin katılacağı proje grubu oluşturulacaktır.

Oluşturulan proje grubu tarafından, üst yönetim istatisikleri, yaşanmış örnekler, başarıdaki üst yönetim faktörü, hedefler, görev ve sorumlulukları kapsayan bir bilgilendirme yapılarak yönetimin projeye desteği sağlanacaktır.

Projede nelerin yapılması planlandığının detaylı bir şekilde açıklandığı proje planı hazırlanacak, yine yönetim onayı ile yayımlanacaktır.

Öncelikle kurumun mevcut süreçleri ve bu süreçleri oluşturan varlıkların belirlenmesi işlemleri tamamlanacaktır. Daha sonra bu varlıkların açıkları ve bunların kullanılarak meydana gelebilecek olası zararlar belirlenecektir.

Risk Analizi yapıldıktan sonra tüm sistem ve uygulamalar üzerinde kabul edilebilir kesinti süreleri, kabul edilebilir veri kayıpları bilgileri oluşturularak iş etki analizi yapılacaktır. Bu analiz kesintilerin kuruma olan etkisini belirleme amaçlı olacaktır. Tüm iş süreçleri çalışma içerisine dahil edilecektir.

Risk analizi ve iş etki analizi yapıldıktan sonra iş sürekliliği yönetim takımı oluşturularak, sorumluluk ve yapılacak işler belirlenecektir. Her sürecin risk ve etki analizi çıktıları görüşülerek senaryolar üzerinde yapılacak kontroller belirlenecektir. Hedefler belirlenerek sistemin eski halini alması için gereken zaman planlanacaktır. Hedefin gerçekleşebilmesi için ihtiyaçlar belirlenerek bunların temin edilmesi sağlanacaktır.

İş Sürekliliği Yönetim Sistemi dokümante edilerek sorumluların heran ulaşabilir niteliğe kazandırılması sağlanacaktır. Dokümantasyona, yapılan tüm çalışmalar eklenecektir. Bunlara örnek olarak Acil Durum Planı, kurtarma prosedürleri, tatbikatların ne şekilde yapılacağı, kriz durumu iletişim ihtiyaçları, iş sürekliliğinin nasıl güncelleştirileceği, eğitim faaliyetleri bilgileri yazılacaktır.

İş sürekliliği organizasyonundaki tüm personele ihtiva edilen konu ve kontrollerle ilgili eğitim verilecektir. Bu eğitimde herkesin görevinin üzerinde ayrı ayrı durularak yapılması gerekenler anlatılacaktır. Eğitimler her yıl yenilenerek, geliştirilecektir. Ayrıca tüm personele genel bir iş süreklilik eğitimi verilerek farkındalık sağlanacaktır.

İş sürekliliğinin etkinliğini ölçmek ve olağanüstü durumlara hazır olmak maksadıyla tatbikatlar yapılacaktır. Tatbikat planları oluşturularak nelerin yapılacağı belirlenecek ve bu plana göre sorumluların hareket tarzları incelenecektir. Tatbikat sonunda planın eksikleri ve güncelleştirilmesi gereken yerleri üzerinde çalışılarak sistemin istenen duruma getirilmesi sağlanacaktır.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

2.11.8.Uyum

Bilgi İşlem Merkezleri'nde kurulumu yapılacak olan ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'nin bir amacı da mevcut kanun ve yürürlükteki diğer bilgi güvenliği unsurlarının kurum tarafından uygulanmasıdır. Standardın bu kısmında yürürlükteki tüm kanun ve bilgi güvenliği unsurları ayrı ayrı incelenerek sisteme entegrasyonları sağlanacaktır. Bu entegrasyon sırasında yapılan tüm işlemler dokümante edilmeli ve standarta eklenmelidir.Bu eklemelerin yapılması işlemlerinin bir süreç dahilinde gerçekleştirilmesi ihtiyacı duyulmaktadır. Bu yüzden Bilgi Güvenliği Yönetim Sistemi uygulayan tüm Bilgi İşlem Merkezleri'nde diğer bilgi güvenliği kanun ve standartlarına uyum politikası geliştirilmeli ve dokümante edilmelidir.Örnek Uyum Politikası;

TSE	SEMBOLİK BILISIM LTD.ŞTİ. UYUM POLİTİKASI	SBS
YAYIN NO: 27001-UYUM-01	DOKUMAN ADI:POL-UYUM-V1	VER:0.1

Amaç

Mevcut ya da daha sonra oluşturulacak bilgi güvenliği kanun ve standart maddelerine uyum işlemlerinin düzenlenmesini sağlamaktır.

Kapsam

Standardın düzenlenmesi işlemlerini yapılmasında BGYS ekibini, işlemlerin tamamlanmasında tüm personeli kapsamaktadır.

Uygulama

Yasal Gereksinimlere Uyum

Kurum ve mevcut bilgi sistemleri için tüm yasal ve sözleşmelerden doğan gereksinimler açıkça tanımlanacak ve ayrı ayrı dokümante edilecektir.

Fikri mülkiyet haklarının korunması ve yazılım ürünlerinin kullanımı konularında yasal gereksinimlerin sağlanması için prosedürler oluşturulacak ve bu prosedürlerin işlenmesi sağlanacaktır.

Bilgi güvenliği ve diğer konularda oluşturulan tüm hassas kayıtlar, kaybolma, çalınma ve değiştirilmeye karşı gereksinimler, yasal ve diğer sözleşmelere göre gerçekleştirilecek ve dokümante edilecektir.

