1. AMAÇ

Bu Prosedür, ISO/IEC 27001:2022 AMD 1:2024, ISO/IEC 27701, ISO/IEC 27006-1:2024 ve ISO/IEC 17021-1:2015 kuralları çerçevesinde CAS tarafından Kuruluşların yönetim sistemlerinin Sistemlerini, Başvuruda belirtilen Kapsam dâhilinde referans doküman şartlarına göre denetim faaliyetinin yürütülmesi amacıyla hazırlanmıştır.

2. TANIMLAR

Büyük Uygunsuzluk: Standart maddelerinden herhangi birinin veya alt başlıklarının ele alınmaması veya uygulanmamasıdır.

Büyük uygunsuzluklar ile ilgili düzeltici faaliyetler yerine getirilmeden, takip denetimi veya doğrulama yapılmadan belge verilme kararı alınamaz.

Küçük Uygunsuzluk: Standard maddelerinden herhangi birinin veya alt başlıklarının yeterli olarak tanımlanmaması, uygulanmaması ve/veya sistemin sağlıklı çalışmasını etkileyecek eksiklik ve aksaklıkların olmasıdır. Küçük uygunsuzluklar için takip denetimi gerektiği denetim ekibi tarafından önerilmemişse, bu uygunsuzlukların giderilip giderilmediği doküman ve kayıtların incelenmesi ile de kontrol edilebilir.

Küçük uygunsuzluklar ile ilgili düzeltici faaliyetleri belirlenmeden veya yerine getirilmeden belge verilme kararı alınamaz.

Çoklu Şubesi/İşletmesi Olan Kuruluşlar: Her biri ayrı adreslerde olan sahalar topluluğundan oluşan ve her bir sahada aynı yönetim sistemi altında gerçekleştirilen faaliyetin mevcut olduğu kuruluşlar. Bu kuruluşlarda belli faaliyetlerin planlandığı, kontrol edildiği belirlenmiş bir merkezi fonksiyondan oluşan tek yönetim sistemi (KYS, ÇYS, GGYS, BGYS/KVYS vb.) ve benzer faaliyetlerin kısmen veya tamamen gerçekleştirildiği saha (geçici, kalıcı, veya sanal) ağı mevcuttur.

Uygulanabilecek çok alanlı kuruluş örnekleri aşağıda belirtilmiştir:

•Franchise sistemi ile işletilen kuruluşlar
•Satış Ofisi ağları ile dağıtım yapan firmalar
•Bir veya birden fazla üretim sahası ve satış ofis ağı bulunan üretim şirketleri
•Benzer hizmeti çoklu sahada sağlayan hizmet kuruluşları

Birleşik Denetim: Bir müşterinin iki veya daha fazla yönetim standartlarının şartlarına göre birlikte tetkik
edildiği denetimdir.

Entegre Denetim: Müşterinin iki veya daha çok yönetim sistemi standartları şartlarının tek bir yönetim
sistemi içine entegre edilmiş uygulamasının, bir standarttan daha fazlasına göre yaptığı denetimdir.

Ortak Denetim: tek bir müşterinin tetkikinin, iki veya daha fazla belgelendirme kuruluşunun birlikte yaptığı tetkiktir.

Bilgi Güvenliği Yönetim Sistemi (BGYS/KVYS): 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]

Kullanılabilirlik: Yetkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliği. [ISO/IEC 13335-1]

Gizlilik: Bilginin yetkisiz kişiler, varlıklar ya da proseslere kullanılabilir yapılmama ya da açıklanmama özelliği. [ISO/IEC 13335-1]

Bilgi Güvenliği: Bilginin gizliliği, bütünlüğü ve kullanılabilirliğinin korunması. Ek olarak, doğruluk, açıkla edememe ve güvenilirlik gibi diğer özellikleri de kapsar. [ISO/IEC 17799]

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]

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]

Bütünlük: Varlıkların doğruluğunu ve tamlığını koruma özelliği. [ISO/IEC 13335-1]

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/KVYS' ni 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

F001 Sertifikasyon Talep Formu
F002 Sertifikasyon Sözleşmesi Formu
F003 Başvuru Değerlendirme Formu
F004 Atama Formu
F005 Katılım Formu
F006 Plan Formu
F007 Program Formu
F008 Düzeltici Faaliyet Formu
F009 A1 Denetim Raporu
F010 A2 Denetim Raporu
F011 BD D TU Değerlendirme Formu-Müşteri
F015 BGYS/KVYS Belgelendirme Başvuru Kontrol Formu
Uzaktan Denetim Analiz Formu
F026 Gözetim-Yeniden Belgelendirme Teyit Formu
F030 Karar Alma Formu
P008 Personel Atama ve Performans Değerlendirme Prosedürü
P005 Düzeltici Önleyici Faaliyet Prosedürü
P002 Kayıtların Kontrolü Prosedürü
P009 Belgelendirmenin Askıya Alınması ve Geri Çekilmesi Prosedürü
P007 İtiraz ve Şikayet Prosedürü
P015 BGYS/KVYS Belgelendirme Prosedürü
T004 Back Up Talimatı
ISO/IEC 17021-1:2015
ISO/IEC 27006-1:2024
ISO/IEC 27001:2022 AMD 1:2024
ISO/IEC 27701
ISO/IEC 27002
ISO/IEC 27003
ISO/IEC 27004
ISO/IEC 27005

4 Süreç Gereklilikleri

4.1 Belgelendirme Öncesi Faaliyetler

4.1.1 Başvuru

CAS, aşağıdaki hususları sağlamak için gerekli bilgiyi müşteri kuruluştan aşağıdaki bilgileri talep eder;

Kuruluşun adı ve sahaların adresleri, belgelendirme için kapsam, prosesleri ve operasyonları insan ve teknik kaynaklarını fonksiyonları, ilişkileri ve her türlü yasal yükümlülükler, bütün dış kaynaklı proseslere ilişkin bilgi, hangi standartlar ve şartlar için belgelendirme istediği, danışmanlık hizmeti alınmasıyla ilgili bilgi.

Belgelendirme başvuruları Sertifikasyon Talep Formu ve BGYS/KVYS Belgelendirme Başvuru Kontrol Formu elden veya posta (e-mail, faks, kargo vb. iletişim araçları) ile alınır. Belgelendirme Başvuru Formu, Planlama sorumlusuna iletilir. Belgelendirme Başvuru Formu, Planlama sorumlusu tarafından incelenerek kuruluşun kapsamı değerlendirilir. CAS'ın akreditasyon kapsamı içindeyse Belgelendirme Müdürü, başvuruyu onaylar.

CAS Belgelendirme, başka bir UDK tarafından ISO/IEC 27001 belgesine sahip bir işletmeyi tek başına ISO/IEC 27701 tetkiki sonucu belgelendiremez. CAS'ın, ISO/IEC 27701 tetkikini ISO/IEC 27001 tetkiki ile birlikte yapması gerekmektedir. Ya da önceden CAS belgelendirme tarafından ISO/IEC 27001 belgesine sahip işletmelerin başvurusu kabul edilir.

Belgelendirme Müdürü tarafından onaylanan Belgelendirme Başvuru Formu, Belgelendirme Teklif ve Sözleşmesi hazırlanarak, kuruluşa sunulur. Kuruluştan istenen belgeler ve belgelendirme esasları bu Başvuru formunda belirtilmektedir. Kuruluş tarafından onaylanan Belgelendirme Teklif ve Sözleşmesi ve kuruluştan istenen belgeler (risk değerlendirme methodolojisi, SoA-uygulanabilirlik bildirgesi ve Ek-A kontrolleri için kullanılan varsa referans kaynakların bilgisi, başvuru formları ve tüzel evraklar) Planlama Sorumlusuna iletilir.

Başvuru kabulü ile kuruluş ile CAS arasında Sertifikasyon Sözleşmesi Formu ile karşılıklı olarak Sözleşme imzalanır. Sözleşme her iki kuruluşun imza atmaya yetkilileri arasında gerçekleştirilir.

ISO/IEC 17021-1:2015,Madde 9.1.1'in gereklilikleri esas alındı.

Belgelendirme Prosedürlerine İlişkin Hususlar

CAS prosedürleri, BGYS/KVYS'nin belirli bir uygulama biçimini, dokümantasyon ve kayıtlar için belirli bir formatı önceden varsaymaz. Müşterinin BGYS/KVYS'nin ISO/IEC 27001'de belirtilen gereklilikleri ve müşterinin politika ve hedeflerini karşıladığını doğrulamaya odaklanır.

ISO/IEC 27006-1:2024,Madde 9.1.1.2'nin gereklilikleri esas alındı.

4.1.2 Başvuru İncelemesi

Başvuru Gözden Geçirmesi;

- Denetime başlamadan önce CAS, belgelendirme için aşağıdakileri sağlamak üzere destekleyici bilgileri ve başvuruyu gözden geçirir.
  - ❖ Başvuran kuruluşun yönetim sistemi hakkındaki bilginin bir denetim programı geliştirmek için yeterliliği
  - ❖ CAS ile başvuran kuruluş arasındaki bilinen herhangi bir anlayış farkının giderilmesi
  - ❖ CAS'ın belgelendirme faaliyetini gerçekleştirme yetkinliği ve yeteneğine sahip olması
  - ❖ Belgelendirmesi istenen kapsam, başvuran kuruluşların operasyonlarının yapıldığı saha/ları denetimleri gerçekleştirmek için gerekli olan zaman ve belgelendirme faaliyetlerini etkileyen diğer hususların (dil, güvenlik şartları, tarafsızlığa olan tehditler vb.) her birinin dikkate alınması

Başvuru değerlendirmesi Başvuru Değerlendirme Formu ile kayıt altına planlama bölümü alınır. Planlama bölümü bu bilgileri değerlendirirken ISO/IEC 27006-1:2024 Ek A'daki yeterliliğe sahip olması aranır. Eğer planlana bölümünde personelin yeterliliği olmaz ise ISO/IEC 27001 denetim ekibinden teknik destek alınarak sağlanır ve kayıt altına alınır.

- Başvurunun gözden geçirilmesinden sonra, planlama bölümü başvuruyu kabul veya red etmektedir. Planlama, başvurunun gözden geçirilmesinin sonucuna göre başvuruyu geri

çevirdiğinde, başvuruyu geri çevrilmesinin sebeplerini müşteriye açık bir şekilde sunmakta ve bunları dokümante etmektedir.
- CAS, bu gözden geçirmeyi esas alarak, denetim ekibi ve belgelendirme kararı için gerekli olan yeterliliği El Kitabında yer alan yetki, sorumluluk ve görev tanımlarında ve tüm görevler için hazırlanmış olan P.015 Prosedürü ve Personel Yetkinlik Matrisinde belirlemiştir.
ISO/IEC 17021-1:2015, Madde 9.1.2'nin gereklilikleri esas alındı.

4.1.3 Denetim Programı

Tam bir belgelendirme çevrimi için bir denetim programı, müşterinin istediği yönetim sisteminin doğrultusunda seçilen standard/standartlar veya diğer hüküm ifade eden doküman/dokümanlara göre belgelendirilmesi için gerekli şartları yerine getirdiğini gösteren denetim faaliyetlerini açıklamak amacıyla geliştirilmiş ve uygulanır. Planlama bölümü tarafından program, Program Formu ile hazırlanarak kayıt altına alınır. Program 3 yıllık denetimi içerir. Normalde 3 yılda bir yenilenir ancak, yıl içerisindeki denetimlerde bir değişiklik olması durumunda revize edilerek değişiklikler kayıt altına alınarak onaylanır.
Planlama sorumlusu 3 yıllık bu çevrimi belgelendirme programında gösterir.
Müşteri vardiya usulü ile çalışıyor ise, denetim programı ve planı geliştirilirken, vardiyada yapılan çalışmalar dikkate alınır.
İlk Belgelendirme Denetim programı; iki aşamalı bir başlangıç denetimini, belgelendirme kararını takip eden birinci ve ikinci yıllarda gözetim denetimlerini ve belgelendirmenin geçerliliğini dolmadan önce üçüncü yılda yeniden belgelendirme denetimini kapsar. Üç yıllık belgelendirme çevrimi, belgelendirme veya yeniden belgelendirme kararıyla başlar. Denetim programının ve takip eden her bir düzenlemenin belirlenmesinde, yönetim sistemi verimliliğinin ispat edilen seviyesinin yanı sıra, müşteri kuruluşun büyüklüğü, yönetim sisteminin, ürünlerin ve proseslerin kapsamı ve karmaşıklığı ile önceki denetim sonuçları dikkate alınır.
Gözetim denetimleri, yeniden belgelendirme yapılan yıllar hariç, bir takvim yılı içerisinde en az 1 kez yapılır. İlk belgelendirmeyi takip eden ilk gözetim denetiminin, belgelendirme karar tarihinden itibaren 12 ay içerisinde tamamlanır
CAS, mevcut belgelendirme veya müşterinin başka bir kuruluş tarafından yapılan denetimlerini dikkate aldığında, herhangi bir uygunsuzluğa uygulanan düzeltici faaliyetlere ait raporlar ve dokümantasyon gibi yeterli kanıtları elde ederek saklar. Elde edilen kanıtlar ve dokümantasyonun, bu standardın şartlarının karşılandığını destekleyecek nitelikte olması sağlanır. CAS, elde ettiği bilgiyi esas alarak, var olan denetim programındaki herhangi bir değişikliği ve önceki uygunsuzluklarla ilgili düzeltici faaliyetlerin takibini doğrular ve kayıt altına alır.
ISO/IEC 17021-1:2015, Madde 9.1.3'ün gereklilikleri esas alındı.

