* Bir uygunluk değerlendirme kuruluşu ile ilgili olarak, belirli uygunluk değerlendirme işlerini yapmaya yeterli olduğunu resmi olarak ifade ~~eder~~ ederek gösteren, üçüncü taraf olarak beyanına Akreditasyon denir

* EA: Avrupa Akreditasyon Birliği
* UKAS: UK National Accreditation Body.
* APLAC: PAC + APLAC = APAC (Asia Pasific Accreditation Company)
  Pacific Accreditation Company + Asia Pasific Laboratory Accreditation Company

IAAC: Institute of Advanced Architecture of Catalonia ✗

* IAF: International Accreditation Forum:
  sistem belgelendirmeye yönelik akreditasyon kuruluşlarının yetkilendirilmesi ve karşılıklı tanıma anlaşması ile ilgili global organization.

ISO 17021: Sistem Belgelendirme Kuruluşları için Akreditasyon Standardı
ISO 17020: uygunluk değerlendirmesi – çeşitli tiplerdeki muayene kuruluşları işletimi şartları
ISO 17065: " – ürün, süreç ve hizmet belgelendirmesi yapan kuruluşlar için şartlar
ISO 17024: personel akreditasyon standardı

* ILAC: muayene ve laboratuvar akreditasyon kuruluşlarının yetkilendirilmesi ve karşılıklı tanıma anlaşması ile ilgili organizasyon
* Eğitim bir uygunluk değerlendirme faaliyeti değildir (Belgelendirme, muayene, test)
* IAF sistem belgelendirme kuruluşlarının verdiği belgelerin karşılıklı kabul edilmesi için MLA (MultiLateral Agreements - Çok Taraflı Anlaşmalar) yapmaya yetkilidir.
* ISO'nun konusu Elektrik ve Elektronik Mühendisliği standartları dışında her türlü standardizasyon alanını kapsar.
* DAkkS: Deutschland National Akkreditation Body

ISO 9001 kalite
ISO 27001 bilgi sistemleri
ISO 14001 çevre
} yönetim sistemleri belgelendirme standardı

* ISO 19011: Yönetim Sistemleri Denetim Standardı

Confidentiality: Gizlilik
Integrity: Tam, doğru, tutarlı, bütünlük
Availability: Erişilebilirlik, kullanılabilirlik

* Temel varlıklar Bilgi, iş süreçleri ve faaliyetlerdir
  Destekleyici varlıklar; donanım, yazılım, ağ, personel, işyeri, organizasyon yapısı vs.
* Gizli ile Özel farklı (Secret vs. Confidential)
* ISO 27001:2013, ISO 27001:2005'ten farklı olarak risklerin saptanmasının ön koşulu olarak açık bir biçimde varlıkların, tehditlerin ve zayıflıkların belirlenmesini gerektirmez. Bu bağlamda etkilerden daha ziyade sonuçlardan bahseder.
* Risk = Etki Şiddeti X Oluşma Sıklığı / Olasılık
  (şiddeti) (frekansı)
* ISO 31000 Risk yönetimi : ISO 27001:2013 değişikliği ile uyumlu kılınmaları amaçlanmıştır.
* KZFT Analizi: SWOT Analizi
* Uygulanabilirlik bildirgesi: Kuruluşun BGYS'si ile ilgili ve uygulanabilir kontrol amaçlarını ve kontrollerini açıklayan dokümante edilmiş bildirge uygulanabilirlik bildirgesidir.
* Riski hedefler üzerindeki belirsizlik etkisi
* Bilgi güvenliği yönetimi sistemi 10 şarttan oluşur ve bunlara uyum iddiasında bulunan bir organizasyonun madde 4-10 arasını hariç tutması kabul edilemez.
* Risk derecelendirme: Riskin önemini tayin etmek amacıyla tahmin edilen riskin verilen risk kriterleri ile karşılaştırılması
  Risk analizi: Kayıpları belirlemek ve riski tahmin etmek amacıyla bilginin sistemli kullanımı
  Risk değerlendirme: Risk analizini ve risk derecelendirmeyi kapsayan süreç.
  Risk yönetimi: Bir organizasyonda risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetler.
  Risk işleme: Riski değiştirmek için alınması gereken önlemlerin seçilmesi ve uygulanması süreci
  BGYS: Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek sürdürmek ve geliştirmek için iş riski yaklaşımına dayalı olan, tüm yönetim sisteminin bir parçasıdır.

