

T.C.
GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ
MÜHENDİSLİK VE FEN BİLİMLERİ
ENSTİTÜSÜ

KAMU KURUMLARI İÇİN BİLGİ
GÜVENLİĞİ YÖNETİŞİM MODELİ

Hakkı TOK
YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

GEBZE

2010

T.C.
GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ
MÜHENDİSLİK VE FEN BİLİMLERİ
ENSTİTÜSÜ

KAMU KURUMLARI İÇİN BİLGİ
GÜVENLİĞİ YÖNETİŞİM MODELİ

Hakkı TOK
YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

TEZ DANIŞMANI
Doç.Dr. İbrahim SOĞUKPINAR

GEBZE

2010

GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ	MÜHENDİSLİK VE FEN BİLİMLERİ ENSTİTÜSÜ JÜRİ ONAY FORMU
---	---

JÜRİ

ÜYE (BAŞKAN).

ÜYE

ÜYE

Gebze Yüksek Teknoloji Enstitüsü Mühendislik ve Fen Bilimleri Enstitüsü Yönetim Kurulu'nun .../...../..... tarih ve/..... sayılı kararı ile yukarıdaki öğretim elemanlarından oluşmuş jüri tarafından düzenlenen/...../..... tarihli Tez Savunma Tutanağı neticesinde Yüksek Lisans öğrencisi **Hakkı TOK**'un çalışması GYTE Mühendislik ve Fen Bilimleri Yönetim Kurulu/...../..... tarih ve/..../..... sayılı kararıyla Bilgisayar Mühendisliği Anabilim Dalında Yüksek Lisans tezi olarak onaylanmıştır.

İMZA/MÜHÜR

ÖZET

TEZİN BAŞLIĞI: KAMU KURUMLARI İÇİN BİR BİLGİ GÜVENLİĞİ YÖNETİŞİM MODELİ

YAZAR ADI : HAKKI TOK

Son yıllarda kamu kurum ve kuruluşlarının hızla artan ihtiyaçlarına paralel olarak, bilgi teknolojilerinin kullanımında büyük bir artış yaşanmış ve bilgi teknolojilerinden en iyi şekilde istifade etmek tüm kuruluşların başlıca amaçlarından biri haline gelmiştir.

Bilgiyi saklayan, ileten, değerlendiren ve yeniden üreten sistemler, kurumların yapılarında hayati bir önem kazandığı gibi, teknolojik imkanlar vesilesiyle kullanılan bilginin güvenliği de yeni bir çalışma alanı olarak ön plana çıkmıştır. Artık bilgi güvenliği için önlem almak ve alınan önlemleri (kararları) titizlikle uygulamak her kurum için dikkatle üzerinde durulan bir çalışma alanı olmuştur.

Bilgi güvenliğine verilen önemin bir gereği olarak, son yıllarda kurumsal organizasyonlar tarafından “Bilgi Güvenliği Yönetişimi” kavramı geliştirilmiştir ve netice itibariyle bugün her kurum, kendi kurumsal işleyişine uygun olan bir “Bilgi Güvenliği Yönetişim Modeli” kurma ihtiyacı ve gayreti içerisine girmiştir.

“Kamu Kurumları İçin Bir Bilgi Güvenliği Yönetişim Modeli” adındaki bu çalışmada; Türkiye için kamu kurum ve kuruluşlarında kullanılacak yeni Bilgi Güvenliği Yönetişimi Modeli önerilmiştir. Öncelikle tek bir kamu kuruluşunda bu modelin nasıl uygulanacağı açıklanmıştır. Ayrıca modelin tek bir kurum ya da kuruluşun da kullanılması için tasarlanmasının yeterli olmayacağı düşüncesinden hareketle, önerilen modelde kurum ve kuruluşların birbirleriyle etkileşimini de içeren yeni bir yapı ortaya konulmuştur. Bu sistemin işleyebilmesi için de tüm kamu kurum ve kuruluşları ile birlikte özel şirketleri de içeren bir Bilgi Güvenliği Stratejisi Kurulu (BGSK)’nun kurulmasının gerekliliğine vurgu yapılarak, bilgi güvenliği konusunun yasal dayanaklarla desteklenmesi önerilmiştir. Bu modelin İstanbul Büyükşehir Belediyesi, bağlı kurumları ve iştirak şirketlerinde nasıl kurulabileceği örnek olarak anlatılmıştır.

SUMMARY

**TITLE : AN INFORMATION SECURITY GOVERNANCE
MODEL FOR GOVERNMENT**

AUTHOR : HAKKI TOK

In parallel to quickly emerging needs of government entities and institutions in recent years, huge advance has appeared in the usage of information Technologies, as a consequence, taking advantage of benefits of information technologies has become one of the primary aims of all organizations.

Security of the information produced by the new technological advances emerged a new work area, like systems - which store, convey, evaluate and reproduce the information - has gained very important position in the structure of organizations. Taking precautions for information security and applying these meticulously is the carefully cared area in every organization, anymore.

Information Security Governance concept is enlarged with respect to the requirement of the importance of information security, as a consequence, nowadays, all organizations are spending effort for implementing a information technology governance model which is suitable with their organizational processes.

The model of Information Security Governance proposed by Solms is discussed in this article and a new model developed based on the Solms's model is offered to use in public sector and government entity. First of all, it is explained how this model is implemented to one sample government entity. Besides, a new structure including the interaction of the public sector and government entities is introduced to the proposed model due to the knowledge that designing a model with respect to only one government entity is not enough sufficiently. Initially, it is defined how Information Security Governance is to be in only one public institution and its related organizations. In addition, it is explained how and at which level the institutions should be interacted in this model. Moreover, it is emphasized that it is necessary to establish an Information Security Strategies Committee consisting of all public sector and government entities to keep running this system properly. Information security issue certainly has to be supported with the appropriate legal basis. The implementation of the model is explained with a sample in Istanbul Metropolitan Municipality.

TEŞEKKÜR

İçerisinde bulunduğumuz iş yoğunluğunun sosyal hayatımızı ve aile hayatımızı da etkisi altına aldığı bir dönemde, başlanmış bir işi bitirme gayreti ve bu alandaki çalışmalara özgün bir çalışmayla katkı sağlama arzusu, bu çalışmanın tamamlanmasında temel motivasyon kaynağıydı.

Bu çalışmanın tamamlanmasında kişisel gayretlerim yanında, çeşitli boyutlarda ilgisini ve desteğini gördüğüm dostlarımın katkısını da görmezden gelemem.

Bu münasebetle; öncelikle bu çalışmada danışmanlığımı üstlenen, ilgi ve desteğini esirgemeyen Sayın Hocam Doç. Dr. İbrahim SOĞUKPINAR'a ve kendilerine yeterli zaman ayıramadığım halde anlayış gösteren, ilgi ve desteklerini her zaman yanımda hissettiğim kıymetli eşim, Sevdâ TOK'a ve çocuklarım Emin Safa, Eren Seza ve Eymen Sina'ya teşekkür ederim.

Ayrıca, bu çalışmanın hazırlanmasında ve özellikle Bilgi Güvenliği Yönetişimi örnek modelin hazırlanmasında, hem konuya ilişkin bilgi ve birikimleriyle hem de yöneticilik tecrübeleri ve yaratıcı fikirleriyle desteklerini hissettiren yönetici arkadaşlarım İBB Bilgi İşlem Müdürü Harun KAYA'ya, İBB Mali Kontrol Müdürü Abdulkadir İNCEOĞLU'na, İSKİ Bilgi İşlem Daire Başkanı Çetin ÇİBUK'a; çalışmanın imla ve redaksiyonu konusunda katkıda bulunan mesai arkadaşlarım Abdulkadir YELER'e ve Ünal GÖK'e, son olarak da bu çalışmanın hazırlanmasına dolaylı yollardan katkıda bulunan bütün dostlarıma teşekkür ederim.

İÇİNDEKİLER DİZİNİ

	<u>Sayfa</u>
ÖZET	iv
SUMMARY	v
TEŞEKKÜR	vi
İÇİNDEKİLER DİZİNİ	vii
SİMGELER VE KISALTMALAR DİZİNİ	ix
ŞEKİLLER DİZİNİ	x
TABLolar DİZİNİ	xii
1. GİRİŞ	1
2. BİLGİ GÜVENLİĞİ YÖNETİŞİMİ VE SOLMS'UN BİLGİ GÜVENLİĞİ YÖNETİŞİM. MODELİ	5
2.1. Bilgi Güvenliği Yönetimi, Bilgi Güvenliği Yönetişimi, Risk Yönetimi	5
2.2. Bilgi Güvenliği Yönetişimi ve İlgili Çalışmalar	20
2.3. Solms'un Bilgi Güvenliği Yönetişim Modeli	22
3. KAMU KURUMLARI İÇİN BİLGİ GÜVENLİĞİ YÖNETİŞİM MODELİ ÖNERİSİ	24
3.1. Tek Kurumda Bilgi Güvenliği Yönetişim Modeli	24
3.2. Bir Kurum ve O Kuruma Bağlı Organizasyonlar (Kurum, Kuruluş, Şirket) Arasında Bilgi Güvenliği Yönetişim Modeli	26
3.3. Kurumların Birbirleri Arasında Bilgi Güvenliği Yönetişim Modeli	27
3.4. Bütünleşik Bilgi Güvenliği Yönetişim Modeli	29
4. İBB, BAĞLI KURUMLAR VE İŞTİRAK ŞİRKETLERİ İÇİN ÖRNEK BİLGİ GÜVENLİĞİ YÖNETİŞİM MODELİ TASARIMI	30

4.1. İBB Yönetim Yapısı	30
4.2. İBB Tek Kurum Olarak Bilgi Güvenliği Yönetişim Modeli	32
4.3. İBB ve Bağlı Kurumlar (İSKİ-İETT) Modeli	33
4.4. İBB İştirak Şirketler için model	35
4.5. İbb Bağlı Kurumlar ve İştirak Şirketler İle Model	36
4.5.1. İBB ile Bağlı Kurumlar(İSKİ-İETT) ve I.Sınıf Bağlı Şirketlerle BGYM	36
4.5.2. İBB ile Bağlı II.Sınıf Bağlı Şirketlerle BGYM	37
4.6. İBB Geneli Entegre Bilgi Güvenliği Yönetişim Modeli	38
4.7. İç Kontrol Teşkilatı ve Önerilenmodelde Kontrol Döngüsünde Kullanılması	42
4.7.1. İç Kontrol Teşkilatı ve COSO Modeli	42
4.7.2. İç Kontrol Teşkilatının Bilgi Güvenliği Yönetişim Modelinde Kontrol Döğüsünde Kullanılması	50
5. SONUÇ ve ÖNERİLER	53
KAYNAKLAR DİZİNİ	55
ÖZGEÇMİŞ	57

SİMGELER VE KISALTMALAR DİZİNİ

BGYS	: Bilgi Güvenliği Yönetim Sistemi
BGYM	: Bilgi Güvenliği Yönetişim Modeli
BGSK	: Bilgi Güvenliği Stratejisi Kurulu
İBB	: İstanbul Büyükşehir Belediyesi
COBIT	: Control Objectives for IT and related Technologies
ITIL	: IT Infrastructure Library
ITGI	: IT Governance Institute
INTOSAI	: Uluslararası Sayıştaylar Birliği
COSO	: Committee of Sponsoring Organizations

ŞEKİLLER DİZİNİ

<u>Şekil</u>	<u>Sayfa</u>
1.1. Bilgi Güvenliği Yönetişimi	2
2.1. IS O27001 Süreçleri	5
2.2. COBIT Olgunluk Modeli	11
2.3. Bilgi Güvenliği Yönetişimi Kavramsal Diyagramı	12
2.4. Kıymet, tehdit ve açıklık fonksiyonu olarak risk	14
2.5. Risk analizi ve yönetiminin yeri	18
2.6. Bilgi Güvenliği Yönetişim Modeli	22
2.7. Solms'un Bilgi Güvenliği Yönetişim modeli	23
2.8. Detaylı Solms'un Bilgi Güvenliği Yönetişim modeli	23
3.1. Tek Kurum Bilgi Güvenliği Yönetişim modeli.	25
3.2. Kurum ve Bağlı-Kurum-Kuruluş-Şirket Bilgi Güvenliği Yönetişim modeli	27
3.3. Entegre Bilgi Güvenliği Yönetişim Modeli.	28
4.1. İBB Tek Kurum Bilgi Güvenliği Yönetişim Modeli.	33
4.2. İBB Bağlı Kurumlar Bilgi Güvenliği Yönetişim Modeli.	34
4.3. İBB Bağlı I.Sınıf Şirketler Bilgi Güvenliği Yönetişim Modeli.	35
4.4. İBB Bağlı II.Sınıf Şirketler Bilgi Güvenliği Yönetişim Modeli.	36
4.5. İBB ile Bağlı Kurumlar Arası Bilgi Güvenliği Yönetişim Modeli.	37
4.6. İBB ile Bağlı II.Sınıf Şirketler Arası Bilgi Güvenliği Yönetişim Modeli.	38
4.7. İstanbul Büyükşehir Belediyesi için Entegre Bilgi Güvenliği Yönetişim Modeli.	39

4.8.	İç Kontrol Yapısı	41
4.9.	COSO Piramidi	42
4.10.	COSO küpü	43
4.11.	İç Kontrol Standartları	44
4.12.	İç Kontrol Sisteminde farklı modellerin birlikte kullanımı	46

TABLÖLAR DİZİNİ

<u>Tablo</u>	<u>Sayfa</u>
1.1. BGYS Doğrular Yanlıřlar	7
4.1. İBB Baėlı I.Sınıf řirketler	31
4.2. İBB Baėlı II.Sınıf řirketler	31

1. GİRİŞ

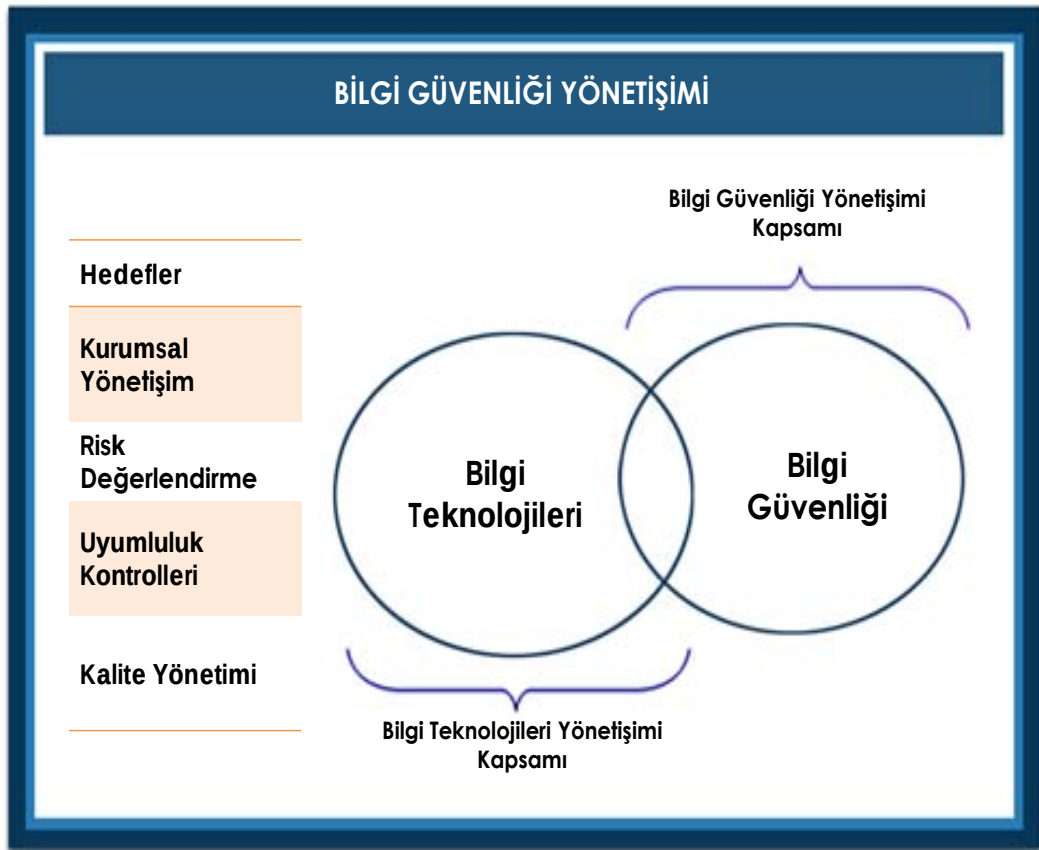
19. yüzyılın ikinci yarısına girilirken bilgisayarın icat edilmesiyle birlikte, dünya tarihinde yeni bir sayfa açılmış ve bu gelişme bilimsel ve teknolojik icatların kısa bir zaman dilimi içerisinde insan hayatının bütün boyutlarını etkisi ve kontrolü altına alacağını işaret etmiştir. İlk icat edilen bilgisayarlar, kapasite ve donanım olarak son derece sınırlı olmakta birlikte sadece kurumsal çalışmalar için kullanılır durumdaydı. Zamanla bilgisayar teknolojisinde çok hızlı ve kapsamlı değişimler yaşandı. Bu değişimlere paralel olarak bilgisayarların kullanımı genişledi ve kurumsal olarak kullanılmanın yanında bireysel anlamda bireysel anlamda bilgisayar kullanımı da yaygınlaştı. Bilgisayarlar arası iletişim sistemine duyulan ihtiyaç, internetin ortaya çıkmasına zemin hazırlarken, internetle birlikte de bilginin erişilebilirliğini çok kolay hale getirdi. Tüm bu gelişmeler, bilgi paylaşımı ve iletişim yöntemlerinde de kapsamlı gelişmelere imkan hazırladı.

İlk olarak Batı toplumlarında kullanılan bilgisayar, 2000’li yıllardan itibaren bütün dünya ülkelerinde bilginin tek kaynağı haline geldi. Bu gelişmeler, içerisinde bulunduğumuz zaman dilimine bilgi çağı denmesine de sebep olmuştur.

Bir şirketin ya da kurumun en önemli varlıklarından biri haline gelen bilginin üretilmesi, edinilmesi veya paylaşılması tamamen bilgisayar kullanımıyla ilişkili hale gelmiştir. Nitekim bilgi teknolojilerinin ve bilgisayar kullanımının yaygınlaşmadığı yıllarda kurumlar birçok uygulamayı kâğıtlar kullanarak yapıyorlardı. Oysa günümüzde kâğıtların yerini tamamen bilgisayarlar almıştır ve kurumsal organizasyonlarda ve süreçlerde bütün çalışmalar bilgi teknolojilerine göre organize edilir hale gelmiştir.

Bilgi teknolojilerinin etkin kullanılmadığı dönemlerde mevcut bilgilerin korunması ve güvenliği belirli önlemlerle sağlanabiliyordu ve bilginin korunması ve güvenliği de bugünkü şartlara göre daha kolaydı. Kurumsal organizasyonlarda bilgi teknolojilerinin kullanılmaya başlaması, bilginin güvenliği ve korunması işlemlerini ciddi bir oranda zorlaştırdı. Çünkü bu sistemde bilginin üretimi ve kontrolü de yine teknolojik yöntemlerle yürütülür hale geldi.

Gelinen noktada, bilgi teknolojilerinin güvenliği konusunda dikkat edilmesi gereken riskleri de göz önünde bulundurma zorunluluğu dikkat çekmektedir. Çünkü bilgi teknolojileri, bilgiye uzaktan erişim imkanı sağlar, bilginin birçok kopyasının oluşturulmasını sağlar, çok fazla sayıda bilginin merkezi olarak tek noktada depolanmasına imkan verir hatta bilinçli veya bilinçsiz bir şekilde çok sayıda bilginin silinmesi, kaybedilmesi gibi durumlara sebep olabilir. Bu nedenle, bilgi teknolojilerinin güvenliği ve kontrolü kurumsal çalışmalar açısından hayati önem taşımaktadır.



Şekil 1.1: Bilgi Güvenliği Yönetişimi

Bilgi güvenliği, “kıymetli varlıkların, bozulma, usulsüz paylaşılma ya da kaybolma riskine karşı korunması ile alakalıdır. Buradaki kıymetli varlıklar, elektronik ortamda iletilen, alınan, paylaşılan, saklanan, işlenen, kaydedilen veri ya da bilgilerdir. Bu veri ve bilgi kaybolmaya bozulmaya, değiştirilmeye, veya usulsüz

paylaşılmaya karşı korunmak zorundadır. Bu koruma yöntemleri birçok teknik, teknolojik ya da teknolojik olmayan yöntemlerden oluşabilir. [1]

Bilgi güvenliği yönetiřimi, řirket ya da kurumsal yönetiřiminin bir alt kümesidir ve ařağıdaki unsurları içermelidir:

- Güvenlik sorumlulukları ve pratikleri
- Güvenlik için stratejiler ve hedefleri
- Risk deęerlendirme ve yönetimi
- Güvenlik için kaynak yönetimi
- Kanunlar, regölasyonlar, güvenlik politikaları ve kuralları ile uyumluluk

Netice itibariyle, iř süreçlerinin büyük bir kısmının bilgi teknolojilerinin kullanımıyla gerçekleşmesi, bilgi güvenliğini zorunlu ve çok yönlü bir hale getirmiřtir.

