TÜRK STANDARDI
TURKISH STANDARD

TS ISO/IEC 27001
Aralık 2013
TS ISO/IEC 27001 : 2006 yerine

ICS 35.040

Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri - Gereksinimler

Information technology - Security techniques - Information Security Management Systems - Requirements

ISO/IEC 27001:2013 standardının Türkçe tercümesidir.

TÜRK STANDARDLARI ENSTİTÜSÜ
Necatibey Caddesi No.112 Bakanlıklar/ANKARA

- Bugünkü teknik ve uygulamaya dayanılarak hazırlanmış olan bu standardın, zamanla ortaya çıkacak gelişme ve değişikliklere uydurulması mümkün olduğundan ilgililerin yayınları izlemelerini ve standardın uygulanmasında karşılaştıkları aksaklıkları Enstitümüze iletmelerini rica ederiz.

- Bu standardı oluşturan İhtisas Grubu üyesi değerli uzmanların emeklerini; tasarılar üzerinde görüşlerini bildirmek suretiyle yardımcı olan bilim, kamu ve özel sektör kuruluşları ile kişilerin değerli katkılarını şükranla anarız.

Kalite Sistem Belgesi
İmalât ve hizmet sektörlerinde faaliyet gösteren kuruluşların sistemlerini TS EN ISO 9000 Kalite Standardlarına uygun olarak kurmaları durumunda TSE tarafından verilen belgedir.

Türk Standardlarına Uygunluk Markası (TSE Markası)
TSE Markası, üzerine veya ambalâjına konulduğu malların veya hizmetin ilgili Türk Standardına uygun olduğunu ve mamulle veya hizmetle ilgili bir problem ortaya çıktığında Türk Standardları Enstitüsü'nün garantisi altında olduğunu ifade eder.

Kritere Uygunluk Belgesi (TSEK Markası Kullanma Hakkı)
Kritere Uygunluk Belgesi; Türk Standardları bulunmayan konularda firmaların ürünlerinin ilgili uluslararası standardlar, benzeri Türk Standardları, diğer ülkelerin milli standardları, teknik literatür esas alınarak Türk Standardları Enstitüsü tarafından kabul edilen Kalite Faktör ve Değerlerine uygunluğunu belirten ve akdedilen sözleşme ile TSEK Markası kullanma hakkı verilen firma adına düzenlenen ve üzerinde TSEK Markası kullanılacak ürünlerin ticari Markası, cinsi, sınıfı, tipi ve türünü belirten geçerlilik süresi bir yıl olan belgedir.

DİKKAT!

TS işareti ve yanında yer alan sayı tek başına iken (TS 4600 gibi), mamulün Türk Standardına uygun üretildiğine dair üreticinin beyanını ifade eder. **Türk Standardları Enstitüsü tarafından herhangi bir garanti söz konusu değildir.**

Standardlar ve standardizasyon konusunda daha geniş bilgi Enstitümüzden sağlanabilir.

Ön söz

- Bu standard, ISO/IEC 27001(2013) standardı esas alınarak, TSE Bilgi Teknolojileri ve İletişim İhtisas Kurulu'na bağlı TK01 Bilişim Teknolojileri Teknik Komitesi'nce hazırlanmış ve TSE Teknik Kurulu'nun 29 Nisan 2014 tarihli toplantısında Türk Standardı olarak kabul edilerek yayımına karar verilmiştir.

- ISO (Uluslararası Standardizasyon Kuruluşu) ulusal standard kuruluşlarının (ISO ülke kuruluşları) dünya çapında federasyonudur. Uluslararası Standard hazırlama çalışması genelde ISO teknik komiteleri aracılığı ile yapılır. Teknik komitenin konusu ile ilgilenen üyelerin o teknik komitede temsil edilme hakkı vardır. ISO ile işbirliği içindeki resmi ya da sivil uluslararası kuruluşlar da, çalışmalarda yer alabilir. ISO, elektroteknik standardizasyonla ilgili tüm konularında Uluslararası Elektroteknik Komisyonu (IEC) ile yakın işbirliği içinde çalışır.

- Uluslararası Standardlar, ISO/IEC Direktifleri Bölüm 2'ye göre yazılmıştır.

- Teknik komitelerin ana görevi, Uluslararası Standard hazırlamaktır. Teknik komitelerin kabul ettiği Taslak Uluslararası Standardlar, oylama için üye ülke kuruluşlarına gönderilir. Bir uluslararası standardın yayınlanması, oy veren üye ülkelerin en az % 75'inin onayını gerektirir.

- Bu dokümanın bazı kısımlarının patent haklarına konu olabileceğine dikkat edilmelidir. Böyle herhangi bir patent hakkının belirlenmesi durumunda ISO sorumlu tutulamaz.

- ISO/IEC 27001, Ortak Teknik Komite ISO/IEC JTC 1, Bilgi teknolojisi alt komitesi SC 27, BT Güvenlik teknikleri tarafından hazırlanmıştır.

  - Bu standard yayımlandığında TS ISO/IEC 27001:2006 nın yerini alır.

- Bu standardda kullanılan bazı kelime ve/veya ifadeler patent haklarına konu olabilir. Böyle bir patent hakkının belirlenmesi durumunda TSE sorumlu tutulamaz.

İçindekiler

0 Giriş

0.1 Genel

Bu standard, bir bilgi güvenliği yönetim sistemi'nin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için şartları ortaya koymak amacıyla hazırlanmıştır. Bir bilgi güvenliği yönetim sisteminin benimsenmesi, bir kuruluş için stratejik bir karardır. Kuruluşun bilgi güvenliği yönetim sisteminin kurulması ve uygulanmasında, kuruluşun ihtiyaç ve amaçları, güvenlik gereksinimleri, kullanılan kurumsal prosesler, kurumun boyutu ve yapısı etkilidir. Tüm bu etkileyen faktörlerin zaman içinde değişmesi beklenir.

Bilgi güvenliği yönetim sistemi, bilginin gizliliği, bütünlüğü ve erişilebilirliğini risk yönetimi prosesini uygulayarak muhafaza eder ve ilgili taraflara risklerin doğru bir şekilde yönetildiğine dair güvence verir.

Bilgi güvenliği yönetim sisteminin kurumsal prosesler ve genel yönetim yapısının bir parçası olması ve bunlar ile entegre olması ve bilgi güvenliğinin süreçlerin, bilgi sistemlerinin ve kontrollerin tasarımında dikkate alınması önemlidir. Bir Bilgi güvenliği yönetim sisteminin kuruluşun ihtiyaçları doğrultusunda ölçeklenmesi beklenir.

Bu standard, iç ve dış taraflar tarafından kuruluşun kendi bilgi güvenliği gereksinimlerini karşılayıp karşılamadığına ilişkin kabiliyetinin değerlendirilmesi amacıyla kullanılabilir.

Bu standarda ortaya konulan şartların sıralaması, önem derecelerini yansıtmaz veya uygulanmaları gereken sıra ile ilgili bir zorunluluk ifade etmez. Liste halindeki maddeler sadece atıf amacı ile numaralandırılmıştır.

ISO/IEC 27000, bilgi güvenliği yönetim sistemleri ailesine (ISO/IEC 27003 [2], ISO/IEC 27004 [3], ISO/IEC 27005 [4], de dâhil olmak üzere) ilgili terim ve tanımlar kapsamında atıfta bulunarak, bilgi güvenliği yönetim sitemlerine genel bakışı ve terimler sözlüğünü tarif eder.

0.2 Diğer yönetim sistemi standardları ile uyumluluk

Bu standard, ISO/IEC Direktifleri Birleştirilmiş ISO Yardımcı Dokümanlarının Ek SL sinde tanımlanan, genel yapı, eşdeğer alt madde başlıkları, eşdeğer metin, ortak terimler ve temel tanımları uygular, bu nedenle Ek SL'yi benimseyen diğer yönetim sistemi standardları ile uyumluluk sağlar.

Ek SL de tanımlanan bu ortak yaklaşım, iki veya daha fazla yönetim sistemi standardının şartlarını sağlayan tek bir yönetim sistemini yürütmeyi seçen kuruluşlar için faydalı olacaktır.

Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri - Gereksinimler

1 Kapsam

Bu standard kuruluşun bağlamı dâhilinde bir bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için şartları kapsar. Bu standard aynı zamanda kuruluşun ihtiyaçlarına göre düzenlenmiş bilgi güvenliği risklerinin değerlendirilmesi ve işlenmesi için şartları da içerir. Bu standardda ortaya konulan şartlar geneldir ve türleri, büyüklükleri ve doğalarından bağımsız olarak tüm kuruluşlara uygulanabilir olması hedeflenmiştir. Bir kuruluşun bu standarda uyumluluk iddiasında bulunması durumda, Madde 4 ila Madde 10 arasında belirtilen şartların herhangi birinin hariç tutulması kabul edilebilir değildir.

2 Atıf yapılan standard ve/veya dokümanlar

Bu standartta aşağıdaki dokümanlara, tamamen veya kısmen, atıf yapılmış olup, söz konusu dokümanlar bu standardın uygulanması için zorunludur. Tarihli atıflar için sadece atıf yapılan sürüm geçerlidir. Tarihsiz atıflar için, atıf yapılan dokümanın (tüm değişiklikler dâhil olmak üzere) son sürümü geçerlidir.
ISO/IEC 27000, Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri - Genel Bakış ve Terimler sözlüğü

3 Terimler ve tarifler

Bu dokümanın amaçları doğrultusunda ISO/IEC 27000 de verilen terimler ve tarifler geçerlidir.

4 Kuruluşun bağlamı

4.1 Kuruluşun ve bağlamının anlaşılması

Kuruluş, amaçları ile ilgili olan ve bilgi güvenliği yönetim sisteminin hedeflenen çıktılarını başarma kabiliyetini etkileyebilecek iç ve dış hususları belirlemelidir.

Not - Bu hususların belirlenmesi, ISO 31000:2009 [5] Madde 5.3 te ele alınan kuruluşun dış ve iç bağlamının oluşturulmasına atıf yapar.

4.2 İlgili tarafların ihtiyaç ve beklentilerinin anlaşılması

Kuruluş aşağıdakileri belirleyecektir:

a) Bilgi güvenliği yönetim sistemi ile ilgili taraflar ve
b) Bu ilgili tarafların bilgi güvenliği ile ilgili gereksinimleri.

Not - İlgili tarafların gereksinimleri yasal ve düzenleyici gereksinimleri ve sözleşmeden doğan yükümlülükleri içeriyor olabilir.

4.3 Bilgi güvenliği yönetim sisteminin kapsamının belirlenmesi

Kuruluş, kapsamını oluşturabilmek için, bilgi güvenliği yönetim sisteminin sınırlarını ve uygulanabilirliğini belirlemelidir.

Kuruluş, bu kapsamı belirlerken aşağıdakileri dikkate almalıdır:

a) Madde 4.1. de belirtilen dış ve iç hususlar,
b) Madde 4.2. de belirtilen şartlar ve
c) Kuruluş tarafından gerçekleştirilen faaliyetler arasındaki arayüzler, bağımlılıklar ve diğer kuruluşlar tarafından gerçekleştirilen faaliyetler.

Kapsam yazılı bilgi olarak mevcut olmalıdır.

4.4 Bilgi güvenliği yönetim sistemi
Kuruluş, bu standardın şartları çerçevesinde bir bilgi güvenliği yönetim sistemini kurmalı, uygulamalı, sürdürmeli ve sürekli iyileştirmelidir.

5 Liderlik

5.1 Liderlik ve bağlılık
Üst yönetim bilgi güvenliği yönetim sistemi ile ilgili olarak aşağıdakileri yerine getirerek, liderlik ve bağlılık göstermelidir:

a) Bilgi güvenliği politikası ve bilgi güvenliği amaçlarının oluşturulmasını ve kuruluşun stratejik yönü ile uyumlu olmasının temin edilmesi,
b) Bilgi güvenliği yönetim sisteminin şartlarının kuruluşun süreçleri ile bütünleştirilmesinin temin edilmesi,
c) Bilgi güvenliği yönetim sistemi için gerekli olan kaynakların erişilebilirliğinin temin edilmesi,
ç) Etkin bilgi güvenliği yönetiminin ve bilgi güvenliği yönetim sisteminin şartlarına uyum sağlamanın öneminin duyurulması,
d) Bilgi güvenliği yönetim sisteminin hedeflenen çıktılarının başarılmasının temin edilmesi,
e) Bilgi güvenliği yönetim sisteminin etkinliğine katkı sağlamaları için kişilerin yönlendirilmesi ve desteklenmesi,
f) Sürekli iyileştirmenin desteklenmesi ve
g) Kendi sorumluluk alanlarında liderliklerini sergileyebilmeleri için diğer ilgili yönetim rollerinin desteklenmesi.

5.2 Politika
Üst yönetim aşağıdakileri karşılayan bir bilgi güvenliği politikası oluşturmalıdır:

a) Kuruluşun amacına uygun,
b) Bilgi güvenliği amaçlarını içeren (Bk. Madde 6.2) veya bilgi güvenliği amaçlarını belirlemek için bir çerçeve sağlayan,
c) Bilgi güvenliği ile ilgili uygulanabilir şartların karşılanmasına dair bir taahhüt içeren ve
d) Bilgi güvenliği yönetim sisteminin sürekli iyileştirilmesi için bir taahhüt içeren bilgi güvenliği politikası,

Bilgi güvenliği politikası:

e) Yazılı bilgi olarak mevcut olmalı,
f) Kuruluş içinde duyurulmalı ve
g) Uygun olan ilgili taraflarca erişilebilir olmalıdır.

5.3 Kurumsal roller, sorumluluklar ve yetkiler
Üst yönetim, bilgi güvenliği ile ilgili olan roller için sorumluluk ve yetkilerin atanmasını ve duyurulmasını temin etmelidir.

Üst yönetim aşağıdakiler için sorumluluk ve yetki ataması yapmalıdır:

a) Bilgi güvenliği yönetim sisteminin bu standardın şartlarına uyum sağlamasını temin etmek ve
b) Üst yönetime bilgi güvenliği yönetim sisteminin performansı hakkında raporlama.

Not - Üst yönetim, kuruluş içinde bilgi güvenliği yönetim sisteminin performansının raporlanması için sorumluluklar ve yetkiler atayabilir.

6 Planlama

6.1 Risk ve fırsatları ele alan faaliyetler

6.1.1. Genel
Bilgi güvenliği yönetim sistemi planlaması yaparken, kuruluş Madde 4.1 de atıf yapılan hususları ve Madde 4.3. de atıf yapılan şartları göz önünde bulundurmalı ve aşağıdakilerin gerçekleştirilmesi için gerekli olan riskleri ve fırsatları belirlemelidir:

a) Bilgi güvenliği yönetim sisteminin amaçlanan çıktıları sağlayabilmesinin temin edilmesi,

b) İstenmeyen etkilerin önlenmesi veya azaltılması ve
c) Sürekli iyileştirmenin başarılması,

Kuruluş aşağıdakileri planlamalıdır:
d) Bu risk ve fırsatların ele alınması için faaliyetler ve
e) Aşağıdakilerin nasıl gerçekleştirileceği,
    1) Faaliyetleri, bilgi güvenliği yönetim sistemi süreçleri ile bütünleştirme ve uygulama,
    2) Faaliyetlerin etkinliğinin değerlendirilmesi.

