ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi

Farkındalık Eğitimi

Alper Öztürk
ISO/IEC 27001:2013 Başdenetçi

Hoşgeldiniz

- Telefonlar-Eğitimin bölünmesine sebebiyet verilmemeli
- Kayıt cihazları-Sınıf içinde bulundurulmamalı
- Öğle yemeği/Aralar – Zamanında dönülmeli
- Eğitimin süresi

Tanışma

İsim/Soyisim

Meslek/Mezun Olunan Okul

Çalıştığı Birim/Konum

Yönetim Sistemleri Bilgisi/Deneyimi

TS ISO/IEC 27001 bilgisi

Eğitimden beklentiler

Giriş

International Organization for Standardization

International Electrotechnical Commission

Tanımlar

Bilgi

- İnsan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bili, malumat (isim,TDK)

- Kurallardan yararlanarak kişinin veriye yönelttiği anlam (bilişim,TDK)

- Kuruluştaki diğer varlıklar gibi, kuruluş için önem taşıyan ve bu nedenle de en iyi şekilde korunması gereken bir varlık


Siber Saldırılar
•DDos
Yönetim sistemi Aksamaları
•Kayıt yetersizliği
•Eğitim Eksikliği
•Prosedür ihlali
Bilgi sistemi Bozulmaları
•Kötü Tasarım
•Yazılım hatası
•Eksik yedekleme
•,,,,
BİLGİ
İnsan faktörleri
•İşleme Hatası
•Bakım hatası
•Kötü niyetli çalşanlar
Çevresel
•Terör
•Patlamalar
•…
Doğal Afetler
•Sel
•Yangın
•Deprem

Tanımlar

Bilgi :

Bilgi hangi şekli alırsa alsın ya da hangi ortamla iletilirse iletilsin, mutlaka uygun bir şekilde korunmalı.

Tanımlar

Bilgi Ortamları

- Kağıt üzerine basılmış, yazılmış
- Elektronik olarak saklanan
- Kurumsal videolarda gösterilen
- Söyleşiler sırasında sözlü olarak aktarılan
- Kuruluş çalışanlarının özlük bilgisi

Tanımlar

- **Güvenlik:** İç veya dış kaynaklı, kasıtlı veya kasıtsız olabilecek tehditlerin kabul edilebilir seviyeye çekilmesi

- **Bilgi güvenliği**: kuruluştaki işlerin sürekliliğinin sağlanması, işlerde meydana gelebilecek aksaklıkların azaltılması ve yatırımlardan gelecek faydanın artırılması için bilginin geniş çaplı tehditlerden korunmasını sağlar.

Tanımlar

- **Varlık (Asset)**
  Kuruluş için değeri olan herhangi bir şey.
- **Bilgi Varlığı (Information Asset)**
  - Kuruluş için değer ifade eden herhangi değerli bilgi veya veri (TS ISO/IEC 27000)

Varlık örnekleri:

- bilgi (satış bilgilerini içeren dosyalar, ürün bilgileri, veritabanları)
- donanım (kişisel bilgisayarlar, yazıcılar, sunucular)
- yazılım (işletim sistemleri, geliştirilen uygulamalar, ofis programları)
- haberleşme cihazları (telefonlar, hatlar, kablolar, modemler)
- dokümanlar(stratejik toplantıların tutanakları, sözleşmeler)
- üretilen mallar ,servisler
- mali değerler (çekler, para, fonlar)
- personel
- kurumun prestiji/imajı

Tanımlar

Uygulanabilirlik bildirgesi (Statement of applicability SOA)

Kuruluşun BGYS' si ile ilgili ve uygulanabilir kontrol amaçlarını ve kontrolleri açıklayan dokümante edilmiş bildirge.

Not - *Kontrol amaçları ve kontroller, risk değerlendirme ve risk işleme süreçlerinin sonuçları ve çıkarımlarını, yasal ve düzenleyici gereksinimleri, anlaşma yükümlülüklerini ve kuruluşun bilgi güvenliği için iş gereksinimlerini temel alır.*

BİLGİ GÜVENLİĞİ NEDİR? NEDEN ÖNEMLİDİR?

KURUMSAL BİLGİ:

Bilgi bir kurumun iş yapabilmesi için sahip olduğu önemli varlıkların en başında gelir. Kurum sahip olduğu bilgiyi derler, üretir, işler, saklar, satar, diğer kişi ve kurumlarla paylaşır. Bilgi;

- Basılı halde kağıtlarda
- Elektronik dosyalarda
- Veritabanlarında
- Telefon konuşmalarında
- Faks mesajlarında
- Masalarda, dolaplarda,
- İletim hatlarında,
- En önemlisi de kurum çalışanlarının akıllarında bulunur.

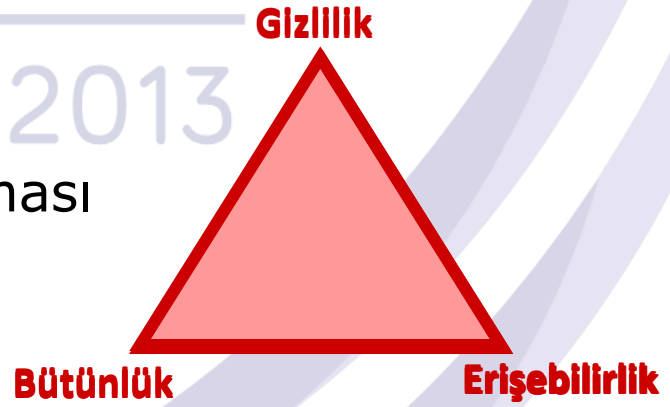
Bilgi hangi ortamda olursa olsun gerektiği şekilde korunmalıdır.

BİLGİ GÜVENLİĞİ NEDİR?

Bilgi güvenliği bilginin tehditlere karşı uygun şekilde korunması demektir.

Bilginin korunması;

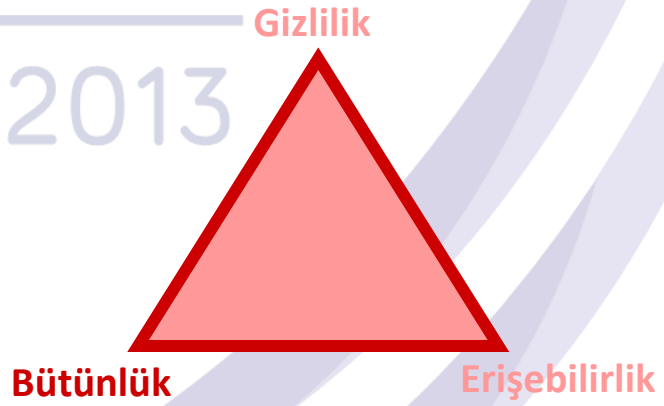
- Gizliliğinin gözetilmesi,
- Bütünlüğünün garanti altında tutulması
- Lazım olduğunda erişilebilir durumda olması anlamına gelir.



BİLGİNİN BÜTÜNLÜĞÜ

Bilginin bütünlüğü;

- **İçeriğinin doğru,**
- **Güncel ve geçerli olduğu,**
- **Yetkisiz kişiler tarafından değiştirilmediği anlamına gelir.**



BİLGİNİN GİZLİLİĞİ

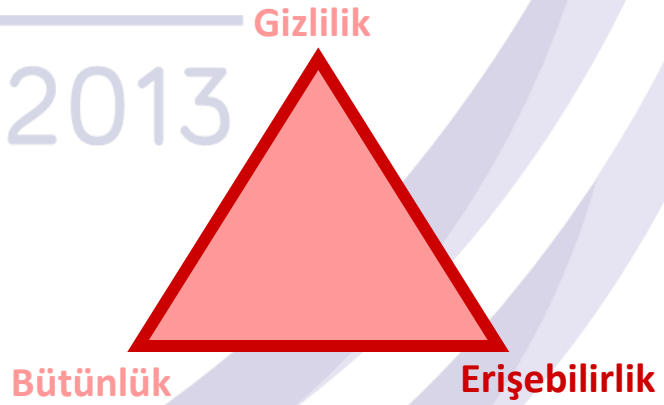
Bilgi gizliliğinin gözetilmesi;

- **Bilginin sadece yetkili kişiler tarafından erişilebilir durumda olması,**
- **Bilgi gizliliğinin gözetilmesi**
- **Yetkisiz kişilerin erişiminin engellenmesidir.**

BİLGİNİN ERİŞEBİLİRLİĞİ

Bilgi gizliliğinin erişilebilirliği;

- **Bilginin olması gereken yerde ve gerektiğinde kullanıma hazır olduğunun güvence altında tutulmasıdır.**



BİLGİ GÜVENLİĞİ NEDEN ÖNEMLİDİR?

Bilgi uygun şekilde korunmazsa;

- **Gizli bilgiler açığa çıkabilir**
- **Bilginin içeriğinde yetkisiz kişiler tarafından değişiklik yapılabilir**
- **Bilgiye erişim mümkün olmayabilir.**

Kullanıcı hataları veya kötü niyetli girişimler bu sonuçları doğurabilir. Bu olayların izlenebilirliği de önemli bir konudur.

BİLGİ GÜVENLİĞİ NEDEN ÖNEMLİDİR?

Bilgi uygun şekilde korunmazsa;

- **Kuruma ait gizli ve hassas bilgiler**
- **Kurum işlerliğini sağlayan bilgi ve süreçler**
- **Kurumun ismi, güvenilirliği, itibarı**
- **Üçüncü şahıslar tarafından emanet edilen bilgiler**
- **Ticari, teknolojik, adli bilgiler**
- **İş sürekliliği <u>zarar görebilir.</u>**

BİLGİ GÜVENLİĞİ NEDEN ÖNEMLİDİR?

Bilgi uygun şekilde korunmazsa;

- **Ülke çıkarının zarar görmesi,**
- **İş sürekliliğinin aksaması,**
- **Kaynak tüketimi,**
- **Müşteri mağduriyeti ve memnuniyetsizliği,**
- **Üçüncü şahıslara yapılan saldırılardan sorumlu tutulma,**
- **Ulusal / kurumsal itibar kaybı,**
- **Yasal yaptırımlar ve tazminatlar gibi olumsuz sonuçlarla karşılaşılabilir.**

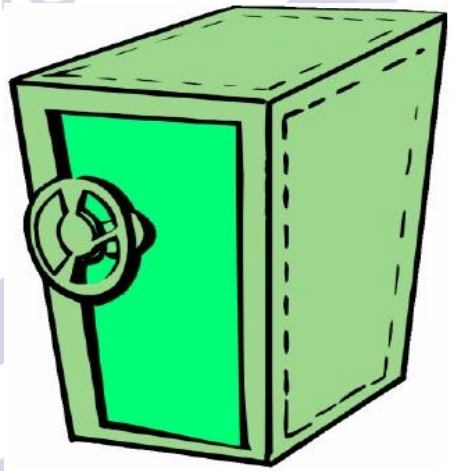
NE TÜR TEHDİTLER VAR?

- Servis dışı bırakma saldırıları
- Kimlik bilgilerinizin ele geçirilerek kötü amaçla kullanılması
- Virüs, kurtçuk, trojan saldırıları
- Bilgisayarınızın başkası tarafından ele geçirilerek suç işlenmesi
- Bilgisayarınızın kurum ağına giriş kapısı olarak kullanılması
- Web sayfası içeriğini değiştirme
- İzinsiz kaynak kullanımı
- Kuruma ait bilgisayardan dışarıya yapılabilecek saldırıla

KURUMSAL BİLGİ GUVENLIGI NASIL SAĞLANIR?

- Kurum çapında bilgi güvenliği farkındalığının yaratılması
- Uygun kullanım, politikalar, prosedürler...
- Kurum organizasyonu; kişiler, roller, uygun atamalar ve iş dağılımı,
- Güvenlik yazılım ve donanımları

Bilgi güvenliği, kurum gereksinimleriyle örtüşecek şekilde ve sistematik bir yaklaşımla ele alınmalıdır.



- Bilgi güvenliği yönetiminin de diğer yönetsel süreçlerden biri olarak kurgulanması,
- Gerekli atamaların yapılması ve kaynak tahsisinin sağlanması,
- Kurum çapında farkındalık ve bilinç yaratılması,
- Güvenlik ihlallerinin değerlendirilmesi,
- Yaptırımların uygulanmasıdır.

BİLGİ GÜVENLİĞİ GEREKSİNİMLERİ NASIL BELİRLENİR?

Kurumsal güvenlik gereksinimleri belirlenirken bazı temel kaynaklara başvurulur:

- **Risk Analizi Sonuçları**
- **Yasal yükümlülükler, yurt içi ve yurt dışı ticari iş bağlantıları nedeniyle yapılan sözleşmeler, devlet kurumlarıyla karşılıklı anlaşmalar vs.**
- **Kurumun işlevlerini destekleyen bilişim sistemleri ile ilgili prensipler ve gereksinimler.**
- **Kurumun daha önce yaşadığı güvenlik olayları**

RİSK ANALİZİ

- Bilgi varlıklarına yönelik tehditler belirlenir.
- Bilgi varlıklarının zayıflıkları (korunmasızlık) gözden geçirilir, tehditlerin bu zayıflıklardan yararlanarak zarar verme olasılığı değerlendirilir.
- Tehditlerin varlıklara olası etkisi değerlendirilir.
- Bu veriler risk hesaplamak için kullanılır ve riskler listelenir.

Bu çalışma kurumun risk ortamını yansıttığı için kuruma özgü sonuçlar verir.

Yasa ve Sözleşmelerle İlgili Yükümlülükler

- Kurumun devlete, diğer kuruluşlara, müşterilerine karşı taahhütleri nelerdir?
- Yasalar ve sözleşmeler neler gerektirmektedir?
- Bilgi güvenliği kontrolleri belirlenirken bu gereksinimler göz önüne alınmalıdır.

(Uluslararası sözleşmeler, ortaklık anlaşmaları, sigorta kanunu, elektronik imza kullanma gerekliliği, 5651 sayılı yasa, kişisel verilerin gizliliği, hasta bilgilerinin gizliliği, şifreli saklama ve iletim gerekliliği vb...)

BT İle İlgili Prensipler ve Gereksinimler

- Bilgi işlem faaliyetleri ve BT altyapısının kurumsal iş hedeflerini karşılamaya uygun olması
- Uygunluk sağlanması gereken BT standartları prensipleri
- BT donanım ve yazılımının yaratacağı yeni güvenlik açıkları

(COBIT, PCI, ITIL vb standartlar, veritabanı şifreleme, kimlik yönetimi, log yönetimi gibi..)

Daha Önce Yaşanan Güvenlik Sorunları

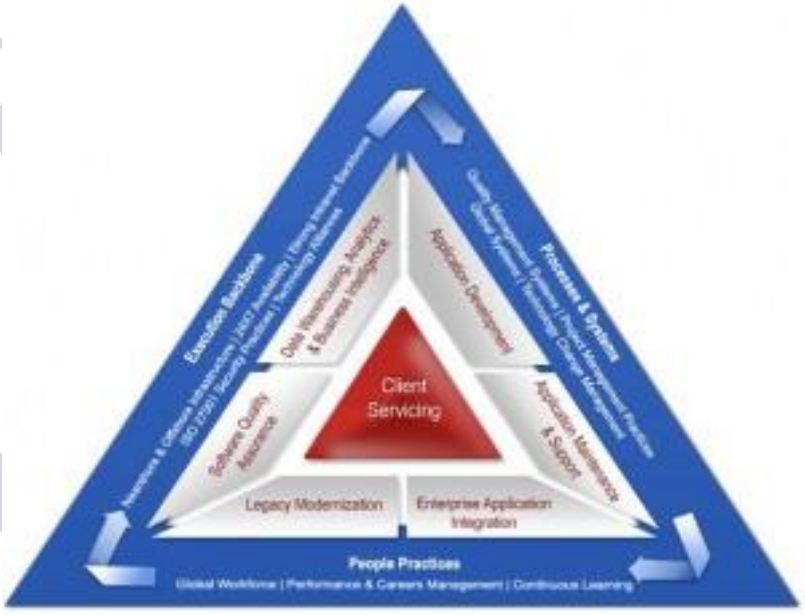
- Kurumda daha önce yaşanan güvenlik olayları, gözlenen güvenlik açıkları,
- Bu olaylardan öğrenerek, tekrarını engellemek için önlemler.

BGYS SÜREÇLERİ NELERDİR?

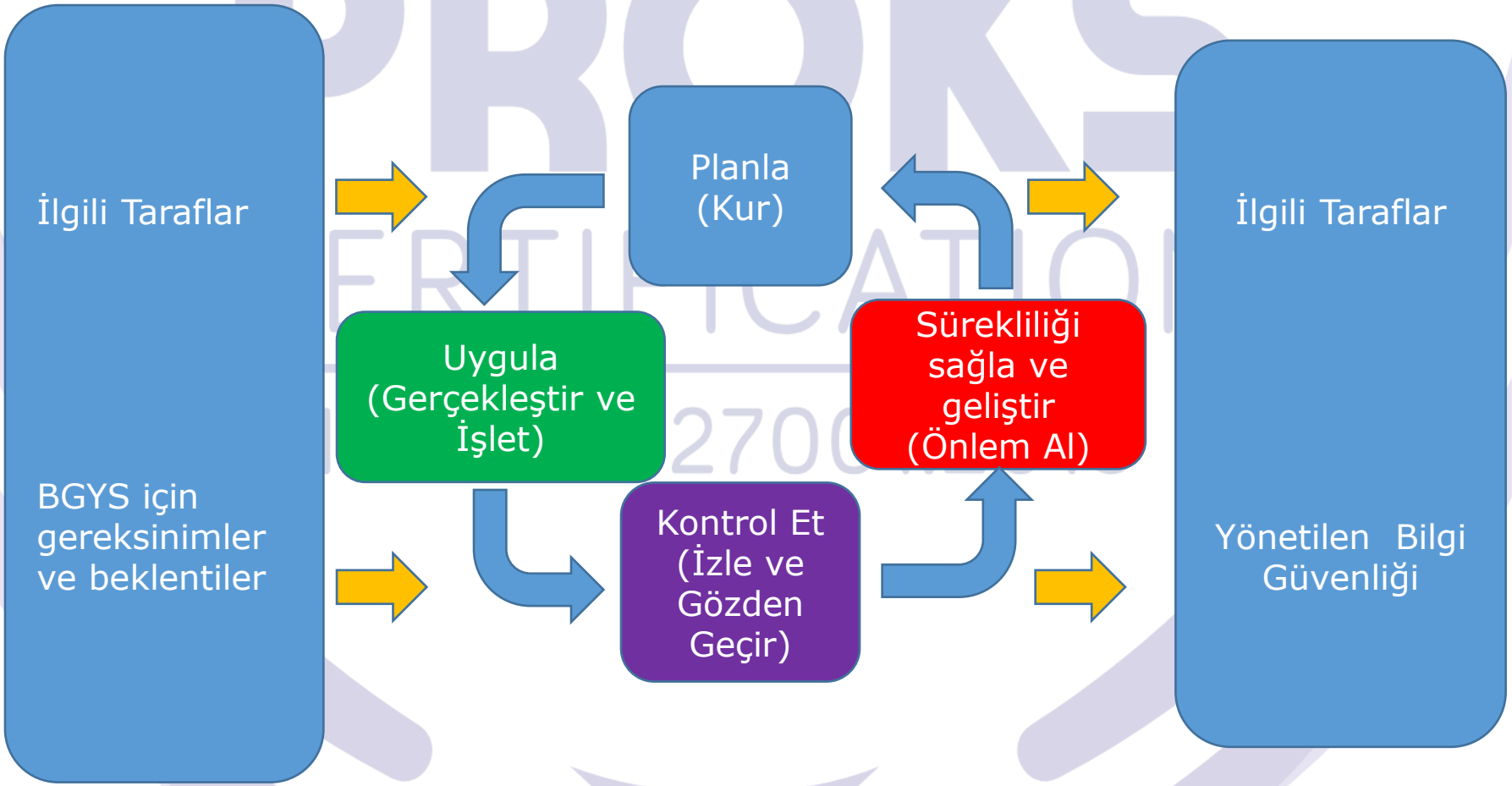
BİLGİ GÜVENLİĞİ YÖNETİMİ NEDİR?

- **Kurumsal iş süreçlerindeki bilgi güvenliği risklerinin tespit edilmesi ve uygun önlemlerle indirgenmesi çalışmasıdır.**

- **Bilgi güvenliği yönetimi sistematik ve döngüsel bir yaklaşımla gerçekleştirilir.**



BGYS Süreçlerine Uygulanan PUKÖ Modeli



BGYS Süreçlerine Uygulanan PUKÖ Modeli

Planla
(BGYS'nin kurulması)

Belirle
Risk yönetimi ve bilgi güvenliği

- BGYS politikası
- BGYS amaçları
- BGYS hedefleri
- BGYS süreçleri ve prosedürleri

BGYS Süreçlerine Uygulanan PUKÖ Modeli

Uygula
(BGYS'nin gerçekleştirilmesi ve işletilmesi)

Gerçekleştir ve İşlet

- BGYS politikası
- BGYS kontrolleri
- BGYS süreçleri
- BGYS prosedürleri

BGYS Süreçlerine Uygulanan PUKÖ Modeli

Kontrol et (BGYS'nin izlenmesi ve gözden geçirilmesi)

Belirle ve yetkilendir

BGYS politikası ve amaçlarına karşılık süreç performansının izlenmesi ve gözden geçirilmesi

Performansın ölçülmesi (uygulanabilen yerlerde)

Sonuçların, gözden geçirilmek üzere yönetime rapor edilmesi

BGYS Süreçlerine Uygulanan PUKÖ Modeli

Önlem al (BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi)

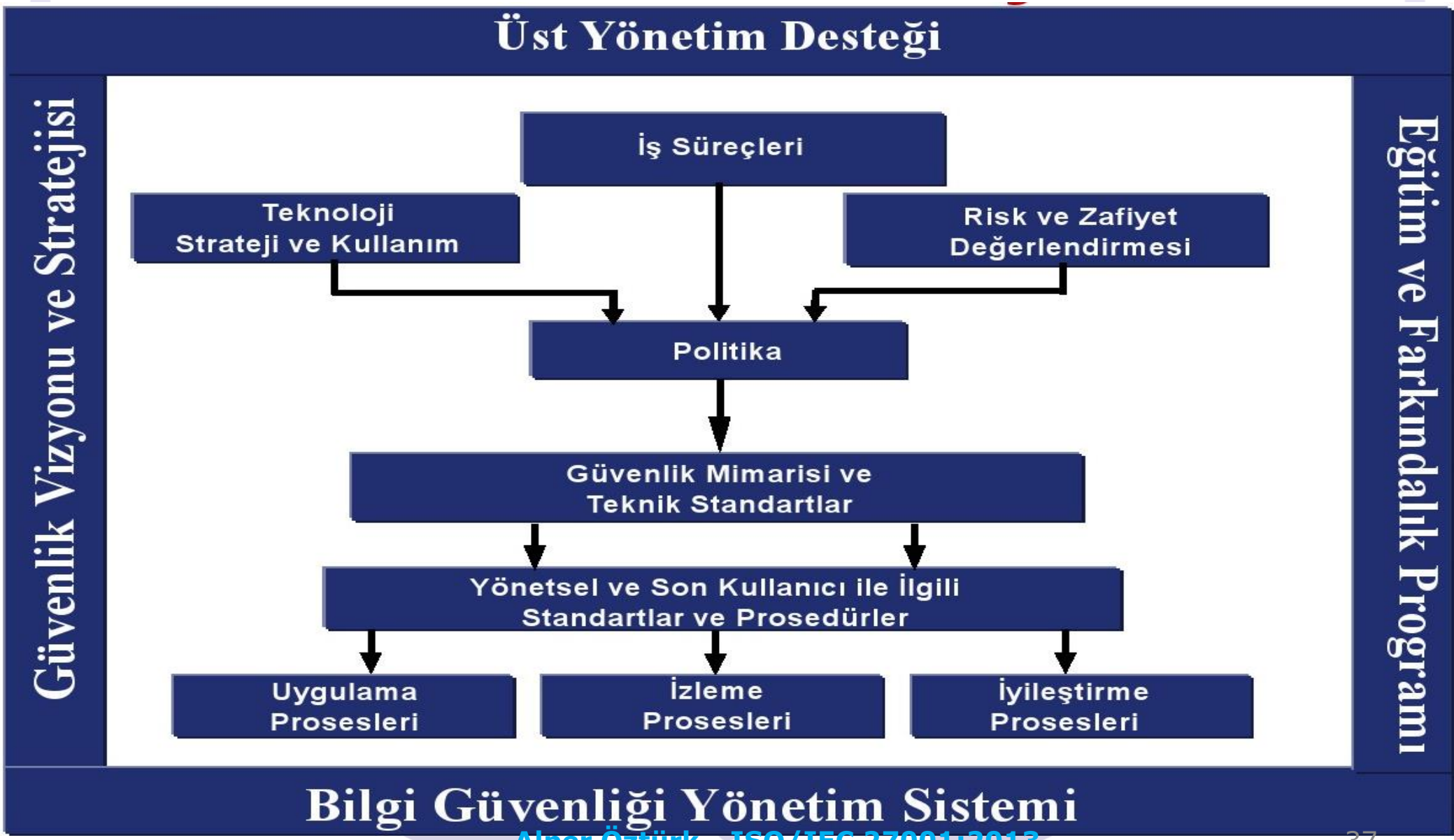
BGYS'nin sürdürülmesi ve iyileştirilmesi

- Yönetimin gözden geçirmesinin sonuçları
- BGYS'nin kapsamının, bilgi güvenliği politikasının ve hedeflerinin yeniden değerlendirilmesi
- Düzeltici faaliyet yapılması

BİLGİ GÜVENLİĞİ YÖNETİMİ SİSTEMİ

- Diğer yönetim sistemleriyle etkileşimli olarak ele alınması gereken bir yönetim sistemidir.
- Kurumsal bilgi güvenliği süreçlerinin planlanması, uygulanması, denetlenmesi ve iyileştirilmesi ile ilgili yöntemler içerir.
- Dokümante edilmiş, işlerliği ve sürekliliği garanti altına alınmış olmalıdır.
- Bilgi Güvenliği teknik değil, yönetsel bir konudur. Bu nedenle BGYS bir İT (Bilgi Teknolojileri) sistemi değildir. Bir Yönetim Sistemidir.
- Kurumsal bir Bilgi Güvenliği Yönetimi Sistemi'nin uluslararası standartlara uygun oluşturulması tavsiye edilir.
- Standartlara uygun oluşturulan sistemler belge almaya adaydır.

BGYS TEMEL BİLEŞEMLERİ



RİSK YÖNETİMİ

RİSK YÖNETİMİ NEDEN ÖNEMLİDİR?

- “%100 güvenlik” mümkün değildir!
- “Sıfır risk” ortamı yoktur ve her zaman yönetilmesi gereken riskler vardır.
- Risk analiziyle ortama özgü riskler anlaşılır.
- Gerekli önlemler (kontroller) bu analiz ışığında belirlenir.
- Kontroller uygulanarak riskler kabul edilir seviyeye indirilir.
- ISO 27001 risk yönetimi tabanlı bir yaklaşımı benimsemiştir.

RİSK YÖNETİMİ NEDEN ÖNEMLİDİR?

- Önemli bir karar verme aracıdır.
- Üst yönetime mevcut güvenlik seviyesi ve hedefe yakınlığı ile ilgili bilgi sağlar, bilgi güvenliği kararlarının verilmesine ışık tutar.
- Kontrolün maliyeti ve faydası arasındaki dengenin kurulabilmesi için yol gösterir.

RİSK ANALİZ TERMİNOLOJİSİ

Varlık : Kurum için değer taşıyan ve korunması gereken her şey varlık olarak tanımlanır. Varlıklar süreç akışları incelenerek belirlenir.

- **Çeşitli ortamlardaki bilgiler**
- **İnsanlar**
- **Kayıtlar**
- **Donanımlar**
- **Yazılımlar**
- **Tesisler**
- **İmaj**
- **Süreçler**
- **İşlemler**

RİSK ANALİZ TERMİNOLOJİSİ

Varlık Sahibi:

- **İş Sahibi**

  Varlığın değerini ve risklerini en iyi bilen ve risk analizi sürecinde bu kararları veren, korunma gereksinimini belirleyen birim veya kişidir.

- **Teknik Sahibi**

  Varlığı belirlenen gereksinimine uygun olarak korunmasından sorumlu olan birim veya kişidir.

RİSK ANALİZ TERMİNOLOJİSİ

Zafiyet: Bir varlığın bir tehditten zarar görmesine yol açacak zayıflıklar, varlığın korunmasız olma halidir.

- Eğitimsiz insanlar
- Zayıf şifreler
- Hatalı kurulan cihazlar
- Kilitsiz kapılar
- Yetkisiz erişilebilen sistemler, odalar vb.

RİSK ANALİZ TERMİNOLOJİSİ

Kontrol: Zafiyeti veya tehditlerin etkisini azaltma yeteneği olan, sistemler ve süreçlerdir.

- Kartlı giriş sistemleri
- Antivirüs sistemleri
- Alarm sistemleri
- Güçlü şifreler
- İzleme sistemleri
- Politika ve prosedürler

VARLIK-TEHDİT-ZAFİYET-KONTROL

Risk analizi bu kavramlar arasındaki ilişkiyi inceleyerek, mevcut risk durumunu ortaya çıkarır.

Risk analizi sonuçları sadece yapıldığı anı gösteren bir fotoğraf gibidir. Varlıklar, tehditler, zafiyetler ve kontroller sürekli değişkenlik gösterir.

BİLGİ GÜVENLİĞİNİ SAĞLAMAK İÇİN

Risklerin farkında olmamız ve

- Varlıklar
- Tehditler
- Zafiyetler
- Kontroller

arasındaki ilişkiyi bilmemiz gerekir.

RİSKLERİN FARKINDA OLMAK

BİLGİ GÜVENLİĞİNİ SAĞLAMANIN İLK ADIMIDIR!

