

T.C.

GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ

SOSYAL BİLİMLER ENSTİTÜSÜ

**BİLGİ GÜVENLİĞİ KAVRAMI VE BİLGİ
GÜVENLİĞİ YÖNETİM SİSTEMLERİ İLE
ŞİRKET PERFORMANSI İLİŞKİSİNE DAİR
BİR UYGULAMA**

KEREM ASLANDAĞ

YÜKSEK LİSANS

STRATEJİ ANABİLİM DALI

DANIŞMANI

PROF. DR. HALİT KESKİN

GEBZE

2010

T.C.

GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ

SOSYAL BİLİMLER ENSTİTÜSÜ

**BİLGİ GÜVENLİĞİ KAVRAMI VE BİLGİ
GÜVENLİĞİ YÖNETİM SİSTEMLERİ İLE
ŞİRKET PERFORMANSI İLİŞKİSİNE DAİR
BİR UYGULAMA**

KEREM ASLANDAĞ

YÜKSEK LİSANS

STRATEJİ ANABİLİM DALI

DANIŞMANI

PROF. DR. HALİT KESKİN

GEBZE

2010



YÜKSEK LİSANS TEZİ JÜRİ ONAY SAYFASI

G.Y.T.E. Sosyal Bilimler Enstitüsü Yönetim Kurulu'nun tarih ve sayılı kararıyla oluşturulan jüri tarafından tarihinde tez savunma sınavı yapılan'ın tez çalışması Anabilim Dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir.

JÜRİ

ÜYE

(TEZ DANIŞMANI) :

ÜYE :

ÜYE :

ONAY

G.Y.T.E. Sosyal Bilimler Enstitüsü Yönetim Kurulu'nun/...../20... tarih ve/..... sayılı kararı.

İMZA/MÜHÜR

ÖZET

TEZİN BAŞLIĞI: Bilgi Güvenliği Kavramı ve Bilgi Güvenliği Yönetim Sistemleri ile Şirket Performansı İlişkisine Dair Bir Uygulama

YAZAR ADI: Kerem ASLANDAĞ

Son 20 yılda teknolojinin ilerlemesi ve teknolojiye dayalı sistemlerin gelişmesiyle bilgi teknolojileri çok önemli bir noktaya geldi. Çetin ekonomik şartlar altında bilginin, firmanın büyümesi ve varlığını devam ettirmesi için çok önemli bir varlık olması, korunmasını gerektirdi ve Bilgi Güvenliği Yönetim Sistemi denilen bir kavram ortaya çıktı.

Eskiden bilgi güvenliği ile ilgili kavramların BT dışından olan insanlar tarafından zor algılanacağı yönünde bir yargı vardı. Bu yüzden BT’de çalışanlara teknik olmayan terimlerle diğer insanlara anlatmaları gerektiği söylenirdi. Şu anda biliyoruz ki bilgi güvenliği eğitimi sadece belli bir gruptaki insanlara değil örgütteki/kurumdaki bütün çalışanlara verilmelidir. Bilgi Güvenliğinin örgüt/kurum kültürü haline gelmesi ve organizasyonel hafızaya kazandırılması, tüm örgüt/kurum çalışanlarının firmanın savunma mekanizmasında önemli bir rol oynayacağı anlamına gelecektir.

Bu tez çalışması ile bir örgütte/kurumda uygulanan Bilgi Güvenliği Yönetim Sisteminin, örgütün/kurumun performansına nasıl etki ettiği tespit edilmeye çalışılmıştır. Örgütte/kurumda anket yöntemi ile Bilgi Güvenliği unsurları olan gizlilik, bütünlük, erişilebilirlik kavramlarının şirketin çalışan memnuniyetine, müşteri memnuniyetine ve süreç yapısına nasıl etki ettiği incelenmiştir.

Anahtar Kelimeler: Bilgi Güvenliği, Bilgi Güvenliği Kavramı, Bilgi Güvenliği Olgunluk Seviyesi, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 17799, COBIT, ITIL, BGYS

SUMMARY

THESIS TITLE: The Concept of Information Security and the relationship between Information Security Management System and Company Performance

AUTHOR NAME: Kerem ASLANDAĞ

Technology was much improved in the last twenty years. Thus information technology with development of technology-based systems has come to a crucial point. Information is a crucial asset for companies to develop and grow that must protect your information under harsh economic conditions. In this way Information Security Management System is a concept that emerged.

Previously, we know that difficult to understand concepts related to information security by people outside of IT. So, we think need to the people working in information technology explain technical issues more simple for non-technical people. We know now that information security training should be given not only a certain group of people, should be given to all employees in the organization / institution. Information security has become the organizational culture and organizational memory to gain the whole organization, the firm's employees will play an important role in defense mechanism means.

In this thesis, are explained that applied for Information Security Management System that affect the organization's performance in an organization. How the components of information security as confidentiality, integrity, accessibility concepts affects to employee satisfaction, customer satisfaction and process structure has been investigated with this survey method.

Keywords: Information Security, Information Security Concept, Maturity Level of Information Security, ISO / IEC 27001, ISO / IEC 27002, ISO / IEC 17799, COBIT, ITIL, ISMS

TEŞEKKÜRLER

Yüksek Lisans çalışmam boyunca benden desteğini esirgemeyen aileme, çalışma arkadaşlarıma, anket çalışmasının tamamlanabilmesi için değerli vaktini ayırarak anketi dolduran herkese yardımları için çok teşekkür ederim.

Tez çalışmam süresinde bana yol gösteren ve anket sonuçlarının analizi konusunda destek olan danışman hocam Prof. Dr. Halit Keskin'e ve Dr. Ayşe Günsel başta olmak üzere derslerini aldığım tüm hocalarıma ayrıca teşekkür ederim.

İÇİNDEKİLER DİZİNİ

ÖZET	iv
SUMMARY	v
TEŞEKKÜRLER	vi
İÇİNDEKİLER DİZİNİ	vii
SİMGELER VE KISALTMALAR DİZİNİ	x
ŞEKİLLER DİZİNİ	xi
TABLolar DİZİNİ	12
1. GİRİŞ	13
2. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ	16
2.1 Bilgi Güvenliği Kavramı	16
2.2 Bilgi Güvenliğinin Unsurları	18
2.2.1 Gizlilik (Confidentiality)	18
2.2.2 Bütünlük (Integrity)	19
2.2.3 Erişilebilirlik/Kullanılabilirlik (Availability)	20
2.3 Bilgi Güvenliği Yönetim Sistemi Standardı	21
2.3.1 4 BGYS'yi Kurmak	21
2.3.2 4.2 BGYS'nin Kurulması ve Yönetilmesi	21
2.3.3 4.3 Dökümantasyon Gereksinimleri	25
2.3.4 5 Yönetimin Bağlılığı	26
2.3.5 6 İç BGYS Denetimi	26
2.3.6 7 Yönetimin Gözden Geçirmesi	27
2.3.7 8 BGYS'yi İyileştirme	27
2.3.8 EK-A KONTROLLERİ	28
2.4 Bilgi Güvenliği Standardının Tarihçesi	32
2.5 Risk Yönetimi	34
2.5.1 Risk İşleme Yöntemleri	35

2.5.2	Kontrollerin Uygulanması	35
2.5.3	Kontrollerin Uygulanmasında İzlenecek Yaklaşım	36
2.5.4	Risklerin Önceliklendirilmesi	36
2.5.5	Uygun Kontrollerin Değerlendirilmesi	36
2.5.6	Kontrollerin Seçilmesi	36
2.5.7	Sorumluların Atanması	36
2.5.8	Kontrol İşleme/Uygulama Planının Hazırlanması	37
2.5.9	Seçilen Kontrolün Uygulanması	37
2.5.10	Artık Risk Kavramı	37
2.5.11	Risklerin izlenmesi, yeniden değerlendirilmesi ve gözden geçirilmesi	37
2.6	BGYS Kurulum Süreci	38
2.6.1	BGYS Sertifikasyon Süreci ve Bilgi Güvenliği Altyapısının Sağlanması	39
2.7	ITIL, COBIT ve ISO/IEC 27002 Çerçeveslerinin Karşılaştırmaları:	42
2.7.1	ITIL (Information Technology Infrastructure Library)	43
2.7.2	COBIT (Control Objectives for Information and Related Technology)	47
2.7.3	ISO/IEC 27002	52
2.7.4	ITIL ve COBIT ilişkisi	56
2.7.5	COBIT ile ISO/IEC 27001:2005 ilişkisi	56
3.	BGYS, FİRMA PERFORMANSI İLİŞKİSİ	59
3.1	Müşteri Memnuniyeti	61
3.2	Çalışan Memnuniyeti	63
3.3	Örgütsel Bağlılık	65
3.4	Süreç Yaklaşımı	68
3.5	Şirket Performansı	70
3.6	Bilgi Güvenliği Olgunluk Seviyesi	71
3.6.1	Seviye 5 : Stratejik (Strategic)	73

3.6.2	Seviye 4 : Yönetilmiş (Managed)	74
3.6.3	Seviye 3: Operasyonel (Operational)	75
3.6.4	Seviye 2 : Teknik (Technical)	75
3.6.5	Seviye 1 : Fonksiyonel (Functional)	76
3.6.6	Seviye 0 : İhmal Edici (Negligent)	76
3.6.7	Seviye -1 : Engelleyici (Obstructive)	76
3.6.8	Seviye -2 : Kibirli (Arrogant)	77
3.6.9	Seviye -3 : Yıkıcı (Subversive)	77
4.	BİLGİ GÜVENLİĞİ KAVRAMI VE BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ İLE ŞİRKET PERFORMANSI İLİŞKİSİNE DAİR BİR UYGULAMA	78
4.1	Araştırmanın Amacı	78
4.2	Araştırma Kısıtları	78
4.3	Ölçeklerin Oluşturulması	80
4.4	Veri Toplama Süreci	80
4.5	Ölçüm Geçerliliği ve Güvenilirliği	83
4.6	Hipotez Testleri	89
5.	SONUÇ ve ÖNERİLER	92
5.1	Sınırlandırmalar	94
5.2	Öneriler	94
	KAYNAKLAR	95
	ÖZGEÇMİŞ	102
	EK-1 Anket Formu Örneği	103

SİMGELER VE KISALTMALAR DİZİNİ

BG	:Bilgi Güvenliği
BGYS	:Bilgi Güvenliği Yönetim Sistemi
KYS	:Kalite Yönetim Sistemi
ISMS	:Information Security Management System
BT	:Bilgi Teknolojileri
IT	:Information Technologies
BS	:Bilgi Sistemleri
PUKÖ	:Planla – Uygula- Kontrol Et- Önlem Al
UEKAE	:Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
BTK	:Bilgi Teknolojileri ve İletişim Kurumu
ISO	:Uluslararası Standartlar Örgütü
SOX	:Sarbanes Oxley Act
COBIT	:Control Objectives for Information and Related Technology

ŞEKİLLER DİZİNİ

<u>Sekil</u>	<u>Sayfa</u>
2.1 BGYS risk bilenlerinin birbirleri ile ilişkisini gösteren akış	34
2.2 PUKÖ Döngüsü	38
2.3 Bilgi Güvenliği Altyapı Bileşenleri	39
2.4 ISO/IEC 27001:2005 BGYS Sertifikasyon Süreci	41
2.5 ITIL'ın Yaşam Döngüsü	44
2.6 BGYS Süreci	55
3.1 Olgunluk Modeli	73
4.1 Araştırma Modeli	79

TABLOLAR DİZİNİ

<u>Tablo</u>	<u>Sayfa</u>
2.1 BGYS'nin gelişim süreci	33
2.2 Yönetişim Model/Standartların Puanları	43
2.3 Planla ve Organize Et	48
2.4 Tedarik ve Uygulama	48
2.5 Teslimat ve Destek	49
2.6 İzle ve Değerlendir	50
2.7 ISO 27001-COBIT ilişkisi	58
3.1 En Popüler Olgunluk Modelleri	72
4.1 Katılımcıların cinsiyetlerine göre dağılımı	81
4.2 Katılımcıların yaşlarına göre dağılımı	81
4.3 Katılımcıların eğitim durumlarına göre dağılımı	82
4.4 Katılımcıların iş yerlerindeki konumlarına göre dağılımı	82
4.5 Kompozit güvenilirlik ve çıkartılmış ortalama varyans değerleri	83
4.6 BG ve Şirket Performansı dinamiklerine ait faktör yükleri	85
4.7 BG ve Şirket Performansı dinamiklerine ait faktör yükleri	87
4.8 Korelasyon, ortalama ve standart sapma değerleri	88
4.9 Gizlilik unsurunun Şirket Performansı dinamikleri üzerindeki etkileri	90
4.10 Bütünlük unsurunun Şirket Performansı dinamikleri üzerindeki etkileri	90
4.11 Erişilebilirlik unsurunun Şirket Performansı dinamikleri üzerindeki etkileri	90
4.12 Şirket Performansı öncüllerinin Şirket Performansı dinamikleri üzerindeki etkileri	91
4.13 Modellerin açıklama kuvveti	91

1. GİRİŞ

Bu tez çalışmasında, bilgi güvenliği yönetim sistemleri ile şirket performansı ilişkisi araştırılmaktadır. Bilgi güvenliği kavramı aslında çok da yeni olmamakla beraber, teknolojinin gelişmesi ile birlikte son yıllarda popülerliğini ve bilinirliğini arttırmış durumdadır. Örneğin, Roma İmparatoru Jül Sezar'ın gizli haberleşmelerini harf atlama gibi şifreleme teknikleri kullanarak gerçekleştirdiğini bilinmektedir. O zamanlarda temelleri atılan bu ve benzeri teknikleri bugün de hala gizlilik gereken durumlarda kullanılmaktadır.

Kuruluşların günümüzde en büyük zorluklarından ve zorunluluklarından birisi iş bilgi ve verilerinin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlayabilmektir. Hiç bir kurum için hatta tek bir iş alanına odaklanmış kurumlar için bile bu çok kolay yerine getirilebilecek olan bir yükümlülük değildir. Aslında her sektörden tüm iş alanlarında dikkate alınması gereken tek bir temel prensip bulunmaktadır; iş süreçlerinin devamlılığını ve müşteri gereksinimlerini, iş veri ve bilgisinin gizlilik, bütünlük ve erişilebilirliğini koruyarak sağlayabilmek. Neyse ki hemen hemen her sektör için mevcut yasa veya yasal düzenlemelerin yetersiz kaldığı durumlar için yönetmelikler, modeller ya da standartlar mevcuttur. Örneğin kredi kartı işlemlerinin güvenli şekilde yapılmasını sağlayan PCI (Payment Card Industry – Ödeme Kartları Endüstrisi) gibi... Bu çalışmada kurumların sahip oldukları bilgi birikiminin güvenliğini sağlama ve etkin bir şekilde faaliyetlerini sürdürebilme amacıyla uyguladıkları Bilgi Güvenliği Yönetim Sistemleri işlenmektedir.

Bilgi Güvenliği Yönetim Sistemi, hangi formatta olursa olsun bilginin saklanması, bir yerden bir yere taşınması, işlenmesi ve kullanılması esnasında bütünlüğünün/güncelliğinin bozulmasını, izinsiz erişimlerle imhasını ve ifşa edilmesini engelleyen, gerektiğinde yetkisi olanlar tarafından erişilebilir olmasını sağlayan faaliyetler bütünüdür. Mevcut tanım ve ifadelerden de anlaşılacağı üzere Bilgi Güvenliği Yönetim Sistemlerinin üç temel boyutu mevcuttur: (1) Gizlilik, (2) Erişilebilirlik ve (3) Bütünlük. Gizlilik, bilgiye erişimin ancak ve ancak yetkili kişilerce sağlanabilmesini ifade etmektedir. Erişilebilirlik, yetkili kişilerin ihtiyaç olduğu zamanda bilgiye erişimlerini rahatça sağlanabilmesi olarak tanımlanmaktadır. Üçüncü bileşen bütünlük ise gizliliği ve erişilebilirliği sağlanmış güncel verinin bütünsel anlamını korumasını ifade etmektedir.

Bilgi Güvenliği Yönetim Sistemleri ile şirket performansı ilişkisi, literatürde henüz araştırılmış bir konu değildir. Oysa ki firmanın sahip olduğu bilgi birikiminin gizliliği, erişilebilirliği ve bütünlüğünün sağlanarak etkin bir şekilde kullanılması olarak da ifade edebileceğimiz bu sistemlerin firma performansını da arttırması beklenmektedir. Ancak bu ilişkinin nasıl olacağı konusu bir soru işareti teşkil etmektedir. Bilgi Güvenliği Yönetim Sistemlerinin etkileri, uzun dönemde süreç üzerinde ortaya çıkacağından bu etkinin direk değil de müşteri memnuniyeti/tatmini, çalışan memnuniyeti/tatmini, örgütsel bağlılık ve süreç yönetimi gibi değişkenler aracılığı ile gerçekleşmesi beklenmektedir.

Bilgi Güvenliği Yönetim Sistemlerinin incelenmekte olduğu bu deneysel çalışmada; hem ilgili literatür hem de iş dünyasındaki mevcut uygulamalar dikkate alınarak, Bilgi Güvenliği Yönetim Sistemleri ile Firma Performansı ilişkisi incelenmekte; böylece mevcut literatürün genişletilmesi hedeflenmektedir. Bu bağlamda;

- a) Bilgi Güvenliği Yönetim Sistemleri kapsamlı bir literatür taraması ile incelenmekte ve Gizlilik, Erişilebilirlik ve Bütünlük boyutları ile tanımlanmaktadır. Bu doğrultuda Bilgi Güvenliği ve Bilgi Güvenliği Yönetim Sistemi kavramlarının ardından Bilgi Güvenliği unsurları açıklanmıştır. Bilgi Güvenliği Yönetim Sistemi risk temelli bir modeldir ve dünyaya bakışı risk odaklıdır. Dolayısıyla risklerin nasıl yönetileceği önem arz etmektedir. Bu yüzden risk işleme yöntemleri, belirlenen risklerin indirgenmesine yönelik uygun kontrol seçimleri, artık risk yönetimi ve risklerin izlenmesi, ölçülmesi gibi konular açıklanmıştır. Bunlara ek olarak Bilgi Güvenliği Yönetim Sistemi Standardı olan ISO 27001 Standardı içerik olarak anlatılmış ve bu standardın bir firmaya nasıl uygulanacağı açıklanmıştır. Aynı zamanda diğer yönetim sistemleri çerçevelerinden COBIT ve ITIL incelenmiştir. ISO 27001 standardı bir kurumun ne gibi aksiyonlar alması gerektiğini tanımlarken ISO 27002 yani eski adıyla ISO 17799, ISO 27001 standardının bir örgüte nasıl uygulanması gerektiğini en iyi uygulamaları göz önüne alarak detaylı bir şekilde açıklamaktadır. Bu bölümde ISO 27002, COBIT ve ITIL yönetim sistemleri de ayrı ayrı tanımlanmış ve ITIL ile COBIT çerçeveleri ve ISO 27001 ile COBIT çerçeveleri karşılaştırılmış, birbirlerine karşı güçlü ve zayıf noktaları belirtilmiştir.

- b) Bilgi Güvenliđi ile Firma performansı arasındaki iliřkinin dođası üzerine durulmakta; bu iliřkinin müşteri memnuniyeti/tatmini, çalışan memnuniyeti/tatmini, örgütsel bađlılık ve süreç yönetimi ara deđiřkenleri üzerinden gerçekteřtiđi tahmin edilerek hipotezler geliřtirilmektedir. Burda, Bilgi Güvenliđi Yönetim Sisteminin bir řirketin performansına nasıl etki ettiđi, bu yönetim sistemi ile çalışan memnuniyeti, müşteri memnuniyeti, örgütsel bađlılık ve řirketin süreç yönetimine nasıl etki ettiđi teorik olarak anlatılmıř, bununla birlikte çalışan memnuniyeti, müşteri memnuniyeti, örgütsel bađlılık ve süreç yönetimi kavramları açıklanmıřtır. Bunlara ek olarak bir örgütte uygulanan Bilgi Güvenliđi Yönetim sisteminin seviyeleri, kısacası Bilgi Güvenliđi olgunluk seviyeleri model ile açıklanmıř, řirket performansı ađısından deđerlendirilmektedir.
- c) Arařtırma kısmında ise Bilgi Güvenliđini sađlayan Gizlilik, Bütünlük ve Eriřilebilirlik unsurlarının Müřteri Memnuniyeti, Örgütsel Bađlılık, Çalışan Memnuniyeti ve Süreç Yaklařımı deđerkenlerine nasıl etki ettiđi ve bu deđerkenler üzerinden Şirket Performansının nasıl etkilendiđi anket arařtırmaları ve analizlerine göre incelenmektedir. Geliřtirilen hipotezler, GSM sektöründen toplanan veriler ıřıđında test edilmekte ve
- d) Nihayetinde elde edilen bulgular yorumlanarak örnekleminizle ilgili deđerlendirmeler yapılmaktadır.

2. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

Günümüzde örgütler ve/veya devlet kurumları işlerini sürdürebilmek için yoğun bir şekilde bilgi kullanımına yönelmişlerdir. Zaman geçtikçe bilginin önemi artmış, sadece güvenli bir şekilde saklanması ve depolanması gelişen ihtiyaçlara cevap verememiş aynı zamanda bir yerden bir yere nakil edilmesi de kaçınılmaz bir ihtiyaç haline gelmiştir. Bilgiye olan bu bağımlılık bilginin korunması ihtiyacını gündeme getirmiştir. Bu anlamda bilgi, kurumun sahip olduğu varlıklar arasında çok önemli bir yere sahiptir.

Bilgi, kurumdaki diğer varlıklar gibi, kurum için önem taşıyan ve bu nedenle de en iyi şekilde korunması gereken bir varlıktır. Bilgiye yönelik olası saldırılar (tahrip edilmesi, silinmesi, bütünlüğünün ve/veya gizliliğinin zarar görmesi), bilgi altyapısının bozulmasına ve bu da beraberinde işlerin aksamasına neden olmaktadır. Dolayısıyla Bu bölümde öncelikle temel olarak bilgi güvenliği kavramı ve bilgi güvenliği yönetim sistemleri üzerinde durulmakta; bunu takiben de bilgi güvenliği yönetim sistemlerinin tarihçesi, kurulum süreci ve temel bileşenleri anlatılmaktadır.

2.1 Bilgi Güvenliği Kavramı

Bilgi güvenliği; kurumdaki işlerin sürekliliğinin sağlanması, işlerde meydana gelebilecek aksaklıkların azaltılması ve yatırımlardan gelecek faydanın artırılması için bilginin geniş çaplı tehditlerden korunmasını sağlar.

Bilgi birçok biçimde bulunabilir. Bilgi, kâğıt dokümanlar üzerinde yazılı olabilir, elektronik ortamlarda saklanıyor olabilir, posta ya da elektronik posta yoluyla bir yerden bir yere iletilebilir ya da kişiler arasında sözlü olarak ifade edilebilir. Bilgi hangi formda olursa olsun, mutlaka uygun bir şekilde korunmalıdır. Bu nedenle Bilgi Güvenliği Yönetim Sistemi uygulanmalıdır.

Bilgi Güvenliği Yönetim Sistemi risk temelli bir yönetim sistemidir. Sistemin temelinde varlıkların belirlenmesi, varlıklara yönelik tehditlerin ve risklerin tespit edilmesi, tespit edilen bu risk ve tehditlerin bertarafına yönelik kontrollerin atanması

ve nihayet bu kontrollerin üst yönetim tarafından belirlenmiş politikalarla desteklenmesi yatmaktadır. Belirtilen bu özet süreç, daima canlı tutulmalıdır.

ISO 27001:2005, Bilgi Güvenliği Yönetim Sistemi kavramını konu almaktadır. Bilgi Güvenliği Yönetim Sistemi(BGYS), bilgi güvenliğinin kurulması, uygulanması, işletilmesi, izlenmesi, sürdürülmesi, iyileştirilmesi ve aynı zamanda iş risklerinin çözümlenmesi kavramı için bazı standartlar tanımlar.

BGYS'nin kuruluşa faydalı olabilmesi için etkin bir biçimde uygulanıyor olması gerekmektedir. BGYS, bir kerede tamamlanacak bir uygulama değildir. Sürekli iyileştirme için sürekli devam edecek bir faaliyet olarak görülmelidir. Bunun için de kuruluşun iş ve işletme kültürünün bir parçası olması gerekir. Bilgi Güvenliği için kontrolleri iyi seçilmiş, uygun olarak uygulanmış ve kullanılmış olan bir yönetim sistemi, günün sonunda bir masraf kalemi olmayacak, organizasyonun başarısına katkı sağlayacaktır (Kajava et al., 2006, s. 2091).

Bir örgüt veya kuruluştaki her işlevsel bölüm, her bölümdeki her proses ve bu proseslerde yer alan herkes, ideal dünyada , işin amaçlarına ve bunun içinde kendi rollerine dair ortak bir kavrayışa sahip olmalıdırlar. Fakat her bir insan, bölüm ya da kısım birbirinden izole bir şekilde çalışamaz. Her biri, bir diğerinin ürününe ve/veya bilgisine bağımlıdır. Her biri, kendi işinden ve işteki bir başkasının kullanıma sunacağı çıktıdan sorumludur. Bu kavrama en bilinen adıyla süreç yaklaşımı denir. Kuruluş içinde herkes, bir müşteri, bir işlemci ve bir tedarikçi, yani üç rolde de görülür. ISO 27001:2005 BGYS Standardı süreç yaklaşımını temel alır ve bu yaklaşımdan hareketle kontrollerini uygulamayı amaçlar. (Kajava et al., 2006, s. 2094)

2.2 Bilgi Güvenliğinin Unsurları

Bilgi güvenliğinin sağlanabilmesi bilginin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin yeterli düzeylerde sağlanabilmesi ile mümkündür.

Bilgi güvenliği temelde aşağıdaki üç unsuru/kavramı hedefler:

- Gizlilik (Confidentiality)
- Bütünlük (Integrity)
- Kullanılabilirlik (Availability)

2.2.1 Gizlilik (Confidentiality)

Bilginin depolanması, işlenmesi, iletilmesi veya herhangi bir prosesi sırasında, sahibi tarafından yetkilendirilmemiş bir kuruluş veya her hangi bir kişi tarafından ulaşılamamasının sağlanması anlamına gelmektedir. Temel olarak erişim kontrolünün bir çok biçimi, gizliliğin korunması ile ilgilidir.

Şifreleme, kitleme, bilinçlendirme vb. gibi kontroller, varlığın hangi formatta olursa olsun gizliliğinin sağlanmasına örnek olarak verilebilir.

Gizlilik Uluslararası Standartlar Örgütü (ISO) tarafından "Bilgiye sadece yetkilendirilmiş kişilerce ulaşılabilmesi" (<http://en.wikipedia.org>) olarak nitelenir. Günümüzde birçok Bilişim ve Telekomünikasyon firmasında şifreleme alt yapılarının kullanılmasının sebebi temel olarak bilginin gizliliğinin sağlanılmasının gerekliliğidir. Gizlilik genel bir tanım olarak ise; "Bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesidir" (Önel ve Dinçkan, 2007, s.6).

Gizlilik, özellikle bir yasa, kanun veya standart dolayısıyla kurum için bir zorunluluk ise önemlidir. Örneğin avukat - müvekkil ilişkisi ya da doktor hasta ilişkisi gibi mesleki bilgiler kanun ile koruma altına alınmıştır. Bazı durumlarda ise taraflar birtakım bilgileri sözleşme ile birbirlerine verirlerken gizlilik anlaşmaları yaparlar. Her iki durumda da gizlilik büyük önem taşımaktadır (Yıldız, 2007, 25).

