

# Kurumlarda Bilgi Güvenliği Yönetim Sistemi'nin Uygulanması

**Mehtap ÇETİNKAYA**

İstanbul Kültür Üniversitesi, Bilgisayar Mühendisliği Yüksek Lisans Bölümü, İstanbul  
mehtapcetinkaya@gmail.com

**Özet:** Bu bildiri, Bilgi Güvenliği Yönetim Sistemleri'nin (BGYS) uygulandığı şirketlerdeki çalışmalarını konu almaktadır. ISO/IEC 27001:2005 standartına uygun olarak dokümanite edilmiş bir BGYS için gerekli faaliyetlerin neler olduğu, nasıl uygulandığı, uygulamalar sırasında karşılaşılan sorunlar ve iş sürekliliğinin sağlanmasında izlenen yöntemlerin, mümkün olduğunca açık şekilde anlatılması kurumlara ve bilgi güvenliğiyle ilgili çalışanlara yardımcı olacaktır.

Bildiride, birinci ve ikinci bölümlerde, Bilgi Güvenliği Yönetim Sistemi ve bu konuda geliştirilen ISO 27001 standartının içeriği anlatılmaktadır. Üçüncü bölümde, ISO 27001 standardı uygulamak isteyen şirketlerde uygulamaya başlamadan önce ve sonraki yapılan çalışmalar anlatılmaktadır. Son bölümde ise, yönetim sistemi kurulmuş olsa bile güvenliğin ve iş devamını sağlamak üzere geliştirilen iş sürekliliği planlarına yer verilmektedir.

**Anahtar Kelimeler:** Bilgi güvenliği, bilgi güvenliği yönetim sistemi, BGYS ISO/IEC 27001:2005

## 1. Giriş

İnternet ve kişisel bilgisayarların kullanımı, 1990'lardan itibaren yaygınlaşmaya başlamıştır. 1990'lardan önce bilgi kâğıt parçası halinde yer alıp, dolaplarda saklanabiliyorken, sonrasında bilgisayar ortamında yer almaya ve çok kolay el değiştirmeye başlamıştır.

Özellikle internet kullanımının hayatın her alanına yayılması göz önüne alındığında, bilgi, küreselleşen iş dünyasının en ciddi rekabet silahı haline gelmiştir. Firmalar kuruluşundan itibaren geçen süre içinde, faaliyet gösterdiği alana ait en özelleşmiş ve uzmanlaşmış bilgileri depolamakta olduğundan, zaman içinde kurumsal yapı taşlarına dönüşen depo edilmiş bu kaynakların erişilebilir ve kullanılabilir olması da giderek vazgeçilmez olmaktadır.

Günümüzde, sadece çalışanlarıyla değil, müşterileri, iş ortakları ve hissedarlarıyla birlikte tanımlanan kurumlarda, bilginin korunmasına

ve gizliliğine ilişkin güven ortamının yaratılması stratejik bir önem taşımaktadır. Yaşanan güvenlik sorunları, iş devamlılığını engellemenin yanı sıra, kurumların; pazar kaybına, müşteriler, iş ortakları ve hissedarlar karşısında güven yitirmesine neden olmaktadır. Bunların geri kazanılması, bunların yitirilmemesi için alınacak önlemlerden her zaman daha pahalıdır.

Bilgi güvenliği; iş devamlılığı, kaçınılmaz felaket durumlarında kaybın en aza indirilmesi, firmaların yapı taşları sayılan kaynakların her koşulda gizliliğinin, ulaşılabilirliğinin ve bütünlüğünün korunması amaçlarını taşır.

Bu amaçları uygulamaya yönelik, ISO 27001 standardı, ülkelere göre özel tanımlar içermeyen, genel tanımların bulunduğu uluslararası bir standarttır.

ISO 27001 Bilgi Güvenliği Yönetim Sistemine sahip olmak, kurumların yüzde yüz gü-

venlik seviyesine sahip olduklarını söylemesi anlamına gelmez. Zaten, yüzde yüz güvenlik seviyesine ulaşmak mümkün değildir.

