TBD Kamu-BİB

Kamu Bilişim Platformu X

Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin Uygulanmasında

İSO/IEC 27001:2005

Bilişim Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler standardı

Sürüm 1.0

1. ÇALIŞMA GRUBU

Nisan 2008

TBD Kamu-BİB

Kamu Bilişim Platformu X

Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin Uygulanmasında

ISO/IEC 27001:2005 - Bilişim Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler standardı

Sürüm 1.0

1. ÇALIŞMA GRUBU

Yayını Hazırlayan

DOĞAN PEKER (1. Çalışma Grubu Üyesi)

Belge No : TBD/Kamu-BIB/2008-ÇG1

Tarihi : 16/4/2008

Durumu : S 1.0

1. Çalışma Grubu :

Çalışma Grubu Başkanı	AHMET PEKEL	(TCMB)
Kamu-BİB YK Temsilcisi	AYLA ALTUN	(ODTÜ)
Çalışma Grubu Başkan Yrd.	ÜVEYİZ ÜNAL ZAİM	(ADALET BAKANLIĞI)
Kamu-BİB	NECATİ ETLACAKUŞ	(OYTEK)
TBD YK	SELÇUK KAVASOĞLU	(DPT)
Grup Üyeleri	ABİDİN TOPAÇOĞLU	(ADALET BAKANLIĞI)
	ADNAN YILMAZ	(YARGITAY)
	ASLIHAN TÜFEKÇİ	(GAZİ ÜNİVERSİTESİ)
	ATİLLA BİLİCİ	(TKİ)
	AYSIM HANÇER	(KIZILAY)
	CENGİZ GÜRAY	(OYTEK)
	CİHAN ONAY	(ANKARA BÜYÜKŞEHİR BLD.)
	CÜNEYT NALÇACI	(SENTİM)
	DENİZ PEKER	(OYTEK)
	DOĞAN PEKER	(KOÇSİSTEM)
	ERDAL NANECİ	(MİLLİ KÜTÜPHANE)
	ERDİNÇ IŞIK	(MALİYE BAKANLIĞI)
	ERHAN KUMAŞ	(TÜRKSAT)
	ERSİN TAŞÇI	(TCDD)
	ERSİN T. YALVAÇ	(MALİYE BAKANLIĞI)
	F.LEYLA ERSUN	(ODTÜ)
	GÜRKAN ERENEL	(TÜRKSAT)
	İ.NEJAT ÇERCİ	(YURTKUR)
	İLHAN AKÇAL	(MİLLİ KÜTÜPHANE)
	İSMAİL YILDIRIM	(ANKARA BÜYÜKŞEHİR BLD.)
	KEMAL NALÇACI	(TÜRK PATENT ENSTİTÜSÜ)
	KÜRŞAT ÇAĞILTAY	(ODTÜ)
	MELİKE ÖZLEM TOSUN	(ÇEVRE ve ORMAN BAKANLIĞI)
	MESUT KÜÇÜKİBA	(ADALET BAKANLIĞI)
	NEZİHA ÇARKIT	(MEB)
	NURAN GÖRGÜN	(ADALET BAKANLIĞI)
	O.KUBİLAY YILMAZ	(MALİYE BAKANLIĞI)
	ORHAN TOPÇU	(BAŞBAKANLIK-TADY)
	OSMAN SARITAŞ	(MALİYE BAKANLIĞI)
	RAGIP GÜLPINAR	(TOKİ)
	SELDA TUNÇ	(MALİYE BAKANLIĞI)
	SEVDA ÖNÜRME	(MALİYE BAKANLIĞI)
	SEVİNÇ OKUMUŞOĞLU	(TİK)
	SUNA SARIOĞLU	(SANAYİ BAKANLIĞI)
	TOLUNAY CUMURCU	(ORBİM)
	TUBA DURMAZ	(HÜ)
	TUNCAY BİLMEZ	(TPAO)
	YASEMİN SEYDİM	(TCMB)
	YAŞAR TOMSUK	(TKİ)

