AMAÇ

Bu prosedürün amacı; ISO/IEC 27006:2015 standardı doğrultusunda hazırlanan BGYS dokümantasyonunun açıklanması, denetçi yetkinliklerinin belirlenmesi, denetimlerin planlanması, gerçekleştirilmesi ve Belgelendirme kararının alınması için yöntem ve sorumlulukları belirlemektir.

KAPSAM

Bu prosedür, UAC tarafından yürütülen Bilgi Güvenliği Yönetim Sistemi Belgelendirme faaliyetleri kapsamında Belgelendirme esaslarını kapsamaktadır.

TANIMLAR

BGYS: Bilgi Güvenliği Yönetim Sistemi

Bilgi Güvenliği Yönetim Sistemi: Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası.

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).

SORUMLULUKLAR

Genel Müdür, Belgelendirme Müdürü, Planlama ve Sertifikasyon Sorumlusu, Belgelendirme Komitesi, UAC ve BGYS sistemleri konusunda müracaat eden/belgeli tüm kuruluşlar sorumludur.

UYGULAMA

1. PRENSİPLER

ISO/IEC 17021-1:2015 standardındaki hükümler geçerlidir.

2. GENEL GEREKLİLİKLER

2.1. Yasal ve Sözleşmeyle İlgili Hususlar

ISO/IEC 17021-1:2015 ve ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 5.1'deki hükümler geçerlidir.

2.2. Tarafsızlığın Yönetilmesi

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 5.2'deki hükümler geçerlidir. Ek olarak, aşağıdaki BGYS'ye özel gereklilikler ve kılavuz uygulanır.

Hazırlayan	Onaylayan
Yönetim Temsilcisi	Genel Müdür

2.2.1. BG 5.2 Çıkar Çatışmaları

UAC, danışmanlık olarak nitelendirilmeyecek şekilde veya potansiyel bir çıkar çatışmasına neden olmadan aşağıdaki görevleri yerine getirebilir:

a) Eğitimlerin; bilgi güvenliği yönetimi, ilgili yönetim sistemleri veya denetimle ilgili olduğu durumlarda, genel katılıma açık, genel bilgilerin verilmesi ile sınırlı kalmak kaydıyla, eğitimlerin düzenlemesi veya eğitmen olarak katılım sağlanması (örneğin, aşağıdaki b) bendinin gereklilikleri ile çelişen müşteri kuruluşa özel tavsiyeler vermemek şartıyla),

b) UAC'nin, belgelendirme denetim standardlarının gerekliliklerinin yorumunu açıklayan bilgilerin, talep üzerine erişime açılması veya yayınlanması,

c) Belgelendirme denetimi için hazır olunup olunmadığını belirlemek için, denetimden önceki faaliyetler (bu tür faaliyetler, bu maddeyle çelişen tavsiyelerin sağlanmasıyla sonuçlanamaz ve UAC, bu tür faaliyetlerin, bu gerekliliklerle çelişmediğini ve bunların belgelendirme denetim zamanında bir azalmayı gerekçelendirmek için kullanılmadığını garanti eder),

d) Akreditasyon kapsamında bulunanların dışındaki standardlara veya düzenlemelere göre ikinci ve üçüncü taraf denetimlerin yapılması,

e) Belgelendirme denetimleri ve gözetimler esnasında katma değer sağlanması (örneğin, özel çözümler önerilmeden denetim esnasında açığa çıkan iyileştirme için fırsatlar tespit edilmesi).

UAC, belgelendirmeye tabi müşteri kuruluşun BGYS'sinin BGYS iç denetimini gerçekleştiren kuruluşlardan (herhangi bir birey de dâhil olmak üzere) bağımsızdır ve bu hizmetleri kendisi sunmaz.

2.3. Yükümlülük ve Finansman

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 5.3'deki hükümler geçerlidir.

3. YAPISAL GEREKLİLİKLER

3.1. Organizasyon Yapısı ve Üst Yönetim

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 6.1'deki hükümler geçerlidir.

3.2. Operasyonel Kontrol

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 6.2'deki hükümler geçerlidir.

4. KAYNAK GEREKLİLİKLERİ

4.1. Personelin Yetkinliği

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 7.1 ile Kaynaklar Prosedüründeki hükümler geçerlidir. Ek olarak, aşağıdaki BGYS'ye özel gereklilikler ve kılavuz uygulanır.

4.1.1. BG 7.1.1 Genel Hususlar

4.1.1.1. Genel Yetkinlik Gereklilikleri

UAC, denetleyeceği müşteri kuruluşun BGYS'si ile ilgili teknolojik ve yasal gelişmelere dair bilgi birikimine sahip personel bulundurur veya ihtiyaç olunca ulaşabilir.

UAC, BGYS Belgelendirmesinin yapılabilmesi için gereken temel yetkinlikleri, denetlenecek faaliyetlere ve ilgili bilgi güvenliği konularına uygun olan kabiliyet ve yetkinliğe sahip denetçi ve/veya teknik uzmanları seçmek, temin etmek ve yönetmek için kriterleri, Kaynaklar Prosedürü doğrultusunda belirlemiş ve dokümante etmiş olup, buna uygun personeli seçer.

4.1.2. BG 7.1.2 Yetkinlik Kriterlerinin Belirlenmesi

4.1.2.1. BGYS Denetimi İçin Yetkinlik Gereklilikleri

4.1.2.1.1. Genel Gereklilikler

UAC, aşağıdakileri sağlamak için yetkin personel bulundurur veya ihtiyaç olunca ulaşabilir:

a) Bilgi güvenliği bilgisi;

b) Denetlenecek faaliyetin teknik bilgisi;

c) Yönetim sistemleri bilgisi

d) Denetim ilkeleri hakkında bilgi;

e) İzleme, ölçme, analiz etme ve değerlendirme bilgisi.

Denetim ekibi, müşteri kuruluşun bilgi güvenliği olaylarının kullanım alanlarını izleme iznine sahiptir.

Denetim ekibi, yukarıdaki maddelere ilişkin uygun iş tecrübesine ve bu maddelerin pratik uygulamasına sahip olacak şekilde (Bu, bir denetçinin tüm bilgi güvenliği alanlarında tecrübeye sahip olması gerektiği anlamına gelmez, ancak denetim ekibinin, denetlenecek BGYS kapsamını kapsayacak şekilde yeterli bilgi ve tecrübeye sahip olması gerekir) görevlendirilir.

4.1.2.1.2. Bilgi Güvenliği Yönetim Terminolojisi, İlkeleri, Uygulamaları ve Teknikleri

UAC, denetim ekipleri için aşağıdakileri temin eden yetkinlik kriterleri oluşturmuştur:

a) BGYS'ye özgü doküman yapıları, hiyerarşi ve ilişkiler;

b) Bilgi güvenliği yönetimiyle ilgili araçlar, yöntemler, teknikler ve uygulamaları;

c) Bilgi güvenliği risk değerlendirmesi ve risk yönetimi;

d) BGYS için uygulanabilir işlemler;

e) Bilgi güvenliği ile ilgili olabilecek güncel teknoloji veya bir husus.

4.1.2.1.3. Bilgi Güvenliği Yönetim Sistemi Standardları ve Normatif Dokümanlar

BGYS denetimine katılan denetçiler;

a) ISO/IEC 27001'de yer alan tüm gereklilikler.

Denetim ekibinin tüm üyeleri aşağıdakiler hakkında bilgi sahibi olacaktır:

b) ISO/IEC 27002'de yer alan tüm kontroller (gerektiğinde ayrıca sektörel standardlara göre belirlenirse) ve bunların uygulanması olarak kategorize edilmiş:

1) Bilgi güvenliği politikaları;

2) Bilgi güvenliğinin organizasyonu;

3) İnsan kaynakları güvenliği;

4) Varlık yönetimi;

5) Yetkilendirme de dahil olmak üzere erişim kontrolü;

6) Kriptografi;

7) Fiziksel ve çevresel güvenlik;

8) IT hizmetleri de dahil olmak üzere operasyon güvenliği;

9) Şebeke güvenliği yönetimi ve bilgi aktarımı da dahil olmak üzere iletişim güvenliği;

10) Sistem edinilmesi, geliştirilmesi ve bakımı;

11) Dış kaynaklı hizmetler de dahil olmak üzere tedarikçi ilişkileri;

12) Bilgi güvenliği olay yönetimi;

13) İş sürekliliği yönetiminin, yedeklilik de dahil olmak üzere bilgi güvenliği boyutları;

14) Bilgi güvenliği gözden geçirmeleri de dahil uyumluluk.