6.1.2. Bilgi güvenliği risk değerlendirmesi

Kuruluş aşağıda belirtilen şartları yerine getiren bir bilgi güvenliği risk değerlendirmesi sürecini tanımlamalı ve uygulamalıdır:

a) Aşağıdakileri içeren bilgi güvenliği risk kriterlerinin oluşturulması ve sürdürülmesi:

    1) Risk kabul kriterleri ve
    2) Bilgi güvenliği risk değerlendirmesi yapılması için kriterler,

b) Tekrarlanan bilgi güvenliği risk değerlendirmelerinin tutarlı, geçerli ve karşılaştırılabilir sonuçlar üretmesinin temin edilmesi,

c) Bilgi güvenliği risklerinin tespit edilmesi:

    1) Bilgi güvenliği yönetim sistemi kapsamı dâhilindeki bilginin gizlilik, bütünlük ve erişilebilirlik kayıpları ile ilgili risklerin tespit edilmesi için bilgi güvenliği risk değerlendirme prosesinin uygulanması ve
    2) Risk sahiplerinin belirlenmesi,

d) Bilgi güvenliği risklerinin analiz edilmesi:

    1) Madde 6.1.2 c) 1) de belirlenen riskler gerçekleştiği takdirde muhtemel sonuçların değerlendirilmesi,
    2) Madde 6.1.2 c) 1) de belirlenen risklerin gerçekleşmesi ihtimalinin gerçekçi bir şekilde değerlendirilmesi ve
    3) Risk seviyelerinin belirlenmesi,

e) Bilgi güvenliği risklerinin değerlendirilmesi:

    1) Risk analizi sonuçlarının Madde 6.1.2 a) da oluşturulan risk kriterleri ile karşılaştırılması ve
    2) Analiz edilen risklerin risk işleme için önceliklendirilmesi.

Kuruluş bilgi güvenliği risk değerlendirme süreci ile ilgili olarak yazılı bilgileri muhafaza etmelidir.

6.1.3. Bilgi güvenliği risk işleme

Kuruluş aşağıdakileri gerçekleştirmek için bir bilgi güvenliği risk işleme süreci tanımlamalı ve uygulamalıdır:

a) Risk değerlendirme sonuçlarını dikkate alarak uygun bilgi güvenliği risk işleme seçeneklerinin seçilmesi,
b) Seçilen bilgi güvenliği risk işleme seçeneklerinin uygulanmasında gerekli olan tüm kontrollerin belirlenmesi,

Not - Kuruluşlar, gerektiğince kontroller tasarlayabilir veya herhangi bir kaynaktan belirleyebilir.

c) Yukarıdaki Madde 6.1.3b) de belirlenen kontroller ile Ek A daki kontrollerin karşılaştırılması ve gerekli hiçbir kontrolün gözden kaçırılmadığının doğrulanması,

Not 1 - Ek A geniş kapsamlı bir kontrol amaçları ve kontroller listesi içermektedir. Bu standardın kullanıcıları, hiçbir gerekli kontrolün gözden kaçırılmaması için Ek A ya yönlendirilirler.

Not 2 - Seçilen kontroller kontrol amaçlarını dolaylı olarak içermektedir. Ek A da listelenen kontrol amaçları ve kontroller eksiksiz değildir ve ilave kontrol amaçları ve kontrollere ihtiyaç duyulabilir.

d) Gerekli kontrolleri (Bk. Madde 6.1.3b) ve c)), bunların dahil edilmesinin gerekçelendirmesi, uygulanıp uygulanmadıklarını ve Ek A dan kontrollerin dışarıda bırakılmasının gerekçelendirmesini içeren bir Uygulanabilirlik Bildirgesi üretilmesi,

e) Bir bilgi güvenliği risk işleme planının formüle edilmesi ve

f) Bilgi güvenliği risk işleme planına dair risk sahiplerinin onayının alınması ve artık bilgi güvenliği risklerinin kabulü

Kuruluş, bilgi güvenliği risk işleme süreci ile ilgili yazılı bilgileri muhafaza etmelidir.

Not - Bu standarddaki bilgi güvenliği risk değerlendirme ve işleme süreci ISO 31000[5] de verilen ilkeler ve genel kılavuzlarla eşgüdümlüdür.

6.2 Bilgi güvenliği amaçları ve bu amaçları başarmak için planlama

Kuruluş, uygun işlevler ve seviyelerde bilgi güvenliği amaçlarını tesis etmelidir.

Bilgi güvenliği amaçları aşağıdakileri sağlamalıdır:

a) Bilgi güvenliği politikası ile tutarlı olmalı,
b) Ölçülebilir olmalı (uygulanabilirse),
c) Uygulanabilir bilgi güvenliği şartlarını ve risk değerlendirme ve risk işlemenin sonuçlarını dikkate almalı,
d) Duyurulmalı ve
e) Uygun şekilde güncellenmelidir.

Kuruluş bilgi güvenliği amaçları ile ilgili yazılı bilgileri muhafaza etmelidir.

Kuruluş bilgi güvenliği amaçlarını nasıl başaracağını planlarken, aşağıdakileri belirlemelidir:

f) Ne yapılacağı,
g) Hangi kaynakların gerekli olacağı,
h) Kimin sorumlu olacağı,
i) Ne zaman tamamlanacağı ve
j) Sonuçların nasıl değerlendirileceği.

7 Destek

7.1 Kaynaklar

Kuruluş bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için gerekli olan kaynakları belirlemeli ve sağlamalıdır.

7.2 Yeterlilik

Kuruluş aşağıdakileri yapmalıdır:

a) Bilgi güvenliği performansını etkileyen kendi kontrolü altında çalışan kişilerin gerekli yeterliliklerinin belirlenmesi,
b) Uygun öğretim, eğitim veya tecrübe temelinde bu kişilerin yeterliliklerinin temin edilmesi,
c) Uygun olduğu durumlarda, gerekli yeterliliğin sağlanması için girişimde bulunulması ve bu girişimlerin etkinliğinin değerlendirilmesi ve
d) Yeterliliğin delili olarak uygun yazılı bilgilerin muhafaza edilmesi.

Not - Uygulanabilir girişimler örneğin, mevcut çalışanların eğitimlerinin sağlanması, yol gösterilmesi veya görev değişikliği ya da yeterlilik sahibi kişilerin çalıştırılması veya sözleşme yapılması şeklinde olabilir.

7.3 Farkındalık

Kuruluşun kontrolü dâhilinde görev yapan kişiler aşağıdakilerin farkında olmalıdır:

a) Bilgi güvenliği politikası,
b) İyileştirilmiş bilgi güvenliği performansının faydaları da dâhil bilgi güvenliği yönetim sisteminin etkinliğine yaptıkları katkı ve
c) Bilgi güvenliği yönetim sistemi şartlarına uyum sağlamama'nın sonuçları.

7.4 İletişim

Kuruluş aşağıdakileri içeren bilgi güvenliği yönetim sistemi ile ilgili dâhili ve harici iletişim ihtiyaçlarını belirlemelidir:

a) İletişimin konusu,
b) Ne zaman iletişim kurulacağı,
c) Kiminle iletişim kurulacağı,
d) Kimin iletişim kuracağı ve
e) İletişimin hangi süreçten etkileneceği.

7.5 Yazılı bilgiler

7.5.1 Genel

Kuruluşun bilgi güvenliği yönetim sistemi aşağıdakileri içermelidir:

a) Bu standardın gerektirdiği yazılı bilgiler ve
b) Kuruluş tarafından bilgi güvenliği yönetim sisteminin etkinliği için gerekli olduğu belirlenen yazılı bilgiler.

Not - Bir bilgi güvenliği yönetim sistemi için yazılı bilgilerin boyutu aşağıdakiler temelinde bir kuruluştan diğer kuruluşa değişebilir:

1) Kuruluşun büyüklüğü ve faaliyetlerinin, süreçlerinin, ürünlerinin ve hizmetlerinin türleri,
2) Süreçlerin ve etkileşimlerinin karmaşıklığı ve
3) Kişilerin yeterliliği.

7.5.2 Oluşturma ve güncelleme

Kuruluş, yazılı bilgileri oluştururken ve güncellerken, aşağıdakileri uygun bir şekilde temin etmelidir:

a) Tanımlama ve tarif etme (örneğin, bir başlık, tarih, yazar veya referans numarası),
b) Biçim (örneğin; dil, yazılım sürümü, grafikler) ve ortam (örneğin, kâğıt, elektronik) ve
c) Uygunluğun ve doğruluğun gözden geçirilmesi ve onaylanması.

