1. AMAÇ

Bu prosedürün amacı; ISO/IEC 27006 standardı doğrultusunda, denetimlerin gerçekleştirilmesi için yöntem ve sorumlulukları belirlemektir.

2. TANIMLAR

Bilgi Güvenliği Yönetim Sistemi (BGYS): Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası.
Varlık: Kuruluş için değeri olan herhangi bir şey. [ISO/IEC 13335-1: 2004]
Kullanılabilirlik: Yetkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliği. [ISO/IEC 13335-1: 2004]
Gizlilik: Bilginin yetkisiz kişiler, varlıklar ya da proseslere kullanılabilir yapılmama ya da açıklanmama özelliği. [ISO/IEC 13335-1: 2004]
Bilgi Güvenliği: Bilginin gizliliği, bütünlüğü ve kullanılabilirliğinin korunması. [ISO/IEC 17799: 2005]
Bilgi Güvenliği Olayı: Olası bir bilgi güvenliği politikası açığı, koruyucuların başarısızlığı ya da güvenlikle ilgili olabilecek önceden bilinmeyen bir durumu belirten bir sistem, hizmet ya da ağ durumunun tanımlanan bir ortaya çıkışı. [ISO/IEC TR 18044: 2004]
Bilgi Güvenliği İhlal Olayı: İş operasyonlarını tehlikeye atma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek istenmeyen ya da beklenmeyen bilgi güvenliği olayı. [ISO/IEC TR 18044: 2004]
Bütünlük: Varlıkların doğruluğunu ve tamlığını koruma özelliği. [ISO/IEC 13335-1: 2004]
Artık Risk: Risk işlemeden sonra kalan risk.[ISO/IEC Guide 73]
Riskin Kabulü: Bir riski kabul etme kararı.
Risk Analizi: Kaynakları belirlemek ve riski tahmin etmek amacıyla bilginin sistematik kullanımı.[ISO/IEC Guide 73]
Risk Değerlendirme: Risk analizi ve risk derecelendirmesini kapsayan tüm proses. [ISO/IEC Guide 73]
Risk Derecelendirme: Riskin önemini tayin etmek amacıyla tahmin edilen riskin verilen risk kriterleri ile karşılaştırılması prosesi. [ISO/IEC Guide 73]
Risk Yönetimi: Bir kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetler. [ISO/IEC Guide 73]
Risk İşleme: Riski değiştirmek için alınması gerekli önlemlerin (kontrollerin) seçilmesi ve uygulanması prosesi. [ISO/IEC Guide 73]
Uygulanabilirlik Beyanı (SOA): Müşteri kuruluşun BGYS'si ile ilgili ve uygulanabilir kontrol amaçlarını ve kontrolleri açıklayan dokümante edilmiş beyan (kontrol amaçları ve kontroller, risk değerlendirme ve risk işleme proseslerinin sonuçları ve çıkarımlarını, yasal ve düzenleyici gereksinimleri, anlaşma yükümlülüklerini ve kuruluşun bilgi güvenliği için iş gereksinimlerini temel alır).

3. İLGİLİ DOKÜMANLAR

BQYSEK.01 Kalite El Kitabı
BQF.44 Aşama 1 Denetim Raporu
BQF.45 Denetim Raporu

Hazırlayan	Onaylayan
Yönetim Temsilcisi	*Genel Müdür*

4. UYGULAMA

4.1. Genel

BGYS denetimleri, Denetim Prosedüründe belirlenen denetim uygulamaları doğrultusunda ve aşağıda verilen esaslar dikkate alınarak gerçekleştirilir.

4.2. BGYS Denetim Şartları

Belgelendirme denetiminden önce müşteri kuruluşa denetim ekibinin görmesini istemedikleri gizli ya da hassas bilgi içeren kayıtları olup olmadığı BGYS Başvuru Kontrol Formunda sorulur.

Sonrasında ASCERT denetim ekibi, bu kayıtların yokluğunda BGYS'nin yeterince denetlenip denetlenemeyeceğine karar verir.

Eğer bu kayıtların yokluğunda denetim yapılamayacağına karar verilirse müşteri kuruluşa erişim için gerekli düzenlemeler yapılmadan denetim yapılamayacağı bildirilir.