4.1.2.1.4. İş Yönetimi Uygulamaları

BGYS denetiminde yer alan Denetçiler şu bilgilere sahip olacaktır:

a) Endüstri bilgi güvenliği iyi uygulamaları ve bilgi güvenliği prosedürleri;

b) Bilgi güvenliği için politikalar ve iş gereklilikleri;

c) Genel iş yönetimi kavramları, uygulamaları ve politika, hedefler ve sonuçlar arasındaki karşılıklı ilişki;

d) Yönetim prosesleri (insan kaynakları yönetimi, iç ve dış iletişim ve diğer ilgili destek proseslerini de içeren) ve ilgili terminoloji.

4.1.2.1.5. Müşteri İş Sektörü Uygulamaları

BGYS denetiminde yer alan Denetçiler bilgisine sahip olacaktır:

a) Belirli bilgi güvenliği alanında, coğrafyada ve yargı alanındaki yasal ve düzenleyici gereklilikler;

b) İş sektörüyle ilgili bilgi güvenliği riskleri;

c) Müşteri terminolojisine ilişkin genel terminoloji, prosesler ve teknolojiler;

d) İlgili iş sektörü uygulamaları.

Kriter a) denetim ekibi arasında paylaşılabilir.

4.1.2.1.6. Müşteri Ürünleri, Prosesleri ve Organizasyonu

BGYS denetimine katılan Denetçiler aşağıdakilerin bilgisine sahip olacaklardır:

a) Müşteri kuruluşun tipi, boyutu, yönetişimi, yapısı, fonksiyonları ve ilişkilerinin, dış kaynak kullanımı da dahil olmak üzere BGYS ve Belgelendirme faaliyetlerinin geliştirilmesi ve uygulanması üzerindeki etkileri;

b) Geniş bir perspektif içinde karmaşık operasyonlar;

c) Ürün veya hizmet için geçerli olan yasal ve düzenleyici gereklilikler.

4.1.2.2. BGYS Denetim Ekibinin Yönetilmesi İçin Yetkinlik Gereklilikleri

Başdenetçiler, 7.1.2.1'deki gerekliliklere ek olarak, rehberlik ve gözetim altında denetimlerde gösterilecek olan aşağıdaki gereklilikleri yerine getirmelidir:

a) Belgelendirme denetim prosesini ve denetim ekibini yönetebilecek bilgi ve beceriler;

b) Sözlü ve yazılı olarak etkili iletişim kurma yeteneğinin gösterilmesi.

4.1.2.3. Başvurunun Gözden Geçirilmesi İçin Yetkinlik Gereklilikleri

4.1.2.3.1. Bilgi Güvenliği Yönetim Sistemi Standardları ve Normatif Dokümanlar

Denetim ekibi yetkinliğini belirlemek, denetim ekibi üyelerini seçmek ve denetim zamanını belirlemek için başvuru gözden geçirme görevlisinin, aşağıdakilerin bilgisine sahip olması sağlanır:

a) İlgili BGYS standardları ve Belgelendirme prosesinde kullanılan diğer normatif dokümanlar.

4.1.2.3.2. Müşteri İş Sektörü Uygulamaları

Denetim ekibinin yetkinliğini belirlemek, denetim ekibi üyelerini seçmek ve denetim zamanını belirlemek için gözden geçirmeleri yapan personelin aşağıdaki konularda bilgi sahibi olması sağlanır:

a) Müşteri iş sektörüne ilişkin genel terminoloji, prosesler, teknolojiler ve riskler.

4.1.2.3.3. Müşteri Ürünleri, Prosesleri ve Organizasyonu

Denetim ekibi yetkinliğini belirlemek, denetim ekibi üyelerini seçmek ve denetim zamanını belirlemek için başvuru gözden geçirme görevlisinin, aşağıdakilerin bilgisine sahip olması sağlanır:

a) BGYS ve Belgelendirme faaliyetlerinin geliştirilmesi ve uygulanmasına ilişkin müşteri ürünleri, prosesler, kuruluş tipleri, boyut, yönetişim, yapı, fonksiyonlar ve ilişkiler, dış kaynak kullanımı dahil.

4.1.2.4. Denetim Raporlarının Gözden Geçirilmesi ve Belgelendirme Kararlarının Verilmesi İçin Yetkinlik Gereklilikleri

4.1.2.4.1. Genel

Denetim raporlarını gözden geçiren ve Belgelendirme kararlarını veren personelin, Belgelendirme kapsamının uygunluğunun yanı sıra, kapsam değişiklikleri ve bunların denetim etkinliği üzerindeki etkilerini, özellikle arayüzlerin ve bağımlılıkların ve ilgili risklerin belirlenmesinin, geçerliliğini korumaya devam etmesi konusunda bilgi sahibi olması sağlanır.

Buna ek olarak, denetim raporlarını gözden geçiren ve Belgelendirme kararlarını veren personel, aşağıdaki konuları bilmelidir:

a) Genel olarak yönetim sistemleri;

b) Denetim prosesleri ve prosedürleri;

c) Denetim prensip, uygulama ve teknikleri.

4.1.2.4.2. Bilgi Güvenliği Yönetim Terminolojisi, İlkeleri, Uygulamaları ve Teknikleri

Denetim raporlarını gözden geçiren ve Belgelendirme kararlarını veren personelin, aşağıdaki bilgilere sahip olması sağlanır:

a) 7.1.2.1.2 a), c) ve d) 'de listelenen maddeler;

b) Bilgi güvenliği ile ilgili yasal ve düzenleyici gereklilikler.

4.1.2.4.3. Bilgi Güvenliği Yönetim Sistemi Standardları ve Normatif Dokümanlar

Denetim raporlarını gözden geçiren ve Belgelendirme kararları veren personelin, aşağıdaki bilgilere sahip olması sağlanır:

a) İlgili BGYS standardları ve Belgelendirme prosesinde kullanılan diğer normatif dokümanlar.

4.1.2.4.4. Müşteri İş Sektörü Uygulamaları

Denetim raporlarını gözden geçiren ve Belgelendirme kararları veren personelin, aşağıdaki bilgilere sahip olması sağlanır:

a) Genel terminoloji ve ilgili iş sektörü uygulamaları ile ilgili riskler.

4.1.2.4.5. Müşteri Ürünleri, Prosesleri ve Organizasyonu

Denetim raporlarını gözden geçiren ve Belgelendirme kararları veren personelin, aşağıdaki bilgilere sahip olması sağlanır:

a) Müşteri ürünleri, prosesler, kuruluş tipleri, boyut, yönetişim, yapı, fonksiyonlar ve ilişkiler.

4.2. Belgelendirme Faaliyetlerinde Görev Alan Personel

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 7.2 ile Kaynaklar Prosedüründeki hükümler geçerlidir. Ek olarak, aşağıdaki BGYS'ye özel gereklilikler ve kılavuz uygulanır.

4.2.1. BG 7.2 Denetçinin Bilgi ve Tecrübesinin Gösterilmesi

UAC, Denetçilerin, aşağıdaki bilgi ve tecrübeye sahip olduklarını gösterir:

a) BGYS'ye özgü nitelikleri;

b) Mümkünse denetçi olarak kayıt;

c) BGYS eğitim kurslarına katılım ve ilgili kişisel göstergelerin elde edilmesi;

d) Güncel mesleki gelişim kayıtları;

e) Başka bir BGYS denetçisinin gözetiminde BGYS denetimleri.