Yönetiřim kavramı farklı alanlarda sıkça kullanılan ve gittikçe önemi artan bir eğilim haline gelmiřtir. Bilgi Güvenlięi Yönetiřimi, Bilgi Teknolojileri Yönetiřimi kapsamında Kurumsal Yönetiřim ile birlikte düşünülmesi gereken bir olgu haline gelmiřtir. Bilgi artık kurumların ve řirketlerin en önemli varlıklarından biridir ve kıymeti gittikçe artmaya devam etmektedir.

Kurum çalışanlarının hiyerarşik olarak en üst yöneticisinden en son elemanına kadar yetkisi oranında sorumlu olmasını gerektirir. Tepe Yöneticinin bilgi güvenlięi ile ilgili kararların alması ve bu kararların uygulanması aşamalarını yakından takip etmesi şarttır. Bu konudaki yetki ve sorumluluğun uygun paylaşımı da yönetiřime anlam kazandırır.

Solms'un bilgi güvenlięi yönetiřim modelinin tasarımında; tek bir kurum ya da řirket uygulaması göz önünde bulundurulmuřtur. Bu organizasyonların başka organizasyonlarla nasıl etkileřimde bulunacakları ve bu etkileřim sırasında önerilen modelin nasıl çalışacağı açıklanmamıřtır. Buna ek olarak ulusal çapta bu Bilgi Yönetiřim Modelinin nasıl tasarlanacağına değinilmemiřtir.

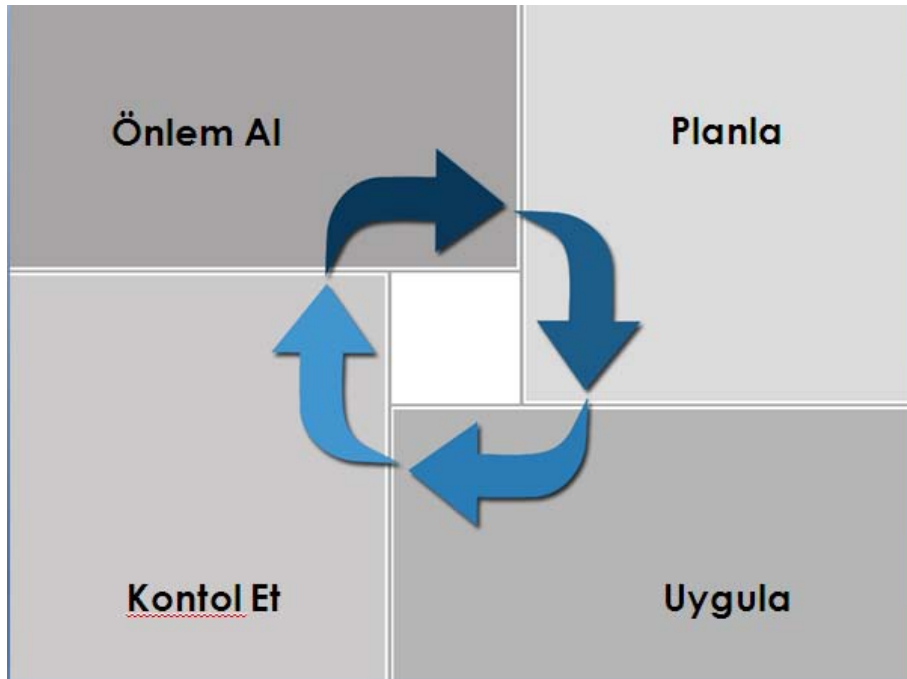
Bu alıřma, sz konusu bilgi gvenlięi ynetiřimine yaptıęı vurguya binaen nemlidir. Arařtırmada kamu kurum ve kuruluřlarında bilgi gvenlięi amacıyla kullanılabilir bir model nerilmektedir. İBB, baęlı kuruluřları (İETT, İSKİ) ve İřtirak řirketlerinde kullanılabilir tarzda bir yapı tasarlanmıřtır ve bu alıřmayla, Bilgi Gvenlięi Ynetiřimi alanında yapılacak alıřmalara zgn bir katkıda bulunmak ve ilgililerin istifadesine sunmak amalanmaktadır.

2. BİLGİ GÜVENLİĞİ YÖNETİŞİMİ VE SOLMS'UN BİLGİ GÜVENLİĞİ YÖNETİŞİM. MODELİ

2.1. Bilgi Güvenliği Yönetimi, Bilgi Güvenliği Yönetişimi, Risk Yönetimi

Bilgi teknolojileri kurumların iş süreçlerinin hemen hemen hepsinin gerçekleştirilmesinde pay sahibi olduğu için bu teknolojilerden kaynaklanan riskler de iş süreçlerini kötü yönde etkileyen etkenler olarak karşımıza çıkmaktadır.

Günümüzde bilgi güvenliği yönetişimi, kurumsal yönetişimin önemli bir parçası olarak değerlendirilmektedir. Bilgi güvenliğinin yönetimi ile alakalı ISO 27001, COBIT, ITIL gibi standartlar geliştirilmiştir.



Şekil 2.1: ISO 27001 Süreçleri

Bu standartlardan ISO 27001 BGYS (Bilgi Güvenliği Yönetişim Sistemi) olarak adlandırılmaktadır. Bilgi güvenliğini yönetmek, geliştirmek ve uygulamak için yoğun olarak kullanılmaya başlamıştır. Ancak bilgi güvenliği yönetim sistemi teknik bir konu olmaktan ziyade içeriğinde teknik bilgilerin de bulunduğu bir

yönetim, organizasyon, belgelendirme ve raporlama anlayışının uygulanmasını ifade etmektedir. ISO 27001’de tanımlanan yaklaşım uyarınca bilgi güvenliğinin bir süreç olarak ele alınması ve sürecin planlama, uygulama, kontrol etme ve önlem alma adımlarından oluşan bir döngü şeklinde çalıştırılması gerekmektedir [2] Yaşayan ve kendini yenileyen bir bilgi güvenliği sistemi ancak bu çevrimin çalıştırılması ile mümkün olabilmektedir (Şekil 2.1).

BGYS için Kuruluşlar için Temel Seviye Yol Haritası:

- Kapsamın Tanımlanması
- Ekip oluşturulması ve Stratejinin Belirlenmesi
- Eğitim İhtiyacının Değerlendirilmesi
- Bilgi varlıklarının saptanması
- Bilgi varlıklarının değerinin belirlenmesi
- Risk belirlenmesi
 - Sızma/Dalış/Entegrasyon/Teknik Uyum Testleri
 - Risk Analizi
- Kontrollerden istenen güvence derecesinin belirlenmesi
- Kontrol Hedeflerinin ve Kontrollerin Saptanması
- Dokümantasyonun hazırlanması
- Prosedürlerin ve dokümanların uygulamaya alınması
- İç Denetimlerin yapılması
- Yönetimin Gözden Geçirilmesinin yapılması

Bilgi güvenliği yönetişimi konusunda belli bir algılamının olduğu kurumlarda ISO27001 standardı çerçevesinde bir BGYS’nin çok kısa zamanda kurulması ve başarı ile işletilmesi beklenen ve doğal bir sonuçtur.

Standarta bilgi güvenliği yönetişimi penceresinden bakıldığı zaman, iki temel fark göze çarpmaktadır. Bunlardan birincisi standarttaki görevlerin tamamının “yönetim” kademesine verilmesi ve yönetim kademeleri arasında bir ayrım yapılmamasıdır. İkinci fark ise, bilgi güvenliği ile kurumsal strateji arasındaki uyumluluk konusunda standartta çok az miktarda bilgi bulunmasıdır.

Bilgi güvenliği ve kurumsal stratejinin uyumu bilgi güvenliği yönetişiminin en önemli bileşenlerinden biridir. ISO27001'in giriş kısmında “bir kuruluş için BGYS'nin benimsenmesi stratejik bir karar olmalıdır” ifadesi yer almaktadır. Bilgi güvenliği yönetişimin uygulandığı kurumlarda bu ifadenin zaten uygulanması beklenir. Bilgi güvenliği yönetişimin uygulandığı bir kurumda BGYS olmasa bile, “bilgi güvenliği stratejik bir karar neticesinde” benimsenecektir. Bunun ardından BGYS çok kolay bir şekilde kurulup işletilebilecektir. Bilgi güvenliği yönetişiminin uygulanmadığı kurumlarda ise BGYS'nin stratejik bir karar neticesinde benimsenmesi çok nadir görülecek bir durumdur.

BGYS Doğrular-Yanlışlar:

	Yanlış	Doğru
1	BGYS'nin kapsamı bilgi işlem birimidir.	BGYS'nin kapsamı nihai olarak kurumun tamamıdır.
2	BGYS'yi kurmaktan ve yürütmekten sorumlu üst düzey yönetici bilgi işlem birimi başkanıdır.	BGYS'yi kurmaktan ve yürütmekten sorumlu yönetici kurumun en üst düzey yöneticisidir.
3	BGYS bir bilgi teknolojileri projesidir.	BGYS bir bilgi teknolojileri projesi değildir. Bir bilgi güvenliği projesidir.
4	BGYS'nin sadece ve doğrudan bilgi işlem birimi ile bağlantısı vardır.	BGYS'nin kurumun tüm birimleri ve süreçleri ile ilişkisi vardır.
5	BGYS'nin sadece ve doğrudan güvenlik teknolojileri ile bağlantısı vardır.	BGYS kapsamında güvenlik teknolojilerinden faydalanılır.
6	BGYS bir yazılım/donanım/servis tedarik projesidir.	BGYS kapsamında yazılım/donanım/servis tedariki yapılabilir.
7	BGYS, tamamen başka bir kuruma yaptırılabilen bir projedir.	BGYS kurulması için başka bir kurumdan danışmanlık hizmeti alınabilir. Ancak BGYS'yi asıl kurması gereken kurumun kendisidir.

Tablo 2.1: BGYS Doğrular Yanlışlar

ISO27001 standardı, bilgi güvenliği yönetişiminin kurumda olduğunu varsayarak bilgi güvenliği yönetiminin oluşturulmasına dair yapılması gerekenleri içermektedir. Bu durumda, bilgi güvenliği yönetişimi kavramının algılanmadığı bir kurum her ne kadar BGYS işletmek ve sertifika almak istese de, bu istek genellikle bilgi işlem birimi içerisinde gelecek, yapılacak olan çalışmalar genellikle bilgi işlem sınırlarını aşamayacak, bu nedenle de BGYS projeleri sürdürülemeyecek veya düzgün bir şekilde sonlandırılmayacaktır. [3]

Diğer bir standart olan COBIT ise, etkin IT yönetişimini başarmak için en önemli standart olarak ön plana çıkmaktadır. Fakat her bir organizasyon için tek bir model önerilmemektedir. Her bir organizasyon kendi ihtiyaçlarını tespit eder, COBIT kaynaklarını esas alarak kendine özel uygulamayı gerçekleştirir. CobiT, daha buyurgan bir yapıya sahip, nasıl yapacağınıza karışmadan, ne yapılması gerektiğini söylüyor. Sonra da hem iç hem de dış denetimlere kolaylık sağlamak için bu yapılması gerekenlerin sorgulanmasına ilişkin bilgiler veriyor. [4]

Etkin bir bilgi güvenliği çerçevesinin oluşturulması, ISO 27001 ve COBIT'in birlikte göz önünde bulundurulmasıyla mümkün olabilmektedir. [5]

COBIT; IT Governance Institute (ITGI) tarafından yayınlanan, bir etki alanı veya süreç çerçevesi içinde iyi uygulamaları bir araya getiren, yönetilebilir faaliyetleri mantıklı bir yapı doğrultusunda sunan bir bilgi kaynağıdır. COBIT daha çok yönetime odaklanmak yerine kontrollere odaklanmaktadır. Bu iyi uygulamalar, IT yatırımlarının, servis sunumuna odaklanmasını ve işler kötü gittiğinde karar verilmesini sağlayan bir ölçüt belirlenmesini sağlar.

COBIT; IT yönetim çerçevesinde aşağıdaki sorulara yanıt verir.

- - Neler tanımlanmalı?
- - Neler ölçülmeli?
- - Neler otomatize edilmeli?
- - En iyi pratikler nelerdir?
- - Bunun için bir sertifikasyon var mıdır?
- - IT kontrollerini nasıl yapmalıyız ve fayda-maliyet analizini nasıl yaparız?
- - Hedefler ve anahtar metrikler nelerdir?

- - IT işlevlerinin yerine getirilememe riskleri nelerdir?
- - Başkaları ne yapıyor ve nasıl yapıyor?
- - Kurumun IT olgunluğunu diğerlerine kıyasla nasıl ölçebiliriz?
- - Kurumun IT gelişim stratejisi nedir?

COBIT'in temel amacı süreç performans metriklerini ve olgunluk modellerini belirleyerek ve IT'nin iş sorumluluklarını tayin ederek, iş hedefleriyle IT hedeflerini bağdaştırmaktır.

Birçok kurum için bilgi ve bilgi teknolojileri en değerli fakat en az anlaşılan varlıktır. IT yönetiřimi; deęer, risk ve kontrol üzerine kuruludur. COBIT IT yönetiřimi için temel hedefleri ve bileřenleri sunar.

COBIT, bu hedeflere ulařılmasını ařaęıdakilerle saęlar:

- İş ihtiyaęlarına baęlantı kurarak
- IT aktivitelerini genel kabul görmüş süreç modelleriyle organize ederek
- Esas gerekli IT kaynaklarını ayırt ederek
- Yönetim kontrol hedeflerini tanımlayarak

COBIT'i IT yönetiřim çerçevesi olarak seçmenin faydaları:

- İş hedeflerine iyi bir baęlantı
- Yönetim tarafından IT'nin işlevlerinin net anlaşılmadı
- Süreçlerin net tanımlaması ile görev ve sorumlulukların netleştirilmesi
- Genel kabul görmüş uygulamalar
- İş ortakları ve dięer taraflarla ortak bir dil kullanma
- Uygun bir iç denetim mekanizması

İş hedeflerine ulařılabilmesi için bilginin belirli kriterlere uyum saęlaması gerekir. Bu kriterlere CoBIT dilinde bilgi kriterleri denir. Kalite, güven ve güvenlik gerekliliklerini esas alacak olursak toplamda yedi adet bilgi kriteri belirlenmiştir, bunlar:

COBIT Bilgi Kriterleri

- - Verimlilik
- - Etkililik
- - Gizlilik
- - Bütünlük
- - Erişilebilirlik
- - Uyumluluk
- - Güvenilirlik

Tedarik zinciri kurmak gibi iş kapasitesinin desteklenmesi için uygun bir teknik kapasite (ERP sistemi vb.) oluşturmak için kaynaklara yatırım yapılması gerekir. Bu yatırımlar IT'nin iş gerekliliklerinin karşılanabilmesini sağlar. Böylece hedeflenen çıktı (satışların artması ve finansal karlılık) elde edilebilecektir.

COBIT'e Göre IT Kaynakları

- - Uygulamalar
- - Bilgi
- - Altyapı
- - İnsanlar

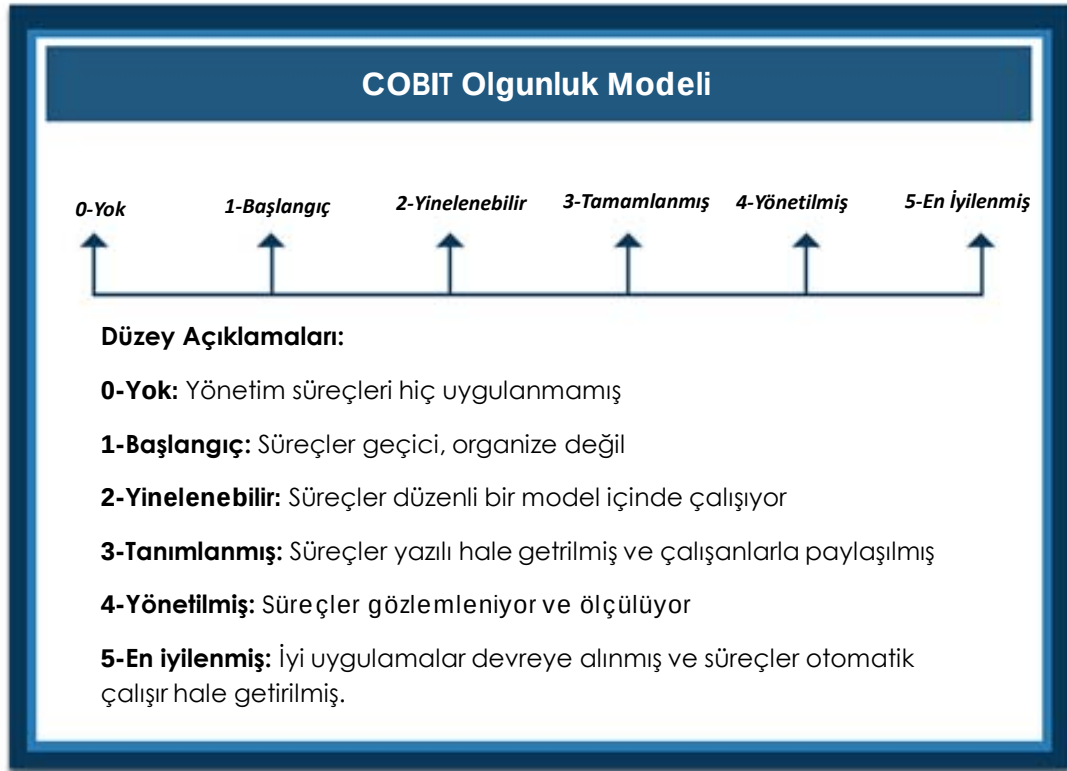
COBIT, IT faaliyetlerini dört temel etki alanında ayırarak genel bir süreç modeli oluşturulmasını sağlar. Bu etki alanları; Planlama ve organizasyon (10 süreç), edinme ve uyarlama (7 süreç), sunum ve destek (13 süreç), izleme ve değerlendirme (4 süreç) olarak tanımlanır ve toplamda 34 süreç söz konusudur.

COBIT bileşenleri, IT yönetim, yönetim, kontrol ve güvence ihtiyaçlarının desteklenmesi için ilişki içindedir.

IT proseslerini yönetebilmek ve kontrol altında tutabilmek için olgunluk modelleri geliştirilmiştir. Böylece organizasyonlar kendilerini olgunluk seviyelerine göre 1'den 5'e kadar değerlendirebilecektir. Aşağıda COBIT'in 34 prosesi için de kullanılabilecek özel bir model bulunmaktadır. COBIT'in 34 IT prosesi için geliştirilmiş olgunluk modellerini kullanmak, şirket yönetiminin aşağıdakileri yapabilmesini sağlayacaktır:

- - Şirketin gerçek performansı – kurumun bugün bulunduğu nokta

- - Endüstrinin mevcut durumu – karşılaştırma
- - Kurumun gelişime yönelik hedefleri – kurumun olmak istediği yer
- - Gerekli gelişim yolu/rotası



Şekil 2.2: COBIT Olgunluk Modeli

Olgunluk Modelleri :

SEI'nin olgunluk modeline dayanan ve 0'dan 5'e kadar seviyelendirilmiş olgunluk modelleri ile IT süreçlerinin olgunluğu modellenmektedir.(Şekil 2.2)

- *0 Mevcut Değil* : Tanımlanmış süreç bulunmaması durumu.
- *1Başlangı* : *Aşamasında:* Organize olmayan ve standartlaşmamış fakat kurumda farkındalığın mevcut olduğu ve adresleme ve standartlaştırma ihtiyacının tespit edildiği seviye
- *2 Tekrarlanabilir* : Bireye dayalı ve tekrarlanan işleri farklı kişilerin aynı şekilde yapabildiği seviye. Bu seviyede formal eğitim ve iletişim metodları belirlenmemiş fakat sorumluluk büyük oranda kişiye bağlı kılınmıştır.