Diğer bir örnek de telekomünikasyon sektöründen verilebilir. Bu sektörde de gizlilik, bilgi güvenliği kavramları arasında en önemli kavram olarak nitelenmektedir. Bu nedenle Bilgi Teknolojileri ve İletişim Kurumu tarafından 2004

yılında 25365 Sayılı Resmi Gazete ile “Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik” yayınlanmıştır. Bu yönetmelikte Telekomünikasyon Sektöründe Gizliliğin önemi Madde 8 ile açıkça belirtilmiştir.

Madde 1 ile de ilgili yönetmeliğin kapsamı belirlenmiştir (<http://www.tk.gov.tr>).

Madde 1 — Bu Yönetmeliğin amacı, Telekomünikasyon sektöründe kişisel bilgilerin işlenmesi ve gizliliğinin korunmasının güvence altına alınmasına ilişkin usul ve esasları düzenlemektir. Bu Yönetmelik, Telekomünikasyon sektöründe hizmet veren ve alan gerçek ve tüzel kişileri kapsar (<http://www.tk.gov.tr>).

Madde 8 — Yasaların ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının izni olmaksızın, telekomünikasyonun üçüncü şahıs tarafından dinlenmesi, kaydedilmesi, saklanması, kesilmesi veya gözetimi yasaktır. İlgili trafik verilerinin ise işletmeci tarafından hizmet amaçları dışında kaydedilmesi, saklanması ve gözetimi yasaktır (<http://www.tk.gov.tr>).

2.2.2 Bütünlük (Integrity)

Bilginin depolandığı yerde ve aktarılırken doğru ve tam olduğunun, yani doğru şekilde işlendiğinin ve yetkisiz bir şekilde değiştirilmediğinin garantilenmesi anlamına gelir.

National Information Assurance'nin tanımına göre veri bütünlüğü güvenlik anlamında verinin yahut bilginin yetkisiz kişilerce değiştirilmesine veya yok edilmesine karşı korunmasıdır (Yıldız, 2007, 26). Bütünlük, bilginin yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı içeriğinin korunmasıdır. Bütünlük için kısaca kazara veya kasıtlı olarak bilginin bozulmaması diyebiliriz (Önel ve Dinçkan, 2007, s.6).

Verinin bozulması kasten yahut kaza ile olabilir ve bu bütünlüğün bozulmuş olduğu gerçeğini değiştirmez. Güvenlik önlemi alanların iki tür riske karşı da tedbir almaları gerekmektedir. Bilginin bütünlüğü için “Kesinlik, Doğruluk ve Geçerlilik” kıstasları sağlamalıdır (Yıldız, 2007, 26).

Disk sürücülerini, telekomünikasyon sistemlerini ve diğer medya ortamlarını içeren bir çok veri işleyen cihazlarda veri bozulmasını garantilemek için bütünlüğü kontrol eden mekanizmalar ve yöntemler mevcuttur. Örnek olarak girdi/çıkı veri doğrulama kontrolleri, kullanıcı eğitimleri ve diğer operasyon tipi kontroller gibi.

2.2.3 Erişilebilirlik/Kullanılabilirlik (Availability)

Bilginin, yetkisi olan kurumlar ve kişiler tarafından gerekli olduğu zamanlar ulaşılabilir veya kullanılabilir olması anlamına gelir.

Matematiksel olarak ifade edilirse, kullanılabilirlik herhangi bir sistemin yapılış amaçlarına göre işlev gördüğü zaman, işlev gördüğü ve görmediği toplam zamana oranıdır. Daha yalın bir anlatımla, doğru yetkilendirilmiş bir kişinin ihtiyacı olduğu anda ihtiyacı olan hizmetin orada olma oranına kullanılabilirlik, diğer bir deyişle ise erişilebilirlik denir. Verilen hizmetin ne kadar güvenilir olduğunun bir ölçütüdür. Kurumlar hizmetin ne kadar önemli olduğunun ölçümünü yapıp sistemleri ve verileri bu ihtiyaca göre yedekli hale getirirler (Yıldız, 2007, 27).

Kullanılabilirliği anlatan bir diğer tanım ise bilginin her ihtiyaç duyulduğunda kullanıma hazır olmasıdır. Herhangi bir sorun ya da problem çıkması durumunda bile bilginin erişilebilir olması kullanılabilirlik özelliğinin bir gereğidir. Bu erişim kullanıcının hakları çerçevesinde olmalıdır (Önel ve Dinçkan, 2007, s.6). Kullanılabilirlik ilkesince her kullanıcı erişim hakkının bulunduğu bilgi kaynağına, yetkili olduğu zaman diliminde mutlaka erişebilmelidir. Bu nedenle özellikle kurumun güvenlik kurallarının verinin erişilebilirliğini engellemesi gerektiği unutulmamalıdır.

Güvenlik olaylarının hizmet seviyelerinin ve sistem performansının düzenli olarak izlenmesi, gözden geçirilmesi ve kontrol edilmesi, kullanılabilirliği garanti altına almak için uygulanacak önleyici kontrollerdir.

2.3 Bilgi Güvenliği Yönetim Sistemi Standardı

Bilgi Güvenliği Yönetim Sistemi, ISO/IEC 27001:2005 BGYS Standardı maddelerine göre bir kuruma uygulanır. Bu standardın maddelerinin ne olduğu ve açıklamaları bu bölümde ayrıntıları ile yer almaktadır.

2.3.1 4 BGYS'yi Kurmak

2.3.1.1 4.1 Genel Gereksinimler

Bilgi Güvenliği Yönetim Sisteminin kurulması, yazı hale getirilmesi, uygulanması, işletilmesi, sürdürülmesi ve sürekli iyileştirilmesi gereksinimi bu maddede tanımlanmıştır(Gerber and Solms, 2008, s.126). Kuruluş, sistem için gereken süreçleri belirlemelidir. Prosesler ölçülmeli, izlenmeli, çözümlenmeli ve planlanan sonuçları başarmak için gerekli faaliyetler gerçekleştirilmelidir(ISO/IEC FDIS 27001:2005, 2005, s.3).

2.3.2 4.2 BGYS'nin Kurulması ve Yönetilmesi

2.3.2.1 4.2.1 BGYS'yi Uygulamak

a. BGYS'nin Kapsam ve Sınırlarını tanımlamak

Bu, işin özelliklerine, kuruluşa, kuruluşun yerine, varlıklarına ve teknolojisine göre yapılmalıdır. BGYS kapsamı kuruluşun tamamı olabileceği gibi bir bölümü de olabilir. Kısaca BGYS'nin kapsamı iyi tanımlanmış ve bütün olmalıdır (ISO/IEC FDIS 27001:2005, 2005, s.4).

b. BGYS Politikası Tanımlamak

İşin özelliklerine, kuruluşa, kuruluşun yerine, varlıklarına ve teknolojisine göre ve yasal gereksinimleri, kontrata bağlı yasal üçüncü taraf zorunlulukları ve bağımlılıkları dikkate alınarak tanımlanmalıdır. Politika yönetim tarafından onaylanmalıdır (ISO/IEC FDIS 27001:2005, 2005, s.4).

BGYS Politikasında; organizasyonun ve süreçlerinin, güvenlik politika hedeflerinin, güvenlik altyapısının açıklanması; bilgi varlıklarının ve bunlara ait tehdit ve risklerin tanımlanması, mevcut durum ve güvenlik önlemleri, acil durum planlarının belirlenmesi gibi konuların örgüte/kuruma nasıl uygulanacağını genel bir şekilde ifade edilmesi gerekmektedir. (Tvrdíková M., 2008, s. 153)

c. Sistematik bir risk değerlendirme yaklaşımı belirlemek

Kuruluşun riskleri kabul etme kriterlerini ve kabul edilebilir risk seviyelerinin tanımlanışını tarifliyen bir yaklaşım olmalıdır. Her kuruluşun kendine özgü bir risk değerlendirme metodolojisi vardır. Ama uygulanacak metodoloji, ISO 27001:2005'deki tüm kontrol alanlarını kapsamalıdır (ISO/IEC FDIS 27001:2005, 2005, s.4).

d. Risklerin Belirlenmesi

Varlıklara yönelik zayıflıklar ve tehditler göz önünde bulundurularak varlıkların bütünlük, gizlilik ve erişilebilirlik değerlerine etkide bulunacak tüm riskler belirlenmelidir (ISO/IEC FDIS 27001:2005, 2005, s.4).

e. Risklerin Çözümlemesi ve Değerlendirilmesi

Belirlenen risklere dayanarak organizasyonel olarak, personel kontrollerini, iş proseslerini, işletme ve bakım proseslerini ve süreçlerini, yasa, düzenleme ve konratlara tabi konuları ve bilgi işleme olanaklarının içeren tüm kontrol alanları dikkate alınmalıdır. Tüm bunların sonucunda, kuruma has kabul edilebilir risk seviyeleri belirlenmelidir (ISO/IEC FDIS 27001:2005, 2005, s.5).

f. Risk İşleme için seçenekleri belirlemek ve değerlendirmek

Örgüt/Kuruluş varlıklarına yönelik riskleri belirledikten sonra bu riskler için çeşitli önlemler almalıdır. Kuruluşun düşüneceği yöntemler (ISO/IEC FDIS 27001:2005, 2005, s.5):

- Riskleri indirgemek için uygun kontrolleri uygulamak,
- Risk içeren bir faaliyette bulunmayarak riskten kaçınmak,
- Riskin tamamını veya bir bölümünü sigorta gibi üçüncü bir tarafa devretmek,
- Bilerek ve nesnel olarak riski kabul etmek.

g. Riskin işlenmesi için kontrol amaçları ve kontrolleri seçmek

Belirlenen risklerin bertaraf etmek için uygulanacak kontroller ISO 27001:2005'deki EK-A ya göre seçilmeli ve uygulanmalıdır. Bu maddeler arasında olmayan ama uygulanması gereken kontrollerde haricen uygulanabilir. Kontrollerin seçimi kabul edilebilir maliyetlerde olmalıdır. Yani kontrolleri uygulamanın maliyeti, indirgenmesi amaçlanan risklerin finansal etkilerinden daha fazla olmamalıdır (ISO/IEC FDIS 27001:2005, 2005, s.5).

h. & i. Yönetimin onayını ve yetkisini almak

Risk yönetimi adımlarını geçtikten sonra BGYS işletimi ve uygulamasını yapmak için yönetimden onay almak gerekmektedir. (ISO/IEC FDIS 27001:2005, 2005, s.5)

j. Uygulanabilirlik Bildirgesi hazırlamak

Uygulanabilirlik bildirgesi, ISO 27001:2005 Belgesi almak isteyen kuruluşlar için zorunluluktur. Uygulanabilirlik Bildirgesi, seçilmiş olanı gösteren bir dokümandır ve bu seçim risk değerlendirme ve risk işleme prosesleri ile ilişkilendirilmiş olmalıdır. Bu bağlantı kontrol amaçları ve kontrollerin seçiminin arkasındaki muhakemeyi ve akıl yürütmeyi gösterir (ISO/IEC FDIS 27001:2005, 2005, s.5).

2.3.2.2 4.2.2 BGYS'yi Gerçekleştirmek ve İşletmek

Kuruluşun belirlediği ve değerlendirdiği bilgi güvenliği risklerini yönetmek için risk işleme planını oluşturmayı kapsar (Gerber and Solms, 2008, s.126). Bu plan, hangi yönetim faaliyetlerine başvurmak gerektiğini, bilgi güvenliği riskleri ile ilgili ve BGYS ile ilişkili kullanıcı faaliyetlerine ilişkin her türlü güvenlik ile ilgili kişilerin sorumluluklarının taslağını çizmelidir (ISO/IEC FDIS 27001:2005, 2005, s.6).

Örgüt ve/veya kuruluş, BGYS için nasıl bütçe sağlanacağını, rollerin ve sorumlulukların tahsis edilmesini, uygun bir farkındalık ve eğitim programının uygulanmasını, kaynakların ve işletimlerin yönetimini ve bilgi güvenliği olaylarının yönetimi için süreçlerin geliştirilmesini ve kullanılmasını hesaba katarak, risk işleme planının ve seçilmiş kontroller sisteminin gerçekleştirilmesi için hali hazırda bir süreçler kümesine sahip olmalıdır.

Aynı zamanda seçilen kontrollerin etkinliği de önemlidir. Kontroller, seçilme nedenleri olan güvenlik risklerinin yönetiminde etkili olmalıdır.

2.3.2.3 4.2.3 BGYS'nin İzlenmesi ve Gözden Geçirilmesi

BGYS'nin bilgi güvenliği risklerini yönetmede etkin olabilmesi için BGYS'yi etkileyebilecek tüm değişiklikleri izlemek ve izini tutmak önemlidir. Bu

değişiklikler aşağıdaki gibi zayıflıklara ve bunlardan ötürü oluşacak tehditlere neden olabilir(ISO/IEC FDIS 27001:2005, 2005, s.6):

- İş Çevresi ve Bağlamının Değişmesi: Yeni iş ortakları, yeni ve farklı tedarik zincirleri, yeni/farklı veya değişen müşteri tabanı, yeni pazarlara açılma, piyasa koşulları, üçüncü taraf düzenlemeleri, vs.
- İş politikası ve amaçlarının değişmesi,
- Organizasyonel yapının, iş gücünü, işletim çevresini değiştirmesi,
- Teknolojinin kullanılması ve geliştirilmesi: Yeni sistemler, uygulamalar ve güncellemeler vs,
- Yasal ve düzenlemelere bağlı çevre koşullarının değişmesi.

Yukarıdaki değişiklikler, bir kuruluşun riskleri ve işi üzerinde etkili olabilir. Risklerin yeniden değerlendirilmesi, artık risklerin seviyesi ve kabul edilebilir risk seviyesi BGYS'nin etkili kalabilmesi için gereklidir.

BGYS'nin kontrol edilmesinde ve yeniden gözden geçirilmesinde aşağıdaki hususlara bakılmalıdır:

- Politikanın kapsamı hala geçerlimi?
- Uygulanan kontroller sistemi hala geçerli ve etkili mi?
- İş süreçleri hala geçerli mi ve işin kapsamında doğru olarak kullanılıyor mu?
- Tahsis edilen roller ve sorumluluklar hala geçerli mi?
 - Güvenlik ihlal olaylarının ele alınış süreçlerinin sonuçları doğru şekilde kullanılmış mı?
 - İş sürekliliği planları hala uygun mu?

2.3.2.4 4.2.4 BGYS'yi Sürdürmek ve İyileştirmek

İç ve dış koşullardan etkilenen riskler sürekli değişir. Güvenlik ihlal olayları, risklerin gerçekleştiğini gösterir ve zamanında tepki gösterilmesini garanti altına almak için eskalasyon süreçleri gerçekleştirilebilir. Riskler:

- Tehditlerin düzenli gözden geçirilmesiyle,
- Var olan kontrol sistemi ve onun etkinliği ile,
- Tetkiklerle,

düzenli olarak izlenmelidir.

Kuruluş, BGYS'nin iyileştirilmesi için, BGYS'nin uygulanması ve işletilmesi sırasında çıkan uygunsuzlukları tespit etmeli, uygunsuzlukların nedenlerini saptamalı, uygunsuzlukların nedenlerini ortadan kaldırmak için gereken önlemleri değerlendirmeli ve bunları tekrarını önlemek için düzeltici faaliyetler yürütmelidir (ISO/IEC FDIS 27001:2005, 2005, s.7).

2.3.3 4.3 Dökümantasyon Gereksinimleri

2.3.3.1 4.3.1 Genel

BGYS'nin, ISO 27001:2005'in 4.3 maddesi ile uyumlu, yazılı bir yönetim sistemi olması önemlidir. BGYS dokümanları aşağıdaki hususları içinde barındırmalıdır (ISO/IEC FDIS 27001:2005, 2005, s.7):

- BGYS'nin kapsamını,
- Güvenlik Politikasını,
- BGYS'i destekleyen süreç ve kontrolleri,
- Risk değerlendirme metodolojisi ve raporunu,
- Risk değerlendirme planını,
- Bilgi Güvenliği süreçlerinin etkili planlanmasını, işletilmesi ve kontrolünü garanti altına almak için gereken süreçleri,
- BGYS'nin gereksinimleri ile uyumluluğu ve etkili işletimini kanıtlayan kayıtları,
- Uygulanabilirlik Bildirgesini.

2.3.3.2 4.3.2 & 4.3.3 Dokümanların ve Kayıtların Kontrolü

ISO 27001:2005, BGYS dokümanlarının uygun şekilde korunduğunu ve kontrol edildiğini garantilemek için, dokümanların ve kayıtların kontrolü için zorunlu olan gereksinimleri, 4.2.3 ve 4.3.3 maddelerinde tanımlamıştır (ISO/IEC FDIS 27001:2005, 2005, s.8).

Kayıtlar, Bilgi Güvenliği açısından çok önemli bir rol oynar. Bir Bilgi Güvenliği ihlal olayı olduğu zaman, olayın yerinde incelenmesi ve geriye dönük analizinin yapılması kritik bir önem taşır. İhlal olaylarının üstesinden gelmenin en iyi yolu, kanıt toplamak ve ne zaman? nerede? kim? vb. sorulara cevaplar bulmaktır. Ancak iyi ve doğru bir şekilde kayıt saklamakla bu soruların cevapları bulunur

(Savola R., 2006, s. 1653). Aynı zamanda kanıtları toplamak ve saklamak içinde bazı yasal gereksinimler vardır. Dolayısıyla sadece kayıtların tutulması değil, kayıtların korunması yani bütünlük, gizlilik ve erişilebilirlik değerlerinin de garantilenmesi önem taşımaktadır.

Tüm bu anlamda, ISO 27001:2005'deki doküman ve kayıt kontrolleri, ISO 9001:2000 ile uyum sağlamaktadır ve bu konuda bir biri ile entegre içindedir (Kajava et al., 2006, s. 2093) (Boehmer W., 2008, s. 224).

2.3.4 5 Yönetimin Bağlılığı

Bilgi Güvenliği Politikasının kurulması, amaçların belirlenmesi, rol ve sorumlulukların atanması, bilgi güvenliği yönetiminin öneminin iş dünyasına anlatılması gerekmektedir (Solms B., 2006, s. 167). BGYS için kaynakların sağlanması, yönetimin gözden geçirmeleri sonucunda kabul edilebilir risk seviyesine karar verilmesi için yönetimde, pozitif, görünür, gerçek destek ve bağlılığın olması gerekir (ISO/IEC FDIS 27001:2005, 2005, s.9).

Aynı zamanda kullanıcılara, çalışanlara, yöneticilere ve gerekiyorsa sözleşmelilere rol ve fonksiyonları, özel bilgi güvenliği sorumlulukları ile orantılı eğitimler verilmelidir (Kajava et al., 2006, s. 2094).

2.3.5 6 İç BGYS Denetimi

BGYS canlı bir sistem olmalıdır. Dolayısıyla BGYS'nin politikalarının prosedürler, standartlarla, talimatlarla, süreçlerle, sözleşmelerle vs uyumlu olması gerekir (ISO/IEC FDIS 27001:2005, 2005, s.10). Bu anlamda tüm bunların doğruluğunun ve uygunluğunun sağlandığının denetimlerle tespit edilmesi gerekmektedir. Denetimlerin periyotları kurumun/örgütün politikalarında belirlenmelidir. Bu örnek olarak senede en az 1 kere yapılabilir. Yapılan denetimler süreçlerin daha iyi işletilmesi ve iyileştirmeye yönelik olmalıdır. Denetlemeler sonucu ortaya çıkan uygunsuzluklar ve gözlemler denetim sonrası izlenmelidir. Bir sonraki denetimde ise önce bu uygunsuzluklara bakılmalı ve hala düzelmemişse bunların kök nedenlerine inilmelidir. Denetim sonrası bulgular üst yönetime raporlanmalıdır. (Humphreys E., 2008, s. 251)

2.3.6 7 Yönetimin Gözden Geçirmesi

BGYS'nin gözden geçirilmesi, organizasyonun BGYS için değişiklik ve iyileştirmelerin gerekip gerekmediğini muhakeme etmeyi ve hesaplamayı sağlar. Kontrol etme aşaması, BGYS nin hala geçerli olup olmadığını ve etkili bir bilgi güvenliği sağlayıp sağlamadığını belirlemek ve değerlendirmek için iş ve işletme çevresindeki değişiklikleri izlemenin ve gözden geçirmenin önemini vurgular. Durum gözden geçirildikten sonra, bazı politikaların ve süreçlerin eklenmesi/değiştirilmesi/iyileştirilmesi, bazı teknik kontrollerin eklenmesi eklenmesi/değiştirilmesi/iyileştirilmesi vs. gerekebilir (ISO/IEC FDIS 27001:2005, 2005, s.11). BGYS düzenli aralıklarla gözden geçirilmez ve tetkik edilmezse zaman aşımına uğrayabilir. Aynı zamanda kuruluşun karşılaştığı riskleri yönetmede etkisiz ve yetersiz kalabilir. Sonuç olarak kuruluş, olmayan bir BGYS'ye yatırım yapar hale gelebilir.

2.3.7 8 BGYS'yi İyileştirme

2.3.7.1 8.1 Sürekli İyileştirme

Kuruluş/örgüt, bilgi güvenliği yönetim sisteminin sürekli iyileştirilmesi için gerekli süreçleri planlayıp yönetmelidir. Tetkik sonuçları, veri çözümlemesini, düzeltici ve önleyici faaliyetleri ve yönetimin gözden geçirmesini kullanarak; BGYS politikası aracılığı ile sürekli iyileştirme sağlamalıdır (ISO/IEC FDIS 27001:2005, 2005, s.12).

2.3.7.2 8.2 Düzeltici Faaliyet

Uygunsuzlukların nedenini ortadan kaldırmak ve tekrarını önlemek için süreçlerin olması gerekir. Uygunsuzlukları ve bunların kök nedenlerini tespit edip tekrarını önlemek için gereken önlemler birlikte alınmalıdır.

2.3.7.3 8.3 Önleyici Faaliyet

Olası uygunsuzlukları ve bunların nedenlerini tespit etmeyi, olmasını engellemeye yönelik faaliyetlerin kayıtlarını tutmayı amaçlar.

2.3.8 EK-A KONTROLLERİ

ISO 27001:2005, tespit edilen risklerin etkilerini en aza indirmek için 11 alanda toplam 133 kontrol maddesi içermektedir(Broderick J.S.,2006, s.27). Bu 11 alan aşağıdaki konu başlıklarına ait kontrolleri ifade eder (ISO/IEC FDIS 27001:2005, 2005, s.13):

- Güvenlik Politikası
- Bilgi Güvenliği Organizasyonu
- Varlık Yönetimi
- İnsan Kaynakları Güvenliği
- Fiziksel ve Çevresel Güvenlik
- Haberleşme ve İşletim Yönetimi
- Erişim Kontrolü
- Bilgi Sistemleri Edinim, Geliştirme ve Bakım
- Bilgi Güvenliği İhlal Yönetimi
- İş Sürekliliği Yönetimi
- Uyum

Bu kontrol maddeleri bir kurumun uygulaması gereken kontrollerdir. Ama bir kuruluş hepsini uygulayamayabilir. Bu durumda, bu kontrol maddelerinden hangilerini uygulayamıyorsa nedenlerini belirtmek zorundadır. Bununla beraber bir kurum/örgüt bu kontrol maddelerine ek, kendine özel başka kontrol maddeleri de uygulayabilir. Bunlarda kayıt altına alınmalıdır.

2.3.8.1 Güvenlik Politikası

Kapsama ve bu kapsamın sınırlarına göre kurumun sahip olduğu bilgi varlıkları ve teknoloji göz önüne alınarak Bilgi Güvenliği Politikaları geliştirilmeli ve dokümanite edilmelidir (Solms S.H., 2005, s.445). Kurumun bilgi varlıklarının nasıl korunacağı, bu politikada tanımlanır. Bu doküman üst yönetim tarafından onaylı olmalı ve olası tüm tehditlere karşı uygulanması gereken önlemleri içermelidir (Day M., 2007, s.4).

2.3.8.2 Bilgi Güvenliği Organizasyonu

Bilgi Güvenliği takımını belirlenmeli, rol ve sorumlukları tanımlanmalıdır. Güvenlik altyapısı olarak, yetkilendirme süreçleri, gizlilik ve ifşa etmeme sözleşmeleri ve uygun iletişim süreçleri vb konular hazırlanmalıdır. Bununla birlikte

dış taraflarla(üreticiler, iş ortakları, yükleniciler, tedarikçiler vb.) olan güvenlik konuları da düzenlenmelidir(Day M., 2007, s.4).

2.3.8.3 Varlık Yönetimi

Bilgi varlıkları tanımlanmalı ve bunlardan sorumlu sahipler belirlenmelidir. Bununla birlikte varlıkların kabul edilebilir kullanım kuralları da belirlenmelidir. Kurumun kendi geliştireceği bir herhangi bir standarda göre bilgi varlıkları sınıflandırılmalı ve etiketlenmelidir. Örnek olarak “Sır”, “Gizli”, “Şirkete Özel” ve “Kamuya Açık” sınıfları verilebilir (Day M., 2007, s.4).

Varlık Sahipliği(İş Sahipliği): Varlığın gizliliğinin, bütünlüğünün, erişilebilirliğinin sağlanmasından birinci derecede sorumlu kişi veya kişilerdir. BGYS Varlık yönetimindeki sahip kavramı daha çok sorumluluk anlamında kullanılmaktadır. Varlık değerinin belirlenmesi, varlığa yönelik risk tanımlamalarının yapılması varlık sahibinin görevleri arasındadır(Ör: Kurum finansal bilgilerinin sahibi kurumun finans bölüm müdürüdür).

İş Sahipliği: Varlığın sahibi olmamasına rağmen, varlığın sağlıklı bir şekilde sürekliliğinin idamesini sağlayan rolündeki kişi veya kişilerdir. Birçok durumda varlık sahibi ile farklı kişi olabilir(Ör: Kurum finansal bilgilerinin sahibi finans bölümü müdürü iken emanetçisi ilgili veri tabanı yöneticisidir) (Koç F., 2008, s.7).

2.3.8.4 İnsan Kaynakları Güvenliği

Personelle, yarı zamanlı çalışanlarla, sözleşmelilerle ilgili işe alım süreçlerine güvenlik taramaları eklenmeli; ifşa etmeme ve gizlilik sözleşmelerine dair maddeler personel sözleşmelerine eklenmelidir(Day M., 2007, s.4). Çalışanların iş tanımlarına güvenlikle ilgili rol ve sorumluluklar eklenmelidir. Güvenlik maddeleri içine transfer, işten ayrılma, göreve son verme gibi koşullar da eklenmeli ve disiplin süreçleri tanımlanmalıdır. (Humphreys E., 2008, s. 251)

2.3.8.5 Fiziksel ve Çevresel Güvenlik

Bilginin ve bilgisayar sistemlerinin bulunduğu alanların fiziksel güvenliği sağlanmalıdır. Bunlar; bilgisayar merkezleri, tedarik alanları, toplama alanları, imha noktalarıdır. (Day M., 2007, s.4). Güvenliğin sağlandığından emin olunmalı; sınırların, çevrenin, yangın koruma sistemlerinin, havalandırma sistemlerinin, kabloların, enerji kaynaklarının, kilitlerin ve alarmların bakımları yapılmalıdır.