RİSK YÖNETİMİ TERMİNOLOJİSİ

Risk Yönetimi: Bir kurumu riskleri açısından kontrol etmek ve yönlendirmek için yapılan koordinasyon altındaki çalışmalardır.

Risk yönetimi, risk analizi, risk işleme, risk kabulü ve riskin duyurulması faaliyetlerinin tümünü kapsar.

Risk İşleme: Risk seviyelerini düşürmek için önlemlerin seçimi, planlanması ve uygulanması gibi etkinlikleridir.

RİSK YÖNETİMİ TERMİNOLOJİSİ

Kalan Risk : Risk işleme sürecinden sonra artakalan risktir. Alınan tüm önlemler, mevcut tehdit ve zafiyet seviyeleri göz önüne alınarak düşünülür.

Risk Kabulü: Yönetimin riski göze alma kararıdır. Bu noktadan sonra yeni kontroller gerekli değildir.

Risk Kabul Kriteri: Yönetimin kabul edilebilir olarak açıkladığı risk seviyesi ve bunu karşılayan kontrollerdir.

UYGUN ÖNLEMLERİN (KONTROLLERİN) BELİRLENMESİ

- Kontroller, tehdide yol açan zafiyetleri azaltacak veya tehdidin gerçekleşme olasılığını düşürecek önlemlerdir.
- ISO 27002 standardında tavsiye niteliğinde yaklaşık 130 tane kontrol bulunmaktadır.
- Her varlık-tehdit çifti için uygun kontroller bu tavsiyeler arasından seçilir.
- Yeterli olmadığı durumlarda, yeni önlemlerde seçilebilir.

UYGUN ÖNLEMLERİN (KONTROLLERİN) BELİRLENMESİ

- Bu aşamada, atanan yeni kontrollerle risk değerleri kabul edilebilir seviyeye çekilmiş olur.
- Bir kontrolün neden seçildiğini, daha önce belirlenen varlık-tehdit atamaları ile ilişkilendirebilmek önemlidir. Böylece risk analizinin sağlıklı bir şekilde yapıldığından emin olabiliriz.
- Kontroller teknik veya yönetsel olabilir. Seçilen kontroller, hazırlanacak olan politika dokümanları, standartlar ve prosedürler içinde yer alır.

RİSK İYİLEŞTİRME ALTERNATİFLERİ

- **Üst yönetimin risklerin kabul edilmesiyle ilgili yaklaşımını, hangi seviyedeki ve/veya ne tür riskleri kabul edeceğini bir diğer deyişle risk kabul kriterlerini kararlaştırması gerekir.**

- **Her risk için kabul kriterlerine uygunluk baz alınarak ele alma yöntemi belirlenir. Riskin;**
  - Kabul edilmesi
  - Transfer edilmesi
  - Yönetilmesi
  - Önlenmesi

  kararları verilebilir

RİSK KARARLARI

Riskler yönetilirken aşağıdaki kararları verebiliriz:

- Riski göze almak (Kapı giriş kontrolü yapmamak, antivirüs sistemi kullanmamak, eğitime önem vermemek ..)
- Risklerimizi başkasına aktarmak (yangın sigortası, mesleki sorumluluk sigortası, hırsızlık sigortası yaptırmak, PCI),
- Risklerin olasılığını düşürecek önlemler almak (Çelik kapılar, alarm sistemleri, temiz masa, temiz ekran, izleme sistemleri, yangın detektörü)
- Risklerin etkisini azaltacak önlemler almak (Yangın söndürücü, antivirüs sistemleri, güvenlik testleri).
- Riskten sakınmak (Belli bir uygulamayı devreye almamak..)

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ STANDARTLARI

BGYS STANDARTLARI

- Endüstrinin çeşitli kesimlerinden yükselen “ortak bir güvenlik modeli” talebi standartlaşma gereğini gündeme getirmiştir.
- Kuruluşlar, birlikte iş yaptıkları taraflara karşı ortak bir asgari güvenlik seviyesi sağladıklarını kanıtlamak istemişler ve bunun için bir referansa gereksinim duymuşlardır.
- Bilgi Güvenliği Yönetimi konusundaki ilk standart BSI (British Standard Institute), tarafından geliştirilmiştir: BS 7799

Giriş

ISO/IEC 17799:2000
Information technology — Code of practice for information security management

ISO/IEC 17799:2005
Information technology — Security techniques — Code of practice for information security management

ISO/IEC 27002:2005
Information technology — Security techniques — Code of practice for information security management
(Numara Tadili, Technical Corrigendum 1, 2007-07-01)

ISO/IEC 27001:2005
Information technology — Security techniques — Information security management systems -- Requirements

ISO/IEC 27001:2013

TS ISO/IEC 27001:2013
Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler

- TS ISO/IEC 27001 BGYS'nin belgelendirilmesi için uygunluk standardıdır.

TS ISO/IEC 27002:2013
Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Kontrolleri İçin İyi Uygulamalar

- Rehber standart
- Bilgi güvenliğini başlatan, gerçekleştiren ve sürekliliğini sağlayan kişilerin kullanımı için bilgi güvenliği yönetimi ile ilgili tavsiyeler

BGYS ile İlgili Diğer Standartlar

- TS ISO/IEC 27000 – Tanımlar
- TS ISO/IEC 27002 — Bilgi Güvenliği Yönetim Sistemleri – Kontroller
- ISO/IEC 27003 — Bilgi Güvenliği Yönetim Sistemleri - Uygulama Kılavuzu
- ISO/IEC 27004 — Bilgi Güvenliği Yönetim Sistemleri –Ölçme
- Tst ISO/IEC 27005 — Bilgi Güvenliği Risk Yönetimi
- ISO/IEC 27006 — BGYS Belgelendirmesi yapan kuruluşlar için klavuz
- ISO/IEC 27011 — ISO/IEC 27002'ye göre telekomünikasyon kuruluşları için bilgi güvenliği yönetim kuralları
- ISO/IEC 27007 — Bilgi Güvenliği Yönetim Sistemleri Denetimi Rehberi (yönetim sistemi odaklı)

BGYS ile İlgili Diğer Standartlar

- ISO/IEC 27008 — BGYS denetçileri (bilgi güvenliği denetimleri odaklı)
- ISO/IEC 27013 — ISO/IEC 20000-1 ve ISO/IEC 27001 bütünleştirme çalışmalarına ilişkin kılavuz
- ISO/IEC 27014 — Bilgi Güvenliği Yönetim Çerçevesi
- ISO/IEC 27015 — Finans ve sigorta sektörleri için bilgi güvenliği yönetim kuralları
- ISO 27799 — ISO/IEC Denetim ve 27002 ile Sağlıkta Bilgi Güvenliği Yönetimi Hazırlık Aşamasında olan belgeler Belgelendirme işlerini sağlayan kuruluşlar için şartlar
- ISO/IEC 27032 — Siber Güvenlik (temelde, İnternet'te 'iyi bir komşu olmak' için rehber)

BGYS ile İlgili Diğer Standartlar

- ISO/IEC 27031 — İş sürekliliği için bilgi ve iletişim teknolojisi hazırlık rehberi
- ISO/IEC 27033 — BT Ağ Güvenliği, ISO/IEC 18028:2006'ya
- ISO/IEC 27033-1 — Ağ güvenliği genel bakış ve kavramlar dayalı çok parçalı standart (Sadece Bölüm 1 yayınlandı)
- ISO/IEC 27034 — Uygulama Güvenliği Rehberi
- ISO/IEC 27035 — Güvenlik Olay Yönetimi
- ISO/IEC 27036 — Dış Kaynak kullanımı için güvenlik rehberi
- ISO/IEC 27037 — Tanımlama, toplama ve / veya satın alma ve dijital kanıt korunması rehberi

- ISO 31000:2009, Risk Yönetimi

ISO/IEC 27001:2013 Yararları

- Piyasada farklılaşma / itibar
- Üst yönetim ve müşteri gereksinimlerinin karşılanması
- Küresel kabul görmüş tek standart
- Bilgi güvenliği bilinci ile odaklanmış çalışanlar
- Yasal zorunlulukların karşılanması
- Zayıflıkların saptanıp giderilmesi/ Yeni ortaya çıkan tehdit ve açıklıklara hazırlıklı olmak

ISO/IEC 27001:2013 Yararları

- Kurumsal yönetim (Uygulamaya konmuş politika ve prosedürler ile belirlenmiş sorumluluk ve yetkiler)
- Üst yönetimin Bilgi Güvenliğini sahiplenmesi
- Daha iyi güvenlik bilinci oluşması
- Diğer yönetim sistemleri ile kaynakların birleştirilmesi
- Sistemin başarısını ölçme mekanizması

- TS ISO/IEC 27001 Belgesinin Yararları :
  - BGYS'nin bağımsız denetçilerce gözden geçirilmesi
  - Ticari ortaklara ve müşterilere güven sağlaması

ISO/IEC 27001:2013 Akredite Belgelendirme Yararları

Saldırıya Uğrayabilecek Değerler

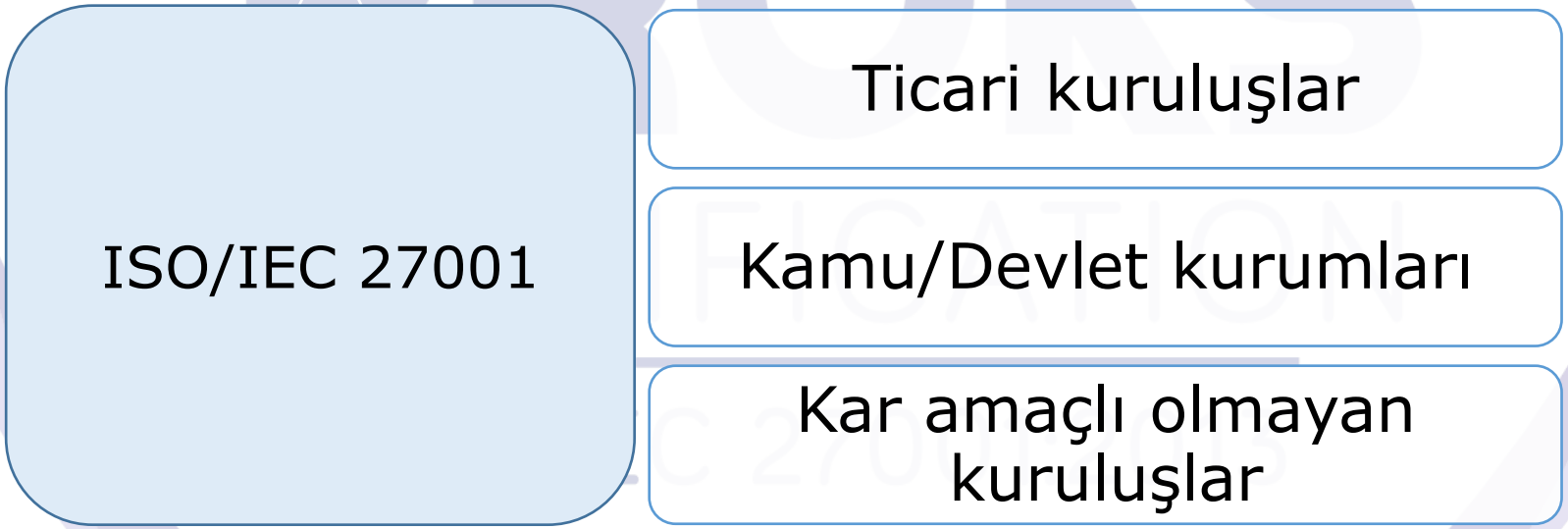
- Kuruluşun itibarı, güvenilirliği
- Kuruluşa ait gizli bilgiler ticari, teknolojik bilgiler
- İş sürekliliğini sağlayan bilgi ve süreçler
- Üçüncü şahıslar tarafından emanet edilen bilgiler

ISO/IEC 27001:2013 Akredite Belgelendirme Yararları

Görülebilecek Zarar

- Müşteri Mağduriyeti
- Kaynakların Tüketimi
- İşin yavaşlaması ya da durması
- Kurumsal imaj kaybı
- Üçüncü şahıslara yapılan saldırı mesuliyeti

ISO/IEC 27001:2013 Kimler Uygulayabilir?



ISO/IEC 27001:2013 kuruluşun türü, büyüklüğü ve doğasından bağımsız olarak tüm kuruluşlara uygulanabilir.

YANILGILAR

- BT ürünü, teknoloji veya servis olarak görülmesi
- Başlangıcı ve sonu belirli olan bir BT proje olarak düşünülmesi
- Dokümantasyondan oluştuğu varsayımı
- BGYS sorumluluğunun BT bölümü olduğunun düşünülmesi

Bilgi Güvenliği Yönetim Sistemi

- **Bilgi Güvenliği Yönetim Sistemi :**

- Bilgi güvenliğini kurmayı, gerçekleştirmeyi, işletmeyi, izlemeyi, gözden geçirmeyi, sürdürmeyi ve iyileştirmeyi temel alan iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası (ISO/IEC 27000)

- Kuruluşun fiziksel ve elektronik bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini korumak için en üstten en alta kadar uygulayacağı iş odaklı yönetim yaklaşımı

Bilgi Güvenliği Yönetim Sistemi

- BGYS'nin benimsenmesi stratejik bir karar olmalı

- BGYS tasarım ve gerçekleştirmesinin etkilendiği hususlar

  - Kuruluşun iş gereksinimleri
  - Kuruluşun ihtiyaç ve hedefleri
  - Güvenlik gereksinimleri
  - Organizasyonel süreçler
  - Kuruluşun büyüklüğü ve yapısı

Bilgi Güvenliği Yönetim Sistemi

- Bir çok bilgi sistemi TS ISO/IEC 27001 standardının paralelinde bir güvenliğe sahip olacak şekilde tasarlanmamıştır
- Teknik yollarla sağlanabilecek güvenlik sınırlıdır, uygun yönetim ve prosedürlerle desteklenmelidir
- Güvenlik için uygulanacak kontrollerin belirlenmesi özenli bir planlama ve detaylara dikkat gerektirir
- Başarılı bir BGYS kuruluştaki tüm çalışanlardan destek gerektirir
- Başarılı bir BGYS paydaşlardan, tedarikçilerden ve diğer dış taraflardan katılım gerektirir

Bilgi Güvenliği Yönetim Sistemi

- BGYS kurulumu bir BT ürünü veya sistemi kurulumundan farklıdır.
- BGYS kuruluşun iş yapma tarzını / tamamını etkiler.
- Tüm kademelerdeki çalışanların işini yaparken bilgi güvenliği prensiplerine uygun hareket etmesini gerektirir.
- BGYS bilincinin oluşması zaman gerektirir.
- BGYS sürekli bir gelişim sürecidir.

ISO/IEC 27001:2013 Standardı

Sunumdaki objelerin anlamları

- Yazılı Bilgi (Politika, Prosedür, talimat vb.)

- Yazılı Bilgi (Tutanak, rapor, erişim yetkileri, personel giriş/çıkış saatleri vb.)

- Gözden geçirme (planlı aralıklar)

ISO/IEC 27001:2013 Standardı

- 0. Giriş
- 1. Kapsam
- 2. Atıf yapılan standartlar ve/veya dokümanlar
- 3. Terimler ve Tarifler
- 4. Kuruluşun İçeriği
- 5. Liderlik
- 6. Planlama
- 7. Destek
- 8. İşletim
- 9. Performans Değerlendirme
- 10. İyileştirme
- Ek A – Referans Kontrol Hedefleri ve Kontroller

Ek-A Referans Kontrol Hedefleri ve Kontroller

- A.5 Bilgi Güvenliği politikaları
- A.6 Bilgi güvenliği organizasyonu
- A.7 İnsan kaynakları güvenliği
- A.8 Varlık yönetimi
- A.9 Erişim kontrolü
- A.10 Kriptografi
- A.11 Fiziksel ve çevresel güvenlik
- A.12 İşletim güvenliği
- A.13 Haberleşme güvenliği
- A.14 Sistem edinimi, geliştirme ve bakımı
- A.15 Tedarikçi İlişkileri
- A.16 Bilgi Güvenliği ihlal Olayı yönetimi
- A.17 İş sürekliliği yönetiminin bilgi güvenliği hususları
- A.18 Uyum

Ek-A Referans Kontrol Hedefleri ve Kontroller

- 14 adet güvenlik kontrol maddesi
- 35 ana güvenlik kategorisi
- 114 kontrol

- Her madde bir veya daha fazla kategori içerir
- Maddelerin sıralaması önemlerini göstermez

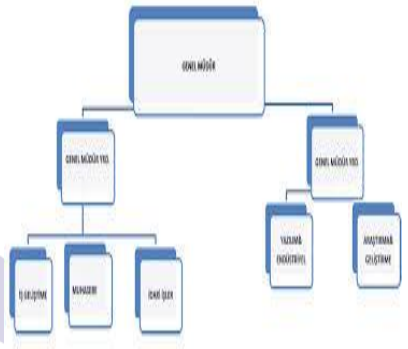
Ek-A Referans Kontrol Hedefleri ve Kontroller

Kontrol Kategorileri

- Kontrol kategorisi
  - Neye ulaşılması gerektiğini belirten kontrol hedefi
  - Kontrol hedefine erişmek için uygulanabilecek bir ya da daha fazla kontrol

- Kontrol (TS ISO/IEC 27001)
  - Uygulama kılavuzu/Implementation guidance (TS ISO/IEC 27002)
  - Diğer bilgi/Other information (TS ISO/IEC 27002)

4
Kuruluşun Bağlamı



4 Kuruluşun Bağlamı

4.1 Kuruluşun ve bağlamının anlaşılması

Bağlam oluşturulurken

- Kuruluş hedeflerine giden yolu ortaya çıkarır
- Kapsam ve risk kriterlerini oluşturmaya katkı sağlar
- Riski yönetirken dikkate alacağı dış ve iç parametreleri ortaya çıkarır

4 Kuruluşun Bağlamı

4.1 Kuruluşun ve Bağlamının anlaşılması

İç Bağlam

- İç Bağlam kuruluşun riski yönetim biçimini etkileyebilen kuruluş içindeki herhangi bir şeydir.

İç Bağlam oluşturulmalı, çünkü:

- Risk yönetimi kuruluşun hedeflerinin kapsamında meydana gelir
- Özel bir proje, süreç veya faaliyetin hedefleri ve kriterleri bir bütün olarak kuruluşun hedefleri ışığında düşünülmelidir

4 Kuruluşun Bağlam

4.1 Kuruluşun ve Bağlamının anlaşılması

İç Bağlam

- İdare, kuruluş yapısı, roller ve yükümlülükler
- Yerine getirilecek politikalar, hedefler ve stratejiler
- Kaynaklar ve bilgi birikimi cinsinden anlaşılan yetenekler (örneğin, anapara, zaman, kişiler, süreçler, sistemler ve teknolojiler)
- Bilgi sistemleri, bilgi akışı ve karar alma süreçleri (resmi ve gayrı resmi)

4 Kuruluşun Bağlam

4.1 Kuruluşun ve Bağlamının anlaşılması

İç Bağlam

- İç paydaşlarla ilişkiler ve onların algılamaları ve değerleri
- Kuruluşun kültürü
- Kuruluş tarafından uyarlanan standartlar, kılavuzlar ve modeller
- Sözleşmeye ilişkin ilişkilerin biçim ve genişliği

4 Kuruluşun Bağlamı

4.1 Kuruluşun ve Bağlamının anlaşılması

Dış Bağlam

- Dış Bağlamın anlaşılması, risk kriterlerini geliştirirken dış paydaşların hedefleri ve kaygılarını dikkate almayı temin için önemlidir.
- Dış kapsam yasal ve mevzuatla ilgili şartlara ait özel ayrıntılar, paydaşların algılamaları ve risk yönetim sürecinin kapsamına özgü diğer risk hususları ile birlikte ele alınır.

4 Kuruluşun Bağlamı

4.1 Kuruluşun ve Bağlamının anlaşılması

Dış Bağlam

- Uluslararası, ulusal, bölgesel veya yerel olmak üzere, sosyal ve kültürel, politik, yasal, mevzuata ilişkin,finansal, teknolojik, ekonomik, doğal ve rekabetçi ortam
- Kuruluşun hedefleri üzerinde etkisi bulunan önemli unsurlar (insanlar, bilgi, teknoloji, vb.) ve eğilimler
- Dış paydaşlarla ilişkiler ve onların algılamaları ve değerleri

4 Kuruluşun Bağlamı

4.2 İlgili tarafların ihtiyaç ve beklentilerinin anlaşılması

- Bilgi güvenliği yönetim sistemi ile ilgili tarafların belirlenmesi
- İlgili tarafların bilgi güvenliği ile ilgili gereksinimlerinin ve beklentilerinin belirlenmesi

İlgili tarafların gereksinimleri

- Yasal ve düzenleyici gereksinimler
- Sözleşmeden doğan yükümlülükler

4 Kuruluşun Bağlamı

4.3 Bilgi güvenliği yönetim sisteminin kapsamının belirlenmesi

- Kapsamın oluşturulabilmesi için, bilgi güvenliği yönetim sisteminin sınırlarının ve uygulanabilirliğinin belirlenmesi
- Kapsam belirlenirken (Dikkate al)
  - Dış ve iç bağlamı
  - İlgili tarafların gereksinimleri ve beklentileri
  - Gerçekleştirilen faaliyetler arasındaki arayüzler ve bağımlılıklar
  - Diğer kuruluşlar tarafından gerçekleştirilen faaliyetler

Kapsam yazılı bilgi olarak mevcut olmalıdır.

4 Kuruluşun Bağlamı

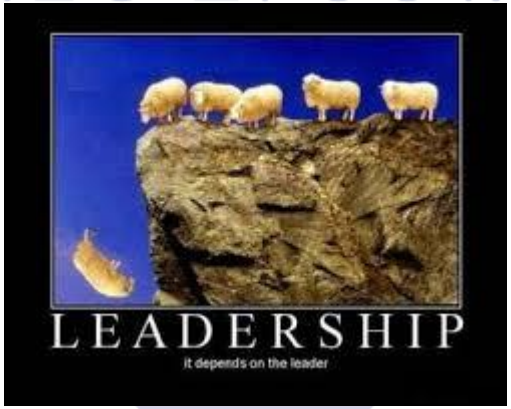
4.4 Bilgi güvenliği yönetim sistemi

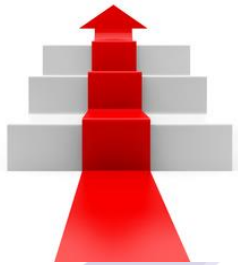
- Kuruluş standardın belirttiği şartlar çerçevesinde

Bilgi Güvenliği Yönetim Sistemini

- **Kurmalı**
- **Uygulamalı**
- **Sürdürmeli**
- **Sürekli iyileştirmelidir**

5
Liderlik





5 Liderlik

5.1 Liderlik ve Bağlılık

Üst Yönetim

- Politikanın oluşturulması
- Hedeflerin oluşturulması
- BGYS gereklerinin kuruluşun süreçleri ile bütünleştirilmesi
- BGYS için gerekli kaynakların erişilebilirliğinin sağlanması
- Etkin BGYS'nin öneminin duyurulması
- BGYS'nin hedeflenen çıktılarına erişimin sağlanması
- Çalışanların BGYS'nin etkinliğine katkı sağlamaları için teşvik edilmesi
- Sürekli iyileştirmenin desteklenmesi

5 Liderlik

5.2 Politika

- Kuruluşun amacına uygun olmalı
- Bilgi güvenliği amaçlarını içermeli
- Bilgi güvenliği ile ilgili uygulanabilir şartların karşılanmasına dair bir taahhüt içermeli
- Bilgi güvenliği yönetim sisteminin sürekli iyileştirilmesi için bir taahhüt içermeli

Bilgi Güvenliği Politikası

- Yazılı bilgi
- Kuruluş içinde duyuru
- Uygun olan ilgili taraflarca erişilebilir

5 Liderlik

5.3 Kurumsal roller, sorumluluklar ve yetkiler

Üst yönetim

- Bilgi güvenliği ile ilgili olan roller için sorumluluk ve yetkilerin atanması ve duyurulması

Sorumluluk ve yetki ataması (Üst Yönetim)

- Bilgi güvenliği yönetim sisteminin bu standardın şartlarına uyum sağlamasını temin etmek
- Üst yönetime bilgi güvenliği yönetim sisteminin performansı hakkında raporlama (Yönetim temsilcisi, bilgi güvenliği yöneticisi vb.)

6
Planlama

6 Planlama

6.1 Risk ve fırsatları ele alan faaliyetler

Risk ve fırsatların belirlenmesi

- Bilgi güvenliği yönetim sisteminin amaçlanan çıktıları başarabilmesinin temin edilmesi
- İstenmeyen etkilerin önlenmesi veya azaltılması
- Sürekli iyileştirmenin başarılması

Planlama

Risk ve fırsatların ele alınması için faaliyetler

- Faaliyetlerin, bilgi güvenliği yönetim sistemi süreçlerine nasıl entegre edileceği ve uygulanacağı
- Faaliyetlerin etkinliğinin nasıl değerlendirileceği

6.1 Risk ve fırsatları ele alan faaliyetler

6.1.2 Bilgi güvenliği risk değerlendirmesi

Bilgi güvenliği risk değerlendirmesi

Risk değerlendirmesi sürecinin tanımlanması ve uygulanması

- Bilgi güvenliği **risk kriterlerinin** oluşturulması
  - Risk kabul kriterleri
  - Bilgi güvenliği risk değerlendirmesi yapılması için kriterler
- Tekrarlanan bilgi güvenliği risk değerlendirmelerinin tutarlı, geçerli ve karşılaştırılabilir sonuçlar üretmesinin temin edilmesi

6.1 Risk ve fırsatları ele alan faaliyetler

6.1.2 Bilgi güvenliği risk değerlendirmesi

Bilgi güvenliği risk değerlendirmesi

- Bilgi güvenliği **risklerinin tespiti**
  - BGYS kapsamındaki **bilginin gizlilik, bütünlük ve erişilebilirlik kayıpları** için risklerin tespit edilmesi amacıyla bilgi güvenliği risk değerlendirme prosesinin uygulanması
  - **Risk sahiplerinin** belirlenmesi

6.1 Risk ve fırsatları ele alan faaliyetler

6.1.2 Bilgi güvenliği risk değerlendirmesi

Bilgi güvenliği risk değerlendirmesi

- Bilgi güvenliği **risklerinin analizi**
  - Belirlenen riskler gerçekleştiği takdirde muhtemel **sonuçların** değerlendirilmesi
  - Belirlenen risklerin gerçekleşmesi **ihtimalinin gerçekçi** bir şekilde değerlendirilmesi
  - Risk **seviyelerinin** belirlenmesi

6.1 Risk ve fırsatları ele alan faaliyetler

6.1.2 Bilgi güvenliği risk değerlendirmesi

Bilgi güvenliği risk değerlendirmesi

- Bilgi güvenliği risklerinin değerlendirmesi
  - Risk **analizi sonuçlarının karşılaştırılması**
    - Risk kabul kriterleri
    - Bilgi güvenliği risk değerlendirmesi yapılması için kriterler
  - Analiz edilen risklerin risk işleme için **önceliklendirilmesi**

Risk değerlendirme süreci için yazılı bilgilerin muhafazası

6.1 Risk ve fırsatları ele alan faaliyetler

6.1.3 Bilgi güvenliği risk işleme

Bilgi güvenliği risk işleme

Bilgi güvenliği risk işleme sürecinin tanımlanması ve uygulanması

- Risk değerlendirme sonuçlarını dikkate alarak uygun bilgi güvenliği **risk işleme seçeneklerinin belirlenmesi**
- Seçilen bilgi güvenliği risk işleme seçeneklerinin uygulanmasında gerekli olan tüm **kontrollerin belirlenmesi**

Not : Gerektiğinde başka kontroller tasarlanabilir veya herhangi bir kaynaktan temin edilebilir

6.1 Risk ve fırsatları ele alan faaliyetler

6.1.3 Bilgi güvenliği risk işleme

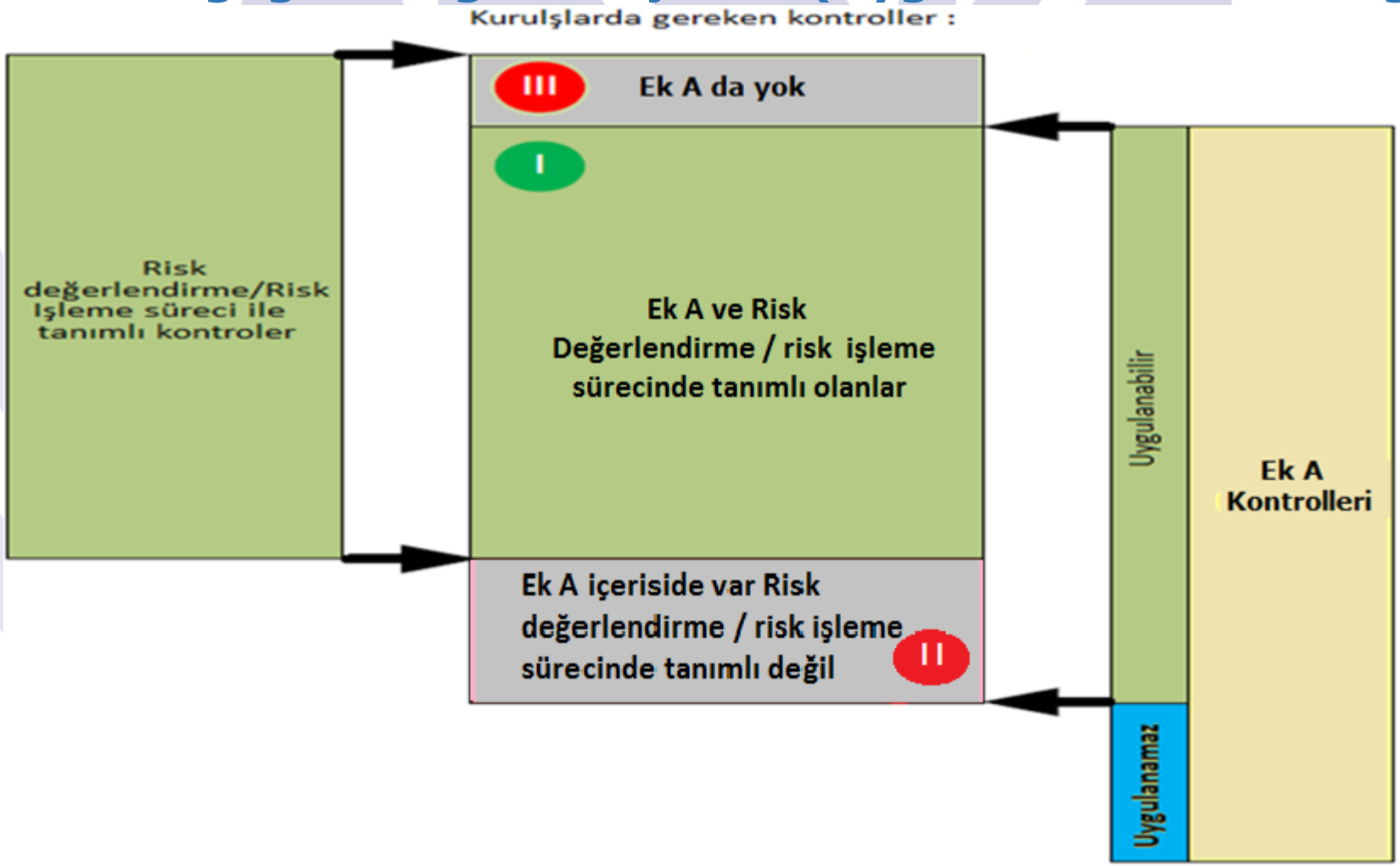
Bilgi güvenliği risk işleme

- Belirlenen kontroller ile Ek-A'daki kontrollerin karşılaştırılması (gerekli hiçbir kontrolün gözden kaçırılmadığının doğrulanması)
- **Uygulanabilirlik Bildirgesi üretilmesi**