Genel Hususlar

BGYS/KVYS tetkikleri için tetkik programı, müşteri tarafından belirlenmiş bilgi güvenliği kontrollerini göz önünde bulundurur.
ISO/IEC 27006-1:2024,Madde 9.1.3.2'nin gereklilikleri esas alındı.

Uzaktan Tetkikin Uygulanması

Uzaktan tetkik faaliyetleri, müşteri BGYS/KVYS'nin tetkikinde uygulanabilecek uzaktan tetkik faaliyetlerinin (uzaktan tetkikler) düzeyini belirlenir.
Müşteri için uzaktan tetkik kullanımına ilişkin risklerin analizini içermeli ve aşağıdaki faktörleri dikkate alınır;
a) CAS ve müşterinin mevcut altyapısı,
b) müşterinin faaliyet gösterdiği sektör,
c) ilk tetkikten yeniden belgelendirme tetkikine kadar belgelendirme döngüsü boyunca gerçekleştirilen tetkik türleri,
d) uzaktan tetkike katılan CAS ve müşteri personelinin yetkinliği,
e) müşteri için daha önce gösterilmiş uzaktan tetkik performansı,
f) belgelendirme kapsamı.
Analiz, herhangi bir uzaktan tetkik gerçekleştirilmeden önce yapılır. Belgelendirme döngüsü sırasında uzaktan tetkik kullanımının analizi ve gerekçesi Uzaktan Denetim Analiz Formu ile kayıt

altına alınır.
Tetkik planı ve tetkik raporu, uzaktan tetkik faaliyetlerinin gerçekleştirilip gerçekleştirilmediğine dair açık göstergeler içerir.
Risk değerlendirmesi, tetkik sürecinin etkinliği açısından kabul edilemez riskler tespit ederse uzaktan tetkikler kullanılmamaktadır.
Risk değerlendirmesi, sürekli uygunluğunu sağlamak için belgelendirme döngüsü sırasında gözden geçirilir.
Müşterinin sanal ortamlar kullanması durumunda (yani, bir kuruluşun fiziksel konumlardan bağımsız olarak süreçleri yürütmesine olanak tanıyan çevrimiçi bir ortam kullanarak iş yaptığı veya hizmet sağladığı konum), uzaktan tetkik teknikleri tetkik planının bir parçası olarak değerlendirilerek Uzaktan Denetim Analiz Formu ile kayıt altına alınır.
ISO/IEC 27006-1:2024,Madde 9.1.3.3'ün gereklilikleri esas alındı.

Ön Tetkik İçin Genel Hazırlıklar

CAS, müşteriden iç tetkik raporlarına ve bilgi güvenliğiyle ilgili bağımsız değerlendirme raporlarına erişim için bütün gerekli hazırlıkları yapmasını planlama bölümü tarafından ister.
ISO/IEC 27006-1:2024,Madde 9.1.3.4'ün gereklilikleri esas alındı.

Değerlendirme Dönemleri

CAS, en az bir yönetim incelemesinden ve iç BGYS/KVYS tetkiklerine ilişkin düzenlemelerin uygulandığını, etkili olduğunu ve belgelendirme kapsamını sağlayacak şekilde sürdürüleceğini gösteren yeterli kanıt olmadığı sürece bir BGYS/KVYS'yi belgelendirmez.
ISO/IEC 27006-1:2024,Madde 9.1.3.5'in gereklilikleri esas alındı.

BGYS/KVYS Belgelendirmesinin Kapsamı

Denetim ekibi, müşterinin tanımlanmış kapsamını içeren BGYS/KVYS'sini her türlü uygulanabilir belgelendirme gerekliliğine göre tetkik eder. CAS, müşterinin BGYS/KVYS kapsamında müşterilerin ISO/IEC 27001, Madde 4.3'te belirtilen gereklilikleri dikkate aldığını doğrular.
CAS, müşterinin bilgi güvenliği risk değerlendirmesinin ve riskleri ele alış biçiminin, müşterinin faaliyetlerini tam anlamıyla yansıttığına ve belgelendirme kapsamında belirtildiği gibi faaliyet sınırlarını da kapsamasını sağlar. CAS, bu hususun, müşterinin BGYS/KVYS ve SoA kapsamına yansıtıldığını doğrular ve belgelendirme kapsamı için bir SoA olduğunu onaylar.
CAS, kapsam dışı hizmetler veya faaliyetler sahip hususların BGYS/KVYS denetimi esnasında değerlendirildiği ve müşterinin bilgi güvenliği risk değerlendirmesinde yer aldığından tespit eder.
ISO/IEC 27006-1:2024,Madde 9.1.3.6'nın gereklilikleri esas alındı.

4.1.4 Tetkik Süresinin (Denetim Zamanı) Belirlenmesi

CAS, denetim zamanını belirlemeye yönelik bu Prosedürde ve Denetim Süreleri Belirleme Talimatı oluşturmuş ve uygulamaktadır.
CAS denetçilerine ilk denetleme, gözetim denetlemesi ya da yeniden sertifikasyon denetlemesinde bütün aktiviteleri tamamlamaları için yeterli zaman belirlenen süre için;
Yönetim sistemi kapsamının karmaşıklığı, denetleme zamanına karar verirken dikkate alınması gerekir. "yüksek", "orta" ve "düşük" olmak üzere üç sınıfta değerlendirilir. Karmaşıklığın tüm etkin sınıfı, dikkate alınan tüm faktörlerin azami sınıfı olarak göz önüne alınabilir ve sonuç ise, ör. "yüksek", "orta" ya da "düşük" sınıfıdır. Bunun içeriği Ek C'de detaylandırılmıştır.
Yönetim sistemi kapsamının karmaşıklığı ve kapsamının büyüklüğü ile ilgili faktörler ve durum bilgisi değerlendirilir. Müşteri organizasyonunun analiz edilmesinde Belgelendirme Başvuru İnceleme Formu ile kapsamının karmaşıklığı ve kapsamının büyüklüğü ile ilgili her ikisinde de yüksek risk içeriyorsa en fazla %30 artırma yapılır. Değerlendirme sonucu düşük risk belirlendiği durumda ise en fazla %30 indirim uygulanır. Risk grupları belirlenerek ilgili kapsamında atanan bu karmaşıklık ile denetleyicinin denetlemesi için denetleme süresi belirlenir.
Yönetim sistemi kapsamına yapılan bütün atıflar prosesler ve ürün/hizmetler değerlendirilmeli denetleme süresini etkileyecek faktörler düzeltme yapılarak etkin bir denetim süresi belirlenmelidir. Düzeltme yapılan durumlarda kayıtlar tutulacaktır.
CAS, her bir müşterisi için müşterisinin yönetim sisteminin tam ve etkili bir denetimini planlamaya ve gerçekleştirmeye yönelik ihtiyaç duyulan süreyi belirler.
Denetim zamanının belirlenmesinde CAS, diğerlerinin yanı sıra aşağıdaki hususları dikkate alır:

1. İlgili yönetim sistem standardının şartlarını,
2. Müşterinin ve yönetim sisteminin karmaşıklığını,
3. Teknolojik ve mevzuat bağlamını,
4. Yönetim sistemi kapsamında yer alan bütün faaliyetlerinden, taşerona verilen faaliyetlerini,
5. Önceki denetimlerin sonuçlarını,
6. Tesislerin büyüklüğü ve sayısı, bunların coğrafi konumları ve birden çok tesis değerlendirmelerini,
7. Ürünler, prosesler ya da kuruluşun faaliyetleri ile ilgili risklerini,
8. Denetimlerin, birleşik, ortak veya entegre olduğunu,

Yönetim sistem denetiminin süresi ve ispatı kaydedilir.
Bir denetçi olarak atanmayan herhangi bir ekip üyesi tarafından harcanan süre (yani, teknik uzmanlar, tercümanlar, gözlemciler ve eğitim almak için katılan denetçiler) yukarıda belirlenen yönetim sistemi denetim süresi içinde sayılmaz.
ISO/IEC 17021-1:2015, Madde 9.1.4'ün gereklilikleri esas alındı.
CAS denetçilerine ilk denetleme, gözetim denetlemesi ya da yeniden sertifikasyon denetlemesinde bütün aktiviteleri tamamlamaları için yeterli zaman belirlenen süre aşağıdaki faktörlere göre belirlenecektir.
*Yönetim sistemi kapsamının büyüklüğüyle ilgili faktörler (ör: kullanılan bilgi sistemi sayısı, düzenlenen bilgi adedinin hacmi, kullanıcı sayısı, ayrıcalıklı kullanıcı sayısı, IT platformu sayısı, ağ bağlantısı sayısı ve bunların büyüklüğü)
*Yönetim sisteminin karmaşıklığıyla ilgili faktörler (ör: bilgi sistemlerinin kritikliği, risk durumu, yapılan ve değerlendirilen kritik bilgilerin hacmi ve tipleri, elektronik işlem sayısı ve tipleri, geliştirme projelerinin sayısı ve genişliği, uzaktan çalışmanın gerçekleşme oranı, dokümantasyonunun oranı)
* Yönetim sistemi kapsamında gerçekleştirilen iş tipleri ve bu işlere ilişkin güvenlik, kanuni, düzenleyici, kontrat ve iş gereklilikleri
* Yönetim sisteminin farklı değişkenlerinin değerlendirilmesi ile ilgili kullanılan teknolojinin oranı ve çeşitliliği (ör: uygulanan kontroller, dokümantasyon ve proses kontrolü, düzeltici/önleyici faaliyet, bilgi sistemleri, IT sistemleri, ağ bağlantıları. Bütün bunların sabit mi, hareketli mi, kablosuz mu, dışsal mı, içsel mi oluşuna bağımlı olarak)
*Yönetim sistemi kapsamındaki işyeri sayısı, bu işyerlerinin benzerlik ve farklılıkları ve bütün bu işyerlerinin mi yoksa numune olarak bir tanesinin mi denetleneceği
* felaket kurtarma planları için yapılan proje sayıları
*Yönetim sisteminin daha önce belirtilmiş performansı
*Yönetim sistemi kapsamındaki outsourcing ve üçüncü parti düzenlemelerinin miktarı ve bu servislere bağımlılık
*Sertifikasyona uygulanan standartlar, kanunlar ve düzenlemelerle birlikte uygulanabilecek sektöre özel gereklilikler
*Gözetim veya yeniden belgelendirme denetimi için süreye etki edecek kıstaslar ISO/IEC 17021-1, 8.5.3 uyarınca Yönetim sistemi ile ilgili değişikliklerin bildirilmesi ile ayarlama için genel parametreleri oluşturur.
*Bir BGYS/KVYS'nin belgelendirmesi genellikle bir kalite yönetim sistemi ya da çevre yönetim sistemini belgelendirmekten daha fazla zaman alır. Bunun sebebi BGYS/KVYS politikası, risk yönetimi ve BGYS/KVYS/BTHY hedefleri ve kontrolü gibi unsurlardan dolayı BGYS/KVYS'nin özel taleplerinde bilgi güvenliği sistemleriyle ilgili gerekliliklerin artmış olmasıdır. Sertifikasyon kuruluşu aşağıdaki gereklilikleri yerine getirmelidir:

- ❖ Müşteri organizasyonun bilgi güvenliği/kişisel veri/ bilgi teknolojileri hizmet risklerinin önemini ve bunların etkilerini dile getirişinin makul ve anlaşılır olup olmadığını denetlemek
- ❖ Uygunluk (bütün ilgili kanuni şartlar ve BGYS/KVYS'ne uygunluk gösteren diğer şartlar) göstermek üzere tasarlanmış sistemin bunu yapabildiğini teyit ederek bu sistemin yerine getirildiğini ve korunduğunu belirtmek
- ❖ Kontrol hedeflerinin ve kontrollerin doğru olarak seçilip belirlendiğinin teyit edilerek

etkinliklerin ölçüldüğünün ve “güvenlik zaaflarını önleme ve doğru karşılık verme” hususunu başarma üzere oluşturulan prosesin uygun ve katılımcı olduğunun belirlenmesi

- ❖ Müşteri organizasyonun yönetim sistemi ile ilgili doküman gerekliliklerinin yerine getirildiğinin teyidi
- ❖ Birinci aşama denetimden kaynaklanan artan talebin karşılanması
- ❖ Denetleme süresi belirlenirken tüm faktörler dikkate alınmalıdır. Her bir sertifikasyon için harcanan zamandaki değişiklik, İş ve Organizasyonu, Bilgi Teknolojisi ortamı parametreleri ve yukardaki faktörlere bağlı olarak değişiklik gösterebilir.

