ISO/IEC 27001 Özdeğerlendirme Soru Listesi

Bu soru listesindeki sorular, kurduğunuz/kuracağınız yönetim sistemdeki belirli alanlara daha fazla ışık tutmak, tekrar değerlendirerek gözden geçirmek ve denetime ne ölçüde hazır olduğunuzu belirleyebilmeniz için hazırlanmıştır.

Eğer bu değerlendirmeyi bizim yapmamızı isterseniz formu doldurduktan sonra info@vericert.com.tr 'ye gönderebilirsiniz. Tüm bilgileriniz gizli tutulacaktır.

Değerlendirme denetçilerimiz tarafından ÜCRETSİZ olarak yapılacaktır.

Buradaki soruları hiç bir zaman nihayi tetkik soruları ve almanız gereken bir takım önemli kararlar olarak görmeyin. Geliştirebileceğiniz alanlar olarak değerlendirin.

Sormak istediğiniz sorular için her zaman VERICERT Belgelendirme ile irtibata geçebilir ve açıklayıcı bilgiler talep edebilirsiniz.

Bu form doldurulabilir şekilde hazırlanmıştır. İlgili yerlere tıklayarak doldurabilirsiniz. Cevabınız Evet ise kutucuğa tıklamanız yeterlidir. Hayır ise soruyu lütfen boş bırakın.

İsminiz :		Telefon :	
Şirketiniz :		E-Posta :	
Şehir :		Web Adresi :	

A. PLANLAMA

☐ 1. Bilgi Güvenlik Yönetim Sistemi (BGYS) kapsamı ve sınırları tanımlanmış mı? Hariç tutumalar gerekçelendirilmiş mi?

☐ 2. Sözleşmesel, Yasal, düzenlemeleri dikkate alan, yapılan işin bilgi güvenliği risklerini ve risk değerlendirme kriterlerini ortaya koyan ve onaylanmış bir Bilgi Güvenlik Politikası bulunuyor mu?

☐ 3. Uygun ve tekrar edilebilir risk değerlendirme metodu ve kabul edilebilir risk düzeyi tanımlanmış ve dokümante edilmiş mi?

☐ 4. BGYS kapsamındaki varlıklar ve bunların sorumluları tanımlanmış mı? Zayıf alanlar tanımlanmış mı? Tehditler karşısında varlıkların gizliliğini yitirmesi, erişilebilirliğinin kaybolması durumundaki etkileri tanımlanmış mı?

☐ 5. Gizliliğin, bütünlüğün ve erişebilirliğin, güvenlik zaafiyetlerinden dolayı kaybedilmesinin işe olan etkisi, mevcut olan güvenlik kontrollerini kullanarak analiz edilmiş ve değerlendirilmiş mi?

☐ 6. Kabul edilebilir veya risk iyileştirmesi gerektirecek seviyede öngörülmüş risk seviyesi belirlenmiş mi?

☐ 7. Risk iyileştirme seçenekleri tanımlanmış ve değerlendirilmiş mi?

☐ 8. Risk Değerlendirme ve risk iyileştirme süreçlerinde belirlenmiş şartları karşılayacak güvenlik kontrollerine karar verilmiş ve uygulanmış mı? (Güvenlik Kontrol Örneklerine Bakın)

☐ 9. Yönetim BGYS uygulanmasına ve artık risk düzeylerine onay vermiş mi?

☐ 10.ISO/IEC 27001 Ek A'da seçilmiş olan konular için hazırlanmış olan Uygulanabilirlik Bildirgesi bulunuyor mu? Uygulanabilirlik Bildirgesinde seçilen veya seçilmeyen maddelerin sebepleri ve uygulama düzeyleri tarif edilmiş mi?

B. UYGULAMA VE OPERASYON

☐ 1. Bilgi Güvenliği Risklerini yönetmek için, öncelikleri belirleyen, faaliyetleri tanımlayan, kaynakları belirleyen ve parasal kaynakları ortaya koyan risk iyileştirme planı mevcut mu?

☐ 2. Risk iyileştirme planları ve tanımlanan güvenlik kontrolleri uygulanabilir mi?

☐ 3. Etkili kontrol için ölçümler tanımlanmış mı?

☐ 4. Eğitim ve bilinçlendirme programları uygulanıyor mu?

☐ 5. BGYS operasyonları ve gerekli kaynaklar yönetiliyor mu?

☐ 6. Prompt tespitini sağlayan kontroller ve güvenlik olaylarına müdahaleler uygulanıyor mu?

C. İZLEME VE GÖZDEN GEÇİRME

☐ 1. İlgili tarafların yaptığı tetkiklerin, gerçekleşen olayların, yapılan ölçümlerin ve geri beslemelerin sonuçları kullanılarak düzenli gözden geçirme yapılmakta mı?

☐ 2. BGYS tetkikleri planlı aralıklarla ve belirlenmiş iş planına göre yapılmakta mı? Bulgular için zamanında ve etkili olarak gerekli tedbirler alınmakta mı?

