KONTROLLERİN ETKİNLİĞİNİ ÖLÇME PROSEDÜRÜ

1. AMAÇ

Bu prosedürün amacı, Bilgi İşlem Daire Başkanlığı Bilgi Güvenliği Yönetim Sistemi kapsamında etkinliği ölçülecek kontrollerin seçim kriterlerini belirlemek, ölçüm süreci ve sorumluluklarını tanımlamaktır.

1.1. Etkinlik Ölçümü İçin Kontrol Seçimi

1.1.1. Etkinliği ölçülecek kontrol seçimleri aşağıdaki kriterlere göre yapılır.

- Risk işlemeden gelen kontroller
- Bilgi teknolojileri teknik altyapısını etkileyen kontroller
- Yoğun oranda yönetim gözetimi ve bakım gerektiren kontroller
- Sürekli operasyon ve bakım maliyeti doğuran kontroller
- Kritik sistemlere ilişkin kontroller
- Yasalardan /mevzuattan kaynaklanan kontroller
- Sözleşmelerden kaynaklanan kontroller
- Üst yönetimin istediği kontroller
- Bir güvenlik kırılmasından sonra yapılan kontroller
- Tespit edilen açıklıkları izlemek amacı ile yapılan kontroller
- Aksiyon alınması kabul edilmiş düzeltici / önleyici faaliyetler için seçilen kontroller

1.1.2. Etkinliği ölçülecek kontroller, yukarıda tanımlanmış kriterlere göre seçilir ve BGYS Temsilcisinin onayına sunulur.

1.1.3. Kontroller seçildikten sonra kriterler, hedef değerler, ölçüm sıklığı ve ölçümden sorumlu personel "**Etkinliği Ölçülecek Kontroller Listesi**"nde belirtilir.

1.1.4. Seçilecek kriterler kontrolün etkinlik ve performansına ilişkin anlamlı, kullanışlı ve ölçüm maliyeti ekonomik kriterler olmalıdır.

1.1.5. Ölçüm sıklığı belirlenirken yapılan ölçümün makul derecede güncel durumu ve etkinlik derecesinin değişimini ifade edecek biçimde belirlenmesine gayret edilir.

1.1.6. Etkinlik hedefleri BGYS Koordinatörlüğü tarafından ilgili kontrolün mevcut etkinlik derecesi, kontrolün ilgili olduğu riskin derecesi, kontrolün ilk uygulanmasından bu yana geçen zaman ve diğer faktörler göz önüne alınarak belirlenir. Kontrol etkinlik hedefleri yılda en az bir defa veya daha önce BGYS Koordinatörlüğü tarafından gerekli görüldüğünde düzenlenir.

1.2. Ölçüm Süreci

1.2.1. BGYS ekibi kendisi tarafından gerçekleştirilen veya kontrol sahiplerinden temin edilen ölçüm sonuçlarını toplar ve listeye aktarır.

1.2.2. Liste güncellenirken aşağıdaki kurallar uygulanır:

a) İptal edilen kontrollere ilişkin daha önceki ölçüm kayıtlarının kaybedilmemesi için kontrolle ilgili "Ölçüm Sıklığı" alanına "İptal" yazılır. Listeden bilgi silinmez.

b) Ölçülecek kriterlerde bir değişiklik olduğu durumlarda kontrolün iptal edilmesi durumunda yapıldığı gibi kontrol ve metrik kaydının "Ölçüm Sıklığı" alanına "İptal" kaydı düşülür. Değiştirilmiş metrik için yeni bir satır açılarak kontrol ve metrik kaydı yapılır.

1.2.3. Yapılan kontrol ölçüm sonuçları düzeltici önleyici faaliyet planlamasının yapılmasına neden olabilir.