ISO/IEC 27701:2022 AMD 1:2024 belgelendirme faaliyetleri için UDK tetkiklerinde tetkikçi/gün süresini
ISO/IEC 27006-1:2024 standardında verilen süreleri dikkate alarak hesaplanır. ISO/IEC 27701 standardı ISO/IEC 27001 ve ISO/IEC 27002 standartlarına ilave şartlar getirdiği için tetkikçi/gün süreleri hesaplanırken ISO/IEC 27006-1:2024 standardında verilen sürelere en az %30 süre ilave edilir.
Yönetim sistemi tetkik süresi, tetkik zamanının %70’inden az olmamalı, planlama ve rapor yazma (off-site) faaliyetleri ise bu zamanın en fazla %30 ‘si kadar olmalıdır. (ilk belgelendirme, gözetim ve yeniden belgelendirme için)
Planlama ve/veya rapor yazımı için ek süre gerekli olduğunda, bu, yerinde denetim süresini azaltmak için bir gerekçe olamaz. Denetçi seyahat süresi bu hesaplamaya dahil edilmez ve çizelgede belirtilen denetim süresine ilave edilir.
“Rapor yazma için ek bir süre gerekmesi yerinde geçirilen denetçi süresinin (on-site) azaltılması için bir gerekçe değildir. Denetçi seyahat süresi, bu hesaplamaya dahil edilmemiştir ve çizelgedeki denetçi süresine ilavedir.’’
Annex Ek B' de ki şartlara Ek olarak kapsam için hesaplanan toplam yerinde denetçi günlerinin sayısı, sahanın yönetim sistemi için uygunluğuna ve belirlenen risklere bağlı olarak farklı sahalar arasında dağıtılır. Dağıtımın gerekçesi, CAS Planlama bölümü tarafından kayıt altına alınır.
İlk belgelendirme denetimi ve gözetim için harcanan toplam süre, her bir sahada harcanan süre artı merkez ofiste harcanan toplam sürenin toplamıdır. Tüm işin tek bir sahada kuruluşu tüm çalışanları ile yapılması halinde, hiçbir zaman operasyonun boyutu ve karmaşıklığı için hesaplanacak olan süreden daha az olmamaktadır.
Gözetim süresi, ilk belgelendirme denetiminde harcanan sürenin yaklaşık 1/3'ü, yeniden belgelendirme denetimi ise ilk belgelendirmenin 2/3’ü kadardır.
Denetimin süresi, planlanan denetim süresinin %80’inden az olamaz. Planlama ya da rapor yazımı için ek süre gerektiği takdirde, bu süre denetim süresinden sayılmayacaktır.
Denetim süresi, müşterinin yönetim sisteminin eksiksiz ve sonuç verici şekilde denetimi için gereken denetim süresi olarak tanımlanır. Denetim süresi, müşterinin konumunda (fiziksel veya sanal) geçen süre ile, planlama, belge denetimi, müşterinin personeliyle etkileşim ve rapor yazımı gibi saha dışı aktiviteler için harcanan sürenin toplamını kapsar. Yönetim sistemi belgelendirme denetimlerinin süresi, açılış toplantısından kapanış toplantısına kadar denetim faaliyetlerini yürütmek için harcanan süre olarak tanımlanır.
İş yerinde çalışan sayısı, bütün vardiyalar dahil olmak üzere, belgelendirmenin kapsamında kalan personelin tamamından oluşur. Belgelendirmenin kapsamına dahil edilirse, kalıcı olmayan (örn:taşeron işçiler) ve yarı zamanlı çalışanlar da çalışan sayısına eklenir. Çalışma saatlerine göre, yarı zamanlı personel sayısı ve kısmen kapsam dahilindeki çalışan sayısı azaltılabilir ya da artırılarak tam zamanlı personel sayısına dönüştürülebilir. Benzer faaliyetleri ve görevleri yerine getiren personel yüzdesinin yüksek olduğu durumlarda, belgelendirme kapsamı dahilinde her müşteriye uygulanması koşuluyla, çalışan sayısı tutarlı bir şekilde azaltılabilir.
Müşterinin hizmet yönetimi sisteminin ve hizmetlerinin bütün özellikleri göz önüne alınarak, gerekiyorsa ilk denetim süresinde azaltma ya da artırma yapılır. Toplam süre üzerinde yapılan düzenlemeler ne olursa olsun, CAS müşterinin hizmet yönetimi sisteminin eksiksiz ve sonuç verici bir denetimine yeterli süre ayırmakla yükümlüdür. Gerekçeler yazılı olarak açıklanır.
Tablo 1.1.a. ve 1.1.b. ilgili faktörlerin Tablo 1.1’de belirtilen denetim sürelerine etkilerini

göstermektedir. Vardiya, ardışık çalışma dönemi yöntemi ile çalışan birden fazla yer ve/veya personel arasındaki geçişler olarak tanımlanır.
Tablo 1.1'de belirtilen denetim süreleri üzerinden en fazla %30'luk bir azaltma yapılabilir.
Müşteri Kuruluşunun Karmaşıklığının ve Sektöre Özel Hususların Analizi Kuruluşun Risk Potansiyelini Belirleme Adımları;
Yönetim Sistemi kapsamının karmaşıklığı, denetleme zamanına ve denetçi yeterliliğine karar verirken dikkate alınması gerekir. Bu amaç için bir müşteri kuruluşunun karmaşıklığını analiz etmeye ait bir örnek verilmiştir.
Bir Yönetim Sistemi kapsamına tahsis edilen karmaşıklık sınıfı,
a) Denetçinin yeterlilik gereksinimlerine;
b) Denetim süresi gereksinimlerine karar vermek için kullanılabilir.
Karmaşıklık Kriterleri kullanılarak bir Yönetim sistemi kapsamının karmaşıklığının hususları, "yüksek", "orta" ve "düşük" olmak üzere üç sınıfa ayrılır.
Karmaşıklık kriterleri denetçi yeterliliklerine karar vermede ve denetim sürelerinin belirlenmesinde arttırıcı veya azaltıcı faktörleri tespit etmede kullanılır.
CAS denetçilerine ilk denetleme, gözetim denetlemesi yada yeniden belgelendirme denetlemesinde bütün faaliyetleri tamamlamaları için gerekli olan yeterli zamana karar verirken; ISO/IEC 27006-1:2024 Ek B ve Ek C de yer alan İş ve Organizasyon yapısı ve Bilgi Teknolojileri alt yapısı ile İlgili Faktörleri dikkate almaktadır. Firma başvuru aşamasında, başvuru formu ile beraber BGYS/KVYS Belgelendirme Başvuru Kontrol Formunu doldurarak belirtilen kriterler planlama sorumluları yada teknik görüş alınabilen Denetim Ekibi üyeleri denetçi yada teknik uzman tarafından değerlendirilir ve denetim süresi belirlenir.
Denetim Bilgi Formu ve Denetim Planı doğrulaması ayrıca aşama.1 de Atama Formu ile denetçi tarafından kontrol edilerek yapılır. Tablo C.1 de yer alan denetim süreleri, Tablo C.3 ve Tablo C.4' de yer alan iş karmaşıklığı ve bilgi teknolojisi karmaşıklığı risk düzeyine bağlı olarak tablo 5'te yer alan matrise göre artırma yada azaltma oranları belirlenerek hesaplanır. Sürelerde en fazla %30 artı/eksi oranlama yapılabilir. Tablo 2'de yer alan bilgilerden denetim süresi hesaplamada ve faktörlerin sınıflandırılmasında yararlanılır. Tablolar ISO/IEC 27006-1:2024 Ek B ve EK C referans alınarak hazırlanmıştır.
Hesaplamalardan sonra sonuç bir ondalık sayı ise, gün sayısı en yakın yarım güne yuvarlanır. (örn:5.3 denetim günü 5.5 denetim günü, 5.2 denetim günü ise 5 denetim günü olur.) Aşağıdaki tablolarda yuvarlama yapılmıştır. Aşama 1 denetimi için harcanan zaman Aşama 2 denetimini için harcanan zamandan fazla olamaz.
Gözetim denetimleri için, ilk belgelendirme denetim süresinin yaklaşık 1/3'ü, yeniden belgelendirme denetimleri için; 2/3'ü ayrılır. Yeniden belgelendirme denetimlerinde yönetim sistemlerinin sistem performansı değerlendirmesi sonucu denetim sürelerinde azaltma veya artırmaya gidilebilir. Gözetim ve yeniden belgelendirme denetim zamanlarının 1 denetim zamanından az olması beklenemez.
Denetim süresinde, aşağıdaki durumlar söz konusu olursa azaltma veya arttırma yapılabilir. Hiç bir durumda azaltma veya arttırma oranı % 30'u geçemez.

CAS tetkik süresini belirlemek için ISO/IEC 27006-1:2024 **Ek C**'yi kullanır.

Tetkik süresinin hesaplanması üzerine daha fazla kılavuzluk ve örnekler ISO/IEC 27006-1:2024 **Ek D**'den faydalanılır.

Ek C Tetkik Süresi

C.1 Giriş

CAS, denetçilere ön tetkik, gözetim tetkiki ve yeniden belgelendirme tetkikiyle ilgili tüm faaliyetleri yürütmeleri için yeterli süreyi tanır. Toplam tetkik süresinin hesaplanması, tetkik raporlaması için yeterli süreyi de içerir.
CAS, her bir müşteri ve belgelendirilmiş BGYS/KVYS için ilk belgelendirme, gözetim ve yeniden

belgelendirme için gereken tetkik sürelerini belirlemekle yükümlüdür.
Ek olarak, tetkik esnasında, özellikle Aşama.1'de bulunanlara göre tetkik süresi ayarlanabilir. (ör. BGYS/KVYS kapsamının karmaşıklığına dair farklı değerlendirmeler ya da kapsama ilave konumlar girmesi).
Bu Ek şunları sunar:

- tetkik süresi hesaplaması için kullanılan kavramlar (C.2);
- ön tetkikin farklı aşamaları için tetkik süresi belirleme prosedürleri için gereklilikler (C.3);
- gözetim (C.4) ve yeniden belgelendirme (C.5) tetkiki için tetkik süresi gereklilikleri;
- çoklu konum tetkikleriyle ilgili gereklilikler (C.6);
- kapsam genişletmeleri için tetkik süresi gereklilikleri (C.7).

Bu ekin uygulanmasında gösterilen tetkik süresi hesaplaması için örnekler Ek D'de verilmiştir.
Bu yaklaşımın temel varsayımı, tetkik süresini belirlemek için olan hesaplama şemasının:

- sadece doğruluğu ispatlanabilecek özellikleri göz önüne alması;
- CAS'ın geçerli, karşılaştırılabilir ve tekrarlanabilir sonuçlar uygulayıp elde edebileceği kadar basit olması;
- nitelik değerlerindeki değişikliklerin, ortaya çıkan tetkik süresinde karşılaştırılabilir değişikliklere yol açmasını sağlayacak kadar gelişmiş olması esastır.

Tetkik süresinin belirlenmesi aşağıda Çizelge C.1'de verilen rakamları esas almaktadır ve değişiklik için katkı sağlayan faktörleri göz önüne alır.
CAS, tarafından belirlenen tetkik süresini belirleme yaklaşımı, BGYS/KVYS'nin karmaşıklığı için yeterli olup olmadığını doğrulamak amacıyla düzenli olarak gözden geçirilir.

C.2 Kavramlar

C.2.1 Kuruluşun kontrolü altında çalışan kişi sayısı

Belgelendirme kapsamındaki tüm vardiyalarda kuruluş kontrolü altında çalışan toplam kişi sayısı tetkik süresini belirlemek için başlangıç noktasıdır.
NOT Kuruluşun kontrolü altında çalışan kişiler, BGYS/KVYS gereklerine göre çalışması gereken belgelendirme kapsamındaki tüm personeli (kuruluşun üyesi olup olmadıklarına bakılmaksızın) içerir.
Kuruluşun kontrolü altında yarı-zamanlı çalışan kişiler, kuruluşun kontrolü altında çalışan kişi sayısına, kuruluş kontrolü altında tam-zamanlı çalışan kişilerin çalışma saatleriyle kıyaslanarak ilgili oranda dâhil edilirler. Bu belirleme, tam-zamanlı bir çalışana kıyasla çalışılan saat sayısına bağlı olmaktadır.
Kuruluşun kontrolü altında belgelendirme kapsamında çalışan kişilerin yüksek bir yüzdesi belirli benzer faaliyetleri gerçekleştirdiğinde, tetkik süresinin hesaplanması için Çizelge C.1'in kullanılmasından önce kişi sayısının azaltılması yapılır.
CAS, belgelendirme kapsamındaki kişi sayısının nasıl azaltılacağını belirlemek için Madde C.3.4'te belirtilen faktörleri kullanır ve faaliyetlerin bilgi güvenliği riskleri üzerindeki etkisini değerlendirir. Şirketten şirkete uygulanabilir ve tekrarlanabilir olan tutarlı ve uyumlu prosedür(ler) dokümante edilir.

C.2.2 Denetçi günü

Çizelge C.1'de atıf yapılan tetkik süresi denetçinin tetkikte geçirdiği gün sayısı cinsinden belirtilir. Bu ek, hesaplamasını 8 saatlik bir çalışma gününe dayandırır.