7.5.3 Yazılı bilgilerin kontrolü

Bilgi güvenliği yönetim sistemi ve bu standardın gerektirdiği yazılı bilgiler aşağıdakileri temin etmek için kontrol edilmelidir:

a) Gereken yerde ve zamanda kullanım için erişilebilir ve uygun olması ve
b) Doğru bir şekilde korunması (örneğin, gizlilik kaybından, uygun olmayan kullanımdan veya bütünlük kaybından).

Yazılı bilgilerin kontrolü için, kuruluş uygunluğuna göre aşağıdaki faaliyetleri ele almalıdır:

c) Dağıtım, erişim, getirme ve kullanım,
d) Okunaklılığın korunması da dâhil olmak üzere saklama ve koruma,
e) Değişikliklerin kontrolü (örneğin sürüm kontrolü) ve
f) Muhafaza etme ve yok etme.

Kuruluş tarafından bilgi güvenliği yönetim sisteminin planlaması ve işletimi için gerekli olduğu belirlenen dış kaynaklı yazılı bilgiler, uygun şekilde tespit edilmeli ve kontrol edilmelidir.

Not - Erişim, sadece yazılı bilgilerin görüntülenmesi konusunda bir izin kararını veya yazılı bilgileri görüntüleme ve değiştirmeye dair izin ve yetkiyi ifade eder.

8 İşletim

8.1 İşletimsel planlama ve kontrol

Kuruluş bilgi güvenliği şartlarını karşılamak ve Madde 6.1'de belirlenen faaliyetleri gerçekleştirmek için gerekli olan süreçleri planlamalı, uygulamalı ve kontrol etmelidir. Kuruluş, Madde 6.2'de belirlenen bilgi güvenliği amaçlarını başarmak için aynı zamanda planları uygulamalıdır.
Kuruluş, süreçlerin planlandığı gibi yürütüldüğünden emin olduğu noktaya kadar yazılı bilgileri saklamalıdır.

Kuruluş, planlanan değişiklikleri kontrol etmeli ve istenmeyen değişikliklerin sonuçlarını gözden geçirerek, gerekiyor ise kötü etkileri azaltmak için eyleme geçmelidir.

Kuruluş, dış kaynaklı süreçlerin belirlenmesini ve kontrol edilmesini temin etmelidir.

8.2 Bilgi güvenliği risk değerlendirme

Kuruluş, Madde 6.1.2 a) da belirtilen kriterleri de dikkate alarak, bilgi güvenliği risk değerlendirmelerini planlanan aralıklarda veya önemli değişiklikler önerildiğinde veya meydana geldiğinde gerçekleştirmelidir.

Kuruluş, bilgi güvenliği risk değerlendirmesinin sonuçlarına dair yazılı bilgileri muhafaza etmelidir.

8.3 Bilgi güvenliği risk işleme

Kuruluş, bilgi güvenliği risk işleme planını uygulamalıdır.

Kuruluş, bilgi güvenliği risk işlemesinin sonuçlarına ait yazılı bilgileri muhafaza etmelidir.

9 Performans değerlendirme

9.1 İzleme, ölçme, analiz ve değerlendirme

Kuruluş, bilgi güvenliği performansı ve bilgi güvenliği yönetim sisteminin etkinliğini değerlendirmelidir.

Kuruluş aşağıdakileri belirlemelidir:

a) Bilgi güvenliği süreçleri ve kontrolleri dâhil olmak üzere neyin izlenmesi ve ölçülmesinin gerekli olduğu,
b) Geçerli sonuçları temin etmek için, uygun İzleme, ölçme, analiz ve değerlendirme yöntemleri,

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

c) İzleme ve ölçmenin ne zaman yapılacağı,
d) İzlemeyi ve ölçmeyi kimin yapacağı,
e) İzleme ve ölçme sonuçlarının ne zaman analiz edileceği ve değerlendirileceği ve
f) Bu sonuçları kimin analiz edeceği ve değerlendireceği.

Kuruluş, izleme ve ölçme sonuçlarına dair delil olarak uygun yazılı bilgileri muhafaza etmelidir.

9.2 İç tetkik

Kuruluş, bilgi güvenliği yönetim sisteminin, aşağıdaki hususları yerine getirip getirmediği konusunda bilgi elde etmek için planlanan aralıklarda iç tetkikler gerçekleştirmelidir:

a) Aşağıdakilerle uyumlu olup olmadığı,

    1) Bilgi güvenliği yönetim sistemi ile ilgili olarak kuruluşun kendi şartları ve
    2) Bu standardın şartları,

b) Etkin bir şekilde uygulanması ve sürdürülmesi.

Kuruluş aşağıdakileri gerçekleştirmelidir:

c) Sıklık, yöntemler, sorumluluklar, gereksinimleri planlama ve raporlama da dâhil olmak üzere bir tetkik programının/programlarının planlanması, oluşturulması, uygulanması ve sürdürülmesi. Tetkik programı/programları ilgili süreçlerin önemini ve önceki tetkiklerin sonuçlarını dikkate almalıdır,
d) Her bir tetkik için tetkik kriterlerinin ve kapsamın tanımlanması,
e) Tetkik sürecinin tarafsızlığı ve objektifliğini temin edecek şekilde tetkikçilerin seçimi ve tetkiklerin yürütülmesi,
f) Tetkik sonuçlarının uygun yönetim kademesine raporlanmasının temin edilmesi ve
g) Tetkik programı/programları ve tetkik sonuçlarının delil teşkil eden yazılı bilgilerinin muhafaza edilmesi.

9.3 Yönetimin gözden geçirmesi

Üst yönetim bilgi güvenliği yönetim sisteminin sürekli uygunluğunu, doğruluğunu ve etkinliğini temin etmek için planlı aralıklarla gözden geçirmelidir.
Yönetimin gözden geçirmesi aşağıdakileri ele almalıdır:

a) Önceki yönetimin gözden geçirmelerinden gelen görevlerin durumu,
b) Bilgi güvenliği yönetim sistemini ilgilendiren dış ve iç konulardaki değişiklikler,
c) Aşağıdakiler deki gelişmeler dâhil bilgi güvenliği performansına dair geri bildirim:

1) Uygunsuzluklar ve düzeltici faaliyetler,
2) İzleme ve ölçme sonuçları,
3) Tetkik sonuçları ve
4) Bilgi güvenliği amaçlarının yerine getirilmesi,

d) İlgili taraflardan geri bildirimler,
e) Risk değerlendirme sonuçları ve risk işleme planının durumu ve
f) Sürekli iyileştirme için fırsatlar.

Yönetimin gözden geçirmesi çıktıları, sürekli iyileştirme fırsatlarına ve bilgi güvenliği yönetim sisteminde gerekli olan değişiklikler için tüm ihtiyaçlara dair kararları içermelidir.

Kuruluş, yönetimin gözden geçirmesinin sonuçlarının delili olarak yazılı bilgileri muhafaza etmelidir.

10 İyileştirme

10.1 Uygunsuzluk ve düzeltici faaliyet

Bir uygunsuzluk oluştuğunda, kuruluş aşağıdakileri yerine getirmelidir:

a) Uygunsuzluğa tepki verilmesi ve mümkün olması durumunda:
   1) Kontrol edilmesi ve düzeltmek için eyleme geçilmesi ve
   2) Sonuçları ile ilgilenilmesi,

b) Aşağıdakilerin yerine getirilmesi yoluyla, uygunsuzluğun başka bir yerde tekrar etmemesi veya oluşmaması için nedenlerinin giderilmesi amacıyla eyleme geçme ihtiyacının değerlendirilmesi:
   1) Uygunsuzluğu gözden geçirerek,
   2) Uygunsuzluğun nedenleri belirlenerek ve
   3) Benzer uygunsuzlukların var olup olmadığını veya olasılıkla gerçekleşip gerçekleşmeyeceğini belirleyerek,

c) Gerekli tüm faaliyetlerin uygulanması,
d) Tüm düzeltici faaliyetlerin etkinliğinin gözden geçirilmesi ve
e) Gerekli olan durumlarda bilgi güvenliği yönetim sisteminde değişikliklerin yapılması.