4.2.1.1. Denetçilerin Seçilmesi

7.1.2.1'e ek olarak, Denetçi seçme kriterleri, her Denetçinin aşağıdakileri yerine getirmesini sağlar:

a) Üniversite eğitimine eşdeğer seviyede mesleki eğitim veya öğrenime sahip olma;

b) Bilgi teknolojileri alanında, en az 2 yıl bilgi güvenliği ile ilgili olmak üzere en az 4 yıl tam zamanlı uygulamalı iş deneyimine sahip olma;

c) BGYS denetimleri ve denetim yönetimini kapsayan en az 5 günlük eğitimi başarıyla tamamlama;

d) Bir denetçi olarak görevlendirilmeden önce, bilgi güvenliğini değerlendirmesinin tüm proseslerinde deneyim kazanma. Bu deneyim, yeniden belgelendirme ve gözetim denetimleri de dahil olmak üzere (En az 5 günü gözetim denetimleri olmalıdır) en az 20 gün boyunca, en az 4 BGYS Belgelendirme denetimine katılmak suretiyle elde edilir. Katılım, dokümantasyonun ve risk değerlendirmesinin gözden geçirilmesini, uygulama değerlendirmesini ve denetim raporlamasını içerir;

e) İlgili ve güncel deneyime sahip;

f) Mevcut bilgi ve becerileri, sürekli mesleki gelişim sayesinde güncel tutma.

Teknik Uzmanlar a), b) ve e) kriterlerine uymak zorundadır.

4.2.1.2. Başdenetçi Seçimi

7.1.2.2 ve 7.2.1.1'e ek olarak, Başdenetçinin aşağıdakileri yerine getirmesi sağlanır:

a) En az 3 BGYS denetiminin tüm aşamalarına aktif olarak katılmış olma. Katılım, başlangıç, kapsam belirleme ve planlama, dokümantasyon ve risk değerlendirmesinin incelenmesi, uygulama değerlendirmesi ve resmi denetim raporlamasını içerir.

4.3. Kuruluş Dışı Bireysel Denetçiler ve Teknik Uzmanların Kullanımı

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 7.3 ve Kaynaklar Prosedüründeki hükümler geçerlidir. Ek olarak, aşağıdaki BGYS'ye özel gereklilikler ve kılavuz uygulanır.

4.3.1. BG 7.3 Denetim Ekibinin Bir Parçası Olarak Kuruluş Dışı Denetçiler ve Teknik Uzmanların Kullanımı

Hazırlayan	Onaylayan
Yönetim Temsilcisi	Genel Müdür

UAC, dış Denetçileri ve Teknik Uzmanları denetim ekibinin bir parçası olarak kullanırken;

- Bu kişilerin yetkin olduklarından ve ISO/IEC 27006:2015 standardının uygulanabilir hükümleri ile uyumlu olduklarından,
- Tarafsızlığı ihlal edecek şekilde doğrudan veya işvereni üzerinden, bir BGYS veya ilgili yönetim sistemlerinin tasarımı, uygulaması veya sürdürülmesinde yer almış olmadıklarından,

yaptığı sözleşmeler ve aldığı güncel bildirimler ile emin olur.

4.4. Personel Kayıtları

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 7.4 ve Kaynaklar Prosedüründeki hükümler geçerlidir.

4.5. Dış Kaynak Kullanımı

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 7.5'de yer alan hükümler geçerlidir.

5. BİLGİ GEREKLİLİKLERİ

5.1. Kamuya Açık Bilgiler

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 8.1'de yer alan hükümler geçerlidir.

5.2. Belgelendirme Dokümanları

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 8.2 maddesinde yer alan hükümler geçerlidir. Ek olarak, aşağıdaki BGYS'ye özel gereklilikler ve kılavuz uygulanır.

5.2.1. BG 8.2 BGYS Belgelendirme Dokümanları

UAC, BGYS'si belgelendirilen müşteri kuruluşların her birine, UAC Genel Müdürü tarafından imzalanan bir sertifika sunar. Sertifikada, Uygulanabilirlik Beyanının sürümü yer alır.

Müşteri kuruluş talep ettiği takdirde, sertifikada, sektöre özgü standard(lar)ın tanımlanması da yer alabilir.

Sertifika kapsamındaki kontrollerin kapsamını değiştirmeyen Uygulanabilirlik Beyanında yapılan değişiklik, sertifikanın güncellenmesini gerektirmez.

5.3. Belgelendirmeye Atıf ve Markaların Kullanımı

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 8.3 ve Sertifika ve Logo Kullanım Talimatındaki hükümler geçerlidir.

5.4. Gizlilik

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 8.4'de yer alan hükümler geçerlidir. Ek olarak, aşağıdaki BGYS'ye özel gereklilikler ve kılavuz uygulanır.

5.4.1. BG 8.4 Kurumsal Kayıtlara Erişim

UAC, Belgelendirme denetiminden önce müşteri kuruluşa, gizli veya hassas bilgi içermesi nedeniyle denetim ekibine incelenmek üzere sunulamayacak olan BGYS'ye ait herhangi bir kaydın olup olmadığını bildirmesini talep eder.

UAC, bu kayıtların eksik olması durumunda, BGYS'nin uygun bir şekilde denetlenip denetlenemeyeceğine karar verir. UAC, tespit edilen gizli ya da hassas kayıtları incelemeden BGYS'nin uygun bir şekilde denetiminin yapılmasının mümkün olmadığına karar verirse, uygun erişim düzenlemeleri sağlanana kadar Belgelendirme denetiminin gerçekleştirilemeyeceğini müşteri kuruluşa bildirir.

5.5. UAC ile Müşterileri Arasındaki Bilgi Alışverişi

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 8.5'da yer alan hükümler geçerlidir.

6. PROSES GEREKLİLİKLERİ

6.1. Belgelendirme Öncesi Faaliyetler

6.1.1. Başvuru

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 9.1.1'de yer alan hükümler geçerlidir. Ek olarak, aşağıdaki BGYS'ye özel gereklilikler ve kılavuz uygulanır.

6.1.1.1. BG 9.1.1 Başvurunun Hazır Olması

BGYS Belgelendirmesi için başvurular, Belgelendirme Başvuru Formu ile alınır.

Planlama Sorumlusu tarafından, BGYS Belgelendirme başvurusunda bulunan müşteri kuruluşlara, başvuru gözden geçirme öncesinde;

1. Kaynaklar için yetkinlikleri değerlendirmek,
2. Faaliyet alanında yetkinlik analizinin uygunluğu ve
3. Belirtilen hariç tutmaların doğrulamasının yapılması amacıyla bilgi edinmek üzere,

BGYS Belgelendirme Başvuru Kontrol Formu gönderilir ve doldurularak UAC'ye geri gönderilmesi istenir.

6.1.2. Başvurunun Gözden Geçirilmesi

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 9.1.2'de yer alan hükümler geçerlidir.

6.1.2.1. BG 9.1.2 Başvurunun Gözden Geçirilmesi

Belgelendirme için başvuran müşteri kuruluşlar için, bir gözden geçirme yapılır ve BGYS Belgelendirme Başvuru Kontrol Formu, bu gözden geçirmeyi yapan personel tarafından imzalanır.

Başvurunun gözden geçirilmesinin tamamlanmasından sonra, Belgelendirme Başvuru Prosedürü, teklif hazırlanır ve müşteri kuruluşa gönderilir.

Teklifi kabul eden müşteri kuruluş ile Belgelendirme Başvuru Prosedürü doğrultusunda sözleşme imzalanır.

6.1.3. Denetim Programı

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 9.1.3'deki hükümler geçerlidir. Ek olarak, aşağıdaki BGYS'ye özel gereklilikler ve kılavuz uygulanır.

6.1.3.1. BG 9.1.3 Genel

BGYS denetimleri için Denetim Programı, belirlenen bilgi güvenlik kontrollerini dikkate alacak şekilde oluşturulur.

6.1.3.2. BG 9.1.3 Denetim Metodolojisi

UAC, müşteri kuruluşun, BGYS' sinin, ISO/IEC 27001'de belirtilen gereklilikleri ve müşteri kuruluşun politikalarını ve hedeflerini karşılayıp karşılamadığını saptamaya odaklanan bir denetim uygulaması için, BGYS Denetim Prosedürü uygular.

