KOTTO BİLİŞİM A.Ş.

ISO 27001 : 2013

Bilgi Güvenliği Yönetim Sistemi

Danışmanlık, Uyum ve Süreç Modernizasyonu

Kasım 2019, Ankara
Sürüm 2.0

KOTTO HAKKINDA

KOTTO A.Ş. müşterilerine stratejik dış kaynak kullanımı, entegrasyon ve e-dönüşüm konularında çözüm ve servis sağlayan bir YETENEK TAKIMI olup, aynı zamanda kamu BT sektörünün en yeni bağımsız kuruluşudur. Şirketimizi farklı kılan güvenilir yapımız, güçlü iş ortaklarımız, uzman kadrolarımız, son teknolojiyi uygulama yeteneğimiz ile müşteri ve sektör odaklı yaklaşımımızdır. 25 yılı aşkın sektör deneyimi barındıran şirketimiz müşterilerinin teknoloji ortağı olarak onlarla uzun dönemli ilişkiler kurmayı ve müşteri memnuniyetini en üst seviyede tutmayı ilke edinmiştir.

Bugün KOTTO olarak kamu sektöründe hem yerli hem milli sermayeli yatırımları tercih eden öncü firmayız. İştiraklerimiz ve stratejik ortaklıklarımız ile birlikte altyapı ve iş çözümlerini destekleyen çok sayıda uzman çalışan istihdam ediyor, imkânlar yaratıyor ve kapsayıcı faydalar sağlıyoruz. Büyüme eğrimiz ve gelirlerimizin dağılımına bakıldığında kuruluşumuzdan bu yana hızlı ve sağlıklı bir büyüme sergilenmiş, 2016 yılından başlayarak kendi çözüm ve hizmetlerimizin toplam gelirler içindeki payı sürekli olarak büyümüştür.

Vizyonumuz

Sahip olduğu teknolojik altyapı, gelişmiş yetkinlikler ve uzman ekibi, kendi geliştirdiği ürün ve servisleriyle müşteriye özel esnek çözümler ve değer üreterek ulusal pazarlardaki faaliyetini sürekli genişleten öncü bir teknoloji şirketi olmaktır.

Misyonumuz

Bilgi teknolojilerinin fikirden uygulama ve uzun dönem yönetimine kadar her aşamasında müşterilerimizin, güvenilir ve profesyonel teknoloji ortağı olarak verimliliklerini artırmak, maliyet ve rekabet avantajı sağlamaktır.

Kalite Politikamız

• Müşterilerimizin ihtiyaç ve beklentilerini, en uygun çözümler ile uçtan uca karşılamak,

• Geleceğe taşıyan uygulamalar ve çözümler sunarak işbirliği yaptığı kurumlara değer katmak

• Çalışan ve müşteri memnuniyetini arttırmak,

• Kalıcı müşteriler edinmek,

şeklinde tanımlanmıştır ve şirketimiz kalite sisteminin temelini oluşturmaktadır.

İş Çözümlerimiz

Danışmanlarımız ürünleri müşteri beklentileri ve sektör ihtiyaçları doğrultusunda belirlemekte ve konumlandırmaktadır. Müşterilere sunulan çözümler arasında, daha önce geliştirilmiş KOTTO markalı hazır iş çözümlerinin yanı sıra, müşteri istekleri doğrultusunda kurumlara özel geliştirilen (White Labeling) yazılım ve çözümler de bulunmaktadır. Bu çözümlerin önemli bir kısmı farklı sektörlerde kullanılabilecek ortak çözümler iken, kalanı belirli sektörlere özel çözümler olarak geliştirilmiştir.

Bütünleşik entegrasyonlarımız, müşteri ihtiyaçlarının ve iş süreçlerinin analizi doğrultusunda; danışmanlık, iş ihtiyaçlarının gerektirdiği bir yazılımın seçimi, yeni bir yazılımın geliştirilmesi, sistem ve çözümün tasarımı, kurulumu, testleri, devreye alınması, işletim ve bakım hizmetlerinin sağlanması konularındaki çalışmaları kapsamaktadır.

