# Kamu Kurumlarında Bilgi Güvenliği Yönetişimi için Bir Model

Hakkı TOK[1] İbrahim SOĞUKPINAR[2]

[1]Bilgi Teknolojileri Daire Başkanlığı, İstanbul Büyükşehir Belediyesi, İstanbul

[2]Bilgisayar Mühendisliği Bölümü, Gebze Yüksek Teknoloji Enstitüsü, Kocaeli

[1] e-posta: hakki.tok@ibb.gov.tr [2]e-posta: ispinar@bilmuh.gyte.edu.tr

## Özetçe

Kurumların ihtiyaçlarına paralel olarak; Kurumsal organizasyonların yönetim bütünlüğü nedeniyle Bilgi güvenliği yönetimi kavramının daha geniş kapsamlı olarak "Bilgi güvenliği yönetişimi" şeklinde uygulanması yaygınlaşmaktadır. Sonuçta kurumların işleyişine uygun Bilgi güvenliği yönetişim modelinin kurulması önemli hale gelmiştir. Bu çalışmada Türkiye için kamu kurum ve kuruluşlarında kullanılacak yeni Bilgi güvenliği yönetişimi modeli önerilmiştir. Ayrıca modelin tek bir kurum ya da kuruluşta kullanılması için tasarlanmasının yeterli olmayacağından hareketle önerilen modelde kurum ve kuruluşların birbirleriyle etkileşimini de içeren yeni bir yapı ortaya konulmuştur. Ayrıca tüm bu sistemin işleyebilmesi için tüm Kamu Kurum ve Kuruluşları ile birlikte özel şirketleri de içeren bir Bilgi Güvenliği Stratejisi Kurulu (BGSK)'nun kurulmasının gerekliliğine vurgu yapılmıştır. Önerilen model örnek bir kurum için uygulaması verilmiştir.

## Summary

The model of Information Security Governance proposed by Solms is discussed in this article and a new model based on the Solms's model is proposed to use in public sector and government entity. First of 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.

## 1. Giriş

Yönetişim kavramı farklı alanlarda sıkça kullanılan ve gittikçe önemi artan bir eğilim haline gelmiştir. Bilgi Güvenliği Yönetişimi, Bilgi Teknolojileri Yönetişimi kapsamında Kurumsal Yönetişim ile birlikte düşünülmesi gereken bir olgu haline gelmiştir. Bilgi artık kurumların ve şirketlerin en önemli varlıklarından biridir ve kıymeti gittikçe artmaya devam etmektedir.Tepe Yöneticinin bilgi güvenliği ile ilgili kararların alması ve bu kararların uygulanması aşamalarını yakından takip etmesi şarttır. Bu konudaki yetki ve sorumluluğun uygun paylaşımı da yönetişime anlam kazandırır.

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. [2]

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. [1] 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. Ancak kurumların kendi aralarında ve bağlı kurum, kuruluşlarla olan etkileşimlerininde 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 bütününün 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)'nun kurulmasının gerekliliğine ve yasal düzenlemelerin yapılması vurgulanmıştır.

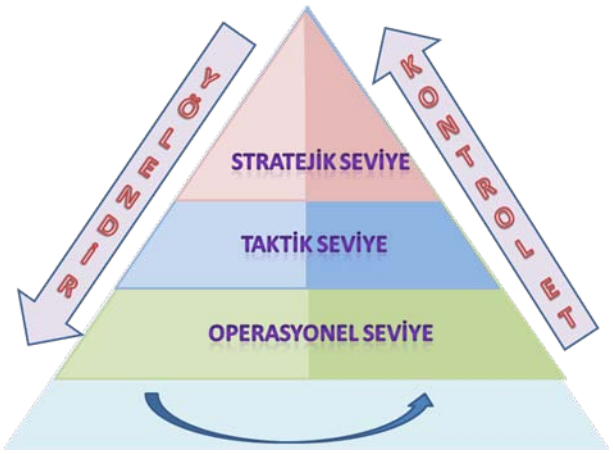
## 2. Bilgi Güvenliği Yönetişimi ve ilgili çalışmalar