  - Gerekli kontroller ve bunların dahil edilmesinin açıklaması
  - Kontrollerin uygulanıp uygulanmadıkları
  - Kontrollerin hariç tutulmasının gerekçelendirmesi
- Bir bilgi güvenliği risk işleme planının formüle edilmesi

6.1 Risk ve fırsatları ele alan faaliyetler

6.1.3 Bilgi güvenliği risk işleme (Uygulanabilirlik bildirgesi)



6.1 Risk ve fırsatları ele alan faaliyetler

6.1.3 Bilgi güvenliği risk işleme


- Bilgi güvenliği **risk işleme planına** dair risk sahiplerinin onayının alınması ve artık risklerin kabulü

Bilgi güvenliği risk işleme süreci ile ilgili yazılı bilgilerin muhafazası

Not - *Bu standarddaki bilgi güvenliği risk değerlendirme ve işleme süreci ISO 31000'de verilen ilkeler ve genel kılavuzlarla paraleldir..*

6.2 Bilgi güvenliği hedefleri ve bu hedeflere erişmek için planlama

- Bilgi güvenliği hedefleri
  - Bilgi güvenliği politikası ile tutarlı
  - Ölçülebilir (pratikte uygulanabilirse)
  - Risk değerlendirme ve risk işlemenin sonuçlarını dikkate almalı
  - Kuruluş içinde duyurulmalı
  - Uygun şekilde güncellenmeli
- **Bilgi güvenliği hedefleri ile ilgili yazılı bilgilerin muhafazası**

6.2 Bilgi güvenliği hedefleri ve bu hedeflere erişmek için planlama

- Bilgi güvenliği hedeflerine erişim planının kapsamı
  - Ne yapılacak
  - Hangi kaynaklar gerekli olacak
  - Kim sorumlu olacak
  - Ne zaman tamamlanacak
  - Sonuçlar nasıl değerlendirilecek

Bilgi güvenliği hedefleri ve bu hedeflere erişmek için planlama

- BAZI HEDEF ÖRNEKLERİ

- Belli bir tarihe kadar TS ISO 27001 belgesi almak
- Çalışanlara BGYS yönelik yılda en az …….eğitim vermek,
- BGYS için yılda en az …….. kaynak ayırmak,
- Potansiyel iş kesintilerine yönelik yılda en az ……..tatbikat yapmak,
- BGYS yönelik personelden yılda en az ……. öneri almak

Bilgi güvenliği hedefleri ve bu hedeflere erişmek için planlama

- BAZI HEDEF ÖRNEKLERİ

- ……. sebeplerden kaynaklanan İhlal olayları sıklığını % ...düşürmek,
- ……süreçlerinde meydana gelecek iş kesintilerinde ortalama kurtarma zamanını %... oranında azaltmak.

- Maliyet Etkin BGYS Sürdürmek

7
Destek

7 Destek

- 7.1 Kaynaklar
- 7.2 Yetkinlik
- 7.3 Farkındalık
- 7.4 İletişim
- 7.5 Yazılı Bilgi

7 Destek

7.1 Kaynaklar

- Kaynaklar belirlenmeli ve sağlanmalı
  - BGYS'nin kurulması
  - BGYS'nin gerçekleştirilmesi
  - BGYS'nin sürdürülmesi
  - BGYS'nin sürekli iyileştirilmesi




7 Destek

7.1 Kaynaklar

- Kaynaklar belirlenmeli ve sağlanmalı
  - Bilgi güvenliği politikasına erişmek
  - Kuruluşun değişen ihtiyaçlarını karşılamak
  - BGYS konuları ile ilgili etkin iletişimi sağlamak (iç ve dış)

7 Destek

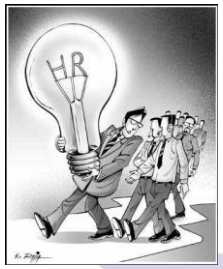
7.1 Kaynaklar

- **Kaynaklar belirlenirken yeterli hazırlıkların yapılması**
  - İnsan ve insanla ilgili kaynaklar
    - Eğitim, öğretim, farkındalık
  - Tesisler (iş lokasyonları ve altyapılar)
  - Bilişim ve iletişim teknolojileri
  - Her türlü dokümante bilginin yönetimi ve kontrolü
  - İlgili taraflarla iletişim
  - Finansman
  - Kaynaklar ve kaynak tahsisinin düzenli gözden geçirilmesi (Üst yönetimin katılımı)

7 Destek

7.2 Yetkinlik

- Bilgi güvenliği performansını etkileyen ve kuruluşun kontrolü altındaki personelin kişinin/kişilerin sahip olması istenen gerekli **yetkinlik düzeyinin** belirlenmesi
- Uygun eğitim, öğretim ve tecrübe yetkinliği
- İstenen yetkinliği sağlamak için gerekli faaliyetlerin yapılması ve etkinliğin değerlendirilmesi
- Yetkinliğe dair delillerin dokümante bilgi olarak muhafazası



7 Destek

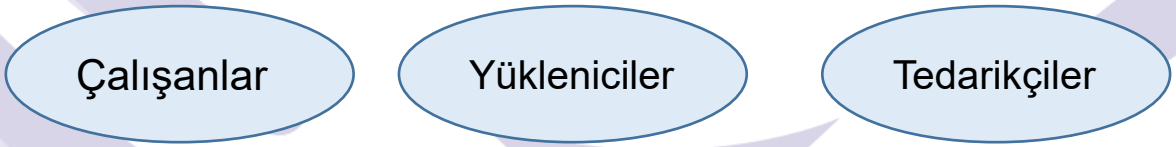
7.2 Yetkinlik

- **Yetkinliği sağlamak için faaliyetler**
  - Eğitim
  - Çalışan personele danışmanlık/kılavuzluk yapılması
  - Personelin görev değişikliğinin yapılması
  - Yeterli yetkinlik düzeyine sahip kişilerin işe alınması

7 Destek

7.3 Farkındalık

- Kuruluşun kontrolü dâhilinde görev yapan kişiler farkında olmalı
  - Bilgi güvenliği politikası
  - Bilgi güvenliği yönetim sisteminin etkinliğine yaptıkları katkı
  - Bilgi güvenliği yönetim sistemi şartlarına uyum sağlamamanın sonuçları
- Kuruluşun kontrolü altında çalışan personel



7 Destek

7.3 Farkındalık

Kuruluşun Bir Kültür Oluşturması ve Geliştirmesi

- Bilgi güvenliği yönetiminin kuruluşun önemli değerlerinin ve yönetiminin bir parçası haline gelmesi
- İlgili tarafların bilgi güvenliği politikası ve ilgili prosedürlerdeki rolleri konusunda farkındalığı

7 Destek

7.3 Farkındalık

- **Bilgi güvenliği kültürü geliştirmeyi destekleyen unsurlar**
  - Kuruluştaki tüm personelin katılımı
  - Kuruluş bünyesinde dağınık liderlik
  - Sorumlulukları tahsisi
  - Performans göstergelerine göre ölçümler
  - Bilgi güvenliğinin normal yönetim uygulamalarına entegrasyonu
  - Farkındalığın artırılması

7 Destek

7.4 İletişim

- **İç ve dış iletişim ihtiyacının belirlenmesi**
  - İletişimin konusu
  - Ne zaman iletişim kurulacağı
  - Kiminle iletişim kurulacağı
  - Kimin iletişim kuracağı
  - İletişimin hangi süreçten etkileneceği

7 Destek

7.4 İletişim

- İlgili taraflar ile kuruluş içerisindeki çalışanlar arasındaki iç iletişim
- Müşteriler, ortak kuruluşlar, yerel halk ve ilgili diğer taraflarla dış iletişim
- İlgili taraflardan gelen bildirimin alınması, yazılı hale getirilmesi ve cevabın verilmesi
- Ulusal veya bölgesel bir tehdit danışma sisteminin planlama ve operasyonel kullanım için entegrasyonu

7.5 Yazılı Bilgi

7.5.1 Genel

- Standardın gerektirdiği yazılı bilgiler
- Kuruluş tarafından bilgi güvenliği yönetim sisteminin etkinliği için gerekli olduğu belirlenen yazılı bilgiler

- **Yazılı bilgilerin boyutu farklılık gösterebilir**
  - Kuruluşun büyüklüğü ve faaliyetlerinin, süreçlerinin, ürünlerinin ve hizmetlerinin türleri
  - Süreçlerin ve etkileşimlerinin karmaşıklığı
  - Kişilerin yeterliliği

7.5 Yazılı Bilgi

7.5.1 Genel

- **Yazılı bilgi, yönetim sisteminin etkin işlemesinin ve gereksinimlere uyumun delillerini oluşturur**
  - **Prosedür:** Bir faaliyeti veya süreci yerine getirmek için belirlenmiş yol
  - **Yazılı (Dokümante) Prosedür:** Prosedürün herhangi bir ortamda bulunması ve muhafazası
  - Bir doküman bir veya daha fazla yazılı prosedür gereklerini karşılayabilir
  - Bir yazılı prosedürün gereksinimi birden fazla doküman tarafından karşılanabilir

7.5 Yazılı Bilgi

7.5.1 Genel

- **TS ISO/IEC 27001 standardının gerektirdiği yazılı bilgi**
  - BGYS Kapsamı (4.3)
  - Bilgi güvenliği politikası (5.2)
  - Bilgi güvenliği risk değerlendirme süreci (6.1.2)
  - Bilgi güvenliği risk işleme süreci (6.1.3)
  - Bilgi güvenliği hedefleri (6.2)
  - Yetkinlik (7.2)
  - Dış kaynaklı dokümanlar listesi (7.5.3)

7.5 Yazılı Bilgi

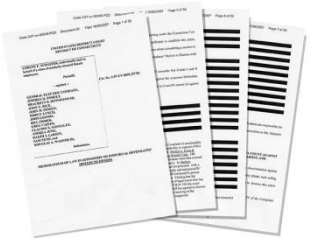
7.5.1 Genel

- **ISO/IEC 27001:2013 standardının gerektirdiği yazılı bilgi**
  - Operasyonel planlama ve kontrol (8.1)
  - Bilgi güvenliği risk değerlendirme sonuçları (8.2)
  - Bilgi güvenliği risk işleme sonuçları (8.3)
  - İzleme ve ölçme sonuçları (9.1)
  - İç tetkik programları ve tetkik sonuçları (9.2)
  - Yönetimin gözden geçirmesi sonuçları (9.3)
  - Uygunsuzlukların yapısı ve takip eden faaliyetler ile düzeltici faaliyet sonuçları (10.1)

7.5 Yazılı Bilgi

7.5.2 Oluşturma ve güncelleme

- Tanımlama ve tarif etme (Örn:Başlık, tarih, yazar veya referans numarası)
- Biçim (Örn:Dil, yazılım sürümü, grafikler) ve ortam (Örn:Kâğıt, elektronik vb.)
- Uygunluk ve yeterlilik için gözden geçirme
- Onay



7.5 Yazılı Bilgi

7.5.3 Yazılı bilginin kontrolü

- Gerekli görüldüğü yer ve zamanda mevcut ve kullanım için uygun olduğu
- Yeterli düzeyde korunduğu (Gizliliğin kaybı, uygun olmayan kullanım, bütünlüğün bozulması)
- Dağıtım, erişim (görüntüleme, değiştirme izin ve yetkisi), geri kazanım ve kullanım
- Saklama ve koruma (Okunaklılığın korunması dahil)

7.5 Yazılı Bilgi

7.5.3 Yazılı bilginin kontrolü

- Değişikliklerin kontrolü (Sürüm kontrolü)
- Muhafaza veya yok etme (imha)
- Dış kaynaklı yazılı bilgilerin tespiti ve kontrolü
- Güncelliğini kaybetmiş dokümanların kullanımının engellenmesi

7.5 Yazılı Bilgi

7.5.3 Yazılı bilginin kontrolü

- Doküman kontrolünün amacı, kompleks doküman kontrol sistemi yerine, BGYS'yi uygun ve yeterli şekilde uygulamak ve işletmek için dokümanların oluşturulması, muhafazası ve korunması olmalı
- Erişim seviyeleri
  - Sadece görüntüle
  - Görüntüle ve değiştir
  - Sınırlandırılmış görüntüleme

7.5 Yazılı Bilgi

7.5.3 Yazılı bilginin kontrolü

- Dokümanların yayınından önce onayı
- Dokümanların gözden geçirilmesi ve yeniden onayı
- Dokümanların okunaklılığının ve kolay tanımlanabilirliğinin sağlanması
- Dokümanların korunması ve arşivlenmesi ile ilgili parametrelerin oluşturulması
- Gizli bilginin korunması ve ifşasının engellenmesi

7.5 Yazılı Bilgi

7.5.3 Yazılı bilginin kontrolü

- Yazılı bilginin bütünlüğünün kurcalanmaya karşı korunması
- Güvenli yedekleme
- Sadece yetkili personelin erişiminin sağlanması
- Bozulmaya ve kayba karşı koruma
- Kayıtların korunması ile ilgili mevcut yasa ve mevzuat ile uyum

8
İşletim

8 İşletim

8.1 İşletimsel planlama ve kontrol

Süreçleri planlama, uygulama ve kontrol

- Bilgi güvenliği şartlarının karşılanması
- Belirlenen faaliyetlerin (6.1) gerçekleştirilmesi
- Belirlenen bilgi güvenliği hedeflerine (6.2) erişmek için planların uygulanması
- Süreçlerin planlandığı gibi yürütüldüğünden emin olacak ölçüde yazılı bilgilerin muhafazası
- Planlanan değişikliklerin kontrolü
- İstenmeyen değişikliklerin sonuçlarının gözden geçirilmesi (Kötü etkilerin azaltılması için faaliyet)
- Dış kaynaklı süreçlerin belirlenmesi ve kontrolü

8 İşletim

8.2 Bilgi güvenliği risk değerlendirme

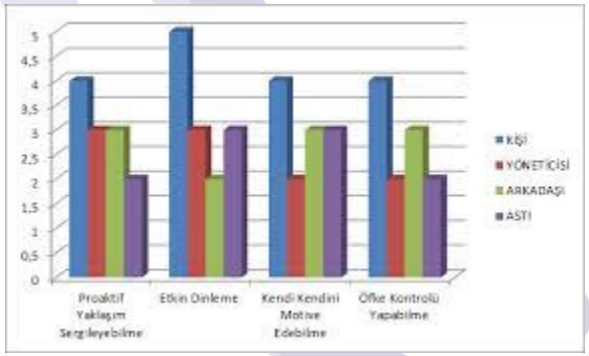
- Risk kabul kriterleri ve bilgi güvenliği risk değerlendirmesi yapılması için kriterlerin göz önüne alarak
  - Planlı aralıklarda veya önemli değişiklikler meydana geldiğinde ya da önerildiğinde
  - Bilgi güvenliği risk değerlendirmesi yapmalı ve sonuçlarına dair yazılı bilgilerin muhafazası

8 İşletim

8.3 Bilgi güvenliği risk işleme

- Bilgi güvenliği risk işleme planının uygulanması
- Bilgi güvenliği risk işlemesi sonuçlarına ait yazılı bilgilerin muhafazası

9
Performans Değerlendirme



9 Performans değerlendirme

9.1 İzleme, ölçme, analiz ve değerlendirme

- Bilgi güvenliği performansı ve bilgi güvenliği yönetim sisteminin etkinliğinin değerlendirilmesi
- Belirle
  - Ne izlenecek ve ölçülecek (Bilgi güvenliği süreçleri ve kontrolleri dahil)
  - İzleme, ölçme, analiz ve değerlendirme yöntemleri

Not - *Seçilen yöntemlerin geçerli kabul edilebilmesi için karşılaştırılabilir ve tekrar üretilebilir sonuçlar üretmesi gerekir.*

9 Performans değerlendirme

9.1 İzleme, ölçme, analiz ve değerlendirme

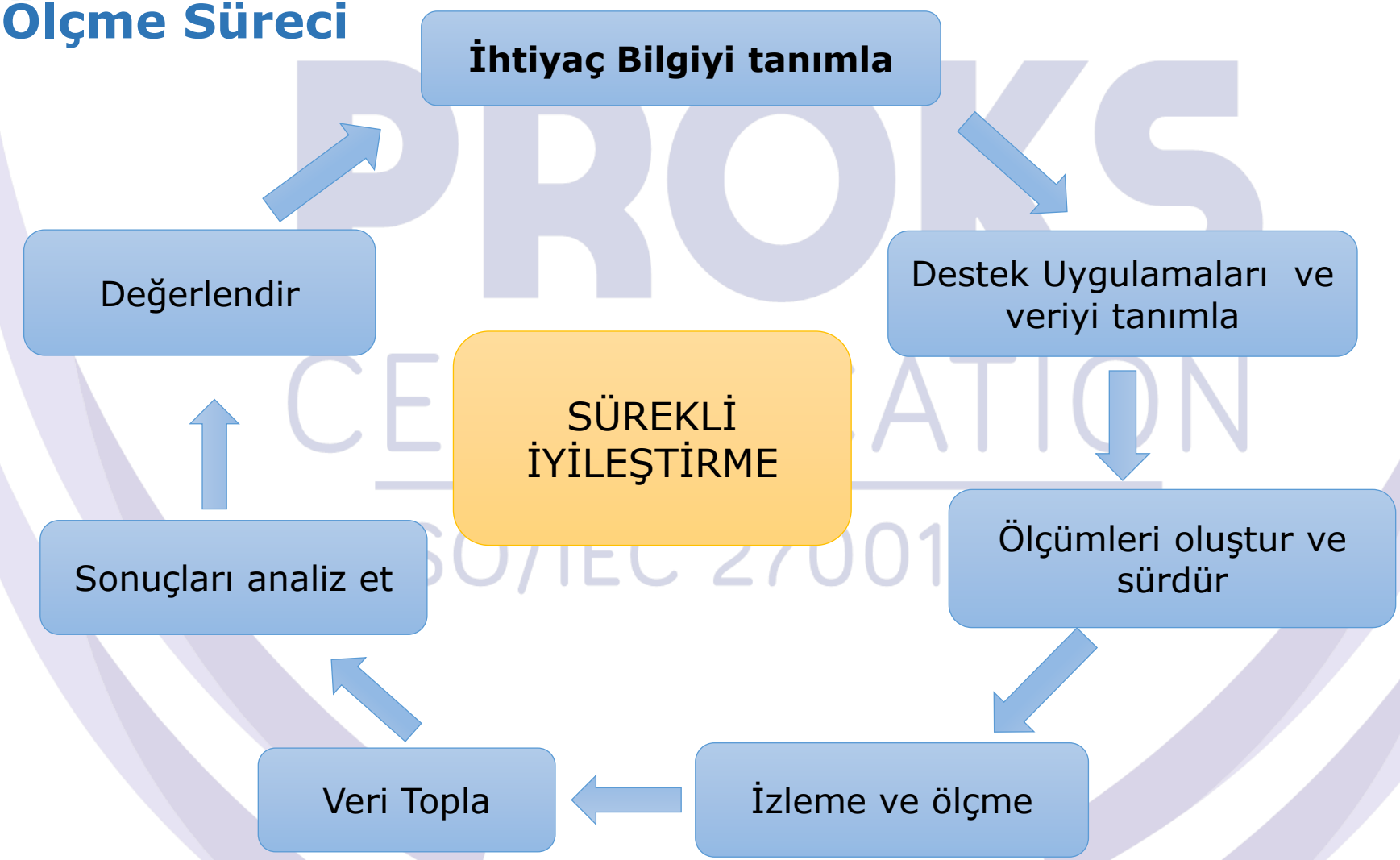
- Belirle
  - İzleme ve ölçmenin ne zaman yapılacak
  - İzlemeyi ve ölçmeyi kim yapacak
  - İzleme ve ölçme sonuçları ne zaman analiz edilecek/değerlendirilecek
  - Sonuçları kim analiz edecek/değerlendirecek
  - İzleme ve ölçme sonuçlarına dair yazılı bilgilerin muhafazası

9.1 İzleme, ölçme, analiz ve değerlendirme

Ölçme Sürecinin mantıksal akışı

ISO/IEC 27004

Ölçme Süreci



Ölçme Süreci

1. İhtiyaç olan bilgiyi tanımla

- Ölçümlerin oluşturulması İhtiyaç olan bilgilerin tanımlaması ile başlar
  - İlgili taraf isterleri
  - Kuruluşun stratejik yönü
  - Bilgi Güvenliği politika ve hedefleri
  - Risk İşleme Planı
- Aşağıdaki Aktiviteler ilgili bilgi ihtiyaçlarını tanımlamayı sağlar

1. BGYS yi inceleme (süreçleri ve diğer elemanları)
2. Kriterlere dayalı b ilgi ihtiyaçlarının önceliklendirilmesi
3. Önceliklendirme listesinden ölçüm faaliyetinde ele alınacak gerekli bilginin alt kümesini seçmek
4. Seçilmiş ihtiyaç olan bilginin oluşturulması Tüm ilgili taraflara ve iletilmesi

Ölçme Süreci

2. Destek Uygulamaları ve veriyi tanımla

- Bilgi ihtiyaçlarını destekleyebilir mevcut uygulamaları tespit
  - Risk Yönetimi;
  - Proje Yönetimi;
  - Uygunluk Raporları
  - Güvenlik politikaları
- Bilgi ihtiyaçlarını destekleyebilir mevcut verilerin tespit
  - Günlük taramalar ve çeşitli log lar
  - Eğitim istatistikleri ve faaliyetler
  - Güvenlik sonuçlarının değerlendirilmesi
  - İlgili araştırma anketler
  - Olay istatistikleri
  - İç tetkikler
  - İş sürekliliği Felaket tatbikatları
  - Yönetim gözden geçirmeleri

Ölçme Süreci

3. Ölçümleri oluştur ve sürdür

- Ölçümleri oluşturma veya güncelleme Adımları
  - BGYS kapsamı
  - Kuruluş yapısı
  - İlgili taraflar ve rol ve sorumuluklar
  - İş hedefleri ve gereksinimleri
  - Uyumluluk Gerekisinimleri
  - Takipedilen döngülerin ölçümleri kabul edilir seviyeye ulaşması
  - Bilgi İşleme teknoloji ve sistemlerinin yenilenmesi veya eskimesi
- Ölçüm Tanımlama
  - Ölçüm sırası ,İhtiyaç bilgi , Ölçüm birimi (oran, sayı, sıklık, ortalama) ,Formul/puanlama , Hedef, Uygulama kanıtı , Veri kaynağı, raporlama formatı
- Ölçümün Güncellenmesi veya değiştirilmesi

Ölçme Süreci

İzleme ve Ölçmek

- İzleme ve ölçüm işlemleri uygulamak
  - Uygulamalar için ölçümlerin dokümante edilmesi ve önceliklendirilmesi
  - Ölçüm faaliyetlerinin uygulanması için insan ve araçları hazırlamak
    - Veriler
      - toplaması
      - Analizi
      - Raporlaması
    - Nasıl yapılacak belirle
  - Yönetimin bilgilendirilmesi
- Ölçümler yönetimin ihtiyaç ve gereksinilerini yansıtmalı

9.1 İzleme, ölçme, analiz ve değerlendirme

Neler izlenip ölçülebilir ?

BGYS için ayrılan bütçenin Tüm bütçeye göre durumu
BG için politikalar gözden geçirilmesinin değerlendirilmesi
Yönetimin gözden geçirmeleri, İç tetkik Programı tamlığı,
İyileştirme çalışmaları , Düzeltici faaliyet uygulamaları
BGYS farkındalığı , BGYS farkındalık faaliyetlerinin etkinliği , BGYS Eğitimleri
Güvenlik olaylar yönetimi, maliyeti, ders çıkarma
Şifre kalitesi, yama yönetimi, erişim hakları,
Fiziksel giriş kontrolleri,
BGYS nin gözden geçirmeleri v.b…

9 Performans değerlendirme

9.2 İç tetkik

- Planlı aralıklar
- Amaç
  - Bilgi güvenliği yönetim sistemi kuruluşun kendi gereksinimlerine uygun mu?
  - BGYS, TS ISO/IEC 27001 standardının gereklerine uygun mu?
  - BGYS, etkin bir şekilde uygulanıyor ve sürdürülüyor mu?

9 Performans değerlendirme

9.2 İç tetkik

- Tetkik programının / programlarının planlanması, oluşturulması, uygulanması ve sürdürülmesi
  - Denetim sıklığı
  - Süreçlerin öneminin ve geçmiş tetkik sonuçlarının gözönüne alınması
  - Yöntemler
  - Sorumluluklar
  - Raporlama

9 Performans değerlendirme

9.2 İç tetkik

- Tetkik programının / programlarının planlanması, oluşturulması, uygulanması ve sürdürülmesi

  - Tarafsızlık/Objektiflik için denetçilerin seçimi
  - Tetkik kriterlerinin ve kapsamın tanımlanması
  - Denetim sonuçlarının yönetime rapor edilmesi
  - Denetim programının ve denetim sonuçlarının gerçekleştirildiğinin kanıtı olarak yazılı bilginin muhafazası

9 Performans değerlendirme

9.3 Yönetimin gözden geçirmesi

- Planlı aralıklar
- Amaç
  - BGYS'nin uygunluğunu, yeterliliğini ve etkinliğini sürdürmesini temin
- **Yönetimin gözden geçirmesi-Girdiler**
  - Önceki yönetimin gözden geçirmelerindeki faaliyetlerin durumu/statüsü
  - BGYS ile ilgili iç ve dış hususlardaki değişiklikler

9 Performans değerlendirme

9.3 Yönetimin gözden geçirmesi

- **Yönetimin gözden geçirmesi-Girdiler**
  - Bilgi güvenliği performansı konusundaki geri bildirim ve eğilimler
    - Uygunsuzluklar ve düzeltici faaliyetler
    - İzleme ve ölçme sonuçları
    - Tetkik sonuçları
    - Bilgi güvenliği hedeflerine erişim
    - İlgili taraflardan geri bildirimler
    - Risk değerlendirme sonuçları ve risk işleme planının durumu
    - Sürekli iyileştirme fırsatları

9 Performans değerlendirme

9.3 Yönetimin gözden geçirmesi

- **Yönetimin gözden geçirmesi çıktıları/Kararlar**
  - Sürekli iyileştirme fırsatları
  - Bilgi güvenliği yönetim sisteminde değişiklik ihtiyacına dair kararlar
  - Yönetimin gözden geçirmesinin sonuçlarının delili olarak yazılı bilgileri muhafazası
  - BGYS'nin kapsamındaki farklılıklar
  - BGYS'nin etkinliğinin iyileştirilmesi
  - Risk değerlendirmesinin ilgili prosedürlerinin güncellenmesi

9 Performans değerlendirme

9.3 Yönetimin gözden geçirmesi

- **Yönetimin gözden geçirmesi-Çıktılar**
  - Riskin kabul edilmesi için risk ve/veya kabul kriteri seviyeleri
  - Kaynak ihtiyaçları
  - Fonlama ve bütçe gereksinimleri
  - Kontrollerin etkinliğinin nasıl ölçüldüğü

10
İyileştirme

10 İyileştirme

10.1 Uygunsuzluk ve düzeltici faaliyet

- Uygunsuzluğun tespiti
  - tepki verilmesi
  - kontrol edilmesi ve düzeltilmesi için faaliyet
  - Sonuçları izleme
- Uygunsuzluğun başka bir yerde tekrar etmemesi veya oluşmaması için nedenlerinin giderilmesi
  - gözden geçirilmesi
  - nedenlerinin belirlenmesi
  - Benzer uygunsuzlukların olup olmadığını veya potansiyel olarak gerçekleşip gerçekleşmeyeceğini belirlemek

10 İyileştirme

10.1 Uygunsuzluk ve düzeltici faaliyet

- Gerekli faaliyetlerin uygulanması
- Düzeltici faaliyetlerin etkinliğinin gözden geçirilmesi
- Gerekli olan durumlarda bilgi güvenliği yönetim sisteminde değişikliklerin yapılması

Düzeltici faaliyetler, karşılaşılan uygunsuzlukların etkilerine uygun olmalı

10 İyileştirme

10.1 Uygunsuzluk ve düzeltici faaliyet

- Yazılı bilgilerin muhafazası
  - Uygunsuzlukların doğası ve gerçekleştirilen müteakip faaliyetler
  - Düzeltici faaliyetin sonuçları.