- *3 Tanımlanmış* : Prosedürler standartlaşmış ve dokümente edilmiş, eğitim aracılığı ile kurum içinde iletilmiştir. Ancak bu prosesleri izleyip izlememe kararı kişinin kendisine bırakılmıştır bu nedenle yapılan işler arasında çeşitli farklılıklar mevcuttur. Prosedürlerin kendisi gelişmiş değildir ancak mevcut uygulamaların biçimselleştirilmiş halidir.
- *4 Yönetiliyor* : Prosedürlerle uyumu izlemek ve ölçmek, proseslerin etkin çalışmadığının anlaşılması durumunda faaliyete geçmek mümkündür. Prosesler sürekli gelişmekte ve iyi uygulamaların tanımlanması sağlanmaktadır. Otomasyon ve araçlar kısıtlı veya parçalı bir biçimde kullanılabilir. [4]
- *5 Optimize Edilmiş* : Prosesler en iyi uygulamalar seviyesine indirgenmiş, sürekli gelişim ve olgunluk modelleme konusunda diğer şirketlerin sonuçları ile çalışmaktadır. IT, iş akışlarının otomatize edilmesi, kalite ve etkinliğin artırılması ve kurumun çabuk adapte olabilmesi için bütünleşik olmuştur. [4]



Şekil 2.3: Bilgi Güvenliği Yönetişimi Kavramsal Diyagramı

Bilgi teknolojilerinin iç çalışması ve operasyonlarının yönetimi, bilgi güvenliğinden bağımsız ele alınan, kendi içinde neredeyse bir meslek haline gelen bir konudur. Üstelik iki ayrı kıtada geliştirilmesine devam edilen iki ayrı standart bu konuya cevap aramaktadırlar. ABD’de geliştirilen COBIT, bilgi teknolojilerinin yönetilmesinde ne yapılacağını tanımlamaya çalışmaktadır. Buna karşın, İngiltere’de geliştirilen “Bilgi Teknolojileri Altyapı Kütüphanesi”, orijinal kısaltmasıyla ITIL, yönetimin nasıl yapılması gerektiğini tanımlamaktadır.

Bilgi güvenliği yönetişiminin gerekliliğini anlamak için bilgi güvenliği risklerinin kapsamını çizmek faydalı olacaktır. Bilgi güvenliğinin küçük bir kısmı teknoloji ile ilgilidir, çok daha büyük bir kısmı ise personel ve süreçlerle ilgilidir. Teknoloji ile ilgili riskler genellikle bilgi güvenliği yönetişimi çerçevesine ihtiyaç duymadan seviyesi düşürülebilecek risklerden oluşurken, personel ve süreçler ile ilgili riskler ise genellikle bilgi güvenliği yönetişimi çerçevesinde seviyeleri düşürülebilecek risklerden oluşmaktadır. Bu nedenle günümüzde birçok kurumda standart güvenlik önlemleri (güvenlik duvarı, antivirüs vb.) tedarik edilip kullanılırken, bu karşı önlemlerin etkinliği (kuralların düzgün girilmesi, sistem günlüklerine bakılması, sistemlerin prosedürlere göre işletilmesi, sistemler üzerine iç denetim yapılması vb.) konusunda bir takım sıkıntılar yaşanmaktadır. Bu konuda teferruatlı bir örnek vermek gerekirse; kurum bilgi sistemlerini dış saldırılardan korumak için tedarik edilip kurulan bir güvenlik duvarı, bilgi güvenliğinin teknolojik yönünü yansıtmaktadır. Ancak, işletmenler tarafından güvenlik duvarına gerekli olan kuralların girilmemesi veya bilgisayar kullanıcılarının modem gibi cihazlar yoluyla internete çıkmaları, bu teknolojik önlemden beklenen faydayı çok azaltır. Bu nedenle işletim prosedürlerinin oluşturulması ve takip edilmesi, iç denetimler yapılması, kurum bilgisayar kullanıcılarının uyması gereken prensiplerin yer aldığı politika dokümanlarının oluşturulması, disiplin sürecinin işletilmesi gibi teknolojik olmayan birçok karşı önlem gerekmektedir. [3]

Bilgi teknolojileri kurumların iş süreçlerinin hemen hemen hepsinin gerçekleştirilmesinde pay sahibi olduğu için bu teknolojilerden kaynaklanan riskler de iş süreçlerini kötü yönde etkileyen etkenler olarak karşımıza çıkmaktadır.

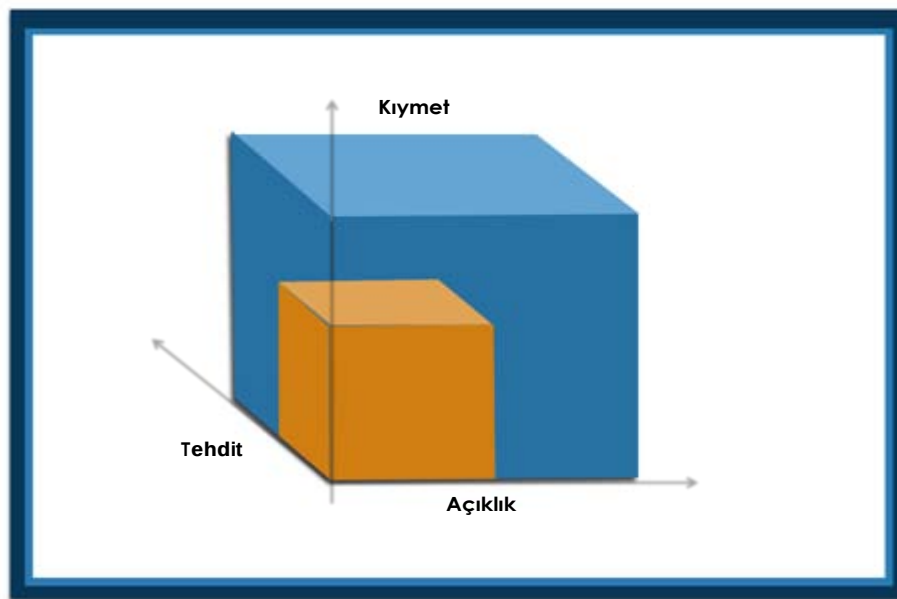
Mutlak güvenlik olmadığından dolayı, her zaman için bir bilgi sisteminde mevcut bir risk vardır. Amaç, varolan bu riski önlemek olmamalıdır. Çünkü, riski

önlemek çok pahalıdır hatta imkansızdır. Bir bilgi sistemi için, sırf riski sıfırlamak için o kıymetin değerinden fazla güvenlik önlemi almak akılcı bir yaklaşım olmayacaktır. Bu nedenle riski önlemek yerine risk ile birlikte yaşamayı öğrenmek daha uygun bir yoldur. Bunun için, bilgi sistemini korumak adına çıkan güvenlik önlemini kullanmanın getirdiği masraf ile o güvenlik önleminin kullanılmadığı zaman olacak saldırılar sonucunda oluşacak masrafları karşılayacak bir araç olması gerekmektedir. Risk analizi ve yönetimi bu işi yapan araçlardır.

Mutlak güvenliğin imkansızlığı ve riskin daima varoluşu güvenliğe bir ürün gözüyle bakmamızı engeller. Artık günümüzde, bilgi teknolojileri güvenliği, gerçek zamanlı risk analizi ve yönetimi işlemi olmuştur. Kısacası, güvenlik artık bir teknoloji konsepti olmaktan çıkmış bir iş konsepti haline gelmiştir. Risk analizi ve yönetimi ise, bu işin çekirdek kısmıdır ve bilgi teknolojileri güvenliği ürünlerinin seçilmesi ve geliştirilmesinde ana karar verme mekanizmasıdır.

Risk, sözlüklerde, “zarara yol açan ya da zarar verme kapasitesi olan kişi ya da nesne” olarak tanımlanmaktadır.

Riskin önceki başlıklar altında değinilen kıymet, açıklık ve tehdit kavramları bağlamındaki bir diğer tanıımı “bir kıymetteki bir açıklığın bir tehdit tarafından kullanılma ihtimalidir” şeklindedir.



Şekil 2.4: Kıymet, tehdit ve açıklık fonksiyonu olarak risk

Risk, kıymet, tehdit ve açıklığın bir fonksiyonudur. Şekil 2.4’de bu fonksiyon soyut olarak ifade edilmiştir. Şekildeki sarı oklar, karşı önlem başlığı altındaki 3 tip karşı önlemi temsil etmektedir. Karşı önlemleri almadan önce, riskin büyük olduğu görülmektedir. (Siyah kübün hacmi) Karşı önlemleri aldıktan sonra ise risk azalmıştır. (Turuncu kübün hacmi)

Karşı önlemler almadan önce sistemde mevcut olan riske taban riski denmektedir. Karşı önlemler alındıktan sonra sistemde mevcut olan riske ise geri kalan risk denmektedir. Buna göre siyah küp taban riski, turuncu küp ise kalan riski ifade etmektedir.

İstenen (taşınabilir) risk seviyesi ise, kurumun kabul ettiği ve taşıyabileceği risk miktarıdır. Karşı önlemler alındıktan sonra, geri kalan riskin, gerekli riskten daha aşağı seviyede olması gerekir. Herhangi bir karşı önlem alınmamışken, eğer bulunan taban risk, istenen riskin aşağısında çıkarsa, karşı önlem alınmaya gerek olmayacaktır.

Riskin önüne geçebilecek büyüklükte bir bütçe bulunmamaktadır. Bu nedenle, giriş başlığı altında da söylendiği gibi, bilgi sistemlerinde risk daima olacaktır. Çünkü risk iş yapmanın maliyetidir. Risk analizi ve yönetiminin ana çıkış noktası budur.

Risk Analizi

Risk analizi, sonucu itibariyle güvenlik ihlallerine neden olan risklerin ortaya konması ve yorumlanması işlemidir. Risk analizi kendi içerisinde uzun ve ayrıntılı bir prosedir. Risk analizinde ilk olarak bilgi sisteminde varolabilecek tüm kıymetlerin, bu kıymetlerdeki açıklıkların ve bu kıymetleri etkileyebilecek tüm tehditlerin ortaya konması yapılır. Ayrıca, halihazırda mevcut olan karşı önlemler incelenir. [6]

Çeşitli risk analizi metodları vardır. Bunlar nitelik bakımından ve nicelik bakımından olanlar şeklinde ikiye ayrılabilir.

Nitel metodolojiler:

- OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) [Alberts and Dorofee 2002]
- The CORAS (Construct a platform for Risk Analysis of Security Critical Systems) methodology [Stolen et al. 2002]

Nicel metodolojiler:

- ISRAM (Information Security Risk Analysis Method) [Karabacak and Sogukpınar 2005]
- Cost-Of-Risk Analysis (CORA) [International Security Technology Inc (IST Inc) 2000]
- Information Systems (IS) analysis based on a business model [Suh and Han 2003]

Bunlar dışında da metodolojiler vardır. Ancak bunlar en iyi dökümanite edilmiş olanlardır. [7]

Daha sonraki aşamada, ortaya konulmuş olan kıymet, açıklık, tehdit ve karşı önlemlerinin değerlendirilmesi işlemi yapılır. Değerlendirilmiş kıymet, açıklık, tehdit ve karşı önlem değerleri girdi olarak alınıp, matematiksel ve mantıksal metodlar kullanılarak risk değeri bulunur. Son olarak risk-kıymet eşleştirmesi yapılır.

Risk analizi karşı önlemlerin nasıl ve ne şekilde alınacağı üstünde durmaz. Bu işi, risk risk yönetimi prosesi yapmaktadır.

Risk Yönetimi

Risk yönetimi, risk analizi sonucunda ortaya konan ve yorumlanan risklerin önüne geçmek ve/veya azaltmak amacıyla uygun, maliyet etkin karşı önlemlerin alınması işlemidir. Karşı önlem maliyetleri ve risk analizi sonucunda çıkan kıymet-risk eşleşmesi risk yönetimi prosesi için en önemli girdilerdir. Uygun karşı önlemlerin alınması işini risk yönetimi yapar. Yerinde bir risk yönetimi ile az bir maliyet ile risk kübünün hacmi büyük bir ölçüde düşürülebilir. Risk yönetimi, genel olarak karşı önlemlerin alınması ile oluşacak maliyeti, geri kalan riskden dolayı oluşacak bir zararın yol açacağı maddi kayıpla karşılaştırır ve daha düşük ise karşı önlemleri alır.

Risk yönetimi prosesinin dayandığı asıl nokta kurumun güvenlik ihtiyaçlarıdır. Kurumun güvenlik ihtiyaçlarına göre, taşınabilir risk oranı

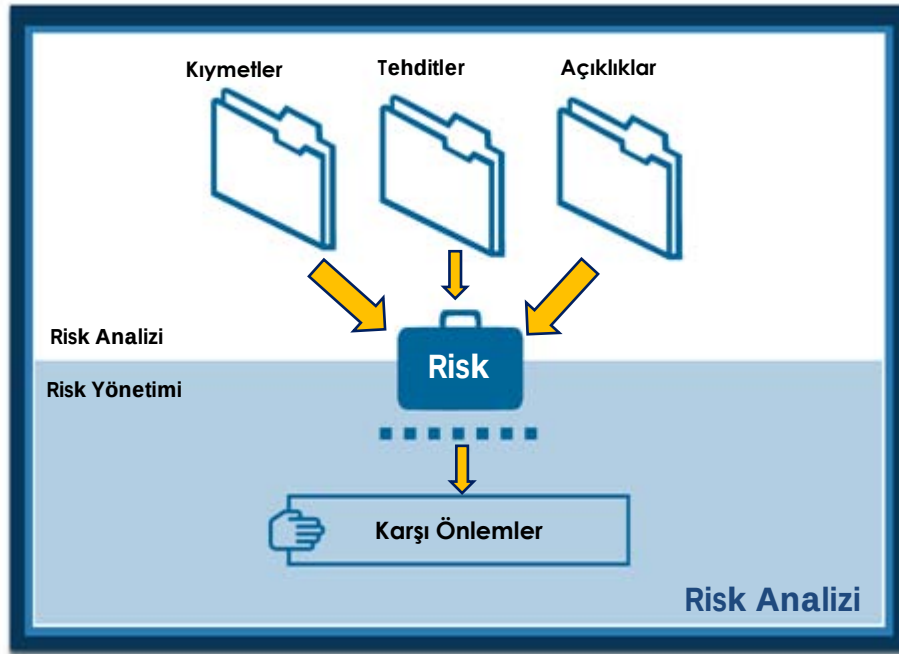
belirlenebilir ve bunun sonucunda uygun karşı önlemlerin seçilmesi işlemi yapılabilir. Güvenlik ihtiyacı, bir kıymeti etkileyen bir tehdit için kurumun ne kadar güvenlik önlemi istediğidir. Askeri bir kurum, belli bir kıymet için tehditin çok az indirgenmesi isteyebileceken, normal bir şirket ise aynı kıymeti etkileyen aynı tehdit için hiç bir güvenlik önlemi almak istemeyebilir.

Risk analizi, yorumlaması ve yönetimi bir defa yapılmaz. Risk analizi ve yönetimi birer sonuç değildir, şekil 2.5’de de görüldüğü gibi risk analizi ve risk yönetimi sürekli birbirini takip eden iki ana prosesdir. Maliyet etkin bir risk yönetiminin temellerini risk analizi prosesi oluşturur. Risk analizi ve yönetimi bir kurumda, yönetimin de kararıyla belli aralıklarla yapılmalıdır. Çünkü kıymetler, açıklıklar, tehditler daima değişecektir. Bütün bunlar değişmese bile daha maliyet etkin çözümler ortaya çıkabilecektir.

Risk analizi sonuçlarına göre, risk yönetimi dört farklı işten birini yapabilir.

1. Risk yüksektir, karşı önlemler yoktur ya da çok pahalıdır. Kıymet kullanılmaz.
2. Uygun karşı önlemler alınarak risk düşürülebilir.
3. Karşı önlemlerin alınmasının maliyeti, riskin açacağı zarardan çok daha fazla olduğu için risk önemsenmeyebilir.
4. Kıymetler sigortalanarak risk transfer edilebilir

Bu dört iş haricinde, risk analizi ve yönetimi sonucunda, karşı önlemlerin azaltılması ya da kaldırılması da yapılabilir. Hali hazırdaki karşı önlemin çok pahalı olması, tehditin varolmaması gibi faktörlerden böyle bir sonuca gidilebilir.



Şekil 2.5: Risk analizi ve yönetiminin yeri

Risk analizi ve yönetimi tanımları kapsamında son olarak, bu iki prosesin yerini tam olarak çizmek gerekirse, (Şekil 2.5) görüldüğü gibi risk analizi riskleri çıkartır ve yorumlar. Bunun için, kıymetleri, kıymetlerdeki açıklıkları, tehditleri çıkarır. Risk yönetimi ise, risk analizi sonucunda çıkarılan risklere göre karşı önlemleri alır.

Risk analizi ve yönetiminin hedefi, kurum içerisinde olabilecek tehlikelere uygun cevap verebilecek, kasıtlı ya da kasıtsız tehditlerin etkisini ve olma ihtimalini azaltacak hazırlıkları, prosedürleri ve kontrolleri teşhis etmektir.

Risk analizi ve yönetimi prosesinin bir çok yararları vardır. Bu yararların başta gelenleri şu şekilde sıralanabilir.

Kurumun yazılı prosedür ve politikalarının olmasını ya da olgunlaşmasını sağlar.

Kurum çalışanlarının ve bilgi işlem personelinin bilgi güvenliği konusunda bilgi sahibi olmasını sağlar.

Bir kurum yönetiminin de bilgi teknolojileri güvenliği konusunda bilgi sahibi olmasını ve bu konularda karar vermesini sağlar.

Risk analizi prosesinin ilk kısmında yapılan kıymet analizi sonuçlarının kurumun yazılım ve donanım envanterlerinin yenilenmesinde yardımcı olur.

Risk analizi ve yönetiminin yapılmadığı bir bilgi sisteminde aşağıdaki gibi durumlar olabilir.

Bu bilgi sisteminde hiç güvenlik olmayabilir ya da çok az güvenlik olabilir

Kullanılabilirliği oldukça azaltan çok fazla güvenlik olabilir

Yanlış güvenlik önlemleri alınmış olabilir

İnsanlarda yanlış güvenlik bilinci olabilir.

Bütün bu anlatılanlar maddi olarak ve zaman olarak kayıplara yol açan durumlardır. [6]

Günümüzde organizasyonlar, bilgi güvenliğini sağlamak için risk yönetiminin öneminin ve uzman bir yöntem kullanımının gerekliliğinin farkındalar.

Referans [8]'deki model, organizasyonun yapısını ve beklentilerini ortaya koyacak şekilde bu yaklaşımı tespit etmektedir. Bu amaçla hazırlanan sorular cevaplandığında, organizasyonun ihtiyaçları ve öncelikleri belirlenirken, risk analizine olan güvenin de güçlenmesi sağlanacaktır.

Soruların yöntemleri analiz eden karşılıklarıyla da, istenilen sayıdaki uygulanması düşünülen yöntem, tarafsız olarak değerlendirilebilir. Organizasyonun ihtiyaçlarına en uygun risk analizi yöntemi, modelde tanımlanan ve uygulanması pratik olan uygunluk formülü yardımıyla tespit edilebilir.

Yeni bir risk analiz yöntemi, organizasyon için değerlendirilmek istendiğinde, organizasyonun ihtiyaçları değişmemişse, sadece bu yöntem için sorular yardımıyla yeni bir değerlendirme yapılır ve yöntemin uygunluğu hesaplanır. Elde edilen sonuç, daha önceki yöntemlerin uygunluk değerleri ile karşılaştırılarak yeni yöntemin organizasyon için daha iyi olup olmadığı belirlenir. Ayrıca organizasyonun ihtiyaçları değiştiği takdirde, sadece organizasyon için değerlendirme soruları tekrar

uygulanarak, tüm yöntemler tekrar sorularla analiz edilmeden, sadece yöntemlerin uygunluk değerleri güncellenir ve karşılaştırma yapılabilir. [8]

Ancak şunu da unutmamak gerekir ki bilgi güvenliğinden yetkisi oranında herkes sorumlu olmalıdır. Dahili riskleri ortadan kaldırmanın yolu herkesi bilgi güvenliği yönetişiminin bir parçası yapmaktan geçirmektedir. [9]

Bilgi güvenliği yönetişimi için literatürde farklı çalışmalar yapılmış ve modeller önerilmiştir. Bu modellerden önemli bir tanesi Solms'un önerdiği katmanlı yapı, **“yönlendir”** ve **“kontrol et”** aktivitelerinden oluşmaktadır. [10] Bilgi Güvenliği Yönetişim Modeli Şekil 1'de gösterilmiş olan Solms'un bu çalışmasında, kurum içerisindeki yönetim seviyeleri stratejik, taktik ve operasyonel seviyeler olmak üzere üç seviyede ele alınmıştır.

Ancak Solms'un modelinde stratejik seviyeye esas olacak temel bir girdi tanımlanmamıştır. Bu modelde bir kurum tek başına değerlendirilmektedir. Kurumların-şirketlerin kendi aralarında ve bağlı kurum, kuruluş, şirketlerle olan etkileşimi de bu modelin bir parçası olması zorunluluğu vardır. Kurumun tek başına bilgi güvenliğini sağlaması mümkün olamaz. Kurulacak modelin bir bütünlük arz etmesi gerekmektedir. Bunun için ülke çapında bir stratejiler bütünü geliştirilmesi ve yasal dayanaklarının oluşturulması kaçınılmaz bir zorunluluktur.