İÇİNDEKİLER

İÇİNDEKİLER **4**

Kısaltmalar **6**

Şekiller **6**

BÖLÜM 1 ..... **7**

1.1 . ISO ve IEC 7

1.2 . ISO/IEC 27001:2005 7

1.3 . Bilgi Güvenliği Nedir? 8

1.4. BGYS - Bilgi Güvenliği Yönetim Sistemi nedir? 9

BÖLÜM 2 ..... **10**

2.1 . ISO/IEC 27001:2005 Standardı ve Süreç Yaklaşımı 10

2.2 . Neleri içerir? 12

BÖLÜM 3 ..... **13**

3.1 . BGYS Proje Ekibinin Oluşturulması 13

3.2 . BGYS'nin kurulması ve yönetilmesi 13

3.2.1. BGYS'nin kurulması 13

3.2.2. BGYS'nin uygulanması ve işletilmesi 14

3.2.3. BGYS'nin izlenmesi ve gözden geçirilmesi 15

3.2.4. BGYS'nin sürdürülmesi ve iyileştirilmesi 16

3.3 . Belgeleme gereksinimleri 16

3.3.1. BGYS belgeleri ve kayıtları geliştirilmelidir 16

3.3.2. BGYS Belgelerinin Kontrolü 17

3.3.3. BGYS Kayıtların Kontrolü 17

BÖLÜM 4 ..... **19**

4.1 . Yönetim bağlılığı 19

4.2 . BGYS Kaynak Yönetimi 19

4.2.1. Kaynakların sağlanması 19

4.2.2. BGYS personelinin eğitimi, farkında olması ve yeterliliği 20

BÖLÜM 5 21

5.1 . BGYS'nin iç denetimleri 21

BÖLÜM 6 22

6.1 . Yönetim gözden geçirmeleri.....22

6.2 . Yönetim gözden geçirme girdileri 22

6.3 . Yönetim Gözden geçirme çıktıları 23

BÖLÜM 7 24

7.1 . BGYS'nin sürekli iyileştirilmesi 24

7.2 . Düzeltici faaliyet.....24

7.3 . Önleyici faaliyet.....25

BÖLÜM 8 27

8.1 . Başarı Etkenleri 27

BÖLÜM 9 28

9.1 . BGYS Kurmanın Yararları.....28

KAYNAKÇA 29

Kısaltmalar

BT	Bilişim Teknolojileri
IEC	Uluslararası Elektroteknik Komisyonu
ISO	International Organization for Standardization : Uluslararası Standartlar Teşkilâtı
KAMU-BİB	Kamu Bilgi İşlem Merkezleri Yöneticileri Birliği
TBD	Türkiye Bilişim Derneği

Şekiller

Şekil 1 – BGYS Süreçlerine Uygulanan PUKÖ Modeli 11

BÖLÜM 1

Giriş

1.1. ISO ve IEC

Uluslararası Standartlar Organizasyonu olan **ISO**[1] 1947 yılında kurulmuştur. Merkezi İsviçre Cenevre'dir. Amacı, uluslararası ticareti kolaylaştırmak ve desteklemek için standartlar geliştirmektir.

Uluslararası Elektroteknik Komisyonu olan **IEC**[2], 1906 yılında kurulmuştur. Merkezi İsviçre Cenevre'dir. Amacı, her türlü elektro teknoloji için standartlar geliştirmektir.

1.2. ISO/IEC 27001:2005

ISO/IEC 27001:2005 - *Bilişim Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler* standardı , bir Bilgi Güvenliği Yönetim Sistemi'ni (BGYS) (ISMS – Information Security Management System) kurmak, geliştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model oluşturmak amacıyla hazırlanmıştır. ISO/IEC 27001, bilgi güvenlik yönetim standardıdır. Bir dizi bilgi güvenlik yönetim gereksinimlerini tanımlar. Gereksinim bir ihtiyaç, beklenti ya da zorunluluktur. Çok çeşitli türden gereksinimler vardır. Bunların bazıları güvenlik gereksinimleri, sözleşmelere bağlı gereksinimler, yönetimsel gereksinimler, düzenleyici ya da yasal gereksinimleri içerir.

ISO/IEC 27001 standardının amacı, bilgi güvenlik yönetim sistemi (BGYS) kurmak ve bakımını sürdürmektir. ISO/IEC 27001 standardı her türlü kuruluşa uygulanabilir. Kuruluşun ne yaptığı ya da büyüklüğü önemli değildir. ISO/IEC 27001 standardı, kuruluşun bilgi güvenlik yönetim gereksinimleri ve gerekliliklerini karşılamaya yardımcı olur.

---

1 International Organization for Standardization

2 International Electrotechnical Commission

Bu standart ISO tarafından 14 Ekim 2005 tarihinde yayınlanmış ve ISO/IEC 27000 standart serisi altında yerini almıştır. Bilgi güvenliği yönetim sistemi ile ilgili belgelendirilebilen bir standardıdır.

Türkiye'de ise, ISO tarafından kabul edilen, ISO/IEC 27001:2005 standardı esas alınarak, TSE Bilgi Teknolojileri ve İletişim İhtisas Grubu'nca hazırlanmış ve TSE Teknik Kurulu'nun 2 Mart 2006 tarihli toplantısında Türk Standardı olarak kabul edilerek, "TS ***ISO/IEC 27001*** *Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri - Gereksinimleri* "adıyla yayınlanmıştır.

ISO/IEC 27000 standart serisi altında yer alan diğer bir standart; ***ISO/IEC 27002:2005*** *- Bilişim Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenlik Yönetimi için Uygulama Kılavuzu'*dur. Bu standardın önceki adı ISO/IEC 17799:2005'dir. 1 Temmuz 2007 tarihinde, ISO tarafından yapılan teknik bir düzenlemeyle ISO/IEC 17799:2005 standardının adı, ISO/IEC 27002:2005 olarak değiştirilmiştir. Bu standart, bilgi güvenliği yönetimi sistemi (BGYS) oluşturmak için gereken 11 ana başlık altında yapılandırılmış 133 adet güvenlik kontrolü tanımlayan bir uygulama kılavuzudur.

1.3. Bilgi Güvenliği Nedir?

Bilgi güvenliği, aşağıdaki konularda bilginin korunmasını sağlar :

- **Gizlilik:** Bilginin sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğunun garanti edilmesi.
- **Bütünlük:** Bilginin ve işleme yöntemlerinin doğruluğunun ve bütünlüğünün sağlanması. Yetkisiz kişilerce değiştirilememesi.
- **Erişebilirlik:** Yetkilendirilmiş kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara erişime sahip olabileceklerinin garanti edilmesi.

Bilgi güvenliği, politikalar, süreçler, prosedürler, organizasyonel yapılar, yazılım ve donanım işlevleri gibi uygun bir kontrol kümesi uygulanarak başarılabilir.

1.4. BGYS - Bilgi Güvenliği Yönetim Sistemi nedir?

Bilgi güvenliği yönetim sistemi, bilgi güvenliği kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçasıdır.