Sistem kullanıcılarının, ziyaretçilerin ve cihazların giriş/çıkışlarının kayıtları tutulmalıdır. (ISO/IEC FDIS 17799:2005, 2005, s.42)

2.3.8.6 Haberleşme ve İşletim Yönetimi

Bilgi işlem süreçlerinin doğruluğu ve güvenliğinden emin olunmalıdır (Day M., 2007, s.4). Bunun için değişim yönetimi, görevler ayrılığı ilkesi, yazılım ve hizmet kabulü ve dağıtım kriterleri (şirket içi, dış kaynak), ağ koruması (kablolu, kablosuz, hareketli), elektronik ticaret, saat senkronizasyonu, yedek alma, yedekten geri dönme, ekipman değişimi veya transferi, iletişim değişimi, e-mail/fax kullanımı gibi konuları içinde barındıran prosedürler yazılmalı ve sorumluluklar atanmalıdır (ISO/IEC FDIS 17799:2005, 2005, s.50).

2.3.8.7 Erişim Kontrolü

Görevlerden doğan tüm erişim ihtiyaçlarının düzenlenmesi ve kurallara bağlanması için prosedürler ve sorumluluklar tanımlanmalıdır. Kısacası ihtiyaca göre yetkilendirme yapılmalıdır (Humphreys E., 2008, s. 252). Bunlar, ağlar (kablolu, kablosuz, hareketli ve çevirmeli ağlar) için kullanıcı tanımlama, işletim sistemi, uygulama ve veri tabanları, yetki ve hakların belirlenmesi, şifre kullanımı ve kritik sistemlere erişimlerin izlenmesi vb. gibi konuları içermelidirler. Aynı zamanda denetimlerle ve kayıt(log) kontrolleri ile bilgiye erişimler izlenmeli ve gözden geçirilmelidir (Day M., 2007, s.4).

2.3.8.8 Bilgi Sistemleri Edinim, Geliştirme ve Bakım

Yeni sistem geliştirmeleri, mevcut sistemlerin güncellemeleri ve konfigürasyonları, test etme, uygulama, süreç, girdi/çıkış, mesaj bütünlüğü ve işletim sistemi değişiklikleri gibi konularda özellikle formal ihtiyaçların güvenlik kontrolleri yapılmalıdır (Day M., 2007, s.4). Özellikle uygulama kaynakları ve objelerinin prosedürlerle korunması gerekmektedir. Kripto kullanımı, dijital imza, sertifikalar ve herkese açık anahtar alt yapısı (PKI) ve bunun gibi diğer gerekli konular da prosedürlerde tanımlanmalıdır (ISO/IEC FDIS 17799:2005, 2005, s.90).

2.3.8.9 Bilgi Güvenliği İhlal Yönetimi

Muhtemel güvenlik vakaları ve zayıflıklarının yönetilmesine yönelik prosedürler ve sorumluluklar tanımlanmalıdır (Humphreys E., 2008, s. 250). Hizmet veya sistemlerde oluşabilecek arıza durumlarında, iş sürekliliği planlarına göre hızlı kurtarma sağlanmalıdır. Delillerin/izlerin toplanması ve raporlanması için özel haberleşme mekanizmalarının kurulması ve vaka çözümleri için kayıtların, denetimlerin ve analizlerin yapılması gerekmektedir (Day M., 2007, s.4).

2.3.8.10 İş Sürekliliği Yönetimi

İş sürekliliği süreçlerinin tanımlanabilmesi için kritik iş alanlarının önceliklendirilmesi gerekmektedir. İş kollarını kesintiye uğratacak olayların ve tehditlerin tanımlanabilmesi için etki analizleri yapılmalıdır. Arıza/felaket ile devamlılık arasındaki zaman boşluğuna/mesafesine uygun iş sürekliliği çerçeveleri belirlenmelidir. Kurtarma işlemleri ile birlikte kapsamlı veri saklama ve yedekleme politikası tasarlanmalıdır(Day M., 2007, s.5). Tüm kritik donanım, ağ, yazılım, veri tabanları ve uygulamaların önleyici bakımları planlanmalıdır. İş sürekliliği planlarının gerçek hayata adapte edilebilmesi için çalışanlar tarafından test edilmesi gerekmektedir. İş Sürekliliği planları efektif olmaları için sektörel iş ihtiyaçlarındaki ve politikalardaki değişikliklere göre sürekli güncellenmelidir. (ISO/IEC FDIS 17799:2005, 2005, s.95)

2.3.8.11 Uyum

Kurum, içinde bulunduğu sektörün uyması gerekli olan kanuni ve uluslararası regülasyonlara uyum içinde olmalı, politika ve prosedürlerin bu ihtiyaçlara uygun hazırlanmış olması gerekmektedir (Solms S.H., 2005, s.445). Kurum, ilgili fikri mülkiyet haklarına ve yazılım telif haklarına uymak zorundadır(Day M., 2007, s.5). Organizasyon kayıtları ve personelin kişisel bilgileri korunmalıdır. Sistem denetimlerinde sektörel regülasyonlara, kanuni regülasyonlara ve diğer otoritelere uyumun sağlandığının kontrolü yapılmalıdır. (ISO/IEC FDIS 17799:2005, 2005, s.113)

2.4 Bilgi Güvenliđi Standardının Tarihçesi

Bu standardın tarihi, 1992 yılında belirli sanayi sektörleri ve hizmet sağlayıcıların, elektronik ofis sistemlerinin kullanımındaki artışı ve bununla beraber bu sistemlerin olası problemleri ve sistemler üzerindeki kontrol mekanizmaları ile ilgili kaygılar sonucu başlamıştır. Ocak 1993'te, sanayinin dile getirdiđi kaygıları gözden geçirmek üzere bir çalışma gurubu kuruldu. Bu çalışma gurubundan elde edilen çıktı, Eylül 1993'te yayınlanan “Uygulama Prensipleri”ydi. Bir sonraki adım “Uygulama Prensipleri”nin bir ingiliz standardına dönüştürölmesiydi ve bu Şubat 1995'te “BS 7799-1”in yayınlanması ile gerçekleşti. Fakat bu hala bir rehber dokümandı. Bu durum sanayiye denetlenebilir bir standarttan mahrum bırakmıştı. Sanayinin talepleri doğrultusunda Şubat 1998'de “BS 7799-2” yayınlandı.

Nisan 1999'da, rehber ve standart aynı doğrultuya sokulmuş ve BS 7799-1:1999, BS 7799-2:1999 olarak yeniden yayınlanmıştır. Bir sonraki büyük adım, 2000'de BS 7799-1'in gözden geçirilmesi sonucu birkaç ufak deđişiklikten sonra uluslar arası bir standart olan ISO 17799:2000 olarak numaralanması olmuştur. BS 7799-2:1999 da uluslar arası bir standart olarak gözden geçirilmeliydi ama bu reddedildi ve ingiliz standardı olarak kaldı. (Broderick J.S.,2006, s.26)

BS 7799-2:2002, ISO 17799:2005'teki deđişiklikleri takiben, ana standardı yeniden numaralandırarak ISO 27001:2005 oldu. Ve en son sürümü 15 Ekim 2005 tarihinde yayınlandı.

Tablo 2.1'de BS 7799 dan son versiyon olan ISO/IEC 27001:2005'e kadar olan gelişim süreçleri gösterilmiştir:

ISO-27001:2005	ISO/IEC-17799:2005	BS-7799-2:2002	ISO/IEC-17799:2000
Güvenlik Politikası	Güvenlik Politikası	Bilgi Güvenliği Politikası	Güvenlik Politikası
Bilgi Güvenliği Organizasyonu	Bilgi Güvenliği Organizasyonu	Organizasyonel Güvenlik	Organizasyonel Güvenlik
Varlık Yönetimi	Varlık Yönetimi	Varlık Sınıflandırması ve kontrolü	Varlık Sınıflandırması ve kontrolü
İnsan Kaynakları Güvenliği	İnsan Kaynakları Güvenliği	Personel Güvenliği	Personel Güvenliği
Fiziksel ve Çevresel Güvenlik	Fiziksel ve Çevresel Güvenlik	Fiziksel ve Çevresel Güvenlik	Fiziksel ve Çevresel Güvenlik
Haberleşme ve işletim Yönetimi	Haberleşme ve işletim Yönetimi	Haberleşme ve işletim Yönetimi	Haberleşme ve işletim Yönetimi
Erişim Kontrolü	Erişim Kontrolü	Erişim Kontrolü	Erişim Kontrolü
Bilgi Sistemleri Edinim, Geliştirme ve Bakım	Bilgi Sistemleri Edinim, Geliştirme ve Bakım	Sistem Geliştirme ve Bakım	Sistem Geliştirme ve Bakım
Bilgi Güvenliği İhlal Yönetimi	Bilgi Güvenliği İhlal Yönetimi	Yok	Yok
İş Sürekliliği	İş Sürekliliği Yönetimi	İş Sürekliliği Yönetimi	İş Sürekliliği Yönetimi
Uyum	Uyum	Uyum	Uyum

Tablo 2.1 BGYS'nin gelişim süreci (Broderick J.S.,2006, s.27)

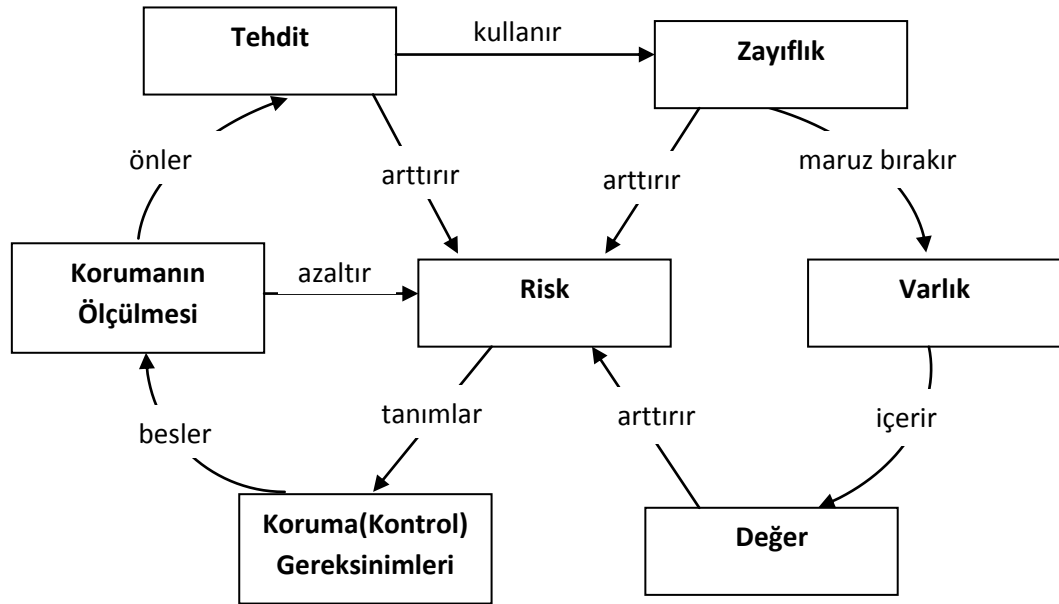
2.5 Risk Yönetimi

Bilgi Güvenliği Yönetim Sistemi, risk temelli bir yaklaşım sergiler (Boehmer W., 2008, s. 224). Bilgi Güvenliği Politikaları risk analizleri sonucuna göre şekillenir ve oluşur (Tvrdíková M., 2008, s. 153). Bu nedenle risk yönetimi çok önemlidir.

Risk Yönetimi,

- Risklerin Değerlendirilmesi,
- Risk İşleme Planlarının oluşturulması,
- İlgili Kontrollerin Seçilmesi
- Risklerin izlenmesi, yeniden değerlendirilmesi ve gözden geçirilmesi,

adımlarından oluşur. (Humphreys E., 2008, s. 249)



Şekil 2.1 BGYS risk bileşenlerinin birbirleri ile ilişkisini gösteren akış (Farn at al.,2004, s.507)

Şekil 2.1’de BGYS risk bileşenlerinin döngüsü görülmektedir. Burada riski arttıran unsurlar varlığın değeri, varlığa ait zayıflıklar ve varlığa yönelik tehditlerdir. Tehditler, varlığın zayıflığını kullanır. İlgili riski azaltmak için kontroller uygulanmalıdır. Bununla beraber uygulanan kontrol/korumanın etkinliğinin ölçülmesi de gerekmektedir. Böylece tehdit önlenmiş ve risk azaltılmış olacaktır(Farn at al.,2004, s.507).

Örgüt, risklerinin değerlendirilmesi ve yönetilmesi için bir risk yönetim çerçevesi oluşturulmalı ve sürdürülmelidir. Risk yönetim çerçevesi, genel ve üzerinde anlaşılmış örgüt risk seviyelerini, risk karşılama stratejilerini ve artakalan

riskleri (residual risk) içermelidir. Örgüt hedefleri üzerinde herhangi bir potansiyel etkinin oluşturacağı beklenmedik olaylar önceden belirlenir, analiz edilir ve değerlendirilir. Artakalan riskleri kabul edilebilir bir seviyeye ulaştırmak için risk işleme yöntemleri uygulanır.

2.5.1 Risk İşleme Yöntemleri

Risk işleme yöntemleri kurumun iş hedeflerine ve misyonuna uygun olarak seçilmelidir. Riski azaltmak için kullanılabilecek yöntemler şu şekilde sıralanabilir. (Eskiyörük D., 2007, s. 22)

- **Riskin Kabulü:** Riskin var olduğunu kabul ederek işe devam etmektir.
- **Riskten Kaçınma:** Riski yaratan sebebi ortadan kaldırmaktır (örneğin bir yazılımın risk yaratan kısmının yüklenmemesi ve kullanılmaması gibi)
- **Riskin Azaltılması:** Açıklığın gerçekleşmesi halinde oluşacak etkinin uygulanan kontroller ile azaltılması.
- **Riskin Transferi:** Riskin gerçekleşmesi durumunda oluşabilecek zararı karşılayacak çözümler bularak (örneğin sigorta yaptırmak) riskin başkalarına aktarılmasıdır.

2.5.2 Kontrollerin Uygulanması

Risk analizi sonrasında sistemdeki mevcut riskler ve bu risklere karşı kullanılabilecek olası kontroller belirlenmektedir. Fakat her risk önlem almaya değecek bir risk olmayabilir. Bu durumda hangi riskler için önlem alınacağı ve olası kontroller içerisinde hangisinin kullanılacağını belirlemek kurumun maliyetleri açısından çok önemlidir.(Eskiyörük D., 2007, s. 22)

- Yapılacak işin riskini indirmeye yönelik uygulanacak olan kontrolün, işin getirisinden fazla maliyete neden olması durumunda risk kabul edilir.
- Bunun dışındaki durumlarda riski indirmeye yönelik kontroller uygulanmalıdır.

2.5.3 Kontrollerin Uygulanmasında İzlenecek Yaklaşım

Kontroller, en büyük risklerden başlayarak, örgütün/kurumun süreçlerine en az zarar verecek, riski en aza indirecek ve en düşük maliyetli olacak şekilde seçilmelidir. Bu süreçte aşağıdaki adımlar izlenebilir. (Eskiyörük D., 2007, s. 24)

2.5.4 Risklerin Önceliklendirilmesi

Risk analizinde belirlenen risk seviyelerine göre riskler önceliklendirilmelidir. Risk işleme için kaynak aktarımı yapılırken öncelik yüksek dereceli risklere verilmeli, bu riski oluşturan açıklıklar ve tehditlere karşı önlemler daha önce alınmalıdır.

2.5.5 Uygun Kontrollerin Değerlendirilmesi

Riskler öncelendirildikten sonra bu riskler için daha önceden belirlenmiş kontroller değerlendirilmelidir. Belirlenen her kontrol en efektif veya en az maliyetli kontrol olmayabilir.

Bir fizibilite çalışması yapılarak riski en aza indirecek en uygun kontrol belirlenmelidir. Bu aşamada kontroller için maliyet-fayda analizi yapmak uygun olacaktır.

2.5.6 Kontrollerin Seçilmesi

Fizibilite çalışmasının ve maliyet-fayda analizinin sonuçlarına göre riski en aza indirecek en uygun kontroller, risk analizinde belirlenen kontroller arasından yönetim tarafından seçilir.

Seçilen kontroller teknik, yönetsel ve operasyonel kontrollerin bir araya getirilmesinden oluşturulmalıdır.

2.5.7 Sorumluların Atanması

Seçilen kontroller uygulanması için bu kontrolleri uygulama yetkinliğine sahip kişiler belirlenmeli ve bu kişilere sorumluluk atanmalıdır.

2.5.8 Kontrol İşleme/Uygulama Planının Hazırlanması

Seçilen kontrolün nasıl uygulanacağını, uygulamanın hangi adımları içereceğini ve ne kadar süreceğini belirleyen bir kontrol uygulama planı oluşturulmalıdır. Bu plan en az aşağıdaki kriterleri içermelidir:

- Riskleri ve risk seviyelerini
- Risk analizi sonucunda belirlenen kontrol önerilerini
- Önceliklendirmeleri
- Seçilen kontrolleri
- Gerekli kaynakları
- Kontrolü uygulamakla yetki ve sorumluluğu verilen kişileri
- Kontrolün uygulanması için belirlenen başlama ve bitiş tarihlerini

2.5.9 Seçilen Kontrolün Uygulanması

Hazırlanan uygulama planına uygun olarak seçilen kontroller uygulanmalıdır. Uygulanması uzun zaman alabilecek kontroller için uygulamanın gidişini değerlendirmek üzere uygun aralıklara toplantılar yapıp sonuçlar üst yönetime raporlanabilir.

2.5.10 Artık Risk Kavramı

Uygulanan kontroller var olan riski tamamen ortadan kaldırmak zorunda değildir(Humphreys E., 2008, s. 250). Risk işleme sonrası kalan riske artık risk adı verilir. Eğer bulunan risk seviyesi kabul edilebilir risk seviyesinin üzerinde ise risk analizi ve risk işleme tekrar yapılmalıdır, eğer bulunan artık risk seviyesi kabul edilebilir riskin altında ise artık risk dokümente edilmeli ve varlığı yönetim tarafından onaylanıp kabul edilmelidir.

2.5.11 Risklerin izlenmesi, yeniden değerlendirilmesi ve gözden geçirilmesi

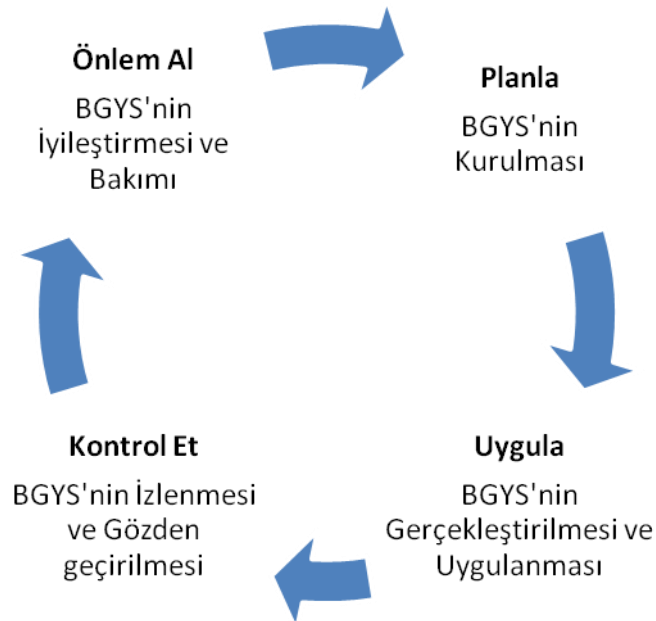
Risk yönetimi bir döngüdür ve burada belirtilen risk analizi ve risk işleme süreçleri periyodik olarak uygulanmalıdır. Bu sayede uygulanan kontrollerin amacına ne kadar ulaştığı belirlenmiş olur. Ayrıca bilişim teknolojileri ve çevresel faktörler çok hızlı değişmektedir. Kurum sistemine yeni dahil olan varlıkların risk yönetimine dahil edilmesi önem arz etmektedir. Bunlara ek olarak zaman içerisinde kurumun iş hedefleri, iş yapma şekli ve önem verdiği konular değişebilir. Bütün bu değişiklikler

varlıklarda, varlıkların değerlerinde, açıklıklarda ve tehditlerde değişiklik olmasına neden olur. Risk yönetim döngüsünün sürekli olarak işletilmesi tüm bu değişikliklerin getirdiği risklerin yönetim tarafından farkına varılmasını ve ele alınmasını sağlayacaktır. (Eskiyörük D., 2007, s. 26)

2.6 BGYS Kurulum Süreci

Bilgi Güvenliği Yönetim Sisteminin bir şirkete kurulması demek, ISO/IEC 27001:2005 BGYS Standardının şirkete uygulanması anlamına gelmektedir. Bilgi Güvenliği Yönetim Sistemi(BGYS) Standardının uygulanması için ne gibi gereksinimler olduğu ISO/IEC 27001:2005 BGYS Standardında tariflenmiştir. Bu standardın bir şirkete nasıl uygulanacağı ise bir kılavuz olan ISO/IEC 27002(Eski adı ISO 17799) de belirtilmiştir.

Bilgi Güvenliği Yönetim Sistemi süreç gereksinimleri, bir kuruluşun BGYS'yi, Şekil 2.2'deki gibi Planla-Uygula-Kontrol Et-Önlem Al (PUKÖ) modeline göre nasıl kuracakları ve sürdürecekleri ile ilgilidir. ISO/IEC 27001:2005 BGYS Standardının 4, 5, 6, 7 ve 8nci maddeleri, standart için olmazsa olmaz maddelerdir ve hepsinin istisnasız uygulanması gerekmektedir. Dolayısıyla bu maddelerde istisnalar kabul edilemez.



Şekil 2.2 PUKÖ Döngüsü (Humphreys E., 2008, s. 249)

ISO 27001:2005, Ek-A'da belirtilmiş olan BGYS gereksinimleri, risk değerlendirme ve risk kabul kriterleri, aksi kanıtlanmadığı sürece her organizasyon için uygulanmalıdır. Bu kontrol maddelerinde hariç tutmalar yapılabilir. Fakat bu hariç tutmaların geçerli nedenleri belirtilmelidir.

2.6.1 BGYS Sertifikasyon Süreci ve Bilgi Güvenliği Altyapısının Sağlanması

Örgüt/Kurum, ISO/IEC 27001:2005 BGYS Sertifikasını almak istiyorsa ISO 27001'in gerekliliklerini yerine getirmeli, bünyesine uygulamalıdır. Bu süreç Şekil 2.4'de anlatılmıştır.

Öncelikle ISO 27001 Bilgi Güvenliği Yönetim Sisteminin şirkete uygulanma kararının alınması ve bunun üst yönetim tarafından onaylanması gerekmektedir. Bununla ilgili sorumluluklar atanmalı ve projelendirme kararı alınmalıdır. Burada unutulmaması gereken önemli bir husus vardır. BGYS bir defa kurulup bırakılacak bir yönetim sistemi değildir. Sürekli yaşayan ve kendini yineleyen bir sistemdir.



Şekil 2.3 Bilgi Güvenliği Altyapı Bileşenleri (Eloff J.H.P. and Eloff M.M., 2005, s.13)

Örgüt/Kurum hizmet verdiği sektöre ve bunların getirdiği kanuni yükümlülükler göre ISO 27001 gerekliliklerini kendine uyarlayacak politikalarını ve prosedürlerini belirlemelidir. Öte yandan ISO 27001'in gerekliliklerinden olan BGYS'nin Örgütün/Kurumun hangi süreçlerine ve/veya bölümlerine uygulanacağını

tarifini yapan bir kapsam dokümanı da hazırlanmalıdır. Bunlar işin dokümantasyon tarafını oluşturur. Kalite Yönetim sistemi ışığında bu dokümantasyonların onay ve yayınlama aşamaları tamamlanmalıdır.

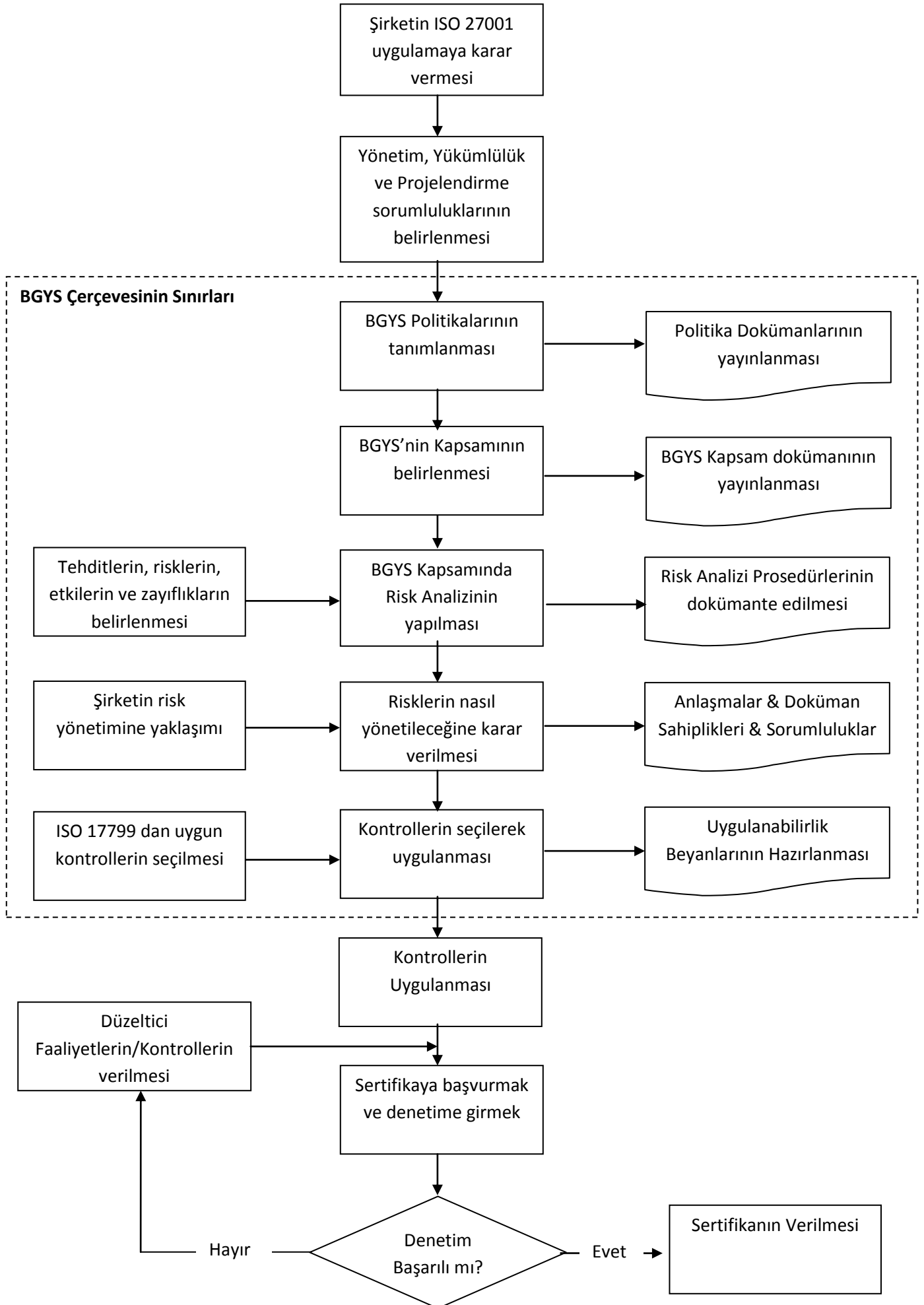
Örgütün/Kurumun faaliyet gösterdiği alanın getirmiş olduğu tehditleri ve riskleri belirlemek, bununla beraber örgütün/kurumun zayıflıklarını girdi olarak BGYS kapsamında risk analizi yapmak, örgüt/kurum içinde risk anlayışını oturtmak açısından gereklidir. Bununla beraber risklerin nasıl yönetileceğine karar verilmesi, örgütün/kurumun risk yönetim yaklaşımını ortaya koyacaktır. Tüm bunların ışığında risk yönetimi sonucu ortaya çıkan risklerin indirgenmesine yönelik ISO 27001'in EK-A'sındaki (Bu kontrollerin nasıl uygulanacağına dair rehberlik yapan ISO 17799 standardı göz önünde bulundurularak) kontrol maddelerinden uygun olanları seçilmelidir. Bu adımın çıktısı ise UB(Uygulanabilirlik Beyanı) dokümanı olacaktır. Bu doküman hangi varlık için hangi kontrol maddesi uygulandığını gösteren bir rehberdir.