10 İyileştirme

10.2 Sürekli iyileştirme

- Bilgi güvenliği yönetim sisteminin sürekli iyileştirmesi

  - BGYS'nin uygunluğu
  - BGYS'nin doğruluğu
  - BGYS'nin etkinliği

**Etkinlik: Planlanmış faaliyetlerin gerçekleştirilmesi ve planlanan sonuçlara ulaşma derecesi*

Ek A
Referans Kontrol Amaçları ve Kontroller

Tablo A.1: Bilgi güvenliği risk işlemede (6.1.3) kullanılmak üzere ISO/IEC 27002:2013 standardının 5-18 maddelerinden çıkarılan kontrol amaçları ve kontroller

A.5
Bilgi Güvenliği Politikaları

1 Güvenlik Kategorisi

- Bilgi Güvenliği için yönetimin yönlendirmesi

A.5 Bilgi Güvenliği Politikası

A.5.1 Bilgi güvenliği için yönetimin yönlendirmesi

Amaç: Bilgi güvenliği için, iş gereksinimleri ve ilgili yasalar ve düzenlemelere göre yönetimin yönlendirmesi ve desteğini sağlamak.

A.5.1.1 Bilgi Güvenliği için politikalar

Bir dizi bilgi güvenliği politikaları, yönetim tarafından tanımlanmalı, onaylanmalı ve yayınlanarak çalışanlara ve ilgili dış taraflara bildirilmelidir.

- Politikalar setinin tanımlanması/Onaylanması (Yönetim)
- Yayınlama
- Bildirim (çalışanlar ve ilgili dış taraflar)

A.5.1 Bilgi güvenliği için yönetimin yönlendirmesi

A.5.1.1 Bilgi güvenliği için politikalar

- En üst seviyede «bilgi güvenliği politikası»
  - Yönetim onayı
  - Bilgi güvenliği hedeflerinin yönetimi için yaklaşım
- Bilgi güvenliği politikaları (gereksinimleri içermeli)
  - İş stratejileri
  - Yasa ve düzenlemeler
  - Mevcut ve gelecek için öngörülen bilgi güvenliği tehdit ortamı
  - Bilgi güvenliği ve hedeflerin tanımlanması
  - Bilgi güvenliği ile ilgili tüm faaliyetler için prensipler
  - Belirlenen roller için sorumluluklar

A.5.1 Bilgi güvenliği için yönetimin yönlendirmesi

A.5.1.1 Bilgi güvenliği için politikalar

- Daha alt seviyede bilgi güvenliği politikaları
  - Erişim kontrolü (A.9)
  - Bilginin sınıflandırılması (A.8.2)
  - Fiziksel ve çevresel güvenlik (A.11)
  - Son kullanıcıya yönelik başlıklar
    - Varlıkların kabul edilebilir kullanımı (A.8.1.3)
    - Temiz masa temiz ekran (A.11.2.9)
    - Bilgi transferi (A.13.2.1)
    - Mobil cihazlar ve uzaktan çalışma (teleworking) (A.6.2)
    - Yazılım kurulumu ve kullanımında sınırlamalar (A.12.6.2)

A.5.1 Bilgi güvenliği için yönetimin yönlendirmesi

A.5.1.1 Bilgi güvenliği için politikalar

- Daha alt seviyede bilgi güvenliği politikaları
  - Yedekleme (A.12.3)
  - Kötü amaçlı yazılımlardan korunma (A.12.2)
  - Teknik açıklıkların yönetimi (A.12.6.1)
  - Kriptografik kontroller (A.10)
  - İletişim güvenliği (A.13)
  - Kişisel bilgilerin mahremiyeti ve korunması (A.18.1.4)
  - Tedarikçi ilişkileri (A.15)

- Politikaların çalışanlara ve ilgili taraflara duyurulması (Bilgi güvenliği farkındalığı, öğretimi ve eğitimi (A.7.2.2))

A.5.1Bilgi güvenliği için yönetimin yönlendirmesi

A.5.1.2 Bilgi güvenliği için politikaların gözden geçirilmesi

*Bilgi güvenliği politikaları, belirli aralıklarla veya önemli değişiklikler ortaya çıktığında sürekli uygunluk, kesinlik ve etkinliği sağlamak amacıyla **gözden geçirilmelidir**.*

- Planlı aralıklar
- Önemli değişiklikler ortaya çıktığında
  - Yeni yasal düzenlemeler , Teknik değişiklikler
  - Lokasyon değişiklikleri , Çevresel değişiklikler(Yeni komşular vb.)
- Politikaların gözden geçirilmesi yönetimin gözden geçirmelerini dikkate almalı
- Politika revize olduğundan yönetim onayı
- Gözden geçirme kayıtları

A.6
Bilgi Güvenliği Organizasyonu

2 Güvenlik Kategorisi

- İç Organizasyon
- Mobil Cihazlar ve Uzaktan Çalışma

A.6 Bilgi Güvenliği Organizasyonu

A.6.1 İç organizasyon

Amaç: Kuruluş içerisinde bilgi güvenliği operasyonu ve uygulamasının, başlatılması ve kontrol edilmesi amacıyla, bir yönetim çerçevesi kurmak

A.6.1.1 Bilgi güvenliği rolleri ve sorumlulukları

Tüm bilgi güvenliği sorumlulukları tanımlanmalı ve tahsis edilmelidir.

- Bilgi güvenliiği politikaları paralelinde sorumlulukların tahsisi
- Önemli varlıkların korunması için sorumluluklar
- Bilgi güvenliği risk yönetimi faaliyetleri ve artık risklerin kabulü için sorumlulukların tanımlanması

A.6.1 İç organizasyon

A.6.1.1 Bilgi güvenliği rolleri ve sorumlulukları

- Kişilerin sorumlu oldukları alanların belirlenmesi
  - Varlıklar ve bilgi güvenliği süreçlerinin belirlenmesi ve tanımlanması
  - Yetki seviyelerinin belirlenmesi
- Kişilerin sorumlu olacağı alanların belirlenmesi
  - Yetkinlik
  - Gelişmelerden haberdar olmalarının sağlanması
  - Her varlık ve güvenlik süreci için sorumlu birimin atanması ve sorumluluk detaylarının dokümante edilmesi (A.8.1.2)

A.6.1 İç organizasyon

A.6.1.1 Bilgi güvenliği rolleri ve sorumlulukları

- Sorumlulukların açıkça tanımlanması
  - Verilen sorumlulukların başka kişilere devredilmesi sorumluluğu ortadan kaldırmaz

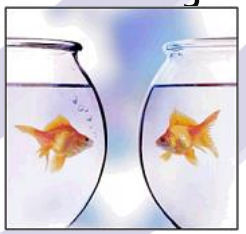
- *Çalışanların günlük bilgi güvenliği sorumlulukları*

A.6.1 İç organizasyon

A.6.1.2 Görevlerin ayrılığı

Çelişen görevler ve sorumluluklar, yetkilendirilmemiş veya kasıtsız değişiklik fırsatlarını veya kuruluş varlıklarının yanlış kullanımını azaltmak amacıyla ayrılmalıdır.

- Bir olayın başlatılması onun yetkilendirilmesinden ayrılmalıdır.
  - Mümkünse yetkiyi veren ile faaliyet yapan farklı kişiler olmalı
  - Mümkün olmaz ise faaliyetlerin izlenmesi denetim kayıtları gibi kontrollerde bu husus dikkate alınmalıdır.
  - Örneğin herhangi bir çalışanın varlıklara erişmesi ve değiştirmesi yetkilendirme ile olmalı



A.6.1 İç organizasyon

A.6.1.3 Otoritelerle iletişim

İlgili otoritelerle uygun iletişim kurulmalıdır.

- Prosedürler (zaman, kiminle temas kurulacak)
  - Resmi kurumlar
    - İtfaiye, adliye
  - Üst kuruluşlar/Düzenleyici kuruluşlar
  - Internet hizmet sağlayıcılar/Telekomünikasyon operatörleri
  - Acil servisler, su, elektrik, soğutma vb.
  - Bilgi güvenliği olaylarının zamanında raporlanması (Yasal ihlal vb. durumlarda)
  - Bilgi güvenliği olay yönetiminin desteklenmesi (A.16)
  - İş sürekliliği planlama sürecinin desteklenmesi (A.17)

Konu ile ilgili Prosedür hazırlanabilir.

A.6.1 İç organizasyon

A.6.1.4 Özel ilgi grupları ile iletişim

Özel ilgi grupları veya diğer uzman güvenlik forumları ve profesyonel dernekler ile uygun iletişim kurulmalıdır.

- İyi uygulamalarla ilgili bilginin geliştirilmesi
- Güvenlikle ilgili bilginin güncellenmesi
- Bilgi güvenliği anlayışının güncel ve tam olmasının güvencesi
- Ataklar ve açıklıklar hakkında alarmlar, tavsiyeler ve yamalarla ilgili erken uyarı
- Bilgi güvenliği uzmanlarına erişim
- Yeni teknolojiler, ürünler, tehditler ve açıklıklar hakkında bilgi paylaşımı
- Uygun bağlantı noktaları (ihlal olayları vb.)

A.6.1 İç organizasyon

A.6.1.5 Proje yönetiminde bilgi güvenliği

Proje yönetiminde, proje çeşidine bakılmaksızın bilgi güvenliği ele alınmalıdır.

- Bilgi güvenliği risklerinin tanımlanması ve projelere entegrasyonu
- Örneğin; çekirdek iş süreci, BT, tesis yönetimi ve diğer destek prosesleri için bir proje
- Proje hedeflerinin bilgi güvenliği hedeflerini içermesi
- Gerekli kontrollerin uygulanması için projenin erken safhalarında bilgi güvenliği risk değerlendirmesinin yapılması
- Bilgi güvenliğinin uygulanan proje metodolojisinin bir parçası olması
- Bilgi güvenliği sorumluluklarının proje yönetimi metotlarında belirlenmesi ve tahsisi,

A.6 Bilgi Güvenliği Organizasyonu

A.6.2 Mobil cihazlar ve uzaktan çalışma

Amaç: Uzaktan çalışma ve mobil cihazların güvenliğini sağlamak

A.6.2.1 Mobil cihaz politikası

*Mobil cihazların kullanımı ile ortaya çıkan risklerin yönetilmesi amacı ile bir **politika** ve destekleyici güvenlik önlemleri belirlenmelidir.*

- Mobil cihazların kullanımı ile ortaya çıkan risklerin yönetilmesi için politika
- Destekleyici güvenlik önlemleri
- Mobil cihaz kullanımında kuruluş bilgisinin ifşasının engellenmesi

A.6.2 Mobil cihazlar ve uzaktan çalışma

A.6.2.1 Mobil cihaz politikası

- Mobil cihaz politikasının kapsamı
  - Mobil cihazların kaydı
  - Fiziksel korunma gerekleri
  - Yazılım kurulumunun sınırlandırılması
  - Mobil cihaz yazılım versiyonları ve yamalar
  - Bilgi sistemlerine bağlantı sınırlamaları
  - Erişim kontrolü
  - Kriptografik teknikler
  - Kötü niyetli yazılım kontrolü
  - Yedeklemeler

A.6.2 Mobil cihazlar ve uzaktan çalışma

A.6.2.2 Uzaktan çalışma

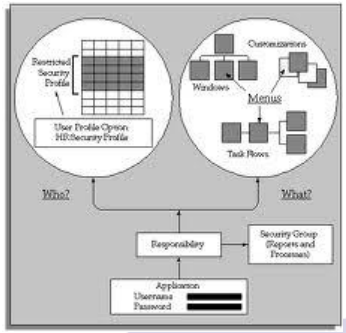
*Uzaktan çalışma alanlarında erişilen, işlenen veya depolanan bilgiyi korumak amacı ile bir **politika** ve destekleyici güvenlik önlemleri uygulanmalıdır.*

- Uzaktan çalışma alanlarının fiziksel korunması
- İletişim güvenlik gerekleri (Uzaktan erişim kuruluşun iç sistemlerine ulaşıyor mu?)
- Uzaktan erişimde yetkisiz erişimler (Aile bireyleri, arkadaşlar vb.)
- Ev ağlarının kullanımı/kablosuz güvenliği
- Yazılım lisanslarının kontrolü
- Kötü yazılım ve güvenlik duvarı gerekleri
- Çalışma saatlerinin tanımlanması/Uzaktan çalışanın dahili sistemlere erişim saatlerinin sınırlandırılması

A.7
İnsan Kaynakları Güvenliği

3 Güvenlik Kategorisi

- İstihdam Öncesi
- Çalışma Esnasında
- İstihdamın sonlandırılması ve değiştirilmesi



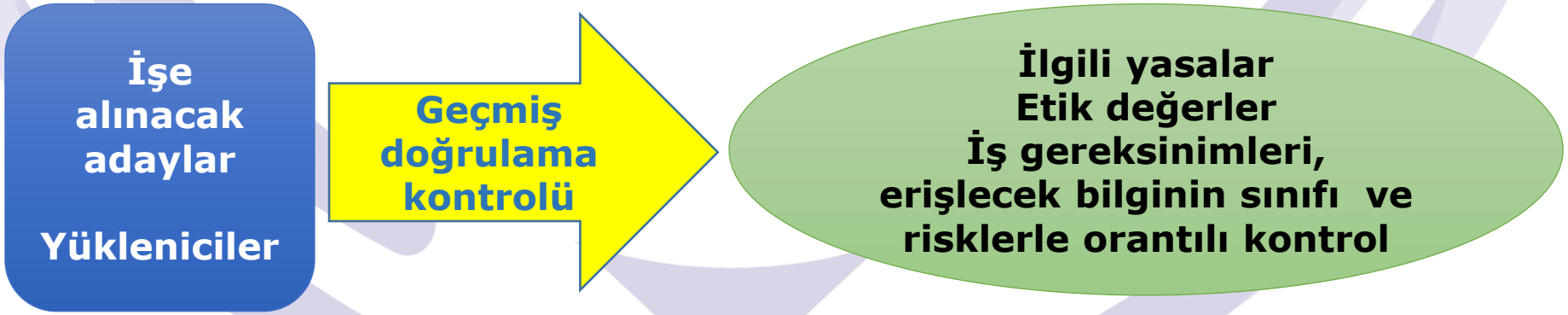
A.7 İnsan Kaynakları Güvenliği

A.7.1 İstihdam öncesi

Amaç: Çalışanlar ve yüklenicilerin kendi sorumluluklarını anlamalarını ve düşünüldükleri roller için uygun olmalarını temin etmek

A.7.1.1 Tarama

- *Tüm işe alım adayları için ilgili yasa, düzenleme ve etiğe göre ve iş gereksinimleri, erişilecek bilginin sınıflandırması ve alınan risklerle orantılı olarak geçmiş doğrulama kontrolleri gerçekleştirilmelidir*



A.7.1 İstihdam öncesi

A.7.1.1 Tarama

- Geçmiş Doğrulama Kontrolleri
  - Özellikle hassas işler için daha detaylı izleme
  - Mahremiyet ve kişisel verilerin korunması
  - Adayın özgeçmişinin kontrolü (eksiksizlik ve doğruluk)
  - Akademik ve diğer profesyonel niteliklerin teyidi
  - Bağımsız/Nitelikli kimlik kontrolü (pasaport vb.)
  - Finansal durum kontrolü (kredi vb.)
  - Kriminal kayıtların kontrolü
  - İşe alım ya da terfilerdeki pozisyon çok gizli bilgilere erişim sağlıyorsa daha detaylı kontroller (Clearance)

A.7.1 İstihdam öncesi

A.7.1.2 İstihdam hüküm ve koşulları

Çalışanlar ve yükleniciler ile yapılan sözleşmeler kendilerinin ve kuruluşun bilgi güvenliği sorumluluklarını belirtmelidir.

- Çalışanlar ve yükleniciler ile yapılan sözleşmeler
  - Kuruluşun ve karşı tarafın bilgi güvenliği sorumluluklarını belirtmeli
  - Bilgiye erişecek tüm çalışanlar ve yüklenicilerle erişim öncesi gizlilik ve ifşa etmeme sözleşmeleri (A.13.2.4)
  - Telif hakları ve veri koruma yasaları ile ilgili sorumluluklar (A.18.1.2, A.18.1.4)
  - Bilgi sınıflandırması ve kuruluş varlıklarının yönetimi ile ilgili sorumluluklar (A.8)

A.7.1 İstihdam öncesi

A.7.1.2 İstihdam hüküm ve koşulları

- Çalışanlar ve yükleniciler ile yapılan sözleşmeler
  - Diğer şirketlerden veya dış taraflardan alınan bilgilerin kullanımı
  - Kuruluşun güvenlik gereklerinin ihmali durumunda yapılacak faaliyetler (A.7.2.3)
  - Tarafların bilgi güvenliği sorumluluk ve yükümlülüklerinin işe alım öncesinde iletilmesi
  - Kurumun kişisel bilgileri muhafazası konusundaki sorumlulukları
  - Mesai saatleri dışındaki sorumluluklar (Evde çalışma vb.)

A.7 İnsan Kaynakları Güvenliği

A.7.2 Çalışma esnasında

Amaç: Çalışanların ve yüklenicilerin bilgi güvenliği sorumluluklarının farkında olmalarını ve yerine getirmelerini temin etmek.

A.7.2.1 Yönetim sorumlulukları

Yönetim, çalışanlar ve yüklenicilerin, kuruluşun yerleşik politika ve prosedürlerine göre bilgi güvenliğini uygulamalarını istemelidir.

- Çalışanlar ve yükleniciler
  - •Bilgi güvenliği rol ve sorumlulukları
  - •Bilgi işleme imkanlarının kullanımı
  - •Organizasyonun güvenlik politikalarının sağlanması için motivasyon
  - •Uygun yetkinliklerin devamlılığının sağlanması

A.7.2 Çalışma esnasında

A.7.2.2 Bilgi güvenliği farkındalığı, eğitim ve öğretimi

Kuruluştaki tüm çalışanlar ve ilgili olan yerlerde, yükleniciler, kendi iş fonksiyonları ile ilgili olduğunda, kurumsal politika ve prosedürlerle ilgili uygun farkındalık eğitim ve öğretimini ve düzenli güncellemeleri almalıdırlar.

- Farkındalık eğitimleri
  - Kurumun güvenlik politikası ve beklentileri
  - Bilgi ve servislere erişim öncesi
- Sürekli eğitim (Periyodik)
  - Güvenlik gereksinimleri, Yasal sorumluluklar
  - Log on süreçleri
  - Yeni işe alınanlar, Yeni yükleniciler
  - Bilgi güvenliği olaylarından çıkarılan dersler

A.7.2 Çalışma esnasında

A.7.2.2 Bilgi güvenliği farkındalığı, eğitim ve öğretimi

- Çalışanlar, (gerektiğinde) yükleniciler
- eğitimleri/öğretim
  - Çalışanın rolüyle uyumluluk
  - Sorumluluklar ve yetkinliklerle uyumluluk
  - Farkındalık artırıcı faaliyetler (Kitapçıklar, broşürler, kampanyalar, bilgi güvenliği günü vb.)

A.7.2 Çalışma esnasında

A.7.2.3 Disiplin süreci

Bir bilgi güvenliği ihlal olayını gerçekleştiren çalışanlara yönelik önlem almak için resmi ve bildirilmiş bir disiplin prosesi olmalıdır.

- Bir güvenlik kırılmasına yol açan çalışanlar için resmi disiplin prosesi
  - Bilgi güvenliği sızmaları (Delil toplama A.16.1.7)
  - Doğru ve adil disiplin süreci
  - Sızmanın doğası, ciddiliği ve iş üzerindeki etkisi
  - Çalışanın ilk hatası mı?/Tekrarlanan bir hata mı?
  - Çalışan uygun şekilde eğitilmiş mi? (İlgili yasalar, iş sözleşmeleri ve diğer faktörler)
  - Önemli sızma durumlarında tüm görevlerden açığa alma, erişim hakları ve ayrıcalıkların kaldırılmasının sağlanması

A.7 İnsan Kaynakları Güvenliği

A.7.3 İstihdamın sonlandırılması ve değiştirilmesi

Amaç: İstihdamın sonlandırılması ve değiştirilmesi sürecinde kuruluşun çıkarlarını korumak.

A.7.3.1 İstihdam sorumluluklarının sonlandırılması veya değiştirilmesi

İstihdamın sonlandırılması veya değiştirilmesinden sonra geçerli olan bilgi güvenliği sorumlulukları ve görevleri tanımlanmalı, çalışan veya yükleniciye bildirilmeli ve yürürlüğe konulmalıdır.

- İstihdamın sonlandırılması/değiştirilmesi
  - Geçerli bilgi güvenliği sorumlulukları ve görevlerinin tanımı
  - Çalışana ya da yükleniciye bildirim
  - Güvenlik gereksinimleri çerçevesinde sonlandırma iletişimi
  - Yasal zorunluluklar

A.7.3 İstihdamın sonlandırılması

A.7.3.1 İstihdam sorumluluklarının sonlandırılması veya değiştirilmesi

- Gizlilik anlaşmalarından kaynaklanan sorumluluklar (A.13.2.4)
- Sonlandırma sonunda belli bir süre devam eden sorumluluk ve şartlar (A.7.1.2) (Çalışan/Yükleniciler)
- İnsan kaynakları birimi,
- Sorumlulukların sonlandırılmasının duyurulması

A.8
Varlık Yönetimi

3 Güvenlik Kategorisi

- Varlıkların Sorumluluğu
- Bilgi Sınıflandırması
- Ortam İşleme




A.8 Varlık Yönetimi

A.8.1 Varlıkların sorumluluğu

Amaç: Kuruluşun varlıklarını tespit etmek ve uygun koruma sorumluluklarını tanımlamak.

A.8.1.1 Varlıkların envanteri

Bilgi ve bilgi işleme tesisleri ile ilgili varlıklar belirlenmeli ve bu varlıkların bir envanteri çıkarılmalı ve idame ettirilmelidir.

- Tanımlama
- Envanterin hazırlanması (Kesin, güncel ve tutarlı)
- Envanterin muhafaza edilmesi

Yaşam döngüsü: Oluşturma, işleme, muhafaza, aktarma, silme, imha.

A.8.1 Varlıkların sorumluluğu

A.8.1.1 Varlıkların envanteri

➢**Varlık Envanterinin Kapsamı**

- Varlık tipi
- Varlık formatı
- Varlığın yeri
- Yedekleme bilgileri
- Lisans bilgileri
- Varlığın değeri
- Varlık sahipliği (8.1.2)
- Varlık sınıfı (8.2)

A.8.1 Varlıkların sorumluluğu

A.8.1.1 Varlıkların envanteri

- Varlık çeşitleri
  - Bilgi varlıkları
  - Yazılım varlıkları
  - Donanımsal varlıklar
  - Haberleşme ile ilgili varlıklar
  - Hizmetler
  - Çalışanlar (Nitelikler, beceriler, tecrübeler)
  - Soyut değerler (itibar, kuruluşun imajı vb.)
  - ..
  - ..

A.8.1 Varlıkların sorumluluğu

A.8.1.1 Varlıkların envanteri

Sıra No	Varlık Grubu	Varlık	Kategori	Varlık Sahibi	Varlık Emanetçisi	Gizlilik Değeri	Bütünlük Değeri	Erişilebilirlik Değeri	Değer	Varlığın Eklenme Tarihi	……	Açıklama
1												
2												
3												

Tablo 1 Örnek bir varlık envanter tablosu

A.8.1 Varlıkların sorumluluğu

A.8.1.2 Varlıkların sahipliği

Envanterde tutulan tüm varlıklara sahip atamaları yapılmalıdır.

- '**Sahip'** varlıkların yaşam döngüsünün (üretimi, geliştirilmesi, bakımı, kullanımı, imhası) kontrolü için onaylanmış yönetim sorumluluğu bulunan kişi veya birimleri tanımlar.
- '**Sahip'** terimi, gerçekten varlık üzerinde mülkiyet hakları olan kişi anlamına gelmez.
- Varlık sahibi ataması
  - Varlık oluşturulduğunda ya da kuruluşa transfer edildiğinde

A.8.1 Varlıkların sorumluluğu

A.8.1.2 Varlıkların sahipliği

- Varlık sahibinin sorumlulukları
  - Varlığın envantere kaydının sağlanması
  - Varlığın uygun şekilde sınıflandırılması ve korunmasının sağlanması
  - Erişim sınırlamaları ve sınıflandırmalarının tanımlanması ve periyodik gözden geçirilmesi
  - Varlığın silinmesi ya da imhasının politikalara uygun yapılması

A.8.1 Varlıkların sorumluluğu

A.8.1.3 Varlıkların kabul edilebilir kullanımı

*Bilgi ve bilgi işleme tesisleri ile ilgili bilgi ve varlıkların kabul edilebilir kullanımına dair kurallar belirlenmeli, **yazılı** hale getirilmeli ve uygulanmalıdır.*

- Varlıkların kabul edilebilir kullanımı
  - Kullanım kurallarının tanımlanması
  - Yazılı hale getirilmesi
  - Uygulanması

A.8.1 Varlıkların sorumluluğu

A.8.1.3 Varlıkların kabul edilebilir kullanımı

- Çalışanlar ve kuruluşun varlıklarını kullanan dış taraflar
  - Bilgi ve bilgi işleme sistemleri ve kaynakları ile ilgili kullanım kurallarına riayet etmeli
    - Bilgi kullanımı ile ilgili hususlar
    - Bilgi İşleme araçları ile ilgili hususlar
    - E-posta ve Internet kullanım kuralları
    - Mobil cihazların kullanımı için kılavuzlar



A.8.1 Varlıkların sorumluluğu

A.8.1.4 Varlıkların iadesi

Tüm çalışanlar ve dış tarafların kullanıcıları, istihdamlarının, sözleşme veya anlaşmalarının sonlandırılmasının ardından ellerinde olan tüm kurumsal varlıkları iade etmelidirler.

- Çalışanlar ve dış taraf kullanıcılar
  - Fiziksel ve elektronik varlıklar
  - Kişisel cihaz kullanımında bilgilerin kuruluşa transferi/cihazdan silinmesi (A.11.2.7)
  - Kuruluşta süren operasyonlar için çalışanda önemli bilgi birikimi olması durumunda, bu bilgi dokümante edilmeli ve kuruluşa transfer edilmeli
  - İş sonlandırma sürecinde bilginin yetkisiz kopyalanmasının engellenmesi

A.8 Varlık Yönetimi

A.8.2 Bilgi sınıflandırma

Amaç: Bilginin kurum için önemine uygun seviyede korunmasını temin etmek.

A.8.2.1 Bilgi sınıflandırması

Bilgi yasal gereksinimler, değeri, kritikliği ve yetkisiz ifşa veya değiştirilmeye karşı hassasiyetine göre sınıflandırılmalıdır.

- Sınıflandırma
  - Erişim kontrol politikası ile tutarlılık

A.8.2 Bilgi sınıflandırma

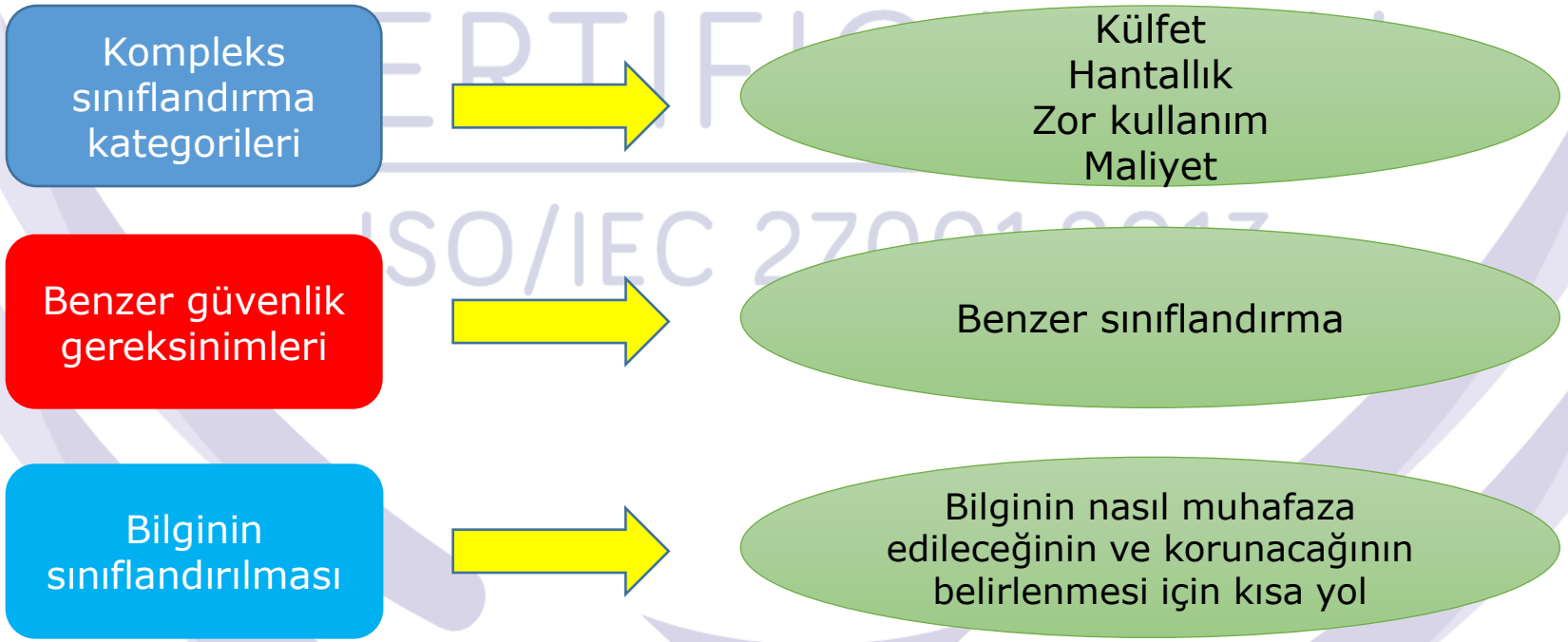
A.8.2.1 Bilgi sınıflandırması

- Varlık sahibinin sorumlulukları
  - Varlığın sınıflandırılması (Bilginin muhafaza edildiği ve işlendiği)
  - Sınıflandırmanın zaman içinde gözden geçirilmesi
  - Koruma seviyesi kriterleri (Gizlilik, bütünlük, erişilebilirlik)
- Erişin Denetimini kolaylaştırır
- Erişim politikası ile tutarlı olmalıdır

A.8.2 Bilgi sınıflandırma

A.8.2.1 Bilgi sınıflandırması

- Sınıflandırma kategorileri



A.8.2 Bilgi sınıflandırma

A.8.2.1 Bilgi sınıflandırması

Bilgi gizliliği sınıflandırması için örnek

1. Bilginin ifşası zarar vermez
2. Bilginin ifşası küçük sıkıntı ya da küçük operasyonel uygunsuzluk yaratır
3. Bilginin ifşası operasyonlarda ya da hedeflerde önemli derecede kısa süreli etki yaratır
4. Bilginin ifşası uzun vadeli stratejik hedeflerde ciddi etki yaratır ya da kuruluşun işine devam etmesini engeller

A.8.2 Bilgi sınıflandırma

A.8.2.1 Bilgi sınıflandırması

	Varlık Değerleri			
Güvenlik Hedefi	DÜŞÜK	ORTA	YÜKSEK	ÇOK YÜKSEK
GİZLİLİK	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz. Açığa çıkan kritik seviyesi altındaki bilgi kurumu etkilemez /çok az etkiler.	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz. Açığa çıkan kritik seviyesi altındaki bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkar. Açığa çıkan kritik bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkar. Açığa çıkan kritik bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.
BÜTÜNLÜK	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen kritik seviyesi altındaki bilgi kurumu etkilemez / çok az etkiler.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen kritik seviyesi altındaki bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişir. Kontrol dışı değişen kritik bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişir. Kontrol dışı değişen kritik bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.
ERİŞİLEBİLİRLİK/ KULLANILABİLİRLİK	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen kritik seviyesi altındaki bilgi kurumu etkilemez / çok az etkiler.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen kritik seviyesi altındaki bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilemez. Erişilebilirliğine zarar gelen bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilemez. Erişilebilirliğine zarar gelen bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.

