BÖLÜM 7

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ

ANAHTAR KAVRAMLAR

Bilgi Güvenliği Yönetim Sistemi,
Kapsam Belirleme, Risk Değerlendirmesi

ÖĞRENME HEDEFLERİ

1. Bilgi Güvenliği Yönetim Sistemini (BGYS) açıklar.
2. BGYS uygulanacak kuruluşun kapsamını açıklar.
3. BGYS'nin uygulanmasında üst yönetimin rolünü açıklar.

YEDİNCİ BÖLÜM

GİRİŞ

Bilgi Güvenliği Yönetim Sistemi, bir bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için gereklilikleri açıklamak amacıyla International Standardization Organization (ISO) tarafından hazırlanmış, ISO/IEC 27001 olarak da anılan, standarttır. Orijinal adı "ISO/IEC 27001 Information security, cybersecurity and privacy protection — Information security management systems — Requirements" şeklinde geçmektedir (ISO, 2023). Bu bölüm ilgili standardın orijinal metnine sadık kalarak oluşturulmaya çalışılmıştır.

Bilgi güvenliği yönetim sisteminin benimsenmesi, kuruluş için stratejik bir karardır. Bir kuruluşta bilgi güvenliği yönetim sisteminin kurulması ve uygulanması, kuruluşun ihtiyaç ve hedeflerine, güvenlik gereksinimlerine, kullanılan organizasyonel süreçlere, kuruluşun büyüklüğüne ve yapısına bağlı olarak farklılık gösterir. Tüm bu faktörlerin zaman içinde de değişmesi beklenir.

Bilgi güvenliği yönetim sistemi, bir risk yönetimi süreci uygulayarak bilginin gizliliğini, bütünlüğünü ve kullanılabilirliğini korur ve ilgili taraflara risklerin yeterince yönetildiğine dair güven verir. Bilgi güvenliği yönetim sisteminin, kuruluşun süreçlerinin ve genel yönetim yapısının bir parçası olarak entegre olması ve süreçlerin, bilgi sistemlerinin ve kontrollerin tasarımında bilgi güvenliğinin dikkate alınması önemlidir. Bir bilgi güvenliği yönetim sistemi uygulamasının, kuruluşun ihtiyaçlarına uygun olarak ölçeklendirilmesi beklenmektedir.

1. KURULUŞUN KAPSAMI

Bu standart kapsamında, kuruluş bağlamında bir bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için gereksinimleri belirtir. Aynı zamanda kuruluşun ihtiyaçlarına göre uyarlanmış bilgi güvenliği risklerinin değerlendirilmesi ve ele alınmasına yönelik gereksinimleri de içermektedir. Standart içerisinde belirtilen gereksinimler geneldir ve türü, boyutu veya niteliği ne olursa olsun tüm kuruluşlar için geçerli olması amaçlanmıştır.

Kuruluşu ve kapsamını tanımak

Kuruluş, amacı ile ilgili olan ve bilgi güvenliği yönetim sisteminin amaçlanan sonuçlarına ulaşma yeteneğini etkileyen dış ve iç bağlamını belirlemelidir. Bu bağlamların belirlenmesi, ISO 31000:2018 Risk Yönetimi Standardında açıklanmıştır (ISO, 2023).

Kuruluşun dış bağlamının incelenmesi aşağıdakileri içerebilir, ancak bunlarla sınırlı değildir:

• Uluslararası, ulusal, bölgesel veya yerel olsun, sosyal, kültürel, politik, yasal, düzenleyici, mali, teknolojik, ekonomik ve çevresel faktörler;

• Kuruluşun hedeflerini etkileyen temel itici güçler ve eğilimler;

• Dış paydaşların ilişkileri, algıları, değerleri, ihtiyaçları ve beklentileri;

• Sözleşmeye dayalı ilişkiler ve taahhütler;

• Ağların ve bağımlılıkların karmaşıklığı

Kuruluşun iç bağlamının incelenmesi aşağıdakileri içerebilir ancak bunlarla sınırlı değildir:

• Vizyon, misyon ve değerler;

• Yönetişim, organizasyon yapısı, roller ve sorumluluklar;

• Strateji, hedefler ve politikalar;

• Kuruluşun kültürü;

• Kuruluş tarafından benimsenen standartlar, kılavuzlar ve modeller;

• Kaynaklar ve bilgi açısından anlaşılan yetenekler (örneğin sermaye, zaman, insanlar, fikri mülkiyet, süreçler, sistemler ve teknolojiler);

• Veriler, bilgi sistemleri ve bilgi akışları;

Algılarını ve değerlerini dikkate alarak iç payd
• aşlarla ilişkiler;

• Sözleşmeye dayalı ilişkiler ve taahhütler;

• Karşılıklı bağımlılıklar ve ara bağlantılar.

