



1. AMAÇ

Bu prosedürün amacı; Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı içerisinde ve tedarikçi firmalarda uygulanacak denetimlerin yöntemi ve organizasyonu açıklamaktır.

2. KAPSAM

Bu prosedür, Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı içi denetimleri, tedarikçi denetimlerini gerçekleştirecek denetçileri kapsar.

3. TANIMLAR

4. REFERANSLAR

Bu dokümana ait referans yoktur.

5. UYGULAMA

İç Denetimler

Başta Bilgi Güvenliği Yönetim Sistemi olmak üzere uygulanan tüm yönetim sistemlerine yönelik standart gerekliliklerini karşılama konusundaki etkinliğinin, bilgi varlıklarının güvenliğinin sağlanması ve kontrol altına alınması konusundaki durumunu analiz etmek ile iş süreçlerinin etkinliği ve verimliliğinin kontrolü için iç denetimler gerçekleştirilir. Bu denetimler planlı, tarihleri belirlenmiş, sorumluları tespit edilmiş ve yeterli kalifikasyona sahip denetçiler tarafından yapılmaktadır.

Denetçiler, denetlenecek süreç üzerinde direkt ilişkisi olmayan, tarafsız kişilerdir. Kendileri ile direkt ilgisi olmayan süreçleri denetlerler. Denetim sonuçları yönetimin gözden geçirme toplantılarında ele alınır. Uygunsuzluklar için düzeltici ve önleyici faaliyetler planlanır ve gerçekleştirilir. Takip denetimleri ile istenilen sonuçlara ulaşıp ulaşılamadığı kontrol edilir.

Bilgi Güvenliği Yönetim Sistemi Denetimi

BGYS Yönetim Sistemi dokümantasyonuna ait gözden geçirmeler prosedür ve gerekli olan talimatlardaki “Gözden Geçirme” maddesi uyarınca minimum 12 ayda 1 defa gözden geçirilir. BGYS yönetim sistemi denetimi her yılın başında, bir önceki yılın sonuçları göz önüne alınarak, bir sonraki yıl için Yönetim Temsilcisi tarafından hazırlanır ve BİDB Yönetici onayı ile uygulamaya geçirilir. Denetim planı, tüm bölümlere duyurulur. Tüm bölümler süreçler bazında denetim kapsamındadır. BGYS iç denetimleri BGYS kapsamına giren bölümleri kapsamaktadır.

BGYS denetimleri ISO 27001, ISO 27002 standartları ve yasalar ile sözleşmelerden doğan şartlar referans alınarak gerçekleştirilir. BGYS tetkikleri planlanırken ISO 27001 Standardının Ek-A dahil olmak üzere tüm maddeleri denetim kapsamına dahil edilmesi standardın zorunluluğudur. Planlamada eksik madde kalmadığından emin olunmalıdır.

Planlama

Firma içi sistem ve süreç denetimleri, firma içerisinde denetçi yetkinliğine sahip kişilerden ve ilgili bölümden bağımsız denetçiler tarafından gerçekleştirilir. Denetimlerin kapsamına bağlı olmak üzere yönetim sistemleri denetimleri (yönetim sistemince aksi talep edilmediği sürece) yılda en az 1 kez, Süreç denetimleri ise bir yıl içerisinde 4 kez gerçekleştirilir.

Denetimler planlanırken, geçmiş yılda oluşmuş iç ve dış uygunsuzluklar, müşteri şikâyetleri, geçmiş iç denetimlerde elde edilmiş performans, müşteri denetim sonuçları, bir ürün veya faaliyetin yeni devreye girmiş olması gibi unsurlar dikkate alınır.

Tüm denetimlerde genel olarak uygulanması gerekli etaplar:

Planlama/Hazırlık: Denetim prosedürlerinde, planlama gerekliliği ve dönemleri açıklanmıştır. Plansız yapılabilen denetimler periyodik olarak gerçekleştirilir.

Denetim: Denetimler ile ilgili hazırlanmış standart soruların sorulması ve ilgili talimatlara göre gerçekleştirilir.

Puanlama/ Sınıflama: Her denetim sonucu bir puanlama yapılması tercih edilmekle birlikte, Puanlama yapılamayacak denetimlerde uygunsuzlukların tespit edilip ortadan kaldırılması amaçlanır.

Raporlama: Tüm denetim sonuçları, talimatlarda belirtildiği şekilde bir rapor ile ilgili kişi ve birimlere yayınlanır. Denetimin yapılma gerekçesi ve hedefi denetim raporunda yer almalıdır.

Denetim sonuçlarının izlenmesi: Yapılan denetim sonucunda tespit edilen uygunsuzluklar için hazırlanmış uygunsuzluk raporları veya düzeltici faaliyet aksiyon planlarına göre uygunsuzlukların giderilmesi için yapılan çalışmaların izlenmesidir. Denetim aksiyonları DÖF olarak açılır ve sistemde DÖF takip tablosuna işlenerek takip edilir.