Tablo 2 Güvenlik hedefi varlık değeri tablosu

A.8.2 Bilgi sınıflandırma

A.8.2.2 Bilgi Etiketleme

Bilgi etiketleme için uygun bir prosedür kümesi kuruluş tarafından benimsenen sınıflandırma düzenine göre geliştirilmeli ve uygulanmalıdır.

Bilgi Etiketleme

- Bilgi ve ilgili varlıkların etiketlenmesi için uygun prosedürler (Bilginin sınıflandırılmasına paralel A.8.2.1)
- Fiziksel bilgi varlıkları
- Elektronik ortamda bilgi varlıkları

A.8.2 Bilgi sınıflandırma

A.8.2.2 Bilgi etiketleme

- Sistemden çıkış yapan kritik veya hassas olarak sınıflandırılmış bilgilerin etiketlenmesi
- Etiketleme/Bilginin paylaşımı için önemli gereksinim
- Basılı raporlar
- Kayıt ortamları (Disk, CD, teyp kasetleri vb.)
- Elektronik mesajlar
- Fiziksel etiketleme
- Elektronik ortamda etiketleme (watermarks, dosya açılışında gelen bildirimler vb.)

A.8.2 Bilgi sınıflandırma

A.8.2.3 Varlıkların kullanımı

*Varlıkların kullanımı için **prosedürler**, kuruluş tarafından benimsenen sınıflandırma düzenine göre geliştirilmeli ve uygulanmalıdır.*

- Her Bilgi düzeyine mahsus koruma gereklilikleri
- Yetkilendirme sonrası bilginin kullanımı
- Prosedür
  - Güvenli işleme
  - Depolama/Arşivleme
  - Aktarım , İmha

A.8 Varlık Yönetimi

A.8.3 Ortam işleme

Amaç: Ortamda depolanan bilginin yetkisiz ifşasını, değiştirilmesini, kaldırılmasını ve yok edilmesini engellemek.

A.8.3.1 Taşınabilir ortam yönetimi

*Taşınabilir ortam yönetimi için **prosedürler,** kuruluş tarafından benimsenen sınıflandırma düzenine göre uygulanmalıdır.*

- Taşınabilir ortam yönetimi için prosedür
- Elden çıkarılacak teyp, disk, disket, kaset, hafıza kartlarındaki bilgilerin temizlenmesi

A.8.3 Ortam işleme

A.8.3.1 Taşınabilir ortam yönetimi

- Organizasyondan çıkarılacak ortam için yetkilendirme ve kayıt
- Depolama ortamlarının üreticinin önerileri doğrultusunda muhafaza edilmesi
- Ortamın ömrü çerçevesinde yedekleme
- Taşınabilir ortamın kayıtları
- Sadece gerekli olan sürücü ve portların aktive edilmesi

A.8.3 Ortam işleme

A.8.3.2 Ortamın yok edilmesi

- Güvenli imha prosedürü (formal)
- Hassas bilginin sızmasının engellenmesi
- Bilginin hassaslığı ile orantılı imha prosedürü
- Yakma, kağıt kırpma, kırma, kimyasal kullanımı vb.
- Güvenli imha gerektiren ortamların listesi
- Ortam toplama ve imha için dış kaynak kullanımı (sözleşme vb.)
- Hassas ortam imha kayıtları (tutanak vb.)

A.8.3 Ortam işleme

A.8.3.3 Fiziksel ortam aktarımı

Bilgi içeren ortam, kuruluşun fiziksel sınırları ötesinde nakil esnasında, yetkisiz erişime, kötüye kullanıma ya da bozulmalara karşı korunmalı

- Güvenilir araç veya kuryeler kullanılmalı
- Yetkili kuryelerin listesi yönetimce belirlenmeli
- Kuryelerin tanımlanması için prosedür geliştirilmeli
- Nakil esnasında varlığı fiziksel hasardan koruyacak paketlemeler yapılmalı
- Ortamın içeriği, uygulanacak korunma, transfer sayısı vb. için logların tutulması

A.9
Erişim Kontrolü

4 Güvenlik Kategorisi

- Erişim kontrolünün iş gereklilikleri
- Kullanıcı erişim yönetimi
- Kullanıcı sorumlulukları
- Sistem ve uygulama erişim kontrolü

A.9 Erişim Kontrolü

A.9.1 Erişim kontrolü için iş gereksinimi

Amaç: Bilgiye ve bilgi işleme olanaklarına erişimi kontrol etmek.

A.9.1.1 Erişim kontrol politikası

*Bir erişim kontrol **politikası**, iş ve bilgi güvenliği şartları temelinde oluşturulmalı, **yazılı** hale getirilmeli ve **gözden** geçirilmelidir.*

- Varlık sahibi belirlemeli
  - Erişim kontrol kuralları
  - Erişim hakları
  - Sınırlamalar

A.9.1 Erişim kontrolü için iş gereksinimi

A.9.1.1 Erişim kontrol politikası

- Erişim denetimi (fiziksel)
- Erişim denetimi (mantıksal:DMZ, Aktif Dizin, vb.))
- Politika
  - İş uygulamalarının güvenlik ihtiyaçları
  - Bilmesi gereken kadar prensibi
  - Erişim hakları ile bilgi sınıflandırma politikalarının uyumu
  - Personelin erişim kontrol kuralları ve hakları

A.9.1 Erişim kontrolü için iş gereksinimi

A.9.1.1 Erişim kontrol politikası

- Bilginin yayılması ve yetkilendirme ile ilgili politikalar
- Dokümante politika/gözden geçirme
- Güvenlik seviyeleri ve "gerektiği kadar bilme" prensibi
- Farklı sistem ve ağlardaki bilginin sınıflandırılması
- Bilgiye erişimle ilgili olarak kontratlardan ve yasal yükümlülüklerden kaynaklanan şartların yerine getirilmesi
- Kurumun yaygın kullanıcı profilleri ile ilgili erişim hakları
- Erişimin talep edilmesi, yetkilendirilmesi ve yönetilmesi görevlerinin birbirinden ayrılması
- Erişim haklarının sonlandırılması

A.9.1 Erişim kontrolü için iş gereksinimi

A.9.1.2 Ağlara ve ağ hizmetlerine erişim

Kullanıcılara sadece özellikle kullanımı için yetkilendirildikleri ağ ve ağ hizmetlerine erişim verilmelidir.

- Ağ ve hizmetlere erişim politikası olmalıdır
  - Erişimine izin verilen ağ ve ağ hizmetleri
  - Kimin hangi ağ ve ağ hizmetlerine erişeceğini belirleyen yetkilendirme prosedürleri
  - Ağ ve ağ hizmetlerine erişim yolları (VPN, wireless vb.)
  - Ağ hizmetlerinin kullanımının izlenmesi

A.9 Erişim Kontrolü

A.9.2 Kullanıcı erişim yönetimi

Amaç: Yetkili kullanıcı erişimini temin etmek ve sistem ve hizmetlere yetkisiz erişimi engellemek

A.9.2.1 Kullanıcı kaydetme ve kayıt silme

*Erişim haklarının atanmasını sağlamak için, resmi bir kullanıcı kaydetme ve kayıt silme **prosesi** uygulanmalıdır.*

- User ID yönetim süreci
  - Kullanıcı kimliklerinin her kullanıcı için farklı olması (Unique user ID)
  - Paylaşımlı ID'ler (Shared ID) sadece gerekli olduğunda
  - Kuruluştan ayrılanların kullanıcı kimliklerinin hemen iptali
  - Kullanıcı kimliklerinin periyodik kontrolü ve gereksiz kimliklerin iptali

A.9.2 Kullanıcı erişim yönetim

A.9.2.2 Kullanıcı erişimine izin verme

*Tüm kullanıcı türlerine tüm sistemler ve hizmetlere erişim haklarının atanması veya iptal edilmesi için resmi bir kullanıcı erişim izin **prosesi** uygulanmalıdır.*

- Erişime izin verme süreci
  - Bilgi sistemi ya da hizmetin sahibinden yetkinin alınması (A.8.1.2)
  - Verilen erişim yetkisinin erişim politikaları ile uyumunun kontrolü (A.9.1)
  - Görevlerin ayrılığı ile uyum (A.6.1.2)
  - Merkezi erişim hakları kayıtlarının muhafazası
  - İş ve rol değiştiren kullanıcıların erişim haklarının anında düzenlenmesinin sağlanması
  - Bilgi sistemleri ya da hizmetlerinin sahipleri ile erişim haklarının gözden geçirilmesi

A.9.2 Kullanıcı erişim yönetim

A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi

Ayrıcalıklı erişim haklarının tahsis edilmesi ve kullanımı kısıtlanmalı ve kontrol edilmelidir.

- Ayrıcalıklı erişim haklarının tahsisi
  - işletim sistemi, veri tabanı yönetim sistemi , EBYS Sistemi gibi yetkilendirmeler
    - Ayrıcalıkların kullanımının sınırlandırılması ve denetlenmesi
    - "Gerektiği kadar kullandır" prensibi (Fonksiyonel role göre)
  - Ayrıcalıkların tahsisi için yetki süreci
  - Mevcut ayrıcalıkların kayıtları

A.9.2 Kullanıcı erişim yönetim

A.9.2.4 Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi

Gizli kimlik doğrulama bilgisinin tahsis edilmesi, resmi bir yönetim prosesi yoluyla kontrol edilmelidir.

- Kullanıcıların kişisel gizli kimlik doğrulama bilgilerini gizli tutması
- Grup bilgilerini grup dışına aktarmama için sözleşme imzalanması (Genellikle istihdam sırasında)
- Personelin kendi gizli bilgisini (parola vb.) istemesi durumunda geçici parola verilmesi/ilk girişte değiştirmeye zorlanması
- Geçici gizli kimlik doğrulama bilgisinin eşsiz olması ve kolay tahmin edilemez olması
- Geçici gizli kimlik doğrulama bilgisinin kullanıcıya güvenli ortamlarda iletilmesi (korunmasız e-posta vb. kullanılmaması) ve aldığının teyit etmesinin sağlanması

A.9.2 Kullanıcı erişim yönetim

A.9.2.5 Kullanıcı erişim haklarının gözden geçirilmesi

Varlık sahipleri kullanıcıların erişim haklarını düzenli aralıklarla ***gözden geçirmelidir****.*

- Periyodik gözden geçirme (6 ay, 1 yıl veya değişikliklerde)
  - İşe giriş
  - Terfi
  - Görevden alınma
  - Geçici görev
  - İşten çıkma
- Ayrıcalıklı hakların gözden geçirilmesi daha sık periyotlarda yapılmalı

Not: Bu kontrol 9.2.1, 9.2.2 ve 9.2.6 daki kontrol lerin yürütülmesinde olası zayıflıkları dengeler.

A.9.2 Kullanıcı erişim yönetimi

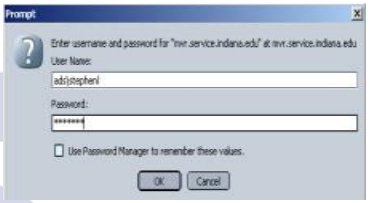
A.9.2.6 Erişim haklarının kaldırılması veya düzenlenmesi

Tüm çalışanların ve dış taraf kullanıcılarının bilgi ve bilgi işleme tesislerine erişim yetkileri, istihdamları, sözleşmeleri veya anlaşmaları sona erdirildiğinde kaldırılmalı veya bunlardaki değişiklik üzerine düzenlenmelidir.

- Tüm çalışanlar ve dış taraf kullanıcılar
  - Bilgi ve bilgi işleme olanaklarına erişim yetkileri
    - İstihdam, sözleşme veya anlaşmalar sona erdirildiğinde kaldırılmalı
    - Sona erdirmenin kim tarafından yapıldığı önemli (çalışan, dış taraf, yönetim vb.)
    - Çalışanın ya da dış taraf kullanıcının mevcut sorumlulukları
    - Halen erişilebilir olan varlığın değeri

A.9 Erişim Kontrolü

A.9.3 Kullanıcı sorumlulukları



Amaç: Yetkili kullanıcı erişimini temin etmek ve sistem sistem, hizmetlere yetkisiz erişimi engellemek

A.9.3.1 Gizli kimlik doğrulama bilgisinin kullanımı

Kullanıcıların, gizli kimlik doğrulama bilgisinin kullanımında kurumsal uygulamalara uymaları şart koşulmalıdır.

- Kimlik doğrulama bilgilerinin gizli tutulması
- Kimlik doğrulama bilgilerinin kağıda, bilgisayara ya da başka bir ortama yazılmaması
- Şüphelenilen durumlarda değiştirme
- Parola kullanılıyorsa nitelikli parola kullanımı
- Kolay hatırlanabilir, tahmin edilemez, sözlük saldırılarına zaafiyeti olmayan, alfanumerik vb.

A.9 Erişim Kontrolü

A.9.4 Sistem ve uygulama erişim kontrolü

Amaç: Sistem ve uygulamalara yetkisiz erişimi engellemek

A.9.4.1 Bilgiye erişimin kısıtlanması

Bilgi ve uygulama sistem fonksiyonlarına erişim, erişim kontrol politikası doğrultusunda kısıtlanmalıdır.

- Uygulama sistem fonksiyonlarına erişim için menüler oluşturulması
- Hangi verinin hangi kullanıcı tarafından erişilebilir olacağının kontrolü
- Erişim haklarının kontrolü (okuma, yazma, silme, vb.)
- Hassas uygulamalara, uygulama verilerine ve sistemlerine fiziksel ve mantıksal erişim kontrolleri

A.9.4 Sistem ve uygulama erişim kontrolü

A.9.4.2 Güvenli oturum açma teknikleri

Erişim kontrol politikası tarafından şart koşulduğu yerlerde, sistem ve uygulamalara erişim güvenli bir oturum açma prosedürü tarafından kontrol edilmelidir.

- Sistem ve uygulamaya ilişkin olarak yetkisiz kullanıcıya yardımcı olabilecek bilgilerin oturuma giriş başarıyla tamamlanana kadar gizlenmesi
- Bilgisayarda sadece yetkili personel tarafından erişilebileceğini bildiren uyarı mesajı gösterilmesi
- Çok sağlam kullanıcı kimlik denetimi gerektiğinde paroladan başka alternatifler (kriptografi, akıllı kart)


A.9.4 Sistem ve uygulama erişim kontrolü

A.9.4.2 Güvenli oturum açma teknikleri

- Oturuma girişin sadece tüm girdi verilerinin doğrulanmasından sonra sağlanması
- Bir hata durumu varsa, sistemin verinin hangi kısmının doğru veya yanlış olduğu bilgisini gizlemesi
- Sistem tarafından izin verilen başarısız giriş denemelerine sınırlama getirilmesi
- Oturuma giriş işlemi için zaman sınırı konulması
- Başarısız giriş denemelerinin kaydı
- Ağ üstünden şifrenin açık olarak gönderilmemesi

A.9.4 Sistem ve uygulama erişim kontrolü

A.9.4.3 Parola yönetim sistemi

Parola yönetim sistemleri etkileşimli olmalı ve kaliteli parolaları temin etmelidir.

- Nitelikli parola sistemleri
- Kullanıcıların bireysel parolaların kullanımına zorlanması
- Kullanıcıların kendi parolalarını seçmelerine ve değiştirmelerine izin verilmesi
- Kullanıcıyı kuvvetli parola seçmeye zorlama
- Kullanıcıyı belli zamanlarda parolasını değiştirmeye zorlama
- Sisteme ilk girişte geçici parolayı değiştirmeye zorlama
- Eski parolaların kaydının saklanması tekrar kullanılmalarına engel olunması
- Parolaların korumalı formda saklanması ve iletilmesi

A.9.4 Sistem ve uygulama erişim kontrolü

A.9.4.4 Ayrıcalıklı destek programlarının kullanımı

Sistem ve uygulamaların kontrollerini ezme kabiliyetine sahip olabilen destek programlarının kullanımı kısıtlanmalı ve sıkı bir şekilde kontrol edilmelidir.

- Destek programları
- Tanımlama, kullanıcı kimlik denetimi, yetkilendirme kullanımı
- Destek programlarının uygulama yazılımından ayrılması
- Destek programı kullanımının sınırlandırılması (güvenilir, yetkili kullanıcılar için)
- Tüm destek programlarının loglarının tutulması
- Yetkilendirme seviyelerinin belirlenmesi ve dokümante edilmesi

A.9.4 Sistem ve uygulama erişim kontrolü

A.9.4.5 Program kaynak koduna erişim kontrolü

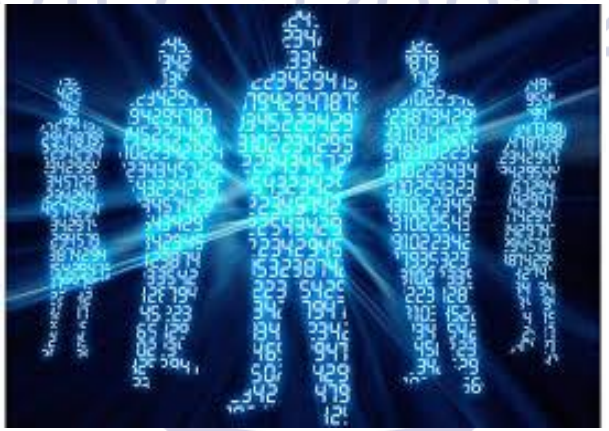
Program kaynak koduna erişim kısıtlanmalıdır

- Kaynak kodlarının bulunduğu kütüphanelere erişim sıkı bir şekilde denetlenmeli
- Kaynak kodları operasyonel sistemlerle birlikte tutulmamalı
- Destek personeli sınırsız erişime sahip olmamalı
- Program kaynak kod kütüphanelerine erişim logları tutulmalı
- Program kaynak kütüphanelerinin bakım ve kopyalanması sıkı bir şekilde kontrol edilmeli (Değişim kontrol prosedürleri)

A.10 Kriptografi

1 Güvenlik Kategorisi

- Kriptografik kontroller


A.10 Kriptografi

A.10.1 Kriptografik kontroller

Amaç: Bilginin gizliliği, aslına uygunluğu ve/veya bütünlüğünün korunması için kriptografinin doğru ve etkin kullanımını temin etmek

A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika

Bilginin korunması için kriptografik kontrollerin kullanımına dair bir politika geliştirilmeli ve uygulanmalıdır.

- Kriptografik kontrol kullanımı için genel prensipler ve yönetimin konuya yaklaşımı
- Kullanılacak güvenlik seviyesine karar vermek için risk değerlendirmesi

A.10.1 Kriptografik kontroller

A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika

- Kriptografi politikası
  - Taşınabilir ortamlar ve iletişim kanallarındaki hassas bilginin korunması için kriptografik kontrollerin uygulanması
  - Anahtar yönetimi ile ilgili güvenlik hususları (anahtarın saklanması, anahtarın kaybolması durumunda şifrelenmiş bilginin kurtarılması)
  - Roller ve sorumluluklar
    - Politikanın uygulanması
    - Anahtar yönetimi (anahtar üretimi dahil)

A.10.1 Kriptografik kontroller

A.10.1.2 Anahtar yönetimi

Kriptografik anahtarların kullanımı, korunması ve yaşam süresine dair bir politika geliştirilmeli ve tüm yaşam çevirimleri süresince uygulanmalıdır.

- Kriptografik anahtarların korunması
  - Değiştirilmeye, Kaybedilmeye, Yetkisiz açıklanmaya
  - Tahribata karşı
- Anahtarların üretilmesinde, saklanmasında ve arşivlenmesinde kullanılan cihazlar için fiziksel koruma
- Standartlar, prosedürler ve güvenli yöntemler seti
  - Farklı şifreleme sistemleri ve farklı uygulamalar için anahtarların üretimi
  - Açık anahtar sertifikası üretimi ve edinimi

A.10.1 Kriptografik kontroller

A.10.1.2 Anahtar yönetimi

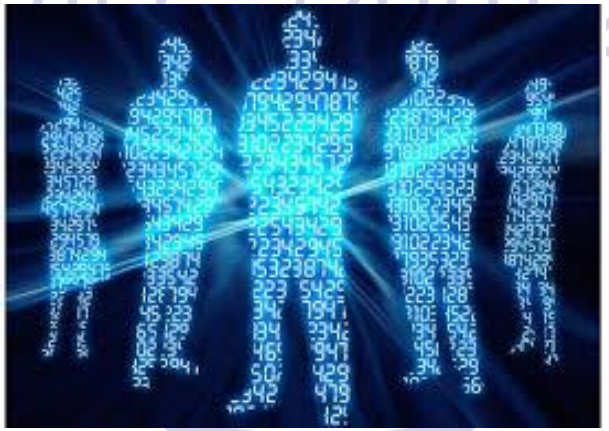
- Standartlar, prosedürler ve güvenli yöntemler seti

  - Teslim alındığında anahtarların nasıl etkinleştirileceği
  - Anahtarların amaçlanan kullanıcılara dağıtımı
  - Yetkili kullanıcıların anahtarlara nasıl erişebileceğinin belirlenmesi
  - Anahtarların saklanması
  - Anahtarların ne zaman değiştirilmesi gerektiği
  - Anahtarların değiştirilmesi ya da güncellenmesi
  - Anahtar değiştirmenin nasıl yapılması gerektiği konusundaki kurallar
  - Zarar görmüş anahtarlara müdahale

A.11
Fiziksel ve Çevresel Güvenlik

2 Güvenlik Kategorisi

- Güvenli alanlar
- Teçhizat


A.11 Fiziksel ve Çevresel Güvenlik

A.11.1 Güvenli alanlar

Amaç: Yetkisiz fiziksel erişimi, kuruluşun bilgi ve bilgi işleme olanaklarına hasar verilmesi ve müdahale edilmesini engellemek

A.11.1.1 Fiziksel güvenlik çevresi

Hassas veya kritik bilgi ve bilgi işleme tesislerini barındıran alanları korumak için güvenlik sınırları tanımlanmalı ve kullanılmalıdır.

- Güvenlik çevreleri
  - Duvarlar (Sağlam/Kesintisiz)
  - Yetkisiz girişi engelleyen dış kapılar (Barlar, alarmlar, kilitler vb.)
  - Kart kontrollü giriş kapıları, Resepsiyon masaları
  - Varlığın güvenlik gereksinimleri ile uyumlu kontroller
  - Risk değerlendirmelerinin sonuçları ile uyumlu kontroller
  - Yangın kapılarının izlenmesi ve testi

A.11.1 Güvenli alanlar

A.11.1.2 Fiziksel giriş kontrolleri

Güvenli alanlar, sadece yetkili personele erişim izni verilmesini temin etmek için uygun giriş kontrolleri ile korunmalıdır.

- Yetkili personelin erişimi
- Ziyaretçi giriş-çıkış tarih ve zamanlarının kaydı
- Daha önce erişimi onaylanmamış ziyaretçilere nezaret
- Ziyaretçilerin güvenlik gereksinimleri ve acil durum halleri konularında bilgilendirilmesi
- Hassas bilgi içeren alanlara erişimin daha sıkı denetimi (giriş kontrol kartı ile birlikte şifreli giriş, retina tarama, parmak izi vb., erişim kayıtlarının muhafazası)

A.11.1 Güvenli alanlar

A.11.1.2 Fiziksel giriş kontrolleri

- Görünür kimlik kartlarının taşınması (Çalışanlar, yüklenici, 3. taraf kullanıcılar ve ziyaretçiler)
- 3. taraf destek personelinin güvenli alanlara ve hassas bilgi işlenen tesislere sadece gerektiğinde erişimi
- Güvenli alanlara erişim haklarının düzenli gözden geçirilmesi, güncellenmesi ve gerektiğinde iptali (A.9.2.5, A.9.2.6)

A.11.1 Güvenli alanlar

A.11.1.3 Ofislerin, odaların ve tesislerin güvenliğinin sağlanması

Ofisler, odalar ve tesisler için fiziksel güvenlik tasarlanmalı ve uygulanmalıdır.

- Ofisler, odalar, tesisler
  - Fiziksel güvenlik
  - Özel tesislere kamunun erişiminin engellenmesi
  - Uygun olduğunda binaların farkedilmesinin/göze batmasının engellenmesi (Minimum tabela bilgisi, bina içinde ya da dışında bilgi işleme tesislerine dair işaret olmaması vb.)
  - Hassas bilgi işleme tesislerine dair klavuz ve telefon rehberlerinin kamu tarafından kolay erişilebilir olmaması

A.11.1 Güvenli alanlar

A.11.1.4 Dış ve çevresel tehditlere karşı koruma

Doğal felaketler, kötü niyetli saldırılar veya kazalara karşı fiziksel koruma tasarlanmalı ve uygulanmalıdır.

- Yangın , Sel/Su baskını ,Deprem ,Patlama, İsyan
- Komşu binalar (Yangın vb.)
- Çatıda/ Bodrum katlarda su kaçağı
- Zehirli ve yanıcı malzemelerin güvenli alanlardan uzak güvenli yerlerde muhafazası
- Yedekleme ortamının ana binadan güvenli bir mesafede muhafazası
- Uygun yangınla mücadele ekipmanının temini ve uygun şekilde konuşlandırılması

A.11.1 Güvenli alanlar

A.11.1.5 Güvenli alanlarda çalışma

*Güvenli alanlarda çalışma için **prosedürler** tasarlanmalı ve uygulanmalıdır.*

- Fiziksel koruma
- Personelin sadece gerektiği zaman güvenli alanın varlığından ya da oradaki aktivitelerden haberdar olması
- Güvenli alanlarda gözetimsiz çalışmanın engellenmesi (Güvenlik sebepleri/Kötü niyetli faaliyet fırsatlarını engellemek)
- Kullanılmayan güvenli alanların kilitlenmesi ve periyodik kontrolü
- Kamera, ses cihazı, fotoğraf makinesi vb. kayıt cihazlarının yetkisiz girişinin engellenmesi
- Çalışanlar, yükleniciler, dış taraflar gözönüne alınmalı
- Güvenli alanda yapılan faaliyetler düzenlenmeli

A.11.1 Güvenli alanlar

A.11.1.6 Teslimat ve yükleme alanları

Yetkisiz kişilerin tesise giriş yapabildiği, teslimat ve yükleme alanları gibi erişim noktaları ve diğer noktalar kontrol edilmeli ve mümkünse yetkisiz erişimi engellemek için bilgi işleme tesislerinden ayrılmalıdır.

- Yükleme alanlarına bina dışından sadece yetkilendirilmiş personelin erişimi
- Yükleme alanlarının binanın diğer bölümlerine erişimi engelleyecek şekilde tasarlanması
- İç kapılar açıldığında dış kapıların güvenliğinin sağlanması
- Gelen malzemelerin kullanım yerlerine yönlendirilmeden önce potansiyel tehditler için incelenmesi
- Gelen malzemenin varlık yönetim prosedürlerine göre kaydı (A.8)
- Gelen/Giden yüklemenin birbirinden ayrılması

A.11 Fiziksel ve Çevresel Güvenlik

A.11.2 Teçhizat

Amaç: Varlıkların kaybedilmesi, hasar görmesi, çalınması veya ele geçirilmesini ve kuruluşun faaliyetlerinin kesintiye uğramasını engellemek.

A.11.2.1 Teçhizat yerleştirme ve koruma

Teçhizat, çevresel tehditlerden ve tehlikelerden ve yetkisiz erişim fırsatlarından kaynaklanan riskleri azaltacak şekilde yerleştirilmeli ve korunmalıdır.

- Çevresel tehditler/tehlikelerden kaynaklanan riskler
- Yetkisiz erişim fırsatları
- Fiziksel tehditler
- Elektrik, kablolama vb.