Bu çalışmada Solms'un Bilgi Güvenliği Yönetişim modeli ele alınmış ve söz konusu modelin geliştirilerek Türkiye'deki kamu kurum ve kuruluşlarında kullanılabilecek hale getirilmesi önerilmiştir. Ayrıca tüm bu sistemin işleyebilmesi için tüm Kamu Kurum ve Kuruluşları ile birlikte özel şirketleri de içeren bir Bilgi Güvenliği Stratejisi Kurulu (BGSK)'nin kurulmasının gerekliliğine ve yasal düzenlemelerin yapılması vurgulanmıştır.

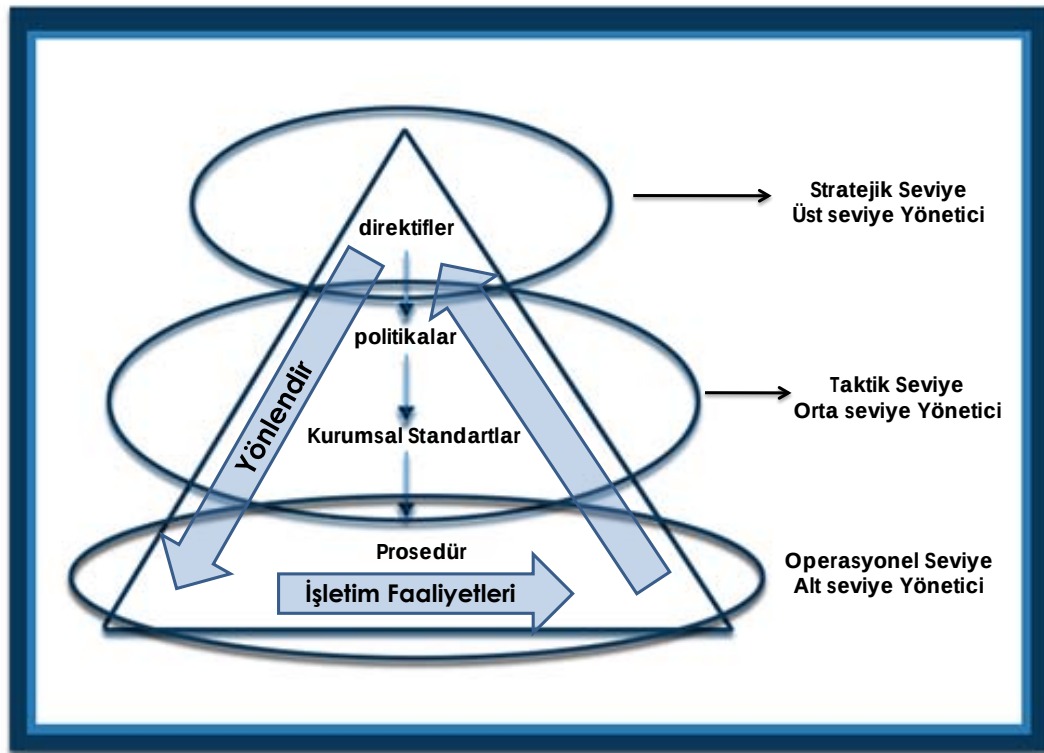
2.2. Bilgi Güvenliği Yönetişimi ve İlgili Çalışmalar

Dlamini ve diğerleri, 'Bilgi Güvenliği: hareketli hedef' makalesinde bilgi güvenliğinin dün, bugün ve geleceği hakkında bilgi vermişlerdir. Bu makalede bilgi güvenliğinin geleceğinin stratejik yönetim seviyesine çıkarılmasını önermişlerdir. [11] Posthumus ve R. Solms, bilgi güvenliği ile kurumsal yönetişimin

bilgi güvenliği yönetim çerçevesi aracılığıyla birleştirilmesini önermişlerdir. Bilgi güvenliğinin sadece teknik bir konu değil, stratejik ve yasal bir konu olduğunu vurgulamışlardır. Bilgi güvenliği yönetim çerçevesi yönetim ve yönetim olarak ikiye ayrılmıştır. Yönetim ayağında kurumun en üst düzey yöneticilerinin bilgi güvenliği politikasını hazırlaması, bu politikaya sadık olması ve organizasyonun strateji, amaç ve hedefleri doğrultusunda bu politikayı desteklemesi gerektiği vurgulanmıştır. Yönetim ayağında ise farklı bölüm yöneticilerinin bilgi güvenliği yönetim çerçevesine göre görevlerini uygulamaları gerektiği belirtilmiştir. Yönetim boyutu strateji, misyon ve vizyondan sorumlu iken yönetim tarafı politikaların uygulanmasından sorumludur. [12]. B. Solms, bilgi güvenliği yönetimi konusunda COBIT ve ISO 17799 metodolojilerini karşılaştırmış, eksilerini ve artıları vererek, her iki metodolojinin birbirlerini tamamlayan yönlerini göstermiştir. COBIT ve ISO 17799 metodolojilerinin karşılaştırılmasının daha kapsamlı ve standart bir bilgi güvenliği yönetim çerçevesi oluşturmada faydalı olacağını belirtmiştir. [5] Yine B. Solms, bilgi güvenliğinin bilgi güvenliği operasyonel yönetimi ve bilgi güvenliği uygunluk yönetimi adlı iki boyutundan söz etmektedir. [13] Bu iki boyutun birbirinden farklı birimler tarafından ayrı ayrı yönetilmesi gerektiğini vurgulamaktadır. Politika ve prosedürler ile bunlara uygun olarak çalışılmasının kontrollerinin yapılması bilgi güvenliği yönetiminin ana kavramıdır. Bilgi güvenliği operasyonel yönetimi politika ve prosedürlerin uygulanmasından sorumlu iken bilgi güvenliği uygunluk yönetimi asıl olarak uygunluğu denetler ve yönetimini sağlar. Ayrıca makalede uygunluk yönetimi ve operasyonel yönetimin karşılaştırılması yapılmış, görev çerçeveleri çizilmiştir. [13] R. Solms ve B. Solms, bilgi güvenliği yönetim modeli üzerine direkt kontrol döngüsü uygulayarak yeni bir model oluşturmuşlardır. Bu modelde, en üst yönetim direktiflerden, orta düzey yönetim politika ve kurum standartlarından, en alt seviye yönetim ise prosedür ve bunların uygulanmasından sorumludur. Her bir yönetim kademesi kendi içinde direkt kontrol döngüsü ile denetlenir. Bu modelin en önemli iki temel prensibinden biri organizasyonun stratejik, taktik ve operasyonel seviyelere bölünmesidir. İkinci önemli prensip ise, yönlendir, yürüt ve kontrol etten oluşan kontrol döngüsüdür. Ayrıca makalelerinde, tüm organizasyonel seviyelerde tüm yönlendir, yürüt ve kontrol et işlevleri için yapılması gerekenler ayrıntılı olarak belirtilmiştir. [10]

2.3. Solms'un Bilgi Güvenliği Yönetişim Modeli

Makaledeki Solms'un modeli [10] “*yönlendir*” ve “*kontrol et*” aktivitelerinden oluşmaktadır. Bu Bilgi Güvenliği Yönetişim Modeli *Şekil 1*'de gösterilmiştir. Solms'un bu çalışmasında, kurum içerisindeki yönetim seviyeleri stratejik, taktik ve operasyonel seviyeler olmak üzere üç seviyede ele alınmıştır. Stratejik seviyede kurumun üst düzey yöneticisi, taktik seviyede orta seviye yöneticileri ve operasyonel seviyede alt seviye yöneticileri yer almaktadır. Bu yönetim kademelerinde “yönlendir” ve “kontrol et” aktiviteleri aşağıdaki şekilde işler:



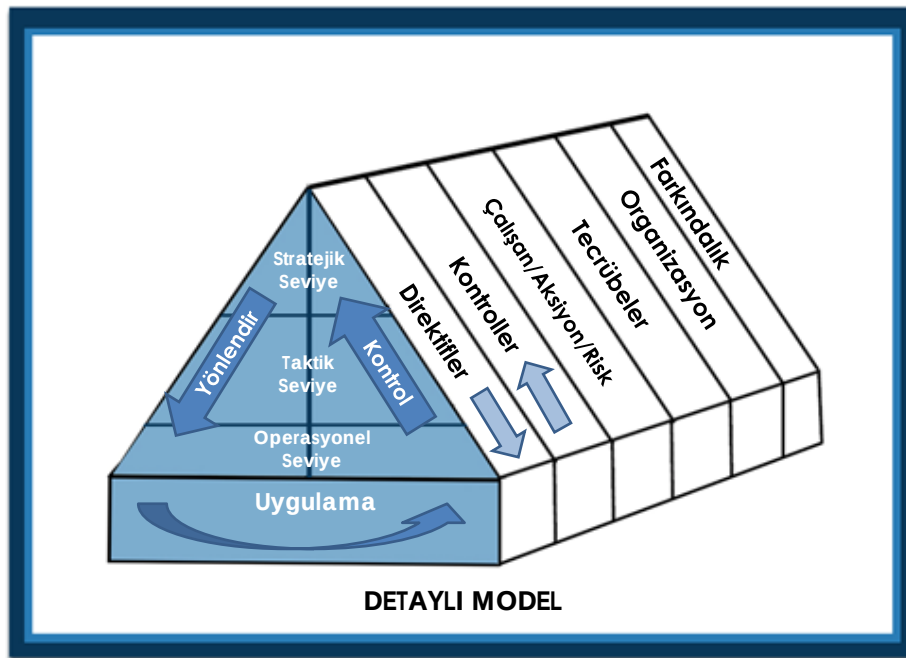
Şekil 2.6: Bilgi Güvenliği Yönetişim Modeli

En üst seviyede yönlendir aşamasında, bilgi güvenliği ile ilgili direktifler (stratejiler) belirlenir, söz konusu stratejiler bir alt seviyedeki yönetim tabakasına girdi olarak verilir. Taktik seviyede söz konusu direktifler politika ve kurumsal standart haline getirilir. Alt seviyedeki yöneticiler ise bu politika ve standartlara göre yordamları hazırlarlar. Bilgi güvenliği faaliyetleri hazırlanmış olan yordamlara göre gerçekleştirilir.



Şekil 2.7: Solms'un Bilgi Güvenliği Yönetişim modeli [10].

Kontrol etme aşamasında ise operasyonel seviyede işlemlerin prosedürlere göre yapılıp yapılmadığı alt seviye yöneticiler tarafından kontrol edilir. Taktik seviyede, bir alt seviyedeki prosedürlerin politika ve standartlara uyumluluğu orta seviye yönetim tarafından kontrol edilir. Stratejik seviyede ise ilgili direktiflerin ne derece yerine getirildiği ve politikaların stratejilerle uyumu üst düzey yönetici tarafından kontrol edilir. [3] Bu şekilde bir döngü sağlanmış olur.



Şekil 2.8: Detaylı Solms'un Bilgi Güvenliği Yönetişim modeli

3. KAMU KURUMLARI İÇİN BİLGİ GÜVENLİĞİ YÖNETİŞİM MODELİ ÖNERİSİ

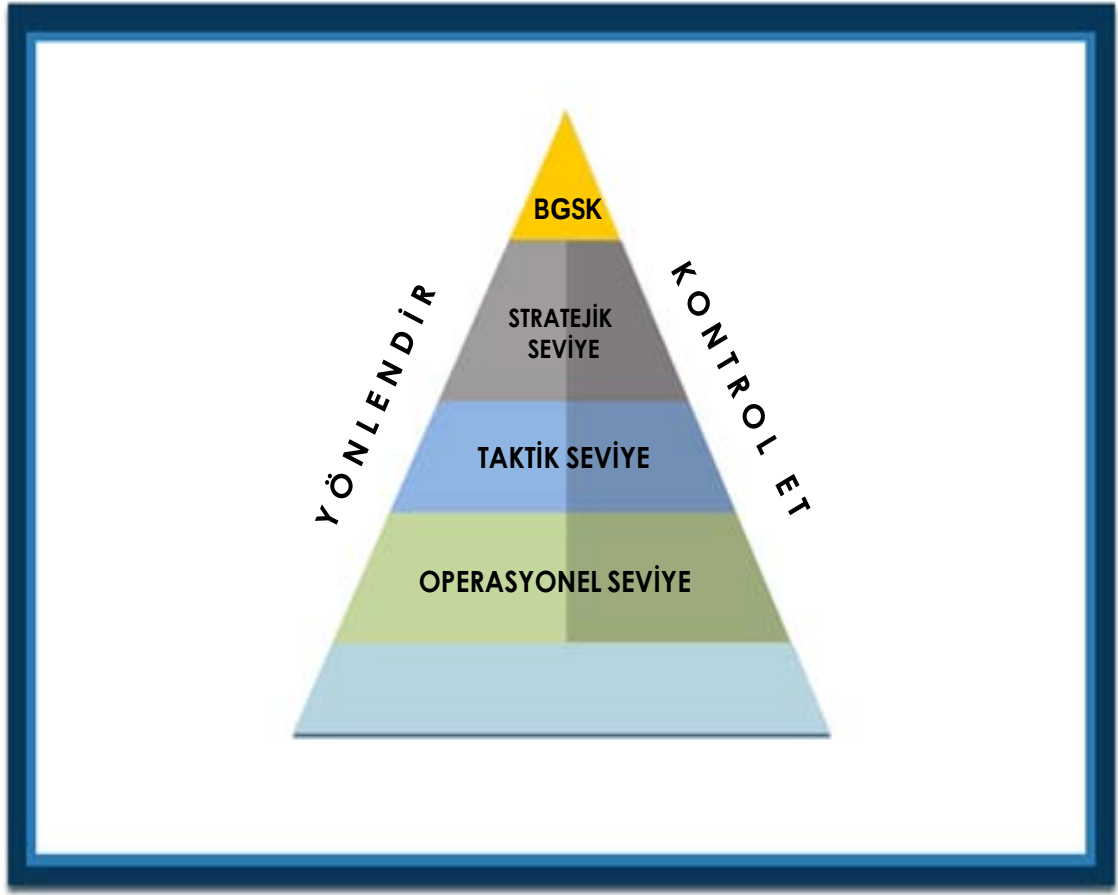
3.1. Tek Kurumda Bilgi Güvenliği Yönetişim Modeli

Solms'un modelinin yönetişimin 3 farklı seviyeden oluşması gerekliliğini önerdiği yukarıda belirtilmiştir. Bunlar stratejik, taktik ve operasyonel seviyelerdir. Her bir seviye üst seviyeden girdi alıp bir alt seviyeye çıktı vermektedir.

Her bir seviyede bir “*yönlendir*” ve tersi yönde de “*kontrol et*” mekanizması kurulması gerekmektedir. Ok yönünde yapılacak işlemler artmakta, tersi yönde kontrol et kısmında ise ok yönünde yapılması gerekenler azalmaktadır.

Stratejik seviyeyi kurumun en üst yöneticileri oluşturmalıdır. Kurumun organizasyon yapısına göre stratejik seviyeyi oluşturan yönetici tipleri farklılık gösterebilir. Taktik seviyeyi orta seviye yöneticiler, operasyonel seviyeyi ise alt seviye yöneticiler oluşturur. Örnek vermek gerekirse eğer bu kurum bir genel müdürlük ise; Stratejik seviyeyi yönetim kurulu başkanı, yönetim kurulu üyeleri, genel müdür ve genel müdür yardımcıları oluşturur. Taktik seviyeyi daire başkanları (ve/veya müdürler) oluşturur. Operasyonel seviyeyi ise müdür (ve/veya müdür yardımcısı, şefler) oluşturur.

Kurumun en üst yönetimi tarafından bilginin kurum için ne kadar önemli olduğu belirtilir ve bu yönde *kurum stratejisi* oluşturulur. İç ve dış riskler belirlenir. Bunlar kurumun en üst yönetiminin beklentilerini yansıtır. Bunların belirlendiği seviye *stratejik seviye*dir. Burada oluşturulan *direktifler* bir alt seviyeye iletilir. Artık bunlar *Taktik Seviye* için girdi kabul edilir. Taktik seviyede de bunlara uygun olarak *güvenlik politikaları*, *kurum standartları* ve *kurum prosedürleri* oluşturulur. Bunlar daha ayrıntılı ve özel olur. *Operasyonel seviyede* bu kurum politika, standart ve prosedürleri *yönetimsel kılavuzlar*, *prensip*ler ve *yönetimsel prosedürlere* dönüştürülür. Tüm bunlar “*Yönlendir*” işlemleri olarak adlandırılır.



Şekil 3.1: Tek Kurum Bilgi Güvenliği Yönetişim modeli.

Bu faaliyetlerin sıkı şekilde gözetlenmesi, izlenmesi ve kontrol edilmesi zorunluluğu vardır. Bu nedenle; direktif, standart ve politikaların ne derece uygulandığının ölçülebilmesi gerekir. Bunun için ölçme yöntemlerinin de tanımlanması gerekir. *Kontrol et* işlemine *operasyonel seviyeden* başlanır. Bu seviyede ölçmek için çeşitli kaynaklardan elde edilmiş veriler kullanılır. Bunlar; mümkün ise bilgi sistemlerinden alınabilecek raporlama verileri ve özel yazılımlardan elde edilecek veriler olabilir. Ya da bilgi sistemlerinden elde edilemeyen, mülakatlar, anketler gibi kaynaklardan elde edilen veriler olabilir. Bu verilerden oluşturulan uyumluluk raporları bir üst seviye olan taktik seviyeye gönderilir. Taktik seviyede ilgili politika, prosedür ve standartlara uyumluluk irdelenir. Stratejik seviyeye iletmek üzere sadeleştirilmiş uyumluluk raporları hazırlanır. Operasyonel ve taktik seviyede kamu kurumları için kurulması zorunlu hale getirilmiş olan iç kontrol teşkilatı da kullanılmalı ve iç kontrol teşkilatının önemli görevlerinden biri bu seviyelerdeki uyumluluk kontrollerini yapmak

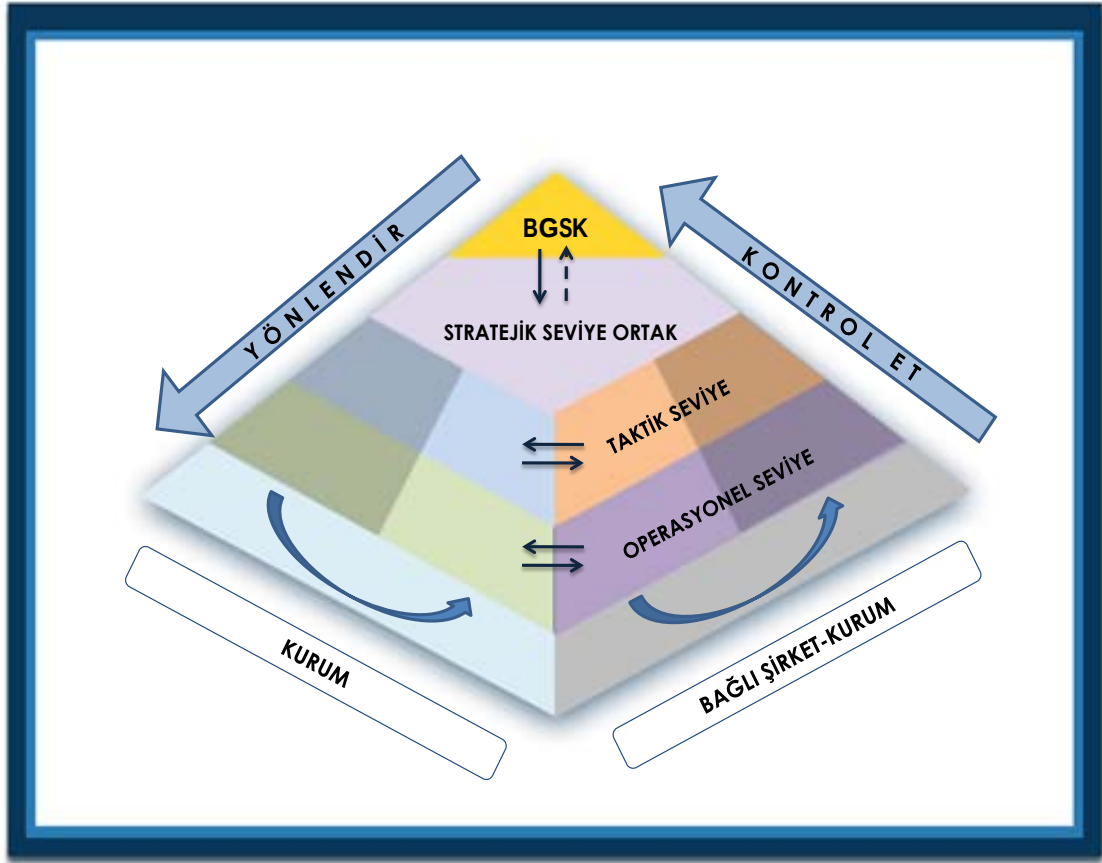
olmalıdır. Tüm bu direktiflere uyumluluğu yansıtan uyumluluk raporları özetlenerek stratejik seviyeye iletilir.

