

BGYS KURULUMU NASIL ÖĞRETİLİR

Askerlik, denetçilik meslekleri sınıfı öğretilebilir mi?

BGYS kurulumundaki zorluklar:

- Kıdemli personelini yetiştirmek
- Maddi/Manevi destek
- BGYS'yi ilk defa kuracaklar için zorluklar ve anlaşılmayan noktaların daha fazla olması



BGYS KURULUMU NASIL ÖĞRETİLİR

Askerlik, denetçilik meslekleri sınıfıta öğretilebilir mi?

BGYS kurulumunun püf noktaları:

- Bu tür durumlarda deneyim en az teorik bilgi kadar önemlidir.
- Bu tür durumlarda mükemmel iyinin düşmanıdır.
- Bu operasyonlarda yeterince deneyimli usta personel her zaman bulundurulmalıdır.



02:07 / 13:39

BGYS KURULUMU NASIL ÖĞRETİLİR

Askerlik, denetçilik meslekleri sınıfıda öğretilebilir mi?

BGYS kurulumundaki zorluklar:

- Kıdemli personelini yetiştirmek
- Maddi/Manevi destek
- BGYS'yi ilk defa kuracaklar için zorluklar ve anlaşılmayan noktaların daha fazla olması



BGYS TEMEL KAVRAMLAR

Gereksinimlerin Bilgi Güvenliği Hedef Terimleriyle Karşılıkları

- Müşterilerin/bireylerin mahrem bilgilerini korumalıyız
- Bilgi sistemleri üzerindeki verilerle oynanarak suistimal yapılmasını engellemeliyiz
- Hizmet kesintilerimizi yıllık 8 saatin altında tutmalıyız
- Bilgi sistemlerimizde tutulan kayıtların yasal geçerliliğini güvence altına almalıyız



BGYS TEMEL KAVRAMLAR

Bilgi Güvenliği Hedeflerini Destekleyici Kontroller (örnekler)

Gizlilik:

- Fiziksel, ağ ve uygulama erişim kontrolleri
- Kamera ve iz kayıtları
- Erişim onay ve gözden geçirme süreçleri

Bütünlük:

- Veriye doğrudan erişimin engellenmesi
- Sistem ve uygulama erişimlerinde görevler ayrılığının uygulanması
- Altyapı erişimlerinin izlenmesi

Erişilebilirlik:

- Kapasite ve performans izleme ve planlama
- Altyapı yatırımları, FKM yatırımı
- Anti DDOS çözümleri

İnkar Edilemezlik / Güçlü Kullanıcı Doğrulama:

- Zaman damgası ve sayısal imza ile kayıt saklama
- İki faktörlü kullanıcı doğrulama
- İşlem bazında ikinci faktör ile kullanıcı ve işlem doğrulama

NEDEN BGYS

BGYS'nın varoluş nedeni

- İş, yasal ve kontraktsal gereksinimlerimiz nelerdir?
- Bu gereksinimleri yerine getirebilmek için ulaşmamız gereken bilgi güvenliği hedeflerimiz neler olmalıdır?
- Bu bilgi güvenliği hedeflerine ulaşabilmek için neleri yapmalıyız, yapmamız gerekenlerin öncelikleri nelerdir, bunlardan ne kadarını ve hangi etkinlikte yapabiliyoruz?
- Geliştirme ve düzeltme faaliyetlerimizin durumları nedir?



DİĞER TEMEL KAVRAMLAR

BGYS'nin kavramları

- Bilgi Güvenliği / Bilişim Güvenliği
- Veri Güvenliği / Kişisel Verilerin Korunması
- Varlık / Tehdit / Açıklık / Kontrol
- Kontrol Türleri
 - Önleyici X Düzeltici X Tespit Edici, Caydırıcı, Somut X Yumuşak, Fiziksel X Teknik X İnsani
- Denetim ve Kontrol Güvencesi Kavramları
- Düzenlemeler ve ISO27001 Standardı İlişkisi
- Varlık Sahibi, Kontrol Sahibi ve Risk Sahibi Kavramları

DİĞER TEMEL KAVRAMLAR

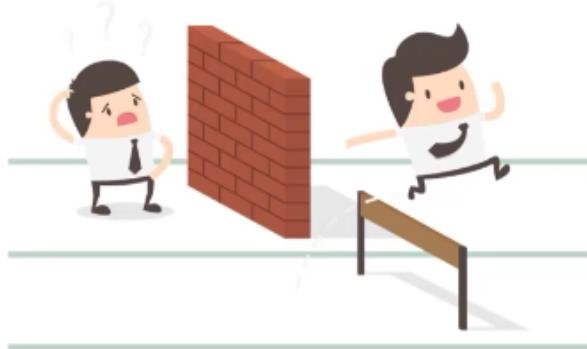
BGYS'nın kavramları

- Bilgi Güvenliği / Bilişim Güvenliği
- Veri Güvenliği / Kişisel Verilerin Korunması
- Varlık / Tehdit / Açıklık / Kontrol
- Kontrol Türleri
 - Önleyici X Düzeltici X Tespit Edici, Caydırıcı, Somut X Yumuşak, Fiziksel X Teknik X İnsani
- Denetim ve Kontrol Güvencesi Kavramları
- Düzenlemeler ve ISO27001 Standardı İlişkisi
- Varlık Sahibi, Kontrol Sahibi ve Risk Sahibi Kavramları
- ISO27001 ve ISO27002 Standartları Arasındaki İlişki
- Diğer Çerçeve ve Standartlar ile ISO27001 Standardı İlişkisi

ISO27001 STANDART DOKÜMANININ ZORLUKLARI

BGYS'nin kavramları

- Belli aktiviteleri belirtir ama belli bir akış tanımlamaz
- İstenen aktivitelerle ilgili detaylı bir yönlendirme yapmaz
- Aktiviteleri detaylı tanımlamadığı için görev ve sorumluluklara ilişkin kapsamlı bir içerik de barındırmaz
- Ek-A'da belirtilen bilgi güvenliği kontrollerinin anlaşılması ve somutlaştırılabilmesi için hatırlı sayılır bir denetim ve kontrol deneyim ve yetkinliği gerekmeli
- Bu belirsizlikler nedeniyle izleyeceğiniz uzun yolda karanlıkta kalmış hissi uyandırması



ISO27001 DENETİMLERİNİN ZORLUKLARI

Denetim

- Denetimin bilgi güvenliğinin özünden ziyade kavramsal konulara odaklanması
- Denetçilerin bilişim güvenliği konusunda yetersiz olabilmesi
- Belgelendirme kuruluşlarının ticari baskılar ve yetersiz denetim nedeniyle etik sınırlara riayet etmemeleri



ISO27001 STANDARDINA NASIL UYULUR

Standart

ISO27001 standardının gereksinimlerini tekrar edilebilir süreçler halinde tasarlama^{HAZ} ve somutlaştmak gerekmektedir.

Bu hedefi desteklemek için:

- Bu tür projelerde daha önce bulunmuş, belgelendirme deneyimine sahip olan proje ekip üyeleri
- Benzer projelerde kullanılmış süreç tanımları, yöntemler, şablonlar projenin hızını artırabilir.
- Ancak kurum yönetimi ve ilgili personelin ISO27001 BGYS'nin faydasına inanmaması veya bu konuda hiç bir fikri bulunmaması bu sürecin bir zulüm haline gelmesine neden olacaktır.
- Böyle bir durumda en iyi danışmanları da çalıştırırsanız hedeflere ulaşmak mümkün olmayacağından emin olun.

ISO27001 UYGULAMA PROJESİİNİN KAPSAMI NEDİR

ISO27001 Proje Kapsamı

- ISO27001 uygulama projesi bir BGYS kurulum projesidir.
- Bilgi güvenliği kontrol ihtiyaçları sürekli ve bazı kontrollerin geliştirilmesi ve uygulanması uzun zamana yayılabilir.
- Bu yüzden ISO27001 uygulama projesi bir kurumun tüm kontrol ihtiyaçlarının karşılanması hedefini içermez.
- ISO27001'in yeri operasyondan ziyade yönetim katmanındadır.