Düzeltici faaliyetler, karşılaşılan uygunsuzlukların etkilerine uygun olmalıdır.

Kuruluş aşağıdakilerin delili olarak yazılı bilgileri muhafaza etmelidir:

f) Uygunsuzlukların doğası ve gerçekleştirilen müteakip eylemler ve
g) Herhangi bir düzeltici faaliyetin sonuçları.

10.2 Sürekli iyileştirme

Kuruluş, bilgi güvenliği yönetim sisteminin uygunluğunu, doğruluğunu ve etkinliğini sürekli olarak iyileştirmelidir.

Ek A

Referans kontrol amaçları ve kontroller

Çizelge A.1 de listelenen kontrol amaçları ve kontroller, Madde 6.1.3 bağlamında kullanılmak üzere, doğrudan ISO/IEC 27002:2013 [1] madde 5'ten madde 18'e kadar listelenenlerden çıkarılmış ve sıraya konulmuştur.

Çizelge A.1 - Kontrol amaçları ve kontroller

A.5 Bilgi güvenliği politikaları		
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	*Kontrol* Bir dizi bilgi güvenliği politikaları, yönetim tarafından tanımlanmalı, onaylanmalı ve yayınlanarak çalışanlara ve ilgili dış taraflara bildirilmelidir.
A.5.1.2	Bilgi güvenliği için politikaların gözden geçirilmesi	*Kontrol* Bilgi güvenliği politikaları, belirli aralıklarla veya önemli değişiklikler ortaya çıktığında sürekli uygunluk ve etkinliği sağlamak amacıyla gözden geçirilmelidir.
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	*Kontrol* Tüm bilgi güvenliği sorumlulukları tanımlanmalı ve tahsis edilmelidir.
A.6.1.2	Görevlerin ayrılığı	*Kontrol* Çelişen görevler ve sorumluluklar, yetkilendirilmemiş veya kasıtsız değişiklik fırsatlarını veya kuruluş varlıklarının yanlış kullanımını azaltmak amacıyla ayrılmalıdır.
A.6.1.3	Otoritelerle iletişim	*Kontrol* İlgili otoritelerle uygun iletişim kurulmalıdır.
A.6.1.4	Özel ilgi grupları ile iletişim	*Kontrol* Özel ilgi grupları veya diğer uzman güvenlik forumları ve profesyonel dernekler ile uygun iletişim kurulmalıdır.
A.6.1.5	Proje yönetiminde bilgi güvenliği	*Kontrol* Proje yönetiminde, proje çeşidine bakılmaksızın bilgi güvenliği ele alınmalıdır.
A.6.2 Mobil cihazlar ve uzaktan çalışma		
Amaç: Uzaktan çalışma ve mobil cihazların güvenliğini sağlamak.		
A.6.2.1	Mobil cihaz politikası	*Kontrol* Mobil cihazların kullanımı ile ortaya çıkan risklerin yönetilmesi amacı ile bir politika ve destekleyici güvenlik önlemleri belirlenmelidir.
A.6.2.2	Uzaktan çalışma	*Kontrol* Uzaktan çalışma alanlarında erişilen, işlenen veya depolanan bilgiyi korumak amacı ile bir politika ve destekleyici güvenlik önlemleri uygulanmalıdır.

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	*Kontrol* Tüm işe alımlarda adaylar için, ilgili yasa, düzenleme ve etiğe göre ve iş gereksinimleri, erişilecek bilginin sınıflandırması ve alınan risklerle orantılı olarak geçmiş doğrulama kontrolleri gerçekleştirilmelidir.
A.7.1.2	İstihdam hüküm ve koşulları	*Kontrol* Çalışanlar ve yükleniciler ile yapılan sözleşmeler kendilerinin ve kuruluşun bilgi güvenliği sorumluluklarını belirtmelidir.
A.7.2 Çalışma esnasında		
Amaç: Çalışanların ve yüklenicilerin bilgi güvenliği sorumluluklarının farkında olmalarını ve yerine getirmelerini temin etmek.		
A.7.2.1	Yönetimin sorumlulukları	*Kontrol* Yönetim, çalışanlar ve yüklenicilerin, kuruluşun yerleşik politika ve prosedürlerine göre bilgi güvenliğini uygulamalarını istemelidir.
A.7.2.2	Bilgi güvenliği farkındalığı, eğitim ve öğretimi	*Kontrol* Kuruluştaki tüm çalışanlar ve ilgili olduğu durumda, yükleniciler, kendi iş fonksiyonları ile ilgili, kurumsal politika ve prosedürlere ilişkin uygun farkındalık eğitim ve öğretimini ve bunların düzenli güncellemelerini almalıdırlar.
A.7.2.3	Disiplin prosesi	*Kontrol* Bir bilgi güvenliği ihlal olayını gerçekleştiren çalışanlara yönelik önlem almak için resmi ve bildirilmiş bir disiplin prosesi olmalıdır.
A.7.3 İstihdamın sonlandırılması ve değiştirilmesi		
Amaç: İstihdamın sonlandırılması ve değiştirilmesi prosesinin bir parçası olarak kuruluşun çıkarlarını korumak.		
A.7.3.1	İstihdam sorumluluklarının sonlandırılması veya değiştirilmesi	*Kontrol* İstihdamın sonlandırılması veya değiştirilmesinden sonra geçerli olan bilgi güvenliği sorumlulukları ve görevleri tanımlanmalı, çalışan veya yükleniciye bildirilmeli ve yürürlüğe konulmalıdır.
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	*Kontrol* Bilgi ve bilgi işleme olanakları ile ilgili varlıklar belirlenmeli ve bu varlıkların bir envanteri çıkarılmalı ve idame ettirilmelidir.
A.8.1.2	Varlıkların sahipliği	*Kontrol* Envanterde tutulan tüm varlıklara sahip atamaları yapılmalıdır.
A.8.1.3	Varlıkların kabul edilebilir kullanımı	*Kontrol* Bilgi ve bilgi işleme tesisleri ile ilgili bilgi ve varlıkların kabul edilebilir kullanımına dair kurallar belirlenmeli, yazılı hale getirilmeli ve uygulanmalıdır.
A.8.1.4	Varlıkların iadesi	*Kontrol* Tüm çalışanlar ve dış tarafların kullanıcıları, istihdamlarının, sözleşme veya anlaşmalarının sonlandırılmasının ardından ellerinde olan tüm kurumsal varlıkları iade etmelidirler.