İlgili tarafların ihtiyaç ve beklentilerini göz önünde bulundurmak

Kuruluş şunları belirlemelidir:

Bilgi Güvenliği Yönetim Sistemi ile ilgili ilgili taraflar;

a) Bu ilgili tarafların ilgili gereklilikleri;

b) Bu gerekliliklerden hangileri Bilgi Güvenliği Yönetim Sistemi aracılığıyla ele alınacaktır.

c) İlgili tarafların gereklilikleri, yasal ve düzenleyici gereklilikleri ve sözleşmeden doğan yükümlülükleri içerebilir.

Bilgi güvenliği yönetim sisteminin kapsamını genişletmek

Kuruluş, kapsamını oluşturmak için bilgi güvenliği yönetim sisteminin sınırlarını ve uygulanabilirliğini belirlemelidir. Bu kapsamı belirlerken, kuruluş şunları dikkate almalıdır:

a) Kuruluşu ve kapsamını tanımak başlığında verilen dış ve iç bağlamları;

b) İlgili tarafların ihtiyaç ve beklentilerini göz önünde bulundurmak başlığında bulunulan gereklilikler;

c) Kuruluş tarafından gerçekleştirilen faaliyetler ile diğer kuruluşlar tarafından gerçekleştirilen etkinlikler arasındaki arabirimler ve bağımlılıklar.

Kapsam, yazılı belge olarak sunulmalıdır. Kuruluş, bu belgenin gerekliliklerine uygun olarak, ihtiyaç duyulan süreçleri ve bunların etkileşimlerini de içeren bir bilgi güvenliği yönetim sistemi kurmalı, uygulamalı, sürdürmeli ve sürekli iyileştirmelidir.

2. LİDERLİK

Liderlik ve Bağlılık

Üst yönetim, bilgi güvenliği yönetim sistemi ile ilgili olarak liderlik ve bağlılığı şu şekilde göstermelidir:

a) Bilgi güvenliği politikasının ve bilgi güvenliği hedeflerinin oluşturulmasını ve kuruluşun stratejik yönü ile uyumlu olmasını sağlamak;

b) Bilgi Güvenliği Yönetim Sistemi gereksinimlerinin kuruluşun süreçlerine entegrasyonunu sağlamak;

c) Bilgi Güvenliği Yönetim Sistemi için ihtiyaç duyulan kaynakların mevcut olmasını sağlamak;

d) Etkin bilgi güvenliği yönetiminin ve bilgi güvenliği yönetim sistemi gerekliliklerine uyumun önemini iletmek;

e) Bilgi Güvenliği Yönetim Sistemi'nin amaçlanan sonuç(lar)a ulaşmasını sağlamak;

f) Bilgi Güvenliği Yönetim Sistemi'nin etkinliğine katkıda bulunmaları için kişileri yönlendirmek ve desteklemek;

g) Sürekli iyileştirmeyi teşvik etmek; ve

h) Sorumluluk alanlarına uygulandığı için liderliklerini göstermek amacıyla diğer ilgili yönetim rollerini desteklemek.

Politika

Üst yönetim, aşağıdakileri içeren bir bilgi güvenliği politikası oluşturmalıdır:

a) Kuruluşun amacına uygun;

b) Bilgi güvenliği hedeflerini içeren veya bilgi güvenliği hedeflerinin belirlenmesi için çerçeve sağlayan;

c) Bilgi güvenliği ile ilgili uygulanabilir gerekliliklerı yerine getirme taahhüdünü içeren;

d) Bilgi Güvenliği Yönetim Sisteminin sürekli iyileştirilmesi taahhüdünü içeren.

Bilgi güvenliği politikası yazılı doküman olarak mevcut olmalıdır. Bunun yanında kuruluş içinde iletişim kurularak, uygun şekilde ilgili taraflara açık bir şekilde oluşturulmalıdır.