Teknoloji Çözümlerimiz

KOTTO, ağ, güvenlik, sistem çözümleri, alanlarındaki farklı uzmanlıkları ile müşteri ihtiyaçlarına yönelik danışmanlık, tasarım, PoC/test/demo, ürün sağlama ve kurulum hizmetlerini sunduğu anahtar teslim sistem entegrasyonu projelerinde yer alırken, müşterilerinde kalıcı olmayı amaçlayan, güvenilir, destek hizmetlerini de beraberinde sunmaktadır.

Temel İlke ve Değerlerimiz

KOTTO ailesinin tüm bireyleri

• GÜVENİLİRLİK,

• MÜŞTERİ MERKEZİYETÇİLİK,

• SONUÇ ODAKLILIK,

• TAKIM ÇALISMASI,

• SÜREKLİ GELİŞİM,

• YARATICILIK ve

• ETKİLİ İLETİŞİM

şeklinde tanımlanabilecek ilke ve değerlere sahip olarak kendisini sürekli geliştirmeye çalışır.

Cevizlidere 1235. Cad. Plenty Plaza No: 9/17 06460 Çankaya / Ankara / TÜRKİYE
+90 312 472 3030 _ info@kottoAS.com _ www.kottoAS.com

Bilgi günümüzde hayatın önemli bir parçasıdır. Toplumun bilgi akışına bağımlılığı hızla yükselmekte, bu durum, bilgiyi ve bilginin ele alınmasını geçmişte hiç olmadığı kadar önemli bir hale getirmektedir.

Bilgi, ALTIN ve URANYUM kadar değerli bir kaynaktır...

Bilgi transferinin kolaylığının yanı sıra gizlilik de özellikle konu kişisel ve finansal veriler veya araştırma ve geliştirme çalışmalarından elde edilen hassas veriler olduğunda hayati bir öneme sahiptir. Ayrıca bilişim sistemlerinin her daim kullanıma hazır olması ve bütünlüğü de önemli unsurlar olarak ele alınmaktadır. Bilginin bilgisayar korsanları veya casuslar tarafından manipüle edilmesi, çalınması, insan hatası, teknik hata veya yıkıcı nitelikteki bir olay nedeniyle kaybedilmesi ya da hasar görmesi öngörülemeyen sonuçlara neden olabilir. Bu risklere çözüm yaratmanın en etkin yolu, yasal, düzenleyici ve sözleşmelerle ilgili yükümlülükleri de hesaba katabilen, kapsamlı bir **Bilgi Güvenliği Yönetim Sistemi'nin (BGYS)** kurulmasıdır.

ISO27001 standardında belgelendirilmiş bir BGYS, geliştirilme, kurulum, işletilme ve bakıma ilişkin şartların yanı sıra sürekli olarak iyileştirilmesine yönelik hususları da belirtmektedir. Bu sistem, tüm şirket ve kuruluşlara uygulanabilir. KOTTO tarafından sunulan danışmanlık, bu standardın şartlarının etkin bir şekilde hayata geçirildiğini ve önemli bilgilerin verimli bir şekilde korunduğunu belgeleme öncesinde teyit eder.

Çeşitli Faydalar

Şirketler ve kuruluşlar ISO27001 doğrultusunda alınan sertifikasyondan birçok şekilde faydalanabilmektedir:

Bilgilerin ele alınmasındaki zayıflıklar keşfedilir.

Personel güvenlik ve etkileri konusunda bilinçlendirilir ve riskler konusundaki bilinçlilik artar.

Bilgilerin sistematik bir şekilde ele alınması güvenliği arttırırken riskleri de en aza indirir.

BGYS'nin tanınan bir sertifikasyon kurumu tarafından onaylanıp belgelendirilmesi halinde müşterilerin, iş ortaklarının ve yatırımcıların itimadı ve güveni artar.