Kontrollerin uygulanması yeteli değildir. Bununla birlikte bu kontrollerin etkinliğinin ölçülmesi de önem arz etmektedir. Öte yandan işletilmeye çalışılan BGYS, belirli periyotlarda gözden geçirilmelidir. Yapılan kontroller sırasında uygunsuzlukların ve/veya ilerleyen zaman içinde uygunsuzluk oluşturacak konuların ortadan kaldırılmasına yönelik Düzeltici/Önleyici Faaliyetler uygulanmalıdır.

Unutulmaması gereken diğer bir husus da Bilgi Güvenliği Yönetim Sistemini örgüt/kurum kültürü haline getirmek, bununla ilgili farkındalık faaliyetleri gerçekleştirmek ve bu kültürü organizasyonel hafızaya kazandırmaktır.

Tüm bunların sonucunda BGYS sisteminin çalıştığına emin olunduktan sonra sertifika başvurusunda bulunulabilir.

Örgütün/Kurumun yapılan dış denetimde ISO/IEC 27001:2005 standardına uygunluğu kontrol edildikten sonra belgelendirme yapılacaktır.



Şekil 2.4 ISO/IEC 27001:2005 BGYS Sertifikasyon Süreci (www.27000.org)

2.7 ITIL, COBIT ve ISO/IEC 27002 Çerçevelerinin Karşılaştırmaları:

Yönetim; insan kaynakları, finansal kaynaklar ve teknolojik kaynaklar olmak üzere bir kaç boyutu kapsar. Son zamanlarda yeni yönetim alanı Bilgi Teknolojileri Yönetimi(BT Yönetimi) olarak adlandırılmıştır. Bu Bilgi Teknolojileri ve Yönetim olmak üzere iki kolda değerlendirilmelidir.

Bilgi Teknolojileri, bir çok farklı perspektifte değerlendirilen boyutlara sahiptir(Sahibudin et al., 2008, s. 743):

1nci Bakış Açısı: BT sistemleri uygulamalar ve altyapılardan oluşur. Bunlar şirket süreçlerine ve servislerine entegre olarak çalışmaktadırlar.

2nci Bakış Açısı: BT organizasyonu çeşitli firma fonksiyonları, paylaşımlı servis birimleri ve kuruluş düzeyinde çekirdek birimleri gibi tiplerde olabilir.

3ncü Bakış Açısı: BT, firma tarafından kullanılan hizmetlerin bir kategorisidir. Bunlar tipik olarak BT uygulamaları ve altyapısıdır. Bu bakış açısıyla BT maliyetleri, işletme giderleri olarak değerlendirilir.

4ncü Bakış Açısı: BT firmanın değerli varlık kategorileri arasında yer almaktadır. Bu bakış açısı ile BT, yatırım maliyeti olarak değerlendirilir.

Yukarıdaki tüm bakış açıları BT'nin önemini vurgulamaktadır. Bu nedenle BT'yi yönetmek ve uygulamak organizasyonlarda önem arz etmektedir. Bunun için birçok standart, araç, çerçeve ve/veya en iyi deneyimler/uygulamalar mevcuttur ki BT hizmetlerinin bakımı ve yönetimi doğru, etkin ve verimli yapılabilsin. En yaygın olan standart ve/veya çerçeveler ISO/IEC 27002 (Bilgi Güvenliği Yönetim Sistemi en iyi uygulamaları), COBIT, ISO 20000 ve ITIL'dır. Her standart veya çerçevenin güçlü olduğu ama yetersiz de kaldığı yerler vardır. Bundan dolayı tek bir standart, kurumun iş süreçlerine ve bağlı bulunduğu sektöre göre yeterli gelmeyebilir. Dolayısıyla buradaki çözüm kurumun bağlı bulunduğu sektörsel ihtiyaçlara cevap verebilecek bir veya birden fazla standart/çerçeve ile çalışmak, eksik kaldıkları yerde diğeri ile tamamlamak olmalıdır. Önceki çalışmalara göre en iyi kombinasyon ITIL, COBIT ve ISO/IEC 17799 ile birlikte olanıdır. ITIL, BT sistemlerinde olması gereken bir standarttır(Sahibudin et al., 2008, s. 743). Bununla birlikte ISO/IEC 17799 yenilenmiş ve değiştirilmiştir. Şu an ISO/IEC 27002 olarak adlandırılmaktadır.

Iran Telecommunication Research Center(ITRC) tarafından, BT Yönetişiminde uygulanan ITIL, COBIT, COSO, TickIT, SAS, ISO 17799, ISO/IEC 17799:2000, NIST 800-14, ASL, SAC, SAS70, ISO/IEC TR 13335, ISO/IEC 15408 standartların/modellerin COBIT'in PO, AI, DS ve M parametrelerine göre yapılan araştırma sonuçları Tablo 2.2'de verilmiştir. Burada 13 BT Yönetişim aracı 1-10 değerleri arasında puanlanmıştır(Fasanghari et al., 2008, s. 516).

	PO	AI	DS	M
ITIL	3	5	9	0
COSO	7	5	6	0
ISO 17799	5	4	8	2
ISO/IEC 17799:2000	5	4	8	2
ISO/IEC TR 13335	4	2	4	2
ISO/IEC 15408:1999	1	3	2	2
TickIT	1	5	0	2
NIST 800-14	5	5	8	2
ASL	3	5	9	0
SAC	8	2	8	3
SAS70	8	2	5	2
SASs	8	2	5	3
COBIT	8	5	10	3

Tablo 2.2 Yönetişim Model/Standartların Puanları (Fasanghari et al., 2008, s. 516)

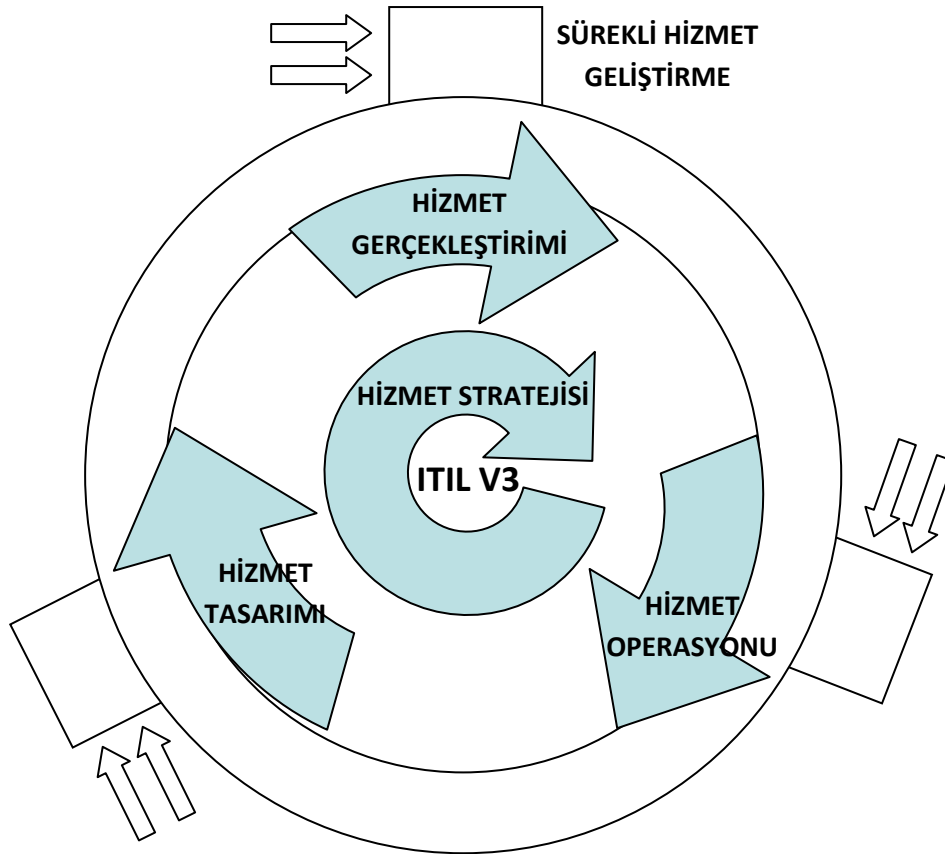
2.7.1 ITIL (Information Technology Infrastructure Library)

ITIL(Information Technology Infrastructure Library=Bilgi Teknolojileri Altyapı Kütüphanesi), Bilgi Teknolojileri için olması gereken bir standarttır. ITIL, dünyada çok geniş bir alanda en çok kabul edilen Bilgi Teknolojileri Hizmet Yönetimi yaklaşımını temsil eder (Sprenić et al., 2008, s. 244).

ITIL, Birleşmiş Krallık Ticaret Ofisi tarafından 1980'li yılların sonlarına doğru geliştirilmiştir. Hazırlanma amacı, Birleşik Krallık hükümetinde Bilgi İşlem

servis yönetimini iyileştirmektir. İlerleyen yıllar ile kendini yenilemeyi başaran ve alternatifi de bulunmayan ITIL, artık bir set kitap olmaktan öteye gitmiş ve hizmet yönetimi konusunda dünyaca kabul gören bir metodoloji haline gelmiştir (Hochstein et al., 2005, s. 704). ITIL şu anda Eğitim Programı, Sertifikalandırması, Danışmanlık hizmetleri, Yazılım Destek programları olan uluslararası bir standarda dönüşmüş durumdadır.

ITIL, ISO/IEC 20000 standardıyla birlikte entegre bir yaklaşıma sahiptir ve aşağıdaki konulara rehberlik eder(Sahibudin et al., 2008, s. 744):



Şekil 2.5 ITIL'ın Yaşam Döngüsü (Nabiollahi and Sahibuddin, 2008, s.2)

2.7.1.1 Hizmet Stratejisi

Hizmet Stratejisi, hizmet yönetiminin nasıl dizayn edildiğine, geliştirildiğine ve uygulandığına dair rehberlik eder. Tabi tüm bunlar yapılırken organizasyonun bakış açısı yeteneğine ve stratejik varlıklarına göre hareket edilir. (Wagner H.-T., 2006, s. 4) Hizmet Stratejisi bu bölümleri kapsar: İç ve Dış piyasaların geliştirilmesi,

hizmet varlıkları, hizmet katalogu ve stratejinin uygulanması, hizmeti aracılığıyla yaşam döngüsü.

Hizmet Stratejisi aşağıdaki süreçleri barındırır:

- Finansal Yönetim
- Hizmet Portföy Yönetimi
- Talep Yönetimi

Bu bölüm, aşağıdaki bazı soruların cevapları için rehberlik edebilir(Nabiollahi and Sahibuddin, 2008, s.2):

- Hangi hizmetler kime ve nasıl sunulmalıdır?
- Müşterilerim için gerçek değeri nasıl oluştururum?
- Paydaşlarım için değeri nasıl yakalarım?
- Stratejik yatırımları gerçekleştirecek nasıl bir durum oluşturabilirim?
- Finansal Yönetim, değer yaratma üzerinde nasıl görünürlük ve kontrol sağlayabilir?
- Hizmet kalitesini nasıl tanımlamak gerekir?

2.7.1.2 Hizmet Tasarımı

Hizmet Tasarımı, hizmet ve hizmet yönetim süreçlerinin nasıl geliştirileceğini ve nasıl dizayn edileceğini tanımlar. Bu madde, hizmet ve hizmet varlıkları portföylerinin yönetimi için yöntem ve prensipleri içerir. Hizmet Tasarımı, esasında yeni bir hizmet tasarlamak anlamına gelmez. (Wagner H.-T., 2006, s. 4) Mevcut hizmetlerin yaşam döngülerini ve hizmet seviyelerini müşteriler için daha değerli ve uygun hale getirmeyi amaçlar. Tüm bunların ilgili standartlar ve yasal zorunluluklara uygunluğu da gözden kaçırılmaz. (Nabiollahi and Sahibuddin,, 2008, s.3)

Hizmet Tasarımı aşağıdaki süreçleri içerir(Sahibudin et al., 2008, s. 750):

- Servis Katalog Yönetimi
- Hizmet Seviyesi Yönetimi
- Kapasite Yönetimi
- Stok Yönetimi
- BT Hizmet Sürekliliği Yönetimi
- Bilgi Güvenliği Yönetim,
- Tedarikçi Yönetimi,
- Uygulama Yönetimi
- Veri ve Bilgi Yönetimi

- İş Hizmet Yönetimi

2.7.1.3 Hizmet Gerçekleştirimi

Hizmet Gerçekleştirimi, yeni ve değiştirilmiş hizmet operasyonlarının gerçekleştirim kapasitelerini artırmak ve geliştirmek noktasında rehberlik eder (Wagner H.-T., 2006, s. 5). Kullanıcılar Hizmet Yönetimiyle ilgili pratik içeriğe ait Yayın Yönetimi, Program Yönetimi ve Risk Yönetimi gibi konuları pratik etmekte kullanırlar (Nabiollahi and Sahibuddin, 2008, s.3).

Hizmet Gerçekleştirim süreçleri aşağıdaki gibidir(Sahibudin et al., 2008, s. 750):

- Değişim Yönetimi
- Hizmet varlık ve Yapılandırma Yönetimi
- Yayın ve Dağıtım Yönetimi
- Bilgi Yönetimi
- Paydaş Yönetimi
- Geçiş Planlama
- Destek ve Hizmet Değerlendirme

2.7.1.4 Hizmet Operasyonu

Hizmet Operasyonunun yönetimini konu alır. Müşteri ve servis sağlayıcılar için teslimat ve destek aşamalarındaki etkinliğin ve efektifliğin oluşturulması noktasından rehberlik eder (Nabiollahi and Sahibuddin, 2008, s.3).

Bu işlemler şunlardır(Sahibudin et al., 2008, s. 750):

- Olay Yönetimi
- Vaka Yönetimi
- Talep Yönetimi
- Problem Yönetimi
- Erişim yönetimi

2.7.1.5 Sürekli Hizmet İyileştirme

Müşterilere verilen hizmetlerin tasarımı, içeriği ve operasyonunu daha iyi hale getirmek için neler yapılması gerektiği noktasında rehberlik eder. Kalite yönetimi, Değişiklik Yönetimi ve Kapasite artırımı gibi konularda metotlar, pratikler ve prensiplerin kombinasyonunu sağlar(Nabiollahi and Sahibuddin, 2008, s.3).

Eğer ITIL V2 ve V3 karşılaştırılırsa, V3 deki Hizmet Gerçekleştirimi ve Hizmet Operasyonu gibi başlıkların, V2 deki Hizmet Sunumu ve Hizmet Desteği gibi konularla benzer oluşunu görürüz. (Wagner H.-T., 2006, s. 6) Bununla birlikte Hizmet Stratejisi ve Hizmet Sunumu konuları yeni bölümlerdir ki ITIL V2 nin majör zayıflıkları, ITIL V3 de kabul edilmiş ve beklide çözülmüştür(Nabiollahi and Sahibuddin, 2008, s.3).

2.7.2 COBIT (Control Objectives for Information and Related Technology)

COBIT(Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri), 1992’de Bilgi Sistemleri Denetim ve Kontrol Birliği(ISACA) ve Bilgi Teknolojileri Yönetişim Enstitüsü(ITGI) tarafından Bilgi Teknolojileri Yönetimi için en iyi uygulamaları içinde barındıran bir çerçeve olarak oluşturulmuştur(Sahibudin et al., 2008, s. 751).

COBIT, temelde “süreç” değil, “kontrol” esaslıdır. Bu nedenle COBIT, şirketlerin işleri nasıl gerçekleştirdikleriyle değil, neler yapmaları gerektiğiyle ilgilenir. “İş Yönetimi”, COBIT çerçevesinin temelini oluşturur. COBIT sadece kullanıcı ve denetçiler için değil, başta yöneticiler olmak üzere iş sürecine dahil olan herkes için kapsamlı bir yol göstericidir. COBIT çerçevesi, Bilgi Sistemleri Kaynakları’nın yönetilmesi için ihtiyaç duyduğu bilgiyi sağlayan gruplanmış süreçler olarak da tanımlanabilir (Fasanghari et al., 2008, s. 516).

COBIT, 4 grup altında ve 34 adet ana kontrol hedefi oluşturmaktadır. Bu guruplar aşağıdaki gibidir (Fasanghari et al., 2008, s. 516):

- Planla ve Organize Et
- Tedarik ve Uygulama
- Teslimat ve Destek
- İzle ve Değerlendir

2.7.2.1 Planla ve Organize Et

Bu bölüm, bir kurumun hedeflerini ve amaçlarını yerine getirebilmesi için teknolojiyi nasıl kullanması gerektiği noktasında yardımcı olur. BT’nin kullanımından en iyi sonuçları alarak fayda sağlamak için BT’nin organizasyonel ve

altyapısal şekline işaret eder. (Sahibudin et al., 2008, s. 751) Planlama ve Organizasyon bölümü için üst seviye kontroller Tablo 2.3'deki gibidir(COBIT 4.1, 2007, s.33):

PO	Planla ve Organize Et
PO1	Stratejik BT Planının Tanımlanması
PO2	Bilgi Mimarisinin Tanımlanması
PO3	Teknolojik Yönün Belirlenmesi
PO4	BT Organizasyon ve İlişkilerinin Tanımlanması
PO5	BT Yatırımlarının Yönetimi
PO6	Yönetimin Hedeflerinin ve Talimatlarının İletilmesi
PO7	İnsan Kaynakları Yönetimi
PO8	Kalite Yönetimi
PO9	BT Risklerinin Değerlendirilmesi ve Yönetimi
PO10	Proje Yönetimi

Tablo 2.3 Planla ve Organize Et

2.7.2.2 Tedarik ve Uygulama

Buradaki amaç, kurumun mevcut iş süreçlerini içeren ve bunlar için gerekli olan teknoloji ve uygulamaları barındıran BT ihtiyaçlarını tanımlamaktır. Bu bölüm aynı zamanda bakım planlarının geliştirilmesini adresler ki kurum, BT sistem ve bunun komponentlerinin ömrünü uzatmaya kendini adapte etmelidir. (Sahibudin et al., 2008, s. 751) Tedarik ve Uygulama bölümü için üst seviye kontroller Tablo 2.4'deki gibidir (COBIT 4.1, 2007, s.78):

AI	Tedarik ve Uygulama
AI1	Otomasyon Çözümlerinin Belirlenmesi
AI2	Uygulama Yazılımı Tedarik Edilmesi ve Bakımı
AI3	Teknoloji Altyapısının Tedarik Edilmesi ve Bakımı
AI4	İş ve Kullanımın Etkin Kılınması
AI5	BT Kaynaklarının Sağlanması
AI6	Değişiklik Yönetimi
AI7	Çözüm ve Değişikliklerin Kurulması ve Kabul Edilmesi

Tablo 2.4 Tedarik ve Uygulama

2.7.2.3 Teslimat ve Destek

Teslimat ve Destek Süreç Alanı, BT'nin teslimat durumlarına odaklanır. Uygulamaların BT sistemi içinde yürütülmesi ve sonuçlarıyla olduğu kadar, BT sistemlerinin etkili ve yeterli işletilmesine olanak sağlayan destek süreçlerini de kapsar. (Sahibudin et al., 2008, s. 751) Destek süreçleri; güvenlik konuları ve eğitimi içerir. Teslimat ve Destek bölümü için üst seviye kontroller Tablo 2.5'deki gibidir(COBIT 4.1, 2007, s.107):

DS	Teslimat ve Destek
DS1	Hizmet Düzeyi Belirleme ve Yönetimi
DS2	Üçüncü Parti Hizmet Yönetimi
DS3	Performans ve Kapasite Yönetimi
DS4	Sürekli Hizmetin Sağlanması
DS5	Sistem Güvenliğinin Sağlanması
DS6	Harcamaların Belirlenmesi ve Bütçelenmesi
DS7	Kullanıcı Eğitimi
DS8	Kullanıcılara Yardım ve Danışmanlık
DS9	Konfigürasyon Yönetimi
DS10	Problem ve Olay Yönetimi
DS11	Veri Yönetimi
DS12	Fiziksel Çevre Yönetimi
DS13	Operasyon Yönetimi

Tablo 2.5 Teslimat ve Destek

2.7.2.4 İzle ve Değerlendir

Bu bölüm, kurumun hedefleri doğrultusunda dizayn edilmiş BT sistemlerinin gerekli olan kanuni zorunluluklar ve politikalara uygunluğunu kontrol eder. BT sistemlerinin etkinliğinin değerlendirilmesinden bağımsız olarak BT nin iş hedefleri ile doğru istikamette olup olmadığını ve bununla ilgili kontrol süreçlerinin doğru kurgulanıp kurgulanmadığını hem iç hem de dış denetçilerle nasıl izlendiğini kapsar. (Sahibudin et al., 2008, s. 751) İzleme ve Değerlendirme bölümü için üst seviye kontroller aşağıdaki Tablo2.6'deki gibidir(COBIT 4.1, 2007, s.160):

ME	İzle ve Değerlendir
ME1	Süreç İzleme
ME2	İç Kontrol Değerlendirme Yeterliliği
ME3	Bağımsız Güvence Elde Edilmesi
ME4	Bağımsız Denetimin Sağlanması

Tablo 2.6 İzle ve Değerlendir

COBIT'in 4 temel Süreç Alanının altında toplam 34 adet BT süreci bulunmaktadır. Bu BT süreçleri 318 adet detaylı kontrol amacı içermektedir. COBIT, BT süreçlerini aşağıdaki bilgi kriterleri ve bilgi kaynakları ile ilişkilendirilir.

Bilgi kriterleri(COBIT 4.1, 2007, s.10)

- **Etkililik**

Bilginin iş süreçleri ihtiyaçları ile ilgili ve bu ihtiyaçlara cevap verir nitelikte olması.

- **Verimlilik**

Bilgi kaynakların en etkin kullanımı ile elde edilmesi.

- **Gizlilik**

Hassas bilginin yetkisiz erişime karşı korunması.

- **Bütünlük**

Bilginin kendi içinde ve çevresel veriler ile bütünlük göstermesi, yetkisiz değişikliğinin engellenmesi.

- **Devamlılık**

Bilginin ihtiyaç duyulduğunda erişilebilir olması.

- **Uyumluluk**

İş süreçlerinde kanun, düzenleme ve kontratlara uyumun sağlanması.

- **Güvenilirlik**

Yönetimin finansal ve diğer raporlamalar için güvenilir veriye ulaşabilmesi.

Bilgi kaynakları

- **İnsan Kaynakları**

BT personel yetenekleri, bilinç, bilgi sistemleri planlama, organizasyon, uygulama, destek, gözetim üretkenliği.

- **Uygulama Sistemleri**

Manuel ve programlanmış iş süreçlerinin tümü.

- **Teknoloji**

Donanım, işletim sistemi, veritabanı yönetim sistemi, bilgi ağı ve diğer teknoloji altyapısı.

- **Fiziksel Ortam**

Bilgi sistemlerini barındıran ve koruyan fiziksel ortamlar.

- **Veri**

En geniş anlamıyla, iç, dış veri türlerinin tamamı.

COBIT, dört Süreç Alanında gruplanmış 34 adet BT sürecini ele alır. Bu dört grup; Planla ve Organize Et, Tedarik ve Uygulama, Teslimat ve Destek İzle ve Değerlendirir şeklindedir. (COBIT 4.1, 2007, s.12)

Her bir sürecin 0-5 arası bir olgunluk seviyesi vardır. Bu ölçek, bir organizasyondaki sürecin olgunluk seviyesi, o sürecin hangi olgunluk seviyesinde olması gerektiği, hangi seviyenin en iyi uygulama olarak varsayıldığı ve diğer organizasyonların ne seviyede olduğu gibi anahtar değerlendirmeler için kullanılır.

Olgunluk modelleri(COBIT 4.1, 2007, s.19);

0 Olmayan: Tanımlanmış süreç bulunmamaktadır.

1 Başlangıç: Organize olmayan ve standartlaşmamış fakat kurumda farkındalığın mevcut olduğu, adresleme ve standartlaştırma ihtiyacının tespit edildiği seviyedir.

2 Tekrarlanan: Bireye dayalı ve tekrarlanan işleri farklı kişilerin aynı şekilde yapabildiği seviyedir. Bu seviyede formal eğitim ve iletişim metodları belirlenmemiş fakat sorumluluk büyük oranda kişiye bağlı kılınmıştır.

3 Tanımlı: Prosedürler standartlaşmış ve dokümente edilmiş, eğitim aracılığı ile kurum içinde iletilmiştir. Ancak bu süreçleri izleyip izlememe kararı kişinin kendisine bırakılmıştır. Bu nedenle yapılan işler arasında çeşitli farklılıklar mevcuttur. Prosedürlerin kendisi gelişmiş değildir. Ancak mevcut uygulamaların biçimselleştirilmiş halidir.

4 Yönetilen: Prosedürlerle uyumu izlemek ve ölçmek, süreçlerin etkin çalışmadığının anlaşılması durumunda faaliyete geçmek mümkündür. Süreçler sürekli gelişmekte ve iyi uygulamaların tanımlanması sağlanmaktadır. Otomasyon ve araçlar kısıtlı veya parçalı bir biçimde kullanılabilmektedir.

5 Optimize: Süreçler en iyi uygulamalar seviyesine indirgenmiş, sürekli gelişim ve olgunluk modelleme konusunda diğer şirketlerin sonuçları ile çalışmaktadır. BT, iş akışlarının otomatize edilmesi, kalite ve etkinliğin artırılması ve kurumun çabuk adapte olabilmesi için entegre olmuştur.

2.7.3 ISO/IEC 27002

ISO/IEC 27002, bilgi güvenliği yönetim sistemi standardıdır. Bu standart Bilgi Güvenliği Yönetim Sistemindeki pratik uygulamaları konu alan bir rehber niteliğindedir. Güvenlik kontrol hedeflerini ve bu kontrollere özel tavsiyeleri, en iyi uygulamaları içerir (Gerber and Solms, 2008, s.125). Bir kurum, ISO/IEC 27002 standardını kendi bünyesine uygulayabilir fakat bu uygunluğu sertifikalandırması isteğe bağlıdır(Sahibudin et al., 2008, s. 752).