Dlamini ve diğerleri, 'Bilgi Güvenliği: hareketli hedef' makalesinde bilgi güvenliğinin dünü, bugünü ve geleceği hakkında bilgi vermişlerdir. Bu makalede bilgi güvenliğinin geleceğinin stratejik yönetişim seviyesine çıkarılmasını önermişlerdir. [3] Posthumus ve R. Solms, bilgi güvenliği ile kurumsal yönetişimin bilgi güvenliği yönetişim çerçevesi aracılığıyla birleştirilmesini önermişlerdir. Bilgi güvenliğinin sadece teknik bir konu değil, stratejik ve yasal bir konu

olduğunu vurgulamışlardır. Bilgi güvenliği yönetişim çerçevesi yönetişim ve yönetim olarak ikiye ayrılmıştır. Yönetişim 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 yönetişim çerçevesine göre görevlerini uygulamaları gerektiği belirtilmiştir. Yönetişim boyutu strateji, misyon ve vizyondan sorumlu iken yönetim tarafı politikaların uygulanmasından sorumludur. [4]. B. Solms, bilgi güvenliği yönetişimi 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 yönetişim çerçevesi oluşturmakta faydalı olacağını belirtmiştir. [5] Yine B. Solms, bilgi güvenliğinin bilgi güvenliği operasyonel yönetimi ve bilgi güvenliği uygunluk yönetimi adlı iki boyutundan söz etmektedir. [6] 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. [6] R. Solms ve B. Solms, bilgi güvenliği yönetişim 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. [1]

Makaledeki Solms'un modeli [1] ***"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 seviye de alt seviye yöneticileri yer almaktadır. Bu yönetim kademelerinde "yönlendir" ve "kontrol et" aktiviteleri aşağıdaki şekilde işler:

En üst seviyede yönlendir aşamasında, bilgi güvenliği ile ilgili direktifler (stratejiler) belirlenir, söz konusu stratejiler bir alt seviyedeki yönetim tabakasına girdi olarak verilir. Taktik seviyede söz konusu direktifler politika ve kurumsal standart haline getirilir. Alt seviyedeki yöneticiler ise bu politika ve standartlara göre prosedürleri hazırlarlar. Bilgi güvenliği faaliyetleri hazırlanmış olan prosedürlere göre gerçekleştirilir. Kontrol etme aşamasında ise operasyonel seviyede işlemlerin prosedürlere göre yapılıp yapılmadığı alt seviye yöneticiler tarafından kontrol edilir. Taktik seviyede, bir alt seviyedeki prosedürlerin politika ve standartlara uyumluluğu orta seviye yönetim tarafından kontrol edilir. Stratejik seviyede ise ilgili direktiflerin ne derece yerine getirildiği ve politikaların stratejilerle uyumu üst düzey yönetici tarafından kontrol edilir. [7] Bu şekilde bir döngü sağlanmış olur




*Şekil 1*: Solms'un Bilgi Güvenliği Yönetişim modeli [1].

## 3. Kamuda Yönlendir ve Kontrol Et Modeli

### 3.1. Tek Kurumda Bilgi Güvenliği Yönetişim Modeli

Solms'un modelinin yönetişimin 3 farklı seviyeden oluşması gerekliliğini önerdiğini yukarda belirtilmiştir. Bunlar stratejik seviye, taktik seviye 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 startejik 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, prensipler ve yönetimsel prosedürlere*

dönüştürülür. Tüm bunlar ***"Yönlendir"*** işlemleri olarak adlandırılır.


*Şekil 2*: Kamu Kurumu Bilgi Güvenliği Yönetişim modeli.

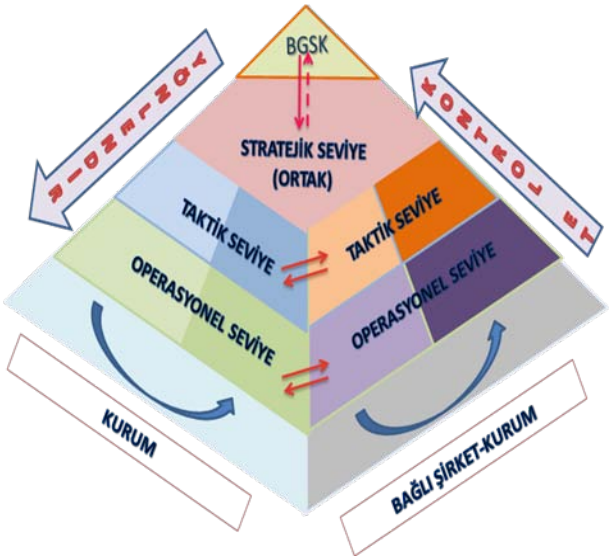
Bu faaliyetlerin sıkı şekilde gözetlenmesi, izlenmesi ve kontrol edilmesi zorunluluğu vardır. Bu nedenle; direktif, standart ve politikaların ne derece uygulandığının ölçülebilmesi gerekir. Bunun için ölçme yöntemlerinin de tanımlanması gerekir. *Kontrol et* işlemine *operasyonel seviyeden* başlanır. Bu seviyede ölçmek için çeşitli kaynaklardan elde edilmiş veriler kullanılır. Bunlar; mümkün ise bilgi sistemlerinden alınabilecek raporlama verileri ve özel yazılımlardan elde edilecek veriler veya 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 iletilmek 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 yönetişim 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*: Kurum ve Bağlı-Kurum-Kuruluş-Şirket Bilgi Güvenliği Yönetişim modeli