Cevizlidere 1235. Cad. Plenty Plaza No: 9/17 06460 Çankaya / Ankara / TÜRKİYE
+90 312 472 3030 _ info@kottoAS.com _ www.kottoAS.com

ISO 27001: 2013

Bilgi Güvenliği Yönetim Sistemi

Bilgi güvenliği; iş devamlılığı, kaçınılmaz felaket durumlarında kaybın en aza indirilmesi, firmaların yapı taşları sayılan kaynakların her koşulda gizliliğinin, ulaşılabilirliğinin ve bütünlüğünün korunması amaçlarını taşır.

Günümüzde, sadece çalışanlarıyla değil, müşterileri, iş ortakları ve hissedarlarıyla birlikte tanımlanan kurumlarda, bilginin korunmasına ve gizliliğine ilişkin güven ortamının yaratılması stratejik bir önem taşımaktadır. Yaşanan güvenlik sorunları, iş devamlılığını engellemenin yanı sıra, kurumların; pazar kaybına, müşteriler, iş ortakları ve hissedarlar karşısında güven yitirmesine neden olmaktadır. Bunların geri kazanılması, bunların yitirilmemesi için alınacak önlemlerden her zaman daha pahalıdır.

Bilgi Nedir?

Bilgi, diğer önemli ticari varlıklar gibi, bir işletme için değeri olan ve bu nedenle uygun olarak korunması gereken bir varlıktır. Bilgi, kuruluşunuzun faaliyetleri ve devamı için büyük bir önem taşır.

Bilgi Güvenliği Nedir?

Bir kurumun bilgi varlıklarının gizliliğinin (bilginin yetkisi olmayan kişiler, kurumlar ya da süreçler için kullanılabilir olmamasını ya da ifşa edilmemesini temin etme özelliği), bütünlüğünün (varlıkların doğruluğunun ve eksiksizliğinin teminat altına alınması özelliği) ve kullanılabilirliğinin (yetkili bir kurumun talebi üzerine kullanılabilir olma özelliği) korunmasıdır.

BGYS Nedir?

ISO/IEC 27001, Bilgi Güvenliği Yönetimi Sistemi (ISMS) gereksinimlerini tanımlayan tek uluslararası denetlenebilir standarttır. Ülkelere göre özel tanımlar içermeyen, genel tanımların bulunduğu bir standarttır. Yeterli ve orantılı güvenlik denetimleri seçilmesini sağlamak için tasarlanmıştır.

Bilgi güvenliği standardı BS 7799-2'nin revize edilip 2005'in sonlarında ISO27001:2005 olarak değiştirilmesiyle yürürlüğe giren bu standart kurumların bilgi güvenliği yönetim sistemi kurmaları için gereklilikleri tanımlamaktadır. Bunun yanı sıra ISO 17799:2002 numaralı standart ISO 17799:2005 "bilgi teknolojileri güvenlik teknikleri en iyi uygulamalar rehberi" olarak revize edilip yayınlanmıştır ve ISO27001'e göre kurulacak bir BGYS'nin nasıl gerçekleştirilebileceğine dair açıklamaları içerir.

ISO 27001 Kimleri ilgilendirir?

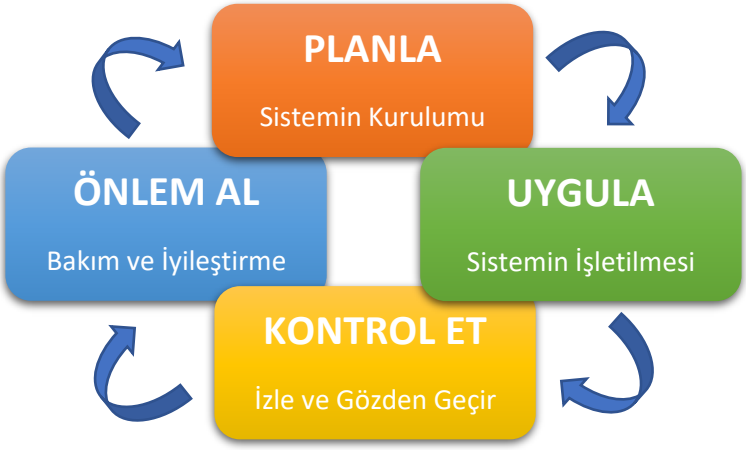
ISO/IEC 27001, dünyanın hangi Ülkesinden veya hangi sektörden olursa olsun büyük küçük tüm kuruluşlara uygundur.