Sene başında gerçekleştirilen denetim planlamasında erteleme ve sapmalar için; denetlenecek bölüm veya tedarikçinin talebi (Firma içinde maksimum 4 hafta- Tedarikçi için 8 hafta), BİDB içerisinde müşteri veya 3. taraf denetimleri ile çakışma durumunda ise, BİDB Yöneticisinin kararı ile maksimum 4 hafta erteleme yapılabilir. Bu ertelemeler denetim planı üzerinde gösterilir.

Denetimden iki hafta önce denetim göreceк bölüm sorumluları ile BGYS Yönetim temsilcisi denetim tarihi konusunda mutabakat sağlar. Ertelemeler bu dönemde talep edilmelidir. Yönetim temsilcisi hangi sürecin/bölgenin kimin tarafından denetleneceğini saptar. Belirlenen kişi veya kişiler denetleneceği süreç ile ilgili hazırlıklarını denetim tarihinden 2 gün öncesine kadar hazırlar. Denetlenecek süreç sorumluları, denetleme tarihine kadar denetim için gerekli olan tüm imkân ve dokümanları hazır bulundurmaktan ve denetçiye gerekli kolaylığı sağlamaktan sorumludur. Her süreç denetlenirken son 3 denetimde çıkmış olan uygunsuzluklar dikkate alınır. Önceden çıkmış uygunsuzluklara öngörölmüş faaliyetin etkinliği denetlenir.

Denetçi Seçimi ve Kalifikasyonları

Firma içerisinde veya tedarikçilerde yapılması gereken her türlü denetim; eğitim ve deneyimi yeterli görölen bağımsız denetçiler tarafından ilgili denetim talimatlarına göre gerçekleştirilir. Denetimlerde görev alan denetçilerin denetlenen



bölüm veya alandan bağımsız olması tüm denetimler için geçerlidir. Denetçilerin herhangi bir standarda ait “İç Tetkikçi” eğitimini almış ve belgesine sahip olması gerekmektedir. En az bir denetim gerçekleştirmiş veya gözlemci olarak katılmış olması gerekmektedir.

Denetim Sonrası Raporlama ve Düzeltici Faaliyetler

Denetçi, denetimi gerçekleştirdikten sonra denetim raporunu veya uygunsuzlukları, iyileştirmeye açık alanları ve güçlü yönleri açıklayan raporu Yönetim Temsilcisine iletir. Denetim raporunda belirtilen uygunsuzluklar için standart Düzeltici – Önleyici Faaliyet Formu kullanılarak uygunsuzluğun kök nedeni, düzeltici faaliyet ve önleyici faaliyetler, bunların sorumluları ve süreleri belirlenir. Bu düzeltici faaliyetlerin takip edilmesi ve koordinasyonu Yönetim Temsilcisi ile birlikte DÖF açılan bölüme / süreç sahibine aittir.

Belirlenen düzeltici ve önleyici faaliyetler için gerekli görülmesi halinde takip denetimi yapılır. Takip denetiminin uygunsuzluğu tespit eden denetçinin gerçekleştirmesi tercih edilir. Uygunsuzluk tespit edilmemiş olsa dahi, iyileştirmeye açık olan konular denetim raporuna yazılır. İç denetimlerde belirlenen eksiklikler kalite geliştirme planlarına alınarak, sürekli iyileştirme prensibine uygun olarak, aksiyonları yaygınlaştırma prensibi ile ele alınarak izlenir.

Denetlemeden amaç, tüm maddelerin UYGUN DURUM seviyesine gelmesinin sağlanmasıdır. Denetçi tarafından belirlenen majör/minör hatalar için DÖF düzenlenir. Uygunsuzlukların kapatılması için öngörülen süre max. 60 gündür. Yatırım gerektiren konular hakkında düzeltici faaliyetlerin yerine getirilmesi süresi ise, BİDB Yöneticisi inisiyatifi ile belirlenir.

Firma içi BGYS Sistem sonuçları yönetimin gözden geçirme toplantılarının gündem maddesidir. Bu toplantılarda açık ve kapalı uygunsuzluklar ve iyileştirmeye açık alanlar ve kapanma süreleri değerlendirilir.

SORUMLULUK

İç tetkik Prosedürünün güncellenmesi BGYS Yönetici temsilcisinin sorumluluğundadır. İç tetkik sürecinin yönetimi ise BİDB Yöneticisi sorumluluğundadır.

KONTROL

Dokümanlar ihtiyaç halinde revize edildiği gibi, yılda bir kez periyodik olarak kontrol edilir.

EKLER

- LS BGYS 002 İç Tetkik Soru Listesi.
- FR 5.4.3_01 Yıllık İç Tetkik Planı Formu