### 3.3. Kurumların Birbirleri Arasında Bilgi Güvenliği Yönetişim Modeli

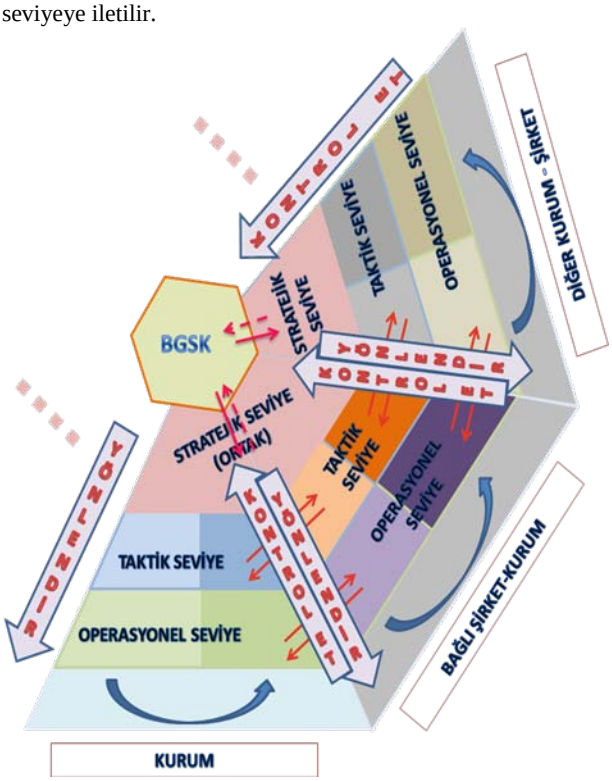
Her kamu kuruluşu kendi *Bilgi Güvenliği Yönetişim Modeli'ni* bölüm 3.4 de belirtilen BGSK'nın kriterleri çerçevesinde kurması gerekmektedir. Stratejik seviyede bir kurumun başka bir kurumla ilişki kurması öngörülmemiştir. Ancak ilgili kurumların birbirleriyle taktik seviyede ve operasyonel seviyede 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.

### 3.4. Entegre Bilgi Güvenliği Yönetişim Modeli

Bilgi güvenliği yönetişiminde olabilecek zaafiyetler, özel ve /veya kamu kurumlarının birbirleriyle etkileşimleri nedeniyle kurumların hepsinde etkili olabilecektir. Bu nedenle, bilgi güvenliği yönetişim modelinin ve uygulamasının kurumlar arası 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 adlandırılabilinir. 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 4*'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.

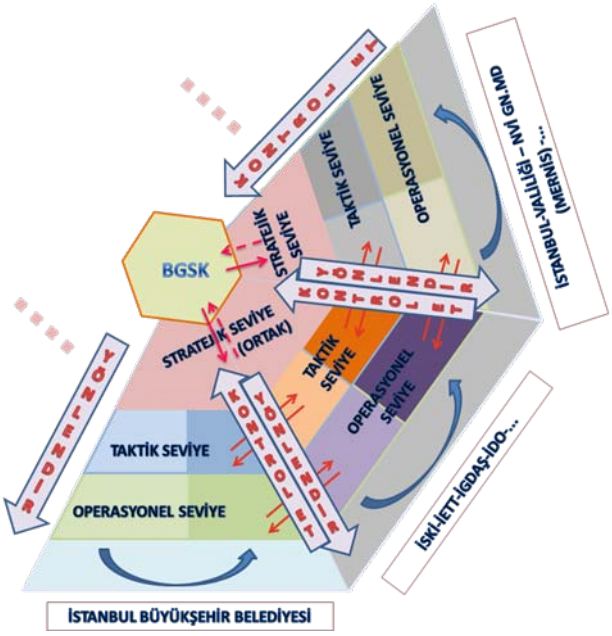



*Şekil 4*: Entegre Bilgi Güvenliği Yönetişim Modeli.

## 4. Örnek Bir Tasarım

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, KİPTAŞ, 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 yardımcıları, daire başkanları, müdürler ve şeflerden oluşmaktadır. Şirketlerin yönetimi ise, şirketin büyüklüğüne göre genel müdür, genel müdür yardımcıları, müdürler ve şeflerden, ya da genel müdür, müdür ve şeflerden oluşmaktadır.