Tüm kullanıcılara yasalar gereği bilgi işlem olanaklarını kötüye kullanmalarında başlarına neler geleceği anlatılacak ve caydırıcı önlemler arttırılacaktır.

Tüm kriptografik kontroller mevcut yasa ve yapılacak sözleşme hükümlerine göre

uygulanacaktır.

Güvenlik Politikaları, Standartlara Uyum ve Teknik Uyum

Bölümlerin tüm yöneticileri mevcut güvenlik politikaları ve standartlara uyumu sağlamak için sorumluluk alanlarındaki tüm prosedürlerin tam ve doğru bir şekilde gerçekleştirilmelerini sağlayacaklardır.

Tüm bilgi sistemlerinin güvenlik uygulamalarının standartlara uygun olarak çalıştığı düzenli aralıklarla kontrol edilecektir.

Bilgi Sistemleri Denetim Hususları

Bilgi sistemleri süreçlerinin denetim gereksinimleri ve bu işlemi yaparken yararlanılacak tüm kontrol ve uygulamalar detaylı bir şekilde planlanacak, dokümante edilecektir.

Oluşturulan tüm kontrol ve uygulamalar yetkisiz erişim ile kötüye kullanım ihtimallerine karşı dikkatlice korunacak ve üzerinde uyuşmazlıklar giderilecektir.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

2.12.BGYS Belgelendirme Süreci

Kuruluşun bilgi güvenliği kültürünün oluşturulması, Bilgi Güvenliği Yönetim Sistemi'nin kurulması, işletilmesi, gözden geçirilmesi ve iyileştirmesi işlemlerini yapmasının amacı öncelikle hizmet ya da mal üretiminin daha sağlıklı ve daha güvenli bir şekilde gerçekleştirilmesidir. Bu karar uygulanırken, yönetim kurulu kararı, yasal zorunlulukların var olması, sektörde diğer kuruluşlara karşı avantaj sağlamak ya da bu işlemleri akredite üçüncü taraflara onaylatmak gibi sebeplerle sistemin belgelendirilmesi istenilebilir. Bu belgelendirme ile kuruluş, ISO/IEC 27001 Standardı'nda belirtilen gerekesinimleri karşılayan Bilgi Güvenliği Yönetim Sistemi'ni kurup işlettiğini kanıtlamış olacaktır.

Belgelendirme sürecinin üç tarafı bulunmaktadır. Bunlardan birincisi belgelendirilmek isteyen kuruluş, ikincisi belgelendirme kontrolünü yapacak belgelendirme/tescil kuruluşu, üçüncüsü ise belgelendirmeyi onaylayacak akreditasyon kuruluşudur. Akreditasyon kuruluşları, uluslararası ve bölgesel akreditasyon ağları ile işbirliği halindedirler ve belgelendirmeyi bazı kurallara göre yaparlar. Türkiye'nin ulusal akreditasyon kurumu TÜRKAK'tır ve bu kuruluş Avrupa Akreditasyon Kurumu EA'nın üyesidir. Kurumlar belgelendirme işlemini başlatmak için öncelikle akredite

belgelendirme kuruluşlarına, bu kuruluşlardan edinecekleri belge ve formları hazırlayarak müracaat etmektedirler.

Tablo 21.TÜRKAK'a Akredite ISO/IEC 27001 Belgelendirme/Tescil Kuruluşları

Sıra No	Akreditasyon Kurumu	İletişim
1	TSE	Ankara/Türkiye 0312 4178330
2	Kalitest	İstanbul/Türkiye 0212 2693741
3	Alberk QA	İstanbul/Türkiye 0216 5724910

Tablo 22. TSE Yönetim Sistemi Belgelendirme Ücretleri

Çalışan Sayısı	**Müracaat ve Dosya İnceleme Ücreti**		**Yıllık Belge Kullanma Ücreti**	
	Yurt İçi	**Yurt Dışı**	**Yurt İçi**	**Yurt Dışı**
1-25	300.00 TL+KDV	250 USD	600.00 TL+KDV	500 USD
26-50	400.00 TL+KDV	250 USD	750.00 TL+KDV	500 USD
51-100	400.00 TL+KDV	250 USD	900.00 TL+KDV	500 USD
101-250	500.00 TL+KDV	250 USD	1100.00 TL+KDV	500 USD
251-500	600.00 TL+KDV	500 USD	1400.00 TL+KDV	750 USD
501- 1000	750.00 TL+KDV	750 USD	2000.00 TL+KDV	1000 USD
1001 ve Üzeri	750.00 TL+KDV	750 USD	2250.00 TL+KDV	1000 USD

Tetkik Tipi	**Tetkik Ücreti (ADAM/GÜN)**	
	Yurt İçi	**Yurt Dışı**
Belgelendirme, Gözetim, Takip, Kapsam Genişletme, Model Değişikliği Tetkiki	300.00 TL+KDV	500 USD
Ön Tetkik	400.00 TL+KDV	500 USD
Ek Belge Basım Ücreti (Unvan değişikliği veya adres değişikliği olduğunda alınır)	100.TL+KDV	100 USD

Buna göre belgelendirme kuruluşu bir veya birden fazla denetçiyi sistemin denetlenmesi için görevlendirmektedir. Denetçiler, yapacakları kontrollerin başarılı olması halinde belgelendirme kuruluşuna istenilen belgenin verilmesi tavsiyesinde bulunurlar. Bu tavsiye üzerine tüm sistem, belgelendirme kuruluşunun atayacağı bir yönetim ekibi tarafından gözden geçirilir. Bu gözden geçirmede de başarılı olunursa kuruluşun BGYS tescili yapılır ve belgelendirme kuruluşu ile akreditasyon kuruluşunun damgalarıyla onayladıkları bir belge verilir.