A.8.2 Bilgi sınıflandırma		
Amaç: Bilginin kurum için önemi derecesinde uygun seviyede korunmasını temin etmek.		
A.8.2.1	Bilgi sınıflandırması	*Kontrol* Bilgi, yasal şartlar, değeri, kritikliği ve yetkisiz ifşa veya değiştirilmeye karşı hassasiyetine göre sınıflandırılmalıdır.
A.8.2.2	Bilgi etiketlemesi	*Kontrol* Bilgi etiketleme için uygun bir prosedür kümesi kuruluş tarafından benimsenen sınıflandırma düzenine göre geliştirilmeli ve uygulanmalıdır.
A.8.2.3	Varlıkların kullanımı	*Kontrol* Varlıkların kullanımı için prosedürler, kuruluş tarafından benimsenen sınıflandırma düzenine göre geliştirilmeli ve uygulanmalıdır.
8.3 Ortam işleme		
Amaç: Ortamda depolanan bilginin yetkisiz ifşası, değiştirilmesi, kaldırılması ve yok edilmesini engellemek.		
8.3.1	Taşınabilir ortam yönetimi	*Kontrol* Taşınabilir ortam yönetimi için prosedürler kuruluş tarafından benimsenen sınıflandırma düzenine göre uygulanmalıdır.
8.3.2	Ortamın yok edilmesi	*Kontrol* Ortam artık ihtiyaç kalmadığında resmi prosedürler kullanılarak güvenli bir şekilde yok edilmelidir.
8.3.3	Fiziksel ortam aktarımı	*Kontrol* Bilgi içeren ortam, aktarım sırasında yetkisiz erişim, kötüye kullanım ve bozulmaya karşı korunmalıdır.
A.9 Erişim kontrolü		
A.9.1 Erişim kontrolünün iş gereklilikleri		
Amaç: Bilgi ve bilgi işleme olanaklarına erişimi kısıtlamak		
A.9.1.1	Erişim kontrol politikası	*Kontrol* Bir erişim kontrol politikası, iş ve bilgi güvenliği şartları temelinde oluşturulmalı, yazılı hale getirilmeli ve gözden geçirilmelidir.
A.9.1.2	Ağlara ve ağ hizmetlerine erişim	Kullanıcılara sadece özellikle kullanımı için yetkilendirildikleri ağ ve ağ hizmetlerine erişim verilmelidir.
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	*Kontrol* Erişim haklarının atanmasını sağlamak için, resmi bir kullanıcı kaydetme ve kayıt silme prosesi uygulanmalıdır.
A.9.2.2	Kullanıcı erişimine izin verme	*Kontrol* Tüm kullanıcı türlerine tüm sistemler ve hizmetlere erişim haklarının atanması veya iptal edilmesi için resmi bir kullanıcı erişim izin prosesi uygulanmalıdır.
A.9.2.3	Ayrıcalıklı erişim haklarının yönetimi	*Kontrol* Ayrıcalıklı erişim haklarının tahsis edilmesi ve kullanımı kısıtlanmalı ve kontrol edilmelidir.
A.9.2.4	Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi	*Kontrol* Gizli kimlik doğrulama bilgisinin tahsis edilmesi, resmi bir yönetim prosesi yoluyla kontrol edilmelidir.

A.9.2.5	Kullanıcı erişim haklarının gözden geçirilmesi	*Kontrol* Varlık sahipleri kullanıcıların erişim haklarını düzenli aralıklarla gözden geçirmelidir.
A.9.2.6	Erişim haklarının kaldırılması veya düzenlenmesi	*Kontrol* Tüm çalışanların ve dış taraf kullanıcılarının bilgi ve bilgi işleme olanaklarına erişim yetkileri, istihdamları, sözleşmeleri veya anlaşmaları sona erdirildiğinde kaldırılmalı veya bunlardaki değişiklik üzerine düzenlenmelidir.
A.9.3 Kullanıcı sorumlulukları		
Amaç: Kullanıcıları kendi kimlik doğrulama bilgilerinin korunması konusunda sorumlu tutmak		
A.9.3.1	Gizli kimlik doğrulama bilgisinin kullanımı	*Kontrol* Kullanıcıların, gizli kimlik doğrulama bilgisinin kullanımında kurumsal uygulamalara uymaları şart koşulmalıdır.
A.9.4 Sistem ve uygulama erişim kontrolü		
Amaç: Sistem ve uygulamalara yetkisiz erişimi engellemek		
A.9.4.1	Bilgiye erişimin kısıtlanması	*Kontrol* Bilgi ve uygulama sistem fonksiyonlarına erişim, erişim kontrol politikası doğrultusunda kısıtlanmalıdır.
A.9.4.2	Güvenli oturum açma prosedürleri	*Kontrol* Erişim kontrol politikası tarafından şart koşulduğu yerlerde, sistem ve uygulamalara erişim güvenli bir oturum açma prosedürü tarafından kontrol edilmelidir.
A.9.4.3	Parola yönetim sistemi	*Kontrol* Parola yönetim sistemleri etkileşimli olmalı ve yeterli güvenlik seviyesine sahip parolaları temin etmelidir.
A.9.4.4	Ayrıcalıklı destek programlarının kullanımı	*Kontrol* Sistem ve uygulamaların kontrollerini geçersiz kılma kabiliyetine sahip olabilen destek programlarının kullanımı kısıtlanmalı ve sıkı bir şekilde kontrol edilmelidir.
A.9.4.5	Program kaynak koduna erişim kontrolü	*Kontrol* Program kaynak koduna erişim kısıtlanmalıdır.
A.10 Kriptografi		
A.10.1 Kriptografik kontroller		
Amaç: Bilginin gizliliği, aslına uygunluğu ve/veya bütünlüğü ’nün korunması için kriptografi’nin doğru ve etkin kullanımın temin etmek		
A.10.1.1	Kriptografik kontrollerin kullanımına ilişkin politika	*Kontrol* Bilginin korunması için kriptografik kontrollerin kullanımına dair bir politika geliştirilmeli ve uygulanmalıdır.
A.10.1.2	Anahtar yönetimi	*Kontrol* Kriptografik anahtarların kullanımı, korunması ve yaşam süresine dair bir politika geliştirilmeli ve tüm yaşam çevirimleri süresince uygulanmalıdır.

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 sınırı	*Kontrol* Hassas veya kritik bilgi ve bilgi işleme olanakları barındıran alanları korumak için güvenlik sınırları tanımlanmalı ve kullanılmalıdır.
A.11.1.2	Fiziksel giriş kontrolleri	*Kontrol* Güvenli alanlar sadece yetkili personele erişim izni verilmesini temin etmek için uygun giriş kontrolleri ile korunmalıdır.
A.11.1.3	Ofislerin, odaların ve tesislerin güvenliğinin sağlanması	*Kontrol* Ofisler, odalar ve tesisler için fiziksel güvenlik tasarlanmalı ve uygulanmalıdır.
A.11.1.4	Dış ve çevresel tehditlere karşı koruma	*Kontrol* Doğal felaketler, kötü niyetli saldırılar veya kazalara karşı fiziksel koruma tasarlanmalı ve uygulanmalıdır.
A.11.1.5	Güvenli alanlarda çalışma	*Kontrol* Güvenli alanlarda çalışma için prosedürler tasarlanmalı ve uygulanmalıdır.
A.11.1.6	Teslimat ve yükleme alanları	*Kontrol* 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 olanaklarından ayrılmalıdır.
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	*Kontrol* Teçhizat, çevresel tehditlerden ve tehlikelerden ve yetkisiz erişim fırsatlarından kaynaklanan riskleri azaltacak şekilde yerleştirilmeli ve korunmalıdır.
A.11.2.2	Destekleyici altyapı hizmetleri	*Kontrol* Teçhizat destekleyici altyapı hizmetlerindeki hatalardan kaynaklanan enerji kesintileri ve diğer kesintilerden korunmalıdır.
A.11.2.3	Kablo güvenliği	*Kontrol* Veri veya destekleyici bilgi hizmetlerini taşıyan enerji ve telekomünikasyon kabloları, dinleme, girişim oluşturma veya hasara karşı korunmalıdır.
A.11.2.4	Teçhizat bakımı	*Kontrol* Teçhizatın bakımı, sürekli erişilebilirliğini ve bütünlüğünü temin etmek için doğru şekilde yapılmalıdır.
A.11.2.5	Varlıkların taşınması	*Kontrol* Teçhizat, bilgi veya yazılım ön yetkilendirme olmaksızın kuruluş dışına çıkarılmamalıdır.

