
BUREAU VERITAS
1828
BUREAU
VERITAS
ISO27001:2022'
YE DOĞRU
GEÇİŞ İÇİN HAZIRLIK
ŞUBAT 2023

AGENDA

01

BUREAU VERITAS & CYBERSECURITY

- ISO27001 Bureau Veritas Portfolyosu

02

ISO27001:2022 İÇİN ARKA PLAN

- The ISO 27000 serisi standartlar
- The ISO 27001 & ISO27002

03

SON GELİŞİMLER & YENİ GEREKLİLİKLER

- ISO27001:2022
- 27001 rehberinin gelişimi– Şubat 2022

04

GEÇİŞ PLANI

BUGÜNKÜ KONUŞMACILAR

Şahin Soysal
BV Türkiye
BGYS –Başdenetçi & Eğitmen

Dr. Duygu Hakan
BV Türkiye
BGYS -Ürün Müdürü & Başdenetçi& Eğitmen

Ozan Susuzlu
BV Türkiye
Belgelendirme Departmanı Satış Müdürü

01

BUREAU VERITAS & SİBER GÜVENLİK

BUREAU VERITAS TURKIYE

1992 yılında ilk ofis İstanbul olmak üzere,

Ankara, **İzmir**, **Bursa**, **Mersin** ve **Antalya'da** 6 yerel ofisi ile 30 yıldır test, gözetim ve belgelendirme hizmetleri müşterilere sunulmaktadır

- Toplam çalışan sayısı 250 civarı olup, belgelendirme departmanında 35 kişilik ekip bulunmaktadır.