☐ 3. BGYS'nin uygunluğunun devam ettiği ve etkililiğini tespit için yönetim gözden geçirmeleri planlanan aralıklarla yapılmakta mı?

D. SÜRDÜRME VE İYİLEŞTİRME

☐ 1. Belirlenen amaçlara ulaşmak için iyileştirmeler tespit ediliyor, uygulanıyor ve değerlendiriliyor mu?

☐ 2. Düzeltici ve önleyici faaliyetler tanımlanıyor ve uygulanıyor mu? iç ve dış kaynaklardan elde edinilen öğrenilmiş dersler hayata geçiriliyor mu?

E. DOKÜMANLAR VE KAYITLAR

☐ 1. Yönetim sistemi ile ilişkili dokümanlar ve kayıtlar belirlenmiş prosedürlere göre yönetiliyor ve kontrol ediliyor mu?

F. YÖNETİMİN BAĞLILIĞI

☐ 1. Yönetimin BGYS'ine olan bağlılığını gösterecek kanıtlar mevcut mu? (Politika ve hedeflerin oluşturulması ve organizasyonun tümünde bu hedeflere ulaşmanın öneminin iletilmesi.)

☐ 2. BGYS'nin oluşturulması, uygulanması, yürütülmesi, izlenmesi ve gözden geçirilmesi için gerekli kaynaklar oluşturulmuş mu? Sorumluluklar tanımlanmış mı?

☐ 3. BGYS'yi yürütmekle yükümlü personelin yetkinliği ve eğitimi, bu işleri yapabilmek için yeterli mi?

☐ 4. İlgili personel bilgi güvenliği faaliyetlerinden haberdar mı? Bu faaliyetlerin hedeflerini yerine getirmeye nasıl katkıda bulunacağını biliyorlar mı?

G. GÜVENLİK KONTROL ÖRNEKLERİ

Bu bölüm risk değerlendirme ve riskleri iyileştirme süreciniz sırasında kullanabileceğiniz güvenlik kontrol örneklerini içermektedir.

☐ 1. Tedarikçilerinizle sözleşmeleri, çalışanlarınızla çalışma şartlarınızı içeren gizlilik anlaşmanız bulunmakta mı?

☐ 2. Dış kuruluşlarla, özel gruplarla ve/veya bilgi güvenliği uygulamalarınızı gözden geçiren bağımsız kişilerle sözleşmeleriniz bulunmakta mıdır?

☐ 3. Dışarıdan gelecek bilgi güvenliği risklerinizi belirlediniz mi? Güvenlik gerekleriniz sözleşme veya anlaşmalarda tarif edilmiş mi?

☐ 4. Organizasyonel varlıklarınızın envanterini, bunların sorumlularını ve kabul edilebilir kullanım şekillerini belirlediniz mi?

☐ 5. Bilgi sınıflama kılavuzu ve bu sınıflama yapısına göre işaretleme ve işlenmesi ile ilgili bir prosedürünüz var mı?

☐ 6. Personel adaylarının geçmişlerini uygun yönetmeliklere göre ve iş gereklilikleri doğrultusunda doğruluyor musunuz?

☐ 7. Güvenlik ihlali yapan personel için disiplin süreci uygulanıyor mu?

☐ 8. Personel değişikliği ve ayrılmaları için uygulanacak yöntemler açık olarak tanımlanmış mı? Varlıkların iade edilmesi, erişimin engellenmesi veya sınırlandırılmasıyla ilgili tanımlamalar yapılmış mı?

☐ 9. Teslim ve yükleme noktalarına erişimde dahil olmak üzere, tesislere, ofislere ve güvenliği hassas olan yerlere giriş kontrolleri yapılıyor mu ? Fiziksel güvenlik alanları oluşturulmuş mu?

☐ 10.Dışarıdan ve çevreden gelecek tehditlere karşı koruma önlemleri aldınız mı? Tesislerinizi ilgili risklere göre donattınız mı?

☐ 11.Destek ekipmanları bozulmalara karşın korunmakta mı? Kablolar hasara ve kesintilere karşı korunmakta mı?

☐ 12.Sürekli kullanılabilir olmasını temin etmek için ekipmanların uygun şekilde bakımları ve testleri yapılmakta mı?

☐ 13.Kullanımdan kalkan ekipman için güvenlik uygulamaları hayata geçiriliyor mu? Ekipman güvenli şekilde atık olarak bertaraf veya tekrar kullanıma hazır ediliyor mu?

☐ 14.Dokümante edilmiş operasyon prosedürleriniz mevcut mu? Değişiklikler kontrol ediliyor mu?

☐ 15.Güvenlik gereklerini dikkate alarak işlerini yapan kişilerin görevlerini belirlediniz mi?

☐ 16.İşletim sistemine giriş yetkisi olmayan kişilerin erişim riskini azaltmak için, geliştirme, test ve operasyon tesisleri birbirlerinden ayrı mı?