YÖNETİŞİM KAVRAMI VE BİLGİ GÜVENLİĞİNİN ÜVEY EVLAT OLMASI

Yönetişim ve Yönetim Nedir?

Yönetişim kavramı Amerikalılar tarafından geliştirilmiştir, ama size kendi tanımlamamızı paylaşmak istiyoruz:

Yönetişim

- yön verme ve denetlemekle ilgilidir. Yani organizasyonun sağlıklı kalması ve varolmaya devam edebilmesini hedefler.

Yönetim

- yüksek kar ve fayda üretmekle ilgilidir. Yani bir süre için parlak sonuçlar üretebilir ama organizasyonun sağlık ve sürekliliğini tehlikeye atma potansiyelini içinde taşıır.

YÖNETİŞİM KAVRAMI VE BİLGİ GÜVENLİĞİNİN ÜVEY EVLAT OLMASI

Yönetişim Nedir? (DEVAM)

- Yönetişim, ne kadar sevilmese de var olmaya devam edebilmek, karlılığı düşürebilecek ancak organizasyonun tehditlere karşı ayakta kalabilmesi için gerekli adımların atılabilmesi ve yatırımların yapılabilmesi için yönetim mekanizmasına ihtiyaç vardır.
- ISO27001'in bilgi güvenliğindeki yeri yönetim katmanındadır. Bu yüzden kimilerine göre kağıt işi olarak değeri azaltılmaya çalışılmaktadır.
- Karlılığı artırıcı ofansif faaliyetlerin gölgesinde kalan, engelleyici ve hatta bazen gereksiz gibi görülen bilgi güvenliği operasyonu ve yönetiminin üvey evlat olması fazlaıyla açıklamaktadır.



11:23 / 13:39



DÜZENLEMELER AÇISINDAN ISO27001 STANDARDI

Regülasyon açısından



BİLGİ
TEKNOLOJİLERİ
VE İLETİŞİM
KURUMU



BANKACILIK
DÜZENLEME VE DENETLEME
KURUMU



T.C.
Ulaştırma Denizcilik ve
Haberleşme Bakanlığı



DÜZENLEMELER AÇISINDAN ISO27001 STANDARDI

Regülasyon açısından (DEVAM)



KİŞİSEL VERİLERİ KORUMA KURUMU

KİŞİSEL VERİ GÜVENLİĞİ REHBERİ (Teknik ve İdari Tedbirler)

DÜZENLEMELER AÇISINDAN ISO27001 STANDARDI

Regülasyon açısından (DEVAM)

4.1. Teknik Tedbirler Özeti Tablosu

Tablo 4.1'de veri sorumlular tarafından alınabilecek teknik tedbirler gösterilmiştir.

Teknik Tedbirler
Yetki Matrisi
Yetki Kontrol
Erişim Logları
Kullanıcı Hesap Yönetimi
Ağ Güvenliği
Uygulama Güvenliği
Şifreleme
Sızma Testi
Saldırı Tespit ve Önleme Sistemleri
Log Kayıtları
Veri Maskeleme
Veri Kaybı Önleme Yazılımları
Yedekleme
Güvenlik Duvarları
Güncel Anti-Virüs Sistemleri
Silme, Yok Etme veya Anonim Hale Getirme
Anahtar Yönetimi

Tablo 4.1. Teknik tedbirler

4.2. İdari Tedbirler Özeti Tablosu

Tablo 4.2'de veri sorumlular tarafından alınabilecek idari tedbirler gösterilmiştir.

İdari Tedbirler
Kişisel Veri İşleme Envanteri Hazırlanması
Kurumsal Politikalar (Erişim, Bilgi Güvenliği, Kullanım, Saklama ve İmha vb.)
Sözleşmeler (Veri Sorumlusu - Veri Sorumlusu, Veri Sorumlusu - Veri İşleyen Arasında)
Gizlilik Taahhütnameleri
Kurum İçi Periyodik ve/veya Rastgele Denetimler
Risk Analizleri
İş Sözleşmesi, Disiplin Yönetmeliği (Kanuna Uygun Hükümler İläve Edilmesi)
Kurumsal İletişim (Kriz Yönetimi, Kurul ve İlgili Kişi Bilgilendirme Süreçleri, İtibar Yönetimi vb.)
Eğitim ve Farkındalık Faaliyetleri (Bilgi Güvenliği ve Kanun)
Veri Sorumluların Sicil Bilgi Sistemine (VERBiS) Bildirim

Tablo 4.2. İdari tedbirler

TEMEL ISO27001 SÜREÇLERİ

Temel Gereksinimler

- Kurum dış ve iç gereksinimlerini belirleme ve yeniden değerlendirme
- Kapsam belirleme ve yeniden değerlendirme
- Periyodik risk değerlendirme
- Sürekli düzeltici faaliyet yönetimi
- (Bilgi güvenliği hedeflerine ulaşılıp ulaşılmadığının işaretini olan ölçütlerle ilişkin) sürekli izleme ve ölçme yönetimi
- Geliştirilmiş olan bilgi güvenliği kontrollerinin sürekli uygulanması
 - Farkındalık eğitimleri, olay yönetimi, sızma testleri, güvenli sistem yazılım geliştirme, değişiklik yönetimi, tedarikçi risk yönetimi, v.d.
- Periyodik iç denetim
- Periyodik yönetimin gözden geçirmesi

DOKÜMANTASYON VE ISO27001

Gerekli Dokümanlar

ISO27001 standardına göre oluşturulması ve yönetilmesi gereken dokümanlar şu şekilde tarif edilmiştir:

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 kuruluşşa değişebilir:

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

(Ref: TS ISO/IEC ISO27001 Aralık 2013)

STANDARDIN GEREKTİRDİĞİ YAZILI BİLGİLER

Dokümanların hazırlanması

- Kapsam [4.3]
- Bilgi güvenliği politikası [5.2]
- Bilgi güvenliği risk değerlendirme süreci ile ilgili bilgiler [6.1.2]
- Bilgi güvenliği risk değerlendirmesinin sonuçlarına dair yazılı bilgiler [8.2]
- Bilgi güvenliği risk işlemesinin sonuçlarına ait yazılı bilgiler [8.3]
- Bilgi güvenliği amaçları (hedefleri) [6.2]
- (Kuruluşun bilgi güvenliği performansını etkileyen personelin) yeterliliğin(in) delili olan yazılı bilgiler [7.2]
- İzleme ve ölçme sonuçlarına dair ~~delili~~ olarak uygun yazılı bilgiler [9.1]
- Tetkik programı (planı) ve tetkik sonuçlarının delil teşkil eden yazılı bilgiler [9.2]
- Yönetim gözden geçirme sonuçlarının delili olan yazılı bilgiler [9.3]
- Uygunsuzlukların içeriği ve alınan önlemler ile uygulanan düzeltici faaliyetlerin sonuçlarına ilişkin yazılı bilgiler [10.1]
- Kuruluş tarafından bilgi güvenliği yönetim sisteminin etkinliği için gerekli olduğu belirlenen yazılı bilgiler [7.5.1]

STANDARDIN GEREKTİRDİĞİ YAZILI BİLGİLER

Dokümanların hazırlanması (DEVAM)

EK-A'da yazılı olmasından bahsedilen kontroller

- A.8.1.3 Varlıkların kabul edilebilir kullanımı
- A.9.1.1 Erişim kontrol politikası
- A.12.1.1 Yazılı işletim prosedürleri (operasyonel prosedürler)
- A.13.2.4 Gizlilik ya da ifşa etmemeye anlaşmaları
- A.14.2.5 Güvenli sistem mühendisliği prensipleri
- A.15.1.1 Tedarikçi ilişkileri için bilgi güvenliği politikası
- A.16.1.5 Bilgi güvenliği ihlal olaylarına yanıt verme
- A.17.1.2 Bilgi güvenliği sürekliliğinin uygulanması
- A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama

(Ref: TS ISO/IEC ISO27001 Aralık 2013)

YAZILI BİLGİLERİN YÖNETİMİ İLE İLGİLİ KURALLAR

Doküman oluşturma ve güncelleme

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.