4.2.1. Denetim Kriterleri

Bir müşteri kuruluşun BGYS denetimi ile ilgili kriterler; BGYS standardı ISO/IEC 27001'de belirtilenler ve ilgili faaliyetler için oluşturulan dokümanlardan oluşur.

4.2.2. Belgelendirme Kapsamı

Müşteri Kuruluş, BGYS Kapsamını Belgelendirme Başvuru Formunda belirtir, ASCERT denetim ekibi, müşteri kuruluşunun BGYS'sinin kapsamının ve sınırlarının, kuruluşun bağlamı doğrultusunda; işin, kuruluşun yerinin, varlıklarının ve teknolojik özelliklerinin dikkate alınarak, açıkça tanımlanmış olduğunu garanti eder.

4.2.3. Çok Sahalı Kuruluşların Denetimi

Çok sahalı kuruluşların denetiminde, aşağıdaki şartların yerine getirildiği incelenir:

- Sistem dokümantasyonu ve sistem değişiklikleri,
- Yönetimin gözden geçirmesi,
- Şikâyetler,
- Uygunsuzluk ve düzeltici faaliyetlerin değerlendirilmesi,
- İç denetimlerin planlanması ve sonucun değerlendirilmesi.

Çok sahalı kuruluşlarda, tespit edilen uygunsuzluklar için gerçekleştirilen takip denetimlerinde, merkez büro veya sahaların en azından birinde, yönetim sisteminde ve/veya uygulamasında devam eden uygunsuzluklar tespit edilmesi durumunda, belgelendirme yapılmaz veya mevcut belgelendirme iptal edilir.

4.2.4. Denetim Metodolojisi

BGYS denetimlerinde; Aşama 1 Denetim Raporu ve Denetim Raporu kullanılarak, sistemin ISO/IEC 27001 standardı gereklerine uygun olarak kurulmuş, dokümante edilmiş ve etkin olarak uygulanmakta olduğu incelenir.

ASCERT denetim ekibi, müşteri kuruluşun;

- ISO/IEC 27001'de belirtilen gereklere, BGYS'nin kapsamında uyduğuna dair hususları,

- Bilgi güvenliği risk değerlendirmesi ve risk karşısındaki davranışının ISO/IEC 27001'de belirtilen gerekliliklerle uyumlu olduğunu ve buna ilişkin ifadelerin BGYS ve Uygulanabilirlik Beyanında açıkça yansıtıldığını,
- BGYS kapsamında bulunmayan hizmet ya da faaliyetlerle olan bağlantı noktalarının, belgelendirmeye tabi BGYS kapsamında belirtilmesini ve müşteri kuruluşun bilgi güvenliği risk değerlendirmesinde yer aldığını

teyit eder.

4.3. İlk Belgelendirme Denetimi

4.3.1. Aşama 1

Aşama 1'de ASCERT denetim ekibi, sistemle ilgili dokümantasyonu ISO/IEC 27001 standardında istenen dokümantasyonu da kapsayacak şekilde Aşama 1 Denetim Raporu ile inceler.

Aşama 1'in amacı, müşteri kuruluşun BGYS politika ve amaçları bağlamında ve özellikle denetim için müşteri kuruluşun hazırlık durumu kapsamında BGYS'sinin anlaşılması ve Aşama 2 planlaması için odaklanma sağlamaktır.

Aşama 1, doküman gözden geçirmeyi içerir ancak bununla sınırlı değildir. ASCERT, müşteri kuruluşu ile doküman gözden geçirmenin ne zaman ve nerede yapılacağı konusunda mutabakat sağlar. Her durumda, doküman gözden geçirme Aşama 2'nin başlangıcından önce tamamlanır.

Aşama 1'in sonuçları, Aşama1 Denetim Raporunda dokümante edilir. ASCERT denetime, Aşama 2 ile devam edip etmeme konusunda karar vermeden önce ve gerekli yeterliliklere sahip Aşama 2 ekip üyelerinin seçilmesi için, Aşama 1 denetim raporunu gözden geçirir.
ASCERT, müşteri kuruluşu, Aşama 2 sırasında detaylı inceleme için gerekli olabilecek daha fazla farklı türde bilgi ve kayıt hakkında bilgilendirir.