3.2. Bir Kurum ve O Kuruma Bağlı Organizasyonlar (Kurum, Kuruluş, Şirket) Arasında Bilgi Güvenliği Yönetişim Modeli

Bir Kurum ve yönetim olarak o kuruma bağlı kurum, kuruluş veya şirket arasında bilgi güvenliği yönetişimi kurulması açısından bakıldığında özel bir model kurulması gerekliliği vardır. Bu kurumların organizasyonu ve yönetim yapısının hiyerarşik ve paralel özellikler içermesi nedeniyle bilgi güvenliği stratejilerinin ortak belirlenmesi gerekir. Bu nedenle kurulacak bilgi güvenliği yönetim modelinde Şekil 3’te gösterildiği gibi stratejik seviyenin ortak olması önerilmiştir.

Stratejik seviyede tüm kurum ve bağlı organizasyonların en üst yöneticilerinin oluşturduğu ortak bir kurul oluşturulmalıdır. Bu kurulda oluşturulan bütün strateji ve direktifler, bağlı tüm organizasyonların taktik seviyeleri için girdi kabul edilir. Bütün organizasyon için taktik seviyesinde oluşturulacak dokümanlar birbirine uyumlu olması stratejinin uygulanabilirliği açısından bir zorunluluk içermektedir.

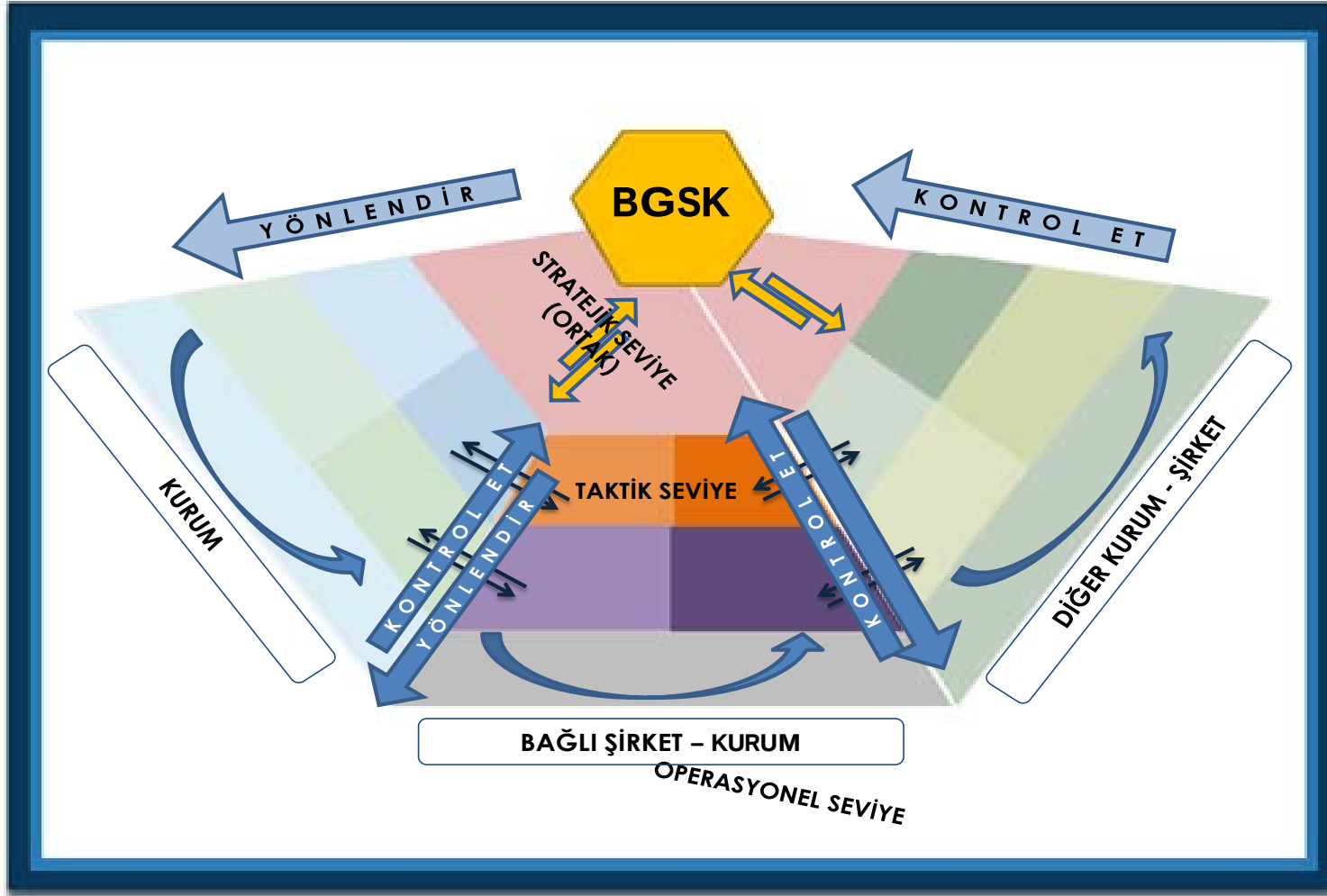
Bir Kurum ve o kuruma bağlı organizasyonlar (bağlı şirket, kurum, kuruluş) arasında taktik seviyede ve operasyonel seviyede çok yakın etkileşimler kaçınılmaz olacağından, çok yakın bir iletişim şekli çalışma biçimi geliştirilmelidir. Dolayısıyla operasyonel seviyede kurallar oluşturulurken bu etkileşim mutlaka göz önüne alınmalıdır. Şekil 3’te bu seviyeler arasındaki ok işaretleri bu etkileşimleri göstermektedir.



Şekil 3.2: Kurum ve Bağlı-Kurum-Kuruluş-Şirket Bilgi Güvenliği Yönetişim modeli

3.3. Kurumların Birbirleri Arasında Bilgi Güvenliği Yönetişim Modeli

Her kamu kuruluşu kendi *Bilgi Güvenliği Yönetişim Modeli*’ni bölüm 3.4 de belirtilen BGSK’nın kriterleri çerçevesinde kurması gerekmektedir. Stratejik seviyede bir kurumun başka bir kurumla ilişki kurması öngörülmemiştir. Ancak ilgili kurumların birbirleriyle taktik seviyede ve operasyonel seviyede ilişki kurmaları gerekebilmektedir. Bu nedenle bu seviyelerde iletişim ve etkileşim kuralları oluşturulmalıdır. Bu oluşturulan ortak çalışma kuralları, güvenlik politikaları, kurumlar arası standartlar, kurumlar arası prosedürler, kılavuzlar, prensipler olabilir.



Şekil 3.3: Bütünleşik Bilgi Güvenliği Yönetişim Modeli.

3.4. Bütünleşik Bilgi Güvenliği Yönetişim Modeli

Bilgi güvenliği yönetiminde olabilecek zaafiyetler, özel ve /veya kamu kurumlarının birbirleriyle etkileşimleri nedeniyle kurumların hepsinde etkili olabilecektir. Bu nedenle, bilgi güvenliği yönetim modelinin ve uygulamasının kurumlararası bütünleştirmeye gereksinimi olacaktır. Kurumların kendi aralarında çalışma prensipleri ortaya koymaları tek başına yeterli olamayacağı için ulusal çapta bir organizasyona ihtiyaç vardır. Bu organizasyon Bilgi Güvenliği Stratejisi Kurulu (BGSK) olarak adlandırılabilir. Bu kurul ulusal çapta Bilgi Güvenliği stratejilerini, kural ve uygulamaları ortaya koymalı ve takibini yapmalıdır. Tüm kamu kurumlarının ve özel şirketlerin bu kurulun oluşturacağı stratejilere uyma zorunluluğu olmalıdır.

Tüm bahsettiğimiz modellerde şekil 3.3'te gösterildiği gibi stratejik seviyelerin girdi olarak bu kurulun oluşturduğu kuralları alması gerekir. Stratejik seviyelerde bu kurallara uygun olarak yeni strateji ve direktifler oluşturulup taktik seviyeye iletilir.

4. İBB, BAĞLI KURUMLAR VE İŞTİRAK ŞİRKETLERİ İÇİN ÖRNEK BİLGİ GÜVENLİĞİ YÖNETİŞİM MODELİ TASARIMI

Bu bölümde, önerilen modelin örnek bir kurum (İstanbul Büyükşehir Belediyesi ve bağlı Kurum/Şirketlerinde) için tasarımı yapılarak uygulamanın nasıl olacağı üzerinde durulmuştur.

4.1. İBB Yönetim Yapısı

İstanbul Büyükşehir Belediyesi'nin kurumsal yapısı, iç birimler, bağlı kuruluşlar (İSKİ, İETT) ve iştirak şirketlerinden oluşmaktadır. Bizzat Belediye bünyesinde hizmet veren birimler, 21 Daire Başkanlığı ve bu Daire Başkanlıklarına bağlı olarak hizmet veren toplam 80 Müdürlükten oluşmaktadır. İstanbul Büyükşehir Belediyesi'ne bağlı kuruluşlardan olan İSKİ, 1981 yılında 2560 sayılı kanunla İstanbul Valiliği denetiminde kurulmuş ve 1984 yılında 3009 sayılı kanunla İstanbul Büyükşehir Belediyesi bünyesine alınmıştır. Hali hazırda İstanbul Büyükşehir Belediyesi'ne bağlı, bağımsız bütçeli, kamu tüzel kişiliğine sahip bir kuruluştur. 1939 yılında kurulan İETT de, yine İSKİ gibi, İstanbul Büyükşehir Belediyesi'ne bağlı, bağımsız bütçeli, kamu tüzel kişiliğine sahip bir kuruluştur.

İstanbul Büyükşehir Belediyesi'nin kurumsal yapısında kendi iç birimleri ve bağlı kuruluşlara (İSKİ, İETT) ilaveten, ayrı bir tüzel kişiliğe ve bütçeye sahip, yarı ticari nitelikte ancak İstanbul Büyükşehir Belediyesi'ne bağlı ve Büyükşehir Belediyesi'nin genel denetimine tabi olarak çalışan özel amaçlı kuruluşlar olan iştirak şirketleri vardır. Bu iştirak şirketlerinin sayısı da hali hazırda 23'tür.

Çalışmamıza konu olan Bilgi Güvenliği Yönetişim Modeli (BGYM) 'ni İstanbul Büyükşehir Belediyesi örneğinde ele alırken, iç birimlerin, bağlı kuruluşların ve şirketlerin çalışma sistemlerini ve bilgi teknolojilerini kullanım yoğunluğunu göz önünde bulundurarak 4'lü bir tasnif yapmak yerinde olacaktır.

Bu tasnife göre; Bu çalışmaya konu olan Bilgi Güvenliği Yönetişim Modeli (BGYM)'nde, İstanbul Büyükşehir Belediyesi iç birimleri; 21 Daire Başkanlığına

bağlı 80 Müdürlüğü, bağlı kuruluşlar; İSKİ ve İETT'yi, 1. Sınıf şirketler ve 2. Sınıf şirketleri kapsamaktadır.(Tablo 4.1 ve 4.2)

<i>I.SINIF ŞİRKETLER</i>	
1	BELBİM A.Ş.
2	BİMTAŞ
3	İDO A.Ş.
4	İGDAŞ
5	İSBAK A.Ş.
6	İSFALT A.Ş.
7	İSTAÇ A.Ş.
8	İSTANBUL HALK EKMEK A.Ş.
9	İSTANBUL ULAŞIM A.Ş.
10	İSTON A.Ş.
11	KİPTAŞ
12	KÜLTÜR A.Ş.
13	SAĞLIK A.Ş.

Tablo 4.1: İBB Bağlı I.Sınıf Şirketler

<i>II.SINIF ŞİRKETLER</i>	
1	AĞAÇ A.Ş.
2	BELTUR A.Ş.
3	HAMİDİYE A.Ş.
4	İSPARK A.Ş.
5	İSTANBUL DÜNYA TİCARET MERKEZİ A.Ş.
6	İSTANBUL ENERJİ A.Ş.
	İSTANBUL İMAR A.Ş.
7	İSTANBUL OTOBÜS A.Ş.
8	SPOR A.Ş.
9	UGETAM A.Ş.

Tablo 4.2: İBB Bağlı II. Sınıf Şirketler

Önerilen modelin bir Kamu kuruluşu olan İstanbul Büyükşehir Belediyesinde (İBB) uygulamasının nasıl olacağına yönelik bir örnek şekil 5'te gösterilmiştir. İBB'ye bağlı kamu kurumu olan 2 Genel Müdürlük (İSKİ,İETT) ve hisselerinin tamamı İBB'ye ait olan ve yönetim kurulları İBB yöneticilerinden oluşan 23 şirketi (İGDAŞ, İDO, KIPTAŞ, BELBİM, İSTON, vb) bulunmaktadır. Belediye yönetimi Başkan, Genel Sekreter, genel sekreter Yardımcıları, daire başkanları, müdürler ve şeflerden oluşmaktadır. Bağlı genel müdürlüklerin yönetimi, genel müdür, genel müdür yardımcısı, daire başkanları, müdürler ve şeflerden oluşmaktadır. Şirketlerin yönetimi ise, şirketin büyüklüğüne göre genel müdür, genel müdür yardımcısı, müdürler ve şeflerden, ya da genel müdür, müdür ve şeflerden oluşmaktadır.

4.2. İBB Tek Kurum Olarak Bilgi Güvenliği Yönetişim Modeli

İBB'de kurulacak Bilgi Güvenliği Yönetişim Modelinde her bir seviyede görevlendirilen personel şu şekilde olmalıdır:

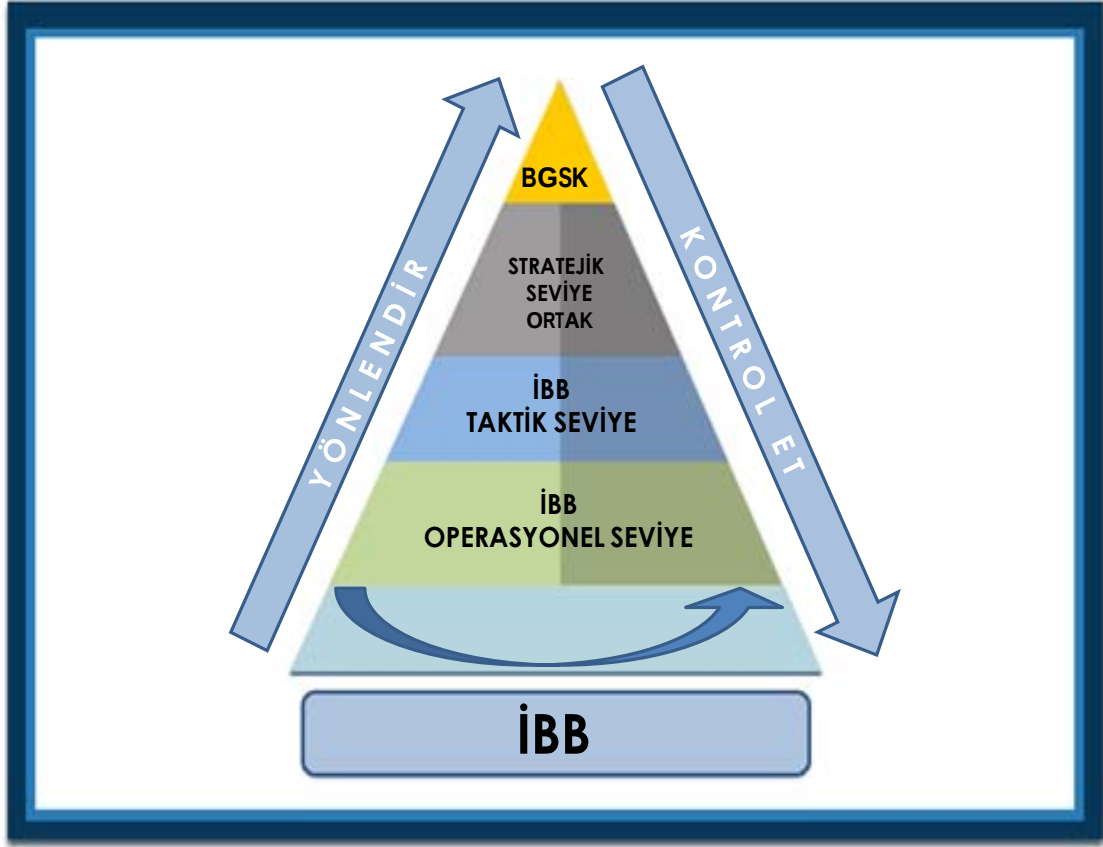
4.2.1. Stratejik Seviye:

Stratejik Seviye İBB ve bağlı kurumlar ve iştirak şirketleri için tek olacağından en üst seviye yöneticilerden oluşması sağlanmalıdır. Bu seviyede İBB ve bağlı kuruluşların üst seviye yöneticileri olmalıdır. Bunlar İBB Genel Sekreteri, Bilgi Teknolojileri Daire Başkanının bağlı bulunduğu Genel Sekreter Yardımcısı, Stratejik Planlama Daire Başkanı, Bilgi Teknolojileri Daire Başkanı, İştirakler Daire Başkanı, bağlı kurumların (İSKİ-İETT) Genel Müdürleri ve belli büyüklükteki bağlı şirketlerin Genel Müdürlerinden oluşmalıdır.

4.2.2. Taktik Seviye:

İBB'de taktik seviyedeki yöneticiler; Bilgi Teknolojileri Daire Başkanı, Bilgi İşlem Müdürü, Elektronik Sistemler Müdürü, Coğrafi Bilgi Sistemi Müdürü, Stratejik Planlama Müdürü, İç-Kontrolde sorumlu müdür (Mali Kontrol Müdürü), İnsan Kaynakları Müdürü, Arşiv Müdürü ve Yazı İşleri Müdüründen oluşmalıdır. Bağlı genel müdürlüklerde bu seviye bilgi işlem biriminin bağlı bulunduğu Genel

Müdür Yardımcısı, Bilgi İşlem Müdürü, Elektronik Sistemler Müdürü, İnsan Kaynakları Müdürü, ilgili müdürlerden oluşmalıdır.



Şekil 4.1: İBB Tek Kurum Bilgi Güvenliği Yönetişim Modeli.

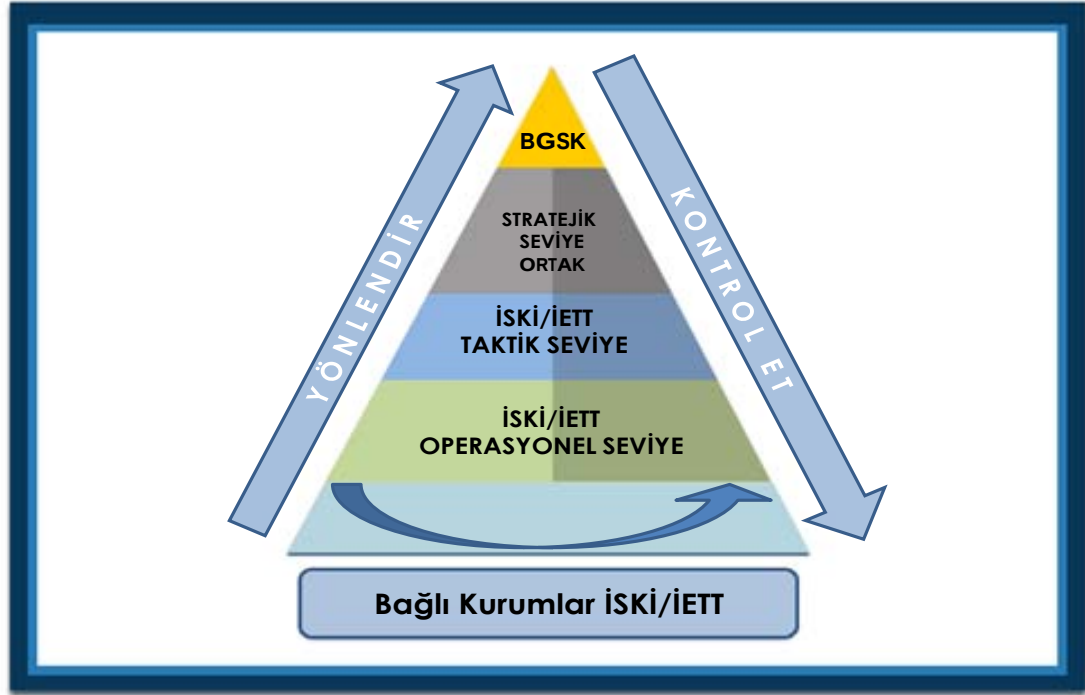
4.2.3. Operasyonel Seviye:

İBB’de operasyonel seviyede Bilgi İşlem Müdür Yardımcıları, Coğrafi Bilgi Sistemi Müdür Yardımcıları, Elektronik Sistemler Müdür Yardımcıları, Security Admin, Unix Admin, MS Sistem Admin, Database Admin, ve kontrol döngüsünde iç kontrol teşkilatının ilgili personelinden oluşur.

