

Bilgi Güvenliği Yönetim Sistemi

ISO 27001

NEDEN ISO 27001?

- İç denetimlerinizin bağımsız bir şekilde sağlandığını gösterir ve kurumsal yönetim ve iş devamlılığı gereksinimlerini karşılar
- Geçerli yasa ve düzenlemelere uygun davranıldığını bağımsız bir şekilde gösterir
- Sözleşmeden doğan gereklilikleri karşılayarak ve müşterilerinize bilgilerinin güvenliğine gösterdiğiniz özeni göstererek bir rekabet avantajı sağlar
- Bilgi güvenliği işlemlerinizi, prosedürlerinizi ve belgelerinizi biçimlendirirken kurumsal risklerinizin gerektiği gibi tanımlandığını, değerlendirildiğini ve yönetildiğini bağımsız bir şekilde doğrular
- Üst yönetiminizin bilgilerinin güvenliğine olan taahhüdünü kanıtlar

Bilgi, kuruluşunuzun faaliyetleri, hatta belki devamı için büyük önem taşır. ISO/IEC 27001 sertifikasyonu, değerli bilgi varlıklarınızı yönetmenize ve korumanıza yardımcı olur.

ISO/IEC 27001, Bilgi Güvenliği Yönetimi Sistemi (ISMS) gereksinimlerini tanımlayan tek uluslararası denetlenebilir standarttır. Yeterli ve orantılı güvenlik denetimleri seçilmesini sağlamak için tasarlanmıştır.

Bu, bilgi varlıklarınızı korumanıza ve ilgili taraflara, özellikle de müşterilerinize güven vermenize yardımcı olur. Bu standart, Bilgi Güvenliği Yönetimi Sisteminizi oluşturmak, uygulamak, işletmek, izlemek, incelemek, sürdürmek ve geliştirmek için süreç yaklaşımını benimser.

Kimi ilgilendirir?

ISO/IEC 27001, dünyanın hangi bölgesinden veya hangi sektörden olursa olsun büyük küçük tüm kuruluşlara uygundur. Bu standart, finans, sağlık, kamu ve BT sektörleri gibi bilginin korunmasının büyük öneme sahip olduğu alanlarda özellikle gereklidir.

ISO/IEC 27001, BT taşıyan şirketleri gibi bilgiyi başkaları adına yöneten kuruluşlar için de oldukça etkilidir: müşterilere bilgilerinin koruma altında olduğu güvencesini vermek için kullanılabilir.

ISO 27001 Eğitimleri

Tetkik ve belgelendirmenin yanı sıra eğitim konusunda da uzmanız ve belgelendirme öncesinde ve sonrasında da ihtiyacınız olan yetenekleri size kazandırmaya yönelik bir genel katılıma açık ve kuruluş içi kurs ağına sahibiz.

Tek günlük giriş eğitimlerinden, uygulama eğitimi ve baş denetçilik kurslarına kadar genel katılıma açık eğitim ve kuruluş içi eğitim ağımlı işlemlerinizin her aşamasında size yardımcı olabilir. Her türden ve boyuttan kurumun standartlara yaklaşımı konusunda bizden daha deneyimli bir kuruluş yok. Bilgi güvenliği yönetimi sisteminizi anlamak, uygulamak, değerlendirmek ve belgelemek için ihtiyacınız olan eğitimi size

ISO/IEC 27001'i her yönüyle ele alan kapsamlı bir eğitim programı sunuyoruz !

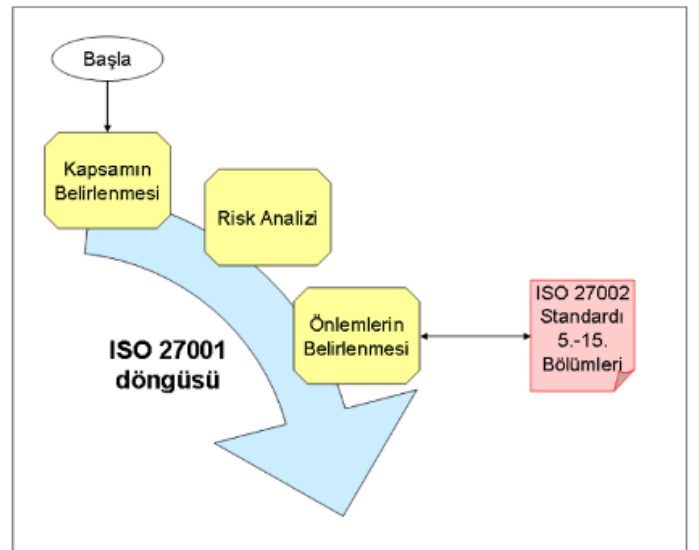
Bu eğitimimizden yararlanabilecek kişiler:

ISO/IEC 27001 ve Bilgi Güvenliği Yönetimi Sistemi konusunda deneyimi olmayan temsilcilere;

- Yeni bir sistemi öğrenme, anlama ve uygulama üzerine dersler,

Mevcut bir sistemi denetlemesi ve geliştirmesi gereken temsilcilere ise;

- Mevcut sistemi denetleme, değerlendirme ve geliştirme



ISO 27001



ISO 27001 sertifikası almanın size ve firmanıza ne gibi avantajları olabilir?

