DENETİM VE DOKÜMANTASYON BEKLENTİLERİ (BGYS)

ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ İÇİN
DENETİM ve DOKÜMANTASYON BEKLENTİLERİ

ISO 27001 belgelendirme denetimleri için beklentiler aşağıda verilmektedir:

1. Bilgi güvenliği yönetim sisteminin etkinliği ve uygunluğunun da görüşülmüş olduğu en az bir adet yönetim gözden geçirme faaliyeti tamamlanmış ve kayıt altına alınmış olmalıdır.

2. Standardın tüm maddelerinin denetlenmiş olduğu bir tam iç denetim çevrimi tamamlanmış ve kayıt altına alınmış olmalıdır.

3. Standardın gerektirmiş olduğu kayıtlarla ilgili en az 3 aylık geçmiş ibraz edilebilir olmalıdır.

4. Standardın ön görmüş olduğu dokümantasyon yapısı oluşturulmuş olmalıdır.

5. Organizasyonun politika, hedefler, uygulanabilirlik bildirgesi ve prosedürlerine uygunluk sağlamasını mümkün kılacak programlarla ilgili bulgular mevcut olmalıdır.

Bu beklentilerden herhangi birisi denetim tarihi itibarı ile eksiklik göstermekte ise lütfen YBM ile irtibat kurunuz.

Kuruluş ve kuruluşun bağlamı (içeriği)

Amaçlar ile ilgili olan ve BGYS'nin hedeflenen çıktılarını başarma kabiliyetini etkileyebilecek iç ve dış hususlar belirlenmiş mi?

İlgili Tarafların ihtiyaç ve beklentilerinin anlaşılması

BGYS ile ilgili taraflar belirlenmiş mi?

Yasal, düzenleyici ve sözleşme şartları dahil bu ilgili tarafların bilgi güvenliği ile ilgili gereksinimleri belirlenmiş mi?

BGYS'nin kapsamı

Dış ve iç hususlar, ilgili tarafların şartları ve kuruluş tarafından gerçekleştirilen faaliyetler arasındaki arayüzler, bağımlılıklar ve diğer kuruluşlar tarafından gerçekleştirilen faaliyetler göz önünde bulundurularak BGYS sınırları ve uygulanabilirliği belirlenmiş mi?

BGYS kapsamı dokümante edilmiş mi?

Dokümantasyon Rehberi

ISO 27001 BGYS için aşağıdaki dokümanların oluşturulması zorunludur:

- BGYS Kapsamı (4.3)
- BGYS Politikası ve Hedefler (5.2 & 5.6)
- Risk Analizi (6.1.2)
- Uygulanabilirlik Bildirgesi (SoA - 6.1.3.-d)
- Risk İşleme Planı (6.1.3-e & 6.2)
- Risk Değerlendirmesi (8.2)

- Roller ve Sorumluluklar (EK-A 7.1.2 & 13.2.4)
- Varlık Envanteri (Ek-A 8.1.1)
- Varlıkların kabul edilebilir kullanımı (EK-A 8.1.3)
- Erişim Kontrol Politikası (Ek-A 9.1.1)
- Bilgi teknolojileri için ihtiyaç duyulan operasyonel prosedürler (Ek-A 12.1.1)
- Güvenli Sistem Mühendisliği (Ek-A 14.2.5)
- Tedarikçi Zinciri Güvenlik Politikası (Ek-A 15.1.1)
- Olay Yönetimi Prosedürü (Ek-A 16.1.5)
- İş Sürekliliği prosedürü (Ek-A 17.1.2)
- Sözleşmelerden, düzenlemelerden ve yasal şartlardan kaynaklanan yükümlülükler (Ek-A 18.1.1)

ISO 27001 BGYS için aşağıdaki kayıtların tutulması zorunludur:

- Eğitim, yetkinlik ve tecrübe kayıtları (7.2)
- Ölçme ve izleme sonuçları (9.1)
- İç tetkik programı ve raporu (9.2)
- Yönetim gözden geçirme toplantı kayıtları (9.3)
- Düzeltici Faaliyet kayıtları (10.1)
- Kullanıcı işlem ve faaliyet kayıtları, hatalar ve ihlal olayları (Ek-A 12.4.1-3)

ISO 27001 BGYS tarafından zorunlu tutulmayan ancak olmasında fayda olan dokümanlar:

- Doküman ve kayıtların kontrolü prosedürü (7.5)
- İç tetkik prosedürü (9.2)
- Düzeltici faaliyetler prosedürü (10.1)
- Kendi cihazını getir politikası (BYOD) (Ek-A 6.2.1)
- Mobil cihazlar ve teleworking politikası (Ek-A 6.2.1)
- Bilgi sınıflandırma politikası (Ek-A 8.2.1-2-3)
- Şifre politikası (Ek-A 9.2.1-2-4, 9.3.1 ve 9.4.3)
- İmha ve yok etme politikası (Ek-A 8.3.2 ve 11.2.7)
- Güvenli alanlarda çalışma politikası (Ek-A 11.1.5)
- Temiz ekran ve temiz masa politikası (Ek-A 11.2.9)
- Değişiklik yönetimi politikası (EK-A 12.1.2 ve 14.2.4)
- Yedekleme politikası (Ek-A 12.3.1)
- Bilgi transferi politikası (Ek-A 13.2.1-2-3)
- İşe etki analizi (iş sürekliliği) (Ek-A 17.1.1)
- Deneme ve test planı (Ek-A 17.1.3)
- Bakım ve gözden geçirme planı (Ek-A 17.1.3)
- İş sürekliliği stratejisi (Ek-A 17.2.1)

UYGUNSUZLUKLAR

Uygunsuzluklar iki seviye olarak kategorize edilirler; minör ve majör uygunsuzluklar.