4.3. İBB ve Bağlı Kurumlar (İSKİ-İETT) Modeli

İBB’ye bağlı kurumlar olan İSKİ ve İETT organizasyon yapıları itibariyle büyük kurumlar olduklarından, Bilgi Güvenliği Yönetişim Modelleri İBB ile benzer olacaktır. Stratejik seviye İBB ile ortak olmakla birlikte taktik ve operasyonel seviyeleri ayrı olmalıdır. İSKİ ve İETT mevzuat ve yönetim açısından benzerlik

gösterdiklerinden Bilgi Güvenliği Yönetişim Modelinde de her bir seviyedeki organizasyon aynı olacaktır. Bu Bunlar:



Şekil 4.2: İBB Bağlı Kurumlar Bilgi Güvenliği Yönetişim Modeli.

4.3.1. Taktik Seviye:

İSKİ ve İETT’de taktik seviyedeki yöneticiler; bilgi işlem biriminin bağlı bulunduğu Genel Müdür Yardımcısı, Bilgi İşlem Daire Başkanı, Bilgi İşlem Müdürü, Elektronik Sistemler Müdürü, Coğrafi Bilgi Sistemi Müdürü (Sadece İSKİ’de), Stratejik Planlama Müdürü, İç-Kontrolden sorumlu Müdür, İnsan Kaynakları Müdürü ve Yazı İşleri Müdüründen oluşmalıdır. Bağlı genel müdürlüklerde bu seviye, Bilgi İşlem Müdürü, Elektronik Sistemler Müdürü, İnsan Kaynakları Müdürü ve ilgili müdürlerden oluşmalıdır.

4.3.2. Operasyonel Seviye:

İBB ve bağlı kurumlarda bu seviyede bilgi işlem müdür ve müdür yardımcıları, ilgili teknik sistem yöneticileri (exchange admin, unix admin, DBA admin, security admin vb.), iç kontrol teşkilatının ilgili personelinden oluşur.

4.4. İBB İştirak Şirketleri İçin Model

4.4.1. I.Sınıf Bağlı Şirketler

I. Sınıf şirketler, organizasyon yapısı, personel sayısı, yönetici sayısı ve bilgi işlem organizasyonu açısından belli bir büyüklüğe sahip şirketlerdir. Bu sebeple bu tür şirketlerin taktik ve operasyonel seviyelerin ayrı olarak tasarlanması gerekmektedir:



Şekil 4.3: İBB Bağlı I.Sınıf Şirketler Bilgi Güvenliği Yönetişim Modeli.

Taktik Seviye:

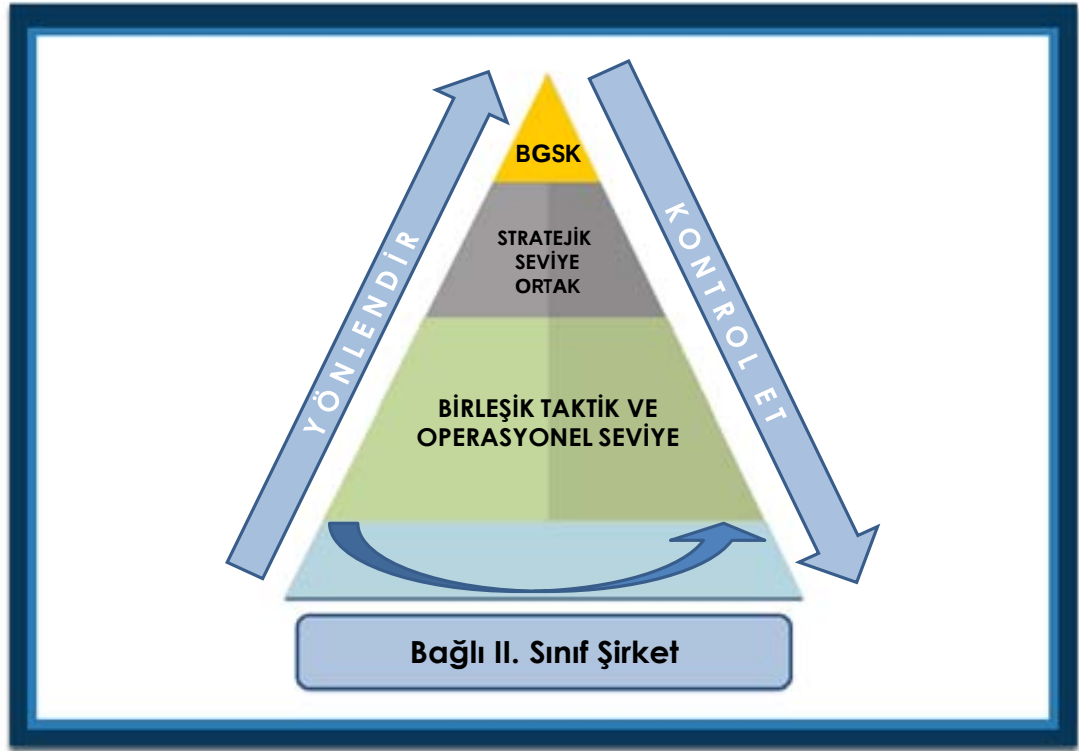
Bu tür şirketlerde taktik seviyedeki yöneticiler; bilgi işlem biriminin bağlı bulunduğu Genel Müdür Yardımcısı, Bilgi İşlem Müdürü, Elektronik Sistemler Müdürü(varsa), Coğrafi Bilgi Sistemi Müdürü(varsa), Stratejik Planlama Müdürü, İç-Kontrol den sorumlu Müdür, İnsan Kaynakları Müdürü ve Yazı İşleri Müdüründen oluşmalıdır.

Operasyonel Seviye :

Bu seviyede bilgi işlem müdür yardımcıları, ilgili teknik sistem yöneticileri (exchange admin, unix admin, DBA admin, security admin vb.), iç kontrol teşkilatının ilgili personelinden oluşur.

4.4.2. II. Sınıf Bağlı Şirketler

II. Sınıf şirketler, organizasyon yapısı, personel sayısı, yönetici sayısı ve bilgi işlem organizasyonu açısından yeterli büyüklüğe sahip olmayan şirketlerdir. Bu sebeple bu tür şirketlerin taktik ve operasyonel seviyelerinin tek olarak tasarlanması gerekmektedir:



Şekil 4.4: İBB Bağlı II. Sınıf Şirketler Bilgi Güvenliği Yönetişim Modeli.

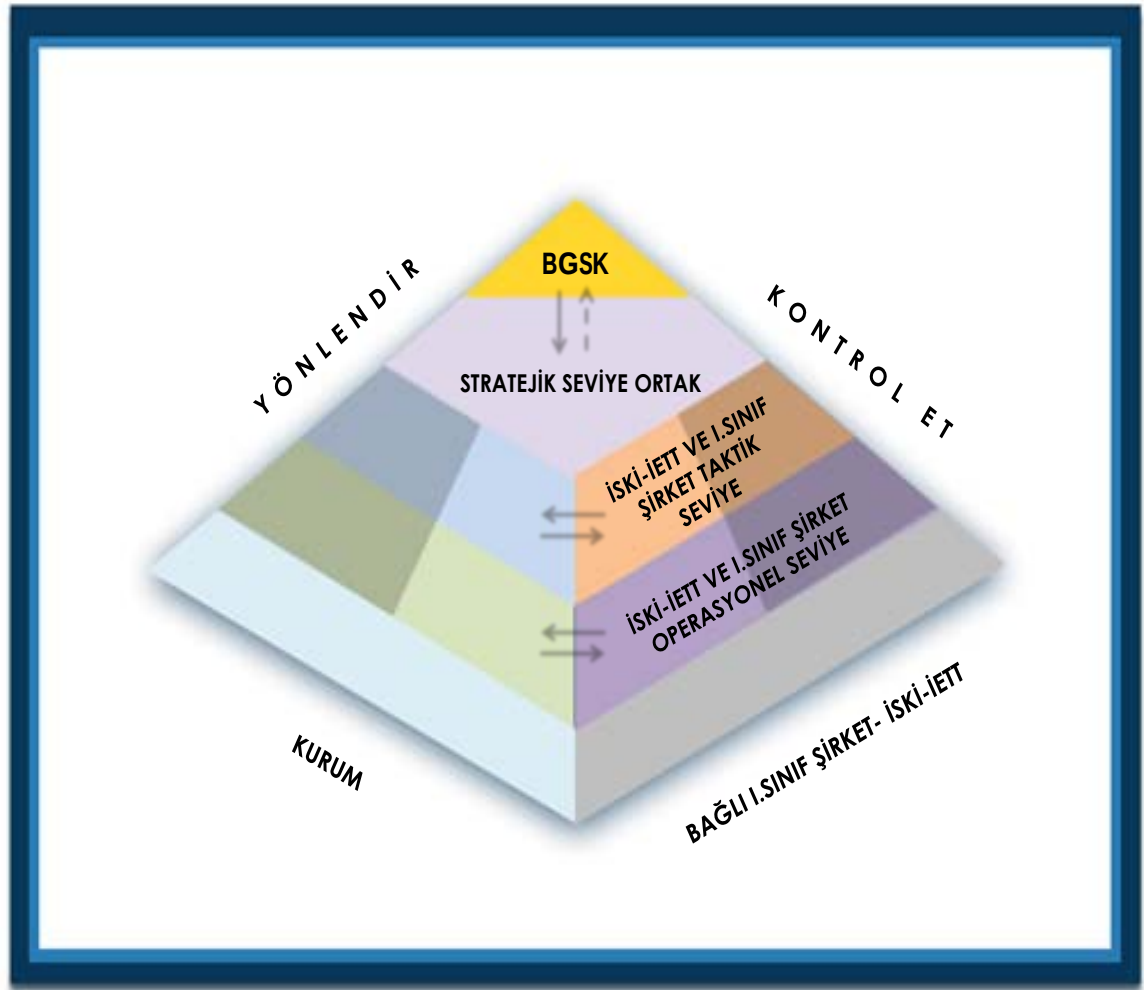
Taktik + Operasyonel Seviye :

Bu tür şirketlerde bu seviyede; bilgi işlem biriminin bağlı bulunduğu Müdür ve ilgili teknik ve idari personelden oluşmalıdır.

4.5. İBB Bağlı Kurumlar ve İştirak Şirketler İle

BGYM

4.5.1. İBB ile Bağlı Kurumlar(İSKİ-İETT) ve I.Sınıf Bağlı Şirketlerle BGYM

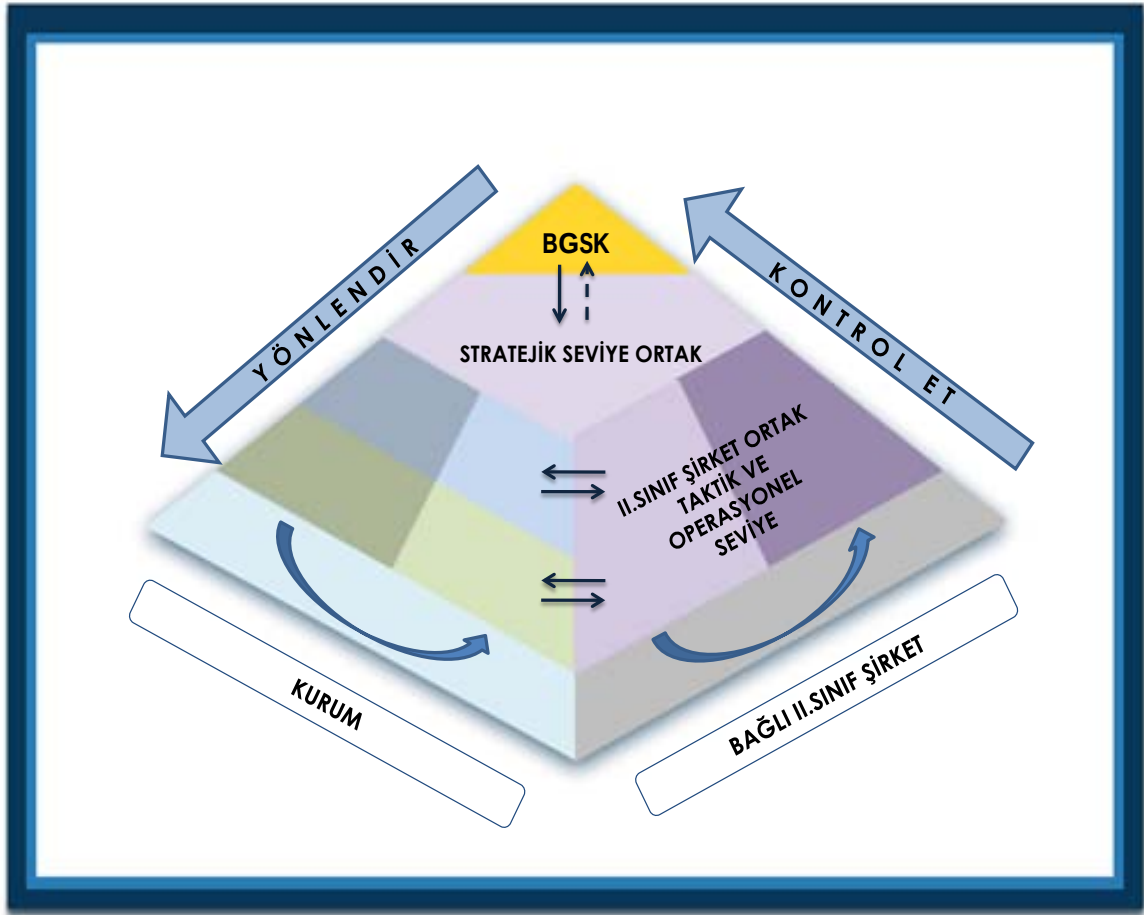


Şekil 4.5: İBB ile Bağlı Kurumlar Arası Bilgi Güvenliği Yönetişim Modeli.

İBB ile bağlı kurumlar (İSKİ-İETT) ve I. Sınıf Şirketler arasındaki Bilgi Güvenliği Yönetişim Modelinde, stratejik seviye ortak taktik ve operasyonel seviyeler ayrı olacaktır. Dolayısıyla stratejik seviye dışındaki seviyelerde etkileşimlerin nasıl olacağı ve kontrollerin nasıl yapılacağı tanımlanmalıdır

4.5.2. İBB ile Bağlı II.Sınıf Bağlı Şirketlerle BGYM

İBB ile bağlı II. Sınıf Şirketler arasındaki Bilgi Güvenliği Yönetişim Modelinde, stratejik seviye ortak taktik ve operasyonel seviyeler İBB’de ayrı, bu şirketlerde ise tek olacaktır. Stratejik seviye dışındaki seviyelerde etkileşimlerin nasıl olacağı ve kontrollerin nasıl yapılacağı tanımlanmalıdır

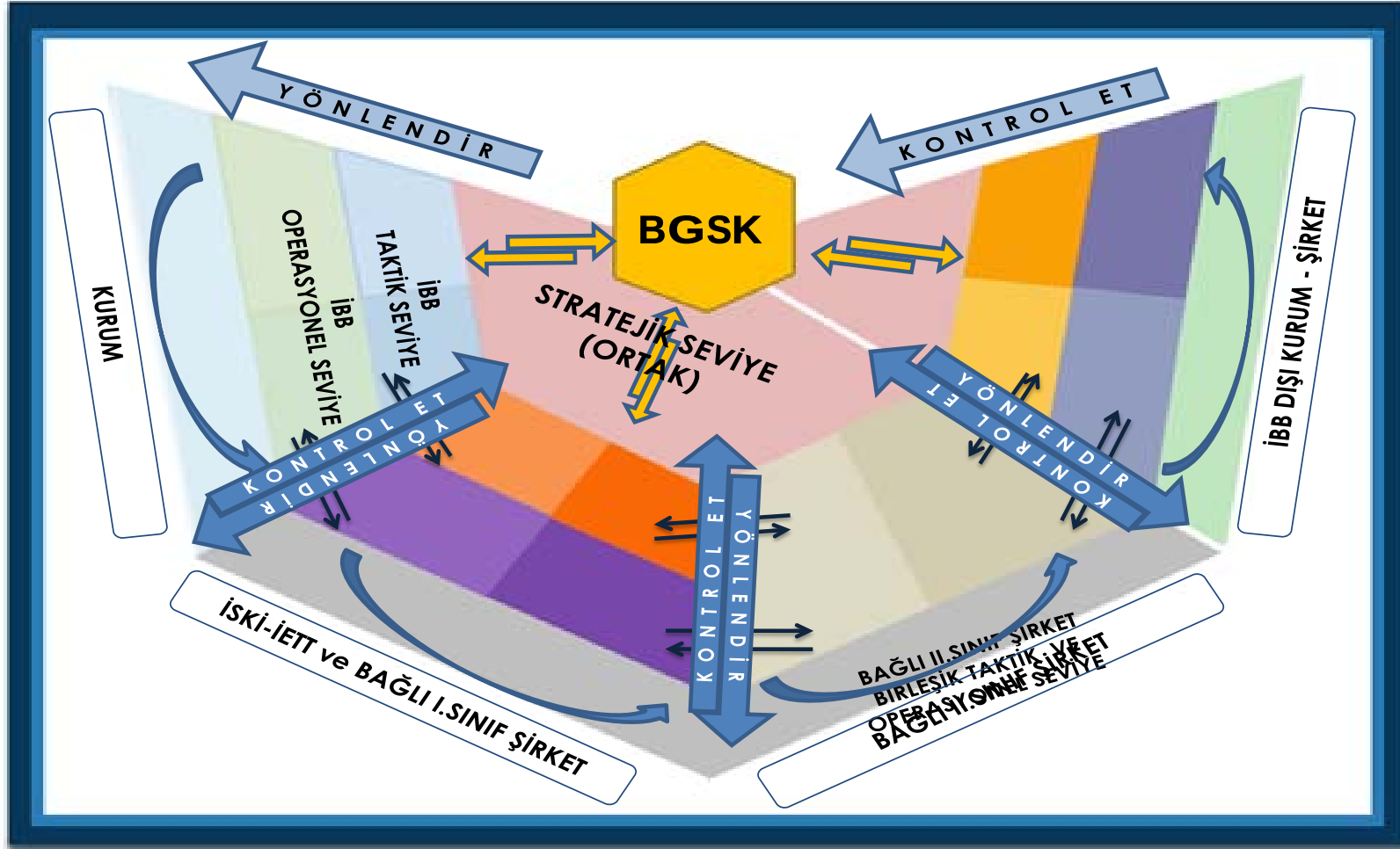


Şekil 4.6: İBB ile Bağlı II. Sınıf Şirketler Arası Bilgi Güvenliği Yönetişim Modeli.

4.6. İBB Genel Bütünleşik Bilgi Güvenliği Yönetişim Modeli

Bilgi Güvenliği Yönetişim Modeli oluşturulurken İBB ve bağlı tüm kuruluşların *tek bir stratejik seviyesi* olmalıdır. Burada oluşturulacak stratejiler her bir organizasyonun stratejik planının bir parçası olmalıdır. Burada stratejiler oluşturulup taktik seviyeye iletilmelidir.

Her bir organizasyonun *taktik seviyesi* farklı olmalıdır. Bu seviyede, stratejik seviyede oluşturulan stratejilere uygun doküman ve direktifler oluşturulur ve operasyonel seviyeye iletilir. Bunlar oluşturulurken Bilgi Güvenliği Yönetim Sistemi (BGYS)'den faydalanılır.



Şekil 4.7: İstanbul Büyükşehir Belediyesi için Bütünleşik Bilgi Güvenliği Yönetişim Modeli.

Operasyonel seviye de her bir kurum için ayrı olmalıdır. İBB ve bağlı organizasyonlar arasında çok yakın bir çalışma ortamı vardır. Bu çalışma şekli aynı zamanda bilgi güvenliği açısından birçok riski de barındırmaktadır. Bu risklerin azaltılması ve ölçülebilmesi açısından taktik seviye ve operasyonel seviyede etkileşim kuralları tanımlanmalı ve gerekli kontrol ve ölçme metodları geliştirilmelidir.

Tüm bu faaliyetlerin yürütülmesi ve uygunluğunun kontrolü için İBB ve bağlı kurumlarda (İSKİ, İETT), artık her bir kurum için zorunluluk olan iç kontrol teşkilatı görevlendirilebilir. Yürütülen çalışmaların uyumluluk açısından kontrol edilmesi ve raporlanması bu birim tarafından yürütülür. İBB İştirak şirketlerinde ise, bu faaliyetler için Genel Müdüre doğrudan bağlı bir kontrol ekibi oluşturulabilir.

İBB ve bağlı kurumlardaki (İSKİ, İETT) İç Kontrol Teşkilatı ve iştirak şirketlerinde bu konuyla ilgili görevlendirilecek personelin bilgi teknolojileri konusunda uzman olması zorunluluğu bulunmamaktadır. Bu personelin denetleyeceği konular sadece ilgili prosedür ve yönergelere uyumluluk kontrolü olmalıdır. İBB çatısı altında da tüm bu kontrol ekibinin faaliyetlerinin raporlanacağı ve takip edileceği yer stratejik seviye olmalıdır. Sayıştay denetlemelerinin de bir kısmı önümüzdeki süreçte, bu bakış açısıyla yapılacaktır. Bütün bu denetlemelere ek olarak, bağımsız denetim firmaları kanalıyla da faaliyetlerin denetlenmesi faydalı olacaktır.