A.11.2 Teçhizat

A.11.2.1 Teçhizat yerleştirme ve koruma

- Teçhizat uygun şekilde yerleştirilmesi (Hassasiyet, Özel koruma, izolasyon vb..)
- Potansiyel fiziksel tehdit risklerinin minimizasyonu
  - Hırsızlık, patlayıcılar, su baskını/kesintisi toz, titreşim, kimyasal etkiler, elektrik akımı değişimleri, iletişim etkileşimleri, elektromanyetik radyasyon
- Ekipmanların yakınında yeme, içme ve sigara vb. hususların belirlenmesi
- Teçhizatı etkileyebilecek sıcaklık, nem, vb. parametrelerin izlenmesi
- Tüm binalarda yıldırım/şimşekten korunma, topraklama
- Endüstriyel alanlarda özel koruma yöntemleri (klavye kılıfı vb.)

A.11.2 Teçhizat

A.11.2.2 Destekleyici altyapı hizmetleri

Teçhizat destekleyici altyapı hizmetlerindeki hatalardan kaynaklanan enerji kesintileri ve diğer kesintilerden korunmalıdır.

- Destek Araçları
  - Elektrik , Su, Kanalizasyon
  - Isıtma/Havalandırma
  - İklimlendirme (Klima vb.)
  - Düzenli olarak gözden geçirme/test
  - Kritik iş operasyonları için UPS
  - Beklenmedik durum planları/Jenerator (Yakıt stoğu)
  - Düzenli kontrol/test (UPS-Jenerator)
  - Farklı güç kaynakları
  - Acil durum aydınlatması ve iletişim

A.11.2 Teçhizat

A.11.2.3 Kablolama güvenliği

Veri veya destekleyici bilgi hizmetlerini taşıyan enerji ve telekomünikasyon kabloları, dinleme, girişim oluşturma veya hasara karşı korunmalıdır

- Güç ve iletişim Kabloları
  - Yeraltı/sıvaaltı kablo kanalları
  - Ağ kablolamasının yetkisiz dinleme veya hasardan korunması (kablo güzergahının kamu alanlarından geçmemesi vb.)
  - Güç ve iletişim kablolarının birbirinden ayrılması
  - Açık ve net kablo ve teçhizat etiketleme (Ağ kablolarının yanlış switch/porta takılmasının engellenmesi)
  - Dokümante switch/port listesi

A.11.2 Teçhizat

A.11.2.3 Kablolama güvenliği

- Hassas/Kritik sistemler
  - Kontrol ve sonlandırma noktalarında kilitli odalar/paneller
  - Alternatif routing/aktarma ortamları
- Optik kablolama
  - Kabloların korunması için elektromanyetik kalkan/koruma kullanımı
  - Kablolara bağlı yetkisiz cihazlar için teknik temizlik ve fiziksel inceleme başlatılması
  - Patch paneller ve kablo odalarına kontrollü erişim sağlanması

A.11.2 Teçhizat

A.11.2.4 Teçhizat bakımı

Teçhizatın bakımı, sürekli erişilebilirliğini ve bütünlüğünü temin etmek için doğru şekilde yapılmalıdır.

- Sürekli kullanılabilirliğin , Bütünlüğün sağlanması
- Bakımın tedarikçinin belirlediği servis aralıklarında yapılması
- Tamir, bakım ve servis ekipmanlarının sadece yetkili bakım personeli tarafından yapılması
- Şüpheli durumların ve arızaların, önleyici ve düzeltici faaliyetlerin kaydının tutulması
- Kurum dışından gelen bakım personeli için kontroller
- Bakım personelinin güvenilirliğinin (clearance) sağlanması
- Bakım öncesi hassas bilgilerin cihazdan çıkarılması
- Sigorta kurallarına uyulması

A.11.2 Teçhizat

A.11.2.5 Varlıkların taşınması

Teçhizat, bilgi veya yazılım ön yetkilendirme olmaksızın kuruluş dışına çıkarılmamalıdır.

- Kuruluştan varlık çıkarılmasına izin verecek yetkiye sahip personelin belirlenmesi
- Varlık taşınması için zaman limitlerinin belirlenmesi ve varlığın geri getirilmesinin kontrolü
- Varlıkların kuruluş dışına çıkması ve geri getirilmesinin kayıtlarının tutulması
- Nokta kontrollerin yapılması (Yetkisiz kayıt cihazları, silah vb. kuruluşa giriş/çıkışı)

A.11.2 Teçhizat

A.11.2.6 Kuruluş dışındaki teçhizat ve varlıkların güvenliği

Kuruluş dışındaki varlıklara, kuruluş yerleşkesi dışında çalışmanın farklı riskleri de göz önünde bulundurularak güvenlik uygulanmalıdır.

- Kuruluş dışında kullanılacak bilgi işleme ekipmanlarının yönetim tarafından yetkilendirilmesi
- Kuruluş dışına çıkarılan teçhizat ve ortamların kamuya açık yerlerde gözetimsiz bırakılmaması
- Taşınabilir bilgisayarların yolculuklarda el bagajı olarak taşınması

A.11.2 Teçhizat

A.11.2.6 Kuruluş dışındaki teçhizat ve varlıkların güvenliği

- Üretici uyarılarına uyum (Güçlü elektromanyetik alanlara maruz kalma vb.)
- Evde çalışma için kontrollerin belirlenmesi (Risk değerlendirme, bilgisayarlar için erişim kontrolü vb.)
- Kuruluş dışındaki teçhizat için sigorta
- Hasar, çalınma vb. güvenlik riskleri bölgeye göre değişebilir
- Bilgi işleme ve depolama araçları (Kişisel bilgisayarlar, organizers, mobil telefonlar, akıllı kartlar, kağıt vb.)

A.11.2 Teçhizat

A.11.2.7 Teçhizatın güvenli olarak elden çıkarılması veya tekrar kullanımı

Depolama ortamı içeren teçhizatların tüm parçaları, yok etme veya tekrar kullanımdan önce tüm hassas verilerin ve lisanslı yazılımların kaldırılmasını veya güvenli bir şekilde üzerine yazılmasını temin etmek amacıyla doğrulanmalıdır.

- Depolama birimi bulunan tüm teçhizat
  - Hassas veri /Lisanslı yazılım için kontrol
  - Teçhizat ya da içindeki hassas bilginin yok edilmesi
  - Normal silme/formatlama yerine üst düzey yok etme
  - Arızalı cihazların risk değerlendirmesi (tamir/yoketme)
  - Dikkatsiz elden çıkarma/yeniden kullanma bilgiyi riske atabilir

A.11.2 Teçhizat

A.11.2.8 Gözetimsiz kullanıcı teçhizatı

Kullanıcılar, gözetimsiz teçhizatın uygun bir şekilde korunmasını temin etmelidir.

- Aktif oturumların işi bittiğinde sonlandırılması
- Parola korumalı ekran koruyucu
- Gerekli olmadığında uygulamalardan çıkılması (log-off)
- Bilgisayar ve mobil cihazların yetkisiz kullanımdan korunması (kilitlenme/parola ile erişim)

A.11.2 Teçhizat

A.11.2.9 Temiz masa temiz ekran politikası

*Kağıtlar ve taşınabilir depolama ortamları için temiz masa **politikası** ve bilgi işleme olanakları için temiz ekran politikası benimsenmelidir.*

- Kağıtlar/taşınabilir depolama ortamları için temiz masa politikası
- Bilgi işleme tesisleri için temiz ekran politikası
- Çalışma esnasında oturuş düzenleri
- Parolalı tuş kilitleri
- Gelen/giden faks makinaları
- Fotokopi/tarayıcı makinaları
- Hafızada kalan bilgilerin silinmesi

A.12
İşletim (Operasyon) Güvenliği

7 Güvenlik Kategorisi

- İşletim prosedürleri ve sorumlulukları
- Kötücül yazılımlardan korunma
- Yedekleme
- Kaydetme ve izleme
- İşletimsel yazılım kontrolü
- Teknik açıklık yönetimi
- Bilgi sistemleri tetkik hususları

A.12 İşletim Güvenliği

A.12.1 İşletim prosedürleri ve sorumlulukları

Amaç: Bilgi işleme olanaklarının doğru ve güvenli işletimlerini temin etmek

A.12.1.1 Yazılı işletim prosedürleri

İşletim Prosedürleri yazılı hale getirilmeli ve ihtiyacı olan tüm kullanıcılara sağlanmalıdır.

- İşletim prosedürleri
  - Sistemlerin kurulması, konfigürasyonu, açılması, kapanması
  - Yedekleme (A.12.3) , Cihazların bakımı , Ortam taşıma
  - Sistem odasının yönetimi ve güvenliği
  - Sistem bozulmalarında sistemin yeniden başlatılması ve geri alma
  - Fiziksel ve çevresel güvenlik prosedürü

A.12.1 İşletim prosedürleri ve sorumlulukları

A.12.1.2 Değişiklik yönetimi

Bilgi güvenliğini etkileyen, kuruluş iş prosesleri, bilgi işleme olanakları ve sistemlerdeki değişiklikler kontrol edilmelidir.

- Önemli değişikliklerin tanımlanması ve kaydı
- Değişikliklerin planlanması ve testi
- Potansiyel etkilerin değerlendirilmesi (değişikliklerin güvenlik etkileri dahil)
- Önerilen değişiklikler için resmi onay prosedürü
- Değişiklik detaylarının tüm ilgili kişilere iletilmesi

A.12.1 İşletim prosedürleri ve sorumlulukları

A.12.1.2 Değişiklik yönetimi

- Başarısız değişikliklerin veya beklenmeyen olayların onarılması ve/veya geri alınması ile ilgili sorumlulukları belirleyen prosedürler
- Değişiklikler yapıldıktan sonra tüm ilgili bilgileri barındıran audit kayıtları (log)
- İş gereksinimi olmadıkça değişiklik yapılmaması

Bilgi işlem sistemlerinde yapılan değişikliklerin yönetilmemesi sonucunda sık sık sistem hatalarının ve güvenlik açıklarının ortaya çıktığı unutulmamalıdır.

Değişiklik yapıldığında ilgili tüm bilgileri içeren denetim kayıtları tutulmalıdır.

A.12.1 İşletim prosedürleri ve sorumlulukları

A.12.1.3 Kapasite yönetimi

Kaynakların kullanımı izlenmeli, ayarlanmalı ve gerekli sistem performansını temin etmek için gelecekteki kapasite gereksinimleri ile ilgili kestirimler yapılmalıdır.

- Kaynak kullanımı
  - İzleme
  - Ayarlama
  - Gelecek için projeksiyon (gerekli sistem performansı için)
    - Yeni iş gereksinimleri
    - Yeni sistem gereksinimleri
  - Sorumluluk
  - İnsan kaynağı, ofisler ve tesislerin kapasitesinin yönetimi

A.12.1 İşletim prosedürleri ve sorumlulukları

A.12.1.3 Kapasite yönetimi

- Kapasite talebinin yönetilmesi
  - Eski verilerin silinmesi (disk alanı)
  - Kullanımı gerekli olmayan/az kullanılan uygulama, sistem ve veritabanlarının devreden çıkarılması
  - Toplu işleme (batch process) ve planlı işlemlerin (schedule) optimizasyonu
  - Uygulama mantığı ve veritabanı sorgularının optimizasyonu
  - Fazla kaynak isteyen (resource hungry) hizmetlerin kaldırılması ya da bant genişliğinin sınırlandırılması (iş için çok kritik değilse)
- Önemli/Kritik sistemler için dokümante kapasite yönetim planı

A.12.1 İşletim prosedürleri ve sorumlulukları

A.12.1.4 Geliştirme, test ve işletim ortamların birbirinden ayrılması

Geliştirme, test ve işletim ortamları, yetkisiz erişim veya işletim ortamlarında değişiklik risklerinin azaltılması için birbirinden ayrılmalıdır.

- Yazılımın geliştirme ortamından operasyon ortamına aktarılmasına ait kuralların tanımlanması ve dokümante edilmesi
- Operasyon, geliştirme ve test ortamlarının canlı çalışma ortamından ayrılması
- Geliştirme ve operasyon yazılımlarının ayrı sistemlerde veya işlemcilerde, ayrı domainlerde ve klasörlerde çalışması

A.12.1 İşletim prosedürleri ve sorumlulukları

A.12.1.4 Geliştirme, test ve işletim ortamların birbirinden ayrılması

- Compilers, editörler ve diğer geliştirme araçlarına operasyonel ortamlardan erişimin engellenmesi
- Hassas dataların test ortamlarına aktarılmaması(Eşdeğer kontrollerin test sistemlerine de uygulanması durumu hariç, A.14.3)
- Geliştirme, test ve operasyonel ortamların ayrılması, operasyonel yazılıma veya iş verilerinin kaza ile değiştirilmesi ya da yetkisiz erişim risklerini azaltır (A.14.3, Test verilerinin korunması)

A.12 İşletim Güvenliği

A.12.2 Kötü niyetli yazılımlardan koruma

Amaç: Bilgi ve bilgi işleme olanaklarının kötü niyetli yazılımlardan korunmasını temin etmek.

A.12.2.1 Kötü niyetli yazılımlara karşı kontroller

Kötü niyetli yazılımlardan korunmak için tespit etme, engelleme ve kurtarma kontrolleri uygun kullanıcı farkındalığı ile birlikte uygulanmalıdır

- Kötü niyetli kodlar
  - Bilgisayar virüsleri, ağ solucanları, truva atları, casus yazılımlar

A.12.2 Kötü niyetli yazılımlardan koruma

A.12.2.1 Kötü niyetli yazılımlara karşı kontroller

- Kötü niyetli kodun önlenmesi, teşhisi ve kurtarma kontrolleri
- Yetkisiz yazılımın tespit eden veya engelleyen kontroller (whitelisting uygulaması)
- Şüpheli ya da bilinen web sayfalarını tespit eden veya engelleyen kontroller (blacklisting uygulaması)
- Yazılım yükleme politikası (Yetkisiz yazılım kullanımının engellenmesi, A.12.6.2, A.14.2)
- Dış ağlardan alınan dosyalar ve yazılımlar için koruyucu önlem
- Anti virüs
- Düzenli gözden geçirme
- Kullanıcı farkındalığı

A.12 İşletim Güvenliği

A.12.3 Yedekleme

Amaç: Veri kaybına karşı koruma sağlamak.

A.12.3.1 Bilgi yedekleme

Bilgi, yazılım ve sistem imajlarının yedek kopyaları alınmalı ve üzerinde anlaşılmış bir yedekleme politikası doğrultusunda düzenli olarak test edilmelidir.

- Yedekleme politikası
- Düzenli geri kazanım testi
- Yedekleme düzeyi
- Yedekleme şekli (Full , differential, incrimental)

A.12.3 Yedekleme

A.12.3.1 Bilgi yedekleme

- Geri dönüş prosedürleri
- Yedeklerin bulunduğu yerlerde uygun fiziksel ve çevresel güvenlik (A.11)
- FKM (Farklı fiziksel lokasyonda muhafaza)
- Yedekleme ortamının düzenli testi
- Ömrünü tamamlayan yedekleme üniteleri
- Kriptolama
- Yedekleme ortamının imhası

A.12 İşletim Güvenliği

A.12.4 Kaydetme ve izleme

Amaç: Olayları kaydetme ve kanıt üretmek

A.12.4.1 Olay kaydetme

*Kullanıcı işlemleri, kural dışılıklar, hatalar ve bilgi güvenliği olaylarını kaydeden olay kayıtları üretilmeli, saklanmalı ve düzenli olarak **gözden geçirilmelidir**.*

- Kullanıcı kimlikleri
- Oturum açma/kapatma gibi önemli olayların tarihleri, saatleri ve detayları
- Mümkünse terminal kimliği ya da lokasyonu

A.12.4 Kaydetme ve izleme

A.12.4.1 Olay kaydetme

- Başarılı ve reddedilmiş, sistemi veri ve diğer kaynaklara erişim girişimleri kayıtları
- Sistem yapılandırma değişiklikleri
- Ayrıcalıkların kullanımı
- Sistem araçları ve uygulamalarının kullanımı
- Erişilen dosyalar ve erişim türü
- Anti-virüs ve saldırı tespit sistemlerinin etkinleştirilmesi ve devre dışı bırakılması
- Uygulamalarda kullanıcının yürüttüğü işlemlerinin kayıtları

A.12.4 Kaydetme ve izleme

A.12.4.2 Kayıt bilgisinin korunması

Kaydetme olanakları ve kayıt bilgileri kurcalama ve yetkisiz erişime karşı korunmalıdır.

- Log kayıt sistemleri ve log bilgisi kurcalanma ve yetkisiz erişime karşı korunmalı
- Kanıt toplama ve koruma gereksinimleri nedeniyle arşivlenmesi gerekli
- Log (Günlük) dosyalarının düzenlenmesi ya da silinmesi
- Olayları kaydetme hatası
- Geçmişte kaydedilen olayların ortam kapasitesini aşması sonucu log üzerine yazma

A.12.4 Kaydetme ve izleme

A.12.4.3 Yönetici ve operatör kayıtları

Sistem yöneticileri ve sistem operatörlerinin işlemleri kayıt altına alınmalı, kayıtlar korunmalı ve düzenli olarak ***gözden geçirilmelidir****.*

- Sistem yöneticisi ve sistem işletmeni faaliyetlerinin günlükleri (log) kaydedilmeli
- Oluşan olay zamanı, türü
- Olay ya da hata hakkında bilgi
- Hangi hesabın ve hangi yöneticinin ya da işletmenin dahil olduğu
- Hangi süreçlerin dahil olduğu
- Sistem yöneticisi ve işletmen logları düzenli olarak gözden geçirilmeli

A.12.4 Kaydetme ve izleme

A.12.4.4 Saat senkronizasyonu

Bir kuruluş veya güvenlik alanında yer alan tüm ilgili bilgi işleme sistemlerinin saatleri tek bir referans zaman kaynağına göre senkronize edilmelidir

- Yerel özellikler (örneğin, gün ışığından yararlanma) dikkate alınmalı
- Bir referans zaman belirlenmesi
- Bu loglar incelemeler ya da yasal ya da disiplin durumlarında kanıt olarak istenebilir

A.12 İşletim Güvenliği

A.12.5 İşletimsel yazılımının kontrolü

Amaç: İşletimsel sistemlerin bütünlüğünü temin etmek

A.12.5.1 İşletimsel sistemler üzerine yazılım kurulumu

İşletimsel sistemler üzerine yazılım kurulumunun kontrolü için prosedürler uygulanmalıdır.

- Güncellemeler yetkin sistem yöneticileri tarafından yapılmalı
- Uygulama ve operasyonel sistem yazılımlarının başarılı test sonrasında uygulanması
- Konfigürasyon kontrol sistemi (Eski ve yeni yazılım sürümleri, yazılımla ilgili konfigürasyon bilgileri ve sistem dokümantasyonu)
- Değişiklikler uygulanmadan önce geri dönüş stratejileri oluşturulması ve değişiklikler için log tutulması
- Uygulama yazılımının geçmiş versiyonlarının tutulması
- Tedarikçiden alınmış yazılımlarda destek alınamaması riskinin göz önüne alınması (destek süresi)

A.12 İşletim Güvenliği

A.12.6 Teknik açıklık yönetimi

Amaç: Teknik açıklıkların kullanılmasını engellemek

A.12.6.1 Teknik açıklıkların yönetimi

Kullanılmakta olan bilgi sistemlerinin teknik açıklıklarına dair bilgi, zamanında elde edilmeli kuruluşun bu tür açıklıklara karşı zafiyeti değerlendirilmeli ve ilgili riskin ele alınması için uygun tedbirler alınmalıdır.

- Bilgi sistemlerinin teknik açıklıkları ile ilgili bilgilerin zamanında toplanması
- Etki analizi/riski azaltmak için tedbirler
- Teknik açıklık yönetimi için ön şart: Varlık envanterinin güncel ve eksiksiz olması
- Teknik açıklık yönetimi ile ilgili Roller ve sorumluluklar (Açıklık izleme, risk değerlendirme, yamalama, varlık izleme dahil)

A.12.6 Teknik açıklık yönetimi

A.12.6.1 Teknik açıklıkların yönetimi

- İlgili teknik açıklıkları tanımlamak ve farkındalığı muhafaza etmek için güncel bilgi kaynakları (yazılım ve varlık envanterine göre diğer teknolojiler)
- Potansiyel teknik açıklıkların takibi
- Yamalar, tolere edilemeyecek yan etkileri olmadığı ve etkin olduklarını belirlemek için test edilmeli
- Yüksek riskli sistemlere öncelik verilmeli
- Etkinlik ve verimlilik için teknik açıklık yönetim süreci düzenli olarak izlenmeli
- Tüm prosedürler için denetim loglarının tutulması

A.12.6 Teknik açıklık yönetimi

A.12.6.1 Teknik açıklıkların yönetimi

- Yamanın olmadığı durumlarda;

  - Açıklığa ait hizmetlerin devre dışı bırakılması
  - Erişim kontrollerinin (firewall, network border) eklenmesi
  - Açıklık farkındalığının artırılması
  - Gerçek saldırıların tespiti için izlemenin arttırılması

A.12.6 Teknik açıklık yönetimi

A.12.6.2 Yazılım kurulumu kısıtlamaları

Kullanıcılar tarafından yazılım kurulumuna dair kurallar oluşturulmalı ve uygulanmalıdır

- Kullanıcıların hangi tip yazılımları kurabileceğini kesin olarak belirlenmesi
- En az ayrıcalık prensibi (Sadece izin verilen kullanıcıların yazılım yükleyebilmesi)
- Hangi tip yazılımların kurulumuna izin verildiği (güncellemeler, mevcut yazılımlara güvenlik yamaları vb.)
- Hangi tip yazılımların yasaklandığı (Kişisel kullanıma dair yazılımlar, potansiyel olrak şüpheli bilinen yazılımlar,
- Kontrolsüz yazılım yüklemeleri açıklıklara, bilgi sızmasına, bilgi bütünlüğünün kaybına, telif hakkı ihlallerine sebep olabilir

A.12 İşletim Güvenliği

A.12.7 Bilgi sistemleri denetim hususları

Amaç: Denetim faaliyetlerinin işletimsel sistemler üzerindeki etkilerini asgariye indirmek.

A.12.7.1 Bilgi sistemleri denetim kontrolleri

İşletimsel sistemlerin doğrulanmasını kapsayan denetim gereksinimleri ve faaliyetleri, iş proseslerindeki kesintileri asgariye indirmek için dikkatlice planlanmalı ve üzerinde anlaşılmalıdır.

- Sistemlere ve verilere erişim uygun yönetimle uzlaşılmalı
- Teknik denetim testlerinin kapsamı uzlaşılmalı ve kontrol edilmeli
- Denetim testleri yazılım ve veriye sadece okuma (read-only) erişim vermeli

A.12.7 Bilgi sistemleri denetim hususları

A.12.7.1 Bilgi sistemleri denetim kontrolleri

- Sadece okunabilir erişim dışında kalan erişim, sistem dosyalarının yalıtılmış kopyalarına kopyalarına verilmeli
- Sistemin erişilebilirliğini etkileyebilecek olan denetim testleri çalışma saatleri dışında yapılmalı
- Tüm erişimler izlenmeli ve log tutulmalı

A.13
Haberleşme güvenliği

2 Güvenlik Kategorisi

- Ağ güvenliği yönetimi
- Bilgi transferi

A.13 Haberleşme güvenliği

A.13.1 Ağ güvenliği yönetimi

Amaç: Ağdaki bilgi ve destekleyici bilgi işleme olanaklarının korunmasını sağlamak.

A.13.1.1 Ağ kontrolleri

Sistemlerdeki ve uygulamalardaki bilgiyi korumak amacıyla ağlar yönetilmeli ve kontrol edilmelidir.

- Yetkisiz erişimin engellenmesi

  - Uzaktan erişim donanımının yönetimi için sorumluluklar ve prosedürler
  - Ağ için operasyonel sorumluluklar bilgisayar operasyonlarından ayrılmalı
  - Kablosuz ve kamusal ağlardan geçen verinin gizlilik ve bütünlüğünün korunması

A.13.1 Ağ güvenliği yönetimi

A.13.1.2 Ağ hizmetleri güvenliği

Tüm ağ hizmetlerinin güvenlik mekanizmaları, hizmet seviyeleri ve yönetim gereksinimleri tespit edilmeli ve hizmetler kuruluş içinden veya dış kaynak yoluyla sağlanmış olsun olmasın, ağ hizmetleri anlaşmalarında yer almalıdır.

- Ağ Hizmetleri Anlaşmaları
  - Güvenlik özellikleri
  - Hizmet seviyeleri
  - Yönetim gereksinimleri

- Tanımlanmalı
  - Alınan hizmetin kuruluş tarafından izlenmesi ve denetlenmesi

A.13.1 Ağ güvenliği yönetimi

A.13.1.2 Ağ hizmetlerinin güvenliği

- Ağ Hizmetleri
  - Firewall/Saldırı tespit sistemleri

- Halka açık ağlar/kablosuz ağlar (VPN/erişim kontrolü/kriptografik önlemler)

***Not** : ISO/IEC 18028, Information technology –Security techniques – IT network security.*

***Not :** ISO/IEC 27033-1:2009 Information technology – Security techniques – Network security*

A.13.1 Ağ güvenliği yönetimi

A.13.1.3 Ağlarda ayrım

Ağlarda, bilgi hizmetleri, kullanıcıları ve bilgi sistemleri grupları ayrılmalıdır.

- Bilgi sistemi üstündeki kullanıcı ve servislerin gruplara ayrılması
- Kurumun ağının dahili ve harici etki alanlarına bölünmesi
- Etki alanlarının kurumun erişim kontrol politikası ve erişim ihtiyaçlarına uygun olması
- Etki alanlarının sınır güvenliği sistemleri ile korunması
- Kablosuz ağların diğer ağlardan ayrılması
- Kablosuz ağlarda güçlü kimlik doğrulama yapılması

A.13 Haberleşme güvenliği

A.13.2 Bilgi transferi

Amaç : Bir kuruluş içerisinde ve herhangi bir dış varlık arasında transfer edilen bilgiyi korumak

A.13.2.1 Bilgi transfer politikaları ve prosedürleri

*Tüm iletişim olanağı türlerinin kullanımıyla bilgi transferini korumak için resmi transfer **politikaları, prosedürleri** ve kontrolleri mevcut olmalıdır.*

- Mesajlara eklenmiş hassas bilgilerin korunması.
- e-iletişim yöntemlerinin kullanımı ile ilgili rehber ve politikalar.
- Kablosuz veri iletişiminin içerdiği risklerin göz önüne alınması.
- Bilginin bütünlüğünü ve gizliliğini korumak için kriptografik tekniklerin kullanılması.

A.13.2 Bilgi transferi

A.13.2.1 Bilgi transfer politikaları ve prosedürleri

- İş ile ilgili yazışmaların saklanması ve imhası
- Fotokopi makinesi, yazıcı ve faks cihazlarında hassas bilgi içeren belgelerin bırakılmaması
- Personelin telefon konuşmaları sırasında hassas bilgilerin açığa çıkmaması için tedbirli davranması
- Otomatik cevap verme makinelerine hassas bilgi içeren mesajlar bırakılmaması
- Faks cihazlarının kullanılması ile ilgili risklerin personele anlatılması
- Gizli görüşmelerin halka açık yerlerde yapılmaması

A.13.2 Bilgi transferi

A.13.2.2 Bilgi transferi anlaşmaları

Anlaşmalar, kuruluş ve dış taraflar arasındaki iş bilgilerinin güvenli transferini ele almalıdır.