Yönetim sistemi, kurumsal yapıyı, politikaları, planlama etkinliklerini, sorumlulukları, uygulamaları, prosedürleri, süreçleri ve kaynakları içerir.

BÖLÜM 2

2.1. ISO/IEC 27001:2005 Standardı ve Süreç Yaklaşımı

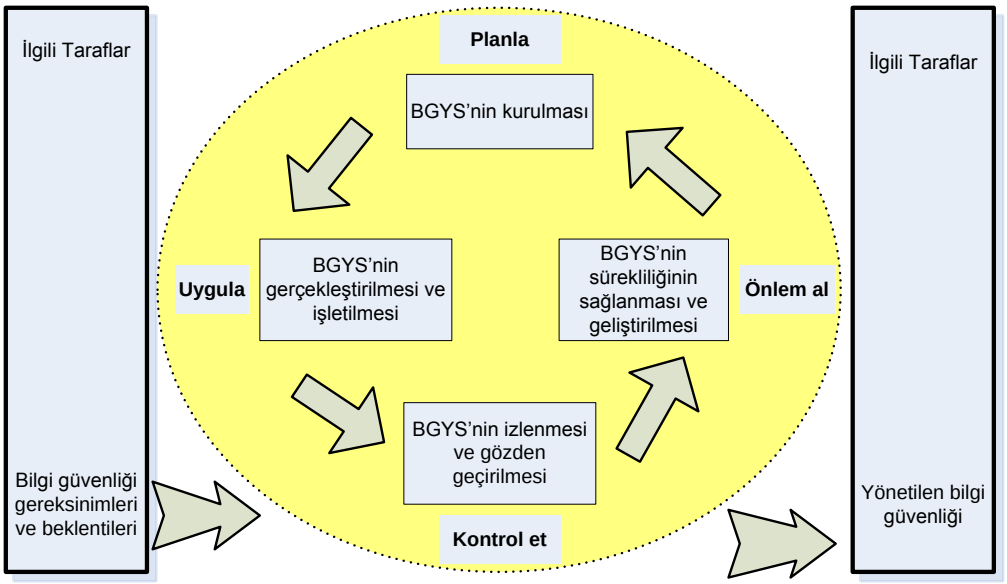
ISO/IEC 27001:2005 standardı, bir kuruluşun BGYS'sini oluşturmasında, süreç yaklaşımını benimser. Kuruluşun görevlerini etkin bir şekilde yapabilmesi için, etkinliklerini tanımlaması ve yönetmesi gerekmektedir. Her etkinlik bir süreç olarak düşünülebilir. Bir sürecin çıktısı, bu süreci izleyen başka bir sürecin girdisini oluşturur.

Bir kuruluş içerisinde, tanımları ve bunların etkileşimi ve yönetimleriyle birlikte süreçlerin oluşturduğu bir sistem uygulaması "süreç yaklaşımı" olarak tanımlanabilir.

Bilgi güvenliği yönetimi süreç yaklaşımı, kullanıcılarını aşağıdaki konuların öneminin vurgulanmasını özendirir:

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

Bu standart, tüm BGYS süreçlerini yapılandırmada uygulanan "Planla-Uygula-Kontrol Et-Önlem al" (PUKÖ) modelini benimser. Aşağıdaki şekil, BGYS'nin bilgi güvenliği gereksinimlerini ve ilgili tarafların beklentilerini girdi olarak nasıl aldığını ve gerekli eylem ve süreçler aracılığıyla, bu gereksinimleri ve beklentileri karşılayacak bilgi güvenliği sonuçlarını nasıl ürettiğini gösterir. (Şekil-1).



Şekil 1 – BGYS Süreçlerine Uygulanan PUKÖ Modeli

Planla (BGYS'nin kurulması)	Sonuçları kuruluşun genel politikaları ve amaçlarına göre dağıtmak için, risklerin yönetimi ve bilgi güvenliğinin geliştirilmesiyle ilgili BGYS politikası, amaçlar, süreçler ve prosedürlerin kurulması.
Uygula (BGYS'nin gerçekleştirilmesi ve işletilmesi)	BGYS politikası, kontroller, süreçler ve prosedürlerin gerçekleştirilip işletilmesi.
Kontrol et (BGYS'nin izlenmesi ve gözden geçirilmesi)	BGYS politikası, amaçlar ve kullanım deneyimlerine göre süreç performansının değerlendirilmesi ve uygulanabilen yerlerde ölçülmesi ve sonuçların gözden geçirilmek üzere yönetime rapor edilmesi.
Önlem al (BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi)	BGYS'nin sürekli iyileştirilmesini sağlamak için, yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve önleyici eylemlerin gerçekleştirilmesi.

ISO/IEC 27001:2005 standardı, ISO 9001 ve ISO 14001 ile uyumludur.

Bu standart, bir kuruluşun BGYS'sini ilgili yönetim sistemi gereksinimleriyle uyumlu yapabilmesi ya da bütünleştirilebilmesi için tasarlanmıştır.

2.2. Neleri içerir?

Bu standart, ticari kuruluşlar, kamu kurumları, kar amaçlı olmayan kuruluşlar, yani tüm kuruluşları kapsar. Bu standart, bir kuruluşun tüm ticari riskleri anlamında belgelenmiş bir BGYS'yi kurması, gerçekleştirmesi, izlemesi, gözden geçirmesi, sürdürmesi ve iyileştirmesi için gereksinim duyduğu konularını içerir.