C.3 Ön tetkik için tetkik süresi hesaplama prosedürü

C.3.1 Genel

CAS, tetkik süresinin hesaplanması için dokümante edilmiş bir prosedüre sahip olur ve bu prosedürü izler.

C.3.2 Uzaktan tetkik yöntemleri

Eğer, interaktif ağ tabanlı işbirliği, ağ toplantıları, tele-konferanslar ve/veya kuruluşun süreçlerinin elektronik doğrulaması gibi uzaktan tetkik teknikleri kuruluş ile iletişim kurulması için kullanılırsa, bu faaliyetlerin tetkik planında gösterilmesi esastır (bk. Madde 9.2.3) ve toplam "saha tetkik süresi"ne kısmi olarak katılımı değerlendirilir.
NOT Saha tetkik süresi, ayrı konumlara tahsis edilen tetkik süresini ifade eder. Uzak konumlara

yapılan elektronik tetkikler, fiziksel olarak kuruluşun kendi konumlarında yapılıyor olsa bile uzaktan tetkik olarak kabul edilir.

C.3.3 Tetkik süresi hesaplama

Çizelge C.1'de sunulan tetkik süresi şablonu, ön tetkik için ortalama gün sayısının belirlenmesi için başlangıç noktasını verir, [bu ek'te ve Ek D'de belirtilen bu sayı ön tetkike ait günleri kapsar (Aşama.1 ve Aşama.2)] bu kuruluş kontrolü altında çalışan kişilerin sayısı ve BGYS/KVYS kapsamına uygun tecrübeyi yansıtmaktadır. Tecrübeler, benzer büyüklükteki BGYS/KVYS kapsamları için, bazılarının daha fazla zamana ihtiyaç duyduğunu gösterir.

Aşağıdaki tetkik süresi şablonu, tetkik planlamasında kullanılacak çerçeveyi sağlar. Başlangıç noktası, tüm vardiyalar için kuruluşun kontrolü altında çalışan kişilerin toplam sayısına dayanır. Denetçi gün sayısı, tetkik yapılacak BGYS/KVYS kapsamı için geçerli olan önemli faktörlere göre ayarlanır ve her bir faktöre esas temel modeli değiştirmek için artırıcı veya eksiltici bir ağırlıklandırmada kullanılır. Çizelge C.1'deki tetkik süresi şablonu, katkıda bulunan faktörleri ve azami sapmaların kısıtlamalarını da göz önünde bulundurarak kullanılır (bkz. Madde C.3.4 ve Madde C.3.5). Çizelge C.1'de kullanılan terimler C.2'de açıklanmaktadır.

Ek D, bu ekteki hesaplama yönteminin kullanımına dair örnekler verilmektedir.

C.3.4 Başlangıç kişi sayısının belirlenmesi

CAS, müşteriden belirli özdeş faaliyetleri gerçekleştiren kişi sayısının fazlalığıyla ilgili olarak aşağıdaki bilgileri talep eder:

- Faaliyette yer alan kişi sayısı,
- Faaliyet veya süreç türü.

Hesaplamada temel alınan ve belirli özdeş faaliyetleri gerçekleştiren kişi sayısını azaltabilecek faktörlere örnek olarak şunlar verilebilir:

- Görevlerini yerine getirmek için bilgilere salt okunur erişimi olan kişiler,
- BGYS/KVYS kapsamında şirketin bilgi işleme tesislerine erişimi olmayan kişiler,
- BGYS/KVYS kapsamında şirketin bilgi işleme tesislerine belirli, kanıtlanabilir kısıtlı erişimi olan kişiler,
- Bilgi ifşasını kısıtlamak için katı uygulamaların uygulandığı faaliyetleri gerçekleştiren kişiler, örneğin; çalışma alanına kişisel eşya ve aygıtların sokulmasını yasaklayan önlemler.

Özdeş faaliyetleri gerçekleştiren kişi sayısındaki azalma, görevlerle ilişkili faaliyetlerin riskine göre yapılır. Her bir aynı faaliyeti gerçekleştiren kişi sayısının karekökü bir sonraki tam sayıya yuvarlanarak etkin kişi sayısını belirlemek ve tetkik süresini hesaplanmak için kullanılır. Elde edilen bu sayı, izin verilen azami kişi sayısı azaltımı olmaktadır.

Görevlerin niteliği, yasal gereklilikler ve kişilerin erişebildiği bilgilerin önemi, azaltımı sınırlayabilir. Bu prosedürden sonra belirlenen kişi sayısı Çizelge C.1'deki başlangıç noktasıdır.

NOT Çizelge IAF MD5 ile aynı şekilde yapılandırılmıştır.

(Annex C) Tablo C.1- ISO/IEC 27006-1:2024 Denetim Süresini Belirleme çizelgesin 'de verilmiştir.

Çalışan sayısı	İlk denetim için BGYS/KVYS denetim süresi (denetçi gün)	Artırıcı ve eksiltici faktörler
1~10	5	27006-1 / C.3.5
11~15	6	27006-1 / C.3.5
16~25	7	27006-1 / C.3.5
26~45	8.5	27006-1 / C.3.5
46~65	10	27006-1 / C.3.5
66~85	11	27006-1 / C.3.5
86~125	12	27006-1 / C.3.5
126~175	13	27006-1 / C.3.5
176~275	14	27006-1 / C.3.5
276~425	15	27006-1 / C.3.5
426~625	16.5	27006-1 / C.3.5
626~875	17.5	27006-1 / C.3.5
876~1175	18.5	27006-1 / C.3.5

1176~1550	19.5	27006-1 / C.3.5
1551~2025	21	27006-1 / C.3.5
2026~2675	22	27006-1 / C.3.5
2676~3450	23	27006-1 / C.3.5
3451~4350	24	27006-1 / C.3.5
4351~5450	25	27006-1 / C.3.5
5451~6800	26	27006-1 / C.3.5
6801~8500	27	27006-1 / C.3.5
8501~10700	28	27006-1 / C.3.5
> 10,700	Yukarıdaki artışa paralel	27006-1 / C.3.5

Denetim zamanını azaltan faktörler bir araya gelse de, belgelendirme denetimi için belirlenen zaman bu faaliyetlerin etkisiyle toplam olarak %30'dan fazla azaltılmaz. Çalışan sayısı BGYS/KVYS' nin kapsamı ile ilişkili olan tüm bireyleri gösterir. BGYS/KVYS kapsamındaki tüm vardiyalar için kuruluşun kontrolü altında çalışan sayısı, denetim süresinin belirlenmesi için başlangıç noktasıdır.
Belgelendirme kapsamındaki tüm vardiyalar için kuruluşun kontrolü altında çalışan toplam kişi sayısı dikkate alınarak denetim süresi belirlenir.

C.3.5 Tetkik süresi ayarlaması için faktörler

Çizelge C.1 tek başına kullanılmaz. Tahsis edilen süre, BGYS/KVYS'nin karmaşıklığı ilgili olan aşağıdaki faktörler ve dolayısıyla BGYS/KVYS tetkiki için gerekli olan çaba göz önünde bulundurulur:

- BGYS/KVYS karmaşıklığı (ör: bilginin kritikliği, BGYS/KVYS risk durumu, vb.);
- BGYS/KVYS kapsamında gerçekleştirilen iş türü/türleri;
- daha önceden gösterilen BGYS/KVYS performansı;
- BGYS/KVYS'nin çeşitli bileşenlerinin uygulamasında kullanılan teknoloji çeşitliliği ve kapsamı (ör. farklı BT platformlarının sayısı, ayrık ağların sayısı);
- BGYS/KVYS kapsamında kullanılan dış kaynak kapsamı ve üçüncü şahıs düzenlemeleri;
- bilgi sistemi geliştirme kapsamı;
- bölge sayısı ve Felaketten Kurtarma (DR) bölgeleri sayısı;
- birinci aşamadan sonra, CAS kontrollerin sayısını ve karmaşıklığını dikkate alacaktır;
- gözetim veya yeniden belgelendirme tetkiki için: ISO/IEC 17021-1:2015, Madde 8.5.3 uyarınca BGYS/KVYS ile ilgili değişiklik kapsamı ve miktarı.

Ek D tetkik süresi hesaplanırken bu farklı faktörlerin nasıl dikkate alınacağına dair örnekler verir.
İlave tetkik süresi gerektiren örnek faktörler:

- BGYS/KVYS kapsamında birden fazla bina veya konum içeren karmaşık süreç lojistiği;
- birden fazla dil konuşan çalışan (tercüman(lar)a ihtiyaç duyulması veya her bir denetçinin bağımsız olarak çalışmasının önlenmesi) veya birden fazla dilde sağlanmış dokümantasyon;
- yönetim sistemi belgelendirmeye tabi olan daimi sahanın/sahaların faaliyetlerini onaylamak için geçici sahaların ziyaretini gerektiren faaliyetler (aşağıdaki paragrafa ve listeye bakınız);
- BGYS/KVYS için geçerli olan çok sayıda standart ve düzenleme.

Daha kısa tetkik süresine imkân veren örnek faktörler:

- risksiz veya düşük riskli prosesler;
- tek bir genel faaliyet içeren prosesler (ör. sadece hizmet);
- kuruluş hakkında önceki bilgiler (örneğin, kuruluşun daha önceden aynı CAS tarafından başka bir standart için belgelendirilmiş olması);
- belgelendirilme için yüksek düzeyde hazırlıklı olunması (örneğin, hâli hazırda belgelendirilmiş veya bir başka üçüncü taraf düzenlemesine göre tanınırlık);
- mevcuttaki yönetim sisteminin olgunluk seviyesinin yüksek olması.

Belgelendirme müşterisi veya belgelendirilmiş kuruluşun geçici sahalarda ürünlerini veya hizmetlerini sunduğu durumlarda, bu sahaların değerlendirmesinin belgelendirme tetkiki ve gözetim programlarına dahil edilmesi önemlidir.

Yukarıdaki faktörler için ayarlamalar yapılır. Tetkik süresinin eklenmesini veya çıkarılmasını gerektiren faktörler birbirini dengeleyebilir. Her durumda, Çizelge C.1'de verilen tetkik süresi şablonunda gösterilen sürede düzenlemeler yapıldığında, değişimin gerekçesine dair yeterli delil ve kayıt sağlanır.

C.3.6 Tetkik süresinin sapmasının kısıtlanması

Etkili tetkiklerin gerçekleştirilmesini sağlamak, güvenilir ve karşılaştırılabilir sonuçları garantilemek için tetkik süresi şablonunda sağlanan süre %30'dan fazla indirilmez. İndirimler için uygun nedenler belirlenir ve Başvuru Değerlendirme Formu ile kayıt altına alınır.

C.3.7 Saha tetkik süresi

Planlama ve rapor yazımı için hesaplanan sürenin, sahadaki toplam "tetkik süresini" (fiziksel/ uzaktan) C.3.3, C.3.4 ve C.3.5 maddelerine göre hesaplanan toplam sürenin %70'nin altına indirmemesi esastır. Planlama ve/veya rapor yazımı için ek sürenin gerekli olduğu durumda, bu durum saha tetkik süresinin azaltılması için gerekçe olmamaktadır. Tetkikçinin seyahat süresi bu hesaplamaya dâhil değildir ve şablonda gösterilen tetkik süresine ek olarak hesaplanır. Tetkik süresi hesaplamaları Başvuru Değerlendirme Formu ile kayıt altına alınır.

NOT 1 %70, BGYS/KVYS tetkik deneyimlerine dayalı bir faktördür.

NOT 2 "(fiziksel/uzaktan)" terimi, "yerinde" tetkiklerin fiziksel veya uzaktan gerçekleştirilebileceği anlamına gelir. (bkz. Madde 9.2.3 ve C.3.2). "Yerinde" tetkikler için ayrıca ISO/IEC 17021-1:2015, Madde 9.4.1'e bakılır.

C.4 Gözetim tetkikleri için tetkik süresi

İlk belgelendirme tetkik döngüsü için, ilgili kuruluş için verilen gözetim süresinin, ön tetkikte harcanan süreye orantılı olması ve yıllık olarak gözetimde harcanan sürenin, İlk Belgelendirmeye harcanan sürenin yaklaşık 1/3'ü kadar olması esastır. Planlanmış gözetim süresinin, tetkik süresini etkileyen değişiklikler bakımından zaman zaman gözden geçirilmektedir. Gözetim tetkikinde geçen süre BGYS/KVYS'deki değişikliklerin (yeni veya değiştirilmiş kontrollerin, süreçlerin ve hizmetlerin tetkiki gibi) tetkikine izin verecek ölçüde artırılır. Gözetim süresi hesaplamaları Başvuru Değerlendirme Formu ile kayıt altına alınır.

NOT 1 %70, BGYS/KVYS tetkik deneyimlerine dayalı bir faktördür.