6.1.3.3. BG 9.1.3 İlk Denetim İçin Genel Hazırlıklar

UAC, bir müşteri kuruluşun, iç denetim raporlarına ve bilgi güvenliğiyle ilgili bağımsız gözden geçirme raporlarına erişmek için gerekli tüm düzenlemeleri yapmasını talep eder.

En azından ilk Belgelendirme denetiminin Aşama 1'i sırasında müşteri kuruluş tarafından aşağıdaki bilgilerin sağlanması talep edilir:

a) BGYS ve kapsadığı faaliyetlerle ilgili genel bilgi;

b) ISO/IEC 27001'de belirtilen gerekli BGYS dokümantasyonunun bir kopyası ve gerektiğinde ilgili dokümanlar.

6.1.3.4. BG 9.1.3 Gözden Geçirme Sıklığı

UAC, en az bir yönetimin gözden geçirmesi ve Belgelendirme kapsamını içeren bir iç denetim yapılmadığı durumda, BGYS belgelendirmesi yapmaz.

6.1.3.5. BG 9.1.3 Belgelendirme Kapsamı

Denetim ekibi, tanımlanan kapsamda, müşteri kuruluşun BGYS' sini tüm gerekliliklerin yerine getirildiğinin doğrulanması amacıyla denetler. UAC, müşteri kuruluşun BGYS' si kapsamında, müşterilerin ISO/IEC 27001 madde 4.3'te belirtilen gereklilikleri yerine getirdiğini teyit eder.

UAC, müşteri kuruluşun Belgelendirme kapsamında tanımlanan faaliyetlerinin sınırları içinde, bilgi güvenliği risk değerlendirmesinin ve risk işlemenin doğru bir şekilde gerçekleştirildiğini teyit eder. UAC bunun, müşteri kuruluşun BGYS ve Uygulanabilirlik Beyanı kapsamına yansıtıldığını teyit eder. UAC, Belgelendirme kapsamı başına en az bir Uygulanabilirlik Beyanı bulunduğunu doğrular.

UAC, tamamen BGYS kapsamına girmeyen hizmetler veya faaliyetlerle ilgili ara yüzlerin, belgelendirmeye tabi BGYS kapsamında ele alınmasını ve müşteri kuruluşun bilgi güvenliği risk değerlendirmesinde yer aldığını kontrol eder. Böyle bir durumun bir örneği, diğer kuruluşlarla paylaşımdır (örneğin IT sistemleri, veri tabanları ve telekomünikasyon sistemleri veya bir iş fonksiyonu için dış kaynak kullanımı).

6.1.3.6. BG 9.1.3 Belgelendirme Denetimi Kriterleri

Bir müşteri kuruluşun BGYS'sinin denetlenmesine ilişkin kriterler için, ISO/IEC 27001 BGYS standardı referans alınır.

6.1.4. Denetim Zamanının Belirlenmesi

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 9.1.4'de yer alan hükümler geçerlidir. Ek olarak, aşağıdaki BGYS'ye özel gereklilikler ve kılavuz uygulanır.

6.1.4.1. BG 9.1.4 Denetim Zamanı

UAC, ilk Belgelendirme, gözetim denetimi ya da yeniden belgelendirme denetimleri için denetim zamanını, BGYS kapsamının büyüklüğünü (Ör: kullanılan bilgi sistemlerinin sayısı, çalışan sayısı) dikkate alarak, denetim ekibine, yeterli zamanı verecek şekilde planlar.

Genel denetim zamanının hesaplanması, denetim raporlaması için yeterli zamanı da içerir.

UAC, denetim zamanını belirlemek için ISO/IEC 27006:2015 Annex B ve C'yi kullanır.

Denetim zamanları, aşağıda verilen tablo doğrultusunda belirlenir:

Çalışan Sayısı	İlk Belgelendirme için BGYS adam/gün			Arttırıcı ya da azaltıcı faktörler
	Toplam	Aşama 1	Aşama 2	
1-10	5	1.5	3.5	ISO/IEC 27006:2015 Annex B.3.4'e bakın
11-15	6	2	4	ISO/IEC 27006:2015 Annex B.3.4'e bakın
16-25	7	2,5	4,5	ISO/IEC 27006:2015 Annex B.3.4'e bakın
26-45	8.5	3	5.5	ISO/IEC 27006:2015 Annex B.3.4'e bakın
46-65	10	3,5	6,5	ISO/IEC 27006:2015 Annex B.3.4'e bakın
66-85	11	3,5	7,5	ISO/IEC 27006:2015 Annex B.3.4'e bakın
86-125	12	4	8	ISO/IEC 27006:2015 Annex B.3.4'e bakın
126-175	13	4,5	8,5	ISO/IEC 27006:2015 Annex B.3.4'e bakın
176-275	14	4,5	9	ISO/IEC 27006:2015 Annex B.3.4'e bakın
276-425	15	5	10	ISO/IEC 27006:2015 Annex B.3.4'e bakın
426-625	16,5	5.5	11	ISO/IEC 27006:2015 Annex B.3.4'e bakın
626-875	17,5	6	11.5	ISO/IEC 27006:2015 Annex B.3.4'e bakın
876-1175	18,5	6	12.5	ISO/IEC 27006:2015 Annex B.3.4'e bakın
1176-1550	19,5	6.5	13	ISO/IEC 27006:2015 Annex B.3.4'e bakın
1551-2025	21	7	14	ISO/IEC 27006:2015 Annex B.3.4'e bakın
2026-2675	22	7,5	14,5	ISO/IEC 27006:2015 Annex B.3.4'e bakın
2676-3450	23	7.5	15.5	ISO/IEC 27006:2015 Annex B.3.4'e bakın
3451-4350	24	8	16	ISO/IEC 27006:2015 Annex B.3.4'e bakın
4351-5450	25	8.5	16.5	ISO/IEC 27006:2015 Annex B.3.4'e bakın
5451-6800	26	8.5	17.5	ISO/IEC 27006:2015 Annex B.3.4'e bakın
6801-8500	27	9	18	ISO/IEC 27006:2015 Annex B.3.4'e bakın
8501-10700	28	9.5	18.5	ISO/IEC 27006:2015 Annex B.3.4'e bakın
>10.700	Yukarıdaki ilerlemeyi izleyin	Yukarıdaki ilerlemeyi izleyin	Yukarıdaki ilerlemeyi izleyin	

UAC, ilk belgelendirme, gözetim ve yeniden belgelendirme denetimlerinde kullanılan zamanı gerekçelendirir.

Ayrılan zaman için aşağıdaki etkenler (ISO/IEC 27006:2015 Annex B.3.4) dikkate alınır:

a) BGYS'nin karmaşıklığı (Ör: Bilgi sistemlerinin kritikliği, BGYS'nin risk durumu), ayrıca ISO/IEC 27006:2015 Ek A'ya göre yukarıdaki tablo dikkate alınır,

b) BGYS kapsamında gerçekleştirilen iş tipleri,

c) BGYS'nin daha önce gösterdiği performans,

d) BGYS'nin çeşitli bileşenlerinin uygulanmasında kullanılan teknolojinin kapsamı ve çeşitliliği (uygulanan kontroller, dokümantasyon ve/veya proses kontrol, düzeltici faaliyet, vb. gibi),

e) BGYS kapsamı dâhilinde kullanılan dış kaynak kullanımı ve üçüncü taraf düzenlemelerinin kapsamı,

f) Bilgi sistemi geliştirmenin kapsamı,

g) Saha sayısı ve felaket kurtarma (DR) sahalarının sayısı,

h) Gözetim veya yeniden belgelendirme denetimleri için: ISO/IEC 17021-1, 8.5.3' e göre BGYS ile ilgili değişikliklerin miktarı ve kapsamı.

6.1.5. Çoklu Saha Örneklemesi

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 9.1.5'de yer alan hükümler geçerlidir. Ek olarak, aşağıdaki BGYS'ye özel gereklilikler ve kılavuz uygulanır.