- Tüm Türkiye'de toplamda 1.200'den fazla müşteri

- Tüm Türkiye'de toplam +150 farklı standardlarda denetçi

* As of June 30, 2022

BUREAU VERITAS BELGELENDİRME

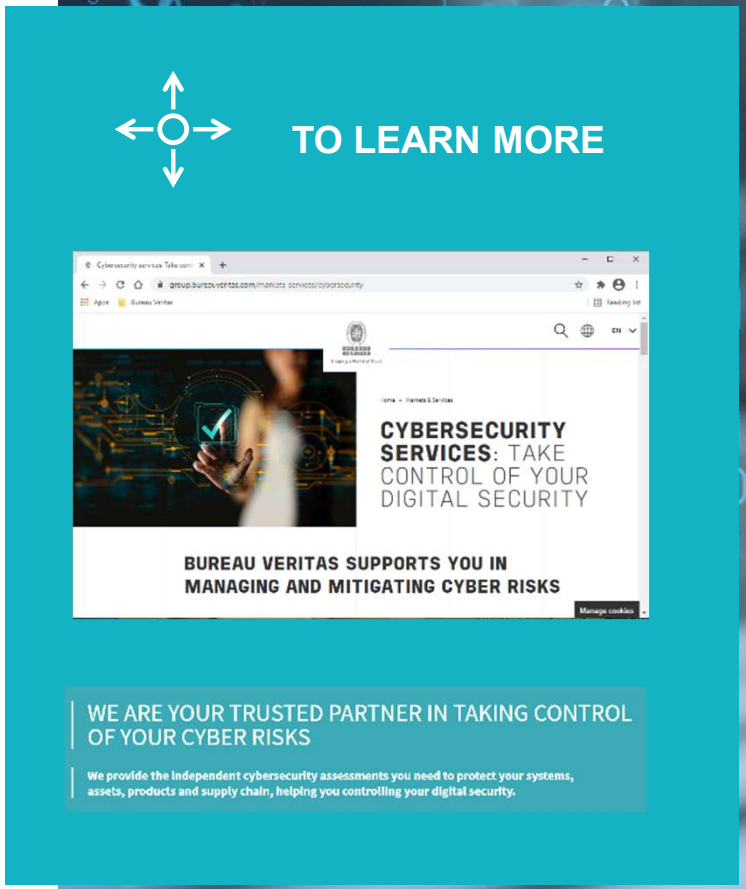
KURUMSAL RİSKİ KAPSAYAN

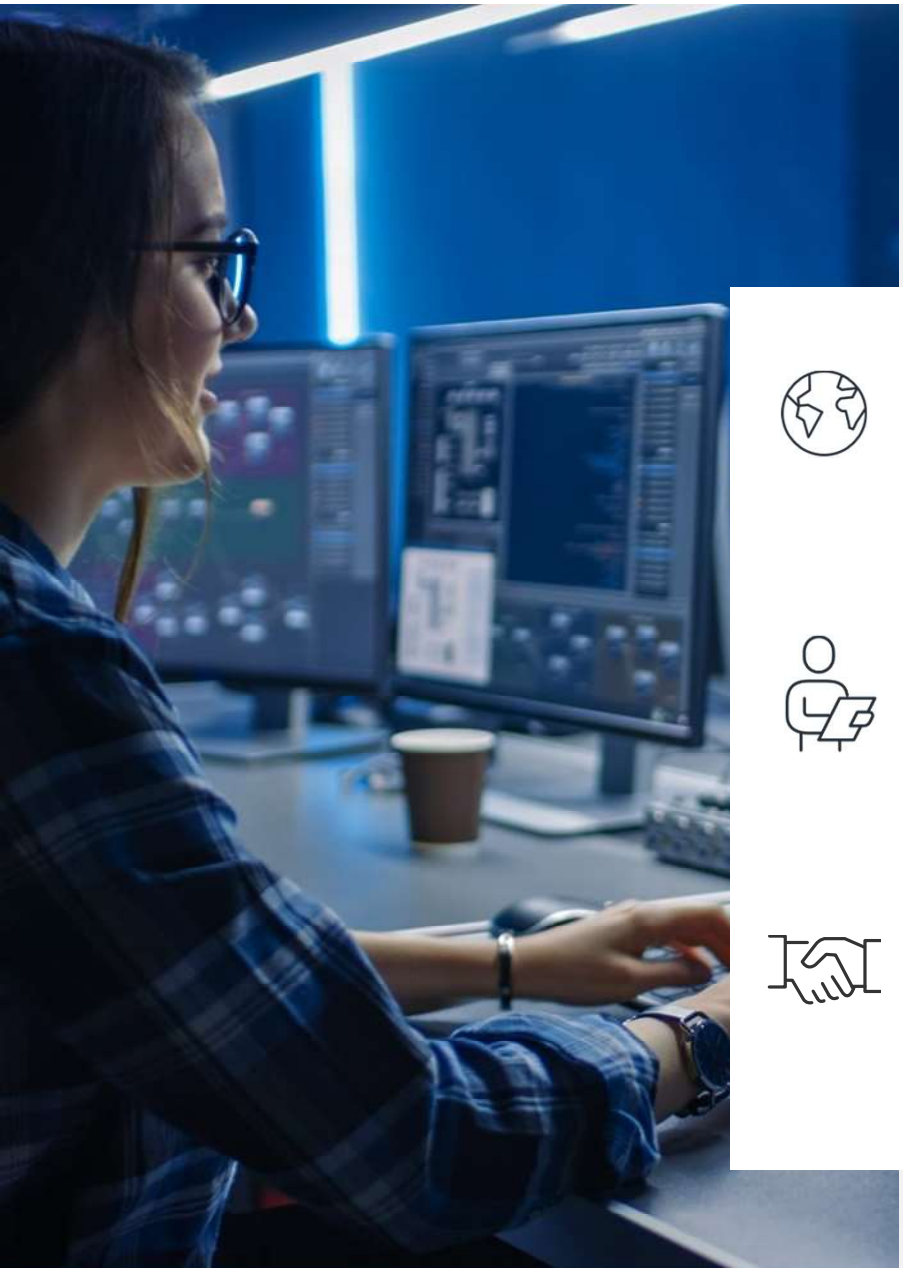
Standartlar aşağıdaki gibidir:

- **ISO27001** Bilgi Güvenliği
- **ISO27701** GDPR Veri Koruması
- **ISO31000** Risk Yönetimi
- **ISO22301** İş Sürekliliği
- **ISO37001** Yolsuzlukla Mücadele
- **ISO55000** Varlık Yönetimi
- **ISO22237** Veri Merkezi Tasarımı & Operasyon

Aşağıdakiler ile eksiksiz bir hizmet yelpazaesi sunar:

- Belgelendirme
- Gözetim ve İçdenetimler
- Özel denetimler
- Mevcut Durum Analizleri
- Eğitim Akademisi





BUREAU VERITAS - SECURA

DİĞER SİBER HİZMETLER

GLOBAL SİBER GÜVENLİK ŞİRKETİ

- 2001 yılında kurulan, Eindhoven ve Amsterdam'da ofisler
- 100+ çalışan
- 2021'den beri Bureau Veritas grubunun üyesi

DİJİTAL GÜVENLİK KONUSUNDA BİLGİ SAĞLAMAK

BT, Nesnelerin İnterneti ve OT (Operasyonel Teknoloji) için denetim, test ve belgelendirme hizmetleri. Fidye Yazılımı, Bulut Güvenliği, Etik Hacking vb. gibi çeşitli konularda teknik uzmanlar.

SEKTÖRDE TANINMIŞ

Enerji, kamu hizmetleri, petrol ve gaz, teknoloji, sağlık, finans, otomotiv ve ulaşım gibi geniş sektör yelpazesinde güçlü uzmanlığa sahip sektörler arası yaklaşım.