Bilgi transferi anlaşmalarının kapsamı

- Bilginin aktarımı, gönderimi ve almanın kontrolü ve bildirimi için yönetim sorumlulukları
- İzlenebilirlik ve inkar edememe prosedürleri
- Paketleme ve aktarım için minimum teknik standartlar
- 3. taraflara emanet edilen bilgi anlaşmaları
- Kurye kimlik tanımlama standartları

A.13.2 Bilgi transferi

A.13.2.2 Bilgi transferi anlaşmaları

Bilgi transferi anlaşmalarının kapsamı

- Bilginin kaybı gibi bilgi güvenliği olaylarında sorumluluk ve yükümlülükler
- Hassas ve kritik bilgi için uzlaşılmış etiketleme sistemi (etiketlerin hemen anlaşılması ve uygun şekilde korunması (A.8.2)
- Bilgi ve yazılımın kaydı ve okunması için standartlar
- Kriptografi gibi hassas verileri koruyan özel kontroller

A.13.2 Bilgi transferi

A.13.2.3 Elektronik mesajlaşma

Elektronik mesajlaşmadaki bilgi uygun şekilde korunmalıdır.

e-posta, elektronik veri değişimi ve sosyal ağlardaki bilgi uygun şekilde korunmalı

- Mesajlar yetkisiz erişimden korunmalı
- Mesajın doğru adrese gitmesi sağlanmalı
- Elektronik posta hizmetinin sürekliliği ve güvenilirliği yüksek olmalı
- Gerekiyorsa elektronik imza gibi yasal yükümlülükler kullanılmalı

A.13.2 Bilgi transferi

A.13.2.4 Gizlilik ya da ifşa etmeme anlaşmaları

*Bilginin korunması için kuruluşun ihtiyaçlarını yansıtan gizlilik ya da ifşa etmeme anlaşmalarının gereksinimleri tanımlanmalı, düzenli olarak **gözden geçirilmeli ve yazılı** hale getirilmelidir.*

- Gizli bilginin tanımının yapılması
- Anlaşmanın süresi
- Anlaşmanın bitiminde yapılacaklar
- Gizli bilginin nasıl korunması gerektiği
- Yasal gereklere dair ifadeler
- Yetkisiz ifşanın engellenmesi için sorumluluklar ve faaliyetler

A.13.2 Bilgi transferi

A.13.2.4 Gizlilik ya da ifşa etmeme anlaşmaları

- Bilginin sahibi
- Ticari sırlar
- Telif hakları
- Gizli bilginin izinle kullanımı
- Gizli bilginin tetkiki ve izlenmesi ile ilgili haklar
- Gizli bilginin sızması durumunda gerekli faaliyetler

Gizlilik ve açıklamama anlaşmalarının periyodik gözden geçirmesi

A.14
Sistem Temini, Geliştirme ve Bakımı

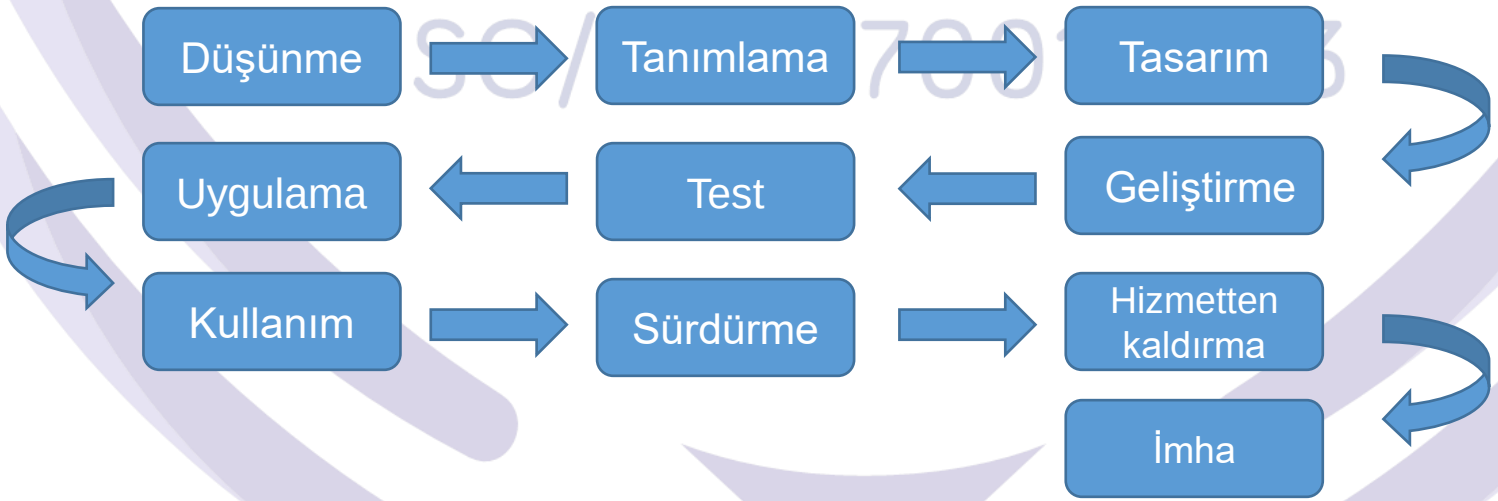
3 Güvenlik Kategorisi

- Bilgi sistemlerinin güvenlik gereksinimleri
- Geliştirme ve destek süreçlerinde güvenlik
- Test verisi

A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri

Amaç: Bilgi güvenliğinin, bilgi sistemlerinin tüm yaşam döngüsü boyunca dâhili bir parçası olmasını sağlamak. Bu aynı zamanda halka açık ağlar üzerinden hizmet sağlayan bilgi sistemleri gereksinimlerini de içerir.

Bilgi Sistemlerinin Doğal Yaşam Döngüsü



A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri

A.14.1.1 Güvenlik gereksinimleri analizi ve özellikleri

Bilgi güvenliği ile ilgili gereksinimler, yeni bilgi sistemleri gereksinimlerine veya var olan bilgi sistemlerinin iyileştirmelerine dâhil edilmelidir.

- Sistem geliştirilirken işin başından itibaren güvenlik ihtiyaçları göz önünde bulundurulmalı (Tasarım aşamasında düşük maliyet)
- Ürün güvenlik şartlarını karşılamıyorsa oluşan risk ve ilgili kontroller
- Güvenlik gereksinimleri bilgi varlıklarının değerini ve bir güvenlik açığı dolayısıyla oluşabilecek zararı yansıtmalı
- Ortak kriter sertifikalı ürünler (TS ISO/IEC 15408)

A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri

A.14.1.2 Halka açık ağlardaki uygulama hizmetlerinin güvenliğinin sağlanması

Halka açık ağlar üzerinden geçen uygulama hizmetlerindeki bilgi, hileli faaliyetlerden, sözleşme ihtilafından ve yetkisiz ifşadan ve değiştirmeden korunmalıdır.

- İletişim yapan tarafların hizmeti kullanmaları için yetkileri konusunda etkin bir şekilde bilgilendirilmesi
- Önemli dokümanların iletimi ve alımı sırasındaki gizlilik ve bütünlük gereksinimlerinin belirlenmesi ve karşılanması
- Sipariş hareketlerinde ödeme bilgileri, gönderim adresi bilgileri ve bilginin alındığının konfirmasyonu bilgilerinin gizliliği ve bütünlüğü

A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri

A.14.1.2 Halka açık ağlardaki uygulama hizmetlerinin güvenliğinin sağlanması

- Müşteri tarafından sağlanan ödeme bilgilerinin doğrulanma seviyesi
- Sahtekarlıklardan korunma için en uygun ödeme biçiminin seçimi
- Sipariş bilgisinin gizlilik ve bütünlüğünün korunması için gerekli koruma seviyeleri
- İşlem bilgilerinin kaybı ya da tekrarının engellenmesi
- Sigorta gereksinimleri
- Kontroller için kriptografi kullanımı

A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri

A.14.1.3 Uygulama hizmet işlemlerinin korunması

Uygulama hizmet işlemlerindeki bilgi eksik iletim, yanlış yönlendirme, yetkisiz mesaj değiştirme, yetkisiz ifşayı, yetkisiz mesaj çoğaltma ya da mesajı yeniden oluşturmayı önlemek için korunmalıdır.

Uygulama servis işlemleri için bilgi güvenliği hususları

- Elektronik imza kullanımı
- İşlem detaylarının kamunun eriştiği yerlerde bulundurulmaması (Internet yerine intranet'in kullanımı)
- İşlemlerin tüm unsurları
  - Kullanıcıların gizli kimlik doğrulama bilgileri
  - İşlemin gizli kalması
  - Tüm tarafların mahrem bilgilerinin korunması

A.14 Sistem Temini, Geliştirme ve Bakımı

A.14.2 Geliştirme ve destek süreçlerinde güvenlik

Amaç: Bilgi güvenliğinin bilgi sistemleri geliştirme yaşam döngüsü içerisinde tasarlanıyor ve uygulanıyor olmasını sağlamak

A.14.2.1 Güvenli geliştirme politikası

Yazılım ve sistemlerin geliştirme kuralları belirlenmeli ve kuruluş içerisindeki geliştirmelere uygulanmalıdır.

- **Güvenli geliştirme politikası**
  - Geliştirme ortamının güvenliği
  - Yazılım geliştirme yaşam döngüsünde güvenlik için kılavuzluk
  - Yazılım geliştirme metodolojisinde güvenlik
  - Her programlama dilinde güvenli kodlama kılavuzu

A.14.2 Geliştirme ve destek süreçlerinde güvenlik

A.14.2.1 Güvenli geliştirme politikası

- Tasarım aşamasında güvenlik gereksinimleri
- Proje adımlarında güvenlik kontrol noktaları
- Güvenli depolama ortamları
- Versiyon kontrolünde güvenlik
- Geliştirenin açıklıkları bulma ve önleme yetkinliği
- Yeni yazılım geliştirmeler için güvenli programlama teknikleri

A.14.2 Geliştirme ve destek süreçlerinde güvenlik

A.14.2.2 Sistem değişiklik kontrolü prosedürleri

Geliştirme yaşam döngüsü içerisindeki sistem değişiklikleri resmi değişiklik kontrol ***prosedürlerinin*** *kullanımı ile kontrol edilmelidir.*

- Yazılı resmi değişim kontrol prosedürleri (ilk tasarım aşamalarından tüm bakım çalışmalarına kadar)
- Yeni sistemlerin dahil edilmesinde ve mevcut sistemlerde yapılacak önemli değişikliklerde; dokümantasyon, şartname, test etme, kalite kontrol ve uygulamanın yönetimi konularında resmi proses
- Prosesler, risk değerlendirmesi, değişikliklerin etkisinin analizi ve güvenlik kontrolleri için gerekli özellikleri içermeli

A.14.2 Geliştirme ve destek süreçlerinde güvenlik

A.14.2.2 Sistem değişiklik kontrolü prosedürleri

- Mümkün olduğunca, uygulama ve işletim değişiklik kontrol prosedürleri bütünleştirilmelidir (Madde 12.1.2 Değişim Yönetimi)

- Değişim kontrol prosedürleri
  - Uzlaşmaya varılmış yetki seviyelerinin bir kaydının tutulması
  - Değişikliklerin yetkili kullanıcılar tarafından yapılmasının temin edilmesi
  - Kontrollerin ve bütünlük prosedürlerinin değişikliklerden zarar görmemelerini temin etmek için gözden geçirilmesi,

A.14.2 Geliştirme ve destek süreçlerinde güvenlik

A.14.2.2 Sistem değişiklik kontrolü prosedürleri

- Değişim kontrol prosedürleri

  - Tadilat gerektiren tüm yazılımın, bilginin, veri tabanın, veri tabanı varlıklarının ve donanımını belirlenmesi
  - Yetkili kullanıcıların uygulanmadan önce değişiklikleri kabul etmesinin sağlanması
  - Her bir değişiklik tamamlandığında sistem dokümantasyonunun güncellendiğinden ve eski dokümantasyonun arşive kaldırıldığından ya da imha edildiğinden emin olunması
  - Tüm yazılım güncellemeleri için bir versiyon kontrolü yürütülmesi

A.14.2 Geliştirme ve destek süreçlerinde güvenlik

A.14.2.3 İşletim platformu değişikliklerinden sonra uygulamaların teknik gözden geçirmesi

İşletim platformları değiştirildiğinde, kurumsal işlemlere ya da güvenliğe hiçbir kötü etkisi olmamasını sağlamak amacıyla iş için kritik uygulamalar gözden geçirilmeli ve test edilmelidir.

- İşletim sistemi değişiklikleri
- Gözden geçirme/Test
- İşletim sistemi değişikliklerinin zamanında haber verilmesinin sağlanması (Testlere ve gözden geçirmelere zaman ayırılması)
- işletim sistemi değişikliklerden zarar görmediğinden emin olmak için uygulama kontrol ve bütünlük prosedürlerinin gözden geçirilmesi,
- iş devamlılığı planlarına ilişkin uygun değişikliklerin yapılmasının temin edilmesi (bk. Madde 17).

A.14.2 Geliştirme ve destek süreçlerinde güvenlik

A.14.2.4 Yazılım paketlerindeki değişikliklerdeki kısıtlamalar

Yazılım paketlerinde yapılacak değişiklikler gerek duyulanlar hariç önlenmeli ve tüm değişiklikler sıkı bir biçimde kontrol edilmelidir.

- Tedarikçiden alınan yazılım paketlerinin değiştirilmeden kullanımı
- Yazılım paketlerinde değişiklik
  - Gömülü kontroller ve bütünlük süreçleri için risklerin belirlenmesi
  - Tedarikçinin yapılacak değişikliğe rızası
  - Gerekli değişikliklerin tedarikçi tarafından standart program güncellemesi olarak sağlanması ihtimali
  - Değişiklik sonrası tedarikçinin bakımla ilgili riskleri
  - Yazılım güncelleme yönetim süreci (Yamalar ve uygulama güncellemeleri)

A.14.2 Geliştirme ve destek süreçlerinde güvenlik

A.14.2.5 Güvenli sistem mühendisliği prensipleri

Güvenli sistem mühendisliği prensipleri belirlenmeli, yazılı hale getirilmeli ve tüm bilgi sistemi uygulama çalışmalarına uygulanmalıdır.

- Güvenlik mühendisliği prensiplerine dayalı güvenli sistem mühendisliği prosedürleri olusturulmalı, dokümante edilmeli ve uygulanmalı
- Yeni teknolojiler güvenlik riskleri için analiz edilmeli ve tasarım bilinen ataklara karşı gözden geçirilmeli
- Gözden geçirme yeni potansiyel tehditlere karşı da yapılmalı

A.14.2 Geliştirme ve destek süreçlerinde güvenlik

A.14.2.6 Güvenli geliştirme ortamı

Kuruluşlar tüm sistem geliştirme yaşam döngüsünü kapsayan sistem geliştirme ve bütünleştirme girişimleri için güvenli geliştirme ortamları kurmalı ve uygun bir şekilde korumalıdır.

- Güvenli geliştirme ortamı, insanlar, süreçler ve sistem geliştirme ve entegrasyonu kapsar.
- Kuruluş güvenli geliştirme ortamları oluşturmalı
  - Sistem tarafından işlenecek, muhafaza edilecek ve iletilecek verinin hassasiyeti
  - Dış ve iç gereksinimler (Yasalar ve politikalar)
  - Halen uygulanan ve sistem geliştirmeyi destekleyen güvenlik kontrolleri

A.14.2 Geliştirme ve destek süreçlerinde güvenlik

A.14.2.7 Dışarıdan sağlanan geliştirme

Kuruluş dışarıdan sağlanan sistem geliştirme faaliyetini denetlemeli ve izlemelidir.

- Lisans anlaşmaları, kod mülkiyeti, fikri mülkiyet hakları
- İşin kalitesinin ve doğruluğunun belgelenmesi
- Kodun kalite ve güvenlik fonksiyonlarının sözleşmeye bağlanması
- Kurulum öncesi kötü niyetli kod ve "Trojan" kod araması için test

A.14.2 Geliştirme ve destek süreçlerinde güvenlik

A.14.2.8 Sistem güvenlik testi

Güvenlik işlevselliğinin test edilmesi, geliştirme süresince gerçekleştirilmelidir.

- Yeni ve güncellenen sistemler geliştirme aşamasında test ve doğrulama gerektirir
- Bağımsız kabul testleri dışarıdan sağlanan ve içeride geliştirilen sistemler için yapılmalı

A.14.2 Geliştirme ve destek süreçlerinde güvenlik

A.14.2.9 Sistem kabul testi

Kabul test programları ve ilgili kriterler, yeni bilgi sistemleri, yükseltmeleri ve yeni versiyonları için belirlenmelidir.

- Kabul testleri
  - Yeni bilgi sistemleri (yazılım/donanım)
  - Güncellemeler
  - Yeni versiyonlar

Dikkate alınacak hususlar

- Mevcut sistemlerle uyum
- Performans
- Şartname/Sözleşme detayları

A.14 Sistem Temini, Geliştirme ve Bakımı

A.14.3 Test verisi

Amaç : Test için kullanılan verinin korunmasını sağlamak

A.14.3.1 Test verisinin korunması

Test verisi dikkatli bir şekilde seçilmeli korunmalı ve kontrol edilmelidir.

- Test amacıyla personel bilgilerini ya da hassas bilgileri içeren işlemsel veri tabanlarının kullanımından kaçınılmalı
- Aktif sistem bilgileri test sırasında kullanılacaksa içindeki gizli bilgiler çıkarılmalı
- Test amacıyla kullanıldığında, işlemsel verilen korunması için kontroller
- İşletim sistemlerine uygulanan erişim kontrol prosedürleri test uygulama sistemleri için de geçerli olmalı

A.14.3 Test verisi

A.14.3.1 Test verisinin korunması

- Test amacıyla kullanıldığında, işlemsel verilen korunması için kontroller

  - İşlemsel bilginin bir test uygulamasına her kopyalanmasında ayrı bir yetkilendirme söz konusu olmalı
  - Test işlemi tamamlandıktan sonra işlemsel bilgi test uygulama sisteminden hemen silinmeli
  - Bir kontrol zinciri oluşturmak amacıyla işlemsel bilginin kopyalanmasının ve kullanımının günlüğü tutulmalı

A.15
Tedarikçi İlişkileri

2 Güvenlik Kategorisi

- Tedarikçi ilişkilerinde bilgi güvenliği
- Tedarikçi hizmet sağlama yönetimi

A.15 Tedarikçi İlişkileri

A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği

Amaç: Kuruluşa ait tedarikçiler tarafından erişilen varlıkların korunmasını sağlamak.

A.15.1.1 Tedarikçi ilişkileri için bilgi güvenliği politikası

*Tedarikçinin kuruluşun varlıklarına erişimi ile ilgili riskleri azaltmak için bilgi güvenliği gereksinimleri tedarikçi ile kararlaştırılmalı ve **yazılı** hale getirilmelidir.*

- **Politika**
  - Tedarikçi türlerinin belirlenmesi ve dokümante edilmesi (BT hizmetleri, lojistik hizmetleri, finansal hizmetler vb.)
  - Kuruluş tedarikçinin eriştiği bilgiler için bilgi güvenliği kontrolleri tanımlamalı ve uygulamaya zorlamalıdır
  - Kuruluşun erişime izin verdiği BT altyapı bileşenleri
  - Tedarikçinin erişebileceği bilgilerin tanımlanması

A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği

A.15.1.1 Tedarikçi ilişkileri için bilgi güvenliği politikası

- Tedarikçi ilişkilerinin yönetimi için standart süreç
- Tedarikçi ve kuruluş tarafından sağlanan bilginin bütünlüğünün sağlanması
- Kuruluş bilgilerinin korunması için tedarikçilere uygulanabilecek yükümlülüklerin belirlenmesi
- Her iki tarafça sağlanan bilginin erişilebilirliğinin sağlanması için kurtarma ve beklenmedik durum düzenlemeleri
- Tedarikçi personeli ile ilişkide bulunan personelin farkındalık eğitimi (Tedarikçi türü ve tedarikçinin eriştiği bilgilerin seviyesinin göz önüne alınması)

A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği

A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme

Kuruluşun bilgisine erişebilen, bunu işletebilen, depolayabilen, iletebilen veya kuruluşun bilgisi için bilgi teknolojileri altyapı bileşenlerini temin edebilen tedarikçilerin her biri ile anlaşılmalı ve ilgili tüm bilgi güvenliği gereksinimleri oluşturulmalıdır.

- Tedarikçilerle bilgi güvenliği konularındaki gereksinimlerin karşılanması konusunda bir anlaşmazlık olmaması için tedarikçi anlaşmaları oluşturulmalı
  - Sağlanan ya da erişime izin verilen bilginin tanımlanması
  - Bilginin sınıflandırılması (A.8.2)
  - Veri koruma, telif hakları vb.

A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği

A.15.1.3 Bilgi ve iletişim teknolojileri tedarik zinciri

Tedarikçiler ile yapılan anlaşmalar, bilgi ve iletişim teknolojileri hizmetleri ve ürün tedarik zinciri ile ilgili bilgi güvenliği risklerini ifade eden şartları içermelidir.

- Tedarikçi anlaşmaları (Tedarik zinciri güvenliği)
  - Tedarik zinciri boyunca kritik bileşenlerin izlenebileceğinin garanti edilmesi
  - Tedarik zinciri ile ilgili olarak bilgi paylaşımının kurallarının belirlenmesi

A.15 Tedarikçi ilişkileri

A.15.2 Tedarikçi hizmet sağlama yönetimi

Amaç: Tedarikçi anlaşmalarıyla uyumlu olarak kararlaştırılan seviyede bir bilgi güvenliği ve hizmet sunumu sürdürmek

A.15.2.1 Tedarikçi hizmetlerini izleme ve gözden geçirme

Kuruluşlar düzenli aralıklarla tedarikçi hizmet sunumunu izlemeli, ***gözden geçirmeli*** *ve tetkik etmelidir.*

- Tedarikçi hizmetlerinin izlenmesi ve gözden geçirilmesi, anlaşmalardaki bilgi güvenliği şart ve hükümlerinin yerine getirilmesini kapsamalı
- Bilgi güvenliği olay ve problemlerinin uygun şekilde yönetilmesi
- Kuruluşla tedarikçi arasında hizmet yönetim ilişkisi süreci
- Hizmet performans seviyelerinin izlenmesi.

A.15.2 Tedarikçi hizmet sağlama yönetimi

A.15.2.1 Tedarikçi hizmetlerini izleme ve gözden geçirme

- Tedarikçi tarafından hazırlanan servis raporlarının gözden geçirilmesi
- Düzenli ilerleme toplantılarının yapılması
- Tedarikçilere tetkik yapılması
- Tedarikçinin tetkik sonuçlarının ve bilgi güvenliği olaylarının kayıtlarının, operasyonel problemlerin ve hatalarının gözden geçirilmesi
- Tedarikçinin kendi tedarikçileri ile ilişkilerinin gözden geçirilmesi

A.15.2 Tedarikçi hizmet sağlama yönetimi

A.15.2.2 Tedarikçi hizmetlerindeki değişiklikleri yönetme

Mevcut bilgi güvenliği politikalarını, prosedürlerini ve kontrollerini sürdürme ve iyileştirmeyi içeren tedarikçilerin hizmet tedariki değişiklikleri, ilgili iş bilgi, sistem ve dâhil edilen süreçlerin kritikliğini ve risklerin yeniden değerlendirmesini hesaba katarak yönetilmelidir.

- Tedarikçi sözleşmelerindeki değişiklikler
- Kuruluş tarafından yapılan değişiklikler
  - Mevcut hizmetlerin iyileştirilmesi
  - Yeni uygulama ve sistemlerin geliştirilmesi

A.16
Bilgi Güvenliği İhlal Olayı Yönetimi

1 Güvenlik Kategorisi

- Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi

A.16 Bilgi Güvenliği İhlal Olayı Yönetimi

A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi

Amaç: Bilgi güvenliği ihlal olaylarının yönetimine, güvenlik olayları ve açıklıklar üzerindeki bağlantısını da içeren, tutarlı ve etkili yaklaşımın uygulanmasını sağlamak.

A.16.1.1 Sorumluluklar ve prosedürler

*Bilgi güvenliği ihlal olaylarına hızlı, etkili ve düzenli bir yanıt verilmesini sağlamak için yönetim sorumlulukları ve **prosedürleri** oluşturulmalıdır.*

Bilgi Güvenliği İhlal Olaylarına Müdahele

- Hızlı
- Etkili
- Sıralı (Düzenli)

A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi

A.16.1.1 Sorumluluklar ve prosedürler

- Farklı bilgi güvenliği olayları için prosedürler
  - Bilgi sistemi arızaları ve hizmet kaybı
  - Kötü niyetli kodlar
  - Tamamlanmamış veya kesin olmayan veriden kaynaklanan hatalar
  - Gizlilik ve bütünlük ihlalleri
  - Bilgi sistemlerinin kötü kullanımı/suistimali

A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi

A.16.1.1 Sorumluluklar ve prosedürler

- Normal beklenmedik olay planlarına ilaveten
  - Olayın sebebine ilişkin analiz prosedürleri
  - Önleme prosedürleri
  - Olayın tekrarlanmasını engellemek için önleyici faaliyet planlanması ve uygulanması
  - Olay sonrasında geri kazanmadan etkilenen ya da geri kazanmada rol alan personel ile haberleşme
  - Faaliyetin uygun yetkililere raporlanması

A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi

A.16.1.2 Bilgi güvenliği olaylarının raporlanması

Bilgi Güvenliği ihlal Olaylar uygun yönetim kanalları aracılığı ile olabildiğince hızlı bir şekilde ***raporlanmalıdır.***

Tüm çalışanlar ve yükleniciler güvenlik olaylarında

- Uygun yönetim kanallarının kullanımı
- Mümkün olduğu kadar hızlı raporlama
- Raporlama prosedürü

Farkında olmalılar

A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi
A.16.1.2 Bilgi güvenliği olaylarının raporlanması

- **Olaya müdahele prosedürü**
  - Olaya müdahele sonrasında sonuçla ilgili uygun geri besleme süreçleri
  - Olay raporlama formları
  - Raporlamanın yapılacağı personelin belirlenmesi
    - Personelin kurumca bilinmesinin sağlanması
    - Personelin her zaman ulaşılabilir olması
    - Personelin zamanında uygun faaliyeti gerçekleştirmesinin sağlanması
  - Rapor alındıktan sonra yapılacak faaliyetler

A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi
A.16.1.2 Bilgi güvenliği olaylarının raporlanması

- **Olaya müdahele prosedürü (Kapsam)**
- Bilgi güvenliği olayı sonrasında doğru davranış/hareketin sergilenmesi
  - Önemli detayların anında not edilmesi (uygunsuzluk ya da ihlalin çeşidi, oluşan arıza, ekrandaki mesajlar, ilginç davranışlar vb.)
  - Kendi başına hareket edilmemesi, raporlamanın ilgili kişiye yapılması
  - Güvenlik ihlaline sebep olan personel, yüklenici ya da 3. taraf kullanıcıya uygulanacak disiplin süreci
- Yüksek riskli kısımlarda baskı altında çalışan personel için alarm tertibatı

A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi
A.16.1.2 Bilgi güvenliği olaylarının raporlanması

- Bilgi güvenliği olayı örnekleri
  - Hizmet, ekipman/cihaz kaybı
  - Sistem arızası ya da aşırı yüklenmesi
  - İnsan hataları
  - Politika ve klavuzlara uygun olmayan faaliyetler
  - Fiziksel güvenlik uygulamalarının ihlali
  - Kontrolsüz sistem değişiklikleri
  - Yazılım/donanım arızaları
  - Erişim ihlalleri

A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi
A.16.1.2 Bilgi güvenliği olaylarının raporlanması

- Kullanıcı farkındalık eğitimlerinde bilgi güvenliği olaylarının anlatımı
  - Neler olabilir
  - Nasıl davranılmalı
  - Gelecekte aynı olayın nasıl engelleneceği
- Arıza ve anormal sistem davranışları
  - Güvenlik ataklarının/güvenlik ihlallerinin göstergesi
  - Her zaman bilgi güvenliği olayı olarak raporlanmalı
- ISO/IEC 27035:2011 Bilgi Teknolojisi- Güvenlik Teknikleri – Bilgi güvenliği olay yönetimi (Information technology -- Security techniques -- Information security incident management)

A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi

A.16.1.3 Bilgi güvenliği zayıflıklarının raporlanması

Kuruluşun bilgi sistemlerini ve hizmetlerini kullanan çalışanlardan ve yüklenicilerden, sistemler veya hizmetlerde gözlenen veya şüphelenilen herhangi bir bilgi güvenliği açıklığına dikkat etmeleri ve bunları ***raporlamaları*** *istenmelidir.*

- Raporlama mekanizması
  - Kolay
  - Erişilebilir
  - Kullanılabilir
- Şüphelenilen zayıflıkların denenmemesi için çalışanların, yüklenicilerin ve 3. taraf kullanıcıların bilgilendirilmesi

A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi

A.16.1.4 Bilgi güvenliği olaylarında değerlendirme ve karar verme

Bilgi güvenliği olayları değerlendirilmeli ve bilgi güvenliği ihlal olayı olarak sınıflandırılıp sınıflandırılmayacağına karar verilmelidir.

- İrtibat noktası, tanımlanmış bilgi güvenliği olayı ve ihlal olayı sınıflama ölçütüne göre değerlendirme yapmalı
- Karar vermeli: Bilgi güvenliği olayı mı, değil mi?
- Kuruluşta bilgi güvenliği olay müdahele takımı (ISIRT) varsa, karar bu takım tarafından verilmeli
- Değerlendirme ve kararlar detaylı olarak kaydedilmeli (Gelecekte kullanım için)

A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi

A.16.1.5 Bilgi güvenliği ihlal olaylarına yanıt verme

Bilgi güvenliği ihlal olaylarına, yazılı prosedürlere uygun olarak yanıt verilmelidir.

- Müdahele atanmış bir kişi ve diğer ilgili kişiler tarafından yapılmalı
- Olaydan hemen sonra delil toplanması
- Adli bir durumun olup olmadığı sorgulanmalı
- Tüm müdahele faaliyetlerinin daha sonra analizi için kaydı (logging)
- Olayın bilmesi gereken iç ve dış taraflara iletilmesi
- Olaya müdahelenin öncelikli amacı, normal güvenlik seviyesine dönmek olmalı

A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi

A.16.1.6 Bilgi güvenliği ihlal olaylarından ders çıkarma

Bilgi güvenliği ihlal olaylarının analizi ve çözümlemesinden kazanılan tecrübe gelecekteki ihlal olaylarının gerçekleşme olasılığını veya etkilerini azaltmak için kullanılmalıdır.

- Bilgi Güvenliği İhlal Olaylarının ölçülmesi ve izlenmesi
- Mekanizmanın bulunması
  - Olayların türleri
  - Olayların miktarları (Hacmi/büyüklüğü)
  - Olayların maliyetleri
- Tekrarlanan ve yüksek etkili olayların belirlenmesi
- Gelecekteki olayların sıklık, hasar ve maliyetlerinin sınırlandırılması için gerekli ilave kontrollere olan ihtiyacın belirlenmesi

A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi

A.16.1.7 Kanıt toplama

*Kuruluş kanıt olarak kullanılabilecek bilginin teşhisi, toplanması, edinimi ve korunması için **prosedür** tanımlamalı ve uygulamalıdır.*

- Bilgi güvenliği ihlal olayı sonrasında yasal faaliyet gerektiğinde

  - Kanıtların toplanması
  - Kanıtların muhafazası
  - Kanıtların ilgili makamlara sunumu
  - Disiplin faaliyeti için iç prosedürler

A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi
A.16.1.7 Kanıt toplama

- **Kanıt için kurallar (Kapsam)**

  - Kanıtın geçerliliği/Yasal makamlarca kabul edilebilirliği
  - Kanıtın değeri (Kalite ve bütünlük)
    - Kağıt kanıtlar
    - Orijinalin güvenliği
    - Dokümanı kimin bulduğu
    - Dokümanın nerede ve ne zaman bulunduğu
    - Dokümanın bulunmasına kimin şahit olduğu
    - Orijinalin tahrif edilmemesinin sağlanması

A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi
A.16.1.7 Kanıt toplama

- **Kanıt için kurallar (Kapsam)**

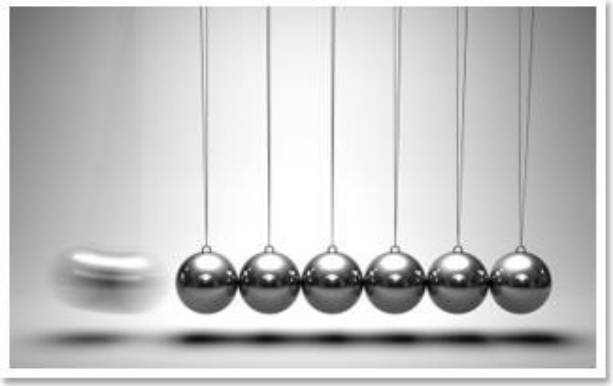
  - Bilgisayar ortamındaki kanıtlar

    - Taşınabilir medyanın imajı/kopyası
    - Kopyalama prosesindeki tüm faaliyetlerin logları
    - Kopyalamanın şahitli yapılması

A.17
İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları

2 Güvenlik Kategorisi

- Bilgi güvenliği sürekliliği
- Yedek fazlalıklar



A.17 İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları

A.17.1 Bilgi güvenliği sürekliliği

Amaç: Bilgi güvenliği sürekliliği, kuruluşun iş sürekliliği yönetim sistemlerinin içerisine dahil edilmelidir

A.17.1.1 Bilgi güvenliği sürekliliğinin planlanması

Kuruluş olumsuz durumlarda, örneğin bir kriz ve felaket boyunca, bilgi güvenliği ve bilgi güvenliği yönetimi sürekliliğinin gereksinimlerini belirlemelidir.