6.1.5.1. BG 9.1.5 Çoklu Saha Örneklemesi

Müşteri kuruluşun aşağıda a) ile c) arasında olan kriterleri karşılayan sahaları olduğu durumlarda UAC, denetimlerde aşağıda verilen yaklaşımla değerlendirme yapar;

a) Tüm sahaların, merkezi olarak yönetildiği, denetlendiği ve merkezi olarak yönetimin gözden geçirmesine tabi olan aynı BGYS altında işletildiği,

b) Tüm sahaların, müşteri kuruluşun BGYS iç denetim programına dâhil edildiği,

c) Tüm sahaların, müşteri kuruluşun BGYS yönetimin gözden geçirmesi programına dâhil edildiği.

Çoklu saha denetimlerinin planlanması, aşağıda verilen esaslara ve tabloya göre yapılır:

a) İlk sözleşmenin gözden geçirilmesinde, yeterli örnekleme seviyesinin belirlenebilmesi için, sahalar arasındaki farklılıklar, mümkün olan en kapsamlı şekilde tanımlanır.

b) UAC tarafından aşağıdakiler dikkate alınarak, temsil edici sayıda saha örneklenir:

1) Merkez ofis ve sahaların iç denetim sonuçları,

2) Yönetimin gözden geçirmesi sonuçları,

3) Saha/ların büyüklüklerindeki farklılıklar,

4) Saha/ların iş kapsamıyla ilgili farklılıklar,

5) Farklı sahalardaki bilgi sistemlerinin karmaşıklığı,

6) Çalışma şekillerindeki farklılıklar,
7) Üstlenilen faaliyetlerdeki farklılıklar;
8) Tasarım ve operasyon kontrolündeki farklılıklar,
9) Kritik bilgi sistemleri veya hassas bilgiyi işleyen bilgi sistemleriyle potansiyel etkileşimler,
10) Değişen yasal gereklilikler,
11) Coğrafi ve kültürel boyutlar,
12) Sahaların risk durumu,
13) Belirli sahalardaki bilgi güvenliği olayları.

c) Müşteri kuruluşun BGYS'si kapsamı dâhilindeki tüm sahalar arasından temsili bir örnek seçilir; bu seçim yukarıdaki b) maddesinde belirtilen etkenleri de yansıtacak şekilde verilecek karara dayanan rastgele bir tercih ile belirlenir.

d) BGYS kapsamında bulunan önemli risklerle karşı karşıya olan tüm sahalar, belgelendirmeden önce UAC tarafından denetlenir.

e) Denetim programı, yukarıdaki gereklilikler doğrultusunda tasarlanır ve BGYS Belgelendirme kapsamının 3 yıllık süre içinde temsili örneklerini kapsar.

f) Merkez ofis veya tek bir sahada, bir uygunsuzluğun gözlemlendiği durumda, Düzeltici ve Önleyici Faaliyet Prosedürü, merkez ofise ve belgelendirmenin kapsadığı tüm sahalara uygulanır.

Denetim, tek bir BGYS' nin tüm sahalara uygulanmasından ve operasyonel seviyesinde merkezi yönetimin sağlandığından emin olunması için müşteri kuruluşun merkez ofis faaliyetlerini ele alır.

Denetimde, yukarıda özetlenen tüm hususlar ele alınır.

Sahaların sayısı (merkez ofis hariç) (1)	İlk denetim için örnekleme sayısı (2)	Gözetim denetimi için örnekleme sayısı* (3)	Belge yenileme denetimi için örnekleme sayısı (4)	Notlar (5)
1-2	%100 (hepsi)	Hepsi	Hepsi	-
3-4	2	2	2	*
5-9	3	2	3	*
10-25	4-5	3	4	*
26-36	6	4	5	*
37-49	7	5	6	*
50-64	8	5	7	*
65-100	9-10	6	8	*
101-121	11	7	9	*
122-144	12	8	10	*
145-169	13	8	11	*
170-225	14-15	9	12	*

Hazırlayan	Onaylayan
Yönetim Temsilcisi	Genel Müdür

****Elektronik nüshasının basılması ve pdf olarak gönderilmesi durumunda, basılmış bu doküman kontrolsüz kopya olarak işlem görür.**

226-256	16	10	13	*
257-289	17	11	14	*
290-324	18	11	15	*
325-400	19-20	12	16	*
> 400	en az 21	en az 13	en az 17	*

Örnek sahaların en az % 25 'i rastgele seçilir. Geri kalanı ise belli bir zaman dilimi için olabildiğince nitelik farklılığı gösteren sahalar arasından seçilir.

6.1.6. Çoklu Yönetim Sistemi Standardları

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 9.1.6'da yer alan hükümler geçerlidir. Ek olarak, aşağıdaki BGYS'ye özel gereklilikler ve kılavuz uygulanır.

6.1.6.1. BG 9.1.6 BGYS Dokümantasyonunun Diğer Yönetim Sistemleri ile Entegrasyonu

Müşteri kuruluş, BGYS ve diğer yönetim sistemleri (kalite, sağlık ve güvenlik ve çevre gibi) için olan dokümantasyonu, BGYS ve diğer sistemlere olan uygun arayüzler açıkça tanımlanabilir olduğu sürece birleştirebilir.

6.1.6.2. BG 9.1.6 Yönetim Sistemi Denetimlerinin Entegrasyonu

KVYS denetimi, başka yönetim sistemlerinin denetimleri ile entegre edilebilir. Bu entegrasyon, denetimde, KVYS belgelendirmesinin tüm gerekliliklerin yerine getirildiği gösterilebilir olduğu sürece mümkündür. Bir KVYS için önemli olan tüm unsurlar, denetim raporlarında, açıkça görülmeli ve doğrudan tespit edilebilir olur. Denetimin kalitesi, denetimlerin entegrasyonundan olumsuz yönde etkilenmemelidir.

Entegre denetimlerin süresi, Denetim Zamanı Belirleme Talimatı baz alınarak belirlenir.

6.2. Denetimlerin Planlanması

Proks, KVYS denetimlerini aşağıdakileri dikkate alarak planlar:

1. Aşama 1'in tamamı, müşteri kuruluşun yerinde (sahada) yapılır.
2. Aşama 1 ile Aşama 2 arasında, Aşama 1'de belirlenen bulgulara bağlı olarak makul bir süre olması göz önünde bulundurulur.
3. Hem Aşama 1 hem de Aşama 2'ye yetkin tetkik ekibi (ilgili kapsamda atanmış) görevlendirilir.

6.2.1. Denetimin Hedef, Kapsam ve Kriterlerinin belirlenmesi

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 9.1.6'da yer alan hükümler geçerlidir. Ek olarak, aşağıdaki BGYS'ye özel gereklilikler ve kılavuz uygulanır.

6.2.1.1. BG 9.2.1 Denetim Hedefi

Denetim hedefi, risk değerlendirmesine dayalı olarak, müşteri kuruluşun, uygulanabilir kontrolleri uyguladığının, belirlenmiş bilgi güvenliği hedeflerine ulaştığının ve yönetim sisteminin etkinliğinin belirlenmesini içerir.

6.2.2. Denetim Ekibinin Seçimi ve Atanması

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 9.2.2'de yer alan hükümler geçerlidir. Ek olarak, aşağıdaki BGYS'ye özel gereklilikler ve kılavuz uygulanır.

6.2.2.1. BG 9.2.2 Denetim Ekibi

Denetim ekibi, Tetkik Gerçekleştirme Prosedürü uyarınca görevlendirilir ve uygun çalışma dokümanları iletilir. Denetim ekibine verilen görevler, açıkça tanımlanır ve müşteri kuruluşa bildirilir.

Bir denetim ekibi, kişinin 7.1.2.1'de belirtilen tüm kriterleri karşılaması koşuluyla 1 kişiden oluşabilir.

6.2.2.2. BG 9.2.2 Denetim Ekibi Yetkinliği

Denetim ekibi için, 7.1.2' de listelenen gereklilikler geçerlidir. Gözetim ve özel denetim faaliyetleri için, sadece planlanmış gözetim faaliyeti ve özel denetim faaliyeti ile ilgili gereklilikler uygulanır.