Bilgi Güvenliği Yönetişim Modeli oluşturulurken İBB ve bağlı tüm kuruluşların *tek bir* ***stratejik seviyesi*** olmalıdır. Bu seviyede İBB ve bağlı kuruluşların üst seviye yöneticileri olmalıdır. Bunlar İBB Genel Sekreteri, Bilgi Teknolojileri Daire Başkanın bağlı bulunduğu Genel Sekreter Yardımcısı, Stratejik Planlama Daire Başkanı, Bilgi Teknolojileri Daire Başkanı, İştirakler Daire Başkanı, bağlı kurumların genel müdürleri ve belli büyüklükteki bağlı şirketlerin genel müdürlerinden oluşmalıdır. Burada oluşturulacak stratejiler her bir organizasyonun stratejik planının bir parçası olmalıdır. Burada stratejiler oluşturulup taktik seviyeye iletilmelidir.




*Şekil 5*: İstanbul Büyükşehir Belediyesi için Bilgi Güvenliği Yönetişim Modeli.

Her bir organizasyonun ***taktik seviyesi*** farklı olmalıdır. İBB ve bağlı kurumlarda (İSKİ, İETT) taktik seviyedeki yöneticiler; Bilgi Teknolojileri Daire Başkanı, Bilgi İşlem Müdürü, Elektronik Sistemler Müdürü, Coğrafi Bilgi Sistemi Müdürü, Stratejik Planlama Müdürü, İç-Kontrolden 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 ve ilgili müdürlerden oluşmalıdır. Bu seviyede, stratejik seviyede oluşturulan stratejilere uygun doküman ve direktifler oluşturulur ve operasyonel seviyeye iletilir. Bunlar oluşturulurken Bilgi Güvenliği Yönetim Sistemi (BGYS)'den faydalanılır.

***Operasyonel seviye*** de her bir kurum için ayrı olmalıdır. 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.

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 kurumlarda 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 Müdürlüğünün 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 loglanacağının 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, olay kayıtlamanın düzgün yapılıp yapılmadığı, uygulamayı kullanan kişilerin şifrelerini paylaşıp 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 geribildirimlerde bulunması da mümkün olabilecektir.

## 5. Sonuç ve Öneriler

Bilgi güvenliğini sağlamak sadece Bilgi Teknoloji birimlerinin görevi değildir. Kurum ve kuruluşların bilgi güvenliğini bir bütün olarak ele alması gerekir. Bunun için her kurum ve kuruluşun bir Bilgi Güvenliği Yönetişim modeli kurması ve işletmesi zorunluluğu vardır. Bu modeller kurulurken, kurumlar arasındaki modeller arasındaki ilişkiler de irdelenmeli ve tanımlanmalıdır. Sağlıklı çalışan bir güvenlik altyapısı için, ulusal çapta değerlendirilip bütün ilgililerin uyacağı bir ulusal bilgi güvenliği stratejisi ve stratejiyi uygulatacak yasal dayanağı olan Bilgi Güvenliği Stratejisi Kurulu (BGSK) olarak da adlandırılabilecek bir yapıya ihtiyaç vardır. Bu kurulun, Bilgi Güvenliği Yönetişim Modelini uygulayan kurumları nasıl denetleyeceği ve bunun için nasıl bir döngü kurulabileceği ile ilgili çalışma yapılabilir.

## 6. Kaynakça


[1] Von Solms, Rossouw ve, 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.

[2] Williams, Patricia A.H., In a 'trusting' environment, everyone is responsible for information security, *Information Security Technical Report*, Vol 13, 2008, s207-215 .

[3] Dlamini, M.T., Eloff, J.H.P, Eloff, M.M, Information security : The moving target, *Computer & Security, 2009, s 1-10*

[4] Posthumus, Shaun, A framework for the governance of information security, *Computer & Security,vol 23*, 2004, s 638-646

[5] Von Solms, Basie, Information security governance: COBIT or ISO 17799 or both?, *Computer & Security,vol 24*, 2005, s 99-104

[6] Von Solms, S.H.Basie, Information security governance – compliance management vs operational management, *Computer & Security,vol 24*, 2005, s 443-447

[7] http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/iso-iec-27001-2005-ve-bilgi-guvenligi-yonetisimi-turkiye-analizi.html

[8] Von Solms, S.H. Basie, Corporate governance and information security, *Computers & Security, 2001,vol 20, s215-128*