1. aşamanın sonuçları yazılı bir rapor halinde belgelenecektir. Belgelendirme kuruluşu, 2. aşamaya devam etmeye karar vermeden önce 1. aşama denetim raporunu gözden geçirecek ve 2. aşama denetim ekibi üyelerinin gerekli yetkinliğe sahip olup olmadığını teyit edecektir; bu, yetkin ve uygun görülmesi halinde, 1. aşama denetimini yürüten ekibe liderlik eden denetçi tarafından yapılabilir.

NOT Bağımsız gözden geçirme (yani, denetime dahil olmayan belgelendirme kuruluşundan bir kişi tarafından), 2. aşamaya kiminle geçilip geçilmeyeceğine karar verilirken ilgili riskleri azaltmak için bir önlemdir.
Bununla birlikte, aynı hedefe ulaşmak için başka risk azaltma önlemleri halihazırda yürürlükte olabilir.

4.3.2. Aşama 2

Aşama 2 her zaman müşterinin sahasında gerçekleştirilir. ASCERT, Aşama 1 denetim raporunda dokümante edilmiş bulgulara dayalı olarak, Aşama 2'nin yürütülmesi için bir denetim planı hazırlar.
Aşama 2'nin amaçları şunlardır:

a) Müşteri kuruluşun kendi politikaları, hedefleri ve prosedürlerine bağlı olduğunun teyit edilmesi.
b) Aşama 2, müşteri kuruluşu ile ilgili olarak aşağıdakilere odaklanır:
c) Üst yönetim liderliği ve bilgi güvenliği politikası ve bilgi taahhüdü güvenlik hedefleri;
d) ISO/IEC 27001'de istenen dokümantasyon şartları,
e) Bilgi güvenliği ile ilgili risklerin değerlendirilmesi ve değerlendirmelerin tutarlı, geçerli ve karşılaştırılabilir sonuçları,
f) Bilgi güvenliği ile ilgili risklerin değerlendirilmesi temelinde, kontrol amaçlarının ve risk işleme proseslerine dayanan kontrollerin seçimi,
g) Bilgi güvenliği performansı, bilgi güvenliği hedefleri ve BGYS'nin etkinliğinin gözden geçirilmesi,
h) Seçilmiş ve uygulanmış kontroller, Uygulanabilirlik Beyanı ve risk değerlendirme ve risk işleme prosesinin sonuçları ve BGYS politikası ve amaçlarının aralarındaki ilişki,
i) Dış ve iç bağlamı da dikkate alarak kontrollerin uygulanması ve belirtilen hedefleri sağlayacak şekilde etkin olup olmadığını belirlemek için, müşteri kuruluş tarafından yapılan bilgi güvenliğini izleme, ölçme ve analizi, prosesler ve kontroller, kontrollerin uygulanıp yürütülmeyeceğini ve etkili olup olmadığının belirlenmesi kontrollerin etkinlik ölçümleri de dikkate alınarak kontrollerin uygulanması,
j) Programlar, prosesler, prosedürler, kayıtlar, iç denetimler ve BGYS etkinliğinin gözden geçirilmesi, bunların üst yönetim kararlarına ve BGYS politikasına ve hedeflerine izlenebilir olmalarının sağlanması.

4.3.3. İlk Belgelendirme İçin Bilgi

ASCERT, belgelendirme kararına ilişkin bir esas sağlamak amacıyla denetim ekibinden, bu karara varmak için yeterli bilgiyi sağlayan Denetim Raporunu açık anlaşılır olarak talep etmektedir.