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

Bir kuruluşun ISO 27001 sertifikasına sahip olması, kurumun güvenlik risklerini bildiği, yönettiği, belli risklerde ortadan kaldırmak için kaynak ayırdığı anlamına gelir. Yoksa ISO 27001 Bilgi Güvenliği Yönetim Sistemine sahip olmak, kurumların yüzde yüz güvenlik seviyesine sahip olduklarını söylemesi anlamına gelmez. Zaten, yüzde yüz güvenlik seviyesine ulaşmak olası değildir.

BÖLÜM 3

Bilgi Güvenliği Yönetim Sistemi

3.1. BGYS Proje Ekibinin Oluşturulması

BGYS'nin kurulması ve yönetilmesini üstlenecek bir proje ekibi oluşturulmalıdır. Ekip yöneticisi ve üyeleri, bilgi güvenliği yönetimi konusunda eğitimli/deneyimli olmalıdır. Çünkü bu ekip, risk yönetimi, politika oluşturma, güvenlik prosedürlerinin hazırlanması ve uygun kontrollerin seçilerek uygulanması gibi çalışmaları yapacaktır. Gerektiğinde bu proje ekibinin konusunda uzman danışmanlardan görüş ve öneri alması sağlanmalıdır.

3.2. BGYS'nin kurulması ve yönetilmesi

Bilgi Güvenliği Yönetim Sistemini kurmayı ve yönetmeyi düşünen bir kuruluşta izlenmesi gerekenler aşağıda anlatılmıştır.

3.2.1. BGYS'nin kurulması

- BGYS'nin kapsamı ve sınırlarını tanımlanır. BGYS'nin, kuruluşun hangi bölümlerinde uygulanacağı, hangi varlıkları ve teknolojileri içereceği yani sınırları belirlenmeli, tanımlanmalı, içeriği ve sınırları tanımlayan belgeler hazırlanmalıdır.
- Kuruluşun BGYS politikası tanımlanır. BGYS'yi kurmak için öncelikle Bilgi Güvenliği Politikası oluşturulmalı, yazılı hale getirilmelidir. Oluşturulan politikalar yönetim tarafından onaylanıp, kurum çalışanlarına duyurulmalıdır. Kuruluş, yaptığı işin, yerleşim yerinin, varlıklarının ve teknolojisinin özelliklerine göre bir BGYS politikası tanımlamalıdır.
- Kuruluşun risk değerlendirme yaklaşımı tanımlanır. Uygun bir risk değerlendirme metodolojisi seçilmelidir. Seçilen risk değerlendirme

metodolojisi, risk değerlendirmelerinin karşılaştırılabilir ve yeniden üretilebilir sonuçlar üretmesini sağlamalıdır. Ayrıca kabul edilebilir risk seviyeleri tanımlanmalıdır.

- Kuruluşun güvenlik riskleri belirlenir. BGYS kapsamındaki varlıkları ve bu varlıkların sahipleri tanımlanır. Bu varlıklar için var olan tehditler tanımlanır. Gizlilik, bütünlük ve kullanılabilirlik kayıplarının varlıklar üzerinde olabilecek etkileri tanımlanır.
- Kuruluşun güvenlik riskleri analiz edilir ve değerlendirilir.
- Risk işleme seçenekleri ve eylemleri belirlenir ve değerlendirilir.
- Riskleri önlemek için kontrol amaçları ve kontroller seçilir. Seçimlerde ISO/IEC 27002 standardının karşılık gelen bölümlerine başvurulmalıdır. Kontrol amaçları ve kontroller, risk değerlendirme ve risk işleme süreçlerince tanımlanan gereksinimleri karşılamak için seçilmeli ve gerçekleştirilmelidir.
- Yönetimin tüm artık riskleri formal olarak onayladığından emin olunmalıdır. Yani sunulan artık risklere ilişkin yönetim onayı edinilmelidir. (Uygulanan risk giderme kararları sonrası arta kalan risklere, artık riskler denilir)
- Kuruluşun BGYS'ni uygulamadan ve işletmeden önce yönetimden yetki alınır.
- Kuruluşa özel kontrol amaçları ve kontrolleri içeren Uygulanabilirlik Bildirgesi hazırlanmalıdır. Uygulanabilirlik Bildirgesi, seçilen kontrol amaçları ve kontrolleri içermeli ve bunların seçilme nedenlerini açıklamalıdır. Kontrol amaçları ve kontrollerden hangilerinin gerçekleştirilmiş olduğunu, hangilerinin dışarda bırakıldığını ve neden dışarda bırakıldığını açıklamalıdır.

3.2.2. BGYS'nin uygulanması ve işletilmesi

- Kuruluşun bilgi güvenlik risklerini yönetmek için risk önleme planı geliştirilir. Risk önleme planı, bilgi güvenlik risklerini yönetmek için gereken yönetim etkinliklerini, kaynakları, sorumlulukları ve öncelikleri içermelidir.
- Hazırlanan risk önleme planı uygulanır.

- Güvenlik kontrolleri uygulanır. Kontrollerin etkinliğinin ölçülmesi, yöneticiler ve personele kontrollerin planlanan kontrol amaçlarını ne kadar iyi düzeyde başardığına karar verme olanağı verir.
- Kuruluşun bu konuyla ilgili eğitim programları gerçekleştirilir.
- Kuruluşun BGYS'i yönetilir ve işletilir.
- Kuruluşun BGYS kaynakları yönetilir.
- Kuruluşun güvenlik olaylarını anında saptayabilme ve güvenlik ihlal olaylarına hemen yanıt verebilme yeteneğine sahip güvenlik prosedürlerini uygulanır.