Verilen belge üç yıl geçerlidir. Bu süre tamamlandığında yeniden belgelendirme yapılması için başvuruda bulunulmalıdır. Belgenin yürürlükte olduğu 3 yıl boyunca kuruluşa, belgelendirme kuruluşu tarafından bir çok kez izleme ziyareti gerçekleştirilir. İzleme faaliyetleri, denetçiler tarafından sistemin güncelliğinin korunduğunun, uygulanan değişikliklerin bilgi güvenliği amacı ile orantılı uygun iyileştirmeleri gerçekleştirdiğinin kontrolüdür.

2.12.1.Belgelendirme Kontrolleri

ISO/IEC 27001 BGYS belgelendirme kontrolü ve diğer işlemlerinin ne şekilde gerçekleştirileceği, hangi kurallara göre uygulanacağı European Accreditation Kurumu'nun 7/03 nolu klavuzunda anlatılmaktadır. Bu klavuza göre yapılacak denetim kuruluş yerleşimlerinde iki aşamalı olarak uygulanmalıdır.

2.12.1.1.Birinci aşama denetim

Belgelendirme sürecinin ilk aşamasında kuruluşun güvenlik politika ve hedefleri kapsamındaki BGYS'nin anlaşılması ve standardın üzerine inşa edileceği Risk Yönetim Yaklaşımı'nın ortaya koyulması sağlanacaktır. Bu aşamada BGYS tasarımı ve gerçekleştirilmesi ile ilgili tüm belgeler için gözden geçirme süreci icra edilir ve diğer aşama için zemin hazırlanır.

Bu aşama sonuçlarını içeren yazılı raporda, sistemin durumu ve bulgularından bahsedilmekte, ikinci aşama için hangi denetçilerin görev alacağı açıklanmakta ve ikinci aşamada istenen ilave bilgi, belge ve kayıtlar belirtilmektedir.

2.12.2.2.İkinci aşama denetim

İkinci aşama BGYS içerik kontrolünün yapıldığı ana ve nihai denetimdir. Burada tüm BGYS tasarımı ve faaliyetleri etraflıca incelenir. Öncelikle Kuruluş Bilgi Güvenliği Yönetim Sistemi'nin bilgi güvenliği hedeflerine uygun olduğunu, ISO/IEC 27001 Standardı'nda geçen gereksinimlerin tamamını karşıladığını ve kendi hedef, politika ve prosedürlerine göre hareket ettiğinin kontrolünü yapmaktadır. Buna göre sırasıyla;

a) Risklerle ilgili bilgi güvenliğinin belirlenmesi ve BGYS'nin nihai tasarımı

b) Kuruluşun Risk Belirleme Yaklaşımı'nın tanımlanması

c) Risklerin tanımlanması

d) Risklerin analiz edilmesi ve değerlendirilmesi

e) Risklerin ortadan kaldırılması seçeneklerinin tanımlanması

f) Risklerin ortadan kaldırılması için kontrol hedeflerinin ve kontrol tedbirlerinin seçimi

g) Bir Uygulanabilirlik Belgesi'nin hazırlanması

h) Bu süreçten elde edilen hedeflerin kontrol edilmesi,

i) Hedefler göz önünde bulundurularak performansın izlenmesi, ölçülmesi, rapor edilmesi ve gözden geçirilmesi.

j) BGYS'nin iyileştirilmesi,

k) Bilgi güvenliği politikası için yönetimin sorumluluğu uygulamalarının istenen şekilde yapılması işlemleri gerçekleştirilmektedir.

Yapılan tüm denetim işlemlerinde belgelendirme kuruluşu, belgelendirme yapılacak kuruluştan standarta göre hariç tutulan hususları ve risk kabul ölçütünün ne şekilde oluşturulduğunu, gerekçeleri ile belgelendirilmesini istemektedir. En son olarak ise tüm BGYS çalışma ve uygulamaları yazıya dökülmüş bir yönetim sisteminin sunumu kontrol edilmektedir.

2.12.2.Belgelendirme

Şekil 5.ISO/IEC 27001 BGYS Sertifika Örneği

ISO/IEC 27001

SERTİFİKA

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

SEMBOLİK BİLİŞİM LİMİTED ŞTİ.

Ankara Cad.Doğu Mah.No:290 Pendik / İSTANBUL

Bilgi Güvenliği Yönetim Sistemi tetkik edilmiş ve aşağıda standardın gerekliliklerine uygunluğu tespit edilmiştir.

ISO/IEC 27001

Bilgi Güvenliği Yönetim Sistemi Sertifikası Aşağıdaki Kapsam İçin Geçerlidir

Sembolik Bilişim Limited Şirketi'nin tüm bölümlerini kapsamaktadır.