Belli bir denetim için görevlendirilecek olan denetim ekibini seçerken ve yönetirken UAC, görevlendirme için gereken yetkinliklerin uygunluğunun sağladığını garanti eder. Ekip, aşağıdakileri sağlar:

a) Belgelendirmenin talep edildiği BGYS kapsamındaki özel faaliyetler ve ilgili prosedürler ve potansiyel bilgi güvenliği riskleri ile ilgili, uygun teknik bilgiye sahip olmak (Teknik Uzmanlar bu fonksiyonu yerine getirebilir);

b) BGYS'nin kapsamı ve bağlamı göz önüne alındığında, müşteri kuruluşun faaliyetleri, ürünleri ve hizmetlerinin, bilgi güvenliği boyutlarını yönetirken, müşteri kuruluşun BGYS'sini güvenilir bir Belgelendirme denetimi yapmak için yeterli şekilde anlamak,

c) Müşteri kuruluşun BGYS'sine uygulanabilir yasal ve düzenleyici gerekliliklerin uygun bir şekilde anlaşılmasını sağlamak.

6.2.3. Denetim Planı

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 9.2.3'de yer alan hükümler geçerlidir. Ek olarak, aşağıdaki BGYS'ye özel gereklilikler ve kılavuz uygulanır.

6.2.3.1. BG 9.2.3 Genel

BGYS denetimleri için denetim planı, belirlenen bilgi güvenliği kontrollerini dikkate alacak şekilde oluşturulur.

6.2.3.2. BG 9.2.3 Ağ Destekli Denetim Teknikleri

Uygulanması gerektiği takdirde, ağ destekli denetim teknikleri için denetim planı, söz konusu denetim sırasında kullanılacak ağ destekli denetim tekniklerine uygun olarak belirlenir.

Ağ destekli denetim teknikleri, örneğin, telekonferans, web görüşmesi, etkileşimli web tabanlı iletişim ve BGYS dokümantasyonuna ve/veya BGYS proseslerine uzaktan elektronik erişimi içerebilir. Bu tür tekniklerin odağı, denetim etkinliğinin ve verimliliğinin arttırılması ve denetim prosesinin bütünlüğünün desteklenmesidir.

6.2.3.3. BG 9.2.3 Denetimin Zamanlaması

UAC, denetlenecek müşteri kuruluşla, kapsamın tamamının en iyi temsil edilebileceği bir zamanda denetimin yapılması konusunda teyitleşir ve denetim mevsim, ay, gün/tarih ve vardiyaya uygun olarak yapılabilir.

6.3. İlk Belgelendirme

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 9.3'de yer alan hükümler geçerlidir. Ek olarak, aşağıdaki BGYS'ye özel gereklilikler ve kılavuz uygulanır.

6.3.1. BG 9.3.1 İlk Belgelendirme Denetimi

BGYS denetimlerinin uygulaması için, BGYS Denetim Prosedürü uygulanır.

BG 9.3.1 Aşama 1

BGYS denetimlerinin uygulaması için, BGYS Denetim Prosedürü uygulanır.

6.3.1.1. BG 9.3.1 Aşama 2

BGYS denetimlerinin uygulaması için, BGYS Denetim Prosedürü uygulanır.

6.4. Denetimin Gerçekleştirilmesi

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 9.4'de yer alan hükümler geçerlidir. Ek olarak, aşağıdaki BGYS'ye özel gereklilikler ve kılavuz uygulanır.

6.4.1. BG 9.4 Genel

BGYS denetimlerinin uygulaması için, BGYS Denetim Prosedürü uygulanır.

6.4.2. BG 9.4 BGYS Denetiminin Özel Unsurları

BGYS denetimlerinin özel unsurlarının belirlenmesi için, BGYS Denetim Prosedürü uygulanır.

6.4.3. BG 9.4 Denetim Raporu

BGYS Belgelendirme denetim raporlarının içeriği ve kullanımı için, BGYS Denetim Prosedürü uygulanır.

6.5. Belgelendirme Kararı

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 9.5'de yer alan hükümler geçerlidir. Ek olarak, aşağıdaki BGYS'ye özel gereklilikler ve kılavuz uygulanır.

6.5.1. BG 9.5 Belgelendirme Kararı

BGYS belgelendirmesinin verilmesi/geri çekilmesi kararları, Değerlendirme ve Belgelendirme Komite İşlemleri Prosedürü ve Askı ve Geri Çekme Prosedürü doğrultusunda, UAC bünyesinde oluşturulmuş Belgelendirme Komitesi tarafından alınır.

Belgelendirme Komitesi, denetim proseslerinin ve denetim ekibi tarafından yapılan tavsiyelerin değerlendirilmesi için yetkin olduğu tüm alanlarda, belirli seviyede bilgi birikimi ve tecrübeye sahip, denetimde yer almamış kişi/kişilerden oluşturulur.

UAC, denetim ekibinden, Belgelendirme kararına esas sağlamak amacıyla, kararı alabilmek için yeterli bilgileri sağlayan açık ve anlaşılır denetim raporları talep eder.

Bir müşteri kuruluşun BGYS'sinin Belgelendirme kararı, ISO/IEC 17021-1'in gerekliliklerine ek olarak, denetim raporunda yer alan Belgelendirme tavsiyesine dayanılarak alınır.

Belgelendirme Komitesinin, normal olarak denetim ekibinin olumsuz bir tavsiyesini geri çevirmemesi esastır. Bu tür bir durum gerçekleşirse UAC, tavsiyenin geri çevrilmesi kararını yazılı hale getirir ve gerekçelendirir.

Hazırlayan	Onaylayan
Yönetim Temsilcisi	Genel Müdür

Yönetimin gözden geçirmeleri ve BGYS iç denetimleri için düzenlemelerin yapıldığı, etkin olduğu ve sürdürüleceğinin gösterilmesine dair yeterli kanıt bulunmadıkça, müşteri kuruluşa Belgelendirme verilmez.

6.6. Belgelendirmenin Sürdürülmesi

6.6.1. Genel

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 9.6.1'de yer alan hükümler geçerlidir.

6.6.2. Gözetim Faaliyetleri

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 9.6.2'de yer alan hükümler geçerlidir. Ek olarak, aşağıdaki BGYS'ye özel gereklilikler ve kılavuz uygulanır.

6.6.2.1. BG 9.6.2 Gözetim Faaliyetleri

9.6.2.1.1 Gözetim denetimlerinde, ISO/IEC 27006 standardında tanımlandığı gibi, müşteri kuruluşun BGYS' sinin, belgelendirme denetimleri ile uyumlu olmasını sağlamak üzere, BGYS Denetim Prosedürü uygulanır.

Gözetimin amacı, onaylanmış BGYS'nin uygulanmasının sürdürüldüğünü doğrulamak, müşteri kuruluşun yapılanmasındaki değişikliklerin olası sonuçlarının etkilerini değerlendirmek ve Belgelendirme gerekliliklerine uygunluğun devam ettiğini doğrulamaktır. Gözetim denetimleri, en azından aşağıdakileri kapsar:

a) Bilgi güvenliği risk değerlendirmesi ve kontrolünün sürdürülmesi, BGYS iç denetimi, yönetimin gözden geçirmesi ve düzeltici faaliyet gibi sistem sürdürme hususları;

b) BGYS standardı ISO/IEC 27001'in gerektirdiği şekilde dış taraflarla iletişimler ve Belgelendirme için gerekli olan diğer dokümanlar;

c) Belgelendirilen sistemde yapılan değişiklikler;

d) Değişime tabi durumlar;

e) Seçilen ISO/IEC 27001 gereklilikleri;

f) Uygun olan diğer seçilmiş durumlar.

9.6.2.1.2 UAC tarafından yapılan her gözetimde, en azından aşağıdaki hususlar incelenir:

a) BGYS'nin müşteri kuruluşun bilgi güvenliği politikasının, hedeflerine ulaşılması bakımından etkinliği;

b) İlgili bilgi güvenliği mevzuatı ve düzenlemeleri açısından, periyodik değerlendirme uygunluğunun gözden geçirilmesi için prosedürlerin işleyişi;

c) Belirlenen kontrollerdeki değişiklikler ve bunların sonucunda SoA'da yapılan değişiklikler;

d) Denetim programına göre kontrollerin uygulanması ve etkinliği.

