ISO/IEC 27001:2022 Değerlendirme anketi

Bu belge, şirketinizin ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi belgelendirme değerlendirmesine hazır olup olmadığını değerlendirmek için tasarlanmıştır. Bu kontrol listesini doldurduğunuzda sonuçlarınız kuruluşunuzu kendi kendinize değerlendirmenizi ve standardın ana gerekliliklerivle ilgili olarak süreçte nerede olduğunuzu belirlemenizi sağlayacaktır.

Kuruluşun bağlamı

- Bilgi Güvenliği Yönetim Sisteminizin (ISMS) amaçlanan sonuçlarına ulaşma yeteneğinizi etkileyen, kuruluşunuzun amacı ile ilgili dış ve iç sorunları belirlediniz mi? ☐
- İlgili tarafların ISMS ile ilgili ihtiyaç ve beklentilerini belirlediniz mi ve bunları düzenli olarak gözden geçiriyor musunuz? ☐
- ISMS'inizin kapsamını belirlediniz mi ve bunu yaparken iç ve dış konuları, ilgili tarafları ve diğer kuruluşlar tarafından gerçekleştirilen faaliyetleri dikkate aldınız mı? ☐
- ISMS'i etkileyebilecek iç ve dış konular dikkate alındı mı? ☐
- Bu sorunlar ve gerekliliklerleilgili riskler ve fırsatlar dikkate alındı mı? ☐
- Düzenleyici ve yasal kuruluşlar ve müşterileriniz dahil olmak üzere ilgili tarafların gereksinimlerinin farkında mısınız? ☐
- Bilgi güvenliği yönetim sistemi aracılığıyla ilgili tarafların gereksinimlerinden hangilerinin ele alınacağını belirlediniz mi? ☐
- Sürekli iyileştirme dikkate alındı mı? ☐
- Bilgi güvenliği yönetim sistemlerini kurmak, sürdürmek, uygulamak ve tesis etmek için ihtiyaç duyulan süreçler ve etkileşimleri belirlendi ve uygulandı mı? ☐

Liderlik

- Oluşturulan bilgi güvenliği politikası ve hedefleri, kuruluşun bağlamı ve stratejik yönüyle uyumlu mu? ☐
- Bilgi güvenliği politikası kuruluş içinde ve ilgili taraflara iletildi mi? ☐
- Politika, bilgi güvenliği hedeflerini içeriyor mu veya bilgi güvenliği hedeflerinin belirlenmesi için çerçeve sağlıyor mu? ☐
- ISMS içindeki roller açıkça tanımlandı, açıklandı ve iletildi mi? ☐
- Roller, sorumluluğun yanı sıra uygunluğu ve raporlamayı sağlama yetkisini de taşıyor mu? ☐
- ISMS'in sonuçlarına, gerekliliklerine ve hedeflerine ulaşmasını sağlayacak bir program geliştirildi ve uygulamaya kondu mu? ☐
- Etkili bilgi güvenliği yönetiminin ve bilgi güvenliği yönetim sistemi gerekliliklerine uymanın önemini ilettiniz mi? ☐

Planlama

ISMS'in amaçlanan sonuçlarına ulaşabilmesini sağlamak için ilgili taraflar ve kapsamda belirlenen riskler ve fırsatlar ele alındı mı? ☐

Risk kabul kriterlerini içerecek bir bilgi güvenliği risk değerlendirme süreci oluşturuldu mu? ☐

Bilgi güvenliği risk değerlendirme süreci, tekrarlanabilir olacak ve tutarlı, geçerli ve karşılaştırılabilir sonuçlar sağlayacak şekilde tanımlandı ve geliştirildi mi? ☐

Risk değerlendirmesi tutarlı, geçerli ve karşılaştırılabilir sonuçlar veriyor mu? ☐

Kuruluş, bu riskleri ve fırsatları ele almak için eylemler planladı mı ve bunların ISMS'e nasıl entegre edileceğini ve uygulanacağını ve bu eylemlerin etkinliğinin nasıl değerlendirileceğini belirledi mi? ☐