☐ 17.3. kişiler tarafından verilen servis hizmeti için güvenlik unsurlarını içeren formal bir anlaşma var mı? Değişim yönetimi dikkate alınarak risk seviyesine göre izleniyor, gözden geçiriliyor mu?

- [ ] 18.Sistem performansını güvence altına almak ve ileride gerekli olacak tahmini sistem gerekliliklerine göre kapasite yönetimi planlanıyor mu?
- [ ] 19.Yeni ve değişen sistem gereklerine göre kabul kriterleri tanımlanmış mı? Kabulden önce geliştirme esnasında testler gerçekleştiriliyor mu?
- [ ] 20.Kötü niyetli kodları tespit etme, önleme ve düzeltmeyle ilişkili kontroller ve gerekli bilinçlendirme prosedürleri uygulanıyor mu?
- [ ] 21.Bilgilerin ve yazılımların yedekleri düzenli olarak alınıyor mu? Yedekler belirlenen yedekleme politikası doğrultusunda test ediliyor mu?
- [ ] 22.Tehditlerden korunmak ve güvenliği temin etmek için uygulama ve sistemlerin bulunduğu ağlar (network) kontrol ediliyor mu? Bu güvenlik gereklerinin bakımı için bir anlaşma var mı?
- [ ] 23.Taşınabilir medya için taşıma, depolama, kullanımıyla ilgili bir prosedür bulunuyor mu?
- [ ] 24. 3. taraflarla paylaşılacak olan bilgilerin ve yazılımlarla ilgili politika mevcut mu?
- [ ] 25.Elektronik mesajlaşma da dahil olmak üzere birbirleriyle etkileşim içinde olan iş sistemlerinin bilgilerinin korunmasına dair bir politika var mı?
- [ ] 26.Elektronik ticaret, online işlemler ve halka açık bilgilerin kontrolleri uygulanıyor mu?
- [ ] 27.Kullanıcıların faaliyetlerine ait loglar, sistem olayları ve üretilen sistem yönetim faaliyetleri tutuluyor mu? Oluşabilecek karışıklığa karşı korunuyor mu?
- [ ] 28.Hata logları ve sistem hataları izleniyor, düzenli olarak gözden geçiriliyor mu? Gerekli faaliyetler yürütülüyor mu?
- [ ] 29.İş ve güvenlik gerekleri için erişim kontrol politikası bulunuyor mu?
- [ ] 30.Düzenli kullanıcı kayıt prosedürü bulunuyor, şifreler ve kullanım hakları yönetiliyor mu? Bu haklar düzenli olarak gözden geçiriliyor mu?
- [ ] 31.Kullanıcılardan ekipman ve tesislerin kullanımına karşı güvenlik yönetim kurallarına uymaları bekleniyor mu?
- [ ] 32.Network hizmetlerinin kullanımına ilişkin bir politika var mı? Network korumasına ve network'e bağlı ekipmanlarının korumasına dair bir iyi yönetim pratiği mevcut mu?
- [ ] 33.İşletim sistemine erişim güvenli log on olma prosedürleriyle kontrol ediliyor, kullanıcılar ayrı ayrı tespit edilebiliyor mu? Sistem araçlarının kullanımı sınırlandırılmış mı?
- [ ] 34.Mobil çalışma ve/veya telefonla çalışmayla ilgili politika, güvenlik ölçümleri ve prosedürler bulunuyor mu?
- [ ] 35.Yeni ve değişen bilgi sistemleri için güvenlik şartları tanımlanmış mı?
- [ ] 36.Kritiptolojik kontroller ve kriptografik anahtar kontrolleri için kullanılan bir politika var mı?

- [ ] 37.Yazılımların yüklenmesi için kontroller uygulanmakta ve sistem veri testleri dikkatle seçilmekte mi ve kontrol edilmekte midir?

- [ ] 38.İşletim sisteminin güncellemesinden sonra kritik uygulamaların teknik gözden geçirmesi yapılıyor mu?

- [ ] 39.Dışarıya taşere edilmiş yazılım geliştirme faaliyetleri izleniyor ve yönetiliyor mu?

- [ ] 40.Güvenlik olayları ve zaafiyetine zamanında tedbir almak, öğrenme vesilesi olarak kullanmak ve bunları uygulamak için rapor hazırlanıyor ve kayıt altına alınıyor mu?

- [ ] 41.İş Sürekliliği için güvenlik unsurları dikkate alınıyor ve test ediliyor mu? Operasyonların tekrar faaliyete geçmesi için güncel planlar oluşturuluyor ve uygulanıyor mu?

- [ ] 42.İlgili bütün yasal ve sözleşmesel şartlar belirlenmiş mi ve bunlara uyumluluğun sürekliliğini sağlamak için bir yaklaşım tanımlanmış mı?

- [ ] 43.Bilgi sistemleryle ilişkili güvenlik politikaları, standartlar ve teknik uygunluk düzenli olarak kontrole tabi tutuluyor mu? Bilgi sistemleri tetkki araçları sınırlandırılmış ve kontrol altına alınmış mı?