Yönetimsel roller, sorumluluklar ve yetkiler

Üst yönetim, bilgi güvenliği ile ilgili rollere ilişkin sorumluluk ve yetkilerin kurum içinde atanmasını ve iletilmesini sağlamalıdır. Üst yönetim, aşağıdakiler için sorumluluk ve yetki verir:

a) Bilgi Güvenliği Yönetim Sistemi'nin 27001 standardının gerekliliklerine uygun olması;

b) Bilgi Güvenliği Yönetim Sistemi'nin performansının üst yönetime raporlanması.

Üst yönetim, kuruluş içinde bilgi güvenliği yönetim sisteminin performansının raporlanması için sorumlu ve yetkililer de atayabilir.

3. PLANLAMA

Riskleri ve fırsatları ele almak için yaptırımlar

Kuruluş, bilgi güvenliği yönetim sistemini planlarken, kapsamını ve ihtiyaçlarını göz önünde bulundurmalı ve ele alınması gereken riskleri ve fırsatları belirlemelidir:

a) Bilgi Güvenliği Yönetim Sisteminin amaçlanan sonuç(lar)ına ulaşabilmesini sağlamak;

b) İstenmeyen etkileri önlemek veya azaltmak;

c) Sürekli iyileştirme elde etmek.

Kuruluş şunları planlamalıdır:

a) Bu riskleri ve fırsatları ele almak için eylemler;

b) Eylemleri bilgi güvenliği yönetim sistemi süreçlerine entegre etmek ve uygulamak;

c) Bu eylemlerin etkinliğini değerlendirmek.

Bilgi güvenliği risk değerlendirmesi

Kuruluş, aşağıdakileri içeren bir bilgi güvenliği risk değerlendirme süreci tanımlamalı ve uygulamalıdır:

1) Aşağıdakileri içeren bilgi güvenliği risk kriterlerini belirler ve sürdürür:

a) Risk kabul kriterleri;

b) Bilgi güvenliği risk değerlendirmeleri gerçekleştirme kriterleri;

2) Tekrarlanan bilgi güvenliği risk değerlendirmelerinin tutarlı, geçerli ve karşılaştırılabilir sonuçlar üretmesini sağlar;

3) Bilgi güvenliği risklerini tanımlar:

a) Bilgi Güvenliği Yönetim Sistemi kapsamında bilginin gizlilik, bütünlük ve kullanılabilirlik kaybı ile ilişkili riskleri belirlemek için bilgi güvenliği risk değerlendirme sürecini uygulamasını;

b) Risk sahiplerini belirlemek;

4) Bilgi güvenliği risklerini analiz eder:

a) Tanımlanan bilgi güvenliği risklerinin gerçekleşmesi durumunda ortaya çıkabilecek olası sonuçları değerlendirmek;

b) Tanımlanan bilgi güvenliği risklerin gerçekçi bir şekilde ortaya çıkma olasılığını değerlendirmek;

c) Risk seviyelerini belirlemek;

5) Bilgi güvenliği risklerini değerlendirir:

a) Risk analizi sonuçlarını;

b) Analiz edilen risklerin giderilmesi için önceliklendirilme yapılması.

Kuruluş, bilgi güvenliği risk değerlendirme süreci hakkında yazılı belge halindeki bilgileri muhafaza etmelidir.

Bilgi güvenliği risklerinin giderilmesi

Kuruluş, aşağıdakiler için bir bilgi güvenliği risk işleme süreci tanımlamalı ve uygulamalıdır:

a) Risk değerlendirme sonuçlarını dikkate alarak uygun bilgi güvenliği risk giderme seçeneklerini seçmek;

b) Seçilen bilgi güvenliği risk işleme seçeneğini/seçeneklerini uygulamak için gerekli tüm kontrolleri belirlemek;

c) Gerekli kontrollerin ihmal edilmediğini doğrulamak;

d) Aşağıdakileri içeren bir Uygulanabilirlik Beyanı oluşturmak:

1) Gerekli kontroller;

2) Dahil edilmeleri için gerekçeler;

3) Gerekli kontrollerin uygulanıp uygulanmadığı;

4) Kontrollerinden herhangi birinin hariç tutulmasının gerekçesi.

e) Bir bilgi güvenliği risk giderme planı formüle etmek;

f) Risk sahiplerinin bilgi güvenliği risk giderme planının onayını ve kalan bilgi güvenliği risklerinin kabul edilmesini sağlamak.

Kuruluş, bilgi güvenliği riskinin ele alınma süreci hakkında yazılı belge haline getirilmiş bilgileri muhafaza etmelidir.