ISO/IEC 27001 standardında tarif edilen döngü, ISO/IEC 27002 standardından seçilen önlemler için çalıştırılarak bilgi güvenliği süreci gerçekleştirilmeye ve yaşatılmaya çalışılmaktadır. Bilgi güvenliğinde esas olanın ISO/IEC 27001 süreci olduğu, bu süreçten kopuk, dolayısı ile ölçülmeyen, kayıtların oluşturulmadığı, tetkik ve gözden geçirmelerin yapılmadığı, düzeltici ve önleyici

faaliyetlerin gerçekleştirilmediği bir sistemde önlemlerin kuruma hizmet etmeyeceği rahatlıkla söylenebilir.

Bilgi güvenliği, ISO/IEC 27001 standardında tarif edilen döngünün ISO/IEC 27002 standardında açıklanan önlemler için çalıştırılması ile sağlanmaktadır. İlgili döngü Şekil 2.6'de gösterilmiştir. Bu konuda esas olanın ISO/IEC 27001 süreci olduğunu, risk analizi gerçekleştirilmeden devreye sokulan önlemlerin kuruma hizmet etmesinin tesadüflere bağlı olacağını söylemek yanlış olmaz (Humphreys E., 2008, s. 248). ISO/IEC 27002 standardında açıklanan öncelikli önlemlerin her kurumun kendi süzgecinden geçirilmesi ve uygulanması ile bilgi güvenliğine büyük katkı sağlanacaktır.

ISO 27001 temelli Bilgi Güvenliği Yönetim Sistemi'nin temele bakış açısı aşağıdaki gibi tanımlanabilir (Tvrdíková M., 2008, s. 154):

- Bilgi Teknolojileri Güvenlik Politikalarının geliştirilmesi,
- Organizasyonda rol ve sorumlulukların belirlenmesi,
- Bilgi sistemlerinin konfigürasyon yönetiminin yapılması,
- Değişiklik yönetiminin yapılması,
- Tüm çalışanların bilgi sistemleri güvenliği konusunda farkındalığının sağlanması,
- Uygun güvenlik kontrollerinin seçilmesi ve etkinliği ölçülmesi,
- Felaket sonrası sistem ve veri kurtarma planlarının, iş sürekliliği planlarının oluşturulması,
- Varlıklar, bunlara ait riskler ve bu riskleri indirgeyecek kontroller atanmalıdır. Zayıflıkları, bunlardan kaynaklı tehditler ve etkileri değerlendirilmeli, risk işleme planları belirlenerek kontroller uygulanmalı, artık riskler yönetilmelidir.
- Bilgi Güvenliği süreçleri süresince, kontrollerin etkinliğinin izlenmesi, bakım, güvenlik denetimleri gibi faaliyetlerde yerine getirilmelidir.

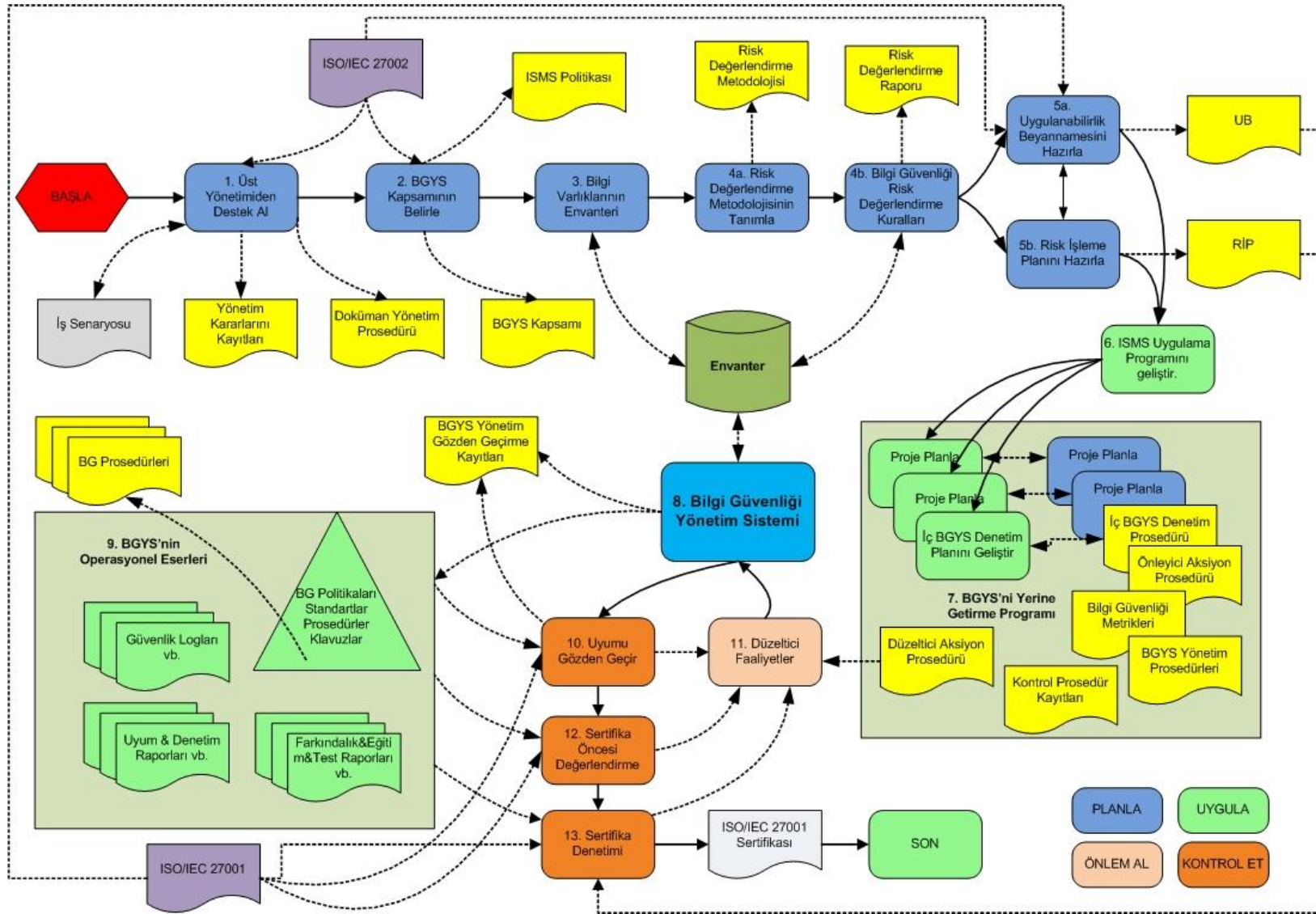
BGYS uygulamalarını teknik olan uygulamalar ve teknik olmayan uygulamalar olmak üzere iki bölüme ayırmak mümkündür (Solms S.H., 2005, s.444): Teknik Uygulamalardan bazıları:

- Mantıksal erişimlerin yönetimi: Erişim kontrol listeleri ile, gerçek erişimlerin artırılması, silinmesi veya değiştirilmesi.

- Kimlik belirleme ve doğrulama yönetimi: Kullanıcıların kimlik doğrulama veritabanına eklenmesi, değiştirilmesi ve silinmesi.
- Güvenlik duvarı yönetimi: Konfigürasyonun doğru yapılması, kuralların doğru tanımlanması.
- Virüs ve zararlı yazılımların yönetimi: Anti-Virüs programlarının sistemlere kurulması ve belirli periyotlarda güncellenmeleri.
- Güvenlik vakalarının yönetilmesi.
- İş istasyonlarının ve sunucuların güvenlik ayarlarının ve konfigürasyonlarının yapılması ve güncellenmesi.
- UPS sisteminin devamlılığının sağlanması.
- Sistemlerin yedeklerinin alınması ve bu yedeklerin güvenliğinin sağlanması.

Teknik Olmayan Uygulamalar(Solms S.H., 2005, s.445):

- Bilgi Güvenliği politikalarının ve prosedürlerinin oluşturulması.
- Tüm kullanıcılar için Bilgi Güvenliği farkındalık programlarına dahil edilmesi, ilgili risklerden haberdar edilmesi, Bilgi Güvenliği rol ve sorumluluklarının kendilerine beyan edilmesi.
- Tüm Bilgi Güvenliği politika ve prosedürleri, kanuni regülasyonlarla uyumlu olmalı, BT riskleri yönetilebilir olmalıdır.



Şekil 2.6 BGYS Süreci (27K implementers' Forum, 2009)

2.7.4 ITIL ve COBIT ilişkisi

COBIT'in yönetime yönelik yaklaşımı ITIL'dan daha farklıdır. Ancak, ikisi de birbirini tamamlamaktadır ve COBIT'in son versiyonu ITIL ile daha da entegre hale gelmiştir. ITIL, BT'de süreçlere daha odaklıdır. COBIT ise ITIL süreçlerini içerir, ancak olay yönetimini bir üst seviyeye taşıyarak, iş ihtiyaçlarının nasıl karşılanacağını hedef alır. İkisi birlikte uygulandığında ihtiyaçlarının BT ile örtüşmesi sağlanmış olur. Böylece masrafların ölçülmesi ve hizmet seviyeleri ile performans hedeflerinin bütünlüğü daha rahat sağlanmış olacaktır. COBIT “en iyi uygulamaları” bir araya getirerek BT birimlerine katma değerlerini sunma imkanı tanımaktadır. (Nicho and Cusack, 2007, s.1)

BT hizmetlerinde kaliteyi yakalamanın yolu, BT süreçlerinin tanımlanmasından, standartlaştırılmasından ve sürekli iyileştirilmesinden geçer. Bu anlamda, ITIL uygulamaları ve COBIT standartları; süreç odaklı olması, temel BT süreçlerini kapsayan bir bütünlüğe sahip olmaları, süreçleri entegre etmeleri ve hizmet kalitesi ile müşteri memnuniyetini öncelikli olarak dikkate almalarından dolayı her sektörden kurumların uygulaması gereken gerekliliklerdir.

2.7.5 COBIT ile ISO/IEC 27001:2005 ilişkisi

Tablo 2.7'de COBIT ile ISO/IEC 27001:2005 arasındaki ilişkinin nasıl kurulduğu, hangi noktalarda birbirleri ile benzerlik gösterdikleri/kesiştikleri ifade edilmiştir(Broderick J.S.,2006, s.27). Kurumun hangi sektörde faaliyet gösterdiği ve hangi kanuni zorunluluklara tabii olduğu göz önüne alınarak bu iki kabul görmüş çerçeve arasındaki ilişkileri yeniden şekillendirmek mümkün olacaktır (Solms B., 2005, s.100).

ISO 27001:2005	COBIT
Güvenlik Politikası	PO1: Stratejik BT Planının Tanımlanması PO3: Teknolojik Yönün Belirlenmesi

	PO6:Yönetimin Hedeflerinin ve Talimatlarının İletilmesi M1: Süreç İzleme
Bilgi Güvenliği Organizasyonu	PO2: Bilgi Mimarisinin Tanımlanması PO4:BT Organizasyon ve İlişkilerinin Tanımlanması M1: Süreç İzleme
Varlık Yönetimi	PO9:BT Risklerinin Değerlendirilmesi ve Yönetimi PO3:Teknolojik Yönün Belirlenmesi PO8:Kalite Yönetimi M1: Süreç İzleme
İnsan Kaynakları Güvenliği	PO7:İnsan Kaynakları Yönetimi DS7: Kullanıcı Eğitimi M1: Süreç İzleme
Fiziksel ve Çevresel Güvenlik	DS12: Fiziksel Çevre Yönetimi PO9: BT Risklerinin Değerlendirilmesi ve Yönetimi AI4: İş ve Kullanımın Etkin Kılınması AI6: Değişiklik Yönetimi M1: Süreç İzleme
Haberleşme ve işletim Yönetimi	AI3:Teknoloji Altyapısının Tedarik Edilmesi ve Bakımı AI4:İş ve Kullanımın Etkin Kılınması PO3:Teknolojik Yönün Belirlenmesi M1:Süreç İzleme
Erişim Kontrolü	PO6:Yönetimin Hedeflerinin ve Talimatlarının İletilmesi DS1:Hizmet Düzeyi Belirleme ve Yönetimi DS2:Üçüncü Parti Hizmet Yönetimi DS3:Performans ve Kapasite Yönetimi DS5:Sistem Güvenliğinin Sağlanması DS7:Kullanıcı Eğitimi DS8:Kullanıcılara Yardım ve Danışmanlık DS9:Konfigürasyon Yönetimi DS10:Problem ve Olay Yönetimi M1:Süreç İzleme
Bilgi Sistemleri Edinim, Geliştirme ve	AI1:Otomasyon Çözümlerinin Belirlenmesi AI2:Uygulama Yazılımı Tedarik Edilmesi ve Bakımı

Bakım	AI3:Teknoloji Altyapısının Tedarik Edilmesi ve Bakımı AI4:İş ve Kullanımın Etkin Kılınması AI5:BT Kaynaklarının Sağlanması AI6:Değişiklik Yönetimi M1:Süreç İzleme
Bilgi Güvenliği İhlal Yönetimi	DS7:Kullanıcı Eğitimi DS8:Kullanıcılara Yardım ve Danışmanlık DS9:Konfigürasyon Yönetimi DS10:Problem ve Olay Yönetimi M1:Süreç İzleme
İş Sürekliliği	PO3:Teknolojik Yönün Belirlenmesi DS1:Hizmet Düzeyi Belirleme ve Yönetimi DS2:Üçüncü Parti Hizmet Yönetimi DS3:Performans ve Kapasite Yönetimi DS5:Sistem Güvenliğinin Sağlanması DS13:Operasyon Yönetimi M1:Süreç İzleme
Uyum	PO8: Kalite Yönetimi M1:Süreç İzleme M2:İç Kontrol Değerlendirme Yeterliliği M3:Bağımsız Güvence Elde Edilmesi M4: Bağımsız Denetimin Sağlanması

Tablo 2.7 ISO 27001-COBIT İlişkisi (Broderick J.S.,2006, s.29)

3. BGYS, FİRMA PERFORMANSI İLİŞKİSİ

Örgütlerde bilgi, en değerli varlıklardan biri olarak düşünülmelidir. Gerekli koruma olmazsa bilgi:

- Yetkisi olmayan kişilerin eline geçebilir, sızdırılabilir veya ifşa edilebilir,
- Değiştirilebilir ve böylece daha az değerli hale getirilebilir,
- Bilgi iz veya geri kazanım umudu bırakmadan kaybolabilir,
- İhtiyaç olduğunda ulaşılamayabilir.

Bilgi, örgütün tüm diğer önemli iş varlıkları gibi korunmalı ve uygun biçimde yönetilmelidir. Tüm bu belirtilen amaçlar, Bilgi Güvenliğinin esası olan bilginin gizlilik, bütünlük ve erişilebilirlik(kullanılabilirlik) unsurlarının korunması gerektiğini sonucunu doğurmaktadır (Kajava et al., 2006, s. 2092).

Bununla birlikte Bilgi Güvenliği Yönetim Sisteminin uygulanması işletmeler açısından masrafları ve riskleri yönetmek gibi önemli katkılarda bulunur. Tüm bunlar aşağıdaki durumları etkiler (Ashenden D., 2008, s.197):

- Bilginin gizliliği, bütünlüğü ve erişilebilirliği(kullanılabilirliği) nin sağlanması,
- Müşteri bağlılığının/sadakatinin sağlanması,
- Çalışan bağlılığının/sadakatinin sağlanması,
- İşin devamının sağlanması,
- Gelir ve Pazar payı gibi işletme sonuçlarını,
- Kurumun Bilgi Varlıklarına yönelik tehditlerin ve zayıflıklarının düzenli olarak gözden geçirilmesi,
- Kaynakların etkili ve verimli kullanılması,
- Hedefe ulaşmak için süreçlerin belirlenmesi,
- Artan kurumsal güç ile rekabet avantajı,
- Kuruluşun performansı, ürün yaşam döngüsü ve itibarı ile göstermiş olduğu finansal ve sosyal faydalardan dolayı ilgili tarafların kurumun etkinliği ve verimliliğine olan güveni,

Bahsedilenlerin ışığında Bilgi Güvenliği Yönetim Sistemlerinin işletmelerin başarı ve performansları üzerinde önemli bir etkiye sahip olmaları beklenmektedir. Nitekim örgütlerin amacı, müşterilerinin ve ilgili taraflarının(kuruluş içindeki çalışanların, tedarikçilerin, sahiplerinin ve toplumun) ihtiyaçlarını ve beklentilerini tespit etmek ve karşılamak; rekabet avantajı elde etmek; bunları etkili ve verimli bir şekilde başarmak ve öylece kurumsal performansını ve gücünü kazanmak, sürdürmek, iyileştirmektir. Bilgi Güvenliği Yönetim Sistemleri ise firmalara bu noktalardan katkıda bulunarak işletme performansını arttırmaktadır. Ancak bu ifadelerin de vurguladığı üzere bu ilişkinin direk bir ilişki olmak yerine çeşitli değişkenler aracılığı ile gerçekleşen dolaylı bir ilişki olması beklenmektedir. Bilgi Güvenliği Yönetim Sistemleri süreç üzerinde etkili olduğu ve uzun dönemde gerçekleşebildiği için böylesi bir dolaylı ilişkinin karşımıza çıkması daha olasıdır.

Bu araştırmada şirket performansı ile bilgi güvenliği yönetim sistemleri ilişkisi incelenirken; Ashenden'in (2008) konu ile ilgili çalışmasından yola çıkılarak müşteri memnuniyeti, örgütsel bağlılık, çalışan memnuniyeti ve süreç yaklaşımı unsurları; ara değişken olarak ele alınmaktadır. Bu değişkenler, aşağıda detaylı bir şekilde tanımlanmaktadır.

3.1 Müşteri Memnuniyeti

Bir firmanın iyi işlediğini gösteren performans kriterleri ve bunların önem dereceleri gün geçtikçe değişmektedir. Firmaların kâr düzeylerinin göstergesi olan yıllık üretim gibi geleneksel performans kriterleri, yerini sahip olunan ve üretilen bilgi, teknolojinin kullanımı, müşteri profili ve müşteri memnuniyeti, üretilen ürün ve hizmet kalitesi, çevreye gösterilen duyarlılık gibi kriterlere bırakmaya başlamıştır. Somut olan, ölçülmesi daha kolay olan kriterler yerine; daha az somut, ölçülmesi ve modellenmesi zor olan kriterler ön plana çıkmaya başlamıştır (Türkyılmaz ve Özkan, 2003; s:1-6). Bu nedenle günümüzde işletmeler için, müşterinin memnun edilmesi stratejisi önemli bir duruma gelmiştir.

Müşteri memnuniyetini ölçmek için, müşterinin kim ve memnuniyetin ne demek olduğunun bilinmesi önemlidir. Belirtmeliyiz ki her zaman kaliteye bakışları farklı olan çok değişik müşteriler vardır ve hiçbir müşterinin memnuniyetsizliği, ille de her müşterinin memnun olduğu anlamına gelmez (Yoshio, 2001; s.871).

Müşteri memnuniyeti, en genel anlamıyla bir ürün veya hizmetin kullanım sonrası müşterinin sergilediği davranış olarak tanımlanmaktadır (Solomon, 1996: 346). Müşteri memnuniyeti; tüketicinin satın aldığı ürünün istek ve ihtiyaçlarına uygun olup olmaması ve tüketicinin ihtiyaçlarını/beklentilerini karşılama derecesinin ölçüsü olarak da tanımlanabilir (Bai et.al, 2008, s.293).

Müşteri memnuniyeti veya diğer bir deyişle müşteri tatmini, şüphesiz ki işletmeler için en önemli stratejilerden biridir. 1980’li yıllardan bu yana, gelişmiş ülkelerin firmaları tarafından tartışılan ana konulardandır. Firmaların kârlılığı, pazar payları ve büyüme oranlarında en önemli etken olan müşteri memnuniyeti, temel olarak firma sadakatine (loyalty) bağlıdır.

Geçmişten günümüze kadar, Toplam Kalite Yönetimi (TKY) anlayışının oluşumunun temel alt yapısını oluşturan müşterinin memnun edilme olgusu, bütünsel işletme performansının ve toplam kalite anlayışının en önemli göstergelerinden biridir (Forza and Filippini, 1998; s:1-20). Müşteri memnuniyeti, müşteri

beklentilerinin karşılanması amacıyla ihtiyaçları anlama, yönetme ve onlara etki etmedir. Projeden beklenenlerin sağlanması, son kullanıcının ürün kullanımında problemler yaşamaması, müşterinin iş gereği kurumla paylaştığı kişisel ve/veya özel bilgilerin mahremiyetinin sağlanması, müşteriye kesintisiz hizmet verilmesi ana hedeflerdir.

Artık işletmeler müşterilerini tanımak ve onların isteklerine göre üretimini yönlendirebilmek için müşteri bilgilerini sürekli olarak takip edip bu bilgileri değerlendirmeye başlamışlardır. Hatta çoğu işletme her yıl müşterilerinin ne oranda memnun olduklarını belirleyebilmek için müşteri anketleri yapmaktadır. Bu anlamda, işletmenin başarısı müşterilerin memnun olup olmamasına da bağlıdır. Müşteri memnuniyeti, herhangi bir işletmenin anahtar performans değerlendirme kriterlerinden biri durumuna gelmiştir (Naumann ve Giel, 1995).

Müşterilerin memnuniyeti, ekonomik aktivitelerin yönünü belirler, çünkü nihai amaç ne kadar ürettiğimiz veya tükettiğimiz değil, ekonominin müşteriye ne kadar çok tatmin ettiği. Müşterinin memnun olmadığı bir ortamda, verimin artması, ekonominin büyümesi, borsada rekorlar kırılması çok da fazla bir şey ifade etmemektedir. Müşteri memnuniyetini artırmadan, ekonomik büyümeyi sağlamak, rekabetçi piyasada mümkün değildir. Pazar ekonomisinde işletmeler müşteri kazanmak için rekabet ederler, müşteriler ürünleri satın alabilmek için pek yarışmazlar.

İşletmelerin finansal ve ekonomik başarılar elde etmesinde müşteri memnuniyeti ile bu müşteriler ile yüksek seviyede ilişkilerin kurulmasının etkisi vardır. Müşteri memnuniyeti sunulan mal / hizmetlerin müşteri beklentilerini karşılayıp karşılamadığına dair, müşterinin tek bir ürün veya hizmeti değerlendirmesi sonucu oluşan kısa süreli duygusal bir durumdur.

Tüketicinin subjektif değerlendirmesi sonucu oluşan müşteri memnuniyetinin sağlanması işletme için anahtar bir konudur. Çünkü müşteri memnuniyeti sadakati ortaya çıkarır. Buda daha yüksek bir işletme performansı oluşturur (Gronholdt, at.all, 2000: 509).

Müşteri memnuniyeti kavramı gerek iç müşteri memnuniyeti gerekse dış müşteri memnuniyeti açısından önemlidir.

3.2 Çalışan Memnuniyeti

Çalışan memnuniyeti, şirketin finansal hedeflerine varma noktasında çok önemli bir rol oynar (Chi and Gursoy, 2009 ,s.247). Çalışan memnuniyeti hizmet sektörünün gelişmesi ile beraber gelişmiştir ki idareciler başarı için memnuniyet oluşumunda soyut bir kavram olan personel dikkati ve havasının (morali) ürün olarak önemli olduğunun farkına varmışlardır. (Transportation Research Board National Research Council, 1999).

Performans ölçmek iyi bir yönetim faaliyeti için gereklidir. Ayrıca hizmetlerin kalitesini artırır. Çalışanların ve yöneticilerin amaç ve hedeflere ulaşmada neyin önemli olduğuna odaklanmalarına ve bunların karşılaştırma olanaklarını artırır. Bütçe incelemesi ve bütçenin sağlıklı bir şekilde işleyebilmesi açısından önemlidir. Kurumlara “kamu kaynaklarının niçin harcandığı” sorusuna yanıt vermede yardımcı olur. (Uludağ Üniversitesi Rektörlüğü Gelişim Planlama Kurulu, 2002)

Çalışan tatmini, bireyin işi ve işyeri hakkındaki genel duygu, düşünce kalıpları hakkında fikir verebilecek önemli bir değişkendir. Diğer bir ifade ile çalışan tatmini, bireyin işyerine yönelik beklentilerini ve işine yönelik tutumunu ifade etmektedir. Yani, bireyin işini ya da işle ilgili yaşantısını, memnuniyet verici veya olumlu bir duygu ile sonuçlanan bir durum olarak algılamasıdır. Aynı zamanda çalışan tatmini, çalışanların bedensel ve zihinsel sağlıkları yanında, bireysel fizyolojik ve ruhsal duyguların bir belirtisidir. Çalışan tatmini denince, işten elde edilen maddi çıkarlar ile çalışanın beraberce çalışmasından zevk aldığı iş arkadaşları ve ürün meydana getirmenin sağladığı bir mutluluk akla gelmektedir (Şimşek ve ark.,1998,s.160)

Çalışan tatmini konusu ele alınırken, temel olarak beş alt boyuttan bahsedilir. Bu boyutlar; “ücret”, “işin niteliği”, “bireyin çalışma koşulları”, “yönetim

politikaları” ve “çalışma arkadaşlarıdır (Luthans, 1992, s.126). Bu boyutlardan “ücret” (araçsal fonksiyon) dışsal bir fonksiyon olarak ele alınırken, diğer faktörler içsel (işin niteliği faktörleri) faktörler olarak sıralanmaktadır(Rose, 2003, s.506). Yönetim Politikaları boyutu içinde ise Bilgi Güvenliği Yönetim Sistemi Politikalarından da bahsedilebilir. Çalışanın kurumu ile paylaştığı kişisel bilgilerinin mahremiyetinin sağlanması, çalışma koşullarının, iş yapış şekillerinin ve süreçlerinin kanuni regülasyonlara uyum sağlayacak şekilde düzenlenmiş olması çalışan memnuniyetini arttırıcı unsurlar arasında düşünülebilir.

Motivasyon, kişinin belli bir amacı gerçekleştirmek üzere kendi arzu ve istekleri doğrultusunda davranma olayıdır. Bu da ancak çalışanın beklentilerinin karşılanması yani iş tatminin sağlanması ile mümkün olabilmektedir (Örücü ve Çolak, 2002, s.12). Çalışanın iş tatminin sağlanması iş gören tarafından verilecek olan hizmetin kalitesinin yükseltilmesinde büyük önem taşır. Zira; iş tatmini, çalışanın işine ve iş ortamına karşı olan olumlu tutumudur ve eğer çalışan üzerinde iş tatmini sağlanamazsa verilecek olan hizmetin kalitesinin düşmesi kaçınılmaz olacaktır. Bu anlamda iş tatmini çalışanların performansını, çalışan devir hızını, örgütün büyüme hızını, verimliliğini nihai olarak da karlılığını etkileyen önemli bir öğedir(Emir ve Baytok, 2004, s.254). Willa M Bruce ve J. Walton Blackburn'unda ifade ettiği gibi çalışanların iş tatminini yükseltmesindeki en büyük etken, onlar için ideal bir ortamın yaratılmasıdır. Böylelikle, çalışanların daha yüksek performansla çalışması sağlanacak ve buna bağlı olarak verilecek olan hizmetin kalitesi yükseltilmiş olacaktır(Murray, 2004, s.3).