Bu standart, finans, sağlık, kamu ve BT sektörleri gibi bilginin korunmasının büyük öneme sahip olduğu alanlarda özellikle gereklidir. ISO/IEC 27001, BT taşeron şirketleri gibi bilgiyi başkaları adına yöneten kuruluşlar için de oldukça önemlidir, müşterilere bilgilerinin koruma altında olduğu güvencesini vermek için kullanılabilir.

ISO 27001 Standart Ailesi

ISO 27001 BGY Sistemi Şartları

- 27000 Tanım ve Tarifler
- 27002 Uygulama Kuralları
- 27003 BGYS Uygulama Kılavuzu
- 27004 BGYS Ölçümü
- 27005 Bilgi Güvenliği Risk Yönetimi



Cevizlidere 1235. Cad. Plenty Plaza No: 9/17 06460 Çankaya / Ankara / TÜRKİYE
+90 312 472 3030 _ info@kottoAS.com _ www.kottoAS.com

ISO/IEC 27001 İle ilgili Terim ve Kavramlar

Bilgi Güvenliği Yönetim Sistemi (BGYS): Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası.

Risk analizi: Kaynakları belirlemek ve riski tahmin etmek amacıyla bilginin sistematik kullanımı

Risk değerlendirme: Risk analizi ve risk derecelendirmesini kapsayan tüm proses

Risk derecelendirme: Riskin önemini tayin etmek amacıyla tahmin edilen riskin verilen risk kriterleri ile karşılaştırılması prosesi.

Risk yönetimi: Bir kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetler.

ISO 27001 Bilgi Güvenliği Yönetim Sisteminin Kurulmasının Planlaması

- Organizasyondaki altyapıyla ilgili bilgilerin toplanması
    - Yapılan işin niteliği
    - Misyon
    - Yerleşim noktaları
- BGYS'nin kurulumda görev alacak anahtar oyuncular Risk yönetimini gerçekleştirecek sorumlular ve BGYS'nin kurulma nedeni
- Mevcut durumda organizasyonun güvenlik durumu
- BGYS'nin kapsamını belirleyecek bilgiler; lokasyonlar, işlemler, iş fonksiyonları, bilgi, bilgi teknolojileri
- BGYS'nin hedefi
- BGYS'nin kapsamının belirlenmesi
- BGYS'nin kurulması için çalışma programının oluşturulması
- BGYS'nin kurulması ve sürekliliği için gerekli olan süreçlerin belirlenmesi

ISO 27001 Bilgi Güvenliği Yönetim Sistemi Kurmanın Yararları

Bilgi varlıklarının farkına varılır, kuruluş hangi bilgi varlıklarının olduğunu ve bunların değerinin farkına varır.

Sahip olduğu varlıkları, kuracağı kontroller ile koruma metotlarını belirleyerek ve uygulayarak korur.

İş sürekliliği sağlar, uzun yıllar boyunca işini garanti eder. Ayrıca bir felaket halinde, işe devam etme yeterliliğine sahip olur.

Tedarikçi ve müşterilerin bilgileri korunacağından ilgili tarafların güvenini kazanır.

Bilgiyi bir sistem sayesinde korur, tesadüfe bırakmaz.

Müşterileri değerlendirirken, rakiplerine göre daha iyi değerlendirilir.

Çalışanların motivasyonunu arttırır.

Yasal takipleri önler.

Yüksek prestij sağlar.