Güvenlik hedefleri ve planları

Kuruluş, ilgili fonksiyon ve seviyelerde bilgi güvenliği hedefleri oluşturmalıdır.

Bilgi güvenliği hedefleri:

a) Bilgi güvenliği politikası ile tutarlı olmalı;

b) Ölçülebilir olmalı (uygulanabilirse);

c) Uygulanabilir bilgi güvenliği gereksinimlerini ve risk değerlendirmesi ve risk giderme adımlarından elde edilen sonuçları dikkate almalı;

d) İzlenmeli;

e) İlgili paydaşlarla iletişim kurulmalı;

f) Uygun şekilde güncellenmeli;

g) Yazılı belge halinde mevcut olmalıdır.

Kuruluş, bilgi güvenliği hedefleri hakkında yazılı belgeleri muhafaza etmelidir. Kuruluş, bilgi güvenliği hedeflerine nasıl ulaşılacağını planlarken şunları belirlemelidir:

a) Ne yapılacak;

b) Hangi kaynaklara ihtiyaç duyulacak;

c) Kim sorumlu olacak;

d) Ne zaman tamamlanacak;

e) Sonuçlar nasıl değerlendirilecek.

Kuruluş, bilgi güvenliği yönetim sisteminde değişiklik yapılması gerektiğini belirlediğinde, değişiklikler de planlı bir şekilde gerçekleştirilmelidir.

4. DESTEK

Kuruluş, bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için ihtiyaç duyulan kaynakları belirlemeli ve sağlamalıdır. Bu amaçla kuruluş:

a) Kontrolü altında iş yapan kişinin/kişilerin bilgi güvenliği performansını etkileyen gerekli yeterliliklerini belirlemeli;

b) Bu kişilerin uygun eğitim, öğretim veya deneyim temelinde yetkin olmalarını sağlamalı;

c) Uygulanabilir olduğunda, gerekli yetkinliği elde etmek için önlemler almak ve alınan önlemlerin etkinliğini değerlendirmeli;

d) Yetkinlik kanıtı olarak uygun belgelenmiş bilgileri saklamalıdır.

Bu kısımda yapılabilecek uygulamalar arasında mevcut çalışanlara eğitim verilmesi, mentorluk yapılması veya yeniden atanması veya yetkili kişilerin işe alınması veya sözleşme yapılması sayılabilir. Kuruluşun kontrolü altında iş yapan kişilerin; Bilgi Güvenliği Politikasının, gelişmiş bilgi güvenliği performansının faydaları da dahil olmak üzere bilgi güvenliği yönetim sisteminin kuruluş etkinliğine katkılarının ve Bilgi Güvenliği Yönetim Sistemi gerekliliklerine uymamanın sonuçlarının farkında olmaları gerekmektedir. Bunun yanında kuruluş, bilgi güvenliği yönetim sistemi ile ilgili ne konuda, ne zaman, kiminle ve nasıl iletişim kurulacağına dair iç ve dış iletişim ihtiyacını da belirlemelidir.

Dokümantasyon

Kuruluşun bilgi güvenliği yönetim sistemi bu standardın gerektirdiği bilgileri yazılı olarak muhafaza etmeli ve Bilgi Güvenliği Yönetim Sistemi'nin etkinliği için gerekli olduğu belirlenen

her şeyi yazılı olarak belgelemelidir. Bir bilgi güvenliği yönetim sistemi için dokümante edilen bilgilerin kapsamı, aşağıdaki nedenlerden dolayı bir kuruluştan diğerine farklılık gösterebilir:

a) Organizasyonun büyüklüğü ve faaliyetleri, süreçleri, ürünleri ve hizmetleri;

b) Süreçlerin karmaşıklığı ve etkileşimleri;

c) Kişilerin yeterliliği.

Yazılı bilgileri oluştururken ve güncellerken, kuruluş kendi sistemine uygun bir şekilde aşağıdaki özellikleri kullanmalıdır:

a) Kimlik ve açıklama (örn. başlık, tarih, yazar veya referans numarası);

b) Biçim (ör. dil, yazılım sürümü, grafikler) ve ortam (ör. kağıt, elektronik);

c) Uygunluk ve yeterlilik için gözden geçirme ve onaylama.