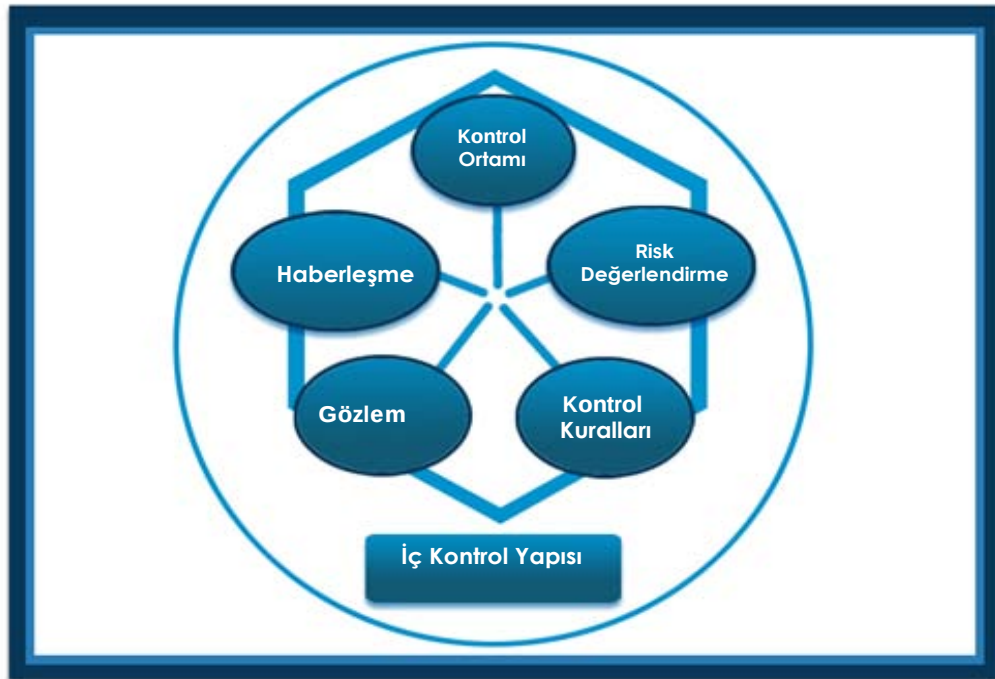
İBB ve bağlı kuruluşları sadece kendi aralarında değil aynı zamanda İlçe Belediyeleri, Valilik, Emniyet, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü, Sosyal Güvenlik Kurumu gibi birçok kamu-kurum ile ayrıca birçok özel şirket ile etkileşim içerisinde bulunmak durumundadır. Bu kurumlarla veya şirketlerle stratejik seviyede bir iletişime ihtiyaç olmamakla birlikte taktik ve operasyonel seviyede mutlaka etkileşim kuralları tanımlanmalıdır.

Buna bir örnek vermek gerekirse, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü'nün kurup işletmekte olduğu MERNİS sistemini, vatandaşa hizmet veren her özel ve kamu kurumu kullanmak durumundadır. Ancak bu sistemden sağlanan bilgiler sadece hizmet amaçlı kullanılması gereken bilgilerdir. Bu sebeple taktik seviyede bu kurumla hangi tür bilgilerin hangi seviyede paylaşılacağı ve

sorgulamalardaki hangi bilgilerin loglanacağını kuralları tanımlanır. Operasyonel seviyede ise Arada kurulacak web servislerinin şekli ve güvenlik standartları, bağlantı şekli ve loglamanın nasıl yapılacağı belirlenir. **(Yönlendir)**

Operasyonel seviyede tüm bu işlemler belirli aralıklarla farklı bir ekip tarafından denetlenir. Bu denetleme faaliyetleri, loglamanın düzgün yapılıp yapılmadığı, uygulamayı kullanan kişilerin şifrelerini paylaşp paylaşmadıkları, bu servisin hizmet amacı dışında kullanılıp kullanılmadığı gibi konulardan oluşur. Bu denetleme faaliyetleri teknik ve sorgulama gibi teknik olmayan unsurlar içerebilir. Taktik seviyede ise konulan kuralların ne derece yeterli olduğu ve kurum stratejisine uygun gerçekleşip gerçekleşmediği denetlenir. **(Kontrol Et)**

Gerek İBB ve gerekse İBB'nin ilişkide olduğu kurum ve kuruluşların stratejik seviyelerinde oluşturdukları stratejilerin Bilgi Güvenliği Stratejisi Kurulu stratejilerine uygun olma zorunluluğu olacaktır. Ancak gerekirse BGSK'nun stratejilerinin eksik ve düzeltilmesi gereken tarafları varsa bu konuda gerekli geri bildirimlerde bulunulması da mümkün olabilecektir.



Şekil 4.8 : İç Kontrol Yapısı

4.7. İç Kontrol Teşkilatı ve Önerilen Modelde Kontrol Döngüsünde Kullanılması

4.7.1. İç Kontrol Teşkilatı ve COSO Modeli

İç kontrol; bir kurumun yönetimi ve personeli tarafından hayata geçirilen tamamlayıcı bir süreç olup aşağıda sıralanan hedefleri gerçekleştirmek suretiyle; kurumun misyonunu başarması için riskleri göğüslemek ve makul bir güvence sağlamak üzere tasarlanmıştır:

- Faaliyetleri düzenli, ahlak kurallarına uygun, ekonomik, verimli ve etkin biçimde gerçekleştirme,
- Hesap verme sorumluluğunun gerektirdiği yükümlülükleri yerine getirme,
- Yürürlükteki kanunlara ve yönetmeliklere uyma,
- Kayıplara, kötü kullanıma ve hasarlara karşı kaynakları koruma.



Şekil :4.9 : COSO Piramidi

İç kontrol ile ilgili en temel kaynak COSO (Commitee on Sponsoring Organizations) Raporu olarak da bilinen ve orijinal ismi Internal Control-Integrated Framework (İç Kontrol-Bütünleşik Çerçeve) olan bir çalışma raporudur.

COSO (Commitee on Sponsoring Organizations) 1985 yılında finansal tablolardaki hata ve hilelerin nedenlerini araştırmak ve engellemek için kurulmuş, bir özel sektör girişimidir. Özel sektör girişimi olmakla birlikte bu çatı altında kamuda iç kontrol düzenlemelerine yönelik önemli araştırmalar ve öneriler gerçekleştirilmiştir. Özel sektörde uygulanmak üzere geliştirilen ve günümüzde kamu sektöründe uygulama alanı bulan COSO İç Kontrol Modeli en çok esas alınan iç kontrol modelidir. Avrupa Birliğinin genişleme sürecinde mali kontrol alanında yapılan çalışmalar sonucunda COSO modeline dayalı bir iç kontrol sistemi benimsenmiştir. Uluslararası Sayıştaylar Birliği (INTOSAI) tarafından, COSO modelini esas alan “Kamu Sektörü İçin İç Kontrol Standartları Kılavuzu” 2004 yılında yayımlanmıştır.



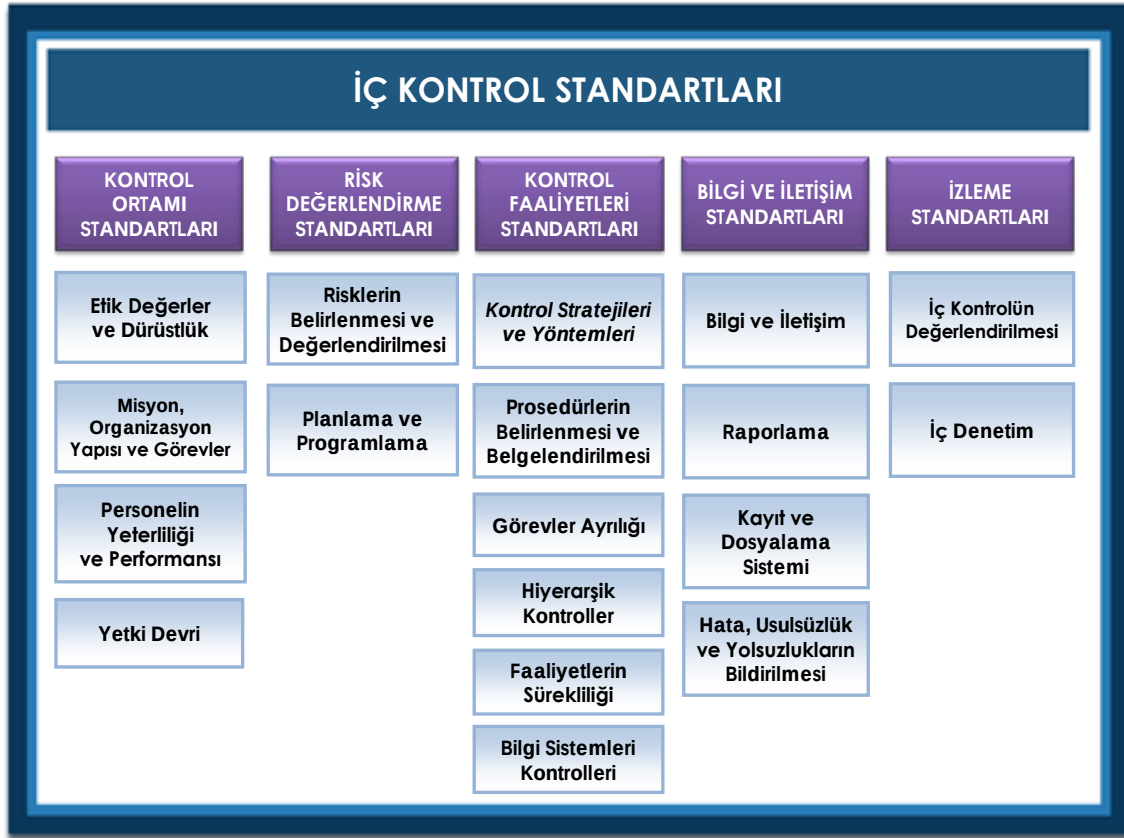
Şekil 4.10 : COSO küpü

COSO küpü ya da piramidi olarak bilinen model iç kontrol uygulamalarında referans olarak kullanılmaktadır.

Çeşitli iç kontrol modeller :

- COSO-Committee of Sponsoring Organisations (Amerika)
- CoCo- Criteria of Control Objectives (Kanada)
- Turnbull Report-(İngiltere)
- King's Report (Güney Afrika)
- CoBit (Teknolojik Sistemler Denetimi Kontrol Standartları)

İç Kontrol Standartları



Şekil 4.11 : İç Kontrol Standartları

Kontrol Ortamı Standartları

Kontrol ortamı iç kontrol sistemi uygulamalarının üzerine inşa edildiği ve yönetildiği bir alan/değerler bütünüdür. İç kontrol ortamının asıl kaynağını kurumun

geçmişi, kurumsal kültür ve yönetim felsefesi oluşturmaktadır. Bir bina için temel ne anlam ifade ediyorsa, bir kurumun iç kontrol sistemi için de çalışma ortamı odur. Çalışanların, kurumun varlık sebebini, kendi görev ve sorumluluklarının neler olduğunu, hangi fiil ve davranışlarının kabul edilebilir, hangilerinin kabul edilemez olduğunu bildikleri, işe alma, terfi, eğitim, disiplin, mali ve sosyal haklar vb. insan kaynakları uygulamalarının yazılı olarak objektif kurallara bağlandığı ve çalışanlar arasında her hangi bir ayrımcılığın söz konusu olmadığı, görev tanımları çerçevesinde kendilerine verilen işlerin yürütülmesi için eğitim ve donanım başta olmak üzere çalışanlara gerekli kaynakların tahsis edildiği, yöneticilerin çalışanları motive ederek onlarla aynı hedefe doğru kilitlendiği, kurum çalışanları ve birimleri arasında raporlama ve hiyerarşik ilişkilerin açık ve net olarak belirlendiği bir ortam, artık amaçların gerçekleştirilmesi için uygun bir çalışma ortamının var olduğuna işaret eder.

Kontrol ortamı, iç kontrolün diğer unsurlarına temel teşkil eder:

- Etik Değerler ve Dürüstlük
- Misyon, organizasyon yapısı ve görevler
- Personelin yeterliliği ve performansı
- Yetki Devri

Standart: 1. Etik Değerler ve Dürüstlük: Personel davranışlarını belirleyen kuralların personel tarafından bilinmesi sağlanmalıdır.

Standart: 2. Misyon, organizasyon yapısı ve görevler: İdarelerin misyonu ile birimlerin ve personelin görev tanımları yazılı olarak belirlenmeli, personele duyurulmalı ve idarede uygun bir organizasyon yapısı oluşturulmalıdır.

Standart: 3. Personelin yeterliliği ve performansı: İdareler, personelin yeterliliği ve görevleri arasındaki uyumu sağlamalı, performansın değerlendirilmesi ve geliştirilmesine yönelik önlemler almalıdır.

Standart: 4. Yetki Devri: İdarelerde yetkiler ve yetki devrinin sınırları açıkça belirlenmeli ve yazılı olarak bildirilmelidir. Devredilen yetkinin önemi ve riski dikkate alınarak yetki devri yapılmalıdır.

Risk Değerlendirme Standartları

Alınan her karar, gerçekleştirilen her işlem beraberinde bazı riskleri getirmektedir. Kurumlar büyüklükleri, içinde bulundukları sektör, organizasyon yapıları, yönetim biçimleri, sundukları ve ürün hizmetler ne olursa olsun çeşitli risklerle karşılaşmaktadırlar. Risk iş hayatının doğasında var olan bir olgudur. Riskin olmadığı bir çalışma ortamı mümkün değildir. Bu yüzden yöneticiler riskleri sıfırlamaya değil, riskleri en aza indirmeye, ortaya çıkabilecek risklerin etkilerini sıfırlamaya odaklanmalıdırlar. Risklerin belirlenebilmesi için de öncelikle kurumsal hedeflerin belirlenmiş olması gerekmektedir. Belirlenen hedefler doğrultusunda kurumun üstlenebileceği/göğüsleyebileceği risk iştahına/düzeyine karar vermek ise üst yönetimin sorumluluğundadır. Kurumsal hedefler doğrultusunda ortaya çıkması muhtemel riskler belirlenmeli, bu risklerin nasıl yönetileceğine karar verilmelidir. Kurumsal süreçlerde ve faaliyetlerde riskli alanlar olarak belirlenmiş konulara ayrı bir özen gösterilmeli ve kontrol faaliyetleri bu süreçlere titizlikle yerleştirilmelidir.

Risk değerlendirmesi, kurumun, faaliyetlerde etkinlik, mali raporlarda güvenilirlik ve düzenlemelere uyum hedeflerini olumsuz etkileyecek iç ve dış olayların tespit ve analiz edilerek bunlara uygun cevaplar verilmesini belirleme sürecidir.

İç Kontrol faaliyeti risk esaslı olarak gerçekleştirilmelidir. Risk Değerlendirmesinde Yöntem öncelikle kurumun amaçları açık, net ve tutarlı biçimde belirlenmelidir. Amaçlar belirlendikten sonra amaçlarla bağlantılı iç ve dış kaynaklı riskler tanımlanır, değerlendirilir ve alınacak tedbirler kararlaştırılır.

Risk değerlendirme, idarenin hedeflerinin gerçekleşmesini engelleyecek risklerin tanımlanması, analiz edilmesi ve gerekli önlemlerin belirlenmesi sürecidir.

Standart: 5. Planlama ve Programlama: İdareler, faaliyetlerini, amaç, hedef ve göstergelerini ve bunları gerçekleştirmek için ihtiyaç duydukları kaynakları içeren plan ve programlarını oluşturmalı ve duyurmalı, faaliyetlerinin plan ve programlara uygunluğunu sağlamalıdır.

Standart: 6. Risklerin belirlenmesi ve değerlendirilmesi: İdareler, sistemli bir şekilde analizler yaparak amaç ve hedeflerinin gerçekleşmesini engelleyebilecek iç ve dış riskleri tanımlayarak değerlendirmeli ve alınacak önlemleri belirlemelidir.

Kontrol Faaliyetleri Standartları

Yönetim faaliyetlerin belirlenmiş ilke ve stratejilere uygun bir şekilde gerçekleştirilmesinde yöneticilere yardımcı olan politika ve yöntemlerdir. Kontrol faaliyetleri ile kurumsal risklerin yönetilmesi amaçlanmaktadır. Kontrol faaliyetleri gerek politika, kültür, değerleri gibi soyut olgular ile onay, belge düzeni, formlar gibi somut olguları kapsamaktadır. Kontrol faaliyetleri kurumun tüm süreçlerine ve faaliyetlerine yerleştirilebilecek işlemler olup, dinamik ve esnek karakterlidirler. Kurumsal süreçler ve faaliyetler göz önünde bulundurularak değişen koşullara uyum sağlayabilecek şekilde tasarlanmalıdırlar. Yetki ve sorumlulukların belirlenmesi, onay silsilesi, tahakkuk, hesap mutabakatları, görev ayrımı, kurum varlıklarının korunması (fiziki ve kaydi), operasyonel süreçlerin gözden geçirilmesi, denetim işlemleri gibi faaliyetler kontrol faaliyetlerine örnek olarak gösterilebilir.

Kontrol faaliyetleri, kurumun amaçlarına ulaşmasını etkileyebilecek risklerle başa çıkmak üzere belirlenen ve uygulamaya konulan politikalar ve prosedürlerdir. Kontrol faaliyetleri riskleri kabul edilebilir düzeylerde yönetmek için kullanılır. Risklerin çeşidine göre, önleyici, tespit edici ve düzeltici her türlü kontrol faaliyeti belirlenir ve uygulanır.

Kontrol Faaliyetlerinin çeşitleri:

- Yetki-onay prosedürleri
- Görevlerin ayrılığı
- Hiyerarşik kontroller
- Varlıkların fiziki güvenliği
- Kayıt ve dosyalama
- Bilgi teknolojileri kontrolleri

Standart: 7. Kontrol stratejileri ve yöntemleri: İdareler, hedeflerine ulaşmayı amaçlayan ve riskleri karşılamaya uygun kontrol strateji ve yöntemlerini belirlemeli ve uygulamalıdır.

Standart: 8. Prosedürlerin belirlenmesi ve belgelendirilmesi: İdareler, faaliyetleri ile mali karar ve işlemleri için gerekli yazılı prosedürleri ve bu alanlara ilişkin düzenlemeleri hazırlamalı, güncellemeli ve ilgili personelin erişimine sunmalıdır.

Standart: 9. Görevler ayrılığı: Hata, eksiklik, yanlışlık, usulsüzlük ve yolsuzluk risklerini azaltmak için faaliyetler ile mali karar ve işlemlerin onaylanması, uygulanması, kaydedilmesi ve kontrol edilmesi görevleri personel arasında paylaştırılmalıdır.

Standart: 10. Hiyerarşik kontroller: Yöneticiler, iş ve işlemlerin prosedürlere uygunluğunu sistemli bir şekilde kontrol etmelidir.

Standart: 11. Faaliyetlerin sürekliliği: İdareler, faaliyetlerin sürekliliğini sağlamaya yönelik gerekli önlemleri almalıdır.

Standart: 12. Bilgi sistemleri kontrolleri: İdareler, bilgi sistemlerinin sürekliliğini ve güvenilirliğini sağlamak için gerekli kontrol mekanizmaları geliştirmelidir.

Bilgi ve İletişim Standartları

Bilgi ve iletişim, iç kontrol uygulamalarının kullanacağı ve üreteceği bilgiler ile bu bilgilerin paydaşları arasındaki iletişimi kapsamaktadır. Bilgi sistemleri aracılığıyla iç kontrole ilişkin finansal ve finansal olmayan bilgileri içeren raporlar hazırlanır. Bu raporların kaynağı ve sunulacağı makam kurum içinden olduğu gibi kurum dışından da olabilmektedir. İç kontrol sisteminin doğru, zamanlı, ekonomik, nesnel bilgiler ile beslenmesi temel şarttır. Diğer taraftan iç kontrol uygulamalarının sonuçlarının paydaşlarla paylaşılması da gerekmektedir. Bu bağlamda yürütülecek iletişim çalışmaları dikey ve yatay iletişim kanallarını kapsamalıdır. Özellikle üst yönetim, iç kontrol uygulamalarını desteklediğini vurgulamak, iç kontrol sisteminin etkinliğinin artırılmasında bütün çalışanların rolünü önemli olduğunu onlara hissettirmek için kurum içi iletişim yollarını kullanmalıdırlar.

Bilgi ve iletişim, kurumu ilgilendiren iç ve dış bilgilerin belirlenmesi, elde edilmesi, işlenmesi ve kurum içindeki ve dışındaki ilgililere zamanında iletilmesidir.