C.5 Yeniden belgelendirme tetkiki için tetkik süresi

Yeniden belgelendirme tetkiki yapılırken harcanan toplam süre, Madde 9.4.3 ve ISO/IEC 17021-1:2015, Madde 9.6.3'te tanımlanan daha önceki tetkik sonuçlarına bağlıdır. Yeniden belgelendirme tetkikinde geçen sürenin aynı kuruluşun ilk belgelendirme tetkikinde harcanacak süre ile orantılı olması ve yeniden belgelendirme tetkikinin yapılacağı zamanda aynı kuruluşun ilk belgelendirme tetkiki için gerekli olacak sürenin en az 2/3'ü olması esastır. Yeniden Belgelendirme süresi hesaplamaları Başvuru Değerlendirme Formu ile kayıt altına alınır.

NOT 1 %70, BGYS/KVYS tetkik deneyimlerine dayalı bir faktördür.

C.6 Çoklu konum tetkik süresi

Genellikle, yerinde tetkik için toplam tetkik süresi, bulundukları yerden bağımsız olarak kuruluşun kontrolü altında çalışan toplam kişi sayısı dikkate alınarak hesaplanır.

Alternatif olarak, dokümante edilmesi gereken haklı gerekçelerle, her bir tesis için ayrı ayrı hesaplanan tetkik sürelerinin, bu maddenin birinci paragrafına göre belirlenen süreden daha uzun olması koşuluyla toplanmasına izin verilir. Merkez ofis veya yerel konumlarla (varsa) ilgili olmayan tetkik bölümleri dikkate alınarak azaltım uygulanabilir. Bu azaltımların gerekçeleri CAS tarafından Başvuru Değerlendirme Formu ile kayıt altına alınır.

Toplam yerinde denetçi gün sayısı - C.3.3 ve C.3.4'te belirtilen prosedür ve bu madde uyarınca kapsam için hesaplanan - yönetim sistemi için konumun önemi, konumda yürütülen faaliyetler ve tanımlanan riskler temelinde farklı konumlara dağıtılır. Dağıtılma gerekçesi CAS tarafından Başvuru Değerlendirme Formu ile kayıt altına alınır.

Herhangi bir azaltım, tetkik süresi genel tetkik süresiyle karşılaştırılmadan önce uygulanır.

C.7 Kapsam genişletmeleri için tetkik süresi

Bir BGYS/KVYS'nin kapsamını genişletmek için gereken tetkik süresi, aşağıdaki faktörler dikkate alınarak hesaplanır:

- genişletme türü;
- mevcut belgelendirme faaliyeti/faaliyetleri;
- faaliyetin/faaliyetlerin gerçekleştirildiği konum sayısı;
- faaliyet/faaliyetlerle ilgili bilgi güvenliği riskleri;
- genişletmeyle ilişkili kontrollerin sayısı;
- yeni kapsam doğrultusunda kuruluşun kontrolü altında çalışan kişi sayısı;
- genişletilmiş kapsamın BGYS/KVYS'ye entegrasyonunun gözden geçirilmesi için gereken süre.

CAS, kapsamın genişletilmesine yönelik tutarlı bir yaklaşım sağlayan prosedürlere sahiptir.
Yeni kapsamın ilk tetkiki için süre, C.3.3, C.3.4 ve C.3.5 kullanılarak mevcut kapsama eklenen kişi ve konum sayısına göre hesaplanır.
Tetkik süresi, müşterinin BGYS/KVYS'sini gözden geçirmek için hesaplanan süreye eklenir. Bu ek süre en az aşağıdaki gibi olur:

- kapsam genişletme tetkikinin gözetim tetkiki veya yeniden belgelendirme tetkiki ile birlikte
- gerçekleştirilmesi halinde 0,5 gün (denetçi günü).
- kapsam genişletme tetkikinin ayrı bir tetkik olarak gerçekleştirilmesi halinde 1,0 gün (denetçi günü).

Ek D Tetkik Süresinin Hesaplaması İçin Yöntemler

D.1 Genel

Bu ek, tetkik süresinin hesaplanması için formül oluşturmaya dair daha fazla kılavuzluk sağlar. D.2 tetkik süresinin hesaplanmasında baz alınabilecek faktörlerin sınıflandırmasına bir örnek verir ve D.3 tetkik süresinin hesaplanması örneğini sağlar.
NOT Bu Ek'teki kavramlar, Madde C.3.4'te açıklandığı gibi, belirli özdeş faaliyetleri yürüten kişilerin sayısı baz alınarak bir azaltım uygulandıktan sonra başlar.

D.2 Tetkik süresi hesaplaması için faktörlerin sınıflandırılması

Çizelge D.1 C.3.5 a) ila i)'de listelendiği gibi, tetkik süresi hesaplaması için ana etkenlerin sınıflandırılmasına dair örnekler verir. Bu sınıflandırma, Madde 9.1.4.2 doğrultusunda tetkik süresi hesaplama taslağı oluşturmak için CAS tarafından kullanılır.

Çizelge D.1 - Tetkik süresi hesaplaması için faktörlerin sınıflandırılması

	Çabaya olan etkisi		
	Azaltılmış çaba	**Normal çaba**	**Artırılmış çaba**
1. BGYS/KVYS/KVYS karmaşıklığı - Bilgi güvenliği ihtiyaçları [gizlilik, bütünlük ve kullanılabilirlik, (CIA)] - Kritik varlıkların sayısı - Süreçlerin ve hizmetlerin sayısı	- Düşük kullanılabilirlik gereksinimleri ve az derecede hassas veya gizli bilgi - Az sayıda kritik varlıklar (gizlilik-bütünlük kullanılabilirlik açısından) - Az sayıda arabirim ve iş birimi içeren tek bir iş süreci	- Yüksek kullanılabilirlik gereksinimleri ya da orta derecede hassas veya gizli bilgi - Orta düzeyde kritik varlıklar - Az sayıda arabirim ve iş birimi içeren 2-3 iş süreci	- Yüksek kullanılabilirlik gereksinimleri veya yüksek oranda hassas veya gizli bilgi (Örneğin sağlık, kişisel bilgiler, sigorta, bankacılık, gıda, ilaç uzay, nükleer) - Yüksek düzeyde kritik varlıklar - Birçok arabirim ve iş birimi içeren 2 den fazla karmaşık iş süreci
2. BGYS/KVYS kapsamında gerçekleştirilen iş türü(leri)	Yasal düzenleyici gereksinimleri olmayan düşük riskli iş(ler)	Yüksek düzenleyici gereksinimleri bulunan iş(ler)	Yasal gereksinimlerle sınırlandırılmış yüksek riskli iş(ler)
3. BGYS/KVYS den önce gösterilmiş yönetim sistemi performansı	-Yakın zamanda belgelendirilmiş -Kurum belgeli değil ancak BGYS/KVYS ile ilgili uygulanmakta olan iç denetimler, yönetim gözden geçirmeleri ve uygulanan	-Yakın zamanda gözetim denetimine katılmış - Kurum belgeli değil ancak kısmen BGYS/KVYS ile ilgili uygulanan bazı yönetim sistem uygulamaları mevcut,	- Belgelendirmesi bulunmuyor ve ve herhangi bir denetime tabi tutulmamış - Kurumda BGYS/KVYS yeni ve tam uygulanmamakta (örneğin; yönetim sistemi, belirli kontrol

	sürekli iyileştirme sistemi de dahil olmak üzere, denetim ve iyileştirme döngüsünün kurumda uygulanmış, kanıtlanabilir olması	sürekli iyileştirme süreçleri uygulanıyor ama kısmen kanıtlanabilir olması	mekanizmaları ve sürekli iyileştirme süreçlerinin eksik uygulanması)
4. **BGYS/KVYS kapsamında kullanılan teknoloji alt yapısının çeşitliliği (örneğin; farklı BT platformları sayısı, ayrılmış ağ sayısı)**	Düşük çeşitlilik, standart ortam (az sayıda BT-platformları, sunucular, işletim sistemleri, veri tabanları, ağlar, vs.)	Standart ortam ama farklı BT platformları, sunucular, işletim sistemleri, veri tabanları, ağlar (çeşitlilik daha çok)	Yüksek çeşitlilik ve karmaşık BT (örn: birçok farklı ağ kategorileri, sunucuların veya veri tabanlarının türleri, anahtar başvuru sayısı)
5. BGYS/KVYS kapsamında kullanılan dış kaynak ve üçüncü parti düzenlemelerin derecesi	- Dış kaynak kullanımı olmaması, tedarikçilere bağımlılığın az olması veya; - İyi tanımlanan, yönetilen ve izlenen dış kaynak düzenlemeleri - Taşeronun BGYS/KVYS sertifikasına sahip olması - Dış proses ile ilgili bağımsız güvence raporunun varlığı	Dış kaynak düzenlemelerinin çeşitli olması ve kısmen yönetilebilmesi	-Önemli iş faaliyetleri büyük etkiye sahip dış kaynaklar veya tedarikçilere bağımlılığın yüksek olması veya; - Belirsiz miktarda dış kaynak kullanımı veya - Yönetilmeyen bazı dış kaynak kullanımı
6. Bilgi sistemi geliştirme derecesi	-Kurum içi sistem geliştirmenin olmaması - standart yazılım platformlarının kullanılması	-Karmaşık şekilde yapılandırılmış/ parametrelendirilmiş standartlaştırılmış yazılım platformların kullanımı - ileri derecede özelleştirilmiş yazılımlar. -Bazı sistem geliştirme faaliyetleri (kurum içi ya da dışardan destek alınan)	-Önemli iş faaliyetlerini gerçekleştirmek amacı ile kurum içinde yapılan yazılım geliştirme faaliyetlerin ve yazılım projelerine sahip olması
7. Alanlar ve Felaket kurtarma alanlarının sayısı	Kullanılabilirlik gereksinimleri düşük, felaket kurtarma alanı yok yada en fazla bir alan mevcut	Kullanılabilirlik gereksinimleri Orta veya Yüksek, felaket kurtarma alanı yok ya da en fazla bir alan mevcut	-Yüksek kullanılabilirlik gereksinimleri örneğin; 7/24 servis hizmetleri -Birkaç alternatif felaket kurtarma sitesi -Birkaç veri merkezi
8. Yeniden belgelendirme veya gözetim denetimi için; ISO/IEC 17021-1:2015 madde 8.5.3 gereği, BGYS/KVYS çerçevesinde bilgi değişikliklerin miktarı ve değişimin kapsamı	Son yeniden belgelendirme denetimden beri hiçbir değişiklik yoksa	-Kapsamda ya da SoA'da küçük değişiklikler örneğin bazı politikalar, belgeler gibi -Yukarıdaki faktörlerde küçük değişiklikler mevcutsa	-Kapsamda ya da SoA'da büyük değişiklikler örneğin yeni süreçler, yeni iş birimleri, alanlar, risk değerlendirme yönetim metodolojisi, politikalar, dokümantasyon, risk tedavisi gibi -Yukarıdaki faktörlerde büyük değişiklikler mevcutsa

Çizelge D.2 - İş ve kuruluşla ilişkili faktörler (BT dışında)

İş ve Organizasyon İle İlgili Faktörler (IT Haricinde)			
İş Tipleri Ve	**DÜŞÜK**	**ORTA**	**YÜKSEK**

Düzenleyici Gereksinimler	Kuruluş Kritik Olmayan Sektörlerde Faaliyet Gösteriyor Ve Yasal Yükümlülüğe Tabi Olmayan Bir Sektörlerde Çalışıyor* ☐ (1 puan)	Kururluş Kritik Sektörlerdeki Müşterilere Sahip* ☐ (2 puan)	Kuruluş Kritik İş Sektörlerinde Faaliyet Gösteriyor* ☐ (3 puan)
Süreç Ve Görevler	Basit , Standart ve Tekrarlayan Süreçler; Kuruluşun Kontrolünde Çalışan Aynı Görevleri Yürüten Çok Sayıda Kişinin Olduğu İş Tipi ☐ (1 puan)	Standart Ama Tekrarlamayan Süreçler ve Çok Sayıda Ürünlerin Veya Hizmetlerin Olduğu İş Tipi ☐ (2 puan)	Karmaşık süreçler, çok sayıda ürünlerin ve hizmetlerin olduğu, çok sayıda iş birimlerinin sertifikasyon kapsamına dahil edildiği iş tipi (BGYS/KVYS son derece karmaşık süreçleri ya da nispeten yüksek derecede veya benzersiz faaliyetleri kapsar) ☐ (3 puan)
Yönetim Sistemi Kuruluş Düzeyi	BGYS/KVYS İyi Kurulmuş ve / veya Diğer Yönetim Sistemleri Mevcut ☐ (1 puan)	Diğer Yönetim Sistemlerinin Tamamı Olmasa da Bazı Gereklilikleri Uygulanmakta ☐ (2 puan)	Başka bir yönetim sistemi uygulanmıyor ve BGYS/KVYS yeni tam performans göstermemiş. ☐ (3 puan)

Not: Kritik iş sektörleri, kritik kamu hizmetlerini etkileyen, sağlığa, güvenliğe, ekonomiye, imaja ve devletin işlev görme yetisine karşı risk oluşturacak şekilde, ülke üzerinde son derece olumsuz bir etkisi olabilen sektörlerdir.