0 Giriş
1 Kapsam
2 Atıf yapılan standartlar ve dokümanlar
3 Tanımlar ve Terimler
4 Kuruluşun yapısı
5 Liderlik
6 Planlama
7 Destek
8 Operasyon
9 Performans Değerlendirme
10 İyileştirme

Ek başlıklar

114 security controls

35 categories.

- A.5 Bilgi güvenliği politikaları → BG için yönetimin yönlendirilmesi
- A.6 Bilgi güvenliği organizasyonu → İç organizasyon
  - ↳ Mobil cihazlar ve uzaktan çalışma
- A.7 İK güvenliği → İstihdam öncesi
  - → Çalışma esnasında
  - → İstihdamın sonlandırılması ve değiştirilmesi
- A.8 Varlık yönetimi → Varlıkların sorumluluğu
  - → Bilgi sınıflandırma
  - → Ortam işleme
- A.9 Erişim kontrolü → Erişim kontrolünün iş gereklilikleri
  - ↳ Kullanıcı erişim yönetimi
  - ↳ Kullanıcı sorumlulukları
  - ↳ Sistem ve uygulama erişim kontrolü
- A.10 Kriptografi → Kriptografik kontroller
  - ↳ X
- A.11 Fiziksel ve çevresel güvenlik → Güvenli alanlar
  - ↳ Teçhizat
- A.12 İşletim güvenliği → İşletim prosedürleri ve sorumlulukları
  - ↳ Kötücül yazılımlardan korunma
  - ↳ Yedekleme
  - ↳ Kaydetme ve izleme
  - → İşletimsel yazılımın kontrolü
  - → Teknik açıklık yönetimi
  - ↳ Bilgi sistemleri tetkik hususları
- A.13 Haberleşme güvenliği → Ağ güvenliği yönetimi
  - ↳ Bilgi transferi
- A.14 Sistem temini, geliştirme ve bakımı → Bilgi sistemlerinin güvenlik gereksinimleri
  - ↳ Geliştirme ve destek süreçlerinde güvenlik
  - ↳ Test verisi
- A.15 Tedarikçi ilişkileri → Tedarikçi ilişkilerinde bilgi güvenliği
  - ↳ Tedarikçi hizmet sağlama yönetimi
- A.16 Bilgi güvenliği ihlal olayı yönetimi → BG ihlal olaylarının ve iyileştirmelerinin yönetimi
- A.17 İş sürekliliği yönetiminin BG hususları → BG sürekliliği
  - ↳ Yedek fazlalıklar
- A.18 Uyum → Yasal ve sözleşmeye tabi gereksinimlerle uyum.
  - ↳ Bilgi güvenliği gözden geçirmeleri

*BGYS kapsam belirlenirken mali ve ekonomik hususlar dikkate alınmak zorunda değildir.
*ISO 27001 Ek A hariç tutulabilir.
*Sürekli iyileştirme önerilir
*BGYS'nın ölçülebilir amaçlar ve vizyon içermez. Üst yönetim tarafından oluşturulur. ~~oluşturulmaz~~.
*Üst yönetim BGYS politikasını ve BG amaçlarını oluşturur.
*BG politikası elektronik olarak hazırlanma zorunluluğu yoktur.

---

*Kaçınma, risk alma, yok etme, risk sonuçlarını değiştirme ve paylaşma risk iyileştirme seçenekleri arasındadır.
*Risk değerlendirmesi; Risk analizi süreci esnasında bulunan risk seviyesini, risk kriterleri ile karşılaştırmayı kapsar.
*Bilgi güvenliği amaçlarının planlanması; ne yapılacak, hangi kaynaklar kullanılacak ve kim sorumluğu kapsar, ne zaman gözden geçirileceği kapsanır.
*Personelin yeterliliğinin sağlanması için Eğitim, yol gösterme ve görev değişikliği uygulanabilir, ancak işten çıkarma bu kapsamda değildir.
*İç ve dış iletişim belirlenirken iletişimin hangi perspektife gerçekleşeceğinin belirlenmesi zorunlu değildir.
*Yeni bir dokümanın oluşturulacağı ya da güncelleneceği zaman formatın belirtilmesi zorunludur.
*Kurulu sistemin teknik şartları ile uyumlu olup olmadığını tespit etmek için iç tetkikler gerçekleştirmez. Kendi şartları ile uyumu tetkik edebilir.
*Üst yönetim BGYS'nin sürekli uygunluğunu, doğruluğunu ve etkinliğini temin etmek amacıyla planlanan aralıklarla gözden geçirmelidir.
*İç iletişim ve Düzeltici toplantıları yönetim gözden geçirmesinde ele alınmaz.