SECURA, BV ŞİRKETİ

DAYANIKLIĞINIZI ARTIRIN

ÇALIŞAN

- Güvenlik farkındalığı
- Eğitim ve E-Öğrenme
- Kimlik Avı Testleri
- S.A.F.E. Davranış Programı

SÜREÇ

- Güvenlik Olgunluğu İncelemesi
- NIS Direktifi uyumluluğu
- Masaüstü kriz simülasyonu
- BT/OT risk ve tesis değerlendirmesi
- BT/OT yönetişimi (stratejiler, politikalar, olay müdahalesi)
- Vendor Değerlendirmesi

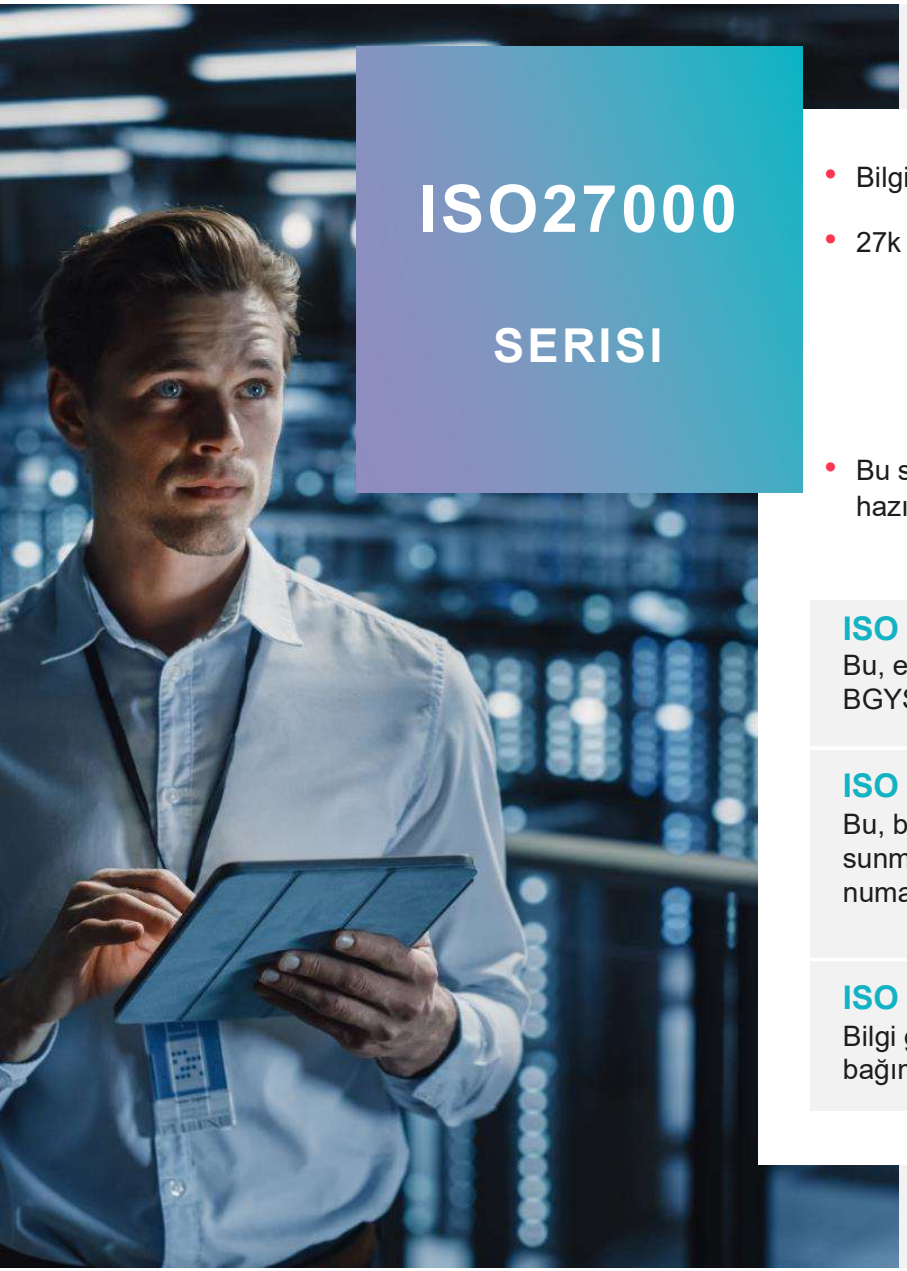
TEKNOLOJİ

- Tehdit modelleme
- BT/OT güvenlik açığı değerlendirmeleri ve sızma testleri
- Tasarım/yetenek incelemesi, konfigürasyon incelemesi, kod incelemesi
- Ürün sertifikası (IEC 62443, Ortak Kriterler, Radyo Direktifi)