Çizelge D.3 - BT alanıyla ilgili faktörler

Bilgi teknolojileri ile ilgili faktörler			
	Düşük	**Orta**	**Yüksek**
Bilgi Teknolojisi Altyapısının Karmaşıklığı	Düşük Yada Yüksek Standarta Sahip BT Platformları, Sunucular, İşletim Sistemleri, Veri Tabanları, Ağlar, Vs. ☐ (1 Puan)	Birkaç Farklı BT Platformları, Sunucular, İşletim Sistemleri, Veri Tabanları, Ağlar ☐ (2 puan)	Çok Sayıda Farklı BT Platformları, Sunucular, İşletim Sistemleri, Veri Tabanları, Ağlar ☐ (3 puan)
Bulut Hizmetleri Dahil Dış Kaynak Kullanımı ve Tedarikçilere Bağımlılık	Dış kaynaklara ve/veya tedarikçilere bağımlılık yok veya çok az ☐ (1 puan)	Dış Kaynaklara Ve/Veya Tedarikçilere Bağımlık Çok Az ,Var Olan Bu İlişki Önemli İş Aktivitelerinde Değil ☐ (2 puan)	Dış Kaynaklara Ve/Veya Tedarikçilere Yüksek Bağımlılık Var Bu Bağımlılığın Önemli İş Aktivitelerindeki Etkisi Büyük ☐ (3 puan)
Bilgi Sistem Geliştirme	Kurumda Sistem Ve Uygulama Geliştirme Sınırlı Olarak Kurum İçinde Yapılıyor Yada Hiç Yapılmıyor. ☐ (1 puan)	Kurumda Sistem ve Uygulama Geliştirme Sadece Bazı Önemli İş Amaçları İçin Kurum İçinde Veya Dış Kaynaklı Yapılıyor ☐ (2 puan)	Kurumda Sistem Ve Uygulama Geliştirme Geniş Kapsamlı Olarak Önemli İş Amaçları Sebebiyle Kurum İçinde Veya Dış Kaynaklı Yapılıyor ☐ (3 puan)

Çizelge D.4 - Faktörlerin tetkik süresine etkisi

Denetim Süresi Artırma/ Azaltma Matrisi (+100/-30)			**Bilgi Teknolojileri Karmaşıklığı**					
			Düşük		**Orta**		**Yüksek**	
			3	**4**	**5**	**6**	**7**	**9**
İş ve Organizasyon Karmaşıklığı	**Düşük**	**3** **4**	-%30	-%5	-%10	-%5	+%5	+%20
	Orta	**5** **6**	-%10	-%5	%0	%0	+%10	+%50
	Yüksek	**7** **9**	+%5	+%20	+%10	+%50	+%20	+%100

D.3 Tetkik süresi hesaplama örneği

Aşağıdaki örnek, bir CAS'ın tetkik süresini hesaplamak için C.3'te verilen faktörleri nasıl

kullanabileceğini gösterir. Örnekte verilen tetkik süresi hesaplaması aşağıdaki gibi işler:
Adım 1: İş ve organizasyonlar ilişkili faktörlerin tayini (BT dışında): Çizelge D.2'de verilen her bir kategori için uygun dereceler tanımlanır ve sonuçlar toplanır.
Adım 2: BT ortamıyla ilişkili faktörlerin tayini: Çizelge D.3'te verilen her bir kategori için uygun dereceler tanımlanır ve sonuçlar toplanır.
Adım 3: Yukarıdaki 1. ve 2. adımların sonuçlarından yola çıkarak Çizelge D.4'te uygun girdiler seçilerek tetkik süresine etki eden faktörler tanımlanır.
Adım 4: Nihai hesaplama: Tetkik zaman çizelgesi (Çizelge C.1) kullanarak belirlenen gün sayısı, 3. adımdan gelen faktör (katsayı) ile çarpılır. Çoklu konumdan örnekleme yapıldığında, hesaplanan tetkik günü sayısı, çoklu konumdan örnekleme planını gerçekleştirmek için gerekli çabalara bağlı olarak artırılır.
Bu sonuç nihai tetkik günü sayısıdır.

4.1.5 Çoklu Saha Örneklemesi

Müşterinin, çeşitli coğrafi bölgelerde aynı faaliyeti kapsayan yönetim sisteminin denetimi için birden fazla sahada örnekleme yapıldığında, CAS yönetim sisteminin denetiminin uygun şekilde olmasından emin olmak için, Belgelendirme Prosedürü doğrultusunda bir örnekleme programı oluşturur. Örnekleme planının gerekçesi, her bir müşteri için dokümante edilmektedir. Belli bazı belgelendirme programları için örneklemeye izin verilmemekte ve belli bir belgelendirme programı özel kriterler oluşturulmuşsa, bunlar kullanılır.
Çoklu sahalarda, her bir saha için tetkik gün sayısı, ayrı ayrı hesaplanır, kapsam için hesaplanan toplam yerinde denetçi günlerinin sayısı, yönetim sistemi için sahanın uygunluğuna ve belirlenen risklere bağlı olarak farklı sahalar arasında dağıtılır. Dağıtımın gerekçesi, Atama Formu ile kayıt altına alınır.
Not: Çoklu sahalarda hesaplanan denetim adam günü hiçbir zaman tüm saha çalışanlarının toplamına karşılık gelen denetim gününden az olamaz.
ISO/IEC 17021-1:2015, Madde 9.1.5'in gereklilikleri esas alındı.

4.1.5.2 Çoklu Sahalar

Müşterinin aşağıda kriterlere uyan birkaç konumu varsa, CAS çoklu konum belgelendirme tetkiki için örnekleme esaslı kullanır,
a) bütün konumların merkezi yönetime sahip, denetlenen ve merkezi yönetim incelemesine tabi olan aynı
BGYS/KVYS altında çalışması;
b) bütün konumların müşterinin iç BGYS/KVYS tetkik programına dâhil edilmiş olması;
c) bütün konumların müşterinin BGYS/KVYS yönetim gözden geçirme programına dâhil edilmiş olması.
Örnekleme esaslı yaklaşım kullanmayı isteyen CAS aşağıda belirtilenleri sağlamak için gerekli prosedürlere sahiptir.
a) Ön sözleşme gözden geçirmesi, mümkün olan en büyük kapsamda, yeterli bir seviyede örneklemeyi sağlayacak şekilde konumlar arasındaki farklılıkları tanımlar.
b) CAS tarafından aşağıdakiler göz önüne alınarak temsili sayıda konumdan örnekleme yapar:
1) merkezde ve konumlarda yapılan iç tetkiklerin sonuçları;
2) yönetim gözden geçirmesinin sonuçları;
3) konum büyüklüklerindeki değişkenlikler;
4) konumların iş amacındaki farklılıklar;
5) farklı konumlardaki bilgi sistemlerinin karmaşıklığı;
6) çalışma uygulamalarındaki farklılıklar;
7) yapılan faaliyetlerdeki farklılıklar;
8) kontrollerin işleyişi ve tasarımındaki farklılıklar;
9) kritik bilişim sistemleriyle veya hassas bilgi işleyen sistemlerle girilecek olası etkileşim;
10) farklı yasal gereklilikler;
11) coğrafi ve kültürel hususlar;
12) konumların risk durumu;

13) belirli konumlardaki bilgi güvenliği ihlal olayları.

c) Müşterinin BGYS/KVYS kapsamı içinde kalan bütün konumlardan bir temsilî örneklem seçilir, bu seçim yapılırken rastgele unsurların yanı sıra b)'de bahsedilen etkenleri yansıtan yargısal bir seçim yapılması esas alır.

d) BGYS/KVYS'ye dâhil olan ve önemli risklere konu olan her konum, belgelendirme öncesinde CAS tarafından tetkik edilir.

e) Tetkik programı, yukarıdaki gereklilikler ışığında tasarlanmış olup ve üç yıllık dönem içerisindeki BGYS/KVYS belgelendirmesi kapsamına ilişkin temsilî örnekleri kapsar.

f) Uygunsuzluğun tek bir konumda gözlemlendiği durumda, düzeltici eylem prosedürü merkezde ve belgelendirmenin kapsamına giren bütün konumlarda uygular.

Tetkik, tek bir BGYS/KVYS'nin bütün konumlara uygulandığına ve operasyonel düzeyde merkezî yönetime ulaştığından emin olmak için müşterinin merkez faaliyetlerini inceler. Tetkik, yukarıda ana hatlarıyla belirtilen bütün konuları ele alır.

Daha Yüksek Denetim Süresi Faktörleri,

*BGYS/KVYS Kapsamında Birden Fazla Bina veya Lokasyonu İçeren Karmaşık Lojistik

* Birden Fazla Dilde Konuşan Çalışan (Çevirmen İsteyen veya Bireysel Denetçileri Bağımsız Çalışmaktan Engelleyen Çalışan) Veya Birden Fazla Dilde Sunulan Belgeler

*Çok Fazla Düzenlemenin Olması

*BGYS/KVYS Fazla Karmaşık Prosesleri veya Göreceli Olarak Yüksek Sayılı veya Tek Aktiviteleri Kapsıyorsa

*Prosesler Donanım, Yazılım, Proses Ve Servislerin Kombinasyonundan Oluşuyorsa.

*Sertifikasyona Konu Olan Ana Merkezlerin Aktivitelerini Teyit Edecek Geçici Yerleri Ziyaret Etmeyi Gerektiren Aktiviteler (Aşağıdaki Not1'e Bakınız)

Daha Az Denetim Süresi Faktörleri,

*Risksiz Yada Düşük Risk İçeren Ürünler/Prosesler

*Organizasyonun Önceden Bilinmesi (Örneğin, Eğer Organizasyon Aynı Sertifikasyon Kuruluşu Tarafından Başka Bir Standartla Sertifikalandırılmışsa)

*Müşterinin Sertifikasyon İçin Hazır Olması (Örneğin, Sertifikalandırılmış Ya Da Başka Bir Üçüncü Parti Danışmanlığı Tarafından Organize Edilmiş)

*Prosesler Tek Bir Genel Aktivite İçeriyorsa (Yalnızca Hizmet)

*Faaliyetteki Yönetim Sisteminin Olgunluğu

*Yüksek Oranda Kişinin Aynı Basit İşleri Yapıyor Oluşu

Not 1: Sertifikasyon müşterisi ya da sertifikalandırılmış organizasyonun geçici yerlerde hizmet verdiği ya da üretim yaptığı durumlarda bu yerlerin değerlendirmesinin sertifikasyon ve gözetim denetlemesinin içine alındığına emin olunur;

BGYS/KVYS kapsamına yapılan bütün atıflar, prosesler ve ürün/hizmetler değerlendirilmeli ve bu faktörler için adil bir düzeltme yapılarak daha fazla ya da az denetleme süresi etkin bir denetim için dâhil edilir.

Denetimlerde azaltma ve artırma yapılırken yukarıdaki parametreler dikkate alınır. Yapılan eksiltme ve azaltmaların haklı nedenlerini ortaya koymak için delil ve kayıtlar muhafaza edilir.

Çoklu saha denetimleri, aşağıda verilen esaslara ve aşağıda verilen tabloya göre yapılır:

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)
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
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

ISO/IEC 27006-1:2024,Madde 9.1.5.2'nin gereklilikleri esas alındı.

4.1.6 Çoklu Yönetim Sistemleri

CAS tarafından, çoklu yönetim sistem standartlarında belgelendirme sağlandığında, denetim planlaması; belgelendirmenin güvenini sağlamak için yeterli saha denetimlerini garanti etmektedir.

ISO/IEC 17021-1:2015, Madde 9.1.6'nın gereklilikleri esas alındı.

BGYS/KVYS Dokümanlarının Diğer Yönetim Sistemleriyle Birleştirilmesi

CAS, BGYS/KVYS diğer sistemlere uygun ara yüzlerle birlikte açıkça tanımlanabildiği sürece (örneğin, bilgi güvenliği, kalite, sağlık ve güvenlik ve çevre için) birleştirilmiş dokümanları kabul eder.

ISO/IEC 27006-1:2024,Madde 9.1.6.2'nin gereklilikleri esas alındı.

Yönetim Sistemi Tetkiklerinin Birleştirilmesi

BGYS/KVYS tetkiki, diğer tetkikin BGYS/KVYS belgelendirmesi için olan gereklilikleri yerine getireceği garanti altına alındığı için diğer yönetim sistemlerinin tetkikleriyle entegre edilir. BGYS/KVYS için önemli olan bütün unsurlar tetkik raporlarında tanımlanarak kayıt altına alınır. Tetkiklerin entegre edilmesi, tetkikin kalitesini olumsuz yönde etkilemez.

ISO/IEC 27006-1:2024,Madde 9.1.6.3'ün gereklilikleri esas alındı.

4.2 Tetkiklerin Planlaması

4.2.1 Tetkik Hedeflerinin, Kapsamının ve Kriterlerinin Belirlenmesi

Denetimin amaçları, CAS tarafından belirlenmektedir. Denetimin kapsamı ve kriterler, herhangi bir değişiklik dahil, müşteri ile karşılıklı görüşmelerden sonra, CAS tarafından oluşturulmaktadır.