Sertifika Yayın Tarihi : 25.05.2010

Sertifika Geçerlilik Tarihi :25.05.2011

Yeniden Değerlendirme Tarihi : 25.03.2013

Sertifikasyon Numarası : TR-Q-2010-6698-3456-01

Onay :

AMBLEM **(BELGELENDİRME KURULUŞU)**	**AMBLEM** **(AKREDİTASYON KURULUŞU)**

Belgelendirme kuruluşu tüm kontrollerini tamamladıktan sonra denetlenen kuruluşa denetim sonuçlarını ihtiva eden bir rapor sunar. Bu rapor, denetim sonunda verilebileceği gibi denetim toplantıları sırasında verilen sözlü ya da yazılı rapor şeklinde de olabilir. Bu raporlarda kuruluşun standarttaki gereksinimleri karşılama seviyesi belirtilmekte, denetimcinin bulguları, uyumsuzlukları içermektedir.

Bir kuruluşa ISO/IEC 27001 BGYS Belgesi verilip verilmeyeceği belgelendirme kuruluşu tarafından çıkan bu rapora göre belirlenir. Belgelendirme kararını verecek heyetin denetim aşamalarında görev almamış olması aranmaktadır. Sonucun olumlu olması halinde belgelendirme kuruluşu ve akreditasyon kuruluşlarının amblemleri ile damgalı bir BGYS belgesi tanzim edilerek belgelendirilen kuruluşa teslim edilir. Bu belgede ayrıca belgelendirmenin kapsamı, yürürlüğe gireceği tarih de belirtilmektedir.

SONUÇ VE ÖNERİLER

Kurumlar için hayati öneme sahip, bir anlamda fark yaratma unsuru olan bilginin, gizlilik, bütünlük ve erişebilirliği ilkelerinin sağlanarak mevcut süreçlerin güvenliğinin oluşturulması bir seçenek değil, önemli bir zorunluluk halini almıştır. Bu zorunluluğu yerine getirmek, tüm personel üzerinde bilgi güvenliği bilincinin oluşturulması ile başlamakta ve piyasada var olma amacı olan mal ya da hizmet üretiminin bütün aşamalarında bilgi güvenliğinin sistematik bir şekilde planlanarak uygulanması ile gerçekleşmektedir.

Günümüzde kurumları bünyesinde bilgi güvenliğini sağlamak isteyen yöneticiler için tüm dünya çapında kabul görmüş en önemli kaynak, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'dir. Ayrıca devletler bazında da kabul gören ve ticari şirketlerin birçok konuda faaliyet gösterebilmeleri için kurulup belgelendirilmiş olmaları istenen standart, yine BGYS'dir. Bu standart ile kurumlar;

-Bilgi varlıklarının farkına varma: Kuruluş hangi bilgi varlıklarının olduğunu ve bunların değerlerini anlar.

-Sahip olduğu varlıkları koruyabilme: Kuracağı kontroller ile koruma metotlarını belirler, uygulayarak korur.

-İş sürekliliği: Uzun yıllar boyunca işini garanti eder. Ayrıca bir felaket halinde, işe devam etme yeterliliğine sahip olur.

-İlgili taraflar ile barış halinde olma: Başta tedarikçileri olmak üzere, bilgileri korunacağından ilgili tarafların güvenini kazanır.

-Bilgiyi bir sistem sayesinde koruyarak tesadüfe yer bırakmaz.

-Çalışanlarının motivasyonu artar.

-Yasal takipler önlenir.

-Yüksek prestij sağlar.

Bilgi Güvenliği Yönetim Sistemi, ilgili aşamalarının kurulması ve dikkat edilmesi gereken hususları ile birlikte sürekli yaşayan bir projedir. Bu projenin başarıyla uygulanıp işletilmesi, Bilgi İşlem Merkezleri'nden hareketle BT'ni azami şekilde

kullanan tüm kurum/kuruluşlarda uygulanması günümüzün rekabetçi global dünyasında gün geçtikçe zorunluluk halini almıştır. Sistemin istenilen başarıya ulaşabilmesi için gerekli etkenler;

-Yönetimin desteği ve bağlılığı görünür olmalıdır.

-Güvenlik Politikaları, iş hedefini yansıtmalıdır.

-Uygulama yaklaşımı ile şirket kültürü arasında tutarlılık sağlanmalıdır.

-Güvenlik gereksinimleri, risk değerlendirme ve risk yönetimi iyi anlaşılmalı ve anlatılmalıdır.

-Bilgi güvenliği politikası ve standartları ile yapılan tüm çalışmalar, personel ve iletişimde bulunulan tüm taraflarla paylaşılmalıdır.

-Eğitime önem verilmeli ve tabana yayılarak farkındalık, sahiplenme duyguları yaratılmalıdır.

-Kapsamlı ve dengeli bir ölçüm sistemi oluşturulup, uygulanmalıdır.

BGYS en başta bir yönetim ve kaynak meselesidir. Kuruluşta öncelikle yönetici kademesindeki kişilerin bilgi güvenliği farkındalıklarının oluşturulması gerekmektedir. Burada Bilgi İşlem Merkezi sorumlularına iş düşmektedir. Bilgi güvenliğinin önemi ve kazandırdıkları detaylı bir şekilde anlatılarak yönetim desteğinin sağlanması bir zarurettir. Yönetim desteğinin sağlanması hem çalışanlar üzerinde yaratılmaya çalışılacak etkiyi arttıracak hem de BGYS süreçlerinde ihtiyaç duyulacak kaynakların sağlanmasını kolaylaştırılacaktır.