A.11.2.6	Kuruluş dışındaki teçhizat ve varlıkların güvenliği	*Kontrol* Kuruluş dışındaki varlıklara, kuruluş yerleşkesi dışında çalışmanın farklı riskleri de göz önünde bulundurularak güvenlik uygulanmalıdır.
A.11.2.7	Teçhizatın güvenli yok edilmesi veya tekrar kullanımı	*Kontrol* 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.
A.11.2.8	Gözetimsiz kullanıcı teçhizatı	*Kontrol* Kullanıcılar, gözetimsiz teçhizatın uygun şekilde korunmasını temin etmelidir.
A.11.2.9	Temiz masa temiz ekran politikası	*Kontrol* Kâğıtlar ve taşınabilir depolama ortamları için bir temiz masa politikası ve bilgi işleme olanakları için bir temiz ekran politikası benimsenmelidir.
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	*Kontrol* İşletim prosedürleri yazılı hale getirilmeli ve ihtiyacı olan tüm kullanıcılara sağlanmalıdır.
A.12.1.2	Değişiklik yönetimi	*Kontrol* Bilgi güvenliğini etkileyen, kuruluş, iş prosesleri, bilgi işleme olanakları ve sistemlerdeki değişiklikler kontrol edilmelidir.
A.12.1.3	Kapasite yönetimi	*Kontrol* Kaynakların kullanımı izlenmeli, ayarlanmalı ve gerekli sistem performansını temin etmek için gelecekteki kapasite gereksinimleri ile ilgili kestirimler yapılmalıdır.
A.12.1.4	Geliştirme, test ve işletim ortamların birbirinden ayrılması	*Kontrol* Geliştirme, test ve işletim ortamlar, yetkisiz erişim veya işletim ortamlarında değişiklik risklerinin azaltılması için birbirinden ayrılmalıdır.
A.12.2 Kötücül yazılımlardan koruma		
Amaç: Bilgi ve bilgi işleme olanaklarının kötücül yazılımlardan korunmasını temin etmek.		
A.12.2.1	Kötücül yazılımlara karşı kontroller	*Kontrol* Kötücül yazılımlardan korunmak için tespit etme, engelleme ve kurtarma kontrolleri uygun kullanıcı farkındalığı ile birlikte uygulanmalıdır.
A.12.3 Yedekleme		
Amaç: Veri kaybına karşı koruma sağlamak		
A.12.3.1	Bilgi yedekleme	*Kontrol* Bilgi, yazılım ve sistem imajlarının yedekleme kopyaları alınmalı ve üzerinde anlaşılmış bir yedekleme politikası doğrultusunda düzenli olarak test edilmelidir.
A.12.4 Kaydetme ve izleme		
Amaç: Olayları kaydetme ve kanıt üretmek		

A.12.4.1	Olay kaydetme	*Kontrol* Kullanıcı işlemleri, kural dışılıklar, hatalar ve bilgi güvenliği olaylarını kaydeden olay kayıtları üretilmeli, saklanmalı ve düzenli olarak gözden geçirilmelidir.
A.12.4.2	Kayıt bilgisinin korunması	*Kontrol* Kaydetme olanakları ve kayıt bilgileri kurcalama ve yetkisiz erişime karşı korunmalıdır.
A.12.4.3	Yönetici ve operatör kayıtları	*Kontrol* Sistem yöneticileri ve sistem operatörlerinin işlemleri kayıt altına alınmalı, kayıtlar korunmalı ve düzenli olarak gözden geçirilmelidir.
A.12.4.4	Saat senkronizasyonu	*Kontrol* Bir kuruluş veya güvenlik alanında yer alan tüm ilgili bilgi işleme sistemlerinin saatleri tek bir referans zaman kaynağına göre senkronize edilmelidir.
A.12.5 İşletimsel yazılımının kontrolü		
Amaç: İşletimsel sistemlerin bütünlüğünü temin etmek		
A.12.5.1	İşletimsel sistemler üzerine yazılım kurulumu	*Kontrol* İşletimsel sistemler üzerine yazılım kurulumunun kontrolü için prosedürler uygulanmalıdır.
A.12.6 Teknik açıklık yönetimi		
Amaç: Teknik açıklıkların kullanılmasını engellemek		
A.12.6.1	Teknik açıklıkların yönetimi	*Kontrol* 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.
A.12.6.2	Yazılım kurulumu kısıtlamaları	*Kontrol* Kullanıcılar tarafından yazılım kurulumuna dair kurallar oluşturulmalı ve uygulanmalıdır.
A.12.7 Bilgi sistemleri tetkik hususları		
Amaç: Tetkik faaliyetlerinin işletimsel sistemler üzerindeki etkilerini asgariye indirmek.		
A.12.7.1	Bilgi sistemleri tetkik kontrolleri	*Kontrol* İşletimsel sistemlerin doğrulanmasını kapsayan tetkik gereksinimleri ve faaliyetleri, iş proseslerindeki kesintileri asgariye indirmek için dikkatlice planlanmalı ve üzerinde anlaşılmalıdır.
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	*Kontrol* Sistemlerdeki ve uygulamalardaki bilgiyi korumak amacıyla ağlar yönetilmeli ve kontrol edilmelidir.
A.13.1.2	Ağ hizmetlerinin güvenliği	*Kontrol* 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.

A.13.1.3	Ağlarda ayrım	*Kontrol* Ağlarda, bilgi hizmetleri, kullanıcıları ve bilgi sistemleri grupları ayrılmalıdır.
A.13.2 Bilgi transferi		
Amaç: Bir kuruluş içerisinde ve herhangi bir dış varlık arasında transfer edilen bilginin güvenliğini sağlamak.		
A.13.2.1	Bilgi transfer politikaları ve prosedürleri	*Kontrol* Tüm iletişim olanağı türlerinin kullanımıyla bilgi transferini korumak için resmi transfer politikaları, prosedürleri ve kontrolleri mevcut olmalıdır.
A.13.2.2	Bilgi transferindeki anlaşmalar	*Kontrol* Anlaşmalar, kuruluş ve dış taraflar arasındaki iş bilgileri'nin güvenli transferini ele almalıdır.
A.13.2.3	Elektronik mesajlaşma	*Kontrol* Elektronik mesajlaşmadaki bilgi uygun şekilde korunmalıdır.
A.13.2.4	Gizlilik ya da ifşa etmeme anlaşmaları	*Kontrol* Bilginin korunması için kuruluşun ihtiyaçlarını yansıtan gizlilik ya da ifşa etmeme anlaşmalarının gereksinimleri tanımlanmalı, düzenli olarak gözden geçirilmeli ve yazılı hale getirilmelidir.
A.14 Sistem temini, geliştirme ve bakımı		
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.		
A.14.1.1	Bilgi güvenliği gereksinimleri analizi ve belirtimi	*Kontrol* Bilgi güvenliği ile ilgili gereksinimler, yeni bilgi sistemleri gereksinimlerine veya var olan bilgi sistemlerinin iyileştirmelerine dâhil edilmelidir.
A.14.1.2	Halka açık ağlardaki uygulama hizmetlerinin güvenliğinin sağlanması	*Kontrol* Halka açık ağlar üzerinden geçen uygulama hizmetlerindeki bilgi, hileli faaliyetlerden, sözleşme ihtilafından ve yetkisiz ifşadan ve değiştirmeden korunmalıdır.
A.14.1.3	Uygulama hizmet işlemlerinin korunması	*Kontrol* Uygulama hizmet işlemlerindeki bilgi eksik iletim, yanlış yönlendirme, yetkisiz mesaj değiştirme, yetkisiz ifşayı, yetkisiz mesaj çoğaltma ya da mesajı yeniden oluşturmayı önlemek için korunmalıdır.
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	*Kontrol* Yazılım ve sistemlerin geliştirme kuralları belirlenmeli ve kuruluş içerisindeki geliştirmelere uygulanmalıdır.
A.14.2.2	Sistem değişiklik kontrolü prosedürleri	*Kontrol* Geliştirme yaşam döngüsü içerisindeki sistem değişiklikleri resmi değişiklik kontrol prosedürlerinin kullanımı ile kontrol edilmelidir.
A.14.2.3	İşletim platformu değişikliklerden sonra uygulamaların teknik gözden geçirmesi	*Kontrol* İşletim platformları değiştirildiğinde, kurumsal işlemlere ya da güvenliğe hiçbir kötü etkisi olmamasını sağlamak amacıyla iş için kritik uygulamalar gözden geçirilmeli ve test edilmelidir.