Kapsar:
- Bilgi güvenliği risk işleme sürecinin tanımlanması ve uygulanması
- Seçilen BG risk işleme seçeneklerinin uygulanması
- BG risk işleme planının formüle edilmesi
- Risk değerlendirme sonuçları ele alınarak uygun BG risk işleme seçeneklerinin belirlenmesi

X
- BG risk işleme planına dair üst yönetimin onayının alınması ve artık BG risklerinin kabulünü kapsamaz

---

Madde numaralandırmada en sona - koyulmuyor madde ismi yazılmıyor
alt madde harfi yazılıyor.

1. Kapsam
2. Atıf yapılan standart ve/veya dokümanlar
3. Terimler ve tarifler
4. Kuruluşun bağlamı
    4.1. Kuruluşun ve bağlamın anlaşılması
    4.2. İlgili tarafların ihtiyaç ve beklentilerinin anlaşılması
    4.3. Bilgi Güvenliği Yönetim Sisteminin kapsamının belirlenmesi
    4.4. BGYS
5. Liderlik
    5.1 Liderlik ve bağlılık.
    5.2 Politika
    5.3 Kurumsal roller, sorumluluklar ve yetkiler
6. Planlama
    6.1 Risk ve fırsatları ele alan faaliyetler
    6.2 BG amaçları ve bu amaçları başarmak için planlama.
7. Destek
    7.1. Kaynaklar
    7.2 Yeterlilik
    7.3 Farkındalık
    7.4. İletişim
    7.5. Yazılı Bilgiler
8. İşletim
    8.1. İşletimsel planlama ve kontrol
    8.2. Bilgi Güvenliği risk değerlendirme
    8.3. BG risk işleme
9. Performans Değerlendirme
    9.1. İzleme, ölçme, analiz ve değerlendirme
    9.2. İç tetkik
    9.3. Yönetimin gözden geçirmesi
10. İyileştirme
    10.1 Uygunsuzluk ve düzeltici faaliyet
    10.2. Sürekli iyileştirme.

ISO 19011:2018 Denetim Yönetimi Sistemi

KYS: Kalite Yönetimi Sistemi
GYS: Çevre Yönetimi Sistemi

* Teknik uzmanlar tetkikçilere dahil değil.
* Tetkik delilleri → Değerlendirme → Tetkik Bulguları → Gözden Geçirme → Tetkik Sonuçları
  (kanıtları) (Tetkik kriterlerine göre)

Bilgi Toplama (Bilgi Toplama & Doğrulama Süreci)
↑
Bilgi Kaynağı

* KD KKD: Kişisel Koruyucu Donanım
* Örnekleme planı: Özellik tabanlı örnekleme / Değişken tabanlı örnekleme
* Muhakemeye dayanan örneklemeye vs. İstatistiksel örnekleme
* ISO/TC 176 kalite yönetimi ile ilgili standartlar
* ISO/TC 207 çevre yönetimi " " "
* OHSAS iş sağlığı ve güvenliği " " "
  IEC
  ISO 27000 : standart serisi
  ISO/IEC 27001 : BGYS standardı
  ISO/IEC 27002 : BGYS için uygulama kodları standardı (yönetim sistemi değildir)
  ISO/IEC 27003 : BGYS için uygulama ve gerçekleştirme kılavuzu
  ISO/IEC 27004 : BGYS için ölçekler ve raporlar standardı
  ISO/IEC 27005 : BGYS için risk yönetimi standardı
  ISO/IEC 27006 : BGYS için denetim ve belgelendirme için şartlar standardı
* ISO/IEC JTC 1/2C27 bilgi güvenliği yönetimi ile ilgili standartlar
* ISO/IEC 27799 Sağlık Bilişimi BGYS
* ISO/IEC 18044 Bilgi güvenliği ihlal olayı yönetimi standardı
* İç tetkik: 1. taraf tetkik belgelendirme esaslı değildir.
  Özellikle küçük kuruluşlarda bağımsızlık, yansızlıktan ve çıkar çatışmalarından uzak olma, tetkik edilen faaliyetler sorumlu olmama olarak açıklanabilir.
* dış tetkik
  2. taraf tetkik: Müşteriler gibi kuruluşta çıkarı olan taraflarca ya da onlar adına başka kişilerce yapılır. Belgelendirme esaslı değildir.
  3. taraf tetkik: Düzenleyici ya da belgelendirme yapan kuruluşlar gibi bağımsız tetkikçiler tarafından yapılır. Belgelendirme esaslıdır.
* Bileşik tetkik: Birden fazla yönetim sistemi (Entegre tetkik)
* ortak tetkik: Birden fazla tetkik kuruluşu (Müşterek tetkik)