4.4. Gözetim Denetimleri

Gözetim denetimlerinin amacı, onaylanmış BGYS'nin uygulanmaya devam ettiğini onaylamak, müşteri kuruluşun operasyonlarının değişmesi nedeniyle başlayan değişimlerin sonuçlarını değerlendirmek ve belgelendirme gerekliliklerine sürekli uyumun devam ettiğini görmektir. Gözetim denetimleri normalde şunları kapsamaktadır:

a) BGYS iç denetimi, yönetim gözden geçirmesi, uygunsuzluk ve düzeltici faaliyetler olmak üzere sistemin sürdürülmesine yönelik unsurlar,
b) ISO/IEC 27001 standardı ve belgelendirme için gerekli olan diğer dokümanların gerektirdiği dış taraflarla olan iletişim,
c) Dokümante edilmiş sistemdeki değişiklikler,
d) Değişikliğe tabi olan alanlar,
e) ISO/IEC 27001'ün seçilen unsurları,
f) Seçilen diğer uygun alanlar,

ASCERT tarafından yapılan gözetim denetimlerinde en az aşağıdakiler gözden geçirilir:

a) BGYS'nin müşteri kuruluşun bilgi güvenliği politikasının amaçlarını başarmak doğrultusunda etkinliği,

b) Periyodik değerlendirme için prosedürlerin işleyişi ve ilgili bilgi güvenliği yasa ve düzenlemeleri ile uyumluluğun gözden geçirilmesi,
c) Bir önceki denetimde tespit edilen uygunsuzluklara dair yapılan işlemler.

Gözetim denetimlerinde, ISO/IEC 17021'de gözetim denetimi için gerekli olan noktalara ek olarak, aşağıdaki konular da kapsanır:

a) ASCERT, varlıklara olan tehditleri, müşteri kuruluşun açıklıkları ve etkiler ile ilgili bilgi güvenliği konularına kendi gözetim programını uyumlaştırmakta ve programı gerekçelendirmektedir.
b) Gözetim programı, ASCERT tarafından belirlenir. Belgelendirilmiş müşteri kuruluşu ile belirli ziyaret tarihleri üzerinde uzlaşma sağlanır.
c) Gözetim denetimleri, diğer yönetim sistemlerinin denetimleri ile birleştirilebilir. Raporlama, her bir yönetim sistemine dair hususları açıkça belirtir.
d) ASCERT, sertifikanın uygun şekilde kullanımı konusunu denetlemektedir.

Gözetim denetimleri esnasında, ASCERT, daha önceden gelen şikâyet ve herhangi bir uygunsuzluk veya belgelendirmenin şartlarını karşılayamama durumu varsa, müşteri kuruluşun kendi BGYS'sini ve prosedürlerini araştırdığı ve uygun düzeltici faaliyetleri gerçekleştirdiğine dair kayıtları kontrol eder.
Bir gözetim raporu, özellikle daha önce belirlenen uygunsuzlukların giderildiğine dair bilgileri içerir. Asgari olarak, gözetimden çıkan raporlar, yukarıdaki a) bendi şartının üzerine eklenir.

4.5. Yeniden Belgelendirme Denetimleri
Yeniden belgelendirme denetimlerinde, müşteri kuruluşun BGYS uygulamalarının, ISO/IEC 27001 standardı ile tutarlılığının sürdürülebilir olduğu incelenir.

4.6. Özel Denetimler
Belgelendirilmiş müşteri kuruluş, sisteme ait büyük değişiklikler yaparsa ya da belgelendirmenin temelini etkileyebilen başka değişiklikler meydana gelirse bu durumlardan ASCERT'i haberdar etmesi istenmektedir. Böyle durumlarda, özel denetimler gerçekleştirilir.

4.7. BGYS Denetiminin Özel Unsurları
ASCERT'in rolü, müşteri kuruluşların, varlıklara yönelik bilgi güvenliği ile ilgili tehditlerin, açıklıkların ve müşteri kuruluş üzerindeki etkilerinin tespit edilmesi, incelenmesi ve değerlendirilmesi için prosedürleri oluştururken ve sürdürürken tutarlı olmasını sağlamaktır.
ASCERT:
a) Müşteri kuruluşun, güvenliğe ilişkin tehditlerin analizinin uygun olduğunu ve müşteri kuruluşun çalışması için yeterli olduğunu göstermesini zorunlu kılar.
b) Varlıklar, açıklıklar ve bunların uygulanmasının sonuçlarına karşın bilgi güvenliğine ilişkin tehditlerin değerlendirilmesi, incelenmesi ve belirlenmesi için müşteri kuruluşun prosedürlerinin, müşteri kuruluşun politikası, amaçları ve hedeflerine uygun olup olmadığını tespit eder.