Bu durum, güdüleme kavramının gündeme gelmesine neden olur. Güdüleme, örgütün bireylerin ihtiyaçlarını tatminle sonuçlandıracak bir iş ortamı yaratarak bireyin harekete geçirilmesi ve desteklenmesi sürecidir. Bu sürecin sağlıklı bir şekilde yürütülebilmesi için öncelikle iş görenin, işyerinden duyduğu beklentilerinin ne olduğunun tespit edilmesi ve bu beklentilerinin ne ölçüde karşılandığının ya da aşıldığının belirlenmesi gerekir(Şimşek,1995,s.92). Bu amaçla yapılan araştırmalar çalışanın birincil, ikincil ve genel güdüler olmak üzere üç tip güdünün etkisi altında olduğunu gösterir. Birincil güdüler; kişinin yaşar halde kalması için organizması için gerekli olan yeme içme, nefes alma, düzenli bir vücut ısısı sağlama, cinsellik gibi güdülerdir. İkincil güdüler ise sonradan öğrenilmiş güç, basan, elde etme, ait olma

gibi güdülerdir. Genel güdüler ise ne birincil ne de ikincil güdüler sınıfına sokulabilen güdülerdir. Bir diğer ifadeyle öğrenilmemiş ve fizyolojik kökenli olmayan güdülerdir. Merak, yetkinlik, çevreyle uğraşma, faaliyet, sevgi gibi. İşte kişinin beklentileri içinde yer alan bu güdülerin işyerinde sağlanması kişide iş tatminine yol açacaktır(Baysal ve Tekarslan,1998, s.102).

3.3 Örgütsel Bağlılık

Örgütsel bağlılık, sadece belirli bir rolün başarı derecesini nitelik ve nicelik yönünden yükselterek devamsızlığın ve işgücü devrinin azalmasına katkıda bulunmanın yanında bireyi örgütsel yaşam ve en üst düzeyde sistem başarısı için gerekli birçok gönüllü eyleme yöneltmektedir.

Örgütsel bağlılık ile bazı kavramlar arasında karmaşa yaşanmaktadır. Bu kavramlardan birisi örgütsel kimliktir. Örgütsel kimlik sadece kabulün ötesinde örgütsel değerleri ve amaçları paylaşmayı, sahiplenmeyi ifade etmektedir (Epitropaki and Martin, 2005, s.571).

Allen ve Meyer örgütsel bağlılığın; psikolojik bir boyutu olduğunu ileri sürmüşlerdir. Bu psikolojik boyutun, çalışanın örgütle ilişkisine paralel olarak şekil aldığını belirtmişlerdir. Bu şekillenmenin sonunda da bireyin örgütte kalması yönünde kararına neden olduğu görüşünü savunmuşlardır (Allen ve Meyer, 1996, s.255).

Steers, örgütsel bağlılığı; örgütün amaçlarının ve değerlerinin örgüt üyeleri tarafından benimsenmesi, çalışanın örgütün önemli bir üyesi olmak için çaba göstermesi, örgütü bir aile olarak değerlendirmesi ve bireyin kendisini de bu ailenin bir ferdi olarak görmesi olarak tanımlamıştır.

Örgütsel bağlılık, örgütün sahip olduğu özelliklerinin veya örgütün bakış açısının, çalışan tarafından benimsenmesi, bir anlamda özümsemesidir (O'Reilly ve Chatman, 1986, s.493).

Örgütsel bağlılık kavramı yukarıda görüldüğü gibi farklı şekillerde tanımlanmıştır. Yapılan bu tanımları iki şekilde sınıflandırmak genel kabul görmüş bir yaklaşımdır. Becker, Staw, Salancik gibi araştırmacılar örgütsel bağlılık kavramının davranış yönünü ele alarak tanımlamışlardır. Allen, Meyer, March ve Simon, Mowday, Steers ve Porter, Boulian gibi araştırmacılar ise; örgütsel bağlılık kavramının tutum yönünü öne çıkartmışlardır. Davranışçılara göre örgütsel bağlılık; bağlılığın açık gösterimiyle kanıtlanır. Çalışanlar, işlerine devam ederek sorumluluklarını arttırırlar. Çalışanın sorumluluklarının artması örgütten ayrılmayı zorlaştırır. Tutumsal yaklaşım ise; çalışanın kimliğinin örgütle ilişkilendirilmesi fikrini ileri sürer.

Çalışan, işverene karşı duygusal bir bağlılık göstereceği savunulur (Çetin, 2004,s.93). Örgütsel davranış alanında çalışan bilim adamları, tutumsal bağlılık üzerinde dururlarken, sosyal psikoloji alanında çalışanlar davranışsal bağlılık üzerinde yoğunlaşmışlardır (Örs vd., 2003, s.218). Örgütsel bağlılığın tutumsal veya davranışsal olmasından öte, çalışanların örgüte bağlılıklarını etkileyen faktörlerin neler olduğu araştırmacıların daha fazla dikkatini çekmiştir. Örgütsel bağlılıkla ilgili araştırmaların önemli bir bölümünün bu yönde gerçekleştiği görülmektedir.

Örgütsel bağlılık ile ilgili olarak Allen ve Meyer tarafından geliştirilen çok boyutlu örgütsel bağlılık modeli yaygın olarak kabul görmüştür. Çalışanın, örgüte bağlılığının duygusal, devam ve normatif olarak üç bileşenden oluştuğunu ileri sürmüşlerdir.

Modelin bileşenlerinden olan duygusal bağlılık, çalışanın örgütsel amaçları ve örgütün değerlerini benimsemesinden kaynaklanmaktadır. Eğer çalışanın bu değer ve amaçları benimseme düzeyi yüksekse, örgütsel bağlılık düzeyi de yüksektir (Obeng ve Ugboro, 2003, s.83) Duygusal bağlılık, örgütte kalma isteği ve duygusal nedenlerle örgüte bağlı olmayı ifade etmektedir. Çalışanın örgüte gösterdikleri duygusal ilginin boyutlarını yani örgüte katılma ve bir anlamda örgütle özdeşleşme anlamı taşımaktadır. Devam bağlılığı veya zorunlu bağlılık ise, çalışanın, örgütten ayrılması durumunda katlanması gereken maliyeti ifade etmektedir. Çalışanın bu anlamdaki algısı, örgütte kalıp kalmaması yönünde belirleyici olmaktadır (Allen ve Meyer, 1991, s.42). Devam bağlılığında, çalışanın örgütte kaldığı süre boyunca,

işletmeye katkılar sağladığı düşünülmekte ve bu bir yatırım olarak görülmektedir (Obeng ve Ugboro, 2003, s.83). Bağlılığın üçüncü unsuru normatif bağlılık, bağlılığın ahlaki değerlere dayandırmaktadır. Çalışan örgütte kalmasını ahlaki veya inancı ile ilgili olarak değerlendirmekte ve örgütte kalmayı ahlaki bir zorunluluk olarak görmektedir.

Örgütsel bağlılığı etkileyen faktörlerin başında demografik ve kişilik özellikleri ile ilgili faktörler yer almaktadır. Örgütsel bağlılık ile demografik ve kişilik özellikleri; yaş, cinsiyet, kıdem, aynı örgütteki iş deneyimi, kişisel ilgi arasındaki ilişkiyi belirlemeye yönelik yapılan araştırmaların amacı, bağlılığın bu faktörlere göre değişiklik gösterip göstermediğini belirlemektir.

Gouldner, Lodahl, Hall ve Shnider'ın iş ve iş özellikleri ile ilgili yaptıkları araştırmalarda, çalışanın örgüte bağlılığını güçlendirmek için “karşılıklı olmanın” önemini açıklamışlardır. İşyerindeki sosyal ilişkilerin, örgüte bağlılığı olumlu yönde etkilediğini ortaya koymuşlar ve göreve bağlı olan değişim ve sorumluluğun örgüte bağlılığı artırdığını ileri sürmüşlerdir. Morris ve Steers, örgütsel yapının ve kontrol alanlarının genişliğinin örgüte bağlılıkla ilişkisi olmadığını açıklamışlardır. Bir başka araştırmada, çalışmak için seçilen örgütün, örgüte bağlılığı belirlemede önemli olduğunu vurgulamışlar ve yenilikçilik için yüksek derecede örgüte bağlı kişilerin önemli olduğunu belirtmişlerdir.

Bazı akademisyenlere göre, örgütsel bağlılık düzeyini etkileyen faktörleri öncelikle iki şekilde sınıflandırmakta fayda vardır. Bunlar; örgüt içi ve örgüt dışı faktörlerdir. Örgüt dışı faktörler; işletmenin içinde bulunduğu sektör, rakip işletmeler, çalışanın işinin yaygınlık derecesi, çalışanın alternatif iş durumu, ülkenin iş gücü arzı ve işle ilgili yasal düzenlemeler ve buna benzer etkenlerdir.

3.4 Süreç Yaklaşımı

Süreç, ISO 9001:2000 Kalite Yönetim Sistemi standardında “girdileri çıktı haline getiren birbirleri ile ilgili ve etkileşimli faaliyetler takımı” olarak tanımlanmıştır(TSE, 2001,s.2). Bu temel tanımın kapsamı genişletilirse, süreç tanımı içerisine aşağıdaki özellikler de düşünülebilir(Ayanoğlu ve Turan, 2003, s.195):

- Girdileri olan, bunlara müşterileri için değer ekleyen ve çıktı üreten faaliyetler dizisidir,
- Belirli bir çıktı (ürün ya da hizmet) elde etmek için birbirleri ile etkileşim içinde bulunan insan, malzeme, ekipman, yöntem ve çerçevenin toplamıdır,
- İşletme girdilerini işletme çıktılarına dönüştüren etkinliklerin bileşimidir,
- Süreçler, üç temel faaliyet çeşidinin bir kompozisyonudur. Değer yaratan yani müşteriler için önem taşıyan faaliyetler; temel olarak fonksiyonel, departmansal veya örgütsel sınırlar arasında iş akışını sağlayan faaliyetler ile kontrol faaliyetlerinin bileşimidir,
- Bir organizasyonel süreç, başı ve sonu olan bir iş demektir. Yani bu işi yapmak için gerekli alt işlerin ve detay işlerin oluşturulduğu kümedir,
- En yalın açıklama ile süreçler bir işletmenin müşterileri için ne yaptığıdır,
- Süreçler işletmenin ürün/hizmetini yaratan mantıksal iş toplamıdır,
- Bir iş süreci, bir veya birkaç çeşit girdinin alınıp bunlardan müşteri için değer oluşturacak bir çıktının yaratıldığı faaliyetler toplamıdır.
- Süreçler birbirini izleyen durum değişikliklerinin analizinden doğarlar, yani bir süreç, ilgili bir veya daha fazla varlığın durumunu değiştirme yoluyla, girdilerin çıktılara dönüştüğü faaliyetler dizisidir.

Bir süreç beş temel özelliği taşımaktadır.

Tanımlanabilirlik: Sürecin temel unsurlarının belirlenebilmesi özelliğidir.

Ölçülebilirlik: Sürecin performans ölçütleri ile izlenebilme özelliğidir.

Yinelenebilirlik: Süreci harekete geçiren aynı veya değişen girdilerin izlenmesi sonucunda oluşan çıktının müşteri ihtiyaç ve beklentilerini sürekli karşılayabilme özelliğidir.

Kontrol edilebilirlik: Süreç sorumlularının sürecin performansı hakkında her zaman için bilgi sahibi olabilmesi ve gerektiğinde düzeltici faaliyetlerin yerine getirilmesi özelliğidir.

Katma değer yaratma: Sürecin, çıktının kalitesi ve çıktıyı kullanan müşterinin tatmini üzerine olumlu etki yaratabilme özelliğidir.

ISO/IEC 27001:2005 BGYS ve ISO 9001:2000 KYS, entegre yönetim sistemleridir. ISO 27001 standardında da süreç yaklaşımı esas alınmıştır. Bu standartta sunulan bilgi güvenliği yönetimi süreç yaklaşımı, kullanıcılarını aşağıdakilerin öneminin vurgulanmasına özendirir (ISO/IEC FDIS 27001, 2005, s.1):

- a) İş bilgi güvenliği gereksinimlerini ve bilgi güvenliği için politika ve amaçların belirlenmesi ihtiyacını anlamak,
- b) Kuruluşun tüm iş risklerini yönetmek bağlamında kuruluşun bilgi güvenliği risklerini yönetmek için kontrolleri gerçekleştirmek ve işletmek,
- c) BGYS'nin performansı ve etkinliğini izlemek ve gözden geçirmek,
- d) Nesnel ölçmeye dayalı olarak sürekli iyileştirmek.

Bu standart, risk değerlendirme, güvenlik tasarımı ve gerçekleştirme, güvenlik yönetimi ve yeniden değerlendirmeyi sağlar.

Süreç Yönetimi, en temel tanımıyla süreçlerin sürekli ve düzenli olarak izlenmesi ve geliştirilmesini garanti altına almak için yapılan faaliyetler dizisidir. Bir sürecin en yüksek performansı sağlaması için gerekli planlama ve yönetim faaliyetlerini gerçekleştirmek ve kaliteyi, operasyonel performansı ve bunun sonucunda müşteri memnuniyetini arttırmak için fırsatları tanımlamak süreç yönetiminin amacı oluşturur(Evans and Lindsay, 2002, s.360).

Süreç yönetimi tüm sistem süreçleri için standart sistem geliştirme yöntemlerinin, araçlarının, tekniklerinin ve teknolojilerinin planlanması, seçimi ve istikrarlı bir şekilde uygulanmasıdır. Süreç yönetimi, sürecin oluşturulmasında başlar ve sürekli iyileştirme çalışmalarını da içine alarak devam eder. Süreç yönetimi temel olarak iş süreçlerine odaklanmıştır. Bütünsel bir yönetim bakış açısının sağlanması ve süreçlerle yönetim kavramı ile gerçekleştirilebilir.

3.5 Şirket Performansı

Tüm firmaların en uzun vadeli amacı firmanın piyasa değerini maksimize etmek olup kendilerini orta ve kısa vadede bu hedefe götürecek başarı kriterleri çeşitli şekillerde sıralanabilir: Örneğin yenilik performansı, kalite performansı, personelin kalitesi, iş tatmini ve örgüte bağlılık, müşteri tatmin ve bağlılığı, ciro ve pazar payı artışı, kar ve sermaye artışı vs. Görüldüğü gibi bu başarı göstergeleri hem ortaya çıkma zamanı ve hem de faaliyet alanı açısından birbirlerinden farklı olup aralarında da sebep-sonuç ilişkileri mevcuttur.

Bazı araştırmacılar (örneğin: Denison ve Mishra, 1996, Fisher, 1997) kavramsal olarak ayrı olmalarına rağmen, birbirleri ile etkileşim halinde olan bu faktörleri iki ana grupta –niteliksel ve niceliksel performans göstergeleri- toplamışlar ve birincinin ikincinin oluşumunda öncül veya aracı olduğunu vurgulamışlardır.

Niteliksel performans daha ziyade örgütün iç çevresindeki kültür, ortam, insan kaynakları ve soyut çıktılarla ilgili olup çalışan memnuniyeti, müşteri memnuniyeti, kalite(süreç yaklaşımı) ve yenilik performansı gibi kriterleri kapsamaktadır. Niceliksel performans ise kısmen niteliksel faktörlerin de etkisinde oluşan ve daha ziyade pazarlama ve finansal yönetim başarısına dayalı olan ciro artışı, pazar payı artışı ve kârlılık artışı gibi kriterleri kapsamaktadır.(Alpkan vd,2005,s.176)

3.6 Bilgi Güvenliđi Olgunluk Seviyesi

Bilgi Güvenliđi olgunluk seviyesi, bir firmanın bütün çalışanları, işleyişleri ve varlıklarıyla beraber bilgi güvenliđi konusundaki bilgi ve durumunu belirten seviyedir. Bilgi Güvenliđi olgunluk seviyesinin belirlenmesi, şu anki durumu göz önüne alarak ileride ne gibi deđişiklikler yapılması gerektiđini planlamamıza yardımcı olur.

Bilgi Güvenliđi Yönetim Sistemi risk temelli bir yönetim sistemidir(Boehmer W., 2008, s. 224). Sistemin temelinde varlıkların belirlenmesi, varlıklara yönelik tehditlerin ve risklerin tespit edilmesi, tespit edilen bu risk ve tehditlerin bertarafına yönelik kontrollerin atanması ve nihayet bu kontrollerin üst yönetim tarafından belirlenmiş politikalarla desteklenmesi yatmaktadır. Belirtilen bu özet süreç, daima canlı tutulmalıdır. Çünkü Bilgi Güvenliđi Yönetim Sistemi, bir kere kurulup bırakılacak bir sistem deđildir. PUKÖ(Planla Uygula Kontrol et, Önlem al) döngüsünü devam ettirecek faaliyetleri firmaların gerçekleştirmesi gerekmektedir (Bialas A., 2006, s.3). Buda firmaların kendi seviyelerini tanımlaması için belirli kriterlere sahip modelleri kullanması ve bu seviyelerini periyodik olarak ölçmeleri ile mümkün olacaktır.

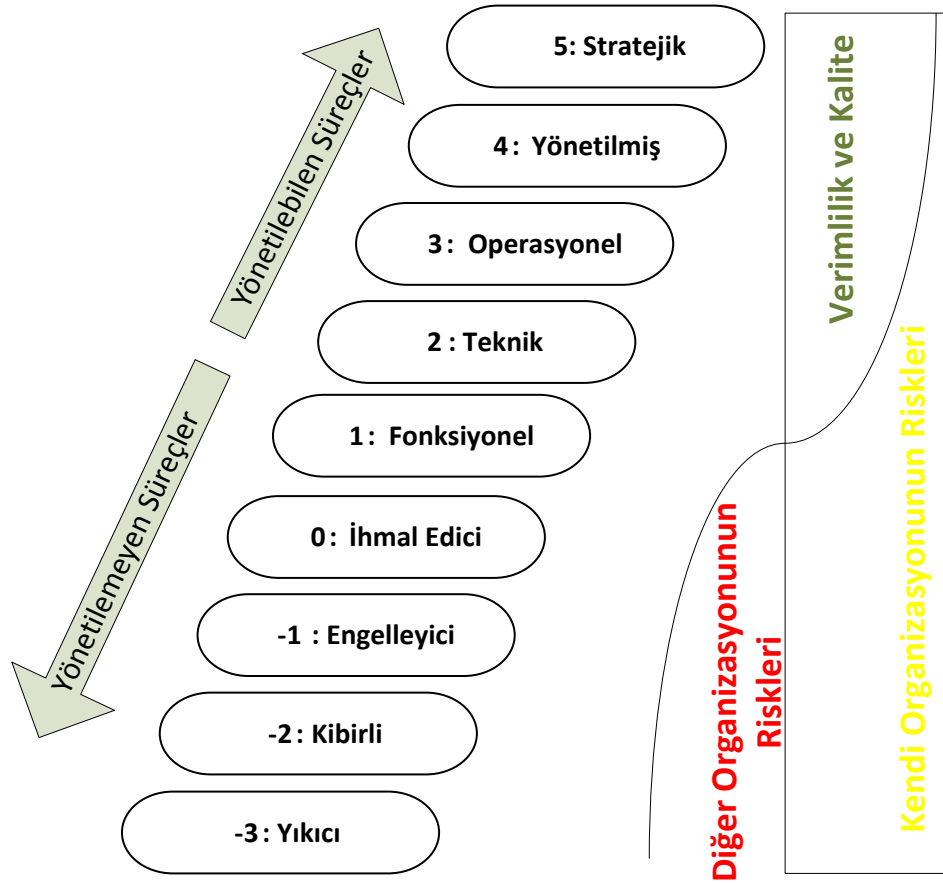
Olgunluk modeli bir firmanın bilgi güvenliđi konusunda gelebileceđi olgunluk seviyelerinin derecelendirilmesi ile oluşur ve firmanın bir alt adıma düşmemek aksine bir üst adıma çıkmak için neler yapması gerektiđini gösterir.

Geleneksel Bilgi Güvenliđi Yönetim Sistemi metrikleri genellikle kontrol listesi&Standart temellidir ve bu iki metrik, günün sonunda eksiklerin en iyi Bilgi Güvenliđi pratiklerinin uygulanması ve bunlarla ilgili teknik kontrollerin atanması konularını kapsar. Yapılan önceki araştırmalara göre idari, operasyonel ve teknik kontrollerin deđerlendirildiđi 3 tip güvenlik kontrollerini ortaya koymaktadır. Dünyadaki yayınlanmış güvenlikle ilgili en popüler olgunluk modelleri Tablo 3.1’de gösterilmektedir(Woodhouse S., 2008, s.243).

Model	Açıklama	Yorumlar
NIST CSEAT IT Security Maturity Model	Beş aşamalı olgunluk seviyeleri: 1. Politika 2. Prosedür 3. Uygulama 4. Test 5. Entegrasyon	Dokümantasyon seviyelerine odaklanmış bir modeldir.
Citigroup's Information Security Evaluation Model (CITI-ISEM)	Beş aşamalı olgunluk seviyeleri: 1. Umursamazlık 2. Kabul 3. Entegrasyon 4. En iyi Uygulamalar 5. Sürekli iyileşen	Organizasyonel farkındalık ve kabullenmelere odaklanmış bir modeldir.
COBIT Maturity Model	Beş aşamalı olgunluk seviyeleri: 1. Başlangıç 2. Tekrarlanabilir fakat sezgisel 3. Tanımlı Prosesler 4. Yönetilebilir ve Ölçülebilir 5. Optimize	Spesifik prosedürlerin denetlenmesine odaklanmış bir modeldir.
SSE-CMM	Altı aşamalı olgunluk seviyeleri: 0. Uygulanmamış 1. İnformal yapılmış 2. Planlı ve İzlenen 3. Tamamen Tanımlanmış 4. Nicelikli Kontrollü 5. Sürekli İyileşen	Güvenlik Mühendisliği ve Yazılım Dizaynına odaklanmış bir modeldir.
CERT/CSO Security Capability Assessment	Beş aşamalı olgunluk seviyeleri: 1. Mevcut 2. Tekrarlanabilir 3. Kişiyeye Atanmış 4. Dokümante edilmiş 5. Gözden geçirilmiş ve güncellenmiş Ölçüm seviyeleri: 1. Başlangıç 2. Gelişen 3. Kurulmuş 4. Yönetilebilir	Kalite ile ilgili dokümantasyon seviyelerinin olgunluk seviyelerine odaklanmış bir modeldir.

Tablo 3.1 En popüler olgunluk modelleri (Woodhouse S., 2008, s.243).

Burada bahsedeceğimiz olgunluk modeli, kurumun tanımlı süreçlerine ve geliştirmiş oldukları uygulamalara dikkat çekmektedir. Bu model yalnızca teknik tabanlı kontrolleri içermez, bununla birlikte idari ve operasyonel kontrolleri de dikkate alır (Solms S.H., 2005, s.444). Tüm bu kontrollerin kurum kültürü ve kurum hafızasına kazandırılıp kazandırılmadığını ölçmeye çalışır (Ruighaver et al., 2007, s.60).



Şekil 3.1 Olgunluk Modeli (Woodhouse S., 2008, s.244)

Bu olgunluk modeli Şekil 3.1’de görülebileceği gibi 9 katmana ayrılmıştır. Katmanlar -3’ten 5’e yıkıcı, kibirli, engelleyici, ihmal edici, fonksiyonel, teknik, operasyonel, yönetilmiş ve stratejik olarak ayrılmıştır. -3’ten 0 a kadar kendi firmasına maksimum risk unsuru oluşturmuş, bununla birlikte aynı zamanda dış firmalar içinde risk unsuru taşımaktadır. 1’den 5’e kadar dış firmalara zarar vermemekle birlikte kendi firması için de giderek risk unsurlarını azaltmaktadır (Woodhouse S., 2008, s.244).

Şimdi bu önerilen olgunluk modelini biraz tanıyalım:

3.6.1 Seviye 5 : Stratejik (Strategic)

Firma PUKÖ döngüsü içerisinde kendini sürekli olarak geliştirmektedir. Belirli Bilgi Güvenliği protokolleri ve iş devamlılığı planları vardır ve sürekli eğitimler, denetimler ve uygulamalarla denetlenmektedir. Bilgi güvenliği firma

çalışanları tarafından bir ağırlık olarak değil işin olabilirliğini sağlayan etken olarak görülmektedir. Süreçlerin gizliliği, bütünlüğü ve erişilebilirliği garanti altına alınmıştır. Süreçlerdeki verimlilik yükseltilirken riskler düşürülmüştür (Woodhouse S., 2008, s.245).

Kısaca;

- PUKÖ Döngüsü tam olarak çalışmaktadır,
- Güvenlik Politikaları doğru tanımlanmış ve özümsemiştir,
- Tüm Süreçler güvenlik perspektifinde değerlendirilmiştir,
- BG Farkındalığı organizasyonel hafızadadır,
- Eğitimler aksamadan düzenli olarak verilmektedir,
- Şirketin tüm BG faaliyetleri izlenebilmektedir,
- Riskler belirlenmiş, kontrol altına alınmış ve yönetilmektedir,
- İş Sürekliliği planları hazırlanmış ve test edilmiştir. Böylece müşterilere verilen hizmetlerde aksama olmaması için gerekli hazırlıklar yapılmıştır.

3.6.2 Seviye 4 : Yönetilmiş (Managed)

Firma bilgi güvenliği yönetim sistemini geliştirmek için yeni yöntemler aramaktadır. Gerekli olduğu ölçüde bilgi güvenliğine yatırımlar arttırılmaktadır. İzleme süreçleri iyi bir şekilde yürütülmektedir.

Bu tür firmalar bilgi güvenliği sistemini gerçekleştirmiş ama firma kültürü olarak daha yeni oturtmuş firmalardır. Bilgi güvenliği eğitimleri hazırlanmıştır ve güncelleştirilmektedir.

İş sürekliliği planları yapılmış ama tam olarak denenmemiştir. Çevresel faktörler izlenmeye başlanmıştır (Woodhouse S., 2008, s.245).

Kısaca;

- PUKÖ Döngüsü henüz tam olarak çalışmamaktadır,
- Güvenlik Politikalarının hepsi tamamlanmamış, tamamlanmayanlar için ise örnekler araştırılmaktadır,
- BG Farkındalığı Organizasyonel hafızaya yeni yeni alınmakta daha henüz bir kültür olarak adlandırılmamaktadır,

- Eğitimler hazırlanmakta ve güncelleştirilmeleri yapılmaktadır,
- İş Sürekliliği planları hazırlanmış fakat daha test edilmemiştir.

3.6.3 Seviye 3: Operasyonel (Operational)

Firma bilgi güvenliği yönetimi için prosedürleri ve politikaları incelemeye başlamıştır. Bilgi güvenliği stratejik planı yapılmıştır. Uygunluğundan ve gösterilen özenden dolayı izleme faaliyetleri bire bir yapılmaktadır. Bilgi güvenliği yatırım planı yapılmış, teknik olarak pozisyonlar belirlenmiştir.

Bu organizasyonlarda kültür olarak bilgi güvenliğinin ve risklerin yönetildiği umudu vardır. Bilgi güvenliği genel olarak BT'nin görevi olmuştur. Bilgi güvenliği eğitimleri ise bire bir yöntemlerle anlatılmaktadır (Woodhouse S., 2008, s.245).

İş sürekliliği planları yapılmış ama denenmemiştir.

Kısaca;

- PUKÖ Döngüsü tasarım aşamasındadır,
- Güvenlik Politikaları yazılması planlanmıştır,
- BG Farkındalığının artırılma yöntemleri planlanmış, diğer yöntemler araştırılmaktadır,
- Bilgi Güvenliği genel olarak BT nin sorumluluğundadır. Bir çok şey teknik olarak düşünülmektedir.
- İş Sürekliliği planları hazırlanmış fakat daha test edilmemiştir.