9.6.2.1.3 UAC, risklere bağlı bilgi güvenliği sorunlarına ve bunun müşteri kuruluşa olan etkilerine göre gözetim programını uyarlar ve doğrular.

Gözetim denetimleri, diğer yönetim sistemlerinin denetimleri ile birleştirilebilir. Raporlama, her bir yönetim sistemi ile ilgili hususları açıkça belirtir. UAC, kendisine iletilen itirazların ve şikâyetlerin kayıtlarını kontrol eder ve Belgelendirme gerekliliklerini yerine getirmede herhangi bir uygunsuzluk veya başarısızlığın bulunduğu durumlarda, müşteri kuruluşun kendi BGYS ve prosedürlerini incelediğini ve uygun düzeltici faaliyetleri gerçekleştirip gerçekleştirmediğini denetler.

Bir gözetim raporu, özellikle, önceden ortaya çıkan uygunsuzlukların giderilmesine ilişkin bilgiler ile SoA'nın denetlenen sürümünü ve önceki denetimden bu yana meydana gelen önemli değişiklikleri içerir. Gözetim sonucu hazırlanan raporlar en azından 9.6.2.1.1 ve 9.6.2.1.2'nin yukarıda belirtilen gerekliliklerinin tamamını içerir.

6.6.3. Yeniden Belgelendirme

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 9.6'da yer alan hükümler geçerlidir. Ek olarak, aşağıdaki BGYS'ye özel gereklilikler ve kılavuz uygulanır.

6.6.3.1. BG 9.6.3 Yeniden Belgelendirme Denetimleri

BGYS yeniden belgelendirme denetimlerinin uygulaması için, BGYS Denetim Prosedürü uygulanır.

6.6.4. Özel Denetimler

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 9.6'da yer alan hükümler geçerlidir. Ek olarak, aşağıdaki BGYS'ye özel gereklilikler ve kılavuz uygulanır.

6.6.4.1. BG 9.6.4 Özel Durumlar

Sertifikalandırılmış bir BGYS'ye sahip olan müşteri kuruluş, sistemindeki büyük çapta değişiklik yaparsa veya belgelendirmenin temelini etkileyebilecek diğer değişiklikler gerçekleştirirse (SoA üzerinden yapılan değişiklikler gibi) bu durumlardan UAC'yi haberdar etmesi istenir. Böyle durumlarda, gerekirse özel denetimler gerçekleştirilebilir.

6.6.5. Belgelendirmenin Askıya Alınması, Geri Çekilmesi veya Kapsamının Daraltılması

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 9.6'da ve Askı ve Geri Çekme Prosedüründe yer alan hükümler geçerlidir.

6.7. İtirazlar

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 9.7'de ve Şikayet ve İtirazların Yönetimi Prosedüründe yer alan hükümler geçerlidir.

6.8. Şikâyetler

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 9.8'de ve Şikayet ve İtirazların Yönetimi Prosedüründe yer alan hükümler geçerlidir. Ek olarak, aşağıdaki BGYS'ye özel gereklilikler ve kılavuz uygulanır.

6.8.1. BG 9.8 Şikâyetler

UAC, BGYS'si belgelendirilmiş her bir müşteri kuruluşa, ISO/IEC 27001:2013'ün gereklilikleri doğrultusunda tüm şikâyetlerin ve gerçekleştirilen düzeltici faaliyetlerin kayıtlarının istendiğinde incelemeye hazır bulundurulmasını, Belgelendirme sözleşmesinde şart koşar.

6.9. Müşteri Kayıtları

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 9.9'da ve Kayıtların Kontrolü Prosedüründe yer alan hükümler geçerlidir.

7. BELGELENDİRME KURULUŞLARI İÇİN YÖNETİM SİSTEMİ GEREKLİLİKLERİ

ISO/IEC 17021-1:2015 ile ISO/IEC 27006:2015 standardları ve ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı madde 10.3'de yer alan gereklilikler uygulanır. Ek olarak, aşağıdaki BGYS'ye özel gereklilikler ve kılavuz uygulanır.

ISO/IEC 17021-1:2015 standardına uygun olarak hazırlanan, aşağıda verilen UAC yönetim sistemi prosedürlerine göre gerçekleştirilir:

- Doküman Kontrol Prosedürü
- Kayıtların Kontrolü Prosedürü
- Yönetimin Gözden Geçirmesi Prosedürü
- İç Tetkik Prosedürü
- Düzeltici ve Önleyici Faaliyet Prosedürü

Hazırlayan	Onaylayan
Yönetim Temsilcisi	Genel Müdür

Teknik Alan Kodu	Teknik Alan	Alt Teknik Alan Kodu	Alt Teknik Alan
A	Yazılım Hizmetleri	A.1	Güvenlik Yazılımları Hizmetleri
		A.2	Kriptolojik ve Şifreleme Yazılımları Hizmetleri
		A.3	Muhasebe ve Bankacılık Yazılımları Hizmetleri
		A.4	Telekomünikasyon ve İşletim Sistemi Yazılımları Hizmetleri
		A.5	Mültimedya ve İnternet Yazılımları Hizmetleri
		A.6	AR-GE Yazılımları Hizmetleri
B	Donanım Hizmetleri	B.1	Mültimedya, Server- Ağ ve İnternet Donanım Hizmetler
		B.2	Telekomünikasyon, Mobil Cihaz ve İşletim Sistemi Donanım Hizmetleri
		B.3	Güvenlik Donanım Hizmetleri
C	Server Hizmetleri	C.1	Hosting Amaçlı Server Hizmetleri
		C.2	Ofis Amaçlı Server Hizmetleri
D	Teknik Servis Hizmetleri	D.1	Güvenlik Yazılımları Servis Hizmetler
		D.2	Kriptolojik ve Şifreleme (Encoder ve Decoder) Yazılımları Servis Hizmetleri
		D.3	Muhasebe ve Bankacılık Yazılımları Servis Hizmetleri
		D.4	Telekomünikasyon ve İşletim Sistemi Yazılımları Servis Hizmetleri
		D.5	Mültimedya ve İnternet Yazılımları Servis Hizmetleri
		D.6	Donanım Hizmetleri Teknik Servisi Hizmetleri
E	Üretim Faaliyetleri	-	-
F	Bankacılık ve Finans Hizmetleri	-	-
G	Kamu Yönetimi	-	-
H	Sağlık Hizmetleri	-	-
I	Eğitim Öğretim Hizmetleri	-	-
J	Elektronik Ticaret	-	-
K	Elektronik ve Sayısal İmzalar	-	-
L	Verilerin korunması, depolama ve mahremiyeti (müşteri ile ilgili veriler)	-	-
M	Network ağ altyapısı işletme ve teknik hizmetleri	-	-

Hazırlayan	Onaylayan
Yönetim Temsilcisi	Genel Müdür

****Elektronik nüshasının basılması ve pdf olarak gönderilmesi durumunda, basılmış bu doküman kontrolsüz kopya olarak işlem görür.**