Denetim amaçları, yapılacak olan denetimin ne olduğunu tarif etmekte ve aşağıdakileri içerir:

1. Denetim kriterleri kullanılarak, müşterinin yönetim sisteminin veya bir bölümünün uygunluğunun tayini,
2. Yönetim sisteminin yeteneği ile müşterinin uygulanabilir, yasal düzenleyici ve sözleşme şartlarını karşıladığından emin olunmasının tayini,
3. Müşterinin, belirlenen amaçlara ulaşılabileceği beklentisini güvence altına almak için yönetim sisteminin etkinliğinin tayini,
4. Uygun olması durumunda, yönetim sisteminin potansiyel iyileştirme alanlarının tanımı.

Denetimin kapsamı, denetimin sınırlarını (örneğin, denetlenecek; sahalar, yönetim birimleri, faaliyetler ve prosesleri gibi) tanımlamaktadır. İlk veya yeniden belgelendirme prosesi birden fazla denetimden (örneğin, farklı sahaları kapsıyorsa) oluşuyorsa, her bir denetimin kapsamı tüm belgelendirme kapsamını içermeyebilir ancak bütün denetimlerin toplamı belgelendirme dokümanındaki kapsamla uyumlu olması sağlanır.

Denetim kriteri, uygunluğun neye göre tayin edildiğinin referansı olarak kullanılmakta ve aşağıdakileri kapsar:

1. Yönetim sistemleri ile ilgili tanımlanan zorunlu hüküm dokümanının şartları,
2. Müşteri tarafından geliştirilen yönetim sisteminin tanımlanmış prosesleri ve dokümantasyonu.

Tetkik hedefleri, kapsamı ve kriterleri belirlenerek denetim planı, Plan Formu ile kayıt altına alınmakta ve müşteri kuruluş yönetim Temsilcisi ile Baş Denetçi tarafından imzalanarak onaylanmaktadır.

ISO/IEC 17021-1:2015, Madde 9.2.1'in gereklilikleri esas alındı.

Tetkik Hedefleri

Tetkik hedefleri aşağıdaki hususları içerir:

a) yönetim sisteminin etkinliğinin belirlenmesi,

b) müşterinin risk değerlendirmesine dayalı olarak gerekli kontrolleri belirlemesi, ve

c) belirlenmiş bilgi güvenliği hedeflerine ulaşıldığının belirlenmesi.
Tetkik hedefleri, Plan Formu ile kayıt altına alınmakta ve müşteri kuruluş yönetim Temsilcisi ile Baş Denetçi tarafından imzalanarak onaylanmaktadır.
ISO/IEC 27006-1:2024,Madde 9.2.1.2'nin gereklilikleri esas alındı.

Tetkik Kriterleri

Bir müşterinin BGYS/KVYS'nin denetlenmesi için kriterler arasında ISO/IEC 27001 yer alır.
Tetkik kriterleri, Plan Formu ile kayıt altına alınmakta ve müşteri kuruluş yönetim Temsilcisi ile Baş Denetçi tarafından imzalanarak onaylanmaktadır.
ISO/IEC 27006-1:2024,Madde 9.2.1.3'ün gereklilikleri esas alındı.

4.2.2 Denetim Ekibinin Seçimi ve Atanması

CAS, denetim ekibinin seçimi ve atanması amacıyla Personel Atama ve Performans Değerlendirme Prosedürü oluşturmuş ve uygulamaktadır. Bu prosedür, denetimin amaçlarına ulaşmak ve tarafsızlık şartlarını karşılamak için yeterliliği dikkate alarak, denetim ekibi lideri ve gerektiğinde teknik uzmanları içerir. Tek bir denetçi varsa, ilgili denetim için denetim ekip liderinin görevlerini yerine getirebilecek yeterliliğe sahip olması ve denetim için denetim ekibinin, CAS tarafından belirlenen yeterliliklerin hepsine sahip olması sağlanır.
Denetim ekibinin büyüklüğüne ve yapısına karar verilirken aşağıdakiler dikkate alınır;

- Denetimin amaçları, kapsamı, kriteri ve tahmini denetim zamanı,
- Denetimin kombine, ortak veya entegre olduğu,
- Denetimin amaçlarına ulaşmak için gerekli denetim ekibinin yeterliliği,
- Belgelendirme şartları (uygulanabilir yasal, düzenleyici veya sözleşme şartları dahil),
- Dil ve kültür.
- Denetim ekibi liderinin ve denetçilerin gerekli bilgi ve yetenekleri, bir denetçinin talimatı altında çalışan, teknik uzman ve tercümanlar ile desteklenir. Tercüman kullanılması durumunda, tercümanlar denetimi olumsuz etkilemeyecek şekilde seçilir.
- Eğitim almakta olan denetçiler, denetçilerden birinin değerlendirici olarak belirlenmesi şartıyla denetime katılabilir.
- Değerlendiricinin, sorumluluklarını yerine getirebilecek şekilde yeterli olması sağlanır. Değerlendirici, aynı zamanda, eğitimdeki denetçinin faaliyetleri ve bulguları ile ilgili son sorumluluğa sahiptir.

Denetim ekibi lideri, denetim ekibi ile istişare ile her bir ekip üyesine denetim esnasında, belirli proseslerin, bölgelerin ve faaliyetlerin denetimi sorumluluğunu verir. Bu görevlendirme yapılırken, denetçiler, eğitimdeki denetçiler ve teknik uzmanların değişik görev ve sorumlulukları da dikkate alınarak, yeterlilik ile denetim ekibinin etkin ve verimli kullanım ihtiyaçları dikkate alınır. Denetim amaçlarına ulaşmayı garanti altına almak için sorumluluk alanlarında değişiklik yapılabilir.

Gözlemciler, Teknik Uzmanlar ve Rehberler

Gözlemciler

Bir denetim faaliyeti esnasında, gözlemcilerin varlığı ve doğrulanması, denetimin gerçekleşmesinden önce CAS ile müşteri arasında anlaşmayla olur. Denetim ekibi, gözlemcinin denetim prosesinde olumsuz etki etmesine veya karışmasına yada denetim sonucunu etkilemesine izin verilmediğini güvence altına alır.
Not Gözlemciler, müşteri kuruluşun mensubu, danışmanlar, tanıklık yapan akreditasyon kuruluşu personeli, düzenleyiciler veya diğer doğrulanan personel olabilir.

Teknik Uzmanlar

Denetim esnasında teknik uzmanın rolü, denetimin gerçekleşmesinden önce CAS ile müşteri arasında anlaşmayla olur. Teknik uzman denetim ekibinde denetçi gibi davranmamakta. Teknik uzmanlara bir denetçi refakat eder.

Rehberler

Denetim ekibi lideri ile müşteri aksi bir şekilde anlaşmadıkça, her bir denetçiye bir rehber eşlik eder. Rehber/rehberler, denetimi kolaylaştırmak için denetim ekibine atanır. Denetim ekibi, rehberlerin denetim prosesinde olumsuz etki etmesine veya karışmasına yada denetim sonucunu etkilemesine izin vermez

ISO/IEC 17021-1:2015, Madde 9.2.2'nin gereklilikleri esas alındı.

4.2.3 Denetim Planı

CAS, denetim faaliyetlerinin yapılması ve programlanması ile ilgili anlaşmanın temelini sağlamak amacıyla, her bir denetim programında yer aldığı şekilde her denetimden önce Denetim Planı oluşturur.

Denetim Planının Hazırlanması

Denetim planı, denetim amaç ve hedeflerine uygun olarak oluşturulmakta ve en azından aşağıdakileri kapsar veya atıfta bulunur:

- Denetim amaçları,
- Denetim kriterleri,
- Denetime tâbi tutulacak kurumsal ve fonksiyonel birimler ve proseslerin tanımı dahil denetim kapsamı,
- Sahadaki denetim faaliyetlerinin gerçekleştirileceği tarihler ve sahalar (uygun olduğu takdirde, farklı sahalar ve uzaktaki denetim faaliyetleri dahil),
- Sahadaki denetim faaliyetlerinin beklenen süresi,
- Denetim ekibi üyelerinin ve eşlik eden personelin (örneğin, gözlemciler ve tercümanlar) görev ve sorumlulukları.

Denetim Planı denetim öncesinde her denetim için Denetim Ekip Lideri (Baş Denetçi) tarafından hazırlanarak onaylanır.

Denetim Ekibinin Görev İletişimi

Uygunluğu sağlayabilecek denetim ekibi görevlilerinin dosyaları incelenerek uygun olan denetim ekibi kombinasyonu Planlama sorumlusu ve ilgili alanda yetkin olan denetçi ya da teknik uzmanlar tarafından belgelendirme müdürü bilgisi dâhilinde belirlenir.

Ayrıca, belirlenen denetim ekibinin doğrulanması amacıyla, Atama Formu ile, denetim ekibi üyelerinden; belirlenen belgelendirme kapsamı, firma kodu, denetim süresi, denetim ekibi uygunluğu konusunda teyit alınır.

Bu teyit alındıktan sonra firmaya denetim ile ilgili bilgilendirme yapılır. Bu bilgilendirme ilk aşama.1 ve aşama.2, gözetim ve yeniden belgelendirmeler için ayrı ayrı yapılır.

Planlama tarafından Belirlenen denetim ekibine (Baş denetçi, denetçi, teknik uzman vs.) Atama Formu yazısı görevlendirme yapılır.

Görev bildirimine 3 iş gün içinde teyit alınmaz ise planlama, belgelendirme müdürüne durumu bildirir yeni Denetim ekibini belirlenir. Yeniden belirlenen denetim ekibi için planlama sorumlusu, görev bildirimlerinde bulunarak ekibin teyidini alınır.

Aşama1 ve Aşama.2 denetimi için tarih ve denetim ekibi belirlenerek, teyit edilmesi amacıyla, denetimden önce, Atama Formu ile ilgili kuruluşa bildirilir.

Denetim ekibine verilen görevler, BGYS/KVYS Belgelendirme Prosedürü doğrultusunda açık bir şekilde tanımlanmakta ve denetim ekibinin aşağıdaki hususları yerine getirmesi öngörülmektedir:

- Müşteri kuruluşun yönetim sistemi ile ilgili yapısının, politikalarının, proseslerinin, prosedürlerinin, kayıtlarının ve ilgili dokümanlarının incelenmesini,
- Bunların amaçlanan belgelendirme kapsamının bütün şartlarını karşıladığının belirlenmesini,
- Müşteri kuruluşun yönetim sistemine güven duyulmasına bir temel sağlamak üzere, prosesler ve prosedürlerin oluşturulduğunun, etkin bir şekilde uygulandığının ve sürdürüldüğünün belirlenmesini,
- Faaliyetlerin ve müşterinin politika, hedef ve amaçları ile sonuçlar arasındaki tutarsızlıkların müşteriye bildirilmesini.

Denetim Planının İletişimi

Denetim Planı, BGYS/KVYS Belgelendirme Prosedürü doğrultusunda, müşteri kuruluşa Planlama Bölümü tarafından iletilmekte ve denetim tarihleri üzerinde müşteri kuruluşla önceden anlaşmaya varılarak onaylatır.

Denetim Ekibi Üyeleri İle İlgili İletişim

CAS, BGYS/KVYS Belgelendirme Prosedürü doğrultusunda, denetim ekibinin her bir üyesinin

adını ve talep edilmesi halinde geçmiş bilgilerini müşteri kuruluşa bildirmektedir.
Bu bildirim, müşteri kuruluşun belirli bir denetçi veya teknik uzmanın atanmasına itiraz etmesine ve CAS'ın geçerli itiraza cevaben ekibi yeniden oluşturmasına yeterli süre verecek şekilde yapılır.
ISO/IEC 17021-1:2015, Madde 9.2.3'ün gereklilikleri esas alındı.

Genel Hususlar

BGYS/KVYS tetkikleri için olan tetkik planı, belirlenen bilgi güvenliği kontrollerini dikkate alınır.
NOT Bir CAS'ın, tetkik yapılan kuruluşla tetkik zamanlaması konusunda anlaşması, kuruluşun tüm kapsamını en iyi şekilde ortaya koymak için iyi bir uygulamadır. Mevsim, ay, gün/tarih ve vardiya gibi hususular uygun şekilde dikkate alınır.
ISO/IEC 27006-1:2024,Madde 9.2.3.2'nin gereklilikleri esas alındı.

Uzaktan tetkik teknikleri

Uzaktan tetkik tekniklerinin amacının, tetkik etkinliğini ve verimliliğini arttırması ve tetkik sürecinin bütünlüğünü destekleyecek şekilde olur.
Tetkik planı, uzaktan tetkike yardımcı olmak için kullanılan araçlara atıfta bulunur.
ISO/IEC 27006-1:2024,Madde 9.2.3.3'ün gereklilikleri esas alındı.