Bilgi güvenliği yönetim sistemi ve bu doküman tarafından gerekli görülen dokümante edilmiş bilgilerin, ihtiyaç duyulan yerde/zamanda kullanıma hazır olması ve uygunluğu ile yeterince korunup kurunmadığı (örn. gizlilik kaybından, uygunsuz kullanımdan veya bütünlük kaybından) kontrol edilmelidir.

Dokümante edilmiş bilgilerin kontrolü için, kuruluş, uygun olduğu şekilde, aşağıdaki faaliyetleri ele almalıdır:

a) Dağıtım, erişim, erişim ve kullanım;

b) Okunabilirliğin korunması da dahil olmak üzere saklama ve koruma;

c) Değişikliklerin kontrolü (örn. sürüm kontrolü);

d) Alıkoyma ve elden çıkarma.

Bilgi güvenliği yönetim sisteminin planlanması ve işletilmesi için gerekli olduğu kuruluş tarafından belirlenen dokümante edilmiş dış kaynaklı bilgiler, uygun olarak tanımlanmalı ve kontrol edilmelidir. Erişim, yalnızca belgelenmiş bilgileri görüntüleme izni veya belgelenmiş bilgileri görüntüleme ve değiştirme izni ve yetkisi vb. ile ilgili bir karar anlamına da gelebilir.

5. İŞLETİM

Kuruluş, gereksinimleri karşılamak için gerekli süreçleri planlamalı, uygulamalı ve kontrol etmeli ve Planlama başlığında belirlenen eylemleri uygulamak için gerekli kriterleri belirlemeli ve kriterlere uygun olarak süreçlerin kontrolünü sağlamalıdır. Kuruluş, planlanan değişiklikleri kontrol etmeli ve istenmeyen değişikliklerin sonuçlarını gözden geçirmeli, gerektiğinde olumsuz etkileri azaltmak için harekete geçmelidir. Kuruluş, bilgi güvenliği yönetim sistemi ile ilgili olarak dışarıdan sağlanan süreçlerin, ürünlerin veya hizmetlerin kontrol edilmesini de sağlamalıdır.

Kuruluş, planlama adımındaki risk değerlendirmesinde belirlenen kriterleri dikkate alarak, planlanan aralıklarla veya önemli değişiklikler önerildiğinde/meydana geldiğinde bilgi güvenliği risk değerlendirmeleri yapmalıdır. Kuruluş, bilgi güvenliği risk değerlendirmelerinin sonuçlarına ilişkin dokümante edilmiş bilgileri muhafaza etmelidir.

Kuruluş, bilgi güvenliği risk giderme planını uygulamalıdır. Kuruluş, bilgi güvenliği risk giderme işlemlerinin sonuçlarına ilişkin belgelenmiş bilgileri muhafaza etmelidir.

6. PERFORMANS DEĞERLENDİRME

Kuruluş izleme, ölçme, analiz ve değerlendirme amacıyla şunları belirlemelidir:

a) Bilgi güvenliği süreçleri ve kontrolleri de dahil olmak üzere izlenmesi ve ölçülmesi gerekenler;

b) Geçerli sonuçları sağlamak için uygun olduğu şekilde izleme, ölçme, analiz ve değerlendirme yöntemleri. Seçilen yöntemlerin geçerli sayılabilmesi için karşılaştırılabilir ve tekrarlanabilir sonuçlar üretmesi gerekir;

c) İzleme ve ölçmenin ne zaman yapılacağı;

d) Kimin izleyip ölçeceği;

e) İzleme ve ölçme sonuçlarının analiz ve değerlendirmeye tabi tutulacağı zaman;

f) Sonuçların analiz edilmesi ve değerlendirilmesi.

Dokümante edilmiş bilgiler, sonuçların kanıtı olarak tutulmalıdır. Kuruluş, bilgi güvenliği performansını ve bilgi güvenliği yönetim sisteminin etkinliğini de değerlendirmelidir.

İç denetim

Kuruluş, bilgi güvenliği yönetim sisteminin aşağıdakileri yapıp yapmadığı konusunda bilgi sağlamak için planlanan aralıklarla iç denetimler yapmalıdır:

a) Gereksinimlere uygunluk

1) Kuruluşun bilgi güvenliği yönetim sistemi için kendi gereksinimleri;

2) Bu standardın gereklilikleri;

b) Etkin bir şekilde uygulanıyor ve sürdürülüyor mu.