3.2.3. BGYS'nin izlenmesi ve gözden geçirilmesi

- BGYS'ni izlemek için prosedürler ve kontroller kullanılmalıdır. Bu sayede izleme sonuçlarındaki hatalar saptanır, ihlal olayları (iş operasyonlarını tehlikeye atma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek ya da bir dizi istenmeyen ya da beklenmeyen bilgi güvenliği olayı) anında tanımlanır. Yönetimin, güvenlik etkinliklerinin beklenen biçimde çalışıp çalışmadığını belirleyebilmesi sağlanır. Güvenlik olaylarını saptama ve kriterler kullanarak güvenlik ihlal olaylarını önlemeye yardım etme ve bir güvenlik kırılmasını çözmek için alınan önlemlerin etkili olup olmadığına karar verme olanakları ortaya çıkar.
- BGYS'ni gözden geçirmek için prosedürler ve kontroller kullanılmalıdır.
- BGYS düzenli olarak gözden geçirilir. Gözden geçirmelerde, güvenlik denetimlerinin sonuçları, ihlal olayları, etkinlik ölçümleri sonuçları, öneriler ve geri bildirimleri dikkate alınır.
- Güvenlik gereksinimlerinin sağlandığı doğrulanmalıdır. Bunun için kontrollerin etkinliği ölçülmelidir.
- Risk analizi ve risk değerlendirmeleri düzenli olarak gözden geçirilmelidir. Kuruluş, teknoloji, İş amaçları ve süreçleri, tanımlanmış tehditler, gerçekleştirilen kontrollerin etkinliği, yasal ve düzenleyici ortamdaki değişiklikler, değiştirilmiş anlaşma yükümlülükleri ve sosyal iklimdeki değişiklikler gibi dış olaylarda meydana gelen değişiklikler dikkate alınarak planlanan aralıklarda kabul edilebilir risk düzeyleri gözden geçirilmelidir.

- Artık riskler (risk işlemeden sonra kalan riskler) düzenli olarak gözden geçirilmelidir.
- BGYS iç denetimleri planlanan aralıklarda düzenli olarak yapılmalıdır.
- BGYS yönetim gözden geçirmeleri düzenli olarak yapılmalıdır. Bu sayede kapsamın uygun kalması ve BGYS sürecindeki iyileştirmelerin tanımlanmasını sağlanır.
- İzleme ve gözden geçirme etkinliklerindeki sonuçlar irdelenerek bilgi güvenlik planları günlenir.
- BGYS'i etkileyen olay ve eylemler ile ilgili kayıtlar tutulmalı ve saklanmalıdır.

3.2.4. BGYS'nin sürdürülmesi ve iyileştirilmesi

- BGYS'de tanımlı olan iyileştirmeler uygulanır.
- Uygun düzeltici eylemler uygulanır.
- Uygun önleyici eylemler uygulanır. Öğrenilen güvenlik deneyimlerinden alınan dersler uygulanır.
- BGYS değişiklikleri yani eylem ve iyileştirmeler tüm ayrıntısıyla ilgili gruplarla paylaşılır.
- Kuruluşun, BGYS değişikliklerinin, tasarlanan amaçları gerçekleştirdiğinden emin olunmalıdır.

Bu çalışmalar belirli aralıklarla yerine getirilmelidir.

3.3. Belgeleme gereksinimleri

3.3.1. BGYS belgeleri ve kayıtları geliştirilmelidir

- Kararları belgeleyen kayıtlar oluşturulur. Yönetim kararları belgelenmeli, eylemlerin yönetim kararları ve politikalarına izlenebilir olmasını sağlamalıdır.
- Kuruluşun BGYS belgelenir. BGYS belgesinde BGYS politikası ve kontrol amaçları, BGYS kapsamı, BGYS'yi destekleyen prosedürler, risk değerlendirme metodolojisi tanımı, risk değerlendirme raporu,

risk işleme planı, prosedür ve kontrollerin etkinliğini ölçme tanımı, bu standart için tutulması gereken kayıtlar ve uygulanabilirlik bildirgesi yer almalıdır.

Belgeler ve kayıtlar herhangi bir biçimde ve ortam türünde olabilir.

3.3.2. BGYS Belgelerinin Kontrolü

- BGYS belgeleri korunmalı ve kontrol edilmelidir.
- BGYS belgelerini kontrol etmede kullanılacak bir prosedür oluşturulmalıdır.

Bu prosedür, aşağıdakilere gereksinim duyan yönetim eylemlerini belirtmek için kurulmalıdır:

a) Yayınlanmadan önce belgeleri uygunluk açısından onaylama,
b) Gerektiğinde belgeleri gözden geçirme, günleme ve tekrar onaylama,
c) Belge değişikliklerinin ve mevcut revizyon durumunun tanınmasını sağlama,
d) Uygulanabilir belgelerin ilgili sürümlerinin kullanım noktalarında kullanılabilir olmasını sağlama,
e) Belgelerin okunaklı ve hazır olarak tanınabilir olmasını sağlama,
f) Belgelerin gereksinim duyanlar için kullanılabilir olmasını, aktarılmasını, saklanmasını ve sınıflandırılmasına uygun prosedürlerle tamamen yok edilmelerini sağlama,
g) Dış kaynaklı belgelerin tanınmasını sağlama,
h) Belge dağıtımının kontrol edilmesini sağlama,
i) Yürürlükte olmayan belgelerin istenmeden kullanımını engelleme ve
j) Herhangi bir amaç için tutuluyorsa, bu belgelere uygun kimlik uygulama.