(Ref: TS ISO/IEC ISO27001 Aralık 2013)



YAZILI BİLGİLERİN YÖNETİMİ İLE İLGİLİ KURALLAR

Doküman oluşturma ve güncelleme (DEVAM)

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.

(Ref: TS ISO/IEC ISO27001 Aralık 2013)

KAPSAM

Kapsamın önemi

- Kapsam önemli, kısmen soyut ve bulanıktır, bu yüzden daha ilk adımda motivasyonunu kaybedebilirsiniz.
- Nasıl ve hangi terimlerle ifade edilebilir?
- Süreç, ürün / hizmet, organizasyon, fiziki alan, ağ bölümü / sistemler
- Kapsam ne zaman netleşir (proje başlangıcında ne kadar net bir görüş mesafemiz olabilir)?
- Kapsama muhasebeyi, üretimi, bölge ve il organizasyonlarını, tüm birimleri dahil edersek ne olur, proje ne kadar uzar?
- Dış kaynak kullanımı olan durumları nasıl ele alacağız, tedarikçiler kapsam içinde mi dışında mı olacak?

KAPSAM İLE İLGİLİ STANDART GEREKSİNİMLERİ

Kapsamın belirlenmesi

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.

(Ref: TS ISO/IEC ISO27001 Aralık 2013)



KAPSAM DOKÜMANI BAŞLIKLARI

Kapsam başlık örnekleri

- Kapsam
 - Kapsam Sınırları
 - Yerleşme Sınırları
 - Sistem Sınırları
- Organizasyonel Sınırlar
 - Arayüzler
 - Fiziksel Arayüzler
 - Sistemsel Arayüzler
- Bağımlılıklar
 - Ağ
 - Enerji
 - Altyapı

4.3 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ'NİN KAPSAMININ BELİRLENMESİ

Kapsam

Sıza testi hizmetleri, bilgi güvenliği ve bilgi teknolojileri yönetim hizmetleri, yazılım ve sistem geliştirme ve destek hizmetleri sureçleridir.

Yerleşme

Çiftlikhavuzlar Mah. Eski Londra Asfaltı Cad. No:151 1/C Esenler İstanbul.

Organizasyon

Tüm sıza testi hizmeti, bilgi güvenliği ve bilgi teknolojileri yönetim hizmeti sunan ve yazılım ve sistem geliştirme ve destek hizmetlerinde görev alan personel kapsama dahildir.

Arayüzler

- **Fiziksel:** Ofis kapısı Teknopark A1 blok zemin katına açılır. Zemin katta bulunan ofis penceresi bina yan tarafına açılır.
- **Ağ:** Internet bağlantısı Türk Telekom TTNet üzerinden sağlanır, internet modemli ofis alanındaki telefon hattına bağlıdır.

Bağımlılıklar

GİZLİ

4

KURULUŞUN BAĞLAMI, DIŞ VE İÇ GEREKSİNİMLER

İlgili bölümler

- Standardın kapsamla ilgili bölümünde (Madde 4.1 ve Madde 4.2'ye) verilen referanstan da tahmin edilebileceği gibi kapsamı en çok etkileyen konu bizim (eski alışkanlıkla) iş, yasal ve kontratsal gereksinimler olarak tanımladığımız kavramlardır. Bu bölümle ilgili bir dokümantasyon şartı bulunmamaktadır, ancak dokümantasyon ihtiyacının hissedilebileceği bir alandır.
- Kapsama ince ayarın yapılması ancak fark analizi dediğimiz sürecin işletilmesi sonrasında mümkün olmaktadır.
- 2013 versiyonuyla birlikte kuruluşun içsel ve çevresel şartlarını ve bir anlamda bilgi güvenliği ihtiyaçlarını ortaya koyması için gerekli arka planı ortaya koyma gereksinimi belirtilmiştir:

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.

(Ref: TS ISO/IEC ISO27001 Aralık 2013)

KURULUŞUN BAĞLAMI BÖLÜMÜNÜN BAŞLIKLARI

İç Bağlam

- İdare, kuruluşla ilişkin yapı, roller ve yükümlülükler
- Yerine Getirilecek Politikalar, Hedefler ve Stratejiler
- Kaynaklar ve Bilgi Birikimi
- İç Paydaşlarla İlişkiler ve Onların Algılamaları ve Değerleri
- Kuruluşun Kültürü
- Bilgi Sistemleri, Bilgi Akışı ve Karar Alma Süreçleri
- Kuruluş Tarafından Uyarlanan Standartlar, Kılavuzlar ve Modeller
- Sözleşmeye İlişkin İlişkilerin Biçim ve Genişliği

IÇ BAGLAM

İdare, kuruluşla ilişkin yapı, roller ve yükümlülükler

Kurumun bilgi güvenliği yönetim sorumlulukları atanmıştır. Kurumun ölçügg itibarıyla tek görevi bilgi güvenliği yönetimi veya BT altyapı yönetimi olan tam zamanlı personel bulunmamakla birlikte kurum kadrosu teknik yetkinliği yüksek bir personel profilinden oluştuğundan bu görevler yarı zamanda olarak belirli personele atanmıştır.

Yerine Getirilecek Politikalar, Hedefler ve Stratejiler

Kurumumuz için öncelikli bilgi güvenliği hedefimiz müşteri bilgilerimizin gizliliğini sağlamak ve kurumumuzun devamlılığı için elzem olan kurum itibarının korunabilmesi için güvenlik ihlal ihtimalini en aza indirebilmektir. Bu doğrultuda ISO27001 tabanlı bir bilgi güvenliği yönetim sistemi kurulmuş olup, ihtiyaçlar ve imkanlar nisbetinde fiziksel, süreçsel ve mantıksal bilgi güvenliği kontrolleri için gerekli yatırımlar yapılmakta ve faaliyetler sürdürülmektedir.

Kaynaklar ve Bilgi Birikimi

BTRisk 2009 yılından bu yana hizmet verdiği alanlarda metodlarını geliştirmiştir, kendi personelini bilgi güvenliği denetim hizmetleri ve danışmanlık hizmetleri konusunda en ileri düzeyde yetiştirebilecek eğitim materyallerini geliştirmiştir. Mevcut kadrosu büyük oranda deneyimli personelden oluşmaktadır.

İç Paydaşlarla İlişkiler ve Onların Algılamaları ve Değerleri

Personelimiz, okulumuzun temelini oluşturmaktadır. Personelimiz, kurumumuzun verdiği

İLGİLİ TARAFLARIN İHTİYAÇ VE BEKLENTİLERİNİN ANLAŞILMASI

Standardın gereksinim başlığı

2005 versiyonunda vurgulanan dış ve iç gereksinimlerin belirlenmesi ihtiyacı 2013 versiyonunda bu başlık altında ele alınmıştır.

Bizim tavsiyemiz proje başlangıcında yüzelsel olarak bu analizin yapılması ve not edilmesi, ancak fark analizi sırasında daha detaylı (ör: düzenleme alt maddesi bazında, sözleşme bazında, konjönktürel bazda) biçimde gereksinimlerin belirlenmesi ve bilgi varlıkları / süreçler ile ilişkilendirilmesidir.

4.2 İlgili tarafların ihtiyaç ve bekłentilerinin 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.

(Ref: TS ISO/IEC 27001 Aralık 2013)



04:58 / 10:24

İLGİLİ TARAFLARIN İHTİYAÇ VE BEKLENTİLERİNİN ANLAŞILMASI

Standardın gereksinim başlığı (ÖRNEK)

- Düzenleyici Otoriteler
- Ortaklarımız ve Personelimiz
- Müşteriler

4.2 İLGİLİ TARAFLARIN İHTİYAÇ VE BEKLENTİLERİNİN ANLAŞILMASI

Türk Standardları Enstitüsü [TSE]

Türk Standardları Enstitüsü'ne Onaylı Sızma Testi Firması olabilmek için başvurumuz bulunmaktadır.TSE bu süreç içi TS 13638 numaralı Bilgi Teknolojileri - Güvenlik Teknikleri - Sızma Testi Yapan Personel ve Firmalar İçin Şartlar dokümanını yayımlamıştır. Bu dokümandaki özellikle personel yetkinlik şartları ve firma yetkinlik şartları (Madde 6) TSE'nin onaylı sızma testi firmalarından beklenenlerini içermektedir. Ayrıca 7. Kişi bilgilerin gizliliği ve 8. Kanunlara ve mevzuata uyum maddeleri de sızma testi firmalarının bu konulardaki yasal ve etik kuralları içermektedir.