BGYS, bu konuda uzman derecesinde bilgi sahibi profesyonellerin işidir. Sistemin kurulup, yönetilmesi aşamalarında dışarıdan destek alınsa dahi, kendi çalışanları içinden konu hakkında yüksek bilgi düzeyine erişmiş ve süreçlere hakim bir ekibin varlığı kaçınılmazdır. Kuruluşlar bu ekibi kurabilmek için öncelikle eğitim ve farkındalık çalışmalarına önem vermeli ve oluşturulacak BGYS ekibinden başlayarak tabana yayılacak şekilde verilecek azami katılım sağlamalıdır. Çünkü bilgi güvenliği en başta farkındalık meselesidir. Ekibin oluşturulması ve çalışanlarda farkındalık yaratılması işlemlerinin başarıyla tamamlanması sonraki süreçlerin uygulanmasını kolaylaşacaktır.

Bilgi Güvenliği Yönetim Sistemi kurulumu ve yönetiminin püf noktalarından biri teknolojinin sıkı takibidir. Bilgi güvenliği konusunda her geçen gün açıklar ve bunlara karşı teknik ve yönetimsel kontroller gerçekleştirilmektedir. Burada önleyici faaliyetlerin önemi ve bunları hayata geçirmek için bilgi güvenliği portal ve gruplarına katılım hususunun gerekliliği ortaya çıkmaktadır. Dünyada ve Türkiye'de birçok bilgi güvenliği grubu bulunmakta ve bunlara katılım her geçen gün artmaktadır. Her Bilgi İşlem Merkezi personelinin bu gruplara katılması ve bilgi güvenliği konusunda güncel olayları takip ederek önlemleri gerçekleştirmesi bir zorunluluktur.

BGYS bir Risk Yönetim Süreci'dir. Bu Risk Yönetim Süreci'nin varlıkların belirlenmesi adlı ilk aşamasından kontrollerin etkinliklerinin ölçülüp, iyileştirmesi aşamasına kadar üzerinde önemle durulması ve en ufak bir açığın bırakılmaması başarı için vazgeçilmez koşuldur. Bu koşulu sağlayabilmek için sistematik bakış açısı ve süreçlerin en ince ayrıntısına kadar dokümante edilip, uygulanması gerekmektedir. Uygulanacak kontroller BGYS Standardı'nın maddelerinden yola çıkılarak kuruluşların kendi bünyelerine göre özelleştirilmelidir. Her detay üzerinde durulmalı ve seçilmeyen kontroller, nedenleri ile birlikte daha sonraki çalışmalara bilgi olması sebebiyle kaydedilmelidir.

Tüm BGYS çalışmaları bilgi varlıklarına yönelik olduğundan, sistemin kurulup işletilmesi aşamalarının ilk muhatabı bilgilerin işlendiği, depolandığı ve saklandığı ortamları yöneten Bilgi İşlem Merkezleri'dir. Bu yüzden standardın pratiğini oluşturan yönetimsel ve teknik uygulamaların büyük bir çoğunluğu bu departman/kuruluşlarda gerçekleştirilmektedir. Bu yüzden tez çalışmasında Bilgi İşlem Merkezlerin'de ISO/IEC 27001 BGYS Standardının ne şekilde kurulacağı ve hangi adımlar uygulanacağı sorusunun cevabı aranarak gerekli aşamalar anlatılmıştır. Tüm süreçler örnekler verilerek detaylandırılmış, çalışmayı kaynak alacak Bilgi İşlem Yöneticileri'nin rehber olacak şekilde hazırlanmıştır.

Belgelendirilmiş olsun ya da olmasın Bilgi Güvenliği Yönetim Sistemi'nden önce süreçlerin güvenilirliğinin ne şekilde sağlanacağı ve yaşanılacak kötü durumlara karşı ne gibi önlemler alınacağı sorularının cevabını bilmeyen ya da kendi aralarında cevaplayan kurum içi ya da müstakil çalışan Bilgi İşlem Merkezleri, standardın getirdiği sistematik bakış açısı ve olayları gelişebilecek senaryolara göre tek tek inceleme

kabiliyeti ile bilgi güvenliği konusunda daha bilinçli, eğitimli ve soğukkanlı olacaktır. Bu bilinç,eğitim ve soğukkanlılık felaket durumlarında dahi bilgi varlıkları kapsamında kurumu en az zararla kurtaracak kabiliyeti kazandıracaktır.

Bunlardan hareketle Bilişim Teknolojileri piyasasında faaliyet gösteren ya da bünyesinde bu hizmetleri kullanan kurum ve kuruluşlar, kendileri için büyük önem arz eden bilginin ve dolayısıyla süreçlerinin güvenliğini sağlamak amacıyla konuya profesyonel bir bakış açısı getiren BGYS'ni benimsemeli ve tüm personeline bilgi güvenliği bilincini oluşturmalıdır. Bu kurumlarda, Bilgi Güvenliği Yönetim Sistemi'nin sonsuz PUKÖ döngüsü içerisinde sürekli yaşayacak yapıda kurulup, sistematik bir şekilde yönetilmesinden sonra faaliyet konularındaki tüm işlemlerinin hissedilebilir derecede daha güvenli olduğu ve daha sağlam temeller üzerine oturduğu görülecektir.

KAYNAKLAR

AKGÜL, Mustafa (2010), "Türkiye'nin İnternet'le Savaşı: Dünya Önderliği mi Yoksa Devekuşulu Hukuk Faciası mı?", *Elektrik Mühendisleri Odası (EMO) 3. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu Bildirgesi*, Ankara

ALPAR, Cengiz (2009), "Kalite Yolculuğu: Bilgi Güvenliği Yönetim Sistemi ISO 27001", *CIO (Chief Information Officer) Club Dergisi*, Yıl 1, Sayı 1, Mart, s.27-30.