- Bilgi güvenliği sürekliliğinin iş sürekliliği yönetimi veya felaket kurtarma yönetimi sürecinde yeraldığının tespiti
- İş sürekliliği ve felaket kurtarma planlamasında bilgi güvenliği gereklerinin belirlenmesi

A.17.1 Bilgi güvenliği sürekliliği

A.17.1.2 Bilgi güvenliği sürekliliğinin uygulanması

*Kuruluş, olumsuz bir olay süresince bilgi güvenliği için istenen düzeyde sürekliliğin sağlanması için prosesleri, prosedürleri ve kontrolleri kurmalı, **yazılı** hale getirmeli, uygulamalı ve sürdürmelidir*

- Kesintiye sebep olabilecek bir olaya müdahele ve etkinin azaltılması için gerekli personel (yetkin, tecrübeli ve yetkili)
- Dokümante planlar, müdahele ve kurtarma prosedürleri
- İş sürekliliği ve felaket kurtarma süreçlerinde bilgi güvenliği kontrolleri

A.17.1 Bilgi güvenliği sürekliliği

A.17.1.3 Bilgi güvenliği sürekliliğinin doğrulanması, gözden geçirilmesi ve değerlendirilmesi

*Kuruluş, oluşturulan ve uygulanan bilgi güvenliği sürekliliği kontrollerinin, olumsuz olaylar süresince geçerli ve etkili olduğundan emin olmak için **belirli aralıklarda doğruluğunu** sağlamalıdır.*

- Organizasyonel, teknik, prosedürsel ve süreç değişiklikler, bilgi güvenliği sürekliliğine etki edebilir.
- Böyle durumlarda bilgi güvenliği için süreçlerin, prosedürlerin ve kontrollerin gözden geçirilmesi gerekir.
- Bilgi güvenliği sürekliliği süreçleri, prosedürleri ve kontrollerinin fonksiyonelliğinin tatbikatı ve testi

A.17 İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları

A.17.2 Yedek fazlalıklar

Amaç: Bilgi işleme olanaklarının erişilebilirliğini temin etmek

A.17.2.1 Bilgi işleme olanaklarının erişebilirliği

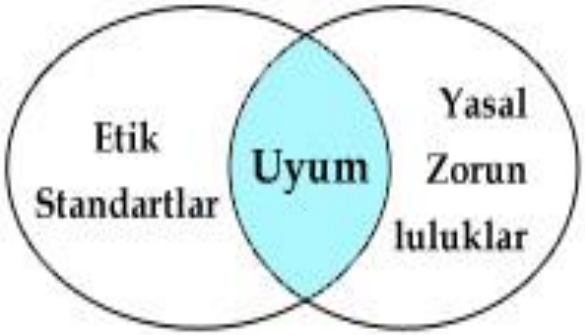
Bilgi işleme imkanları, erişilebilirlik gereksinimlerini karşılamak için yeterli fazlalık/yedek ile gerçekleştirilmelidir.

- Bilgi sistemlerinin temini için iş gereksinimlerinin belirlenmesi
- Teminin garanti edilemediği durumlarda yedek bileşenler bulundurulmalı
- Mümkünse yedek bilgi sistemlerinin testi (Gerektiğinde kullanılabilir olduğunun garanti edilmesi)

A.18
Uyum

2 Güvenlik Kategorisi

- Yasal ve sözleşmeye tabi gereksinimlerle uyum
- Bilgi güvenliği gözden geçirmeleri



A.18 Uyum

A.18.1Yasal ve sözleşmeye tabi gereksinimlerle uyum

Amaç: Yasal, meşru, düzenleyici veya sözleşmeye tabi yükümlülüklere ve her türlü güvenlik gereksinimlerine ilişkin ihlalleri önlemek.

A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama

İlgili tüm yasal mevzuat, düzenleyici, sözleşmeden doğan şartları ve kuruluşun bu gereksinimleri karşılama yaklaşımı her bilgi sistemi ve kuruluşu için açıkça tanımlanmalı, yazılı hale getirilmeli ve güncel tutulmalıdır.

- Gerekleri karşılayan özel kontroller ve bireysel sorumluluklar benzer şekilde tanımlanmalı ve dokümante edilmeli
- Yöneticiler kuruluşa uygulanan tüm yasal mevzuatı tanımlamalı
- Eğer başka ülkelerde iş yapılıyorsa, yöneticiler o ülkelerdeki mevzuatı da göz önüne almalı

A.18.1 Yasal ve sözleşmeye tabi gereksinimlerle uyum

A.18.1.2 Fikri mülkiyet hakları

*Fikri mülkiyet hakları ve patentli yazılım ürünlerinin kullanımı üzerindeki yasal, düzenleyici ve anlaşmalardan doğan şartlara uyum sağlamak için uygun **prosedürler** gerçekleştirilmelidir.*

- Fikri mülkiyet haklarının korunması için

  - Yazılım vb. diğer ürünlerin yasal olarak kullanılmasını öngören "Fikri Mülkiyet Haklarına Uyum" politikasının yayınlanması
  - Kullanım haklarının çiğnenmemesi için yazılımın sadece güvenilir kaynaklardan sağlanması
  - Fikri mülkiyet haklarını korumak için politikaların bilincinde olmak ve personele ihlal durumunda disiplin işlemi uygulanacağını önceden bilgi vermek

A.18.1 Yasal ve sözleşmeye tabi gereksinimlerle uyum

A.18.1.2 Fikri mülkiyet hakları

- Fikri mülkiyet haklarını korumak için

  - Uygun varlık kayıtlarının muhafaza edilmesi ve fikri mülkiyet haklarının korunması gereken tüm varlıkların belirlenmesi
  - Lisansların, ana disklerinin (master disks) ve kılavuzlarının v.b. kanıt olarak muhafazası
  - İzin verilen kullanıcı sayısının aşılmamasını sağlayan kontrollerin uygulanması
  - Yalnızca yetkili yazılım ve lisanslı ürünlerin yüklenmiş olduğunun kontrolü için gözden geçirme yapılması

A.18.1 Yasal ve sözleşmeye tabi gereksinimlerle uyum

A.18.1.2 Fikri mülkiyet hakları

- Fikri mülkiyet haklarını korumak için

  - Uygun lisans şartlarının devamının sağlanması için bir politika belirlenmesi
  - Yazılımın elden çıkarılması veya başkalarına transferi için politika belirlenmesi
  - Kitap, makale, rapor veya diğer dokümanların izinsiz çoğaltılmaması

A.18.1 Yasal ve sözleşmeye tabi gereksinimlerle uyum

A.18.1.3 Kayıtların korunması

Kayıtlar kaybedilmeye, yok edilmeye, sahteciliğe, yetkisiz erişime ve yetkisiz yayımlamaya karşı yasal, düzenleyici, sözleşmeden doğan şartlar ve iş şartlarına uygun olarak korunmalıdır.

- Kayıtlar kategorilendirilmeli (Muhasebe kayıtları, veritabanı kayıtları, işlem günlükleri (transaction logs), denetim günlükleri (audit log) ve çalışma prosedürleri gibi)

- Her bir kayıtın saklama süreleri, ayrıntıları ve kağıt, mikrofilm, manyetik, optik gibi saklama ortamı türü

A.18.1 Yasal ve sözleşmeye tabi gereksinimlerle uyum

A.18.1.3 Kayıtların korunması

- Tüm ilgili kriptografik anahtarlar ve şifreli arşiv veya elektronik imza ile ilişkilendirilmiş programlar (A.10) kayıtlar saklandığı sürece kayıtların şifresini çözmek için saklanmalı
- Kayıtların muhafaza edildiği ortamın bozulma ihtimaline dikkat edilmeli
- Organizasyonun kayıtları kanun, kontrat, anlaşma ve işin doğasından kaynaklanan gereksinimler uyarınca üretilen kayıtlar
- Kaybolmaya ve bozulmaya karşı korumalı

A.18.1 Yasal ve sözleşmeye tabi gereksinimlerle uyum

A.18.1.3 Kayıtların korunması

- Saklama planı olmalı
- Veri saklama sistemi seçilirken belli bir süre sonra teknoloji değişikliği dolayısıyla kayıtların erişilemez hale gelmemesi için gerekli tedbirlerin alınması
- Donanımsal ve yazılımsal format uyumunu sağlamak için gerekli program ve teçhizatın kayıtlarla birlikte saklanması
- Kayıtların ve bilgilerin tutulması, saklanması, işlenmesi ve yok edilmesi için rehber/prosedür
- Kayıtların ve bilginin, kayıptan, yıkımdan ve tahriften korunmasını sağlayan uygun kontroller

A.18.1 Yasal ve sözleşmeye tabi gereksinimlerle uyum

A.18.1.4 Mahremiyet ve kişi tespit bilgisinin korunması

Kişiyi tespit bilgisinin gizliliği ve korunması uygulanabilen yerlerde ilgili yasa ve düzenlemelerin gerektirdiği şekilde sağlanmalıdır.

- Yasalar veya mevcut kontratlar uyarınca veriyi ve kişisel bilgilerin gizliliğini korumak için kurumsal politika ve kontrollerin oluşturulması
- Kişisel bilginin işlenmesi ile ilgisi olan tüm personelin politikadan haberdar edilmesi
- Bazı ülkeler, kişisel verilerin toplanması, işlenmesi ve iletiminde kontrolleri yerleştirmek için mevzuat yayınlamıştır.

A.18.1 Yasal ve sözleşmeye tabi gereksinimlerle uyum

A.18.1.5 Kriptografik kontrollerin düzenlemesi

Kriptografik kontroller tüm ilgili sözleşmeler, yasa ve düzenlemelere uyumlu bir şekilde kullanılmalıdır.

- Yasa, düzenleme ve anlaşmalara uyum
  - Kriptografik işlemler yapan bilgisayar yazılım ve donanımının eklenmesi/çıkarılması ile ilgili kısıtlamalar
  - Kriptografik işlemlerin eklenmesine hazır olarak tasarlanmış bilgisayar yazılım ve donanımının eklenmesi/çıkarılması ile ilgili kısıtlamalar
  - Şifreleme kullanımıyla ilgili kısıtlamalar
  - Kriptolu bilgiye ulusal otoriteler tarafından erişilmek istenmesi durumunda kullanılacak yöntemler

A.18.2 Bilgi güvenliği gözden geçirmeleri

Amaç: Bilgi güvenliğinin kurumsal politika ve prosedürler uyarınca gerçekleştirilmesini ve yürütülmesini sağlamak.

A.18.2.1 Bilgi güvenliğinin bağımsız gözden geçirmesi

*Kuruluşun bilgi güvenliğine ve uygulamasına (örn. bilgi güvenliği için kontrol hedefleri, kontroller, politikalar, prosesler ve prosedürler) yaklaşımı belirli aralıklarla veya önemli değişiklikler meydana geldiğinde bağımsız bir şekilde **gözden geçirilmelidir**.*

A.18.2 Bilgi güvenliği gözden geçirmeleri

A.18.2.1 Bilgi güvenliğinin bağımsız gözden geçirmesi

- Yönetim bağımsız **gözden geçirmeyi** başlatmalı

- Organizasyonun bilgi güvenliği yönetimi yaklaşımının sürekli uygunluğu, yeterliliği ve etkinliğinden emin olunması

  - Belirli aralıklar/Önemli değişikliklerde
  - Politikalar ve kontrol hedeflerinin de dahil olduğu güvenliğe olan yaklaşım için değişiklik gereksinimlerinin ve iyileştirmelerin değerlendirilmesi
  - Sonuçlar raporlanmalı
  - Uygunsuzluklar varsa düzeltici faaliyetler başlatılmalı

A.18.2 Bilgi güvenliği gözden geçirmeleri

A.18.2.2 Güvenlik politikaları ve standartlar ile uyum

Yöneticiler kendi sorumluluk alanlarında bulunan, bilgi işleme ve prosedürlerin, uygun güvenlik politikaları, standartları ve diğer güvenlik gereksinimleri ile uyumunu düzenli bir şekilde ***gözden geçirmelidir.***

- Etkin düzenli gözden geçirme için otomatik ölçme ve raporlama araçları kullanılmalı
- Uyumsuzluğun nedenini ve tekrar etmemesi için alınması gereken tedbirleri almalı

A.18.2 Bilgi güvenliği gözden geçirmeleri

A.18.2.2 Güvenlik politikaları ve standartlar ile uyum

- Yöneticiler kontrol ya da **gözden geçirme** sonucunda bir uyumsuzluğun bulunması halinde
  - Düzeltici faaliyetin uygulanması ve sonuçlarının gözden geçirilmesi
  - Uygulanan düzeltici faaliyetin ve gözden geçirmenin sonuçları kayıt altına alınmalı ve bağımsız gözden geçirmeyi yapan tetkik görevlilerine raporlanmalı

A.18.2 Bilgi güvenliği gözden geçirmeleri

A.18.2.3 Teknik uyumun gözden geçirilmesi

*Kuruluşun bilgi güvenliği politika ve standartları ile uyumu için bilgi sistemleri düzenli bir şekilde **gözden geçirilmelidir**.*

- Bilgi sistemleri, güvenlik uygulama standartları ile uyumun sağlanması için düzenli olarak kontrol edilmeli
- Teknik uyumluluk testleri otomatik araçlar yardımı ile yapılmalı ve teknik uzman tarfından değerlendirilmeli
- Sızma (Penetrasyon) testleri ve açıklık analizleri yapılıyorsa bu esnada sistem güvenliğinin sekteye uğramaması için gerekli tedbirler alınmalı
- Alternatif olarak manuel gözden geçirme tecrübeli bir sistem mühendisi tarafından yapılabilir

A.18.2 Bilgi güvenliği gözden geçirmeleri

A.18.2.3 Teknik uyumun gözden geçirilmesi

- Sızma testleri veya açıklık değerlendirmeleri yapılırsa faaliyetlerin sistem güvenliğini riske atmasının engellenmesi
- Testler planlanmalı, dokümante edilmeli
- Uyumun gözden geçirilmesi, bağımsız uzmanların yaptığı sızma testlerini ve açıklık değerlendirmeyi de kapsar.

Risk Yönetimi

- Risk Değerlendirme Metodolojisinin Belirlenmesi
- Risk Değerlendirmenin yapılması
- Risk İşlemenin yapılması

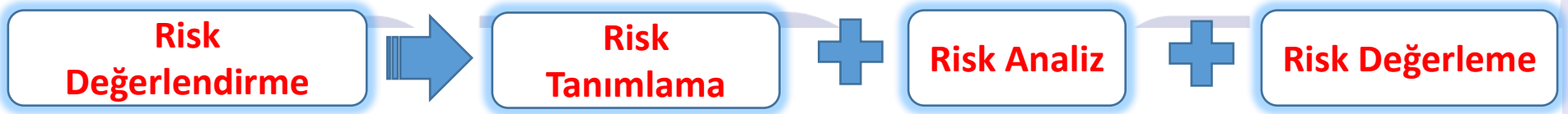
Risk Yönetimi

BGYS nin kapsamını dikkate alarak

- işin
- kuruluşun
- yerleşim yerinin
- varlıkların
- teknolojinin

özelliklerine göre Risk Yönetim çerçevesinin belirlenmesi

Risk Değerlendirme



Risk Tanımlama

Bilginin üzerindeki Gizlilik , Bütünlük ve Erişilebilirlik kayıpları ile ilgili risklerin tespit edilmesi

- yöntemler
- Risk Listesi
- Literatür taraması
- Kurum tecrübesi
- Dokümantasyon incelemesi

Risk Değerlendirme

Risk Tanımlama

- **Risk *ƒ*(ihtimal x etki)**

  - İhtimali etkileyen parametreler
    - Tehditler
    - Açıklıklar

Tehdit: Açıklığın kullanılması yolu ile varlıklara zarar verme potansiyeli

Açıklık : Bilgi güvenliği ihlal olayına neden olabilecek zayıflık, hata, kusur

Tehdidin kullandığı yol

Risk Değerlendirme

Risk Tanımlama

Tehditlerin belirlenmesi

- Doğal Tehditler
  - Deprem , Sel, Yıldırım, Fırtına, vb.
- Çevresel tehditler
  - Güç Kesintisi, internet kesintisi vb.
- İnsan Kaynaklı (Bilerek, Kaza ile)
  - Yazılım hataları, parolaların çalınması, hırsızlık, yetkisiz ağa erişim

Risk Değerlendirme

Risk Tanımlama

Tehdit Örnekleri

- Bombalı/silahlı saldırı
- Endüstriyel bilgi sızması etişim hatlarına/kablolarına zarar verilmesi
- Saklama ortamının tahrip edilmesi
- Dinleme (tele-kulak)
- Sıcaklık ve nemdeki anormal değişiklikler
- Yazılımın yasa dışı biçimde kullanımı

Risk Değerlendirme

Risk Tanımlama

- Kötü niyetli yazılımlar (virüsler, kurtlar, truva atları)
- Bakım hataları/eksiklikleri
- Kullanıcı kimliğinin maskelenmesi
- Mesajların yanlış yönlendirilmesi
- Hırsızlık
- Ağ şebekesinin yetki dışı kullanımı
- Yazılım arızası , Donanım arızası
- Güç dalgalanmaları
- Personel hataları

Risk Değerlendirme

Risk Tanımlama

- **Açıklıkların belirlenmesi:**
- **Açıklık belirlemede kullanılabilecek yöntemler**
  - Anketler
  - Yüz yüze görüşmeler
  - Dokümantasyon incelemesi
  - Otomatik tarama araçları/cihaz tanıma araçları
  - Kuruluşun bildiği açıklıklar
  - Üreticiler tarafından yayınlanan uyarılar/açıklıklar

Risk Değerlendirme

Risk Tanımlama

Açıklıkların belirlenmesi:

- **Açıklık belirlemede kullanılabilecek yöntemler**
  - Alt yapı ve çevresel açıklıklar
  - Donanımsal ,Yazılımsal
  - Personel ile ilgili açıklıklar
  - Önceki risk değerlendirme dokümanları
  - Sistem güvenlik taramalarının ve sızma testlerinin sonuçları
  - Güvenlikle ilgili web sayfaları ve e-posta listeleri

Risk Değerlendirme

Risk Tanımlama

Açıklıkların belirlenmesi- Örnek açıklıklar

- **Altyapı ve çevreyle ilgili açıklıklar**

  - Binada yeterli fiziksel güvenliğin bulunmaması (hırsızlık)
  - Binalara ve odalara girişlerde yetersiz fiziksel kontrol (kasten zarar verme)
  - Eski güç kaynakları (güç dalgalanmaları)
  - Deprem bölgesinde bulunan yapılar (deprem)
  - Herkesin erişebildiği kablosuz ağlar (hassas bilginin açığa çıkması, yetkisiz erişim)
  - Dış kaynak kullanımında işletilen prosedür ve yönetmeliklerin veya şartnamelerin eksikliği/yetersizliği (yetkisiz erişim)

Risk Değerlendirme

Risk Tanımlama

Açıklıkların belirlenmesi- Örnek açıklıklar

- **Donanımlarla ilgili açıklıklar**
  - Periyodik yenilemenin yapılmaması (saklama ortamlarının eskimesi)
  - Donanımların bozulması nedeniyle erişimin durması
  - Voltaj değişikliklerine, ısıya, neme, toza duyarlılık (güç dalgalanmaları, erişim güçlükleri vs.)
  - Periyodik bakım eksikliği (bakım hataları)
  - Değişim yönetimi eksikliği (kullanıcı hataları)

Risk Değerlendirme

Risk Tanımlama

Açıklıkların belirlenmesi- Örnek açıklıklar

- **Yazılımlarla ilgili açılıklar**
  - Yama yönetimi eksikliği/yetersizliği (yetkisiz erişim, hassas bilginin açığa çıkması)
  - Kayıt yönetimi eksikliği/yetersizliği (yetkisiz erişim)
  - Kimlik tanımlama ve doğrulama eksiklikleri (yetkisiz erişim, başkalarının kimliğine bürünme)
  - Şifre yönetimi yetersizliği (yetkisiz erişim, başkalarının kimliğine bürünme)
  - Şifre veritabanlarının korunmaması (yetkisiz erişim, başkalarının kimliğine bürünme)

Risk Değerlendirme

Risk Tanımlama

Açıklıkların belirlenmesi- Örnek açıklıklar

- **Yazılımlarla ilgili açılıklar**
  - Erişim izinlerinin yanlış verilmesi (yetkisiz erişim)
  - İzinsiz yazılım yüklenmesi ve kullanılması (zararlı yazılımlar, yasal gerekliliklere uyum)
  - Saklama ortamlarının doğru silinmemesi ve imha edilmemesi (hassas verinin ortaya çıkması, yetkisiz erişim)
  - Yazılım gereksinimlerinin yanlış veya eksik belirlenmesi (yazılım hataları)
  - Yazılımların yeterli test edilmemesi (yetkisiz erişim, yazılımların yetkisiz kullanımı)

Risk Değerlendirme

Risk Tanımlama

Açıklıkların belirlenmesi- Örnek açıklıklar

- **Haberleşmeyle ilgili açıklıklar**
  - Korunmayan haberleşme hatları (dinleme)
  - Hat üzerinden şifrelerin açık olarak iletilmesi (yetkisiz erişim)
  - Telefon hatlarıyla kurum ağına erişim (yetkisiz erişim)
  - Ağ yönetimi yetersizliği/eksikliği (trafiğin aşırı yüklenmesi)
- **Dokümanlarla ilgili açıklıklar**
  - Dokümanların güvensiz saklanması (hırsızlık)
  - Dokümanların kontrolsüz çoğaltılması (hırsızlık)
  - Dokümanların imha edilmemesi (hırsızlık, hassas bilginin açığa çıkması)

Risk Değerlendirme

Risk Tanımlama

Açıklıkların belirlenmesi- Örnek açıklıklar

- **Personel ile ilgili açıklıklar**
  - Eğitimi eksikliği (personel hataları)
  - Güvenlik farkındalığı eksikliği (kullanıcı hataları)
  - Donanımların veya yazılımların yanlış kullanılması (personel hataları)
  - İletişim ve mesajlaşma ortamların kullanımını düzenleyen politikanın eksikliği/yetersizliği (yetkisiz erişim)
  - İşe alımda yetersiz özgeçmiş incelemesi ve doğrulaması (kasten zarar verme)

Risk Değerlendirme

Risk Analizi

- **İhtimal değerlendirilmesi (Tehdit, Açıklık)**
  - Tehdit motivasyonu, becerisi
  - Uygulanan kontroller
  - Açıklığın cinsi

İhtimal seviyesi	İhtimal Tanımı
1	Çok Düşük (kontroller var, açıklık az, motivasyon yok)
2	Düşük (kontroller var, açıklık az, motivasyon var)
3	Orta (kontroller var, yeterli değil, açıklık az, motivasyon var)
4	Yüksek (kontroller var, yeterli değil, açıklık var, motivasyon var)
5	Çok Yüksek (kontroller var, yeterli değil, açıklık var, motivasyon yüksek)

Bilgi neden korunmalıdır ?

- Bilginin üzerindeki Etkisi olan tehditler

Bu tehditler nasıl zarar verir ?

- **Bu tehditler hangi risk koridorlarını kullanır**

Önlem almasak olmaz mı ?

Riskleri azalmak için hangi karşı önlemleri a

Risk Değerlendirme

Risk Analizi

- **İş Sonuç (Etki) Analizi**
  - Varlığın görevi, kritikliği, varlığın etkilediği verinin hassasiyeti ve varlığın mali değeri göz önüne alınmalı
  - Gizlilik, Bütünlük, Elverişlilik (Değer parametresi Max[1,2,3])
  - İş etki analizlerinden alınacak veriler İş Etkisi =Etki X Varlık Değeri

Etki Şiddeti	Etkinin Tanımı
1	Çok Düşük (Kuruluş Etkilenmez)
2	Düşük (Bazı varlıklar zarar görür)
3	Orta (Mali zarar)
4	Yüksek (İş sürekliliği sekteye uğrar)
5	Çok Yüksek (Felaket)

Risk Değerlendirme

Risk Analizi

- **İş Sonuç (Etki) Analizi**

		Varlık Değeri (Max (G B E)[1,2,3])		
		(1)	(2)	(3)
Etki	Çok Düşük (1)	1	2	3
	Düşük (2)	2	4	6
	Orta (3)	3	6	9
	Yüksek (4)	4	8	12
	Çok Yüksek (5)	5	10	15

Risk Değerlendirme

Risk Analizi

Risk değeri = (İhtimal x İş Etki)

Risk Tablosu		İş Etki										
		(1)	(2)	(3)	(4)	(5)	(6)	(8)	(9)	(10)	(12)	(15)
Olasılık	Çok Düşük (1)	1	2	3	4	5	6	8	9	10	12	15
	Düşük (2)	2	4	6	8	10	12	16	18	20	24	30
	Orta (3)	3	6	9	12	15	18	24	27	30	36	45
	Yüksek (4)	4	8	12	16	20	24	32	36	40	48	60
	Çok Yüksek (5)	5	10	15	20	25	30	40	45	50	60	75

Risk Değerlendirme

- **Uygulanan Mevcut kontrollerin belirlenmesi**

- Belirlenen tehditlerin, açıklıkların gerçekleşme olasılıklarını azaltacak veya ortadan kaldıracak kontrollerin halihazırda uygulanıp uygulanmadığı
- Uygulanan kontroller açıklıkların gerçekleşme olasılıklarını düşürür
- Uygulanan kontroller risk derecelendirmesinde önemlidir.

Risk Değerlendirme

Risk Kriterleri

- Kabul Kriterleri

  Yasal durum

  Maliyet Etkin (fayda-maliyet dikkate alınarak)……

- Risk Değerlendirmesi için kriterler

  [0 - 5] arası ihmal edilebilir risk

  [6 - 12] arası izlenmesi gerekir , gerekirse önlem al

  [15-36] arası düşürülmesi gerekir (kontrol uygula)

  [40- ...] Felaket , düşür

Risk İşleme

- **Risk işleme Seçeneklerinin Belirlenmesi**
  - Kontrollerin Belirlenmesi, (Riskin azaltılması)
  - Risk Transferi (Sigorta vb.)
  - Riskten Kaçınma (yazılımın bir parçasının kullanılmaması)
  - Riski Kabul Etme (Risk Kabul Kriterlerine göre)
- **Uygulanacak Kontrollerin Belirlenmesi**
  - Yönetimsel Kontroller
  - Teknolojik Kontroller
  - Fiziksel Kontroller

Ek A en iyi kontrol örnekleridir.

Ek A kontrol maddeleri eksiksiz değildir, İlave kontrollere ihtiyaç duyulabilir

Koruduğumuz değer nedir ?

Fiziksel Önlemler

Teknolojik Önlemler

Yönetsel Önlemler

Risk İşleme

- **Uygulanacak Kontrollerin Belirlenmesi**

- **Yönetimsel Kontroller**
  - Sorumluluk Ataması,
  - Eğitimler
  - Periyodik olarak sistem denetlemesi,
  - Risk Yönetimi Uygulanması
  - Güvenlik politikaları
  - Standartlar, yönergeler ve prosedürler
  - Acil Durum Müdahale Ekiplerinin kurulması
  - İş sürekliliği planları …v.b

Risk İşleme

- **Uygulanacak Kontrollerin Belirlenmesi**

- **Teknolojik Kontroller**
  - **Kimlik tanımlama** (erişim kontrol listeleri)
  - **Kriptografik anahtar yönetimi (**Anahtar üretimi, saklanması, dağıtımı ve bakımı**)**
  - **Güvenlik yönetimi (**bir veritabanındaki bilgileri kimin okuyacağı, kimin oluşturucağı ve kimin güncelleyebileceğinin ayarlanabilmesi**)**
  - **Sistem koruma kontrolleri (**bilmesi gereken prensibi, süreçlerin ayrımı)

Risk İşleme

- **Uygulanacak Kontrollerin Belirlenmesi**
- **Fiziksel Kontroller**
  - Ziyaretçi Refakati, anti virüs, Veri yedekleme, Kapı ve Giriş Kontrolü
  - Güvenlik Kameraları, yangın alarmları..

Risk İşleme

- **Risk İşleme Planının Formüle edilmesi**
  - Fayda maliyet,
  - Termin Tarihi
  - Etkinliğin değerlendirilmesi için yöntem
- **Riskin sahibinden Risk işleme planını onayının alınması ve artık risklerin kabulü**

Risk İşleme

- **Sonuçların dokümantasyonu**
  - Mevcut risk ve kontrollerin ilgililerce bilinmesi
  - Daha sonra yapılacak risk analizlerine girdi teşkil etmesi
  - Risk analizi süreci tamamlandığında sonuçların bir rapor olarak dokümante edilmesi

İçindekiler

İçindekiler

ISO 27001 KONTROL ALANLARI