3.6.4 Seviye 2 : Teknik (Technical)

Firma bilgi güvenliği yönetim sistemini tam olarak belirlememiştir. Bilgi güvenliğini kapsayan politikalar yoktur. Bilgi güvenliği sistemine yatırım düşünülmektedir. Teknik kontroller ve iç güvenlikler oluşturulmuştur. Bilgi güvenliği ile ilgili görevler belirlenmemiştir (Woodhouse S., 2008, s.245).

Bilgi güvenliği işleri BT'nin işleri olarak gözükmektedir. BT ise sadece belirli konularda eğitim almıştır.

Firma risklerini bilmektedir ve risk yönetimi uygulamaktadır. Aynı zamanda dış firmaların riskleri de gözetilmektedir.

3.6.5 Seviye 1 : Fonksiyonel (Functional)

Firma bilgi güvenliği üzerinde hiçbir politika veya prosedür belirlememiştir. Sadece özel bilgiler anti-virüs ve güvenlik duvarlarıyla güvenlik altına alınmıştır. Firma kültürü içinde bilgi güvenliği kültürü yoktur. Aynı zamanda firma kültürü bilgi güvenliği kültürünün artmasını desteklememektedir. Firma bilgi güvenliğini tamamen BT'nin sorunu olarak görmektedir (Woodhouse S., 2008, s.246).

Firma risklerini bilmektedir ve risk yönetimi uygulamaktadır. Aynı zamanda dış firmaların riskleri de gözetilmektedir.

3.6.6 Seviye 0 : İhmal Edici (Negligent)

Firma belli kişilerin denemelerini engelleyerek kısmen bir koruma sağlamaktadır. Genellikle bu tür firmalar kişilerin yapmak istediklerini engelleyerek bilgi güvenliğini sağlamaya çalışır. Eğer herhangi bir yöntem veya yönetim belgesinde değişiklik olursa, o bilgileri tekrar elde edemezler (Woodhouse S., 2008, s.246).

Bu tür firmalardaki kültür genellikle kanıtların yönetimine dayanır. Bilgi güvenliği BT'nin sorumluluğu olarak görünür. Firmanın genellikle bir vizyonu ve hedefi yoktur.

Firma sadece kendi güvenliğini değil iş yaptığı dış firmalarında güvenliğini düşünüyor gibi görünür.

3.6.7 Seviye -1 : Engelleyici (Obstructive)

Bu tür firmalarda bilgi güvenliği yöneticiler tarafından engellenmiştir. Yönetimdeki bütün işler fazlasıyla formaldır. Firma kültürü tamamen eylemsizlik üzerine kurulmuştur. Risk yönetimi uygulaması ve bilgi varlıklarının

değerlendirilmesi bu şekilde engellenmiş olur (Woodhouse S., 2008, s.246). Firmada hiçbir farkındalık ve bilgi güvenliği eğitimi yada dökümanı bulunmamaktadır. İşlerin nasıl yapıldığına dair dokümanlar vardır ve bunlar bire bir uygulanmalıdır. Aktif katılım engellenmiştir.

Bu firmalar sadece kendilerine değil başka firmalara da risk oluşturmaktadır.

3.6.8 Seviye -2 : Kibirli (Arrogant)

Bu tür firmalar kendilerinin tek ve bilgi güvenliği sistemlerinin ise tartışmasız doğru olduklarına inanır. Hiçbir şekilde iyileştirme veya değiştirme yapılmasına izin vermez (Woodhouse S., 2008, s.246).

Bu tür firmalar kendi bünyelerinde maksimum seviyede riskler barındırmakta, bununla birlikte diğer firmalara da ciddi anlamda risk unsuru oluşturmaktadırlar.

3.6.9 Seviye -3 : Yıkıcı (Subversive)

Bu tür firmalar diğer firmaların işlerini yapamaması için aktif olarak yol arayan firmalardır ve kendi varlıklarını da hiç önemsemezler. Bu firmalar suç örgütleri ya da uluslar arası şebekeler olabilir (Woodhouse S., 2008, s.246).

Bugünün belirsiz şartlarında bilgi güvenliği çok önemli bir rol oynamaktadır. Sürekli yeni tehditler ortaya çıkarken firma kendini sürekli olarak geliştirmelidir. Bu modelin amacı firma kültürünün bilgi güvenliği için ne kadar önemli olduğunu vurgulamaktadır (Woodhouse S., 2008, s.247). Çalışanların Bilgi Güvenliği Politikalarını önemsemeleri ve bu kuralların uygulanmasında olabildiğince aktif rol oynamaları, konunun organizasyonel hafızaya alınması anlamına gelmektedir. Bu durum, organizasyonel öğrenmeyi de Bilgi Güvenliği perspektifinde yapmalarını sağlayacaktır.

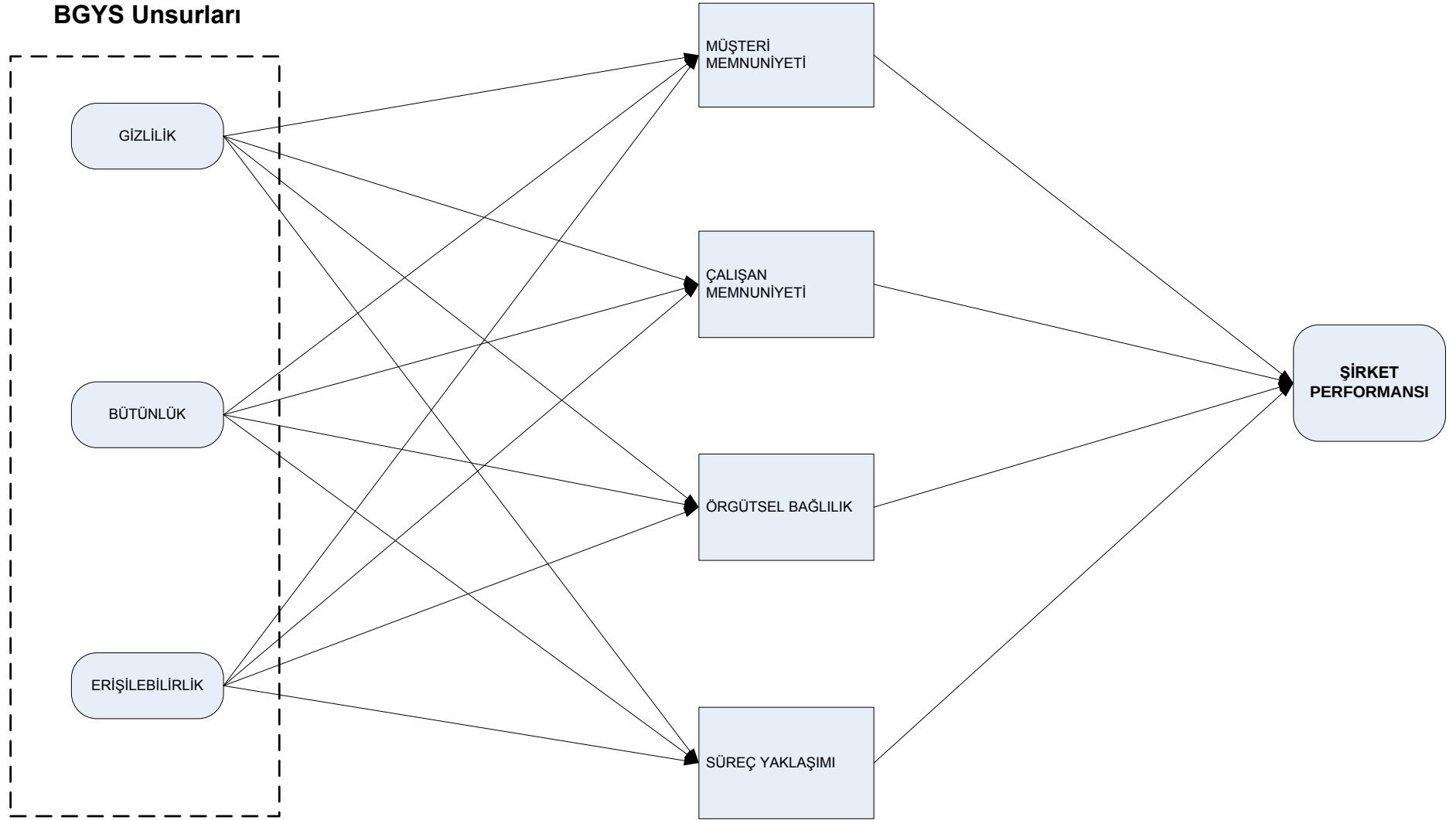
4. BİLGİ GÜVENLİĞİ KAVRAMI VE BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ İLE ŞİRKET PERFORMANSI İLİŞKİSİNE DAİR BİR UYGULAMA

4.1 Araştırmanın Amacı

Bu çalışmanın amacı Bilgi Güvenliği Yönetim Sisteminin, Şirket performansına olumlu yönde etki ettiğini tanımlamaktır. Bunun için öncelikle Bilgi Güvenliğinin altyapısını oluşturan Gizlilik, Bütünlük ve Kullanılabilirlik unsurlarının, Müşteri Memnuniyeti, Örgütsel Bağlılık, Çalışan Memnuniyeti ve Süreç Yaklaşımı kavramlarına etkisi incelendi. Tüm bunlardan hareketle Bilgi Güvenliği Yönetim Sisteminin Şirket performansına etkisi araştırıldı. Bu model Şekil 4.1’de gösterilmiştir.

4.2 Araştırma Kısıtları

Bu araştırma Bilgi Güvenliği Yönetim Sisteminin GSM sektörüne olan etkilerini tespit etmeyi amaçladığı için anket çalışması GSM şirketlerinde çalışanlar ile sınırlandırılmıştır.



Şekil 4.1 Araştırma Modeli

4.3 Ölçeklerin Oluşturulması

Geliştirilen hipotezlerin test edilmesi amacıyla çoktan seçmeli ölçek kullanılmıştır. Cevaplar (1= kesinlikle katılmıyorum'dan, 5=kesinlikle katılıyorum'a) 1-5 tipi Likert ölçeği kullanılarak ölçülmüştür. Ölçeklerin bulunduğu anket formu eklerde verilmektedir. Ölçeklerin kısa bir özeti ise aşağıda anlatılmaktadır.

Bilgi Güvenliğini oluşturan Gizlilik, Erişilebilirlik/Kullanılabilirlik ve Bütünlük/Doğruluk olmak üzere üç unsurunu ölçmek amacıyla soru setleri belirlenmiştir. Bu anlamda Gizlilik unsuru için altı soru, Erişilebilirlik/Kullanılabilirlik unsuru için beş soru ve Bütünlük/Doğruluk unsuru için ise beş soru kullanılmıştır.

Şirket performansı için düşünülen değişkenler ise araştırma içinde Müşteri Memnuniyeti, Örgütsel Bağlılık, Çalışan Memnuniyeti ve Süreç Yaklaşımı olarak seçilmiştir. Bunlardan Müşteri Memnuniyeti için dört soru, Örgütsel Bağlılık için beş soru, Çalışan Memnuniyeti için beş soru ve Süreç Yaklaşımı için beş soru kullanılmıştır. Şirket Performansı değişkeninin ölçümü için ise altı soru kullanılmıştır.

4.4 Veri Toplama Süreci

Araştırma evreni, Türkiye'deki GSM sektöründe faaliyet gösteren Yönetici, Uzman ve Mühendisleri kapsamaktadır. Bu sektörde faaliyet gösteren bu firmaların İstanbul'da konumlandığı dikkate alınarak örneklem popülasyonu, 200 kişiden oluşmuştur. İlave olarak bu firmalar, batı tarzında bir yönetim ve organizasyon anlayışını benimsemiş firmalardır. Örnek olarak ISO 9001 Kalite Yönetim Sistemi, 27001 Bilgi Güvenliği Yönetim Sistemi, OHSAS 18001 İş Sağlığı ve Güvenliği Yönetim Sistemi ve Avrupa Kalite Standartlarına uygun olarak faaliyette bulunmaktadırlar.

Örnekleminizdeki katılımcılar iş yerlerindeki ünvanlarına göre departman yöneticileri (%9), kıdemli mühendisler (%2), mühendis (%9,5) ve uzmanlardan (%79,5) oluşmuştur. Katılımcıların %51'i erkeklerden, %49'u kadınlardan oluşmaktadır. Örneklemin karakteristikleri Tablo 4.1, 4.2, 4.3 ve 4.4'de verilmektedir.

Cinsiyet	Sıklık	Oran (%)
Erkek	102	51,0
Kadın	98	49,0
Toplam	200	100

Tablo 4.1. Katılımcıların cinsiyetlerine göre dağılımı

Yaş	Sıklık	Oran (%)
18-24	4	2,0
25-34	175	87,5
35-50	21	10,5
Toplam	200	100

Tablo 4.2. Katılımcıların yaşlarına göre dağılımı

Eğitim Durumu	Sıklık	Oran (%)
Lise	4	2,0
Ön Lisans	21	10,5
Lisans	134	67,0
Lisans Üstü	41	20,5
Toplam	200	100

Tablo 4.3. Katılımcıların eğitim durumlarına göre dağılımı

Unvan	Sıklık	Oran (%)
Departman Yöneticisi	18	9,0
Kıdemli Mühendis	4	2,0
Mühendis	19	9,5
Uzman	159	79,5
Toplam	200	100

Tablo 4.4. Katılımcıların iş yerlerindeki konumlarına göre dağılımı

4.5 Ölçüm Geçerliliği ve Güvenilirliği

Analizde Bilgi Güvenliğini oluşturan Gizlilik, Erişilebilirlik/Kullanılabilirlik ve Bütünlük/Doğruluk olmak üzere üç unsur, Şirket performansını oluşturan Müşteri Memnuniyeti, Örgütsel Bağlılık, Çalışan Memnuniyeti ve Süreç Yaklaşımı değişkenleri ile çarpıştırılmış ve sonuçların Şirket Performansına olan etkileri araştırılmıştır.

Bu çalışmada, tüm değişkenler için reflektif ölçekler kullanılmış, ölçüm araçlarının psikometrik özelliklerini değerlendirebilmek amacıyla; herhangi bir yapısal ilişkinin olmadığı boş (null) bir model hesaplanmıştır. Güvenilirliğin hesaplanmasında kompozit ölçek güvenilirliği (CR) ve çıkartılan ortalama varyans (AVE) kullanılmıştır. Tüm ölçümler için PLS tabanlı CR değerinin eşik değeri olan 0,70'in üstünde seyrettiği ve AVE değerlerinin de eşik değeri 0,50'yi aştığı görülmektedir.

Değişken	CR	AVE
Müşteri Memnuniyeti	0.821	0.540
Örgütsel Bağlılık	0.908	0.664
Çalışan Memnuniyeti	0.854	0.540
Gizlilik	0.872	0.533
Erişilebilirlik/Kullanılabilirlik	0.932	0.734
Bütünlük/Doğruluk	0.856	0.544
Süreç Yaklaşımı	0.906	0.660
Genel Performans	0.934	0.701

Tablo 4.5. Kompozit güvenilirlik ve çıkartılmış ortalama varyans değerleri

Bunlarla birlikte ölçümlerin ilgili kavramlar üzerindeki standardize edilmiş yüklemeleri hesaplanarak yakınsak geçerlilik de test edilmiş ve tüm ölçümlerin 0,57'yi aşan bir standardize yükleme gösterdiği bulunmuştur (bakınız Tablo 4.6 ve 4.7). Bunu takiben de ölçümlerin ayrışma geçerliliği test edilmiştir. Fornell ve Larcker'in (1981) ifade ettiği üzere, her bir değişken için hesaplanan AVE değeri, değişken çiftleri arasındaki latent faktör korelasyonlarının karesinden yüksektir. Böylece ölçümlerimizin geçerlik ve güvenilirlik kriterlerini karşıladığı görülmektedir.

Değişken	Faktör 1	Faktör 2	Faktör 3	Faktör 4
Müşteri Memnuniyeti				
* İş yaptığım ve/veya hizmet aldığım şirketin ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemi standardının olmasını isterim.	0.71			
* İş yaptığım ve/veya hizmet aldığım şirketle paylaştığım her türlü bilginin mahremiyetine önem verilmesini isterim.	0.74			
* İş yaptığım ve/veya hizmet aldığım şirketle aramdaki iş süreçlerinin güvenlik anlamında devamlı denetleniyor ve bu denetleme sonucunda açık noktalarının düzeltiliyor olmasını isterim.	0.87			
* Aldığım hizmetin süresinin devamlı ölçülüyor olması ve iyileştirme noktalarının devamlı gözden geçiriliyor olmasını isterim.	0.58			
Örgütsel Bağlılık				
* Örgütün değerleri ile benim kişisel değerlerimi birbirine çok yakın bulmaktayım.		0.73		
* Bu firma, benim işimi en iyi şekilde yapmam konusunda beni motive etmektedir.		0.83		
* Bu firma, benim çalışabileceğim en iyi firmadır.		0.84		
* Bu firmanın geleceği benim için büyük bir önem taşımaktadır.		0.81		
* Bu örgütte çalışmayı tercih ettiğim için çok memnunum.		0.86		

Çalışan Memnuniyeti				
* Çalıştığım şirkette ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Standardının olmasını isterim.			0.65	
* Çalışacağım şirketin ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Standardına uygun olması, tercih sırasında önemli bir rol oynar.			0.76	
* Çalıştığım şirketin işe alım sürecinde referans kontrolü ve güvenlik analizi yapılması beni memnun eder.			0.79	
* Çalıştığım şirketin fiziksel güvenliğini sağlayan yangın söndürme sistemlerine sahip olmasını, özel güvenlik güçleri ile çalışıyor olmasını, giriş/çıkış ları denetim altına alıyor olmasını isterim.			0.74	
* Çalıştığım Şirketteki iş süreçlerinin Bilgi Güvenliği Yönetim Sistemine göre oluşturulmuş olmasını isterim.			0.73	
Gizlilik				
* Kritik Bilgilerin erişim izinleri belirli aralıklarla kontrol edilerek, tekrar düzenlenmektedir.				0.74
* Şirket bilgisayarına kullanıcı adı ve şifre ile girmemi zorunlu kılan sistem, bilgilerin mahremiyetini sağlar.				0.76
* Şirket bilgisayarındaki anti-virüs programı, bilgilerin mahremiyetini korur.				0.74
* Şifrelerin post-it'lerin üzerinde olmasını, mesai saatleri dışında çalışma belgelerinin herkesin erişimine açık(muhafazasız) bir şekilde tutulmasını engelleyecek Temiz Masa politikası uygulanmalıdır.				0.73
* Kullanıcıların bilgisayar başından uzaklaştıktan kısa bir zaman sonra bilgisayar ekranının otomatik olarak kilitlenmesini sağlayacak Temiz Ekran Politikası uygulanmalıdır.				0.72
* Elektronik ortamda kritik bilgiler, bir yerden başka bir yere transfer edilirken ve her hangi bir medya da saklanırken kriptolanmalıdır/şifrelenmelidir.				0.69

Tablo 4.6. BG ve Şirket Performansı dinamiklerine ait faktör yükleri

Değişken	Faktör 1	Faktör 2	Faktör 3	Faktör 4
Erişilebilirlik/Kullanılabilirlik				
* Uygulamalara ve sistemlere erişim yetkilendirmeleri belirli periyotlarda kontrol edilmektedir.	0.86			
* İlgili çalışan veya müşterinin, yetkilendirilerek ihtiyacı olduğu anda doğru bilgiye erişmesi sağlanmaktadır.	0.87			
* Felaket durumları için gerekli bilgiler yedeklenmekte ve erişilebilirlikleri düzenli olarak kontrol edilmektedir.	0.88			
* Yangın söndürme ve Jenaratör/UPS sistemleri, uygulamaların devamlılığını sağlamaktadır.	0.81			
* Uygulamalar ve üzerlerinde çalıştıkları sistemlerin hizmet seviyeleri ve sistem performansları düzenli olarak izlenmekte, gözden geçirilmekte ve kontrol edilmektedir.	0.86			
Bütünlük/Doğruluk				
* Bilgi hangi formda(elektronik posta, kağıt... vb.) olursa olsun bütünlüğü/doğruluğu en iyi şekilde korunması gereken bir varlıktır.		0.74		
* Doğruluğu/bütünlüğü/güncelliği sağlanamayan bilginin herhangi bir değeri yoktur.		0.72		
* Bilginin bütünlüğünün bozulmasını engellemek için kritik bilgiler düzenli olarak yedeklenmektedir.		0.80		
* Şirket için önemli olan bilgilerin yetkisiz kişiler tarafından değiştirilmesine veya yok edilmesi karşı gerekli önlemler alınmaktadır.		0.77		
* İş yaparken güncel bilgilerle çalışmak doğru sonuçların üretilmesini sağlar.		0.65		
Süreç Yaklaşımı				
* Şirketin iş süreçlerinin Bilgi Güvenliği Yönetim Sistemine göre yapılandırılmış olması iş yapış hızını olumlu yönde etkiler.			0.70	
* İş süreçlerinin performans hedefleri tanımlanmış ve bu hedefler sürekli ölçülmektedir.			0.87	

* Tanımlı olan hedefler, periyodik olarak gözden geçirilmekte, sürekli iyileştirilmektedir.			0.88	
* İş süreçlerinin bilgi varlığı olarak tanımlanması, risklerinin değerlendirilmesi için önemlidir.			0.79	
* Kritik Bilgilerin erişim izinleri için şirket süreçleri mevcuttur.			0.81	
Genel Performans				
* Daha başarılıdır				0.85
* Daha yüksek Pazar payına sahiptir				0.85
* Daha hızlı büyümektedir				0.80
* Daha karlıdır				0.83
* Daha yenilikçidir				0.87
* Daha büyük ölçeğe sahiptir				0.83

Tablo 4.7. BG ve Şirket Performansı dinamiklerine ait faktör yükleri

	Değişkenler	2	2	3	4	5	6	7	8
1	Gizlilik	--							
2	Bütünlük	,525(**)	--						
3	Erişilebilirlik	,548(**)	,593(**)	--					
4	Müşteri Memnuniyeti	,472(**)	,374(**)	,487(**)	--				
5	Çalışan Memnuniyeti	,577(**)	,458(**)	,435(**)	,489(**)	--			
6	Örgütsel Bağlılık	,377(**)	,389(**)	,364(**)	,275(**)	,280(**)	--		
7	Süreç Yaklaşımı	,631(**)	,483(**)	,622(**)	,303(**)	,478(**)	,391(**)	--	
8	Genel Performans	,479(**)	,431(**)	,520(**)	,274(**)	,376(**)	,543(**)	,557(**)	--
	Ortalama	4,48	4,57	4,42	4,68	4,43	3,87	4,19	4,41
	Standart Sapma	0,50	0,46	0,61	0,39	0,49	0,62	0,66	0,65

* $p < .05$, ** $p < .01$

Tablo 4.8. Korelasyon, ortalama ve standart sapma değerleri

4.6 Hipotez Testleri

Şekil 4.1'de gösterilen teorik model kapsamındaki ilişkileri test etmek amacıyla latent değişken (LV) skorlarının açık ve net bir şekilde hesaplanmasına izin veren PLS yol modeli analizi kullanılmaktadır.

Tablo 4.9'dan tablo 4.12'e gösterildiği üzere sonuçlar, hipotezlerimizin büyük bir kısmını doğrular niteliktedir. Öncüllerle ilgili olarak baktığımızda; Bilgi Güvenliği Gizlilik unsurunun Müşteri Memnuniyeti ($\beta = .0,28, p < 0,01$), Çalışan Memnuniyeti ($\beta = .0,44, p < 0,01$), Örgütsel Bağlılık ($\beta = .0,20, p < 0,01$) ve Süreç Yaklaşımı ($\beta = .0,40, p < 0,01$) ile pozitif ilişkili olduğu; böylece de H1'in tamamen desteklendiği görülmektedir. Bilgi Güvenliği Bütünlük/Doğruluk unsurunun ise Çalışan Memnuniyeti ($\beta = .0,16, p < 0,01$) ve Örgütsel Bağlılık ($\beta = .0,20, p < 0,01$) ile pozitif ilişkili olduğu; böylece de H2'in kısmen desteklendiği görülmektedir. Buna ilaveten Bilgi Güvenliği Erişilebilirlik/Kullanılabilirlik unsurunun Müşteri Memnuniyeti ($\beta = .0,32, p < 0,01$) ve Süreç Yaklaşımı ($\beta = .0,38, p < 0,01$) ile pozitif ilişkili olduğu; böylece de H3'ün kısmen desteklendiği görülmektedir. Son olarak ise Şirket Performansının, şirket performansına etki eden değişkenlerden Örgütsel Bağlılık ($\beta = .0,37, p < 0,01$) ve Süreç Yaklaşımı ($\beta = .0,39, p < 0,01$) ile pozitif ilişkili olduğu, böylece de H4'ün kısmen desteklendiği görülmektedir.

Tablo 4.13'de PLS kullanılarak elde edilen verilen sonuçlara göre model; Müşteri Memnuniyeti dinamiklerindeki değişimin %31'ini, Çalışan Memnuniyeti dinamiklerindeki değişimin %72'sini, Örgütsel Bağlılık dinamiklerindeki değişimin %21'ini, Süreç Yaklaşımı dinamiklerindeki değişimin %52'sini ve Şirket Performansı dinamiklerindeki değişimin %46'nı açıkladığını göstermektedir.

Hipotez	İlişkiler	β	Sonuçlar
H1	Gizlilik → Müşteri Memnuniyeti	0,28***	Tamamen Desteklendi
	Gizlilik → Çalışan Memnuniyeti	0,44***	
	Gizlilik → Örgütsel Bağlılık	0,20***	
	Gizlilik → Süreç Yaklaşımı	0,40***	

Tablo 4.9. Gizlilik unsurunun Şirket Performansı dinamikleri üzerindeki etkileri

Hipotez	İlişkiler	β	Sonuçlar
H2	Bütünlük → Müşteri Memnuniyeti	0,03	Kısmen Desteklendi
	Bütünlük → Çalışan Memnuniyeti	0,16***	
	Bütünlük → Örgütsel Bağlılık	0,20***	
	Bütünlük → Süreç Yaklaşımı	0,05	

Tablo 4.10. Bütünlük unsurunun Şirket Performansı dinamikleri üzerindeki etkileri

Hipotez	İlişkiler	β	Sonuçlar
H3	Erişilebilirlik → Müşteri Memnuniyeti	0,32***	Kısmen Desteklendi
	Erişilebilirlik → Çalışan Memnuniyeti	0,10	
	Erişilebilirlik → Örgütsel Bağlılık	0,14	
	Erişilebilirlik → Süreç Yaklaşımı	0,38***	

Tablo 4.11. Erişilebilirlik unsurunun Şirket Performansı dinamikleri üzerindeki etkileri

Hipotez	İlişkiler	β	Sonuçlar
H4	Müşteri Memnuniyeti → Şirket Performansı	0,02	<i>Kısmen Desteklendi</i>
	Çalışan Memnuniyeti → Şirket Performansı	0,08	
	Örgütsel Bağlılık → Şirket Performansı	0,37****	
	Süreç Yaklaşımı → Şirket Performansı	0,39****	

Tablo 4.12 Şirket Performansı öncüllerinin Şirket Performansı dinamikleri üzerindeki etkileri

Uyum ölçekleri	İçsel Değişkenler	Nihai model
R^2	Müşteri Memnuniyeti	0,31
	Çalışan Memnuniyeti	0,72
	Örgütsel Bağlılık	0,21
	Süreç Yaklaşımı	0,52
	Şirket Performansı	0,46

* $p < .1$, ** $p < .05$, *** $p < .01$

Tablo 4.13 Modellerin açıklama kuvveti

5. SONUÇ ve ÖNERİLER

Kuruluşların günümüzde en büyük zorluklarından ve zorunluluklarından birisi iş için kullandıkları bilgi ve verilerin gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanmasıdır. Kuruluşlar, günden güne rekabetin her alanda arttığı pazarda rakiplerinden bir adım daha önde olmak için iş yapış şekillerini belirleyen süreçlerini bilgi güvenliği bakış açısında oluşturmaktadır. Yasal ve düzenleyici gereksinimlere, en iyi uygulamalar göz önüne alınarak uyumluluğu sağlamayı, yalnızca ülke içinde değil, dünyada en büyükler arasında yer alabilmenin temel şartı olarak görmelidirler.