MİNÖR uygunsuzluk, yönetim sisteminin yapısından kaynaklanmayan ve önemli bilgi güvenliği riski oluşturmayan uygunsuzluk türüdür.

1. Firmanın dokümante edilmiş yönetim sistemi ya da gereksinimlerle ilgili kısmi uygunsuzluklar

2. Firma yönetim sisteminin uygulanmasında ciddi bilgi güvenliği riski oluşturmayan sapmalar

MAJÖR uygunsuzluk örnekleri aşağıda verilmektedir:

1. Sistemin gereksinimleri karşılayacak yapıyı oluşturmamış olması. Belirli bir gereksinimle ilgili olarak sistemsizliğe işaret olabilecek çok sayıda minör uygunsuzluk.

2. Önemli bilgi güvenliği problemine neden olabilecek her hangi bir uygunsuzluk. veri kaybı, sızmalar, yasalara uygun olmayan işlemler.

Uygunsuzluklar için cevaplar

Müşterilerin YBM tarafından tespit edilen uygunsuzluklar için kök sebep tespiti, düzeltici faaliyetlerin yürütülmesi ve doğrulanması konusunda kendi düzeltici faaliyet sistemlerini kullanmaları beklenir. Müşteri düzeltici faaliyet formları YBM uygunsuzluk numarasına referans vermeli ve denetçi tarafından tespit edilen zamanda işlem görmelidir.

Müşteri tarafından sağlanan düzeltici faaliyetler aşağıdaki şartları sağlamalıdır.:

Kök sebep analizi

Kök sebep analizi yapılmaması durumunda uygunsuzluğun tekrarının önüne geçilememesi muhtemeldir. Esasen kök sebep tespitinin yapılıp yapılmadığı şu sorunun cevaplanması ile ortaya çıkacaktır. “sebebi ortadan kaldırdık, ancak yine de bu uygunsuzluk tekrarlanabilir mi?” Eğer cevap hayır ise sebep doğru edilmiştir. Eğer cevap evet ya da belki ise sebebin daha detaylı analiz edilmesi gereklidir. Kök sebebe daha rahat ulaşım için “neden” sorusunun bir kaç kez sorulması çoğu zaman yeterli olur. Böylece düzeltici faaliyet uygunsuzluğun tekrarının önlemek üzere gerçekleştirilebilir.

Aşağıda bazı zayıf kök sebep tespitleri yer almaktadır:

- “Operatör hatası” ya da “Operatör gözden kaçırmış”
- “Zayıf eğitim” ya da “Eğitim etkin olmamış”,
- “Standart anlaşılmamış, ya da bunu bilmiyorduk”
- “Tek sefer yaşanan bir durum”

Bu kök sebeplerin kullanımı belgelendirme kurumunun daha derin araştırma talep etmesine sebep olacaktır zira tespitler olaya has değildir ve bu tespite istinaden yapılan düzeltici faaliyet uygunsuzluğun tekrarının önüne geçilmeyebilir. Bu tür durumlarda neden sorusu en azından bir kere

sorulmalıdır. Örnek vermek gerekirse, eğer operatör hatası ise acaba operatör doğru anahtarı kapatmak isterken benzer görünümlü bir diğerini mi seçmiştir. Bu kök sebep bizi hata önleme prensipleri uyarınca anahtarların birbirinden açık olarak ayrılmasına götürecektir.

Kök sebepler yönetimin üzerinde kontrolü olabileceği şekilde tespit edilmelidir. Kötü hava koşulları bir sebep olabilir ancak bu durumun tekrarını önlemek mümkün değildir. Bu hallerde kötü hava koşullarına karşı yetersiz acil durum planlaması daha doğru bir tespit olacaktır.

2. Aşağıdaki hususları içeren düzeltici faaliyet:

• Uygunsuzluğun boyutunun belirlenmesi, durdurulması ve düzeltilmesi ile ilgili düzeltici faaliyetler

• Kök sebebin ortadan kaldırılması ve böylece tekrarının önlenmesi amacıyla gerçekleştirilen düzeltici faaliyetler . Bu düzeltici faaliyetler proses değişikliklerine odaklanmalıdır.

Genel olarak düzeltici faaliyetler sadece durumun yani hatanın tamiri ile ilgilenmekte ancak tekrarının önlenmesi ile uğraşmamaktadır.

3. Düzeltici faaliyetlerin uygulanmasının doğrulama

Düzeltici faaliyetlerin doğrulanması ve bu doğrulamanın uygulama nesnel kanıtları ile gönderilmesi gereklidir (prosedürler, kayıtlar, resimler, kontrol planları vb.). Genel olarak, uygulanmayan düzeltici faaliyetler kabul edilemezler. Yapılan işin tabiatı gereği, zaman gerektiren ve uygulama doğrulaması daha sonra yapılabilen düzeltici faaliyetler hedef tarih ve yeterli gerekçe ile birlikte gönderilmelidir.

Not: Standard maddeleriyle ilgili verilen bilgiler rehber niteliği taşımaktadır. Eksik veya denetlenen tarafa uygun olmayan bir durum söz konusu olduğunda YBM bu durumda sorumlu tutulamaz.