Bankacılık Düzenleme ve Denetleme Kurumu [BDDK]

sekktöründen kuruluşlara sızma testi hizmetleri vermektedir.
BDDK 0.77.00.00/010.06 02-1 sayılı Bilgi Sistemlerine İlişkin
apsamında gerçekleştirilen testlerimizde bu genelgede
e yöntemlere uygun biçimde faaliyet göstermemiz

İç Güvenlik Kurumu [BTK]

İç Güvenlik Kurumu'ndan kuruluşlara sızma testi hizmetleri vermektedir.
kurum içinde ve bizim gibi firmaların tedarik ettiğleri

GİZLİ

3

ÜST YÖNETİMİN DESTEĞİNİN ÖNEMİ

Üst yönetimin gereklilikleri

Üst yönetim ibaresi ISO27001:2013 versiyonunda defalarca kullanılmakta ve üst yönetimin
desteğinin altı çizilmektedir.

5.1 Liderlik ve bağlılık

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

5.2 Politika

- Üst yönetim aşağıdakileri karşılayan bir bilgi güvenliği politikası oluşturmalıdır: ...

5.3 Kurumsal roller, sorumluluklar ve yetkiler

- Üst yönetim, bilgi güvenliği ile ilgili olan roller için sorumluluk ve yetkilerin atanmasını ve duyurulmasını temin etmelidir.

9.3 Yönetimin gözden geçirmesi

- Üst yönetim bilgi güvenliği yönetim sisteminin sürekli uygunluğunu, doğruluğunu ve etkinliğini temin etmek için planlı aralıklarla gözden geçirmelidir.

(Ref: TS ISO/IEC ISO27001 Aralık 2013)

ÜST YÖNETİMİN DESTEĞİNİN ÖNEMİ

Üst yönetimin gereklilikleri (DEVAM)

7. Destek

bölümündeki başlıkların arkasında yönetim iradesine ihtiyaç bulunmaktadır:

- 7.1 Kaynaklar
- 7.2 Yeterlilik (güvenlik organizasyonu v.d. ilgili personel için)
- 7.3 Farkındalık
- 7.4 İletişim

(Ref: TS ISO/IEC ISO27001 Aralık 2013)



ISO27001 AÇISINDAN ÜST YÖNETİM

Kim olmalıdır?

- Genel Müdür
- Yönetim kurulu içinde oluşturulmuş bir komite
- BT organizasyonu
- Bilgi güvenliği yöneticisi
- KVKK yöneticisi
- Hukuk
- İnsan kaynakları
- İş birimleri yönetimleri



ÜST YÖNETİMİN DESTEĞİ

Nasıl somutlaştırılır?

- Organizasyon kurma ve sorumlulukların net biçimde atanması
- İç denetim ve yönetim gözden geçirme aktivitelerinin etkinliği
- Bütçe içinde net destek
- Bilgi güvenliği eğitimlerinin planlanması, kariyer planlarına dahil edilmesi, izleme ölçümleri kapsamında izlenmesi



POLİTİKA

Politika içeriği

- Bizim kurum kültürümüzde Politika kavramının yeri (yönetişim – yön verme – yazılı olmayan değerler, prensipler)
- BGYS kurulum projesinde Politika'nın netleşebileceği zaman:
 - 5.2 Politika başlığı ilişkisel olarak **5 Liderlik grubu** altında yer almaktadır. Ancak tıpkı kapsamda olduğu gibi politikanın netleşmesi de BGYS kurulum projesinin ihtiyaç belirleme safhasından sonra (yani risk değerlendirme ve bunun ana adımlarından olan fark analizi adımlarında) mümkün olabilecektir.

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,

(Ref: TS ISO/IEC ISO27001 Aralık 2013)

POLİTİKA

Hangi dokümanlar? (ÖRNEK)



ANASAYFA

KURUMSAL

ÜRÜNLER

HİZMETLER

EĞİTİMLER

İLETİŞİM

Türkçe

ANASAYFA > BİLGİ GÜVENLİĞİ POLİTIKAMIZ

Bilgi Güvenliği Politikamız

Bilgi Güvenliği Politikamız

- ✓ Bilgi güvenliğinin sağlanması BTRisk'in başarısı ve sürekliliği için kritik öneme sahiptir.
- ✓ Bu nedenle BTRisk yönetimi, ISO27001 BGYS standardının, ilgili yasa ve mevzuatların şartlarını sağlamayı taahhüt eder.
- ✓ BTRisk yönetimi, bilgi güvenliği düzeyinin sürekli iyileştirilmesi için gerekli maddi kaynak ve personel zamanını temin etmeyi, bilgi güvenliği tehdit ve fırsatlarını sürekli gözden geçirmeyi taahhüt eder.
- ✓ Bilgi güvenliği amaçları, tehdit ve fırsatlardaki değişimler yönetim gözden geçirme toplantılarında periyodik olarak gözden geçirilerek ISO27001 gereksinimlerine uygun biçimde planlanır. Bilgi güvenliği amaçları ilgili personele duyurulur ve belirlenen zamanlarda amaçlara ulaşma başarısı ölçülür.



BİLGİ GÜVENLİĞİ ORGANİZASYONU

BGYS'nin sürdürülmesi için gerekli aktiviteler

- Periyodik risk değerlendirme
- Periyodik iç denetimler
- Yönetim gözden geçirme faaliyetlerinin koordinasyonu
- Düzeltici faaliyetlerin koordinasyonu
- Farkındalık eğitimlerinin gerçekleştirilmesi ve koordinasyonu
- Politika, standart, prosedür v.b. gözden geçirilmesi ve bakımı
- Bilgi güvenliği farkındalık ve ihtiyaçlarının yoğunlaşmasıyla gündeme gelen yeni aktiviteler
 - Sistem ve yazılım projelerinde tehdit modelleme, görüş sunma
 - Tedarikçi / iş ortağı risk değerlendirme, tedarikçi kabul ve denetim süreçleri
 - Kurum içi bilişim incelemesi ve soruşturmalarda uzman desteği
- Güvenlik gereksinimlerinin yoğun olduğu operasyonel görevler
- Görevlerin güvenliği ilkesi ve organizasyonel sayının az olduğu durumda oluşan zorluk



01:48 / 11:13

BİLGİ GÜVENLİĞİ ORGANİZASYONU

BGYS'nin sürdürülmesi için gerekli aktiviteler (DEVAM)

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.

(Ref: TS ISO/IEC ISO27001 Aralık 2013)



ISO27001 EL KİTABI

5.3 KURUMSAL ROLLER, SORUMLULUKLAR VE YETKİLER

Kurumsal roller, sorumluluklar ve yetkiler aşağıdaki gibidir:

BGYS Komitesi

- Genel olarak BGYS'nin ISO27001 standardının gereksinimlerine uygun şekilde işletildiğinden emin olunması
- Bilgi güvenliği yönetici tarafından raporlanacak olan BGYS performansının izlenmesi
- Bilgi güvenliği politikası doğrultusunda yönetimin taahhütlerini yerine getirdiğinden emin olunması
- Periyodik risk değerlendirme faaliyetinin yapıldığından emin olunması
- Periyodik iç denetim faaliyetinin yapıldığından emin olunması
- Periyodik yönetim gözden geçirme faaliyetlerinin ISO27001 standardının ilgili maddesinin gereksinimlerini karşılayacak biçimde gerçekleştirilmesi