A.14.2.4	Yazılım paketlerindeki değişikliklerdeki kısıtlamalar	*Kontrol* Yazılım paketlerine yapılacak değişiklikler, gerek duyulanlar hariç önlenmeli ve tüm değişiklikler sıkı bir biçimde kontrol edilmelidir.
A.14.2.5	Güvenli sistem mühendisliği prensipleri	*Kontrol* Güvenli sistem mühendisliği prensipleri belirlenmeli, yazılı hale getirilmeli ve tüm bilgi sistemi uygulama çalışmalarına uygulanmalıdır.
A.14.2.6	Güvenli geliştirme ortamı	*Kontrol* Kuruluşlar tüm sistem geliştirme yaşam döngüsünü kapsayan sistem geliştirme ve bütünleştirme girişimleri için güvenli geliştirme ortamları kurmalı ve uygun bir şekilde korumalıdır.
A.14.2.7	Dışarıdan sağlanan geliştirme	*Kontrol* Kuruluş dışarıdan sağlanan sistem geliştirme faaliyetini denetlemeli ve izlemelidir.
A.14.2.8	Sistem güvenlik testi	*Kontrol* Güvenlik işlevselliğinin test edilmesi, geliştirme süresince gerçekleştirilmelidir.
A.14.2.9	Sistem kabul testi	*Kontrol* Kabul test programları ve ilgili kriterler, yeni bilgi sistemleri, yükseltmeleri ve yeni versiyonları için belirlenmelidir.
A.14.3 Test verisi		
Amaç: Test için kullanılan verinin korunmasını sağlamak.		
A.14.3.1	Test verisinin korunması	*Kontrol* Test verisi dikkatli bir şekilde seçilmeli, korunmalı ve kontrol edilmelidir.
A.15 Tedarikçi ilişkileri		
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	*Kontrol* Tedarikçinin kuruluşun varlıklarına erişimi ile ilgili riskleri azaltmak için bilgi güvenliği gereksinimleri tedarikçi ile kararlaştırılmalı ve yazılı hale getirilmelidir.
A.15.1.2	Tedarikçi anlaşmalarında güvenliği ifade etme	*Kontrol* 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.
A.15.1.3	Bilgi ve iletişim teknolojileri tedarik zinciri	*Kontrol* Tedarikçiler ile yapılan anlaşmalar, bilgi ve iletişim teknolojileri hizmetleri ve ürün tedarik zinciri ile ilgili bilgi güvenliği risklerini ifade eden şartları içermelidir.
A.15.2 Tedarikçi hizmet sağlama yönetimi		
Amaç: Tedarikçi anlaşmalarıyla uyumlu olarak kararlaştırılan seviyede bir bilgi güvenliğini ve hizmet sunumunu sürdürmek.		
A.15.2.1	Tedarikçi hizmetlerini izleme ve gözden geçirme	*Kontrol* Kuruluşlar düzenli aralıklarla tedarikçi hizmet sunumunu izlemeli, gözden geçirmeli ve tetkik etmelidir.

A.15.2.2	Tedarikçi hizmetlerindeki değişiklikleri yönetme	*Kontrol* 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.
A.16 Bilgi güvenliği ihlal 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	*Kontrol* Bilgi güvenliği ihlal olaylarına hızlı, etkili ve düzenli bir yanıt verilmesini sağlamak için yönetim sorumlulukları ve prosedürleri oluşturulmalıdır.
A.16.1.2	Bilgi güvenliği olaylarının raporlanması	*Kontrol* Bilgi güvenliği olayları uygun yönetim kanalları aracılığı ile olabildiğince hızlı bir şekilde raporlanmalıdır.
A.16.1.3	Bilgi güvenliği açıklıklarının raporlanması	*Kontrol* 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.
A.16.1.4	Bilgi güvenliği olaylarında değerlendirme ve karar verme	*Kontrol* Bilgi güvenliği olayları değerlendirilmeli ve bilgi güvenliği ihlal olayı olarak sınıflandırılıp sınıflandırılmayacağına karar verilmelidir.
A.16.1.5	Bilgi güvenliği ihlal olaylarına yanıt verme	*Kontrol* Bilgi güvenliği ihlal olaylarına, yazılı prosedürlere uygun olarak yanıt verilmelidir.
A.16.1.6	Bilgi güvenliği ihlal olaylarından ders çıkarma	*Kontrol* Bilgi güvenliği ihlal olaylarının analizi ve çözümlemesinden kazanılan tecrübe gelecekteki ihlal olaylarının gerçekleşme olasılığını veya etkilerini azaltmak için kullanılmalıdır.
A.16.1.7	Kanıt toplama	*Kontrol* Kuruluş kanıt olarak kullanılabilecek bilginin teşhisi, toplanması, edinimi ve korunması için prosedürler tanımlamalı ve uygulamalıdır.
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	*Kontrol* Kuruluş olumsuz durumlarda, örneğin bir kriz ve felaket boyunca, bilgi güvenliği ve bilgi güvenliği yönetimi sürekliliğinin gereksinimlerini belirlemelidir.
A.17.1.2	Bilgi güvenliği sürekliliğinin uygulanması	*Kontrol* Kuruluş, olumsuz bir olay süresince bilgi güvenliği için istenen düzeyde sürekliliğin sağlanması için prosesleri, prosedürleri ve kontrolleri kurmalı, yazılı hale getirmeli, uygulamalı ve sürdürmelidir.

A.17.1.3	Bilgi güvenliği sürekliliği'nin doğrulanması, gözden geçirilmesi ve değerlendirilmesi	*Kontrol* Kuruluş, oluşturulan ve uygulanan bilgi güvenliği sürekliliği kontrollerinin, olumsuz olaylar süresince geçerli ve etkili olduğundan emin olmak için belirli aralıklarda doğruluğunu sağlamalıdır.
A.17.2 Yedek fazlalıklar		
Amaç: Bilgi işleme olanaklarının erişilebilirliğini temin etmek.		
A.17.2.1	Bilgi işleme olanaklarının erişilebilirliği	*Kontrol* Bilgi işleme olanakları, erişilebilirlik gereksinimlerini karşılamak için yeterli fazlalık ile gerçekleştirilmelidir.
A.18 Uyum		
A.18.1 Yasal 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	*Kontrol* 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.
A.18.1.2	Fikri mülkiyet hakları	*Kontrol* Fikri mülkiyet hakları ve patentli yazılım ürünlerinin kullanımı üzerindeki yasal, düzenleyici ve anlaşmalardan doğan şartlara uyum sağlamak için uygun prosedürler gerçekleştirilmelidir.
A.18.1.3	Kayıtların korunması	*Kontrol* Kayıtlar kaybedilmeye, yok edilmeye, sahteciliğe, yetkisiz erişime ve yetkisiz yayımlamaya karşı yasal, düzenleyici, sözleşmeden doğan şartlar ve iş şartlarına uygun olarak korunmalıdır.
A.18.1.4	Kişi tespit bilgisinin gizliliği ve korunması	*Kontrol* Kişiyi tespit bilgisinin gizliliği ve korunması uygulanabilen yerlerde ilgili yasa ve düzenlemeler ile sağlanmalıdır.
A.18.1.5	Kriptografik kontrollerin düzenlemesi	*Kontrol* Kriptografik kontroller tüm ilgili sözleşmeler, yasa ve düzenlemelere uyumlu bir şekilde kullanılmalıdır.
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	*Kontrol* 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.18.2.2	Güvenlik politikaları ve standartları ile uyum	*Kontrol* Yöneticiler kendi sorumluluk alanlarında bulunan, bilgi işleme ve prosedürlerin, uygun güvenlik politikaları, standartları ve diğer güvenlik gereksinimleri ile uyumunu düzenli bir şekilde gözden geçirmelidir.
A.18.2.3	Teknik uyum gözden geçirmesi	*Kontrol* Kuruluşun bilgi güvenliği politika ve standartları ile uyumu için bilgi sistemleri düzenli bir şekilde gözden geçirilmelidir.

KAYNAKÇA

[1] ISO/IEC 27002:2013, Information technology — Security Techniques — Code of practice for information security controls
[2] ISO/IEC 27003, Information technology — Security techniques — Information security management system implementation guidance
[3] ISO/IEC 27004, Information technology — Security techniques — Information security management — Measurement
[4] ISO/IEC 27005, Information technology — Security techniques — Information security risk management
[5] ISO 31000:2009, Risk management — Principles and guidelines
[6] ISO/IEC Directives, Part 1, Consolidated ISO Supplement – Procedures specific to ISO, 2012