Bilgi güvenliği risk değerlendirme süreci, ISMS kapsamındaki bilgilerin gizlilik, bütünlük ve erişilebilirlik kaybıyla ilişkili riskleri belirlemek için yeterli mi? ☐

Risk sahipleri belirlendi mi? ☐

Bilgi güvenliği riskleri, gerçekleşmeleri durumunda ortaya çıkacak gerçekçi olasılıkları ve olası sonuçları değerlendirmek için analiz ediliyor mu ve risk seviyeleri belirlendi mi? ☐

Bilgi güvenliği riskleri belirlenen risk kriterleriyle karşılaştırılıyor ve önceliklendiriliyor mu? ☐

Bilgi güvenliği risk değerlendirme süreciyle ilgili bilgiler belgelendi mi? ☐

Uygun risk ele alma seçenekleri belirlendi ve uygulandı mı? ☐

Tercih edilen risk ele alma seçeneğini uygulamak için kontroller belirlendi mi? ☐

Belirlenen kontroller, gerekli kontrollerin atlanmadığını doğrulamak için ISO/IEC 27001:2022 Ek A ile karşılaştırıldı mı? ☐

ISO 27001:2022'ye uygun olarak revizyon geçmişi olan bir Uygulanabilirlik Beyanı var mı? ☐

Uygulanabilirlik Beyanı gerekli kontrollerin uygulanıp uygulanmadığını içeriyor mu? ☐

Uygulanabilirlik Beyanı, Ek A'dan kontrollerin seçilmesi veya hariç tutulması için gerekçe içeriyor mu? ☐

Bir bilgi güvenliği risk ele alma planı oluşturuldu mu? ☐

- Risk sahipleri planı gözden geçirip onayladı mı? ☐
- Artık bilgi güvenliği riskleri, risk sahipleri tarafından onaylandı mı? ☐
- Belgelendi mi? ☐

Ölçülebilir ISMS hedefleri oluşturuldu, belgelendi ve kuruluş genelinde iletildi mi? ☐

Kuruluş, hedeflerini tanımlarken neyin, ne zaman ve kim tarafından yapılması gerektiğini belirledi mi? ☐

Hedeflerin nasıl izleneceğini belirlediniz ve belgelediniz mi? ☐

ISMS'de değişiklik planlarken, ISMS'de değişiklik ihtiyacını ve değişikliklerin planlı bir şekilde nasıl gerçekleştirileceğini belirlediniz mi? ☐

Destek

ISMS'i oluşturmak, uygulamak, sürdürmek ve sürekli iyileştirmek için gerekli kaynakları (süreçlerin işletilmesi için insan, altyapı ve ortam dahil) belirlediniz ve sağladınız mı? ☐

ISMS rollerini yerine getirenler için gerekli yetkinliği belirlediniz mi? (örn. risk sahipleri, iç denetçiler, vb.) ☐

Bu roller için yetkinlik kanıtı var mı? ☐

Kuruluşun kontrolü altında çalışan kişilerin

i) ISMS politikasından haberdar olmasını sağladınız mı? ☐

ii) iyileştirilmiş bilgi güvenliği performansının faydaları da dahil olmak üzere, bilgi güvenliği yönetim sisteminin etkinliğine yapacakları katkıları belirlediniz mi? ☐

iii) bilgi güvenliği yönetim sistemi gerekliliklerine uymamalarının sonuçlarını belirlediniz mi (örneğin, disiplin cezaları)? ☐

Standardın gerektirdiği ve ISMS'in etkin bir şekilde uygulanması ve işletilmesi için gerekli olan belgelenmiş bilgiler oluşturuldu mu?

Kuruluş hangi iç ve dış iletişimlerin ilgili olabileceğini belirledi mi?