3.3.3. BGYS Kayıtların Kontrolü

- Kuruluşun BGYS için kayıtlar oluşturulmalıdır. Bu kayıtlar, BGYS'nin gereksinimlere uygun olduğuna ve etkin işlediğine ilişkin kanıtlar oluşturmalı ve sürekliliği sağlanmalıdır.

- Bu kayıtlar muhafaza edilmeli ve kontrol edilmelidir. Kayıtlar okunabilir, hemen erişilebilir ve yedekli olarak tutulmalıdır. Kayıtların tutulması, korunması, düzenleme zamanları için gerekli denetimler belgelenmelidir. Kayıtlara örnek olarak giriş/çıkış kontrol sistemlerinde oluşan bilgiler, denetim kayıtları, erişim yetkilendirme formları verilebilir.

BÖLÜM 4

Yönetim Sorumluluğu

4.1. Yönetim bağlılığı

Yönetimin BGYS'ni desteklediği kanıtlanmalıdır. Kısaca :

- Yönetimin BGYS oluşturulmasını desteklediği gösterilmelidir.
- Yönetimin BGYS uygulamasını desteklediğini gösterilmelidir.
- Yönetimin BGYS işletimini desteklediğini gösterilmelidir.
- Yönetimin BGYS izlenmesini desteklediğini gösterilmelidir.
- Yönetimin BGYS gözden geçirilmesini desteklediğini gösterilmelidir.
- Yönetimin BGYS bakımının yapılmasını desteklediğini gösterilmelidir.
- Yönetimin BGYS geliştirilmesini desteklediğini gösterilmelidir.

4.2. BGYS Kaynak Yönetimi

4.2.1. Kaynakların sağlanması

- Kuruluşun BGYS kaynak gereksinimleri belirlenir.
- BGYS'nin gereksinim duyduğu kaynaklar sağlanır.
- İş gereksinimlerinizi destekleyen ve kuruluşun bilgi güvenlik prosedürlerini garanti etmede gerekli olacak kaynaklar belirlenir.
- Kuruluşun yasal güvenlik gereksinimlerini karşılayacak kaynaklar belirlenir.
- Kuruluşun düzenleyici güvenlik gereksinimlerini karşılayacak kaynaklar belirlenir.
- Kuruluşun, sözleşmelerle belirlenen güvenlik zorunluluklarını karşılayacak kaynaklar belirlenir.
- Tüm uygulanan güvenlik önlemlerinin doğru olarak uygulandığını garanti edecek gerekli kaynaklar belirlenmelidir.
- BGYS yönetim gözden geçirmelerinin düzenli olarak yapılmasını sağlayacak kaynaklar belirlenmelidir.

- BGYS yönetim gözden geçirmeleri sonuçlarına uygun olarak hareket edilmelidir.
- Gerektiğinde BGYS'nin etkinliğini iyileştirmek için kaynak sağlanmalıdır.

4.2.2. BGYS personelinin eğitimi, farkında olması ve yeterliliği

- Tüm BGYS personelinin BGYS konusunda yeterliliği ve kendilerine atanan tüm görevleri yapabileceğinden emin olunmalıdır.
- Kuruluşun BGYS personel eğitimi ve istihdam etkinliklerinin etkinliğini değerlendirilmelidir.
- BGYS etkileyecek çalışmaları yapan personelin yeterliliğini (eğitim, öğretim, beceriler, deneyim ve niteliklere ilişkin) belgeleyen kayıtlar tutulmalı ve korunmalıdır.
- Bilgi güvenlik etkinliklerinin ne kadar önemli olduğu konusunda personel bilgilendirilmelidir.

BÖLÜM 5

5.1. BGYS'nin iç denetimleri

Kuruluş BGYS iç denetimlerini, BGYS kontrol amaçlarının, kontrollerinin, süreçlerinin ve prosedürlerinin standarda uygun olarak gerçekleştirip gerçekleştirmediğini belirlemek için planlanan aralıklarda gerçekleştirilmelidir.

İç denetim prosedürü oluşturulmalıdır:

- BGYS iç denetim prosedürü oluşturulmalıdır.
- BGYS iç denetim prosedürü belgelenmelidir.

İç denetimler planlanır:

- BGYS iç denetim projeleri ve etkinlikleri planlanır
    - İç denetimlerin hangi sıklıkta yapılacağını şekillendirilir.
    - Planlanan aralıklarda yapılacak iç denetimlerin çizelgesi oluşturulur.
    - Her bir BGYS iç denetiminin kapsamı netleştirilmelidir.
    - Her bir iç denetim için denetim kriterleri belirtilmelidir.
    - BGYS iç denetim yöntemleri tanımlanır.
    - BGYS iç denetçileri seçilir.

İç denetimler yönetilir:

- BGYS iç denetimleri uygulanır.
    - Kuruluşun BGYS kontrol amaçları denetlenir.
    - Kuruluşun BGYS kontrolleri denetlenir.
    - Kuruluşun BGYS süreçleri denetlenir.
    - Kuruluşun BGYS kontrol prosedürleri denetlenir.

Düzeltici eylemler:

- Uygunsuzluklar ve bunların nedenleri ortadan kaldırılmalıdır.
- Uygunsuzlukların ve nedenlerinin ortadan kaldırılmasına yönelik eylemleri gecikmeksizin hayata geçirme çalışmaları başlatılır:
    - Düzeltici eylemlerin gerçekten uygulandığı doğrulanmalıdır.
    - Doğrulama etkinliklerinin sonucu raporlanmalıdır.