Nasıl ki ISO 9001 Toplam Kalite Yönetimi uygulanan bir kurum, dünyanın en kaliteli ürününü ya da hizmetini ürettiğini değil, ne kalitede ürün üreteceğini bilerek, takibini yazılı süreçleriyle yapan ve bu sayede ürettiği her ürünün ya da hizmetin özelliğinin birbiriyle aynı olmasını sağlaması ve söz verdiği şekilde ve kalitede ürün veya hizmet üretiyorsa, kurumun ISO 27001 sertifikasına sahip olması da, kurumun güvenlik risklerini bildiği anlamına gelir. Kurum herhangi bir saldırıya uğramaya çağı, hack edilmeyeceğini ya da bir başkasının bilgisayarlarını çalmayacağını söylemez ve garanti edemez. Ancak, kurumun riskleri bildiği, yönettiği, belli risklerde ortadan kaldırmak çok pahalıysa bunu kabul ettiğini söyler.

Herhangi bir kuruluşun başarısı ve sürekliliği için etkin bir risk yönetimi prosesinin işliyor olması hayati önem taşımaktadır. Kurumsal değerlerin korunması ve verimliliğin sağlanabilmesi; yapılan yatırımların ve hedeflere uygunluğunun denetimini ve gerekli kontrollerin kurum içine yerleştirilerek uygulanmasını gerektirir.

ISO 27001 Kurumların risk yönetimi ve risk işleme planlarını, görev ve sorumlulukları, iş devamlılığı planlarını, acil durum olay yönetimi prosedürleri hazırlamasını ve uygulamada bunların kayıtlarını tutmasını gerektirir. Kurum tüm bu faaliyetlerin de içinde yer aldığı bir bilgi güvenliği politikası yayınlamalı ve personelinin bilgi güvenliği ve tehditler hakkında bilinçlendirmelidir. Seçilen kontrol hedeflerinin ölçülmesi ve kontrollerin amacına uygunluğunun ve performansının sürekli takip edildiği yaşayan bir süreç olarak bilgi güvenliği yönetimi ancak yönetimin aktif desteği ve personelin katılımıyla başarılabilir.

## 2. ISO 27001

İngilizler tarafından hazırlanan ve 1998'den beri var olan BS 7799 adındaki ilk standart uluslararası bir standart niteliğinde değildi. ISO 17799 Standartı ise Bilgi Güvenliği'nin nasıl yapılırsa daha iyi olabileceğine yönelikti. Kurumların, kendilerini sertifikalandırabilecekleri bir standart değildi. Eski adıyla BS 7799 yeni adıyla 27001 tam ve uluslararası bir standart olarak yer almıştır.

ISO 27001 süreçlerinin güvenliğini sağlamayı hedefleyen bir bilgi güvenliği standarttır. İşin içinde sadece bilgisayar, bilişim güvenliği yoktur. Bunların yanında, kâğıttaki dokümanların güvenliği, her tür sürecin güvenliğinde kapsar.

Bu standart, bir Bilgi Güvenliği Yönetim Sistemi'ni (BGYS) kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model sağlamak üzere hazırlanmıştır.

Bilgi Güvenliği Yönetim Sistemi (BGYS) standardı, tüm kuruluş türlerini (örneğin, ticari kuruluşlar, kamu kurumları, kar amaçlı olmayan kuruluşlar) kapsar. Bu standart, doküman- te edilmiş bir BGYS'yi kuruluşun tüm ticari riskleri bağlamında kurmak, gerçekleştirmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için gereksinimleri kapsar. Bağımsız kuruluşların ya da tarafların ihtiyaçlarına göre özelleştirilmiş güvenlik kontrollerinin gerçekleştirilmesi için gereksinimleri belirtir.

BGYS, bilgi varlıklarını koruyan ve ilgili taraflara güven veren yeterli ve orantılı güvenlik kontrollerini sağlamak için tasarlanmıştır.

### 3.Bilgi Güvenliđi Yönetim Sistemi Kurmak

ISO 27001 dünya üzerinde geçerliliđi olan ve gitgide birçok alanda zorunlu hale getirilmeye çalışılan bir standarttır. Bu standart, kurumlara genel anlamda bilgi güvenliđini nasıl yapabileceklerini anlatmaktadır.