Rekabet avantajı kazandırır.

Düzenli değerlendirme işlemi performansınızı sürekli izlemenize ve geliştirmenize yardımcı olur.

Cevizlidere 1235. Cad. Plenty Plaza No: 9/17 06460 Çankaya / Ankara / TÜRKİYE
+90 312 472 3030 _ info@kottoAS.com _ www.kottoAS.com

ISO 27001 Bilgi Güvenliği Sistemi Kurma Aşamaları

Bilgi güvenliği yönetim sistemi, kurumunuzdaki tüm bilgi varlıklarının değerlendirilmesi ve bu varlıkların sahip oldukları zayıflıkları ve karşı karşıya oldukları tehditleri göz önüne alan bir risk analizi yapılmasını gerektirir. Kurum kendine bir risk yönetimi metodu seçmeli ve risk işleme için bir plan hazırlamalıdır.

Risk işleme için standartta öngörülen kontrol hedefleri ve kontrollerden seçimler yapılmalı ve uygulanmalıdır. Planla-uygula-kontrol et-önlem al (PUKÖ) çevrimi uyarınca risk yönetimi faaliyetlerini yürütmeli ve varlığın risk seviyesi kabul edilebilir bir seviyeye geriletilene kadar çalışmayı sürdürmelidir.

ISO 27001 Kurumların risk yönetimi ve risk işleme planlarını, görev ve sorumlulukları, iş devamlılığı planlarını, acil durum olay yönetimi prosedürleri hazırlamasını ve uygulamada bunların kayıtlarını tutmasını gerektirir. Kurum tüm bu faaliyetlerin de içinde yer aldığı bir bilgi güvenliği politikası yayınlamalı ve personelini bilgi güvenliği ve tehditler hakkında bilinçlendirmelidir. Seçilen kontrol hedeflerinin ölçülmesi ve kontrollerin amacına uygunluğunun ve performansının sürekli takip edildiği yaşayan bir süreç olarak bilgi güvenliği yönetimi ancak yönetimin aktif desteği ve personelin katılımcılığıyla başarılabilir.

Kurum içerisinde bu çalışmaları yürütecek BGYS takımının ve BGYS yöneticisinin bilgi güvenliği yönetimi konusunda iyi eğitimli olmaları gerekmektedir. Risk yönetimi, politika oluşturma, güvenlik prosedürlerinin hazırlanması ve uygun kontrollerin seçilerek uygulanması aşamalarında uzman desteği ve danışmanlık almaları faydalı olacaktır.

ISO 27001'den bahsederken karıştırılan ve dikkatle ayrılması gereken şey ISO 27001'in Yönetim Sistemi öngörmesidir. ISO 27001 size nasıl virüs bulaşmayacağını anlatmaz. Bilgisayar ağınıza saldırganların nasıl sızabileceğini söylemez. Size toplam bilgi güvenliği ve "yaşayan bir süreç olarak" bilgi güvenliğinin nasıl "yönetileceğini" tanımlar.

Kurma aşamalarını maddeler halinde sıralayacak olursak aşağıda belirtildiği şekilde bir sıralama uygundur.

1. Varlıkların sınıflandırılması,
2. Gizlilik, bütünlük ve erişebilirlik kriterlerine göre varlıkların değerlendirilmesi,
3. Risk analizi,
4. Risk analizi çıktılarına göre uygulanacak kontrolleri belirleme,
5. Dokümantasyon oluşturma,
6. Kontrolleri uygulama
7. İç tetkik,
8. Kayıtları tutma,
9. Yönetimin gözden geçirmesi,
10. Belgelendirme.