BÖLÜM 6

Yönetimin BGYS'yi Gözden Geçirmesi

6.1. Yönetim gözden geçirmeleri

- BGYS ile ilgili yönetim gözden geçirme çalışmaları yapılır
  - Kuruluşun yönetim personelinin, planlanan aralıklarla (en az yılda bir kez), BGYS'ni gözden geçirme işlevini yerine getirmesi sağlanır.
- BGYS'nin performansı sınanır:
  - Kullanılan BGYS'nin uygun olup olmadığını sınanır.
  - Kullanılan BGYS'nin yeterli olup olmadığını sınanır.
  - Kullanılan BGYS'nin etkin olup olmadığını sınanır.
- BGYS'nin değiştirilmesi ya da iyileştirilmesi konusunda değerlendirme yapılır.
  - Bilgi güvenlik politikası değiştirilmesi mi yoksa iyileştirilmesi mi gerektiği konusunda değerlendirme yapılır.
  - Bilgi güvenlik amaçlarının değiştirilmesi mi yoksa iyileştirilmesi mi gerektiği konusunda değerlendirme yapılır.

Gözden geçirme sonuçları açıkça belgelenmeli ve kayıtlar tutulup saklanmalıdır.

6.2. Yönetim gözden geçirme girdileri

- BGYS (girdiler) hakkındaki bilgiler gözden geçirilmelidir:
  - Yönetim gözden geçirmeleri öncesi sonuçlar gözden geçirilir.
  - Önceki BGYS denetim sonuçları gözden geçirilir.
  - Önceki BGYS ölçüm sonuçları gözden geçirilir.
  - Önceki düzeltici eylemlerin durumunu gözden geçirilir.
  - Önceki risk değerlendirmesi sırasında uygunsuz olarak adreslenen(belirlenen) güvenlik sorunları gözden geçirilir.
  - BGYS'ni geliştirme fırsatlarını gözden geçirilir.
  - BGYS'ni etkileyebilecek değişiklikler gözden geçirilir.

6.3. Yönetim Gözden geçirme çıktıları

- Yönetimin gözden geçirmesinin çıktıları, aşağıdaki konularda kararları ve eylemleri içermelidir:
  - Kuruluşun BGYS etkinliğini iyileştirme,
  - Kuruluşun BGYS'ni (risk değerlendirme ve risk işleme planını) güncelleme,
  - BGYS'ni etkileyen olaylara karşılık vermek için bilgi güvenliğini etkileyen prosedür ve kontrol değişiklikleri,
  - Kuruluşun BGYS kaynak gereksinimleri.

BÖLÜM 7

BGYS'nin İyileştirilmesi

7.1. BGYS'nin sürekli iyileştirilmesi

- BGYS'nin etkinliğini sürekli iyileştirmek için :
  - Bilgi güvenlik politikanızı kullanınız,
  - Bilgi güvenlik amaçlarınızı kullanınız,
  - Bilgi güvenlik denetim sonuçlarını kullanınız,
  - Yönetim gözden geçirmelerinizi kullanınız,
  - Düzeltici eylemlerinizi kullanınız,
  - Önleyici eylemlerinizi kullanınız,
  - İzleme süreçlerinizi kullanınız.

7.2. Düzeltici faaliyet

- Gerçek uyumsuzlukların yinelenmesini önlemek için düzeltici faaliyet prosedürü oluşturulmalıdır. Düzeltici faaliyet prosedürü aşağıdaki gereksinimleri tanımlamalıdır :
  - Gerçek uygunsuzlukları tanımlama,
  - Uygunsuzlukların nedenlerini belirleme,
  - Faaliyete geçmeye gerek olup olmadığını değerlendirilmesini belirleme,
  - Gerektiğinde düzeltici faaliyetleri geliştirmeyi belirleme,
  - Gerçek uygunsuzlukların yinelenmesini önleme,
  - Kuruluşun uygunsuzluklarının nedenlerini yok etmeyi belirleme,
  - Uygulanan düzeltici faaliyetlerin sonuçlarını kaydetme,
  - Uygulanan düzeltici eylemlerin sonuçlarını gözden geçirme.
- Düzeltici faaliyet prosedürünüzü belgelenmelidir.
- Düzeltici faaliyet prosedürünüzü uygulanmalıdır.
  - Uygunsuzlukları belirlemek için kurumun düzeltici faaliyet prosedürü kullanılır.
  - Uygunsuzluk nedenlerini belirlemek için kurumun düzeltici faaliyet prosedürü kullanılır.

- Düzeltici eylemin gerekip gerekmediğini değerlendirmek için kurumun düzeltici faaliyet prosedürü kullanılır.
- Düzeltici eylemler gerçekten gerekiyorsa, düzeltici faaliyetleri geliştirmek için kurumun düzeltici faaliyet prosedürü kullanılır.
- Düzeltici faaliyetleri uygulamak için kurumun düzeltici faaliyet prosedürü kullanılır.
- Gerçek uygunsuzlukların yinelenmesini önlemek için kurumun düzeltici faaliyet prosedürü kullanılır.
- Gerçek uygunsuzlukların nedenlerini yok etmek için kurumun düzeltici faaliyet prosedürü kullanılır.
- Uygulanan düzeltici faaliyetlerin sonuçlarını kaydetmek için kurumun düzeltici faaliyet prosedürü kullanılır.
- Uygulanan düzeltici faaliyetleri gözden geçirmek için kurumun düzeltici faaliyet prosedürü kullanılır.

- Düzeltici faaliyet prosedürünün bakımı yapılmalıdır.