ISO 27001 standardını uygulayan ve sertifikasını alan bir şirketin, dünyanın güvenliđi en yüksek firması olması gerekmez. Ancak güvenliđin ne seviyede olduđu o kurumun yöneticileri tarafından bilinir ve onların kararı ölçüsünde ortaya konmuş durumda olup zaman içinde artan bir güvenlik seviyesi vardır.

Özellikle, elektronik imza servis sağlayıcıları, bankalar, hastaneler, sigorta şirketleri, e-ticaret ile uğraşan şirketlerde BGYS'nin uygulanması önemli bir ihtiyaçtır.

Bilgi Güvenliđi Yönetim Sistemi'ni uygulamak isteyen bir kurumda yapılması gereken adımlar aşağıdaki şekildedir:

• **Proje Ekibinin Kurulması:** BGYS Projesi çalışmalarını düzenleyecek, uygulayacak ve yönetebilecek bir takım oluşturulmalıdır. Kurum içerisinde bu çalışmaları yürütecek BGYS takımının ve BGYS yöneticisinin bilgi güvenliđi yönetimi konusunda iyi eğitilmiş olmaları gerekmektedir. Risk yönetimi, politika oluşturma, güvenlik prosedürlerinin hazırlanması ve uygun kontrollerin seçilerek uygulanması aşamalarında uzman desteđi ve danışmanlık almaları faydalı olacaktır. Böylece BGYS'yi en iyi nasıl uygulayacağı konusunda bağımsız danışmanlardan görüş ve tavsiye alabilir.

• **Kurum içinde stratejinin belirlenmesi:** Üst yönetimle birlikte organizasyonel strateji hazırlanmalıdır.

• **Kapsamın Belirlenmesi:** BGYS'nin kurum içinde uygulanacak ve belgelendirilecek kap-

sam belirlenmeli. Hangi departmanlarda bu sistemin uygulanacağı planlanarak yazılı ve görsel kapsam dokümanları hazırlanmalıdır.

• **Proje ve İletişim Planının Hazırlanması:** Kurum ön proje hazırlıklarını tamamlayıp, proje takımını, kapsamını, stratejisini, danışmanlarını belirledikten sonra artık projede ilerleyeceği adımlar için bir proje planı hazırlanmalıdır. Nelerin, ne zaman, kimlerle uygulanacağı proje planında yer alarak çalışmalara başlanır. Yapılan tüm çalışmalar, toplantılar çeşitli rapor ve tutanaklarla kayıt altında tutulurken yine kurum tarafından belirlenen aralıklarda (haftalık, aylık) ilgili yönetimle bilgilendirme ve görüş alışverişi yapılır.

• **Bilgi Güvenliđi Politikası:** Projeye başlanmasıyla birlikte, öncelikle ilgili kapsam ve yönetim çalışanlarıyla birlikte, standartin gerektirdiđi kişi ve birimlerin (hukuk, vs..) görüşleri alınarak Bilgi Güvenliđi Politikası yazılarak, yönetim tarafından onaylanıp, kurum çalışanlarına duyurulur.

Bilgi Güvenliđi Politikaları, tüm kurum çalışanlarının görev ve sorumluluklarını tanımlamaktadırlar. Hedef; bilgi güvenliđi konusunda yönetimin bakış açısını, onayını ve desteđini çalışanlara uygun araç ve denetim mekanizmaları eşliğinde iletmektir, amaç ise; Bilgi Güvenliđi hakkında üst yönetimin isteklerini ve kararlarının tüm çalışanlarla paylaşan politika dokümanlarının hazırlanmasıdır.

• **Varlıkların Belirlenmesi:** Varlık Yönetimi için, kapsam dahilinde ve kapsama destek veren birimlere yönelik varlıklarla ilgili prosedür, varlık kayıt tablosu gibi dokümanlar hazırlanır. İlgili varlıklar varlık sahipleri tarafından belirtilerek, kayıt altına alınır. Varlıklar, sınıflandırılıp, gizlilik, bütünlük ve kullanılabilirlik kriterlerine göre değerlendirilir.