* Gözlemci, rehber
* uygunluk / uygunsuzluk
* Tetkik prensipleri: Bütünlük (Dürüstlük), Adil Sunum (ayrıntılar görüş ayrılıkları), Profesyonel özen, Gizlilik
Bağımsızlık, Delile dayalı yaklaşım, Risk temelli yaklaşım (risk ve fırsatlar)

* yönetim sistemi tetkiklerinin sürdürülmesi için ISO/IEC 17023'te yer alan kılavuzlar kullanılabilir
* NACE: Nomenclature for Economic Activities: Ekonomik aktiviteler için bilimsel adlandırma
* gidiş-geliş süreleri tetkik süresi hesaplamasına ilave edilmez
* Çoklu alan (multi-site) tetkiki için örnekleme ekstü belirlenmesi
ilk belgelendirme tetkiki: Numune ekstü = $\sqrt{}$Alan sayısı + Merkez ofis
gözetim tetkiki : " " = 0,6 x $\sqrt{}$ Alan sayısı + Merkez ofis
yeniden belgelendirme tetkiki: " " = 0,8 x $\sqrt{}$ Alan sayısı + Merkez ofis
(en yakın tam sayıya yuvarlanır)

* Tetkik edilen tetkike ilişkin bir tavsiyi belirtir.
* Azana 1 tetkik + Azana 2 tetkik = İlk belgelendirme tetkiki
resmi tetkik planı gerekmez
Sahada gıda masa başında olur
aralarında makul süre olmalı
şartların tamamının karşılanması gerekmez
* Tetkik yürütülürken dokümanın gözden geçirilmesinde dokümanların tam, doğru, tutarlı ve geçerli olmasına dikkat edilmelidir.
* Tetkik edilen ile tetkik müşterisi farklı olabilir.
* Uygunsuzluklar: Majör / Minör / Gözlemler → İleride minör uygunsuzluk olma riski var.
uygunsuzluk değildir.
* Tetkik ekibi lideri baş denetçi midir?
* Entegre tetkik: Bileşik tetkikle aynı (combined)
* Müşterek tetkik: ortak tetkikle aynı (joined)
* Objektif kanıt: gözlem, ölçüm, test yada başka yollarla elde edilebilir
* Kayıtlar ve ifadeler tetkik kanıtlarıdır.
* Etkililik planların faaliyetlerin gerçekleştirilme derecesi ve planların sonuçların elde edilmesi
* Gözlemci tetkik ekibinin bir üyesi değildir
Ekip: Teknik uzman, Baş tetkikçi, Tetkikçi.

A.1 Tetkik metotlarının uygulanması
A2. Tetkikte süreç yaklaşımı
A3. Profesyonel muhakeme
A.4 Performans sonuçları
A.5 Bilginin doğrulanması
A.6 Örnekleme
A.7. Bir yönetim sistemi içinde uygunluğun tetkik edilmesi
A.8. Bağlamın tetkiki
A.9 Liderlik ve taahhüdün tetkik edilmesi
A.10. Risk ve fırsatların tetkiki
A.11 Yazım denetimi
A.12. Tedarik zinciri tetkiki
A.13. Tetkik çalışma dokümanlarının hazırlanması
A.14. Bilgi kaynaklarının seçilmesi
A.15. Denetlenen lokasyona ziyaret
A.16 Uzak (sanal) faaliyet ve lokasyonların tetkik edilmesi
A.17 Mülakat gerçekleştirme
A.18 Tetkik bulguları

Tetkik yapmak için gerekli bilgi ve beceriler sektöre özel örnekler

* Rehber, tetkik edilen kuruluş tarafından tetkik ekibine yardımcı olması için görevlendirilmiş kişidir.
* Adil Sunum Dürüst Sunum olarak da geçiyor
* Adil Sunum tüm ve gerçeğe yakın rapor verme zorunluluğudur.
  Profesyonel özen tetkikte titizlik ve muhakeme etmektir. Gerekçeli hüküm verebilmektir.
  Bağımsızlık yanlılık ve çıkar çatışmasından arınmış olarak hareket etmektir.
* Tetkik süresi hesaplama ? ***
* Dokümanlara erişim ve tetkik yapma yetkisi tayini İlk temasın organizasyonudur
* Tetkike katılacak personel ve bilgileri tetkik planında bulunması gerekmez
* Mevcut tetkik delilleri tetkik hedefine ulaşılmasının mümkün olmadığını gösterirse tetkik sonlandırılır, tetkik planı tekrar teyit edilir gerekirse değiştirilir veya tetkik hedefleri / kapsamında değişikliğe gidilir. Tetkik ekibi değiştirilmez
* Bilgi toplama yöntemleri: Kayıtlar dahil dokümanların gözden geçirilmesi, görüşmeler ve gözlemler. Denetçi toplantıları bilgi toplama yöntemi değildir.