ALTUN, Ayla (2009), "5651 Sayılı Kanun: İnternet Kanunu", http://cisn.odtu.edu.tr/2009-16/5651.php, 22.04.2010

ARNASON, Sigurjon Thor ve Keith D. Willet (2008), *How To Achieve 27001 Certification: An Example of Applied Compliance Management*, Auerbach Publications, Boca Raton/FL-ABD

ATSEC (2007), "ISMS Implementation Guide", http://www.atsec.com/downloads/documents/ISMS-Implementation-Guide-and-Examples.pdf, 22.03.2010

Başbakanlık, Personel ve Prensipler Genel Müdürlüğü, (2003), *Bilgi Sistem ve Ağları İçin Güvenlik Kültürü*, Ankara

BESTEL, Burak (2008), "Bilgi Güvenliğinde Risk Analizi; Nedir? Nasıl Yapılır, Sorunlar Nelerdir?", www.navigator.com.tr/download/BGRiskAnalizi.pdf, 10.02.2010

BSI (British Standart Institute), (2007), "*ISO/IEC 27002 Information Technology, Security Technics, Code of Practice for Information Security Management International Standart*", LONDON-INGILTERE

CQR Consulting (2010), "ISMS, How to Manage Security", http://www.cqrconsulting.com/media/Whitepapers/ISMS%20how%20to%20manage%20information%20security.pdf, 07.04.2010

ÇETİNKAYA, Mehtap (2008), "Kurumlarda Bilgi Güvenliği Yönetim Sistemi'nin Uygulanması", *Çanakkale Onsekiz Mart Üniversitesi Akademik Bilişim 2008 Raporu*, s.511-516.

DİNÇKAN, Ali (2008), "Merkezi Kayıt Yönetimi ve Denetim Amaçlı Kullanımı", *TUBİTAK-UEKAE Bilgi Teknolojileri Güvenlik Konferansı*, Kocaeli

DİNÇKAN, Ali (2008), Veri Yedekleme Klavuzu", http://www.bilgiguvenligi.gov.tr/dokuman-yukle/bgys/uekae-bgys-0010-veri-yedekleme-kilavuzu/download.html, 26.03.2008

DİNÇKAN, Ali (2008), "İş Sürekliliği Yönetim Sistemi Kurulum Klavuzu", http://www.bilgiguvenligi.gov.tr/dokuman-yukle/bgys/uekae-bgys-0009-is-surekliligi-yonetim-sistemi-kurulum-kilavuzu/download.html, 20.10.2008

DOĞANTİMUR, Fatma (2009), *ISO 27001 Standardı Çerçevesinde Kurumsal Bilgi Güvenliği*, Mesleki Yeterlilik Tezi, T.C. Maliye Bakanlığı Strateji Geliştirme Daire Başkanlığı

EĞRİ, Fırat (2008), "Maliye Bakanlığı Muhasebat Genel Müdürlüğü-BGYS", http://www.muhasebat.gov.tr/twinning/toplantilar/KimlikYonBilgiGuv/docs/BGYS_MUH.pdf, 03.05.2010

EROL, Berrin (2007), "Turkcell'de Bilgi Güvenliği Yolculuğu", *TUBITAK-UEKAE Bilgi Teknolojileri Güvenlik Konferansı*, Kocaeli

ESKİYÖRÜK, Doğan (2008), "BGYS Risk Yönetim Süreci Klavuzu", http://www.bilgiguvenligi.gov.tr/dokuman-yukle/bgys/uekae-bgys0004-bgys-risk-yonetim-sureci-kilavuzu/download.html , 26.03.2008

ESKİYÖRÜK, Doğan (2008), "Bilgi Sistemleri Kabul Edilebilir Kullanım Politikası Oluşturma Klavuzu", http://www.bilgiguvenligi.gov.tr/dokuman-yukle/bgys/uekae-bgys0007-bilgi-sistemleri-kabul-edilebilir-kullanim-politikasi-olusturma-kilavuzu/download.html, 18.04.2008

Gelişim Yönetim Sistemleri A.Ş. (2009), "Bilgi Güvenliği Yönetim Sistemi Nedir?", http://bgys.org/yazlar/35-iso27001/50-iso27001nedir, 30.07.2009

Gelişim Yönetim Sistemleri A.Ş. (2009), "Elektronik Haberleşme Yönetmeliği ve ISO27001:2005'e Uyum", http://bgys.org/yazlar/35-iso27001/75-elektronik haberlesme 01.08.2009

Gelişim Yönetim Sistemleri A.Ş. (2009), "Kapasite Yönetimi", http://bgys.org/yazlar/36-iso20000-itil/77-capacity-management, 10.08.2009

HENNING, David (2009), "Tackling ISO 27001: A Project to Build an ISMS", http://www.sans.org/reading_room/whitepapers/leadership/tackling-iso-27001-project-build-isms_33169, 29.04.2010

HINSON, Garry (2007), "Organization of Information Security", http://www.iso27001security.com/ISO27k_Organization_of_information_security.rtf, 03.05.2010

HINSON, Garry (2007), "Information Security Policy: E-Mail Security", http://www.iso27001security.com/ISO27k_model_policy_on_email_security.rtf, 03.05.2010

HINSON, Garry (2007), "Laptop Security Policy", http://www.iso27001security.com/ISO27k_model_policy_on_laptop_security.rtf, 03.05.2010