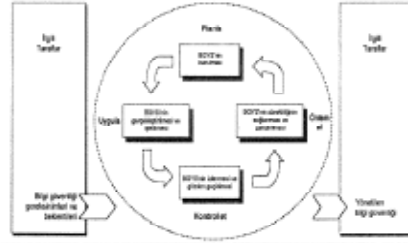
• **Risklerin Belirlenmesi, Risk Yönetimi:** Yapılan yatırımlarda amaç hep en yüksek sonucun alınmasıdır. Risk Analizi, bilgi güvenliğine yapılacak yatırımların öncelikli konulara yönltilmesi için gerçekleştirilir.

Risk Analiz hizmeti sırasında önce bilgi varlıklarının envanteri çıkartılır, yapılan özel bir elemenin ardından tehditler, zayıf noktalar ve bunlara karşılık gelen riskler belirlenir. Risklerin sıralanmasının ardından, öncelikli riskler belirlenir ve alınması gereken önlemlere karar verilir. Amaç, risklerin tanımlanması, gerekli tedbirlerin alınmasını ön plana çıkaran bir risk analizi prosesini başlatmaktır.

Bu çalışmalar sırasında oluşturulan risklerin izlenmesi ve ölçülmesi ile ilgili teknikler, alınacak önlemlerin yeterliliğini denetlemek için anahtar görev görmektedir.

Yapılan Risk Analizini gerçekçi kılan en önemli faktör ise, bu çalışmanın her aşamasında fayda/maliyet dengesini gözetmek ve bu konuda yapılacak optimizasyondur. Adım, varlıkların belirlenmesiyle birlikte standartında oluşturulması ve uygulanmasındaki en önemli nedenlerden biri olan Risk Yönetiminin uygulanmasıdır. Bilgi Güvenliği Yönetim Sistemi, kurumunuzdaki tüm bilgi varlıklarının değerlendirilmesi ve bu varlıkların sahip oldukları zayıflıkları ve karşı karşıya oldukları tehditleri göz önüne alan bir risk analizi yapılmasını gerektirir. Kurum kendine bir risk yönetimi metodu seçmeli ve risk işleme için bir plan hazırlamalıdır.

Risk işleme için standartta öngörülen kontrol hedefleri ve kontrollerden seçimler yapılmalı ve uygulanmalıdır. Planla-uygula-kontrol-önlem al (PUKÖ) çevrimi uyarınca risk yönetimi faaliyetlerini yürütmeli ve varlığın risk seviyesi kabul edilebilir bir seviyeye getirilene kadar çalışmayı sürdürmelidir.



Şekil 1- BGYS Proseslerine uygulanan PUKÖ Modeli

Şekil 1 - BGYS proseslerine uygulanan PUKÖ modeli

<b>Planla (BGYS'in kurulması)</b>	Sonuçları kuruluşun genel politikaları ve amaçlarına göre değerlendiren yönetimi ve bilgi güvenliğinin geliştirilmesine bağlı BGYS politikası, amaçlar, hedefler, prosedürler ve prosedürlerin kurulması
<b>Uygula (BGYS'in gerçekleştirilmesi ve iyileştirilmesi)</b>	BGYS politikası, kontroler, prosedürler ve prosedürlerin perçende işlenmesi
<b>Kontrol Et (BGYS'in izlenmesi ve gözden geçirilmesi)</b>	BGYS politikası, amaçlar ve kullanım denetimlerine göre prosedür performansının değerlendirilmesi ve uygulanabilir yerlerde ölç sonuçlarının gözden geçirilmesi üzere yönltilme rapor edilmesi
<b>Önlem al (BGYS'in sürekliliğinin sağlanması ve)</b>	BGYS'in sürekli iyileştirilmesi sağlamak için yönetimi geliştirme sonuçlarına dayalı olarak düzenli ve birciklikli

## BGYS Proseslerine uygulanan PUKÖ Modeli Açıklamaları

### • Değişim Yönetimi:

Bilgi işleme olanakları ve sistemlerinde olan değişiklikler kontrol edilmeli, değişimle ilgili prosedür ve diğer dokümanlar hazırlanmalıdır. Rol ve Sorumluluklar ile ilgili hazırlanan dokümanda kurumdaki değişim yöneticisinin kim olduğu belirtilmelidir.

### • Olay Yönetimi:

Güvenlik olaylarını anında saptayabilme ve güvenlik ihlal olaylarına hemen yanıt verebilmek için olay yönetimine yönelik planlar, prosedür ve diğer dokümanlar hazırlanmalıdır. Rol ve Sorumluluklar ile ilgili hazırlanan dokümanda kurumdaki olay yöneticisinin kim olduğu belirtilmelidir.