* Kapanış toplantısında tetkik sürecinin doğasında var olan belirsizlik dikkate alınarak tetkik sonuçlarında mutabık kalınır - ana tetkik planında yoksa tavsiye hazırlanmaz.

* Tetkik ekibinin kabiliyeti ve etkinliği tetkik sonuçlarında ele alınma konumunda değildir.

* Çözülemeyen görüş ayrılıkları kaydedilir - (raporda) Uygunsuzluklar kaydedilir - Çözümlemek zorunda değildir

*

collapse of Barings Bank

Segregation of duties.

public → internal use → confidential → top secret

access control need to know & need to use

Everything is generally forbidden unless it is expressly permitted ✓
not vice versa ✗

symmetric → single key } cryptography
assymmetric → public key

* blog of Panayiotis Vryonis cryptography

* ISO 11770 – Key management Cryptography.

tampered: kurcalanmış
revoke: feshedilmek.

* ISO 27033 Network security

* ISO 27035 Incident management

* point of contact: for security events. (it can be a department)

* ISO 27037 guideline for identification, collection, acquisition and preservation of digital evidence

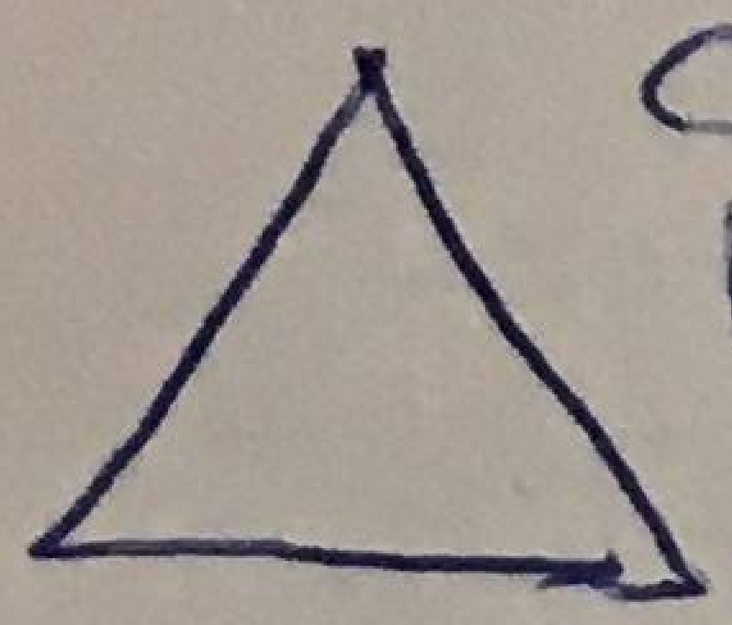
* ISO 22301 – Business Continuity Management System

* privacy officer

ISO 27002 <u>guidance for the implementation</u> of controls in Annex A of ISO 27001
↓
15 parts

Annex A – list of control objectives & controls for IS

ISMS: Information Security Management System



Confidentiality
Integrity
Availability – DDoS

27000 – general overview terms & definitions
27003 – general guidance for implementation of ISMS
27004 – advice to monitor & measure ISMS guideline
27005 – guidance for risk management
27006 – audit & certification of ISMS
27007 – guideline of audit ISMS
27011 – telecommunication of sector security controls
27015 – IS for financial services.

Context of the organization: External issues / Internal issues / Interested Parties & their needs & expectations

---

management support is vital for ISMS
nominate a person or structure responsible for ISMS → top management
risk level: impact x likelihood

ISO 31000
ISO 31010 } Standards on risk assessment
ISO 27005

---

risk treatment (avoid, control, transfer, accept... (izleme?))

EK A → kontroller sayfası
Statement of Applicability SoA → nelerin kurulacağı tutulacağını, uygulanacak olduğunu söyler.
Risk treatment plan: actions, who is in charge, risk and its level, budget, timeframe
IS objectives: timeframe, evaluation of results, responsible person, resources, things to do
Lower level policies should be documented.
nonconformities and corrective actions should be documented.
retention period is important