HUMPHREYS, Edward (2007), *Implementing the ISO/IEC 27001 Information Security Management System Standart*, Artech House INC, MA/ABD

HUMPHREYS, Edward (2010), "Information Security Risk Management, Handbook for ISO/IEC 27001", http://www.bsigroup.com/sectorsandservices/Forms/BIP-0076-Sample-chapter-form/, 29.04.2010

HUMPHREYS, Ted ve Angelika Plate (2005), Guideliness on Requirements and Preperation for ISMS Certification Based on ISO/IEC 27001, British Standart Institute, LONDON/INGILTERE

HUMPHREYS, Ted (2006), "ISO ISMS Standarts ", *ETSI Security Workshop*, NICE-FRANSA

İRAZ, Fırat (2003), "Organizasyonlarda Karar Verme ve İletişim Sürecinin Etkinliği Bakımından Bilgi Teknolojilerinin Rolü", http://www.sosyalbil.selcuk.edu.tr/sosmak/makaleler/R%C4%B1fat%20%C4%B0RAZ/BT%20ve%20Karar%20Verme.pdf, 08.01.2010

JOSANG, Audun, B. Alfayyadh, T. Grandison, M. Alzomai, J. Macnamara (2007), "Security Usability Principles for Vulnerability Analysis and Risk Assesment" http://198.4.83.38/cs/projects/iis/hdb/Publications/papers/ACSAC2007.pdf, 13.05.2010

KAHRAMAN, Erol (2008), "Kamu Sertifikasyon Merkezi Bilgi Güvenliği Öyküsü", *TUBITAK-UEKEA Bilgi Teknolojileri Güvenlik Konferansı*, Ankara

KAHRAMAN, Sunay (2006), *Yönetimde Bilgi Güvenlik Sisteminin Yapısı İşleyişi ve ASELSAN A.Ş.'de Uygulaması*, Basılmamış Yüksek Lisans Tezi, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü

KAMAT, Mohan (2010), "The User Awareness Training of ISMS", www.iso27001security.com/ISO27k_Awareness_presentation.ppt, 13.05.2010

KARABACAK, Bilge, Sevgi Özkan (2010), "Bilgi Güvenliği Yönetim Sistemi İçin Süreç Tabanlı Risk Analizi", *Elektrik Mühendisleri Odası (EMO) 3. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu Bildirgesi*, Ankara

KILIÇ, Mehtap, Orhan Gökçöl (2010), "Türkiye'deki İşletmelerin Bilgi Güvenliği Yönetim Sistemi Altyapısının Değerlendirilmesi", *Elektrik Mühendisleri Odası (EMO) 3. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu Bildirgesi*, Ankara

KOÇ, Fatih (2008), "BGYS Varlık Envanteri Oluşturma ve Sınıflandırma Klavuzu", http://www.bilgiguvenligi.gov.tr/dokuman-yukle/bgys/uekae-bgys0003-varlik-envanteri-olusturma-kilavuzu/download.html, 21.05.2008

MATARACIOĞLU, Tolga, Ünal Tatar (2009), "Neden BGYS?", http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/neden-bgys.html, 04.08.2009

MATARACIOĞLU, Tolga, Ünal Tatar (2009), "Örnek Varlık Envanteri Oluşturma Metodolojisi", http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/ornek-varlik-envanteri-olusturma-metodolojisi.html, 15.09.2009

MEDENİ, İhsan, Tunç Durmuş Medeni (2008), "Bilgi Güvenliği Yönetim Sistemi ve ISO 27001", *Türkiye Bilişim Derneği Bilişim'08 Kurultayı Bildirisi*, Ankara

NAZLI, Mikail (2009), "Bilgi Güvenliği Açısından Haberleşme ve İşletim Yönetimi", http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/bilgi-guvenligi-acisindan-haberlesme-ve-isletim-yonetimi.html, 09.09.2009

NISAR, Hamid (2007), "Information Security Risk Analysis Spreadsheet", http://www.iso27001security.com/ISO27k_RA_spreadsheet_version_2.xls, 03.05.2010

NORDIN, Inger (2003), "Implementation of an ISMS: A Prosses Approach", http://www.ivpk.lt/dokumentai/prezentacijos/09%20Information%20Security%20Management%20System%20-%20Implementatio.ppt, 06.05.2010

OTTEKİN, Fikret (2008), TS ISO/IEC 27001 Denetim Listesi", http://www.bilgiguvenligi.gov.tr/dokuman-yukle/bgys/uekae-bgys0013-iso-iec-27001-denetim-listesi/download.html, 27.03.2008

OTTEKİN, Fikret (2008), "Çok Katmanlı ISO 27001 Süreci", http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/cok-katmanli-iso-27001-sureci.html, 06.05.2010

ÖNEL, Dinçer (2007), "Erişim Kontrol Politikası Oluşturma Klavuzu", http://www.bilgiguvenligi.gov.tr/dokuman-yukle/bgys/uekae-bgys-0006-erisim-kontrol-politikasi-olusturma-kilavuzu/download.html, 26.03.2008

ÖNEL, Dinçer (2008), "Bilgi Güvenliği Bilinçlendirme Süreci Oluşturma Klavuzu", http://www.bilgiguvenligi.gov.tr/dokuman-yukle/bgys/uekae-bgys-0008-bilgi-guvenligi-bilinclendirme-sureci-olusturma-kilavuzu/download.html, 26.03.2008