BGYS Komitesi Üyeleri

- Başkan- Genel Müdür

BİLGİ GÜVENLİĞİ İHTİYAÇLARININ BELİRLENMESİ VE ÖNCELİKLENDİRİLMESİ

Bilgi Güvenliği Risk Değerlendirmesi

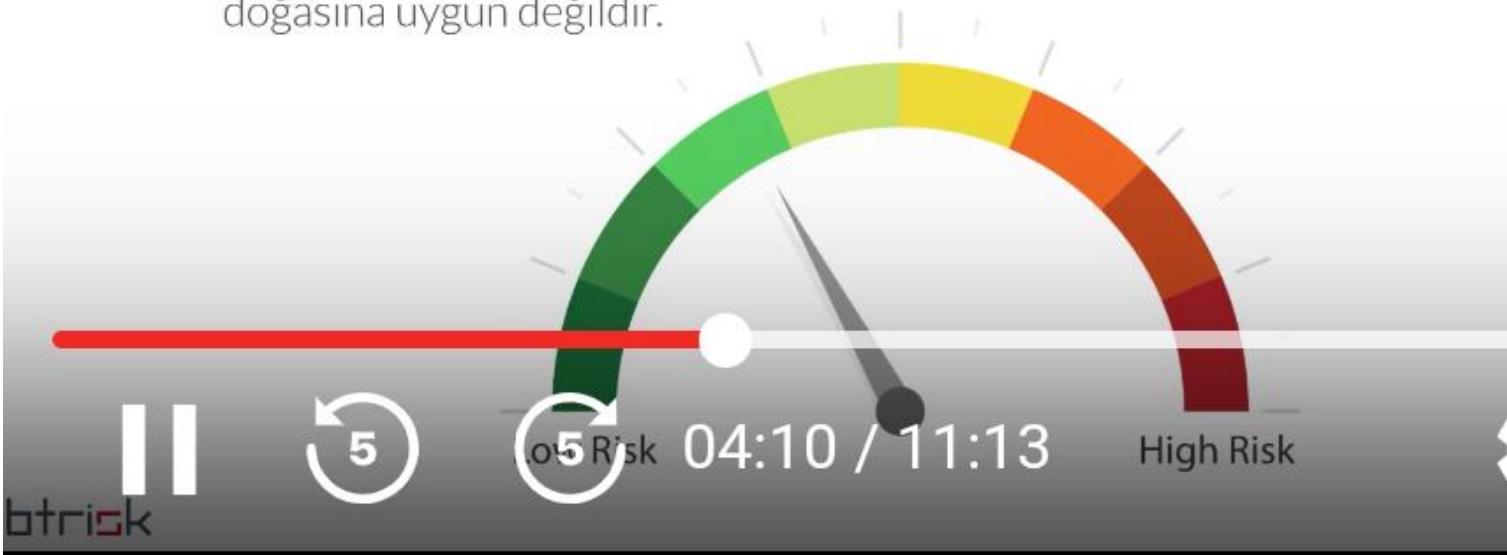
- BGYS kurulumunun en korkutucu bölümü
- Çünkü; nesnel bir süreç, çok geniş bir uzmanlık gerektiriyor, bilgi güvenliği risklerinin kantitatif (ör: parasal) ifade edilmesi imkansız yakını ve bu nedenlerden dolayı eleştiriye açık



BİLGİ GÜVENLİĞİ İHTİYAÇLARININ BELİRLENMESİ VE ÖNCELİKLENDİRİLMESİ

Risk değerlendirmesi ile ilgili yanlış algılar

- Risk değerlendirmesinin her an güncel tutulması:
 - Risk değerlendirme süreci periyodik olmalı ve belli bir süre içinde bitirilmelidir.
- Risk değerlendirmesinin bir şeyi gözden kaçırılmaması:
 - Risk değerlendirme faaliyeti bir tetkik faaliyeti değildir ve büyük oranda beyana dayalıdır. Dolayısıyla risk gözden kaçırma potansiyeli yüksektir. Eğer tetkik faaliyeti olsaydı çok daha fazla kaynak ve zaman gerektirirdi ki bu da planlama faaliyetinin doğasına uygun değildir.



BİLGİ GÜVENLİĞİ DEĞERLENDİRMEŞİ İLE İLGİLİ GEREKSİNİMLER

Standartın özetlenmiş ve yorumlanmış hali

- Tekrarlanabilen bir risk değerlendirme metodunun geliştirilmesi
- Risk kabul kriterlerinin belirlenmesi (yani bir risk formülünün geliştirilmesi ve kabul edilebilir seviyenin belirlenmesi)
- Gizlilik, bütünlük ve erişilebilirlik kayıpları ile ilgili risklerin tespit edilmesi (yani kayıp / etki türlerinin bu başlıklarda belirlenmesi)
- Risk sahiplerinin belirlenmesi
- Belirlenen riskler gerçekleştiği takdirde muhtemel sonuçların değerlendirilmesi (yani etki değerinin belirlenmesi)
- Belirlenen risklerin gerçekleşmesi ihtimalinin gerçekçi bir şekilde değerlendirilmesi (yani ihtimali destekleyecek verilerle risk senaryosunun geliştirilmesi)
- Risk seviyelerinin belirlenmesi (yani bir formüle göre hesaplanması)
- (ve doğal olarak) risklerin kabul kriterleri ile karşılaştırılması ve önceliklendirilmesi



05:16 / 11:13



RİSK DEĞERLENDİRME GEREKSİNİMLERİ

- Risk değerlendirme sürecine kimler dahil olmalıdır?
- Risk değerlendirme metodunun detayları nelerdir?
- Risk değerlendirme varlık bazlı mı, süreç bazlı mı yoksa hiçbir kavrama bağlı olmadan mı yapılır?
- Risk değerlendirme formülü ne olmalıdır?
- Kabul edilebilir risk seviyesi ne olmalıdır?
- Risk değerlendirme çalışması ne kadar süre içinde tamamlanmalıdır?



BİLGİ GÜVENLİĞİ RİSK İŞLEME İLE İLGİLİ GEREKSİNİMLER

Özetlenmiş ve yorumlanmış hali

- (Risk senaryosu bazında) uygun bilgi güvenliği risk işleme seçeneklerinin seçilmesi (yani kabul etme, kaçınma, transfer etme ve azaltma seçimlerinden birisinin yapılması)
- Seçilen bilgi güvenliği risk işleme seçeneklerinin uygulanmasında gerekli olan tüm kontrollerin (Ek-A'daki kontroller ve kendi geliştirebileceğiniz ek kontroller kastediliyor) belirlenmesi
- Belirlenen kontroller ile Ek-A'daki listenin karşılaştırılması (gözden kaçan bir kontrol ihtiyacı olmaması için)
- Uygulanabilirlik bildirgesinin hazırlanması ("gerekli kontrolleri ve bunların dahil edilmesinin gerekliliklendirmesi, uygulanıp uygulanmadıklarını ve Ek A'dan kontrollerin dışında bırakılmasının gerekliliklendirmesini içeren bir UB üretilmesi")
- Risk işleme planının formüle edilmesi
- Risk işleme planına dair risk sahiplerinin onayının alınması ve artık bilgi güvenliği risklerinin kabulu

RİSK DEĞERLENDİRME ÜZERİNE DEĞERLENDİRMELERİMİZ

Özetlenmiş ve yorumlanmış son hali

- Risk değerlendirme sürecinin konudan sapma potansiyeli çok yüksek
 - ör: su sebiline ilaç atılarak IT personelinin uyutulması gibi senaryolar gündeme gelebilir
- Tüm riskleri değerlendirdip değerlendirmediğinizden emin olabilmeniz kolay değil
- Üzerinde durduğunuz senaryoların gerçekten kayda değer olup olmadıklarını baştan anlamak, gereksiz detayda kayıt üretmekten kaçınmak zor olabilir
 - ör: demirbaş varlık kayıtları üzerinde bir risk değerlendirme yaptığınızda aynı risk senaryosunu gereksiz yere defalarca not etmek durumunda kalabilirsiniz, yanı risk profiline göre graplama imkanını zamanında fark edemeyebilirsınız



07:40 / 11:13

BİZİM RİSK DEĞERLENDİRME YAKLAŞIMIMIZ

Sondan başa değerlendirme

- Denetim sürecinden edindiğimiz deneyime göre konudan sapmadan ve gözden kaçırma riskini en aza indirerek bir değerlendirme yapmanın yolu kontrol aktivitelerinin üzerinden gitmektir.
- Kontrol aktivitesi tartışılmaya başlandığında (tabi bu aşamanın öncesiinde ürün / hizmet / süreç / organizasyon / tesisler / düzenleme ve kontratlar'ın üzerinden yüzeysel olarak geçilmiş olması gerekmektedir, ki bu çalışma kapsam belirleme aşamasında zaten yapılmış olacaktır) bu aktiviteye tabi olması gereken konular (varlıklar / süreçler v.d.) su yüzüne çıkacaktır.
- Bu yüzden biz kontrol aktivitelerinin sorulara dönüştürüldüğü bir liste baz alınarak risk değerlendirme yapılmasını öneriyoruz.