Standartla İlgili Yasal Şartlar

- 5651 Sayılı Kanun İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
- 5809 Sayılı Kanun Elektronik Haberleşme Kanunu
- 26942 Sayılı Elektronik Haberleşme Güvenliği Yönetmeliği Kanun kapsamında yapılması gerekenler;
- Bilgisayarların aldığı IP loglarını kayıt altına almak
- Geçmişe yönelik hangi kullanıcının hangi IP adresine sahip olduğunu kayıt altına almak
- Kullanıcının web üzerindeki yaptığı gezintilerin loglarını kayıt altına almak
- Atılan e-mail loglarını kayıt altına almak
- Geçmişe yönelik hangi kullanıcının web üzerinde hangi sayfalara gittiği ve ne kadar zaman geçirdiğini kayıt altına almak
- Web erişimlerini içerik bazlı filtreleyerek kısıtlı erişimler sağlamak
- Toplanan tüm kayıtların bütünlüğünü sağlayarak değiştirilmediğini kanıtlamak

Elektronik haberleşmeye ilişkin başlıca tehditler

- Yetkisiz olarak veya yetki aşımıyla güvenlik hassasiyetli alana girilmesi,
- Yetkisiz olarak veya yetki aşımıyla silme, ekleme, değiştirme, geciktirme, başka bir ortama kaydetme veya ifşa etme yoluyla veri gizliliğinin, bütünlüğünün ve/veya devamlılığının bozulması,
- Donanım-yazılım bileşenlerinin ulusal düzenleme ile ulusal ve/veya uluslararası standartlar uyarınca belirlenen gereklilikleri yerine getirmesinin kısmen veya tamamen engellenmesi,
- Kullanıcıyı yanıltarak doğru tarafla elektronik haberleşmede bulunduğu izleniminin verilmesi,
- Elektronik haberleşmenin yasal olmayan bir şekilde izlenmesi ve/veya dinlenmesi,
- Doğru olmayan bir bilgi üretilerek bu bilginin başka bir taraftan alındığının iddia edilmesi veya başka bir tarafa gönderilmesi,
- Elektronik haberleşme altyapısının kısmen veya tamamen hizmet veremez hale getirilmesi veya altyapıya ait kaynakların, hizmet sunumunu aksatacak şekilde tüketilmesidir.

Elektronik haberleşmeye ilişkin başlıca zayıflıklar

- Gelecekte gerçekleşmesi muhtemel tehditlerin öngörülememesi,
- Bir sistem veya protokolün tasarımında yapılan yanlışlıklar,
- Bir sistem veya protokolün kurulumu sırasında oluşan problemler,
- Geliştiricilerin hataları,
- Uygulayıcıların hataları,
- Sistemin işletimi sırasında oluşan uygunsuzluklar veya yetersizliklerdir.

Belgelendirme Süreci

Diğer hususların yanı sıra sertifikasyon için gereken ön şartlar arasında bir güvenlik politikasının ve bir risk yönetimi sürecinin (risk değerlendirmesi ve riskin ele alınması) uygulamaya konulması ve ayrıca Uygulanabilirlik Beyanı da yer almaktadır.

Ardından sertifikasyon şu aşamalardan geçer:

- İlk bilgilendirme süreci
- Tetkike hazırlık
- Belge incelemesi
- Tetkik
- Sertifikanın düzenlenmesi

Sertifika üç yıllığına geçerlidir ve her yıl gözetim amaçlı tetkik uygulanır. Sistem bünyesinde farklı koşullara veya düzenlemelere yer vermek amacıyla ihtiyaç duyulması halinde tetkikin değiştirilmesi de mümkündür.

Hizmetimiz, tüm sektörlerden ve tüm kamu hizmetlerinden müşterilere yöneliktir. İş süreçlerinizin sorunsuz bir şekilde yürütülmesi için ayrıca ISO20000-1 (BT Hizmeti Yönetim Sistemleri) doğrultusunda alınacak sertifikasyonu da önermekteyiz. Böylece aynı eforla çok daha yüksek bir fayda sağlanabileceğine inanmaktayız.

Cevizlidere 1235. Cad. Plenty Plaza No: 9/17 06460 Çankaya / Ankara / TÜRKİYE
+90 312 472 3030 _ info@kottoAS.com _ www.kottoAS.com