Red Teaming Fidye Yazılımı Dayanıklılık Değerlendirmesi

02

ISO27001:2022 İÇİN ARKA PLAN



ISO27000

SERISI

- Bilgi Güvenliği Yönetim Sistemi (**ISMS**) ailesi standartları.
- 27k serisi sayesinde kuruluşlar, yönetim için bir çerçeve geliştirebilir ve uygulayabilir.:
  - finansal bilgiler, fikri mülkiyet ve çalışan detayları dahil olmak üzere bilgi varlıklarının güvenliği veya
  - Müşteriler veya üçüncü şahıslar tarafından kendilerine emanet edilen bilgiler.
- Bu standartlar, bilgilerin korunmasına uygulanan BGYS'lerinin bağımsız bir değerlendirmesine hazırlanmak için de kullanılabilir.

ISO 27001
Bu, eski BS7799-2 standardının yerini alan bir BGYS'nin özelliğidir.

ISO 27002
Bu, orijinal olarak ISO 17799 standardının 27000 serisi standart numarasıdır.

ISO 27003
Bu, bir BGYS'nin uygulanması için rehberlik sunmayı amaçlayan yeni bir standardın resmi numarası olacaktır.

ISO 27004
Önerilen ISO27002 ile uyumlu kontroller dahil olmak üzere bilgi güvenliği sistemi yönetimi ölçümünü ve metriklerini kapsar.

ISO 27005
Bilgi güvenliği risk yönetimi için metodolojiden bağımsız ISO standardı

ISO 27006
BGYS sertifikası sunan kuruluşların akreditasyonu için yönergeler sağlar.

ISO27000 SERIES

27001 & 27002’ E ODAKLANALIM

27001

- Sertifikalandırılabilir
- Bir gereksinim listesi belirler (“Shall”)
- Bölüm 6.1 risk bazlı yaklaşımla aşağıdakileri tanımlar:

  Her kuruluşun risk profiline göre (örn. olasılık x şiddet)

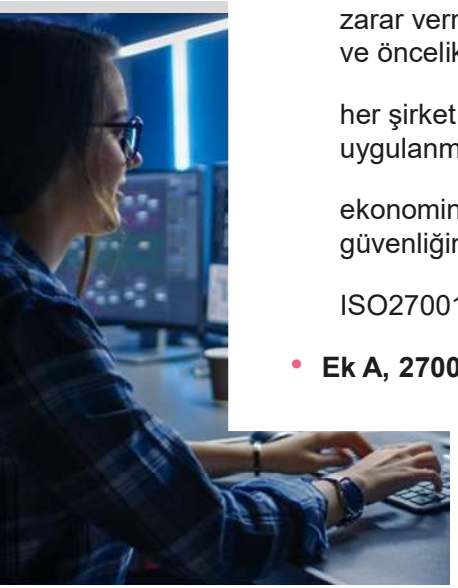
  zarar verme potansiyeline sahip riskleri ele aldı (analizler ve öncelikler)

  her şirket için uygun kontrol prosedürlerinin uygulanmasını talep eder;

  ekonominin "Maliyet-Fayda" analizi kavramına bilgi güvenliğinin yanıtıdır.

  ISO27001:2013 10 madde + Annex A içerir.

- **Ek A, 27002 ile uyumlu kontrolleri içerir.**



27002

- Sertifikalandırılamaz
- Siber güvenliğini güçlendirmek isteyen her tür şirket tarafından takip edilebilecek kontrollerin (veya önlemlerin) bir listesini içeren yönergeler (“Gerekir”) oluşturur.
- ISO27001 standardı Ek A'da listelenen kontrollerin uygulanmasına yönelik rehberlik sunar
- Şubat 2022'de yeni bir sürüm yayınlandı (ISO 27002:2013'ü geri çekiyor)

Yeni bir sürüm, ISO27001'in Ek A'sının güncellenmesi gerektiğini ima eder.

03

SON GELIŞMELER VE YENI GEREKLİLİKLER

ISO27001:2022 WHAT'S NEW?

Information technology
-
Security techniques

Information security, cybersecurity and privacy protection

Major changes in the updated revision of the standard

- **Başlık**: ISO/IEC 27001:2022 Bilgi Güvenliği, Siber Güvenlik ve Gizlilik Koruması
- **Annex A of ISO/IEC 27001** ISO/IEC 27002:2022 ile uyumlu
- **4'ten 10'a kadar olan maddeler** önceki 2013 baskısında olduğu gibi kalır

Ek A ile ilgili notlar hariç

ISO27002:2022

WHAT'S NEW?