08:45 / 11:13

BİZİM RİSK DEĞERLENDİRME YAKLAŞIMIMIZ

Soru bazlı değerlendirmenin avantajları

- Risk değerlendirmeyi yapacak kişinin konunun uzmanı olmasa da belli bir alana yönlendirilmesini sağlar, dolayısıyla daha somut kavramlar üzerinde düşünmesini destekler. Bu sayede risk analiz görevlerini kontrol sahiplerine yayma imkanı da doğar.
- Uygulanabilirlik bildirgesi ve Ek-A'da bulunan kontrollerin üzerinden geçilmesi gibi zaten yapılması gereken işlemlerin risk değerlendirme sürecinin başında yapılması nedeniyle vakit kazandırır.
- Fark analizi de diyebileceğimiz bu safha risk değerlendirme sürecinin bir noktasında zaten yapılmak durumundadır (bkz. ISO27005:2018).
- Soru üzerinde düşünüldüğünde etrafında düşünülmesi gereken kavram daha netleşir, risk profiline göre gruplama imkanı doğar, gereksiz varlık, süreç, v.b. üzerinde kaybedilecek zaman azaltılır.
- Bu tür bir risk değerlendirme yaklaşımı varlıklardan veya süreçlerden yola çıkarak değerlendirme yapmayı engellemez, tam aksine belli bir varlık veya süreçle ilgili düşünülmüş olan senaryolar kolaylıkla listelenebilir ve risk değerlendirmesinin konusunda daha emin olunabilir.

BİZİM RİSK DEĞERLENDİRME YAKLAŞIMIMIZ

Taşıyıcı (container) bazlı değerlendirme

- Bizim yaklaşımız soruları taşıyıcı bazlı (yani bilgi varlığı bazlı) olarak değerlendirmeyi gerektiriyor. Zira bilgi güvenliği kontrolleri taşıyıcılara yönelik olarak uygulanır, doğrudan bilgiye yönelik bir kontrol olma durumu çok azdır.
 - Örn: erişim kontrolü ele aldığında; ofis, veri merkezi, işletim sistemi, uygulama, v.b. taşıyıcılara yönelik olarak uygularız, doğrudan veriye yönelik değil.
- Varlık bazlı yaklaşım kaybın ifadesini de kolaylaştırmaktadır.
- Gizlilik, bütünlük ve erişilebilirlik kayıplarının değerlendirilmesini bu yöntem ile kolaylaştırmaktadır.



BİLGİ GÜVENLİĞİ AMAÇLARI, İZLEME VE ÖLÇME

ISO27001'de hedef, izleme ve ölçme

Diger ISO yönetim sistemi standartlarında da olduğu gibi ISO27001'de hedefler, izleme ve ölçmeye önem vermektedir.

6.2 Bilgi güvenliği amaçları ve bu amaçları başarmak için planlama

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.

(Ref: TS ISO/IEC ISO27001 Aralık 2013)

BİLGİ GÜVENLİĞİ AMAÇLARI, İZLEME VE ÖLÇME

ISO27001'de hedef, izleme ve ölçme (DEVAM)

Kuruluş bilgi güvenliği amaçlarını nasıl başaracagini planlarken, aşağıdakileri belirlemeli:

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

(Ref: TS ISO/IEC ISO27001 Aralık 2013)



BİLGİ GÜVENLİĞİ AMAÇLARI, İZLEME VE ÖLÇME

ISO27001'de hedef, izleme ve ölçme (DEVAM)

9.1 İzleme, ölçme, analiz ve değerlendirmeye

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 değerlendirmeye yöntemleri,
- 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 edeceğini ve değerlendireceği.

(Ref: TS ISO/IEC ISO27001 Aralık 2013)

BİLGİ GÜVENLİĞİ AMAÇLARI, İZLEME VE ÖLÇME

ISO27001'de hedef, izleme ve ölçme (DEVAM)

- Ne yazık ki bilgi güvenliği ile ilgili yapılabilecek ölçümler malesef kalite ölçümleri gibi kolay parasallaştırılamamaktadır.
- Bu yüzden bizim önerimiz genel olarak kontrol bazlı yönetim sistemlerinde olduğu gibi hedeflerin kapsam bazlı (yani kontrolün kapsama alanının oranı veya uygulanma sıklığı gibi kriterlerle) belirlenmesi ve ölçülmesidir.



ISO27001 EL KİTABI

6.2 BİLGİ GÜVENLİĞİ AMAÇLARI VE BU AMAÇLARI BAŞARMAK İÇİN PLANLAMA

Bilgi güvenliği amaçları ISO27001 BGYS standardının gereksinimlerine uygun olarak belirlenir ve takip edilir.

Bilgi güvenliği amaçlarının dokümantasyonu, sonuç değerlendirme kayıtları her bir dönem için hazırlanacak ayrı dokümanlarda kaydedilir.

Bilgi Güvenliği Amaçlarının Duyurulması

Bilgi güvenliği amaçları ofis alanındaki duyuru ofis alanındaki duyuru panosunda yayınlanır. Dönem ile ilgili BGYS_002_Bilgi Güvenliği Amaçları dokümanında belirtilen bilgi güvenliği amaçlarında değişiklik olduğunda panodaki kopya da yenilenir.

2018 yılı için bilgi güvenliği amaçları aşağıdaki gibidir:

Amaç	Personelle ISO27001 iç denetim eğitimi sağlanması
İletişimi Yapılacak Taraflar	Eğitime davet edilecek olan personel ve eğitmen personel
Gerekli Kaynaklar	Eğitim materyallerinin gözden geçirilmesi [2 Gün] ve eğitimin sağlanması için eğitmen zamanı [2 Gün], eğitime katılacek olan personelin zamanı [2 şer Gün]
Sorumlu(lar)	Bilgi Güvenliği Yöneticisi [Eğitmen]
Tamamlanma Hedef Tarihi	31 Ağustos 2018
Başarı Kriteri	Eğitime en az 2 personelin katılıması
Başarı Değerlendirme Sonucu	

İÇ TETKİK

ISO27001'de iç denetim ve prensipleri

- İç tetkik BGYS'nin kurumun kendi koyduğu kurallara ve ISO27001 standardına uygunluğununu denetlemek amacıyla (periyodik olarak) yapılır. (9.2.a)
- İç tetkik sonuçları Yönetim Gözden Geçirme faaliyetinin en önemli girdilerinden birisini oluşturmaktadır. (9.3.c.3)
- İç tetkik programının yapılması ve yazılı olarak saklanması gereklidir. (9.2.c, 9.2.g)



İÇ TETKİK

Denetim program yönetimi ve türleri

- Denetim organizasyonu ve denetim yönetiminin bağlı bulunduğu seviye
- Denetim yetkilendirmesi
- Denetim prosedürleri (planlama, denetim kriterleri, kaynak yönetimi, dokümantasyon, kalite yönetimi)
- Denetçi yetkinlikleri ve eğitim yönetimi
- Birinci taraf denetimleri
 - Kurumun kendi içinde yaptığı denetim
 - İkinci taraf denetimleri
- Üçüncü taraf / belgelendirme denetimleri
 - Kurumun çalışmış olduğu tedarikçi için yapılan denetim
 - Bağımsız bir kuruluş tarafından yapılan denetim