7.3. Önleyici faaliyet

- Potansiyel uygunsuzlukların meydana gelmesini önlemek için önleyici faaliyet prosedürü oluşturulmalıdır. Önleyici faaliyetler için belgelenmiş bu prosedür, aşağıdaki gereksinimleri tanımlamalıdır:
  - Potansiyel uyumsuzlukları tanımlama,
  - Potansiyel uyumsuzlukların nedenlerini belirleme,
  - Önleyici eyleme geçip geçmemeye gerek olup olmadığını değerlendirme,
  - Gerektiğinde önleyici eylemleri geliştirme,
  - Potansiyel uygunsuzlukların oluşmasını önleme,
  - Potansiyel uygunsuzlukların nedenini yok etme,
  - Uygulanan önleyici eylemlerin sonucunu kaydetme,
  - Uygulanan koruyucu önlemlerin sonuçlarını gözden geçirme.
- Önleyici faaliyet prosedürü belgelenmelidir.
- Önleyici faaliyet prosedürü uygulanmalıdır.
  - Potansiyel uygunsuzluklarınızı belirlemek için kuruluşun önleyici faaliyet prosedürü kullanılır.

- Potansiyel uygunsuzluklarınızın nedenini yok etmek için kuruluşun önleyici faaliyet prosedürü kullanılır.
- Önleyici eylem uygulanmasına gerek olup olmadığını değerlendirmek için kuruluşun önleyici faaliyet prosedürü kullanılır.
- Gerektiğinde önleyici eylemler geliştirmek için kuruluşun önleyici faaliyet prosedürü kullanılır.
- Koruyucu önlemlere başvurmak için kuruluşun önleyici faaliyet prosedürü kullanılır.
- Potansiyel uyumsuzlukların oluşmasını önlemek için kuruluşun önleyici faaliyet prosedürü kullanılır.
- Potansiyel uyumsuzlukların nedenini yok etmek için kuruluşun önleyici faaliyet prosedürü kullanılır.
- Uygulanan koruyucu önlemlerin sonuçlarını kaydetmek için kuruluşun önleyici faaliyet prosedürü kullanılır.
- Uygulanan koruyucu önlemleri gözden geçirmek için kuruluşun önleyici faaliyet prosedürü kullanılır.

Kuruluş, değişen riskleri tanımlamalı ve dikkati önemli derecede değişen riskler üzerinde yoğunlaştırarak önleyici faaliyet gereksinimlerini tanımlamalıdır.

Önleyici faaliyetlerin önceliği, risk değerlendirme sonuçlarına bağlı olarak belirlenmelidir.

Uygunsuzlukların önlenmesi için gerçekleştirilen faaliyetler çoğunlukla düzenleyici faaliyetlerden daha az maliyetlidir.

BÖLÜM 8

8.1. Başarı Etkenleri

- Güvenlik politikaları, iş hedefini yansıtmalıdır.
- Uygulama yaklaşımını ve şirket kültürü tutarlılığı sağlanmalıdır.
- Yönetimin desteği ve bağlılığı görünür olmalıdır.
- Güvenlik gereksinimleri, risk değerlendirmesi ve risk yönetimi iyi anlaşılmalıdır.
- Güvenlik tüm yöneticilere ve çalışanlara etkili bir biçimde anlatılmalıdır.
- Bilgi güvenliği politikası ve standardları ile ilgili çalışmalar, tüm çalışanlarla ve sözleşmelilerle paylaşılmalıdır.
- Uygun eğitim sağlanmalıdır.
- Kapsamlı ve dengeli bir ölçüm sistemi oluşturulmalıdır.

BÖLÜM 9

9.1. BGYS Kurmanın Yararları

- Kuruluş hangi bilgi varlıklarına sahip olduğunu bilir ve değerinin farkına varır.
- Oluşturacağı kontrol amaçları ve kontroller ile koruma yöntemlerini belirler ve uygulayarak sahip olduğu varlıkları korur.
- Uzun yıllar boyunca işini sürdürmeyi garanti eder. Ayrıca bir felaket halinde, işe devam etme yeterliliğine sahip olur.
- Bilgileri korunacağından başta tedarikçileri olmak üzere, ilgili tarafların güvenini kazanır.
- Rakiplerine göre daha iyi güven avantajı sağlar.
- Çalışanların güdüsünü arttırır.
- Yasal takiplerin oluşmasını önler
- Yüksek prestij sağlar

KAYNAKÇA

[1] Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri - Gereksinimler

TSE Türk Standardı
TS ISO/IEC 27001 Mart 2006
ICS 35.040

[2] Deloitte

Bilgi Güvenliği Yönetim Sistemi
Deloitte Security Services Group Hizmet Perspektifi
http://www.deloitte.com/dtt/cda/doc/content/DeloitteHizmetPerspektifi-BGYS.pdf

[3] http://www.gammassl.co.uk/bs7799/works.html

Copyright © Gamma Secure Systems Limited 2001-2003

[4] atsec the Information Security Provider

http://www.atsec.com/01/isms-iso-iec-27001-BS-7799-faq.html#2

[5] http://www.praxiom.com/iso-27001.htm

On the Web since May 25, 1997. Updated on February 14, 2008.
Praxiom Research Group Limited

[6] Kurumlarda Bilgi Güvenliği Yönetim Sistemi'nin Uygulanması

Mehtap ÇETİNKAYA
İstanbul Kültür Üniversitesi, Bilgisayar Mühendisliği Yüksek Lisans Bölümü, İSTANBUL