Akredite bir kurumdan ISO 27001 sertifikasının alınması; kuruluşunuzun bilgi güvenliğini dikkate aldığını, gerekli adımları uyguladığını ve kontrol ettiğini göstermektedir. Fakat sertifikasyonun getirileri bununla sınırlı değildir;

- Bilgi varlıklarının farkına varma;
- Kuruluş, hangi bilgi varlıklarına sahip olduğunu bilir ve değerinin farkına varır.
- Sahip olduğu varlıkları, kuracağı kontroller ve koruma metotları ile belirlemiş olduğu süreç içerisinde korur...
- Bu farkındalık; yönetim ve bilgi sistemlerinin güvenli olduğu konusunda

müşterilerinizi, çalışanlarınızı, hissedarlarınızı, iş ve çözüm ortaklarınızı da rahatlatmaktadır.

- Şirketinizin kredibilitasını ve piyasaya güvenini arttırmaktadır.
- Basta tedarikçileri olmak üzere, bilgileri korunacağından ilgili tarafların güvenini kazanır.
- Bilgi, bu sistem sayesinde korunur ve hiçbir detay tesadüfe bırakılmaz.
- Ayrıca, bir felaket halinde ise devam etme yeterliliğine sahip olunur.
- Ufak bir güvenlik ihlali bile çok yüksek maliyetlere yol açabileceği için, kontrollerin uygulanması ile maliyetler uzun vadede düşürülmektedir.
- Çalışanların motivasyonunu artırmakta ve yasal takipleri önlemektedir.
- Kanun ve yönetmeliklere uyulduğu bir

Kuruluşların uyguladığı bazı kontroller şunlardır;

- Şifre kullanarak kişisel bağlanma,
- Virüs kontrolleri, yedekleme ve saklama (şirket dışında saklama da dahil) uygulamaları,
- Yetki tabloları,
- İK ile işbirliği,
- İş planlama (kaza sonucunda ve iş sürekliliği için yapılacakların listesi),
- BT hata raporlamaları,
- E-posta, faks, internet ve fotokopi için kullanma koşulları,
- Dosyalara erişimde yetkiler...

ISO 27001 kapsamı nasıl belirlenebilir?

ISO 27001' in kapsamı, belirli iş süreçleri, bölgeler, departmanlar ya da kuruluşun bütünüyle sınırlandırılabilir.

Kapsam açık ve net olarak belirtilmelidir. Bunun, sertifikayla ilişkilendirilmiş Uygunluk Beyanında belirtilmesi

ISO 27001

Maddelerinin Yapısı

0. Giriş

1. Kapsam

2. Atıf yapılan

standartlar ve/veya dokümanlar

3. Terimler ve tarifleri

4. Bilgi güvenliği

yönetim sistemi

5. Yönetim sorumluluğu

6. BGYS iç denetimleri

7. BGYS'yi yönetimin

gözden geçirmesi

8. BGYS iyileştirme

Ek A – Kontrol amaçları ve kontroller

Ek B (Bilgi için) –

OECD prensipleri ve bu standart

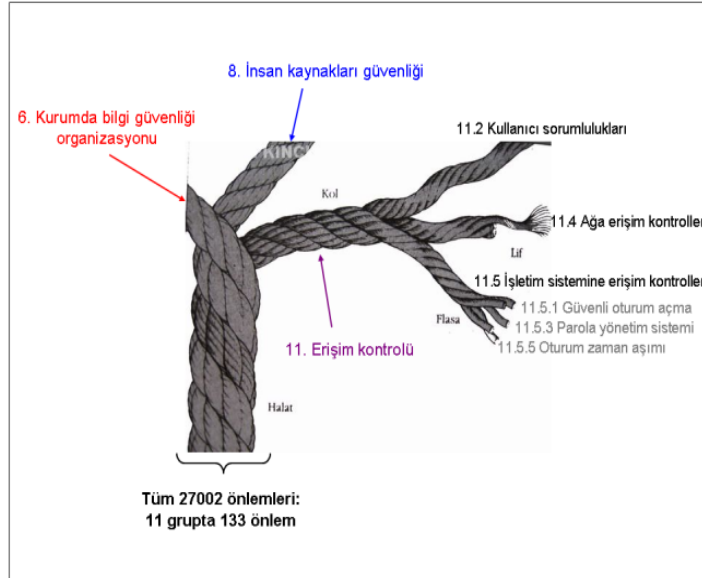
Ek C (Bilgi için) – TS EN

ISO 9001, TS EN ISO

14001 ve bu standart

arasındaki

benzerlikler



ISO 27001 uygulanmaya nasıl başlanabilir?

ISO 27001 standardına dayanan Bilgi Güvenliği Yönetim Sistemi'nin oluşturulması

kısaca üç adımdan oluşmaktadır;

1. Bilgi için bir Yönetim Platformu oluşturulması; hedeflerin, amaçların, bilgi güvenliği politikasının belirlenmesi,
2. Güvenlik risklerinin belirlenmesi ve değerlendirilmesi,
3. Kontrollerin seçimi ve uygulanması. ISO 27001 standardına uygun bir bilgi güvenliği yönetim sisteminin kurulması, kuruluşunuzu güvenlik saldırılarına karşı tamamen korumayabilir. Ancak, bu tür saldırıların başarılı olma olasılığını önemli ölçüde



Bva Belgelendirme ve Dış Tic. Ltd. Şti. olarak, ISO 27001 Bilgi Güvenliği Yönetim Sisteminizi temsilcisi olduğumuz Certification Europe üzerinden INAB akreditasyonlu olarak belgelendirmekteyiz.



BVA Belgelendirme ve Dış Ticaret Ltd. Şti.

Gayrettepe Mah. Yıldız Posta Cad. Akın Sitesi 1. Blok No:6 Kat:4 D:9 Beşiktaş 34349 - İstanbul - TÜRKİYE
Tel +90-212-347 0865 (pbx) Faks : +90-212-273 2829 Web: www.bva.tc e-mail: info@bva.tc