Bilgi; çalışanların görev ve sorumluluklarını yerine getirebilmesi, sağlıklı karar alabilmesi, şeffaf ve hesap verebilir bir şekilde raporlama yapabilmesi, hedeflerin gerçekleşme performansının takip edilmesi, risklerin yönetilebilmesi için gereklidir.

Bilgi ve iletişim, gerekli bilginin ihtiyaç duyan kişi, personel ve yöneticiye belirli bir formatta ve ilgililerin iç kontrol ve diğer sorumluluklarını yerine getirmelerine imkan verecek bir zaman dilimi içinde iletilmesini sağlayacak bilgi, iletişim ve kayıt sistemini kapsar.

Standart: 13. Bilgi ve iletişim: İdareler, birimlerinin ve çalışanlarının performansının izlenebilmesi, karar alma süreçlerinin sağlıklı bir şekilde işleyebilmesi ve hizmet sunumunda etkinlik ve memnuniyetin sağlanması amacıyla uygun bir bilgi ve iletişim sistemine sahip olmalıdır.

Standart: 14. Raporlama: İdarenin amaç, hedef, gösterge ve faaliyetleri ile sonuçları, saydamlık ve hesap verebilirlik ilkeleri doğrultusunda raporlanmalıdır.

Standart: 15. Kayıt ve dosyalama sistemi: İdareler, gelen ve giden her türlü evrak dahil iş ve işlemlerin kaydedildiği, sınıflandırıldığı ve dosyalandığı kapsamlı ve güncel bir sisteme sahip olmalıdır.

Standart: 16. Hata, usulsüzlük ve yolsuzlukların bildirilmesi: İdareler, hata, usulsüzlük ve yolsuzlukların belirlenen bir düzen içinde bildirilmesini sağlayacak yöntemler oluşturmaktadır.

İzleme Standartları

İzleme faaliyetinin temel amacı iç kontrol sisteminin performansı hakkında sağlıklı bir değerlendirme yapmaktır. İç kontrol uygulamalarının kalitesini değerlendirmek ve iç kontrol sisteminin güncel koşullara uyum sağlayacak şekilde değiştirilip değiştirilmediği izleme faaliyetleri ile anlaşılmaktadır. İç kontrol sisteminin izlenmesi sürekli izleme, özel değerlendirme ya da her ikisinin bir arada kullanılmasıyla gerçekleştirilebilir. İç kontrol sisteminin, değişen hedeflere, ortama, kaynaklara ve risklere ayak uydurabilmesi için yönetim tarafından değerlendirilmesi gerekir.

İzleme Yöntemleri

- Hiyerarşik kontroller
- İç kontrol öz değerlendirme çalışmaları
- İç denetim faaliyetleri

İzleme, iç kontrol sisteminin kalitesini değerlendirmek üzere yürütülen tüm izleme faaliyetlerini kapsar.

Standart:17. İç kontrolün değerlendirilmesi: İdareler iç kontrol sistemini yılda en az bir kez değerlendirmelidir.

Standart: 18. İç denetim: İdareler, fonksiyonel olarak bağımsız bir iç denetim faaliyetini sağlamalıdır. [14]

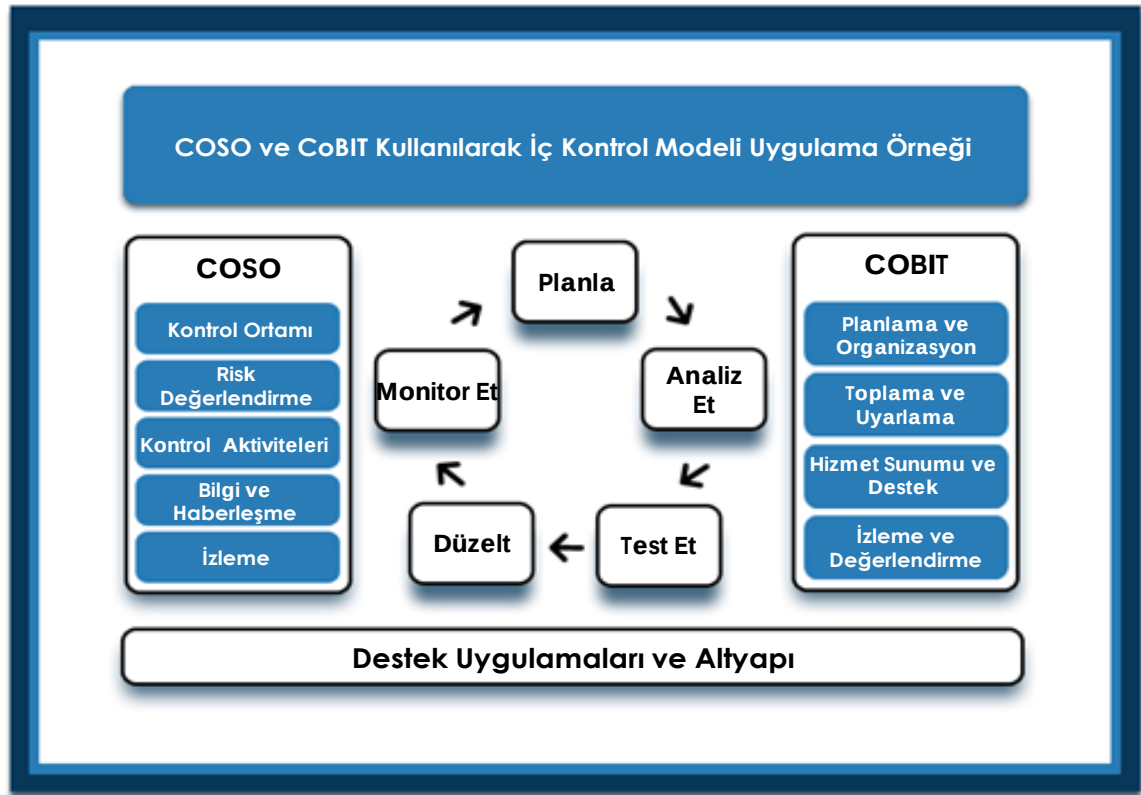
4.7.2. İç Kontrol Sisteminin Bilgi Güvenliği Yönetişim Modelinde Kontrol Döngüsünde Kullanılması

Ülkemizde, 2001 ekonomik krizi ve Avrupa Birliği uyum sürecinin hızlandırıcı etkisi ile son yıllarda “kamu yönetimi alanında” önemli gelişmeler yaşanmaktadır.

Özel sektör uygulamalarında, müşteri memnuniyetini sağlayarak işletmenin amaçlarına ulaşabilmesi için geliştirilen Toplam Kalite anlayışı ve bunu sağlamaya yönelik yönetim metodolojilerinin kamu kurumlarının yapısına uygulanması düşüncesi mevzuatımızda yer bulmuştur.

Nitekim 24.12.2003 tarihli ve 25326 sayılı Resmi Gazetede yayımlanan 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu ile “İç Kontrol Sistemi” kavramı getirilmiştir. Bununla yönetim sorumluluğu ilkesi esas kabul edilerek kontrol ve denetim sorumluluğu idarelere devredilmiştir. Kamu kurumlarının bu sorumluluklarını yerine getirebilmek ve ilgili mercilere hesap verebilmek için etkili ve yeterli bir iç kontrol sisteminin oluşturulması ve işleyişinin sağlanması kamu idarelerinin üst yöneticisi ve yöneticileri için temel bir zorunluluk olarak belirlenmiştir. Ayrıca etkin bir iç kontrol sisteminin, kamu kurumlarında modern bir mali ve idari yönetim yapısının kurulması ve mali disiplinin sağlanması, Stratejik

Yönetim ve Planlama ile çok yıllık Performans Esaslı Bütçelemenin yapılabilmesi için bir zorunluluk olduğu belirtilmiştir.



Şekil 4.12: İç Kontrol Sisteminde farklı modellerin birlikte kullanımı

Bahsi geçen kanunun 55. Maddesi ile başlayan Beşinci Kısım, İç Kontrol Sistemi başlığını taşımakta olup iç kontrolün tanımı, amacı, yapısı ve işleyişi ayrıntılı şekilde belirlenmiştir. Ayrıca Maliye Bakanlığı, görev ve yetkileri çerçevesinde, mali yönetim ve iç kontrol süreçlerine ilişkin standartların ve yöntemlerin belirlenerek geliştirilmesi, uyumlaştırılması ve sistemlerin koordinasyonu konularında, kamu kurumlarına rehberlik etmekle görevlendirilmiştir.

Kanunla yapılan bu düzenlemelere uygun şekilde, 31/12/2005 tarih ve 26040 sayılı üçüncü mükerrer Resmî Gazetede, “İç Kontrol ve Ön Mali Kontrole İlişkin Usul ve Esaslar” belirlenmiştir. Daha sonra ulusal düzeyde iç kontrol çalışmalarının koordinasyonunu yürüten Maliye Bakanlığınca 26.12.2007 tarihinde Kamu İç Kontrol Standartları Tebliği ile kamu idarelerinde iç kontrol sisteminin oluşturulması, uygulanması, izlenmesi ve geliştirilmesi amacıyla 18 standart ve 79 genel şart belirlenmiştir.

Belirlenen standartlar için hem özel sektörde hem de kamu sektöründe yaygın uygulama alanı bulan COSO İç Kontrol Modeli esas alınmıştır. Ayrıca INTOSAI (Uluslar arası Sayıştaylar Birliği) Kamu Sektörü İç Kontrol Standartları Rehberi ve Avrupa Birliği İç Kontrol Standartları, mevzuat düzenlemelerinde dikkate alınmıştır.

COSO modeli esas alınarak, Türkiye’de 10/12/2003 tarihli ve 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunuyla kamu malî yönetim sistemimiz uluslararası standartlar ve Avrupa Birliği uygulamalarına uygun bir şekilde yeniden düzenlenmiş ve bu kapsamda etkin bir iç kontrol sisteminin oluşturulması amaçlanmıştır.

Dolayısıyla tüm kurum ve şirketlerde, modelimizde tanımlanan **“Kontrol Et”** döngüsünde iç kontrol sisteminin kullanılması uygun olacaktır. Böylece daha etkin bir kontrol yapısının ortaya konması sağlanmış ve iç kontrol sistemi ile BGYM (Bilgi Güvenliği Yönetişim Modeli)’nin uyumluluğu sağlanmış olacaktır. İBB kontrol sistemi ile bağlı kurum ve iştirak şirketlerinin iç kontrol sisteminin kurulması ve uygulanması esnasında mutlaka bir işbirliği ve bilgi birikimi paylaşımına da ihtiyaç vardır. Bunun yanı sıra iç kontrol sisteminin bilgi güvenliği yönetim modelinde, kontrol döngüsü olarak kullanılması ile ilgili de işbirliğinin ve etkileşimine de ihtiyaç vardır. Nasıl ki; İBB bağlı kurum ve iştirak şirketlerin Bilgi Güvenliği Yönetişim modelinde organizasyonun nasıl kurulacağına yönelik tanımlama yapılmasına ihtiyaç varsa, iç kontrol sisteminin de bu amaca yönelik yapılandırılmasına ihtiyaç vardır.

Bu kapsamda her kurumun kendi eylem planını yapması zorunluluğu getirilmiştir. Bu eylem planlarının hazırlanması esnasında, iç kontrol sistemi ile Bilgi Güvenliği Yönetişimi arasındaki etkileşimlerin de tanımlanmasına ihtiyaç vardır.

Bu döngüde iç kontrol sisteminin kullanılması, işin sadece sonuçlarını denetlemek yerine güvenliğin daha iyi bir noktaya taşınması için, her geçen gün daha da iyileştirmelerin yapılmasına da imkan tanıyacaktır.

5. SONUÇ VE ÖNERİLER

Bilgi güvenliğini sağlamak sadece Bilgi Teknoloji birimlerinin görevi değildir. Kurum ve kuruluşların bilgi güvenliğini bir bütün olarak ele alması gerekir. Güvenlik söz konusu olduğunda, özel veya resmi statüde olmaları fark etmeksizin kamu kurumlarından ve özel şirketlerden her birinin güvenlik konusunu ciddiye alması ve yönetimin bir parçası olarak değerlendirmesi gerekmektedir. Çünkü her gün daha fazla gelişen teknoloji iş üretme yöntemlerini de değiştirmekte, bu değişimin bir neticesi olarak da bilgi güvenliğinin önemini ve risklerini ön plana çıkarmaktadır. Bu sebeple özel veya resmi bütün kurumların ve şirketlerin Bilgi Güvenliği Yönetişim Modeli oluşturması ve işletmesi gerekmektedir.

Bilgi Güvenliği Yönetişim Modeli tasarlanırken, modeli tasarlayan kurum veya şirket sadece kendi organizasyonlarını dikkate alırsa, model sağlıklı çalışmayacaktır. Bu nedenle ilgili kurumun veya firmanın, çalışma alanları açısından iletişimde ve etkileşimde bulunduğu/bulunacağı kurumları ve şirketleri dikkate alarak, onlarla yapılacak iletişim ve etkileşim tasarlanan modele yansıtılmalıdır. Temelde tasarlanan Bilgi Güvenliği Stratejisi Modelinin, Solms'un önerdiği 3 katmanlı (stratejik, taktik ve operasyonel) modeli esas alması gerekir. Buna ek olarak iletişim ve etkileşimde bulunulan diğer kurum ve şirketlerin bu modeldeki yeri ve şekli tanımlanmalıdır.

Etkileşimde bulunan kurumların veya şirketlerin birbirleriyle olan bağlarına göre modeller de değişiklik gösterecektir. Bu organizasyonlar bir kuruma bağlı ise ya da bir holdinge bağlı şirketler ise, bunların birbirleri arasındaki model farklı tasarlanmalıdır. Böyle bir ilişkide bulunan şirketlerin stratejik seviyelerinin tek olarak tasarlanması gerekmektedir ve stratejik seviyede en üst düzey yöneticiler bulunmalıdır. Stratejik seviyede tüm bağlı kurum ve şirketlerin uygulayacağı Bilgi Güvenliği Stratejileri oluşturulmalıdır. Bu stratejileri girdi kabul ederek her bir bağlı kurum veya şirkette diğer seviyelerde gerekli kurallar oluşturulmalıdır. Bilgi Güvenliği Stratejileri, kurumsal stratejilerin bir parçası olmalıdır.

Şirketlerin personel sayısı, teknolojiyi kullanma miktarı ve diğer şirketlerle etkileşim oranları göz önünde bulundurularak bu tür şirketlerde taktik ve operasyonel seviye birleştirilebilir.

Bu modeller kurulurken, kurumlar arasındaki modeller ve modeller arasındaki ilişkiler de irdelenmeli ve tanımlanmalıdır. Bu kurallar her bir seviye için ve her bir etkileşimde bulunan şirket için ayrı ayrı tanımlanmalıdır.

Bilgi Güvenliği Yönetişim Modeli'nde her bir seviyedeki faaliyetlerin de kontrol edilmesi büyük önem taşımaktadır. Kontrol faaliyetlerinin sağlanabilmesi için de kuralların tanımlanması gerekmektedir. Bunun için İç Kontrol Sisteminden faydalanılabilir.

Sağlıklı çalışan bir güvenlik altyapısı için, ulusal çapta değerlendirilip bütün ilgililerin uyacağı bir ulusal bilgi güvenliği stratejisi ve stratejinin uygulanmasını sağlayacak, yasal dayanağı olan Bilgi Güvenliği Stratejisi Kurulu (BGSK) olarak da adlandırılacak bir yapıya ihtiyaç duyulmaktadır. Bilgi Güvenliği Stratejisi Kurulu'nun oluşturacağı stratejiler, her bir kurum veya şirket tarafından esas alınarak kendi organizasyonları için stratejiler oluşturulur.

Bilgi Güvenliği Stratejisi Kurulu (BGSK)'nun, Bilgi Güvenliği Yönetişim Modelini uygulayan kurumları nasıl denetleyeceği ve bunun için nasıl bir döngü kurulabileceği ile ilgili çalışma yapılabilir. Ayrıca bu modele paralel olarak ya da bu modelle bütünleşik olarak COSO ve COBIT/ITIL modellerinin nasıl bütünleşik hale getirilebileceği konusunda da bir çalışma çok faydalı olacaktır.

Son olarak, bu modelde birbirleriyle etkileşim içinde bulunan kurum ve şirketlerin, etkileşim yöntemleri ve etkileşim şekillerinin nasıl tanımlanacağı konusunda da teferruatlı bir çalışma yapılması, modelin tasarımına ve işleyişine yönelik faydalı ve gerekli bir ön çalışma olacaktır.

KAYNAKLAR DİZİNİ

- [1] Paul Williams, Andersen, Information Security Governance, Information Security Technical Report, Vol 6, No.3,2001,s60-70
- [2] International Standard ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements.
- [3] Karabacak Bilge, ISO/IEC 27001:2005 ve Bilgi Güvenliği Yönetişimi - Türkiye Analizi , <http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/iso-iec-27001-2005-ve-bilgi-guvenligi-yonetisimi-turkiye-analizi.html>, (10.02.2009)
- [4] COBIT 4.1 , IT Governance Institute, 2007
- [5] Von Solms Basie, Information security governance: COBIT or ISO 17799 or both?, Computer & Security,vol 24, 2005, s 99-104
- [6] Karabacak Bilge, Risk Analizi,
http://www.enderunix.org/docs/disabled/risk_analizi/, (10.02.2009)
- [7] Vorster Anita, Labuschagne Les, A framework for comparing different information security risk analysis methodologies, Proceedings of SAICSIT 2005, 95–103
- [8] Aktaş F.Özden, Soğukpınar İbrahim, Bilgi güvenliğinde uygun risk analizi ve yönetimi yönteminin seçimi için bir yaklaşım, Eleco, 2008
- [9] Williams Patricia A.H., In a ‘trusting’ environment, everyone is responsible for information security, Information Security Technical Report, Vol 13, 2008, s207-215 .
- [10] Von Solms Rossouw, Von Solms, S.H. Bassie, Information security governance a model based on the direct-control cycle , Computer & Security,vol 25, 2006, s 408-412.5.
- [11] Dlamini M.T., Eloff J.H.P, Eloff M.M, Information security : The moving target, Computer & Security, 2009, s 1-10
- [12] Posthumus Shaun, A framework for the governance of information security, Computer & Security,vol 23, 2004, s 638-646
- [13] Von Solms S.H.Basie, Information security governance – compliance management vs operational management, Computer & Security,vol 24, 2005, s 443-447

- [14] TÜBİTAK, TÜSSİDE, İç Kontrol Nedir,
<http://www.tusside.gov.tr/ickontrolnedir>, (10.02.2009)
- [15] Von Solms S.H. Basie, Corporate governance and information security,
Computers & Security, 2001,vol 20, s215-128
- [16] Conner F.William; Covielle Arthur W.; Information Security Governance, A
call to action; ISG, April 2004
- [17] Von Solms Rossouw, Von Solms S.H. Bassie, Information Security
Governance: Due Care, Computer & Security,vol 25, 2006, s 494-497
- [18] Poole Vernon, Why Information Security Governance is Critical to Wider
Corporate Governance Demands – a European Perspective, The ISACA Journal,
Volume 1, 2006
- [19] Von Solms S.H.Basie, Corporate Governance and Information security,
Computer & Security,vol 20, 2001, s 215-218
- [20] Moulton Rolf, Coles Robert S., Applying Information Security Governance,
Computer & Security,vol 22, 2003, s 580-584
- [21] Information Security Governance: Guidance for Boards of Directors and
Executive Management, 2nd Edition, IT Governance Institute, 2006
- [22] Karabacak Bilge, Soğukpınar İbrahim ISRAM: Information Security Risk
Analysis Method, Computers&Security 24(2), 2005, 147-159
- [23] D Wawrzyniak, Information Security Risk Assesment-The Development Of
The Standard Approaches, 5th International Scientific conference Bussiness And
Management, 2008, p.759-764
- [24] Bojanc Rok, Blazic Borka Jerman, An economic modelling approach to
information security risk management, International Journal of Information
Management, 28(2008), 413–422

ÖZGEÇMİŞ

Hakkı Tok, 1968 yılında Trabzon-Çaykara’da doğdu. İTÜ Elektrik-Elektronik Fakültesi, Elektrik Mühendisliği Bölümü'nden 1990 yılında mezun oldu. 1991-1995 yılları arasında Türk Telekom; İstanbul-Bilişim Ağları'nda Sistem Mühendisi olarak çalıştı. 1995-1998 yıllarında İstanbul Büyükşehir Belediyesi'nde Bilgi İşlem Müdürü ve Bilgi İşlem Daire Başkanı olarak görev yaptı. Yedek Subay olarak yaptığı askerlik görevinden sonra, Bilisis Bilişim Sistemleri'nde Teknik Koordinatör olarak çalıştı. 2002-2003 tarihleri arasında AYCELL’de IT Direktörlüğü yaptı. AYCELL-ARIA birleşmesinden sonra AVEA IT'de müdür olarak çalışırken, Şubat 2006 tarihinde İstanbul Büyükşehir Belediyesi Bilgi Teknolojileri Daire Başkanlığına atandı. Evli ve üç çocuk babasıdır.