### • Uygulanabilirlik Bildirgesi

Uygulanabilirlik Bildirgesi risk işlemeyi ilgilendiren kararların bir özetini sağlar. Standarttaki seçilen kontrol amaçları ve kontroller ve bunların seçilme nedenleri, mevcut gerçekleştirilmiş kontrol amaçları ve kontroller ile standart Ek A'da ki kontrol amaçları ve kontrollerden herhangi birinin dışarıda bırakılması ve bunların dışarıda bırakılmasının açıklaması, uygulanabilirlik bildirgesinde ele alınır. Uygulanabilirlik bildirgesinin ardından, kurumdaki yapılacak bazı işlemlerle ilgili ilgili bölümlerle yapılacağına dair mutabakat zaıtları hazırlanır.

### • Döküman ve Kayıt Yönetimi:

Belirtilen politikalara bağılı olarak tüm şirket standart, kural ve prosedürleri gözden geçirilir ve bunun şirket içi işleyişe nasıl yansıtacağı belirlenir. Hizmet, güvenlik ile ilgili prosedürlerin geliştirilmesi ve dokümanite edilmesi ile tamamlanır. Politika, prosedür, talimatlar ve ilgili formlar hazırlanır. Dokümanlarda belirtilen şartlara göre hareket etmeyecek ve istisna durumların olduğı kullanıcılar için, bu kuralların dışında kullanacağı ve bununla ilgili riskleri kabul ettiğı, yönetici onayını alacağı, istisna ile ilgili dokümanlar hazırlanır. Kayıtlara yönelik doküman ve prosedürler hazırlanarak, kayıtlar tutulur.

### • Eğitim ve Farkındalık Çalışmaları

Bir bilgi güvenliği sistemi kurulurken ve kurulduktan sonra, bunla ilgili tüm çalışanlarını, şirketine düzenli olarak dışarıdan gelip giden ama şirketinin bordrosunda yer almayabilir kontratla çalıştırdığın kişilerde dâhil olmak üzere bilgilendirme ve farkındalık eğitimi verir. Politika, prosedür ve ilgili diğere dokümanları duyurur. Kapsam dâhilinde, varlıkları listeleyip, sınıflandıracak kişilere bunları nasıl yapacaklarına yönelik eğitimler verir. Ve ku-

rumda bilgi güvenliğinin bir yaşam tarzı olması gerektiğini, kurum kültürüne yerleşmesi ve benimsenmesi için çalışmalar yapar.

### • İç denetim

Kuruluş BGYS iç denetimlerini, BGYS kontrol amaçlarının, kontrollerinin, proseslerinin ve prosedürlerinin standarta göre gerçekleştirip gerçekleştirmediğini belirlemek için planlanan aralıklarda gerçekleştirilmiştir:

### • Yönetimin Gözen Geçirme

Yönetim tarafından BGYS denetimleri be gözden geçirmelerinin sonuçları, ilgili taraflardan edinilen geribildirimler alınarak sistem gözden geçirilmelidir. Yönetim, kuruluşun BGYS'sini planlanan aralıklarla (en az yılda bir kez), sürekli uygunluğunu, doğruluğunu ve etkinliğini sağlamak için gözden geçirmelidir. Bu gözden geçirme, bilgi güvenliği politikası ve bilgi güvenliği amaçları dâhil BGYS'nin iyileştirilmesi ve gereken değişikliklerin yapılması için fırsatların değerlendirilmesini içermelidir. Gözden geçirme sonuçları açıkça dokümanite edilmeli ve kayıtlar tutulup saklanmalıdır.

### • Düzenleyici Önleyici Faaliyetler (DÖFİ)

Kuruluş tekrar ortaya çıkmalarını önlemek için, BGYS şartlarıyla olası uygunsuzlukların nedenlerini gidermek üzere alınacak önlemleri belirlemelidir. Gerçekleştirilen düzeltici, önleyici faaliyetler, olası sorunların yapacağı etkiye uygun olmalıdır. Önleyici faaliyetler için dokümanite edilmiş prosedürler bulunmalıdır.