Karmaşıklık Faktörleri	Risk Sınıfı			Önem
1-BGYS&KVYS Karmaşıklık Faktörleri	Yüksek	Orta	Düşük	
1.1 Çalışan Sayısı +Sözleşmeli Personel	≥ 250 (3 Puan)	≥ 50 (2 Puan)	< 50 (1 Puan)	*BGYS&KVYS uygulamasının ölçeği *Bilgi sisteminin yönetimi *Üretim yönetimi ile ilgili sistemler *Satış/dağıtım/genel servisle ilgili sistemler *Bilgi teknolojisi/bilgi hizmetleriyle ilgili hizmetler *İnşaat/gemi yapımı/fabrika
1.2 Yasal uygunluğa verilen önem	Kurala uymama durumunda muhtemel cezai yaptırıma sebep olması (3 Puan)	Kurala uymama durumunda önemli finansal yaptırıma sebep olması (2 Puan)	Kurala uymama durumunda önemsiz finansal yaptırıma sebep olması (1 Puan)	İlgili mevzuat, kılavuzlar ve ilkeler ISO/IEC 27001 A.15
1.3 Sektöre özel risklerin uygulanabilirliği	Öze kanun ve yükümlülüklerin uygulanması durumu (3 Puan)	Sektöre özel kanun ve düzenleme uygulanamaz ancak önemli derecedeki sektöre özel risk uygulanması durumu (2 Puan)	Özel kanun ya da düzenlemede sektöre özel risk de uygulanamaz durumu (1Puan)	*BGYS&KVYS uygulamasının ölçeği *İlgili mevzuat, kılavuzlar ve ilkeler ISO/IEC 27001 A.15
1.4 Ağ bağlantısı şifreleme teknolojisi	Dış veriler şifrelenmiş internet bağlantısı dijital imza PKI gereklilikleri durumu (3 Puan)	Dışsal veriler şifrelenmiş internet bağlantısı dijital imza olmadan durumu (2 Puan)	Dış veriler şifresiz internet bağlantısı sayısal imza/PKI gereksinimleri durumu (1 Puan)	* Telekomünikasyon ve operasyon yönetimi ISO/IEC 27001 A.10 *Erişim Kontrolü ISO/IEC 27001 A.11
1.5 risk durumu yapılan ve değerlendirilen kritik bilgilerin hacmi	≥50 (3 Puan)	≥ 10 (2 Puan)	< 10 (1 Puan)	
1.6 Projelerinin sayısı ve büyüklüğü	≥ 7 (3 Puan)	≥ 3 (2 Puan)	< 3 (1 Puan)	
1.7 Uzaktan çalışmanın kapsamı	≥ 25% (3 Puan)	≥ 10% (2 Puan)	< 10% (1 Puan)	
1.8 BGYS&KVYS Belgelendirme kapsamı	Karmaşık (3 Puan)	Normal (2 Puan)	Basit (1 Puan)	
2- BGYS&KVYS kapsamının büyüklüğü ile ilgili faktörler				
2.1 Kullanılan bilgi sistemi sayısı (Program sayısı)	≥10 (3 Puan)	≥5 (2 Puan)	< 5 (1 Puan)	
2.2 Kullanıcı sayısı	≥ 100 bin (3 Puan)	≥ 50 bin (2 Puan)	< 50 bin (1 Puan)	
2.3 İmtiyazlı kullanıcı sayısı	≥50 (3 Puan)	≥10 (2 Puan)	<10 (1 Puan)	

Hazırlayan	Onaylayan
Yönetim Temsilcisi	Genel Müdür

****Elektronik nüshasının basılması ve pdf olarak gönderilmesi durumunda, basılmış bu doküman kontrolsüz kopya olarak işlem görür.**

2.4 İşletim sistemi platform sayısı	≥3 (3 Puan)	≥2 (2 Puan)	< 2 (1 Puan)	
2.5 Ağ bağlantısı sayısı ve boyutu				
Server sayısı	≥20 (3 Puan)	≥10 (2 Puan)	< 5 (1 Puan)	
Çalışma istasyonu +PC +laptop	≥300 (3 Puan)	≥50 (2 Puan)	< 50 (1 Puan)	
Belgelendirme denetlemesinden önce kuruluşa Denetçilerin görmesini istemedikleri gizli ya da hassas bilgi içeren bir kayıt olup olmadığı sorulur. Bu kayıtların yokluğunda BGYS&KVYS'nin yeterince denetlenip denetlenemeyeceğine karar verir. Eğer bu kayıtların yokluğunda denetleme yapılamayacağına karar verirse kuruluşa erişimi için gerekli düzenlemeler yapılmadan denetleme yapılamayacağına dair bilgi verilir.				
3-Kulanılan teknolojinin kapsamı ve çeşitliliği				
3.1 Proseslerin ve dokümanların kontrolleri	Yetersiz (3 Puan)	Normal (2 Puan)	Mükemmel (1 Puan)	
3.2 Düzeltici ve Önleyici Faaliyet	Yetersiz (3 Puan)	Normal (2 Puan)	Mükemmel (1 Puan)	
3.3 Bilgi sistemleri				
3.3.1) Şebeke	Wireless (3 Puan)	Mobile (2 Puan)	Sabit (1 Puan)	
3.3.2) Lokasyon	Harici (3 Puan)	Dahili (2 Puan)		
4. BGYS&KVYS kapsamı içinde				
4.1 Alan sayısı	≥ 5FarklıBenzer (3 Puan)	≥ 2FarklıBenzer (2 Puan)	1FarklıBenzer (1 Puan)	
4.2 Denetim alanları	Tüm alan (3 Puan)	Örnek alan (2 Puan)	-	
5- Bu hizmetlere bağlılık ve BGYS&KVYS'nin kapsamında kullanılan dış kaynak kullanımının ve üçüncü taraf anlaşmalarının kapsamı				
5.1 Dış kaynak kullanımı:	Evet (3 Puan)	Hayır (1 Puan)		
5.2 BGYS&KVYS kapsamında dış kaynak kullanımının oransal büyüklüğü	≥ 50% (3 Puan)	≥ 20% (2 Puan)	< 20% (1 Puan)	
5.3 Bu hizmetlere bağlılık	Düşük (3 Puan)	Orta (2 Puan)	Yüksek (1 Puan)	
6. Belgelendirmeye uygulanan standardlar				
6.1 Diğer standardlar:	Hayır (3 Puan)	-	Evet (1 Puan)	
6.2 Mevzuat ve düzenlemeler:	Hayır (3 Puan)	-	Evet (1 Puan)	
6.3 Uygulanabilen sektöre ilişkin diğer gereklilikler	Hayır (3 Puan)	-	Evet (1 Puan)	

Arttırma/ Azaltma Puanı	Artırma/ Azaltma Kriteri	Risk Sınıfı	
91~100	+ 30 %	Yüksek	- Toplam denetim gün sayısı, tablolardaki karmaşıklık faktörlerine göre ve arttırma/azaltma faktörler göz önünde bulundurularak hesaplanır. - Arttırma/Azaltma Yüzdesi = Toplam Puan X (100/78)
86~90	+ 20 %		
76~85	+ 10 %	Orta	
66~75	0 %		
61~65	- 10 %		

Hazırlayan	Onaylayan
Yönetim Temsilcisi	Genel Müdür

****Elektronik nüshasının basılması ve pdf olarak gönderilmesi durumunda, basılmış bu doküman kontrolsüz kopya olarak işlem görür.**

56~60	- 20 %	Düşük	
50~55	- 30 %		

İLGİLİ DOKÜMANLAR

ISO/IEC 17021-1:2015
ISO/IEC 27006:2015
ISO/IEC 27001:2013
ISO/IEC 17021-1 EK-Yönetim Sistemi El Kitabı
FR.07-02 Yönetim Sistemleri belgelendirme Başvuru Formu
FR.22-01 BGYS Belgelendirme Başvuru Kontrol Formu
PR.01 Kaynaklar Prosedürü
PR.05 Belgelendirme Usul ve Esasları Prosedürü
PR.12 Askı ve Geri Çekme Prosedürü
PR.23 BGYS Denetim Prosedürü
PR.14 Doküman Kontrol Prosedürü
PR.15 Kayıtların Kontrolü Prosedürü
PR.16 Yönetimin Gözden Geçirmesi Prosedürü
PR.17 İç Tetkik Prosedürü
PR.18 Düzeltici Faaliyet Prosedürü
PR.13 Şikayet ve İtirazların Yönetimi Prosedürü
PR.08 Tetkik Süresi Belirleme Prosedürü
TL.07-03 Belge, Logo ve Marka Kullanma Talimatı

REVİZYON BİLGİLERİ

REV. NO.	REVİZYON TARİHİ	REVİZYON AÇIKLAMASI
00	30.06.2021	İlk Yayın

Hazırlayan	Onaylayan
Yönetim Temsilcisi	Genel Müdür

****Elektronik nüshasının basılması ve pdf olarak gönderilmesi durumunda, basılmış bu doküman kontrolsüz kopya olarak işlem görür.**