→

Ana değişiklikler aşağıdaki gibidir:

- Standart başlığı güncellendi;
- Doküman yapısı değiştirildi; kontroller basit bir taksonomi ve ilişkili öznitelikler kullanılarak sunuldu.
- bazı kontroller birleştirildi ve birkaç yeni kontrol eklendi. Tam yazışma Ek B'de bulunabilir.

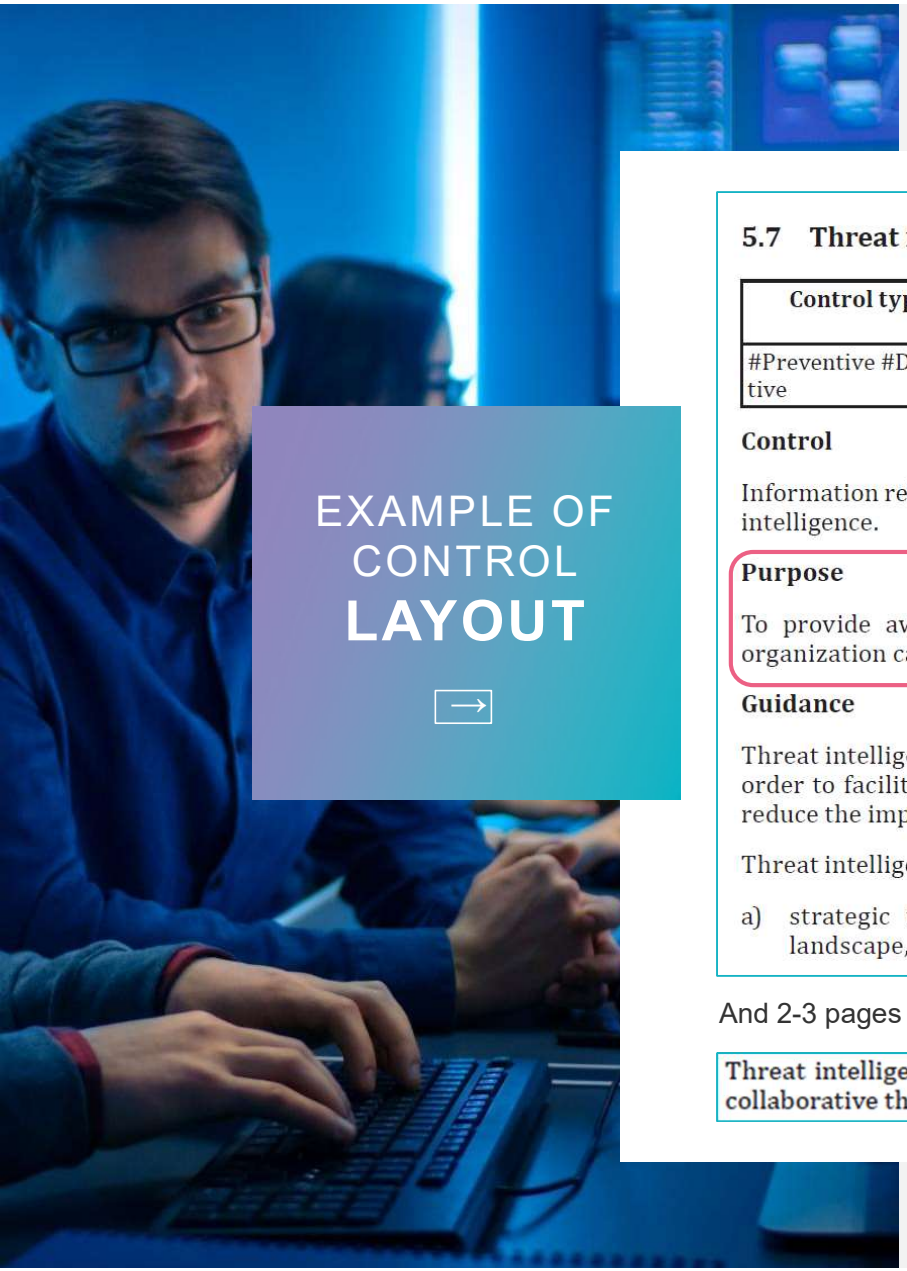
ISO 27002 YENİ YAPISI

- Kontrol noktaları **114 ten 93 e indirildi.**
- **4 domains (4 ANA BAŞLIK)**
  - Organizasyonel (Madde 5)
  - Kişisel (Madde 6)
  - Fiziksel (Madde 7)
  - Teknolojik (Madde 8)

Organizational controls

5.1	Policies for information security
5.2	Information security roles and responsibilities
5.3	Segregation of duties
5.4	Management responsibilities
5.5	Contact with authorities
5.6	Contact with special interest groups
5.7	Threat intelligence

- Her kontrol, **aşağıdakileri içerir**:
  - Control title
  - **Attribute table** ← New
  - Control text
  - **Purpose** ← New
  - Guidance
  - **Other information** ← New



EXAMPLE OF CONTROL **LAYOUT**

5.7 Threat intelligence

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Confidentiality #Integrity #Availability	#Identify #Detect	#Threat_and_vulnerability_management	#Defence #Resilience

Control

Information relating to information security threats should be collected and analysed to produce threat intelligence.