Analiz bulguları, bilgi güvenliği yönetim sistemi boyutlarından gizlilik ile müşteri memnuniyeti, çalışan memnuniyeti, örgütsel bağlılık ve süreç yaklaşımı arasında pozitif bir ilişkinin varlığını göstermekte; bütünlük ile çalışan memnuniyeti ve örgütsel bağlılık arasında olumlu bir ilişkinin varlığını ortaya çıkartmakta; bilgi yönetim sistemlerinin son boyutu erişilebilirlik ile de müşteri memnuniyeti ve süreç yaklaşımı arasında pozitif ve anlamlı bir ilişkinin olduğunu ortaya koymaktadır. Dolayısıyla bu çalışma, bilgi yönetim sistemleri ile bahsi geçen bu örgütsel değişkenler arasındaki varlığını destekler nitelikte kanıt sağlamaktadır. Bu çok önemli bir bulgudur. Nitekim bilgi güvenliği yönetim sistemleri böylesi bir ampirik araştırma kapsamında incelenerek örgütsel değişkenler üzerindeki etkileri gözler önüne serilmektedir.

Analizlerimizin ikinci kısmında ise bahsi geçen bu örgütsel değişkenlerin firma performansı ile olan ilişkileri araştırılmaktadır. Sonuçlar, örgütsel bağlılık ve süreç yaklaşımı ile firma performansı arasındaki ilişkiyi ortaya koyarak; bilgi güvenliği yönetim sistemlerinin bu değişkenler aracılığı ile firma performansını etkilediğini göstermektedir. Dolayısıyla araştırmamızın başından beri öngördüğümüz üzere; bilgi güvenliği yönetim sistemleri, firma performansı üzerinde dolaylı ancak önemli bir etkiye sahip bir yönetim uygulaması olarak karşımıza çıkmaktadır

Bu noktada firmaların bilgi güvenliği husunda ele almaları gereken bazı öncelikli konular mevcuttur. Kuruluşlar Bilgi Güvenliği Yönetim Sistemini bünyelerine uygulayabilmek için öncelikle üst yönetimin desteğini almalıdırlar ki bu yönetim sisteminin kurulması için yeterli ve doğru kaynak aktarılabilsin. Öncelikle tüm kurumun istisnasız uyması gereken Bilgi Güvenliği politikaları tanımlanmalıdır. Burada önemli olan nokta yazılacak politikaların, kurumun iş ihtiyaçlarına ve kabiliyetlerine uygun olmasıdır. Aksi takdirde politikalar yazılı olarak kalacak, süreçlere uygulanmayacaktır. Bilgi Güvenliğinde önemli olan diğer bir konu da üst yönetimin desteği alınarak hazırlanan politikaların ve aynı zamanda Bilgi Güvenliği temellerinin istisnasız tüm kurum çalışanlarına anlatılması, gerekli farkındalığın sağlanmasıdır. Burada amaç Bilgi Güvenliğinin örgütsel hafızaya kazandırılarak örgüt kültürü haline getirilmesidir.

Genelde Bilgi Güvenliği sorumluluğunun kurumun/örgütün güvenlik temsilcilerinde olduğu düşünülmektedir. Bu yanlış bir kanıdır. Güvenlik takım oyunudur ve bu görev sadece şirketlerdeki güvenlik birimlerinde görev alan veya güvenlik danışmanlarının görev ve sorumluluğu olmamalıdır. Tüm şirket çalışanlarının görev ve sorumluluğu altında şekillenmeli ve yürütülmelidir.

Bilgi Güvenliği Yönetim Sistemi, kurulup bırakılacak bir yönetim şekli olmamalıdır. Güvenlik, bir ürün değil bir süreç olarak düşünülmeli, şirket süreçlerine dahil edilmeli kısaca PUKÖ döngüsü döndürülmelidir. Yüzde Yüz güvenliğin olmadığı unutulmamalı, kurumun içinde olduğu sektörsel ihtiyaçlar göz önüne alınarak güvenlik kontrolleri dengeli bir şekilde uygulanmalıdır.

Kurumun/Örgütün içinde bulunmuş olduğu sektörsel güvenlik ihtiyaçlarına göre uygulanmış Bilgi Güvenliği Yönetim Sistemi, gerek bu kurumdan hizmet alan müşterilerin ve gerekse ilgili kurumda çalışan personelin memnuniyetini olumlu yönde arttıracak, bu memnuniyet beraberinde kurumun performansını olumlu yönde etkileyecektir.

5.1 Sınırlandırmalar

Bu çalışmanın sonuçlarının genellenebilirliğini engellemekte olan bir takım metodolojik sınırlandırmalar mevcuttur: Öncelikle veri toplama süreci, sadece İstanbul kapsamında bir GSM firmasına gerçekleştirilmiştir; daha homojen bir örneklem kitlesinin daha genellenebilir sonuçlara götürebilmesi muhtemeldir. İkinci olarak analiz süresince sektörsel bir dağılıma gidilmemiştir; oysa sonuçlar GSM dışındaki farklı sektörler ve farklı firmalar için değişim gösterebilir; bu değişim, bilgi güvenliği yönetim sistemi dinamiklerinin farklı sektörlerde nasıl işlediğinin anlaşılmasına katkıda bulunabilir. Son olarak da burada gerçekleştirilen analizler 200 adet katılımcıdan alınan verilere dayanmaktadır; daha geniş bir örneklem kitlesinin daha doğru sonuçlar verebileceği de göz önüne alınması gereken bir husustur.

5.2 Öneriler

Bilgi güvenliği kavramı ve bilgi güvenliği yönetim sistemi olgusu, özellikle de enformasyon ve iletişim teknolojilerindeki gelişmelerin artan ivmesi de dikkate alındığında günümüz ekonomi ve yönetim literatüründe popüleritesi artmakta olan bir konudur. Bilgi ekonomisinin beraberinde getirdiği yeni koşullar dahilinde artık özelleşmiş bir bilgi güvenliği kavramı ve bilgi güvenliği yönetim sistemi mekanizmalarının ve performans üzerindeki nihai etkilerinin daha iyi anlaşılması, bu konuyla ilgili yapılacak bir çok çalışmaya ışık tutacaktır. Bilgi Güvenliği Yönetim Sistemleri üzerine gelecekte çalışmalarda bulunacak olan araştırmacılara:

- i. Öncelikle örneklem kitlesini tek bir firma ile sınırlı kalmayıp daha geniş ve daha homojen bir örneklem kitlesi kullanmaları,
- ii. Örneklem kitlesini sadece İstanbul ile sınırlandırmayıp; ülke geneli hatta mümkünse uluslar arası verilere ulaşmaları,
- iii. Bilgi algısal bir kavram olduğundan bu süreci etkileyebilecek yeni değişkenler de katarak teoriyi genişletmeleri,
- iv. Bilgi Güvenliği Yönetim Sistemleri ile firma yenilikçiliği arasındaki ilişkileri de inceleyerek olayı daha geniş perspektiften ele almaları önerilmektedir.

KAYNAKLAR

Allen N.J., Meyer J.P., (1991), A Three Component Conceptualization of Organizational Commitment. Human Resource Management Review,1, 61–89.

Allen N.J., Meyer J.P., (1996). Affective, Continuance, and Normative Commitment to the Organization: An Examination of Construct Validity, Journal of Vocational Behavior, 49, 252–276.

Alpkan L.,Ergün E.,Bulut Ç., Yılmaz C.,(2005),"Şirket Girişimciliğinin Şirket Performansına Etkileri",Doğuş Üniversitesi Dergisi, 6 (2),175-189

Ashenden D.,(2008),"Information Security management: A human challenge?", Information security technical report 13 (2008), 195-201

Bai B., Law R., Wen I.,(2008),"The impact of website quality on customer satisfaction and purchase intentions: Evidence from Chinese online visitors", International Journal of Hospitality Management 27,391–402

Baysal C., Tekarslan E.,(1998) "Davranış Bilimleri",İstanbul Üniversitesi, İşletme Fakültesi Yayını, No:275, s. 102

Broderick J.S.,(2006), "ISMS, security standards and security regulations", information security technical report II (2006), 26–31

Boehmer W.,(2008),"Appraisal of the effectiveness and efficiency of an Information Security Management System based on ISO 27001", The Second International Conference on Emerging Security Information, Systems and Technologies, 224-231

Bialas A.,(2006),"Information Security Systems vs. Critical Information Infrastructure Protection Systems – Similarities and Differences",Proceedings of the International Conference on Dependability of Computer Systems (DEPCOS-RELCOMEX'06),1-8

Chi C.G.,Gursoy D., (2009),"Employee satisfaction, customer satisfaction, and financial performance: An empirical examination",International Journal of Hospitality Management 28,245–253

COBIT 4.1 (Control Objectives for Information and Related Technology), (2007), Framework Control Objectives Management Guidelines Maturity Models, IT Governance Institute ,1-196

Çetin M.Ö., (2004), Örgüt Kültürü ve Örgütsel Bağlılık. Ankara: Nobel Yayın Dağıtım

Day M., (2007),"Information Security Management - A Practical Approach", IEEE, 1-6

Epitropaki O., Martin R., (2005). The Moderating Role of Individual Differences in The Relation Between Transformational/ Transactional Leadership Perceptions and Organizational Identification. The Leadership Quarterly, 16, 569–589.

Emir O., Baytok A., (2004), 1. Balıkesir Turizm Kongresi, s.254

Evans J.R., Lindsay W.M., 2002, "The Management and Control of Quality", 5th Ed., South-Western Thomas Learning, USA,

Eloff J.H.P., Eloff M.M.,(2005),"Information security architecture",Coumputer Fraud & Security,10-16

Farn K.J., Lin S.K. and Fung A.R.W.,(2004), "A study on information security management system evaluation—assets, threat and vulnerability", Computer Standards & Interfaces, 501–513

Fasanghari M., NasserEslami F., Naghavi M., (2008), "IT Governance Standard Selection Based on Two Phase Clustering Method", Fourth International Conference on Networked Computing and Advanced Information Management, 513-518

Forza, C., and Filippini, R., (1998), "TQM Impact ofn Quality Conformance and Customer Satisfaction", International Journal of Production Economics, Vol:55, Issue:1, 1-20.

Gronholdt, L., Martensen, A. and Kristensen, K., (2000), "The Relationship Betwen Customer Tatisfaction and Loyalty: Cross – Industry Differences". Department of Marketing. Copenhagen Business School. Denmark

Gerber M., Solms R., (2008), "Information security requirements – Interpreting the legal aspects", Computers & Security 27(2008), 124-135

ISO/IEC FDIS 27001:2005, (2005), Information technology - Security techniques - Information security management systems – Requirements, International Standart, 1-34

ISO/IEC FDIS 17799:2005, (2005), Information technology — Security techniques — Code of practice for information security management, International Standart, 1-115

Humphreys E., (2008), "Information security management standards: Compliance, governance and risk management", Information Security Technical Report 13 (2008), 247–255

Hochstein A., Zarnekow R., Brenner W., (2005), "ITIL as Common Practice Reference Model for IT Service Management: Formal Assessment and Implications for Practice", The 2005 IEEE International Conference, 704-710

Kritzinger E., Smith E.,(2008),"Information security management: an information security retrieval and awareness model for industry",Computers & Security 27, 224-231

Koç F.,(2008),"Varlık Envanteri Oluşturma Klavuzu", ULUSAL ELEKTRONİK VE KRİPTOLOJİ ARAŞTIRMA ENSTİTÜSÜ,1-17

Kajava J., Anttila J., Varonen R., Savola R, Roning J.,(2006), "Information Security Standards and Global Business", IEEE,2091-2095

Luthans F.,(1992),"Organizational Behaviour", 6th Ed. McGraw Hill

Miirray R., (2004), "Job Satisfaction of Professional and Praprofessional Library Staff at the University of North Caralina at Chapel HilF, s.3

Naumann, E., Jackson, D.W. and Rosenbaum, M.S. ,(2001), “How to Implement a Customer Satisfaction Program”, Business Horizons, January-February 2001, New York, USA, 37-46.

Nicho M., Cusack B.,(2007),"A Metrics Generation Model for Measur ing the Control Objectives of Information Systems Audit",Proceedings of the 40th Hawaii International Conference on System Sciences - 2007,1-11

Nabiollahi A., Sahibuddin S.,(2008),"Considering Service Strategy in ITIL V3 as a Framework for IT Governance", White Paper

O'Reilly C., Chatman J.,(1986), Organizational Commitment and Psychological Attachment: The Effects of Compliance, Identification and Interlization on Prosocial Behaviour. Journal of Applied Psychology, 71, 492–499.

Obeng K., Ugboro I., (2003), Organizational Commitment Among Public Transit Employees: an Assessment Study. Journal of the Transportation Research Forum, 57, 83–98

Önel D., Dinçkan A.,(2007),"Bilgi Güvenliği Yönetim Sistemi Kurulumu",
ULUSAL ELEKTRONİK VE KRİPTOLOJİ ARAŞTIRMA ENSTİTÜSÜ, 1-16

Örücü E., Çolak R.,(2002),"Üniversite Öğretim Elemanlarında İş Doyumu ve
Motivasyon",Muğla Üniversitesi İ.İ.B.F.,İktisat İşletme ve Finans, Sayı:3,Cilt:16,
s.12.

Örs M., Acuner A.M., Sarp N., Önder Ö.R., (2003). Antalya Tıp Fakültesi
Hastanesin’de ve Antalya Devlet Hastanesinde Çalışan Hekimler ile Hemşirelerin
Örgülerine Bağlılıklarına İlişkin Görüşlerinin Değerlendirilmesi. Ankara Üniversitesi
Tıp Fakültesi Mecmuası, 56 (4), 217–224.

Ruighaver A.B., Maynard S.B.,Chang S.,(2007),"Organisational security culture:
Extending the end-user perspective", Computers & Security 26 (2007), 56-62

Rose M., (2003) ,"Good Deal, Bad Deal? Job Satisfaction in Occupations", Work,
Employment and Society, Vol:17 (3), s.506

Sahibudin S., Sharifi M. and Ayat M.,(2008), "Combining ITIL, COBIT and
ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in
Organizations", Second Asia International Conference on Modelling & Simulation,
749-753

Savola R.,(2006),"Information Security Management in Industrial Automation
Systems", IEEE,1648-1653

Spremić M., Zmirak Z., Kraljevic K.,(2008),"IT and Business Process
Performance Management: Case Study of ITIL Implementation in Finance Service
Industry", Proceedings of the ITI 2008 30th Int. Conf. on Information Technology
Interfaces,243-250

Solms S.H.,(2005),"Information Security Governance - Compliance management vs operational management",Computers & Security (2005) 24, 443-447

Solms B.,(2006),"Information Security – The Fourth Wave", Computers & security 25(2006),165–168

Solms B.,(2005),"Information Security governance: COBIT or ISO 17799 or both?",Computers & Security 24 (2005), 99-104

Solomon, M., (1996), Consumer Behavior. 2.nd ed. Allyn&Bacon. Boston. Yamak, O. (1998). Kalite Odaklı Yönetim. İstanbul: Komputron Ltd.

Şimşek L., (1995), "İş Tatmini" Verimlilik Dergisi, s.92

Şimşek Ş, Akgemici T., Çelik A., (1998), "Davranış Bilimlerine Giriş ve Örgütlerde Davranış", Nobel Yayın Dağıtım - Ankara

Türkyılmaz, A. ve Özkan, C., (2003), “Ulusal Müşteri Memnuniyet İndeksleri”, Üretim Araştırmaları Sempozyumu, 19-20 Nisan 2003, İstanbul.

Tvrđíková M.,(2008),"Information system integrated security", 7th Computer Information Systems and Industrial Management Applications,153-154

TS EN ISO 9001:2000, (2001),"Kalite Yönetim Sistemi - Şartlar", Türk Standartları Enstitüsü, s.27

Yıldız B., (2007), “Bilgi Güvenliği ve E-Devlet Kapsamında Kamu Kurumlarında Bilgi Güvenliği Yönetimi Standartlarının Uygulanması”, Gebze Yüksek Teknoloji Enstitüsü - Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi

Yoshio K., (2001), “Customer satisfaction: How can I measure it?”, Total Quality Management, Vol. 12, No: 7-8, 867- 872.

Woodhouse S.,(2008), "An ISMS (Im)-Maturity Capability Model", IEEE 8th International Conference on Computer and Information Technology Workshops, 242-247

Wagner H.-T.,2006,"Managing the Impact of IT on Firm Success: The Link between the Resource-based View and the IT Infrastructure Library",Proceedings of the 39th Hawaii International Conference on System Sciences,1-10

27K implementers' Forum, (2009 January, 3),Version 3,
www.iso27001security.com

<http://www.27000.org/ismsprocess.htm>

ÖZGEÇMİŞ

1979 yılında Isparta’da doğdu. İlk, orta ve lise öğrenimini İzmir’de tamamladıktan sonra 1997 yılında İstanbul Üniversitesi Bilgisayar Bilimleri Mühendisliği bölümünde lisans eğitimine başladı ve 2001 yılında mezun oldu.

2003 yılında askerlik hizmetini Malatya 2nci Ordu 550. İs. İnş. Tb.’da Yedek Subay olarak tamamladı. 2003-2007 yılları arasında VESTEL Şirketler Grubuna bağlı DEXAR Mutimedya ve Telekomünikasyon A.Ş.’de Network Mühendisi olarak çalıştı. 2007 yılı Mart ayında başladığı Turkcell Şirketler Grubuna bağlı GLOBAL BİLGİ A.Ş.’de Bilgi Güvenliği Uzmanı olarak halen devam etmektedir.

EK-1 Anket Formu Örneđi



GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ

Sayın İlgili,

Bu anket formu, Gebze Yüksek Teknoloji Enstitüsü İşletme Fakültesi tarafından yürütölmekte olan “**Bilgi Güvenliđi Kavramı ve Bilgi Güvenliđi Yönetim Sistemleri ile Şirket Performansı İlişmesine Dair Bir Uygulama**” konulu araştırmanın uygulama kısmı ile ilgilidir. Bu araştırma çalışması tamamen akademik bir çalışma olup, bilimsel bir amaca yönelik olarak kullanılacaktır. Gönderilecek cevaplarda firmalarla ilgili bilgiler kesinlikle gizli tutulacak olup, elde edilecek sonuçlar firma adı belirtilmeksizin genel ve ortalama değerler ile tez çalışmasında kullanılacaktır.

Anketi oluşturan soruları cevaplandırmak şüphesiz çok kıymetli zamanınızın bir kısmını alacaktır. Şimdiden teşekkür eder, çalışmalarınızda başarılar dileriz.

Saygılarımızla,

Doç.Dr. Halit KESKİN

GYTE İşletme Fakültesi, Strateji Bilimi Bölümü

Kerem ASLANDAĞ

GYTE İşletme Fakültesi, Strateji Bilimi Bölümü Öğrencisi

A. Kişisel özellikler

Cinsiyetiniz: Kadın () Erkek ()
Yaşınız: 18 altı () 18-24 () 25-34 () 35-50 () 50-65 () 65 ve üstü ()
Mesleğiniz:
Eğitim Durumunuz: İlkokul () Ortaokul-Lise () Ön Lisans () Üniversite () Yüksek Lisans-Doktora ()
Çalıştığınız firmadaki ünvanınız? (lütfen birini seçiniz) _____ 1 Başkan/Sahip _____ 2 Genel Müdür _____ 3 Bölüm/Takım Müdürü _____ 4 Mühendis/ Teknisyen 5_____ Kıdemli Mühendis _____ 6 Diğer:

B. Aşağıda cevaplayacağınız bölümde her soru için 1-5 arasında sadece bir rakam işaretlenecektir. Rakamların anlamları aşağıdaki kutuların içinde belirtilmiştir.

1	2	3	4	5					
(Kesinlikle katılmıyorum)	(Katılmıyorum)	(Kararsızım)	(Katılıyorum)	(Kesinlikle katılıyorum)					
Müşteri Memnuniyeti									
1. İş yaptığım ve/veya hizmet aldığım şirketin ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemi standardının olmasını isterim.	1	2	3	4	5				
2. İş yaptığım ve/veya hizmet aldığım şirketle paylaştığım her türlü bilginin mahremiyetine önem verilmesini isterim.	1	2	3	4	5				
3. İş yaptığım ve/veya hizmet aldığım şirketle aramdaki iş süreçlerinin güvenlik anlamında devamlı denetleniyor ve bu denetleme sonucunda açık noktalarının düzeltiliyor olmasını isterim.	1	2	3	4	5				
4. Aldığım hizmetin süresinin devamlı ölçülüyor olması ve iyileştirme noktalarının devamlı gözden geçiriliyor olmasını isterim.	1	2	3	4	5				
Örgütsel Bağlılık									
5. Örgütün değerleri ile benim kişisel değerlerimi birbirine çok yakın bulmaktayım.	1	2	3	4	5				

6. Bu firma, benim işimi en iyi şekilde yapmam konusunda beni motive etmektedir.	1	2	3	4	5
7. Bu firma, benim çalışabileceğim en iyi firmadır.	1	2	3	4	5
8. Bu firmanın geleceği benim için büyük bir önem taşımaktadır.	1	2	3	4	5
9. Bu örgütte çalışmayı tercih ettiğim için çok memnunum.	1	2	3	4	5
Çalışan Memnuniyeti					
10. Çalıştığım şirkette ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Standardının olmasını isterim.	1	2	3	4	5
11. Çalışacağım şirketin ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Standardına uygun olması, tercih sırasında önemli bir rol oynar.	1	2	3	4	5
12. Çalıştığım şirketin işe alım sürecinde referans kontrolü ve güvenlik analizi yapılması beni memnun eder.	1	2	3	4	5
13. Çalıştığım şirketin fiziksel güvenliğini sağlayan yangın söndürme sistemlerine sahip olmasını, özel güvenlik güçleri ile çalışıyor olmasını, giriş/çıkış ları denetim altına alıyor olmasını isterim.	1	2	3	4	5
14. Çalıştığım Şirketteki iş süreçlerinin Bilgi Güvenliği Yönetim Sistemine göre oluşturulmuş olmasını isterim.	1	2	3	4	5
Gizlilik					
15. Kritik Bilgilerin erişim izinleri belirli aralıklarla kontrol edilerek, tekrar düzenlenmektedir.	1	2	3	4	5
16. Şirket bilgisayarına kullanıcı adı ve şifre ile girmemi zorunlu kılan sistem, bilgilerin mahremiyetini sağlar.	1	2	3	4	5
17. Şirket bilgisayarındaki anti-virüs programı, bilgilerin mahremiyetini korur.	1	2	3	4	5
18. Şifrelerin post-it'lerin üzerinde olmasını, mesai saatleri dışında çalışma belgelerinin herkesin erişimine açık(muhafazasız) bir şekilde tutulmasını engelleyecek Temiz Masa politikası uygulanmalıdır.	1	2	3	4	5
19. Kullanıcıların bilgisayar başından uzaklaştıktan kısa bir zaman sonra bilgisayar ekranının otomatik olarak kilitlenmesini sağlayacak Temiz Ekran Politikası uygulanmalıdır.	1	2	3	4	5
20. Elektronik ortamda kritik bilgiler, bir yerden başka bir yere transfer edilirken ve her hangi bir medya da saklanırken kriptolanmalıdır/şifrelenmelidir.	1	2	3	4	5
Erişilebilirlik/Kullanılabilirlik					
21. Uygulamalara ve sistemlere erişim yetkilendirmeleri belirli periyotlarda kontrol edilmektedir.	1	2	3	4	5
22. İlgili çalışan veya müşterinin, yetkilendirilerek ihtiyacı olduğu anda doğru bilgiye erişmesi sağlanmaktadır.	1	2	3	4	5
23. Felaket durumları için gerekli bilgiler yedeklenmekte ve erişilebilirlikleri düzenli olarak kontrol edilmektedir.	1	2	3	4	5
24. Yangın söndürme ve Jenaratör/UPS sistemleri, uygulamaların devamlılığını sağlamaktadır.	1	2	3	4	5
25. Uygulamalar ve üzerlerinde çalıştıkları sistemlerin hizmet seviyeleri ve sistem performansları düzenli olarak izlenmekte, gözden geçirilmekte ve kontrol edilmektedir.	1	2	3	4	5

Bütünlük/Doğruluk					
26. Bilgi hangi formda(elektronik posta, kağıt... vb.) olursa olsun bütünlüğü/doğruluğu en iyi şekilde korunması gereken bir varlıktır.	1	2	3	4	5
27. Doğruluğu/bütünlüğü/güncelliği sağlanamayan bilginin herhangi bir değeri yoktur.	1	2	3	4	5
28. Bilginin bütünlüğünün bozulmasını engellemek için kritik bilgiler düzenli olarak yedeklenmektedir.	1	2	3	4	5
29. Şirket için önemli olan bilgilerin yetkisiz kişiler tarafından değiştirilmesine veya yok edilmesi karşı gerekli önlemler alınmaktadır.					
30. İş yaparken güncel bilgilerle çalışmak doğru sonuçların üretilmesini sağlar.	1	2	3	4	5
Süreç Yaklaşımı					
31. Şirketin iş süreçlerinin Bilgi Güvenliği Yönetim Sistemine göre yapılandırılmış olması iş yapış hızını olumlu yönde etkiler.	1	2	3	4	5
32. İş süreçlerinin performans hedefleri tanımlanmış ve bu hedefler sürekli ölçülmektedir.	1	2	3	4	5
33. Tanımlı olan hedefler, periyodik olarak gözden geçirilmekte, sürekli iyileştirilmektedir.	1	2	3	4	5
34. İş süreçlerinin bilgi varlığı olarak tanımlanması, risklerinin değerlendirilmesi için önemlidir.	1	2	3	4	5
35. Kritik Bilgilerin erişim izinleri için şirket süreçleri mevcuttur.	1	2	3	4	5
Genel Performans: Rakiplerle karşılaştırdığımızda şirketimiz:					
36. Daha başarılıdır	1	2	3	4	5
37. Daha yüksek Pazar payına sahiptir	1	2	3	4	5
38. Daha hızlı büyümektedir	1	2	3	4	5
39. Daha karlıdır	1	2	3	4	5
40. Daha yenilikçidir	1	2	3	4	5
41. Daha büyük ölçeğe sahiptir	1	2	3	4	5

Değerli zamanınızı ayırdığınız ve bilimsel çalışmamıza katkılarınız için teşekkürlerimizi sunarız.