ÖNEL, Dinçer, Ali Dinçkan (2007), "Bilgi Güvenliği Yönetim Sistemi Kurulumu", http://www.bilgiguvenligi.gov.tr/dokuman-yukle/bgys/uekae-bgys-0001-bilgi-guvenligi-yonetim-sistemi-kurulumu/download.html, 26.03.2008

ÖZTÜRK, Günce (2008), "Bilgi Güvenliği Politikası Oluşturma Klavuzu", http://www.bilgiguvenligi.gov.tr/dokuman-yukle/bgys/uekae-bgys-0005-bilgi-guvenligi-politikasi-olusturma-kilavuzu/download.html, 28.03.2008

PARK, Cheol-Soon, S. Jang ve Y. Park (2010), "A Study of Effect of Information Security Management System (ISMS) Certification on Organization Performance", *IJCSNS International Journal of Computer Science and Network Security*, VOL.10, No.3, March 2010, s.10-21.

PERENDİ, Ünal (2008), "BGYS Kapsamı Belirleme Klavuzu", http://www.bilgiguvenligi.gov.tr/dokuman-yukle/bgys/uekae-bgys0002-bgys-kapsami-belirleme-kilavuzu/download.html, 26.03.2008

REGALADO, Richard (2007), "ISO 27K Statement of Applicability Sample", http://www.iso27001security.com/ISO27k_SOA_sample.xls, 01.03.2010

SALAH, Osama, Gary Hinson (2009), "Mandatory Information Security Management System Documents Required for ISO/IEC 27001 Certification", http://www.iso27001security.com/ISO27k_mandatory_ISMS_documents.rtf, 01.03.2010

SAYARI, Neşe (2007), "BGYS Çözümleri", *Bilgi Güvenliği ve Yazılım Kalitesi Sempozyumu Bildirisi*, Ankara

TUĞLULAR, Tuğkan (2003), "Üniversitelerde Bilgi Güvenliği Politikaları", *Ulaknet Sistem Yönetimi Konferansı Bildirisi*, Ankara

TBD (Türkiye Bilişim Derneği), (2006), "*Bilişim Sistemleri Güvenliği El Kitabı*", Türkiye Bilişim Derneği Yayınları, Ankara

TBD (Türkiye Bilişim Derneği), (2008), "*Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin Uygulanmasında ISO/IEC 27001:2005 Standardı*", 2008

TSE (Türk Standartları Enstitüsü), (2006), "*TS ISO/IEC 27001 Bilgi Teknolojisi, Güvenlik Teknikleri, Bilgi Güvenliği Yönetim Sistemleri, Gereksinimler Standardı*", Ankara

TSE (Türk Standartları Enstitüsü), (2008), "Sistem Belgelendirme Başvuru Formu" http://www.tse.org.tr/Turkish/KaliteYonetimi/Ek12-TSESistemBelgBasvuruFormu.doc

TÜRKAK (Türk Akreditasyon Kurumu), (2009), "Sistem Belgelendirme Kuruluşları" http://www.turkak.org.tr/akredite/sistem.htm

VURAL, Yılmaz, Şeref Sağıroğlu (2008), "Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme", *Gazi Üniversitesi Müh. Mim. Fak. Der.*, Cilt 23, No 2, s.507-522,

Wikipedia (2009), "Gap Analysis", http://en.wikipedia.org/wiki/Gap_analysis, 07.01.2010

YILDIZ, Bünyamin (2007), *Bilgi Güvenliği ve E-Devlet Kapsamında Kamu Kurumlarında Bilgi Güvenliği Yönetim Standartlarının Uygulanması*, Basılmamış Yüksek Lisans Tezi, Gebze Yüksek Teknoloji Enstitüsü Sosyal Bilimler Enstitüsü

Kanunlar

1) 15/04/2004 Tarih ve 5070 Sayılı Elektronik İmza Kanunu

2) 26/09/2004 Tarih ve 5237 Sayılı Türk Ceza Kanunu

3) 04/05/2007 Tarih ve 5156 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

4) 05/11/2008 Tarih ve 5809 Sayılı Elektronik Haberleşme Kanunu

Yönetmelikler

1) İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik

2) İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik

3) Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik

4) Elektronik Haberleşme Güvenliği Yönetmeliği

ÖZGEÇMİŞ

Hakan METE, 21.03.1984 tarihinde İstanbul'da doğdu. Çapa Gazi İlköğretim Okulu'nda başladığı İlk ve orta öğretimini 1998 yılında Çapa Atatürk İlköğretim Okulu'nda tamamladı. Lise öğrenimi için Deniz Astsubay Hazırlama Okulu'nu kazanan Hakan METE 3 yıllık öğrenimi tamamladıktan sonra Bilgi Sistemleri eğitimi almak amacıyla 1 yıl süren Muhabere Elektronik Bilgi Sistemleri Okulu'nu 2002 yılında tamamlayarak mezun oldu. Yine 2002 yılında Anadolu Üniversitesi İktisat Fakültesi Kamu Yönetimi bölümünde başladığı lisans öğrenimini 2006 yılında tamamladı. 2008 yılında Sakarya Üniversitesi Çalışma Ekonomisi ve Endüstriyel İlişkiler Anabilim dalı İnsan Kaynakları Yönetimi ve Endüstriyel İlişkiler bölümüne girmeye hak kazanan Hakan METE, evli olup halen Deniz Kuvvetleri Komutanlığı bünyesinde Bilgi Sistem Uzmanı Astsubay olarak görev yapmaktadır.