Kuruluş, sıklığı, yöntemleri, sorumlulukları, planlama gereklilikleri ve raporlama dahil olmak üzere bir denetim programı planlamalı, oluşturmalı, uygulamalı ve sürdürmelidir. Kuruluş, iç denetim program(lar)ını oluştururken, ilgili süreçlerin önemini ve önceki denetimlerin sonuçlarını göz önünde bulundurmalıdır. Kuruluş:

a) her denetim için denetim kriterlerini ve kapsamını tanımlamalı;

b) denetçileri seçmeli ve denetim sürecinin tarafsızlığını ve tarafsızlığını sağlayan denetimler yapmalı;

c) Denetim sonuçlarının ilgili yönetime raporlanmasını sağlamalıdır.

Belgelendirilmiş bilgiler, denetim program(lar)ının ve denetim sonuçlarının uygulandığına dair kanıt olarak sunulmalıdır.

Yönetimin Değerlendirmesi

Üst yönetim, kuruluşun bilgi güvenliği yönetim sistemini, uygunluğunun, yeterliliğinin ve etkinliğinin sürekliliğini sağlamak için planlı aralıklarla değerlendirme yapar. Yönetimin değerlendirmesi aşağıdakilerin dikkate alınmasını içermelidir:

a) Önceki yönetim incelemelerinden elde edilen eylemlerin durumu;

b) Bilgi güvenliği yönetim sistemi ile ilgili dış ve iç konulardaki değişiklikler;

c) Bilgi Güvenliği Yönetim Sistemi ile ilgili ilgili tarafların ihtiyaç ve beklentilerindeki değişiklikler;

d) Eğilimler de dahil olmak üzere bilgi güvenliği performansı hakkında geri bildirim:

1) Uygunsuzluklar ve düzeltici faaliyetler;

2) İzleme ve ölçüm sonuçları;

3) Denetim sonuçları;

4) Bilgi güvenliği hedeflerinin yerine getirilmesi;

e) İlgili taraflardan geri bildirim;

f) Risk değerlendirme sonuçları ve risk tedavi planının durumu;

g) Sürekli iyileştirme fırsatları.

Yönetimin değerlendirme sonuçları, sürekli iyileştirme fırsatları ve bilgi güvenliği yönetim sisteminde herhangi bir değişiklik ihtiyacı ile ilgili kararları içermelidir. Dokümante edilmiş bilgiler, yönetimin değerlendirme sonuçlarının kanıtı olarak sunulmalıdır.

7. GELİŞTİRME

Kuruluş, bilgi güvenliği yönetim sisteminin uygunluğunu, yeterliliğini ve etkinliğini sürekli iyileştirmelidir. Bir uygunsuzluk meydana geldiğinde, kuruluş uygunsuzluğa tepki vermeli ve bu uygunsuzluğu gidermek için gerekli kontrolleri yapmalı, düzeltmek için harekete geçmeli ve ortaya çıkan sonuçlarla başa çıkabilmelidir. Uygunsuzluğun nedenlerini ortadan kaldırmak için harekete geçerken, başka bir yerde tekrarlanmaması veya ortaya çıkmaması için uygunsuzluk gözden geçirilmeli, nedenleri belirlenmeli ve benzer uygunsuzlukların mevcut olup olmadığı veya potansiyel olarak ortaya çıkıp çıkamayacağı belirlenmelidir.

Bunun yanında gerekli herhangi bir eylemi uygulamaktan geri durulmamalı, alınan herhangi bir düzeltici faaliyetin etkinliğini gözden geçirmeli ve gerekirse bilgi güvenliği yönetim sisteminde değişiklikler yapılmalıdır. Düzeltici faaliyetler, karşılaşılan uygunsuzlukların etkilerine uygun olacaktır. Yapılan işlemlere dair belgelenmiş bilgiler uygunsuzlukların niteliği ve daha sonra alınan önlemler ile herhangi bir düzeltici eylemin sonuçlarının kanıtı olarak sunulmalıdır.

BÖLÜM ÖZETİ

Bilgi Güvenliği Yönetim Sistemi (BGYS), kuruluşların bilgi güvenliğini sağlamak için ISO/IEC 27001 standardına dayanan bir çerçevedir. BGYS, bir bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için gereklilikleri belirler.