ASCERT ayrıca, önemli analizlerde kullanılan prosedürlerin doğru olup olmadığını ve uygun bir şekilde uygulanıp uygulanmadığını belirler. Müşteri kuruluşa ait varlıklara, açıklığa ya da etkisine ilişkin bilgi güvenliği tehditleri, önemli olarak belirlenirse, BGYS içinde ele alınır.

4.8. Denetim Raporu

Denetim raporunda, aşağıdaki bilgiler bulunur veya bilgilere ulaşmak için referansı gösterilir:

a) Doküman gözden geçirmesinin özetinin de içeren denetimin bir değerlendirmesi,
b) Müşteri kuruluşun bilgi güvenliği risk analizinin bir değerlendirmesi
c) Denetim planından sapmalar (örneğin belirli zamanlanmış faaliyetlerde harcanan zaman daha fazla veya daha az),
d) BGYS kapsamı,
e) Müşteri Kuruluşun iş sektörüne göre ilgili spesifik standart ile ilgili değerlendirme.

Denetim raporu, belgelendirme kararını kolaylaştırmak ve desteklemek için aşağıda verilen yeterli ayrıntıyı da içermelidir:

a) İzlenen önemli denetim yolları ve kullanılan denetim metodolojileri,
b) Hem gözlemler, hem de pozitif (ör. kayda değer özellikler) ve negatif (ör. potansiyel uygunsuzluklar),
c) Müşteri kuruluşun BGYS'sinin, belgelendirme şartları ile uygunluğuna ilişkin veya uygunsuzluğun tanımını içeren açıklamalar, Uygulanabilirlik Beyanının güncel versiyonuna bir atıf ve uygulanabildiği durumda müşteri kuruluşun önceki belgelendirme denetimlerinin sonuçları ile herhangi bir faydalı karşılaştırma.

Doldurulmuş anketler, kontrol listeleri, gözlemler, logolar veya denetçi notları, denetim raporunun bütünleyici bir parçasını oluşturabilir. Bu yöntemler kullanılırsa, bu dokümanlar, belgelendirme kararını desteklemek üzere ASCERT'e delil olarak verilir. Denetim sırasında değerlendirilmiş örnekler hakkında bilgiler, denetim raporuna dâhil edilir.
Rapor, müşteri kuruluşun dahili organizasyonun yeterliliği ve müşteri kuruluşun BGYS'sine güven sağlamak için Denetim Raporu, aşağıdakileri kapsamalıdır:

- BGYS'nin etkinliği ve uygulanmasına ilişkin en önemli olumlu ve olumsuz gözlemlerin bir özeti,
- Müşteri kuruluşun BGYS'sine ilişkin, belgelendirmenin verilmesi veya verilmemesine dair denetim ekibinin tavsiyesi ve bu tavsiyenin desteklenmesi için bilgiler.

4.9. Belgelendirmeyi Askıya Alma veya Geri Çekme

BGYS gözetim denetimlerinde, aşağıdaki şartların oluşması söz konusu olursa belgelendirmenin askıya alınması yönünde, öneride bulunulacağı ifade edilir:

- Gerçekleştirilen denetimler sonucunda majör uygunsuzluklar bulunması,
- Önceki denetimlerde tespit edilen minör uygunsuzlukların, belirlenmiş sürelerde giderilmemesi,
- Yasal şartların yerine getirilmediğinin tespiti,
- Belgelendirme kurallarına uyulmaması.

BGYS belgelendirmesi askıya alınmış müşteri kuruluşların takip denetiminde, belirlenen uygunsuzluklar kapatılmış ise belgelendirmenin geçerliliğinin devamı, kapatılmamış ise belgelendirmenin geri çekilmesi yönünde, öneride bulunulacağı ifade edilir.

5. REVİZYON BİLGİLERİ

Revizyon Tarihi	Revizyon No	Madde No	Yapılan Revizyonun Açıklaması
20.08.2022	02	-	ISO/IEC 27006:2015 geçişi yapılmıştır.

Hazırlayan	Onaylayan
Yönetim Temsilcisi	*Genel Müdür*