Purpose

To provide awareness of the threat environment that can impact the organization so that the organization can take appropriate mitigation actions.

Guidance

Threat intelligence is about collecting and analysing information about existing or emerging threats in order to facilitate informed actions to prevent the threats from causing harm to the organization, or reduce the impact of such threats.

Threat intelligence can be divided into three layers, which should all be considered:

a) strategic threat intelligence: exchange of high-level information about the changing threat landscape, e.g. types of attackers or types of attacks;

And 2-3 pages later … **Other information**

Threat intelligence is often provided by independent providers or advisors, government agencies or collaborative threat intelligence groups.

KONTROL NOKTALARI-YENİ YAPI

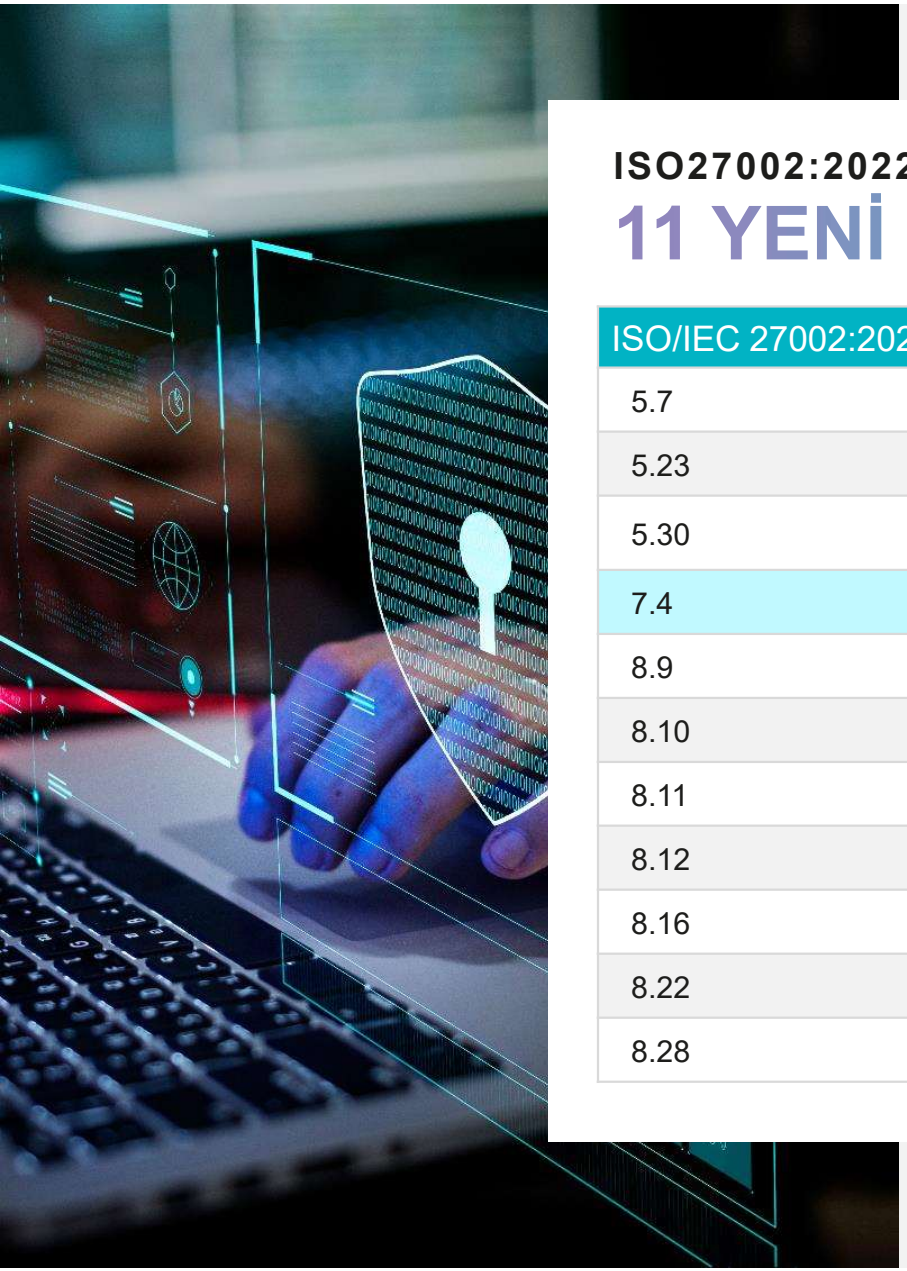
14 domains & 114 Controls

A.5	Information security policies (2 controls)
A.6	Organization of information security (7 controls)
A.7	Human resource security (6 controls)
A.8	Asset management (10 controls)
A.9	Access control (14 controls)
A.10	Cryptography (2 controls)
A.11	Physical and environmental security (15 controls)
A.12	Operations security (14 controls)
A.13	Communications security (7 controls)
A.14	System acquisition, dev. and maint. (13 controls)
A.15	Supplier relationships (5 controls)
A.16	Information security incident management (7 controls)
A.17	business continuity management (4 controls)
A.18	Compliance (8 controls)