BGYS, bir kuruluşun iç ve dış bağlamlarını, ilgili taraflarını ve bilgi güvenliği risklerini belirleyerek başlar. Üst yönetim, BGYS ile ilgili liderlik ve bağlılığını göstererek politikaların oluşturulması, kaynak sağlanması ve sürekli iyileştirmeyi teşvik etme sorumluluğunu üstlenir. Bilgi güvenliği politikalarının oluşturulması ve sürdürülmesi, yönetim tarafından yürütülmelidir. Ayrıca, bilgi güvenliği ile ilgili rollerin ve sorumlulukların atanması ve iletilmesi gerekmektedir.

Planlama aşamasında, bilgi güvenliği risklerinin belirlenmesi, analizi ve değerlendirilmesi yapılır. Belirlenen risklere yönelik uygun önlemler seçilir ve uygulanır. Bilgi güvenliği hedefleri belirlenerek bu hedeflere ulaşmak için planlar oluşturulur.

BGYS'nin destek mekanizmaları arasında dokümantasyon süreci yer alır. Gereklilikler belgelendirilmeli ve dokümantasyon kontrol edilmelidir. Ayrıca, çalışanların bilgi güvenliği performansını artırmak amacıyla gerekli eğitim ve farkındalık çalışmaları sağlanmalıdır.

İşletim aşamasında, bilgi güvenliği süreçleri ve kontrolleri izlenmeli, ölçülmeli, analiz edilmeli ve değerlendirilmelidir. Planlanan aralıklarla iç denetimler gerçekleştirilerek sonuçları raporlanmalıdır.

Performans değerlendirmesi kapsamında, üst yönetim tarafından BGYS'nin uygunluğu, yeterliliği ve etkinliği değerlendirilmelidir. Bu değerlendirme, sürekli iyileştirme fırsatlarını belirlemek açısından önemlidir.

Geliştirme sürecinde, BGYS'nin sürekli iyileştirilmesi için kuruluş tarafından belirlenen fırsatlar uygulanmalıdır. BGYS'nin temel amacı, kuruluşların bilgi varlıklarını korumasını sağlamak ve bu alanda sürekli iyileştirmeler yapmasına rehberlik etmektir. Kuruluşların bu unsurları nasıl uygulayacağı, büyüklüklerine, yapılarına ve faaliyet gösterdikleri sektöre bağlı olarak değişiklik gösterebilir.

GÖZDEN GEÇİRELİM

1. **Bilgi Güvenliği Yönetim Sistemi (BGYS) nedir?**
   a) Bir kuruluşun bilgi güvenliğini sağlamak için rehberlik eden bir çerçeve
   b) Bir bilgisayar güvenlik yazılımı
   c) Bir ağ güvenlik protokolü
   d) Bir şifreleme algoritması
   e) Bir veri tabanı yönetim sistemi

2. **ISO/IEC 27001 standardı neyi açıklar?**
   a) Bilgi güvenliği politikalarının oluşturulması
   b) Bir bilgi güvenliği yönetim sistemi kurma, uygulama, sürdürme ve sürekli iyileştirme için gereklilikleri
   c) Risk değerlendirme süreçleri
   d) Bilgi güvenliği hedeflerinin belirlenmesi
   e) Bilgi güvenliği risklerinin giderilmesi

3. **BGYS'nin temel amacı nedir?**
   a) Veri tabanlarını yönetmek
   b) Ağ güvenliğini sağlamak
   c) Bir kuruluşun bilgi varlıklarını korumasını ve bu alanda sürekli iyileştirmeler yapmasını sağlamak
   d) Kullanıcı kimlik doğrulaması yapmak
   e) İnternet trafiğini izlemek

4. **BGYS'nin kuruluşun hangi yönlerini dikkate alması beklenir?**
   a) Yalnızca teknolojik yönler
   b) Yalnızca finansal yönler
   c) İç ve dış bağlamlar, ilgili taraflar ve bilgi güvenliği riskleri
   d) Yalnızca yasal yönler
   e) Yalnızca operasyonel yönler

5. **Bilgi güvenliği yönetim sistemi kapsamında, bilginin gizliliği, bütünlüğü ve kullanılabilirliği ile ilişkili riskler nasıl belirlenir ve değerlendirilir?**

6. **Bilgi güvenliği yönetim sisteminin sürekli iyileştirilmesi için hangi adımlar izlenmelidir ve bu süreçte liderliğin rolü nedir?**

Yanıt Anahtarı: 1-A, 2-B, 3-C, 4-C

Kaynakça

ISO. (2023, 8). Retrieved from https://www.iso.org/standard/27001

ISO. (2023, 9). Retrieved from https://www.iso.org/standard/65694.html