### • Belgelendirme

Belgelendirme tetkiki seçilen belgelendirme kurumu tarafından yapılacaktır. Bu noktada, belgelendirme kurumu BGYS'nizi gözden geçirecek ve belgelendirme için önerilip önerilemeyeceğinizi tespit edecektir.

Piyasada faaliyet gösteren birçok belgelendirme kurumu olmasından dolayı bir tanesinin seçilmesi oldukça zor bir konu olabilir. Göz önünde bulundurulması gereken faktörler arasında endüstriyel deneyim, coğrafik kapsam, fiyat ve sunulan hizmet kalitesi yer almaktadır. Anahtar önem taşıyan husus, sizin gerekliliklerinize en iyi yanıt verecek belgelendirme kurumunu bulmaktır.

#### 4. İş Sürekliliđi

Kurumlar her durumda ayakta kalmak için zorluklarla baş etmek zorundadırlar. Bir kurum için İş Devamlılıđı yapısını kurmak, kritik iş fonksiyonlarının her durumda çalışabilirliğini sağlamak anlamına gelir.

Organizasyonların bilgi ve süreçlerine yönelik güvenlik tehditleri, günümüzde rekabet şansı, iş kalitesi ve verimliliğine yönelik tehditler haline almıştır. Kritik iş fonksiyonlarının devamlılıđı için gerekli altyapı; teknoloji ve insan unsurlarından oluşur. Bu unsurların iş devamlılıđını sağlamak için yeterli kaliteye sahip hale getirilmesi kadar, en kötü durum senaryoları düşünülerek alternatif devamlılık yatırımlarının belirlenmesi gerekir.

#### 5. Başarı Faktörleri

- İş hedefini yansıtan güvenlik politikası,
- Uygulama yaklaşımının şirket kültürü ile tutarlı olması
- Yönetimin görülür desteđi ve bađlılıđı
- Güvenlik gereksinimlerinin, risk değerlendirmesinin ve risk yönetiminin iyi anlaşılması
- Güvenliđin tüm yöneticilere ve çalışanlara etkili bir biçimde pazarlanması
- Bilgi güvenliđi politikası ve standartları ile ilgili kılavuzların tüm çalışanlara ve sözleşmelilere dağıtılması
- Uygun eğitim ve öğretimin sağlanması

- Bilgi güvenliđi yönetimi performansının ve iyileştirme için geri bildirimlerle sunulan önerileri değerlendirilmek için kullanılan kapsamlı ve dengeli bir ölçüm sistemi

#### 6. Bilgi Güvenliđi Yönetim Sistemi Kurmanın Yararları:

- Bilgi varlıklarının farkına varma: Kuruluş hangi bilgi varlıklarının olduğunu, değerinin farkına varır.
- Sahip olduđu varlıkları koruyabilme: Kuracağı kontroller ile koruma metodlarını belirler ve uygulayarak korur.
- İş sürekliliđi: Uzun yıllar boyunca işini garanti eder. Ayrıca bir felaket halinde, işe devam etme yeterliliđine sahip olur.
- İlgili taraflar ile barış halinde olma: Başta tedarikçileri olmak üzere, bilgileri korunaçağından ilgili tarafların güvenini kazanır.
- Bilgiyi bir sistem sayesinde korur, tesadüfe bırakmaz.
- Müşterileri değerlendirirse, rakiplerine göre daha iyi değerlendirilir.
- Çalışanların motivasyonunu artırır.
- Yasal takipleri önler
- Yüksek prestij sağlar

#### 7. Kısaltmalar

**BGYS:** Bilgi Güvenliđi Yönetim Sistemi

**TSE:** Türk Standartları Enstitüsü

**IEC:** Uluslar arası Elektroteknik Komisyonu

**ISO:** Uluslararası Standard Organizasyonu

#### 8. Kaynaklar

- Lostar Bilgi Güvenliđi A.Ş. ( <http://www.lostar.com/tr/> Murat Lostar)
- <http://www.tse.org.tr/>
- TS ISO/IEC 27001 Bilgi Teknolojisi Güvenlik Teknikleri – Bilgi Güvenliđi Yönetim Sistemleri Şartlar
- <http://www.sans.org/>