11 YENİ KONTROL

82 REV. KONTROL

4 Yeni Başlık & 93 Kontrol Noktası



ISO27002:2022

11 YENİ KONTROL

ISO/IEC 27002:2022	Kontrol Adı	Kontrol Başlığı
5.7	Tehdit İstihbaratı	#Organizational_control
5.23	Bulut hizmetlerinin kullanımı için bilgi güvenliği	#Organizational_control
5.30	İş sürekliliği için Bilgi ve İletişim Teknolojisileri(ICT) hazırlığı	#Organizational_control
7.4	Fiziksel Güvenlik İzleme	#Physical_controls
8.9	Konfigürasyon Yönetimi	#Technological_control
8.10	Bilgi silme	#Technological_control
8.11	Veri maskeleme	#Technological_control
8.12	Veri sızıntısı önleme	#Technological_control
8.16	İzleme faaliyetleri	#Technological_control
8.22	Web filtreleme	#Technological_control
8.28	Güvenli Kodlama	#Technological_control

Canlandırıcı bir yenilik, her ölçüm/kontrol için bir dizi temanın ve özelliğin eklenmesidir.

AMAÇ

1) Kontrollerin farklı bir perspektiften veya temadan kategorize edilmesi

2) Nitelikler, gerektiğinde farklı görünümleri filtrelemek, sıralamak veya sunmak için kullanılabilir

KONTROL ÖZELLİKLERİ

- KONTROL TİPİ
- BGYS ÖZELLİKLERİ
- SİBER GÜVENLİK KAVRAMLARI
- OPERASYONEL YETENEKLER
- GÜVENLİK ALANLARI

A DETAILED VIEW ON
CONTROL TYPES & ATTRIBUTES

CONTROL TYPES	**#Önleyici, #Tarayıcı, #Düzeltici**)
IS PROPERTIES	**#Gizlilik, #Bütünlük, #Erişilebilirlik**
CYBERSECURITY CONCEPTS	ISO/IEC TS 27110 standard. **#Tanımlamak, #Korumak, #Tespit Etmek, #Cevap Vermek, #Kurtarmak** (Is also an alignment against NIST Cybersecurity Framework version 1.1)
OPERATIONAL CAPABILITIES	**#Yönetim #Varlık Yönetimi, #Bilgi Koruma, #İnsan Kaynakları Güvenliği, #Fiziksel Güvenlik, #Sistem ve Ağ Güvenliği, #Uygulama Güvenliği, #Konfigurasyon Güvenliği, #Kimlik ve Erişim Yönetimi, #Tehdit ve Güvenlik Açığı Yönetimi, #Süreklilik, #Tedarikçi İlişkileri Güvenliği, #Yasal Uyumluluk, #Bilgi Güvenliği Olay Yönetimi #Bilgi Güvenliği Güvencesi**
SECURITY DOMAINS	Güvenlik Etki Alanları, Birlik genelinde ağ ve bilgi sistemlerinin yüksek düzeyde ortak Siber güvenlik önlemleriyle ilgili NIS Direktifi (AB) 2016/1148'den türetilmiştir.**#Yönetim ve Ekosistem, #Koruma, #Savunma, #Dayanıklılık**

BUREAU VERITAS BELGELENDİRME

GEÇİŞ AŞAMALARI?

AGENDA-AKREDİTASYON GEÇİŞİ

ISO27001:2022'nin yayınlanması 3 yıllık bir geçiş dönemini başlatır (31 Ekim 2025'e kadar tamamlanacak):

25 Ekim 2022 tarihinde ISO 27001:2022 yayınlandı.

- Sonra:
  - Uluslararası Akreditasyon Forumu geçiş kılavuzlarını yayınladı
  - Akreditasyon Kuruluşları (AB) geçiş yönergelerini yayınladı
  - Belgelendirme Kuruluşları, AB'lerine bağlı olarak yeni standardı (ISO27001:2022) yayınlamaya başlar.– En geç Ekim 2023

- 31 Ekim 2025 tarihi sonrası BV Türkiye **yeni** (recert/cert) ISO 27001:2013 sertifikaları vermeyi durduracaktır. Bunun sağlanabilmesi için en az 3 ay öncesinde eski versiyon denetimlerin tamamlanıp uygunsuzluklar var ise kapatılmış olması gerekmektedir.