İÇ TETKİK

Denetim planlama ve iç denetim planlaması

- Denetim uzayı oluşturma
- Risk tabanlı planlama
- ISO27001 maddeleri
- Düzeltici faaliyetlerin gözden geçirilmesi
- Önceki denetim bulguları takip denetim



İÇ TETKİK

Denetim süreci

- Denetimin başlatılması
- Denetim ekip liderinin atanması
- Denetim hedeflerinin, kapsamının ve kriterlerinin tanımlanması
- Denetim fizibilite analizi (denetim gerçekleştirilebilir mi?)
- Denetim ekibinin oluşturulması
- Denetlenen ile ilk iletişimin gerçekleştirilmesi
- Doküman inceleme
- Yönetim sistemi dokümantasyonunun incelenmesi
- Denetim kriterleri ile karşılaştırılması

İÇ TETKİK

Saha denetimine hazırlık ve denetim kriterlerinin oluşturulması

- Denetim planının hazırlanması
- Denetim ekibinin görevlerinin belirlenmesi (bu görevler saha çalışması sırasında değişebilir)
- Çalışma kağıtlarının hazırlanması
- Standart maddeleri
- Kontrat yükümlülükleri
- Yasal düzenlemeler
- Kontrollerin tespiti (sureç dokümantasyonu, iş akış şemaları)
- Walkthrough (bir işlemin başından sonuna oluşan tüm kayıtların incelenmesi, prosedürün ve kontrol noktalarının belirlenmesi)



07:35 / 12:01

İÇ TETKİK

Saha denetiminin gerçekleştirilmesi ve raporlama

- Açılış toplantısının gerçekleştirilmesi
- Denetim sırasında iletişim
- Kanıtların toplanması ve doğrulanması
- Denetim bulgularının tespiti
- Denetim görüşünün oluşturulması
- Kapanış toplantısının gerçekleştirilmesi

- Denetim raporunun hazırlanması
- Denetim raporunun onaylanması
- Denetim raporunun dağıtımı



08:10 / 12:01

3

İÇ TETKİK

Kontrol denetim türleri ve denetimde kanıt toplama teknikleri

- Kontrol tasarım etkinliğinin denetimi
- Kontrol operasyonel etkinlik denetimi
- Organizasyonun incelenmesi
- Politika ve prosedürlerin incelenmesi
- Mülakat
- Doküman inceleme
- Kontrollerin gözlenmesi
- Kontrolün tekrar uygulanması (reperformance)
- Sürecin bir örnek üzerinden takibi (walkthrough)



08:38 / 12:01

İÇ TETKİK

Mülakat soruları

- Açık ve kapalı uçlu sorular
- Yönlendirici sorulardan kaçınma
- Suçlayıcı veya denetleneni kapanmaya itecek sorulardan kaçınma
- Doğrulayıcı ek kanıtlar
- Not almanın amacının açıklanması
- Anlaşılan konuların geri bildirimi
- Sözü kesmeme ve konunun dağılmaması



09:28 / 12:01

İÇ TETKİK

Kanıtın güvenilirliği, örnekleme ve denetim dokümantasyonu

- Kanıtı sağlayan/tespit eden kişinin bağımsızlığı
- Kanıtı sağlayan/tespit eden kişinin yetkinliği
- Kanıtın objektifliği
- Kanıtın tekrar elde edilebilirliği
- Makul güvence kavramı
- İstatistiksel örnekleme
- Profesyonel kanaatle örnekleme
- Çalışma kağıtları (work papers)
- Denetim prosedürünün dokümantasyonu



İÇ TETKİK

Rapor bölümleri ve Rapor yazarken dikkat edilmesi gerekenler

- Yönetici özeti
- Denetim hedefleri
- Denetim kapsamı
- Denetim kriterleri
- Denetim süresi
- Denetime katılan kişiler
- Bulgu istatistikleri
- Denetim görüşü (conclusion)
- Teknik bulgular
- Rapor dağıtım listesi
- Net, açık, ağıdalı cümlelerden uzak
- Önceden mutabık kalınmış, sürprizlerden uzak
- Çalışma kağıtlarıyla desteklenebilir
- Hedef kitleye uygun bölümler ve/veya teknik detay barındırın
- Kaliteli öneriler içeren, ancak yönetim adına karar verme riskine girmeyen ifadeler
- Kapsamı ve denetim hedeflerini net ifade eden
- Görüş verilemeyen alanları ve nedenlerini belirten

iç TETKİK

Düzen konular

- Denetim ekibine teknik uzmanların katılımı
- Yönetim temsilcisinin ve diğer gözlemcilerin denetimdeki rolü
- Bulgular ve iyileştirme önerileri
- Denetçilerin danışman rolü alması
- Suistimal ihtimali veya işaretinin tespiti
- Majör ve minör bulgular
- Bilgisayar destekli denetim araçları (CAAT)
- Entegre denetim
- Özdeğerlendirme (control self assessment)
- Sürekli denetim (continuous audit)



12:01 / 12:01

DÜZELTİCİ FAALİYET YÖNETİMİ

ISO 27001'de düzeltici faaliyet ve ilgili konular

- Standartta düzeltici faaliyet kavramı uygunsuzluk etrafında kullanılmaktadır.
- Ancak düzeltici faaliyet oluşturma, izleme ve gözden geçirme süreçleri risk değerlendirme sonuçlarından kaynaklanan risk işleme planından, olay / zayıflık ve gereksinimlerden de doğacak bulgu ve gereksinimlerin takibi için etkili bir yönetim imkanı sağlamaktadır.
- Bizim önerimiz (CobiT 4.1'de DS 5.2 BT Güvenlik Planı olarak da geçen) tüm bilgi güvenliği düzeltme, yeni geliştirme projelerinde oluşturulacak Düzeltici Faaliyet Yönetimi'nin kullanılmasıdır.
- Uygunsuzluğun (kök) nedenlerinin belirlenmesi, benzer uygunsuzlıkların var olup olmadığıının değerlendirilmesi (10.1.b)
- Tüm düzeltici faaliyetlerin etkinliğinin gözden geçirilmesi (10.1.d)
- Düzeltici faaliyet planı ve sonuçları ile ilgili yazılı kayıtların tutulması (10.1.f – g)



YÖNETİMİN GÖZDEN GEÇİRMESİ

YGG içeriği

Üst yönetim tarafından periyodik olarak gerçekleştirilmesi gereken YGG aktivitesinin standartda göre kapsamı aşağıdaki gibi olmalıdır:

- a) Önceki yönetimin gözden geçirmelerinden gelen görevlerin durumu,
- b) Bilgi güvenliği yönetim sistemini ilgilendiren dış ve iç konulardaki değişiklikler,
- c) Aşağıdaki gelişmeler dahil bilgi güvenliği performansına dair geri bildirim:
 - 1) Uygunluklar 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.

Ayrıca kararlar da kayıt altına alınmalıdır.



01:45 / 04:45

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ KURULUMU

Örnek proje adımları

- Proje ekibinin kurulması, proje ekibine ISO27001 eğitiminin verilmesi
- (Taslak) Kuruluşun bağlamı, ilgili tarafların ihtiyaç ve bekleyenlerin anlaşılması
- (Taslak) BGYS kapsamının belirlenmesi
- ISO27001 Ek-A Fark analizi ve varlıkların belirlenmesi
- Bilgi güvenliği risk değerlendirme sürecinin gerçekleştirilmesi ve onaylanması
- Kapsam, kuruluşun bağlamı ve ilgili tarafların bekleyenlerinin netleştirilmesi
- Hedeflerin ve bilgi güvenliği politikasının geliştirilmesi
- İzleme ve ölçme kriterlerinin, yöntemlerinin ve sorumluluklarının belirlenmesi
- Zorunlu BGYS dokümanlarının ve tasarlanan kritik süreçlerin dokümantasyonu, ilgili personele tebliği



03:51 / 04:45



BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ KURULUMU

Örnek proje adımları (DEVAM)

- Farkındalık eğitimlerinin gerçekleştirilmesi
- Acil güvenlik kontrollerinin uygulanması
- Güvenlik yatırımlarının planlanması ve şartnamelerinin hazırlanmasına destek
- İzleme ve ölçme faaliyetlerinin gerçekleştirilmesi
- Risk analizinin tazelenmesi
- İç tetkikin gerçekleştirilmesi
- Yönetim gözden geçirme toplantısının gerçekleştirilmesi ve kararların alınması
- Sürekli düzeltici faaliyet yönetimi
- Sürekli kontrollerin uygulanması
- Sürekli olay / zayıflık ve gereksinim yönetimi
- Sürekli doküman ve kayıt yönetimi



04:41 / 04:45

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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.



EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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 amacıyla bir politika ve destekleyici güvenlik önlemleri belirlenmelidir.
A.6.2.2	Uzaktan çalışma	Kontrol Uzaktan çalışma alanlarında erişilen, işlenen veya depolanan bilgiyi korumak amacıyla bir politika ve destekleyici güvenlik önlemleri uygulanmalıdır.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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 güncellemlerini almalıdır.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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 olanağıları 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.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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 ellişinde olan tüm kurumsal varlıkları iade etmelidirler.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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 düzenine göre geliştirilmeli ve uygulanmalıdır. 

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

A.8.3 Ortam işleme

Amaç: Ortamda depolanan bilginin yetkisiz ifşası, değiştirilmesi, kaldırılması ve yok edilmesini engellemek.

A.8.3.1	Taşınabilir ortam yönetimi	Kontrol Taşınabilir ortam yönetimi için prosedürler kuruluş tarafından benimsenen sınıflandırma düzenine göre uygulanmalıdır.
A.8.3.2	Ortamın yok edilmesi	Kontrol Ortam artık ihtiyaç kalmadığında resmi prosedürler kullanılarak güvenli bir şekilde yok edilmelidir.
A.8.3.3	Fiziksel ortam aktarımı	Kontrol Bilgi içeren ortam, aktarım sırasında yetkisiz erişim, kötüye kullanım ve bozulmaya karşı korunmalıdır.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

A.9 Erişim kontrolü

A.9.1 Erişim kontrolünün iş gereklilikleri

Amaç: Bilgi ve bilgi işleme olanaklarına erişimi kısıtlamak

		Kontrol
A.9.1.1	Erişim kontrol politikası	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.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

A.9.2.4	Kullanıcılarla 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.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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.
---------	-------------------------------	--

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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 kısıtlanmalıdır ve sıkı bir şekilde kontrol edilmelidir.
A.9.4.5	Program kaynak koduna erişim kontrolü	Kontrol Program kaynak koduna erişim kısıtlanmalıdır.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

A.10 Criptografi

A.10.1 Criptografik kontroller

Amaç: Bilginin gizliliği, aslına uygunluğu ve/veya bütünlüğü 'nın korunması için criptografi'nin doğru ve etkin kullanımın temin etmek

A.10.1.1	Kriptografik kontrollerin kullanımına ilişkin politika	<p>Kontrol</p> <p>Bilginin korunması için kriptografik kontrollerin kullanımına dair bir politika geliştirilmeli ve uygulanmalıdır.</p>
A.10.1.2	Anahtar yönetimi	<p>Kontrol</p> <p>Kriptografik anahtarların kullanımı, korunması ve yaşam süresine dair bir politika geliştirilmeli ve tüm yaşam çevirimleri süresince uygulanmalıdır.</p>

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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

		Kontrol
A.11.1.1	Fiziksel güvenlik sınırı	Hassas veya kritik bilgi ve bilgi işleme olanakları barındıran alanları korumak için güvenlik sınırları tanımlanmalı ve kullanılmalıdır.
A.11.1.2	Fiziksel giriş kontrolleri	Güvenli alanlar sadece yetkili personele erişim izni verilmesini temin etmek için uygun giriş kontrolleri ile korunmalıdır.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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 er noktaları ve diğer noktalar kontrol edilmeli ve mümkünse yetkisiz erişimi engellemek için bilgi işleme olanaklarından ayrılmalıdır.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

A.11.2 Teçhizat

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

		Kontrol
A.11.2.1	Teçhizat yerleştirme ve koruma	Teçhizat, çevresel tehditlerden ve tehlikelerden ve yetkisiz erişim fırsatlarından kaynaklanan riskleri azaltacak şekilde yerleştirilmeli ve korunmalıdır.
A.11.2.2	Destekleyici altyapı hizmetleri	Teçhizat destekleyici altyapı hizmetlerindeki hatalardan kaynaklanan enerji kesintileri ve diğer kesintilerden korunmalıdır.
A.11.2.3	Kablo güvenliği	Veri veya destekleyici bilgi hizmetlerini taşıyan enerji ve telekomünikasyon kabloları, dinleme, girişim oluşturma veya hasara karşı korunmalıdır.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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 kullanıcılaraya sağlanmalıdır.
A.12.1.2	Değişiklik yönetimi	Kontrol Bilgi güvenliğini etkileyen, kuruluş, iş prosesleri, bilgi işleme olanakları ve sistemlerdeki değişiklikler kontrol edilmelidir.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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 Kötüçül yazılımlardan koruma		
Amaç: Bilgi ve bilgi işleme olanaklarının kötüçül yazılımlardan korunmasını temin etmek.		
A.12.2.1	Kötüçül yazılımlara karşı kontroller	Kontrol Kötüçül yazılımlardan korunmak için tespit etme, engelleme ve kurtarma kontrolleri uygun kullanıcı farkındalığı ile birlikte uygulanmalıdır.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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.
----------	---------------	---

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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.
----------	---	---

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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 zayıfeti 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.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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.
----------	-------------------------------------	---

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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 üzerinden veya dış kaynak yoluyla sağlanmış olsun olmasın, ağ hizmetleri anlaşmalarında yer almalıdır.
A.13.1.3	Ağlarda ayrim	Kontrol Ağlarda, bilgi hizmetleri, kullanıcıları ve bilgi sistemleri grupları oluşturulmalıdır.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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 yansitan gizlilik ya da ifşa etmeye anlaşmalarının gereksinimleri tanımlanmalı, düzenli olarak gözden geçirilmeli ve yazılı hale getirilmelidir.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

A.14 Sistem temini, geliştirme ve bakımı

A.14.1 Bilgi sistemlerinin güvenlik gereksinimleri

Amaç: Bilgi güvenliğinin, bilgi sistemlerinin tüm yaşam döngüsü boyunca dâhil 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.
----------	---	--

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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 bütünlendirme girişimleri için güvenli geliştirme ortamları kurmalı ve uygun bir şekilde korumalıdır.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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 işlevsellüğünün 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.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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.
----------	--------------------------	--

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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.
----------	--	---

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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 teşhis, toplanması, edinimi ve korunması için prosedürler tanımlamalı ve uygulamalıdır.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

A.17 İş sürekliliği yönetiminin bilgi güvenliği hususları

A.17.1 Bilgi güvenliği sürekliliği

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

		Kontrol
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.
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.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

A.17.1.3	Bilgi güvenliği süreklilığı'nın 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.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

A.18 Uyum

A.18.1 Yasal ve sözleşmeye tabi gereksinimlerle uyum

Amaç: Yasal, meşru, düzenleyici veya sözleşmeye tabi yükümlülüklerle 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.

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

A.18.1.3	Kayıtların korunması	<p>Kontrol</p> <p>Kayıtlar kaybedilmeye, yok edilmeye, sahteciliğe, yetkisiz erişime ve yetkisiz yayımlamaya karşı yasal, düzenleyici, sözleşmeden doğan şartlar ve iş şartlarına uygun olarak korunmalıdır.</p>
A.18.1.4	Kişi tespit bilgisinin gizliliği ve korunması	<p>Kontrol</p> <p>Kişiyi tespit bilgisinin gizliliği ve korunması uygulanabilen yerlerde ilgili yasa ve düzenlemeler ile sağlanmalıdır.</p>
A.18.1.5	Kriptografik kontrollerin düzenlenmesi	<p>Kontrol</p> <p>Kriptografik kontroller tüm ilgili sözleşmeler, yasa ve düzenlemelere uyumlu bir şekilde kullanılmalıdır.</p>

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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.
----------	--	---

EK-A KONTROLLER

ISO27001'deki EK-A Maddeleri

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.