Belgelenmiş bilgi, kuruluşun ISMS için ihtiyaç duyduğu dış kaynaklı belgeler de dahil olmak üzere, kullanılabilir ve yeterince korunacak, dağıtılacak, depolanacak, saklanacak ve değişiklik kontrolü altında olacak şekilde kontrol ediliyor mu?

Operasyonlar

Madde 6'da belirlenen eylemleri uyguladınız mı veya uyguluyor musunuz:
— süreçler için kriterleri belirleyerek;
— kriterlere uygun olarak süreçlerin kontrolünü yaparak?

Süreçlerin planlandığı gibi yürütüldüğünü gösteren belgelenmiş kanıtlar saklanıyor mu?

ISMS'de değişiklik ihtiyacını belirlemek ve bunların uygulanmasını yönetmek için bir plan var mı?

Değişiklikler planlandığında, kontrollü şekilde uygulanıyor mu ve olumsuz etkileri azaltmak için önlemler alınıyor mu?

Dışarıdan sağlanan süreçler uygun şekilde kontrol ediliyor ve uygulanıyor mu?

Bilgi güvenliği risk değerlendirmeleri, planlı aralıklarla veya önemli değişiklikler meydana geldiğinde gerçekleştiriliyor mu ve belgelenmiş bilgiler saklanıyor mu?

Kuruluş, riskleri ve fırsatları ele almak ve bunları sistem süreçlerine entegre etmek için eylemler planladı mı?

Bilgi güvenliği risk değerlendirmesinin sonuçları hakkında belgelenmiş bilgileri saklamak için bir süreç var mı?

Risk sahiplerinden risk ele alma ve artık risk için onay almaya yönelik bir süreç var mı?

Performans değerlendirmesi

Nelerin, ne zaman ve kimler tarafından izlenmesi ve ölçülmesi gerektiğini, kullanılacak yöntemleri ve sonuçların ne zaman değerlendirileceğini belirlediniz mi?

İzleme ve ölçüm sonuçları belgeleniyor mu?

İç denetim yapmak üzere seçilen denetçiler süreç boyunca objektiflik ve tarafsızlık gösterebiliyor mu?

Kuruluş, ISMS'in etkili olduğunu ve ISO/IEC 27001 gerekliliklerine ve kuruluşun kendi gerekliliklerine uygun olduğunu kontrol etmek için bir iç denetim programı oluşturdu mu?

Bu denetimlerin sonuçları yönetime rapor ediliyor mu, belgeleniyor mu ve saklanıyor mu?

Uygunsuzlukların belirlendiği durumlarda, kuruluş uygunsuzlukları ve ilgili düzeltici faaliyetleri yönetmek için uygun süreçler oluşturdu mu?

Üst yönetim ISMS'i düzenli ve periyodik olarak gözden geçiriyor mu?

Yönetim incelemesine sağlanan girdi, dış ve iç konulardaki değişiklikleri ve ilgili taraflara duyulan ihtiyaçtaki değişiklikleri içeriyor mu?

Bilgi güvenliği performansına ilişkin geri bildirim, yönetim incelemesi için bir girdi olarak değerlendirildi mi?

ISMS yönetim incelemesinin çıktısı değişiklikleri ve iyileştirmeleri tanımlıyor mu?

Yönetimin incelemesinin sonuçlarını kanıtlamak için belgelenmiş bilgi mevcut mu?

İyileştirme

Uygunsuzlukların sonuçlarını kontrol etmek, düzeltmek ve çözümlemek için eylemler belirlendi mi? ☐

Uygunsuzlukların kök nedenini ortadan kaldırmak ve tekrar oluşmasını önlemek için eylem ihtiyacı değerlendirildi mi? ☐

Belirlenen herhangi bir eylem uygulandı mı, etkinlik açısından gözden geçirildi mi ve ISMS'de iyileştirmelere yol açtı mı? ☐

Belgelenmiş bilgiler, uygunsuzlukların niteliği, alınan önlemler ve sonuçların kanıtı olarak tutuluyor mu? ☐