GEÇİŞİNİZİ YÖNETİN

- Standardı ISO.ORG tan indirin.
- Yeni kontrollerin sizin için geçerli olup olmadığını kontrol etmek için risk değerlendirme planını gözden geçirin
- Yeni standarda referanslarla **Uygulanabilirlik Bildiriminizi** oluşturun
- Yeni niteliklere karşı Operasyonel Yeteneklerinizi değerlendirin

BUREAU VERITAS BELGELENDİRME

GEÇİŞ AŞAMALARI?

AGENDA- AKREDİTASYON GEÇİŞİ

- **1 Kasım 2023** tarihi itibari ile eski versiyon üzerinden belgelendirme denetimi (ilk kez belge) **gerçekleştirilmeyecektir.**
- Bu tarih itibari ile teklifler ISO 27001:2022 versiyonu olarak düzenlenecektir.

GEÇİŞİNİZİ YÖNETİN

- Standardı ISO.ORG tan indirin.
- Yeni kontrollerin sizin için geçerli olup olmadığını kontrol etmek için risk değerlendirme planını gözden geçirin
- Yeni standarda referanslarla **Uygulanabilirlik Bildiriminizi** oluşturun
- Yeni niteliklere karşı Operasyonel Yeteneklerinizi değerlendirin

BUREAU VERITAS CERTIFICATION

GEÇİŞ AŞAMALARI?

Sertifikalı müşteriler, geçişlerine **BV akreditasyon geçiş tarihten itibaren** başlayabilirler. Müşterilerimizin tüm geçişleri **31/10/2025** tarihine kadar tamamlanacaktır.

Geçiş denetimi:

- Gözetim denetimi (ara kontroller), yeniden belgelendirme denetimi ile birlikte veya ayrı bir denetim (özel ara kontrol) aracılığıyla yürütülebilir.
- Özellikle teknolojik bilgi güvenliği kontrollerinin gözden geçirilmesi için sadece belge incelemesi yeterli olmayıp ayrı bir denetim gereksinimi doğmaktadır. Bu denetim sınırlandırıcı olmamakla birlikte aşağıdakileri içerecektir:

- **ISO/IEC 27001:2022'nin gap analizi ve müşterinin BGYS'sinde değişiklik ihtiyacı.**
- **Uygulanabilirlik beyanının güncellenmesi (SoA-Uygulanabilirlik Bildirgesi).**
- **Uygulanabildiği ölçüde, risk iyileştirmelerinin güncellenmesi.**
- **Müşteriler tarafından seçilen yeni veya değiştirilmiş bilgi güvenliği kontrollerinin uygulanması ve etkinliği.**

BUREAU VERITAS BELGELENDİRME

GEÇİŞ AŞAMALARI?

Bir yeniden belgelendirme denetimi ile bağlantılı olarak gerçekleştirildiğinde, geçiş denetimi için en az 0,5 denetçi günü artış olacaktır.

Gözetim denetimi ile bağlantılı olarak veya ayrı bir denetim olarak gerçekleştirildiğinde, geçiş denetimi için en az 1,0 Denetçi günü artış olacaktır.

ISO/IEC 27001:2013'e versiyonundaki sertifikaların süresi 31/10/2025'ten sonra sona erecek veya geri çekilecektir.

Çalışan sayısı, kapsam vb değişkenlere göre gün süresi hesaplama cetveline göre farklılık gösterebilmektedir. dhakan

BUREAU VERITAS CERTIFICATION

WHAT'S NEXT?

AGENDA-TÜRKAK AKREDİTASYONU

Belgelendirme Kuruluşlarının geçişlerini 31.03.2023 tarihine kadar ISO 27001:2022 versiyonuna geçiş planı iletmeleri istenmekte olup, tüm Geçişler 31.10.2023 tarihine kadar tamamlanmış olacaktır. Kuruluşların geçişleri İse 31.10.2025 tarihine kadar tamamlanmış olacaktır.

ZAMAN ÇİZELGESİ:

TARİH	FAALİYET
25 Ekim 2022	ISO/IEC 27001:2022 standardının yayınlanması
31 Ekim 2023	Akredite olan tüm Belgelendirme Kuruluşlarının geçişinin tamamlanması
31 Ekim 2023	Belgelendirme Kuruluşlarının ilk belge başvurularını ISO/IEC 27001:2022'ye göre almaları
31 Ekim 2025	Belgeli tüm müşterilerin ISO/IEC 27001:2022'ye geçişinin tamamlanması

WWW.BUREAUVERITAS.COM