Uzaktan Tetkik Yöntemleri

Eğer, interaktif ağ tabanlı işbirliği, ağ toplantıları, tele-konferanslar ve/veya kuruluşun süreçlerinin elektronik doğrulaması gibi uzaktan tetkik teknikleri kuruluş ile iletişim kurulması için kullanılırsa, bu faaliyetlerin tetkik planında gösterilir ve toplam "saha tetkik süresi"ne kısmi olarak katılımı değerlendirilir.
NOT Saha tetkik süresi, ayrı konumlara tahsis edilen tetkik süresini ifade eder. Uzak konumlara yapılan elektronik tetkikler, fiziksel olarak kuruluşun kendi konumlarında yapılıyor olsa bile uzaktan tetkik olarak kabul edilir.
ISO/IEC 27006-1:2024,C.1.1'in gereklilikleri esas alındı.

4.3 İlk Belgelendirme

4.3.1 Genel

Yönetim sisteminin ilk belgelendirme denetimi Aşama.1 ve Aşama.2 olmak üzere, iki aşamada yapılır.

Aşama.1

CAS Aşama.1'in planlanmasını gerçekleştirirken, Aşama.1'in amaçlarına ulaşılabileceğini ve müşterinin bu aşama esnasında "sahada" yürütülecek faaliyetle ilgili bilgilendirileceğini güvence altına alır.
Not Aşama.1 resmi bir denetim planı IAF MD5 ve IAF MD1'de gereklilik olarak belirtilen aşağıdaki unsurlar sebebiyle CAS tarafından oluşturulup müşterilere iletilir.

- Aşama 1 için gereken denetim süresinin belirlenmesi
- Denetim ekibinin atanması
- Denetimin amacı
- Denetimin kapsamı
- Denetimin gerçekleşeceği lokasyon(lar)

Aşama.1 denetiminin amacı aşağıdakileri hususları gerçekleştirmektir:

- Müşterinin yönetim sisteminde dokümante edilmiş bilgiyi gözden geçirmek,
- Müşteri mahallini ve sahaya özgü koşulları değerlendirmek ve Aşama.2 denetimine hazırlığın belirlenmesindeki müşterinin personeli ile müzakereleri yapmak,
- Müşterinin statüsünün gözden geçirilmesi ve özellikle temel performansın veya önemli hususların, proseslerin, hedeflerin ve yönetim sisteminin çalışmasının tanımlanmasıyla ilgili standard şartlarını anlamak,

Aşağıdakiler dahil yönetim sisteminin kapsamı ile ilgili gerekli bilgileri elde etmek:

- Müşterinin sahası/sahaları,
- Prosesler ve kullanılan teçhizat,
- Oluşturulan kontrol seviyeleri (özellikle birden fazla sahası olan müşterilerde),
- Uygulanabilir durumsal ve düzenleyici şartlar,

- ❖ Aşama.2 denetimine yönelik kaynak tahsisinin gözden geçirmek ve Aşama.2 denetiminin ayrıntıları üzerinde müşteri ile anlaşmaya varmak,
- ❖ Yönetim sistemi standardının veya diğer hüküm ihtiva eden dokümanlar bağlamında, müşterinin yönetim sisteminin ve saha operasyonlarının yeterli bir şekilde anlaşılmasının sağlanmasıyla, Aşama.2 denetiminin planlanmasına odaklanmak,
- ❖ İç denetimlerin ve yönetimin gözden geçirmesinin planlanıp planlanmadığı ve gerçekleştirilip gerçekleştirilmediğinin değerlendirilmesi ve uygulanan yönetim sisteminin uygulama seviyesi ile müşterinin Aşama.2 denetimi için hazır olup olmadığını değerlendirmek.

Aşama.1'in amaçlarının karşılanması ve Aşama.2 için hazırlıkla ilgili dokümante edilmiş sonuçlar (Aşama.2 denetimi esnasında uygunsuzluk olarak sınıflandırılabilecek) Denetim Prosedürü doğrultusunda müşteriye bildirilir.
Aşama.1 ve Aşama.2 denetimleri arasındaki aralığın belirlenmesinde, Aşama.1 denetimi esnasında belirlenen hususların çözüme kavuşturulmasına yönelik müşterinin ihtiyaç duyacağı zaman dikkate alınır.
Aşama.1 denetiminde uygunsuzluk tespit edilmiş ise uygunsuzluk kapatıldıktan Aşama.2 denetimi planlanarak gerçekleştirir.
Aşama.1 ve Aşama.2 denetimleri arasındaki süre 6 aydan fazla olamaz. Daha uzun sürelerde, Aşama.1 denetimi tekrar yapılır.
Ancak uygunsuzluk yok ise asgari bir süre için planlanarak gerçekleştirir. CAS Aşama.1 ve Aşama.2 denetimleri arasındaki süre asgari olarak 1 haftadır. Planlama bölümü denetim planlama aşamasında bu sürelere uyarak denetimleri planlar.
CAS Aşama.2 için düzenlemelerini revize etme ihtiyacı da duyabilir. Yönetim sistemini etkileyecek önemli değişiklikler olursa, CAS tamamının veya Aşama.1'in bir kısmının tekrarını talep edebilmektedir. Müşteri, Aşama.1 'in sonuçlarının Aşama.2'yi ertelemeye veya iptal etmeye yol açabileceği konusunda bilgilendirir.
Aşama.2 denetimine geçmeden önce, aşama.1 denetim raporunu gözden geçirilir ve aşama.2 denetim ekibi üyelerinin gerekli yeterliliğe sahip olup olmadığını teyit edilir; bu karar, yetkin ve uygun görülmesi halinde aşama.1 denetimini yürüten ekibe liderlik eden denetçi tarafından yapılabilir.
Not: Bu kararın, Bağımsız gözden geçirme yani denetimde yer almayan, CAS'tan bir kişi tarafından verilmesi, Aşama.2 'ye geçilip geçilmeyeceğine ve kiminle devam edileceğine karar verilirken ortaya çıkan risklerin azaltılmasına yönelik bir önlemdir. Bu kontroller Aşama.1 denetiminde aktif görev alan baş denetçi tarafından da yapılabilir.

Aşama.2

Aşama.2 denetiminin amacı, müşterinin yönetim sisteminin etkinliği dâhil, uygulamayı değerlendirir. Aşama.2 denetimi, müşterinin bütün sahasında/sahalarında yapılmaktadır. Aşama.2 denetimi en azından aşağıdaki hususları içerir:

- ❖ Uygulanabilir yönetim sistem standardı veya diğer hüküm ifade eden dokümanların şartlarına uygunluk hakkındaki bilgi ve kanıt,
- ❖ Temel performans hedefleri ve amaçlarına yönelik (uygulanabilir yönetim sistem standardı veya diğer hüküm ifade eden dokümanlardaki beklentilerle tutarlı) performansın izlenmesi, ölçülmesi, kayıt altına alınması ve gözden geçirilmesi,
- ❖ Müşterinin yönetim sistemi kabiliyeti ve uygulanabilir statüsel, düzenleyici ve yapısal şartların karşılanması ile ilgili performansı,
- ❖ Müşteri proseslerinin operasyonel kontrolü,
- ❖ İç denetim ve yönetimin gözden geçirmesi,
- ❖ Müşteri politikaları için yönetimin sorumluluğu.

İlk Belgelendirme Denetim Sonuçları

Denetim ekibi, Aşama.1 ve Aşama.2 denetimleri esnasında toplanan bütün bilgileri ve denetim kanıtlarını, denetim bulgularını gözden geçirmek ve denetim sonuçları üzerinde uzlaşmak için analiz etmektedir.

ISO/IEC 17021-1:2015, Madde 9.3'ün gereklilikleri esas alındı.

Aşama 1

Tetkikin bu aşamasında CAS ISO/IEC 27001'de gerekli gösterilen dokümanları kapsayacak şekilde BGYS/KVYS'nin tasarım dokümanlarını temin eder.

Müşteri, belgelendirme tetkikinin 1. aşamasında en azından aşağıdaki bilgileri verir:

a) BGYS/KVYS ve kapsadığı faaliyetler hakkında genel bilgi,

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

CAS; müşterisinin, organizasyonu, riski değerlendirme ve iyileştirme şekilleri (belirlenmiş kontrolleri içerecek şekilde), bilgi güvenliği politika ve hedefleri, özelde tetkik için hazır olma durumu açısından BGYS/KVYS'nin tasarımını yeterli şekilde anlar. Bu bilgi, Aşama.2 tetkikin planlanmasında kullanılır.

Aşama.1'in sonuçları yazılı bir rapor haline getirilir. CAS, Aşama.2'ye geçmeye karar vermeden önce Aşama.1'in tetkik raporunu inceler. CAS, Aşama.2 tetkik ekibi üyelerinin gerekli yetkinliğe sahip olduğunu teyit eder. Bu genelde, yeterli ve uygun görülmesi halinde Aşama.1 tetkikini gerçekleştiren ekibe liderlik eden denetçi tarafından yapılır.

CAS Aşama 2'de detaylı inceleme için gerekebilecek diğer bilgi ve kayıtlar hakkında müşteriyi bilgilendirir.

Aşama 2

CAS Aşama.1 tetkik raporundaki bulgulardan yola çıkarak Aşama.2'de uygulanacak tetkik için Denetim Planı Denetim Ekip Lideri tarafından hazırlanır. BGYS/KVYS'nin etkin uygulanmasına ilişkin değerlendirmeye ek olarak, Aşama.2'nin amacı müşterinin kendi politikalarına, hedeflerine ve yöntemlerine uyduğunu doğrular.

Bunu yapabilmek için tetkikin odağı, müşterinin:

a) bilgi güvenliği hedefleri için üst yönetimin liderliği ve bağlılığı;

b) bilgi güvenliği ile alakalı risklerin değerlendirilmesi; tetkik ayrıca, değerlendirmelerin tekrarlandığında tutarlı, doğru ve karşılaştırılabilir sonuçlar vermesinin sağlanması;

c) bilgi güvenliği risk değerlendirmesi ve risk iyileştirme süreçlerine dayalı olarak kontrollerin belirlenmesi;

d) bilgi güvenliği performansının ve BGYS/KVYS'nin etkinliğinin bilgi güvenliği hedeflerine göre değerlendirilmesi;

e) tanımlanmış kontroller arasındaki uyum, Uygulanabilirlik Beyanı ile bilgi güvenliği risk değerlendirmesi ve risk iyileştirme süreçlerinin sonuçları ve bilgi güvenliği politikaları ve hedefleri arasındaki uyumun belirlenmesi;

f) kontrol uygulamaları (tetkik kontrollerine ilişkin örnekler için Ek E'ye bakılmalıdır), iç ve dış bağlam ve ilişkili riskler, organizasyonun bilgi güvenliği süreçleri ve kontrollerinin izlenmesi, ölçümü ve analizini dikkate alarak, uygulandığı beyan edilen kontrollerin uygulanıp uygulanmadığının ve bir bütün olarak etkili olup olmadığının belirlenmesi;

g) üst yönetim kararları ile bilgi güvenlik politika ve hedeflerine uygunlukları için BGYS/KVYS programlarının, süreçlerinin, yöntemlerinin, kayıtlarının ve iç tetkiklerinin yeniden incelenmesini içerir.

ISO/IEC 27006-1:2024,Madde 9.3.2'nin gereklilikleri esas alındı.

4.4 Tetkiklerin Yapılması

4.4.1 Genel

CAS saha denetimlerinin gerçekleştirilmesi için Denetim Prosedürü oluşturmuş ve uygulamaktadır. Bu prosedür, denetimin başlangıcında bir açılış toplantısı, denetimin bitiminde de bir kapanış toplantısını içermektedir.

Denetimin bir parçasının elektronik ortamda gerçekleşmesi veya denetlenecek sahanın sanal olması durumunda, CAS bu tip faaliyetlerin yeterli personel tarafından yapıldığını güvence altına almaktadır. Böyle bir denetim esnasında elde edilen kanıt, söz konusu şartın karşılandığı konusunda denetçinin bilgiye dayalı karar vermesini sağlamaktadır.

4.4.2 Açılış Toplantısının Gerçekleştirilmesi

Resmi açılış toplantısı, müşterinin üst yönetimi ve denetlenecek fonksiyon ve proseslerin sorumlu uygun personeli ile gerçekleştirilir. Açılış toplantısının amacı, denetim faaliyetlerinin nasıl gerçekleştirileceğine dair kısa bir açıklamanın sağlanması olup genellikle denetim ekibi lideri tarafından yürütülür. Açılış toplantısında aşağıdakiler dikkate alınır ve Katılım Formu bu bilgileri içerir:

- Katılımcıların görevleri dahil tanıtımı,
- Belgelendirme Kapsamı (Hariç tutulan madde teyidi) ve Çalışan Sayısı Teyidi,
- Denetim planının teyit edilmesi (denetimin tipi ve kapsamı, amaçlar ve kriterler dahil), herhangi bir değişiklik ve kapanış toplantısının tarih ve zamanı, denetim ekibi ve müşterinin yönetim otoritesi arasındaki ara görüşmeler gibi müşteri ile ilgili diğer düzenlemeler,
- Denetim ekibi ve müşteri arasındaki resmi iletişim kanallarının teyit edilmesi,
- Denetim ekibi tarafından ihtiyaç duyulan kaynakların ve tesislerin mevcut olduğunun teyit edilmesi
- Gizlilik ile ilgili konuların onaylanması,
- Denetim ekibi ile ilgili iş güvenliği, acil durum ve güvenlik prosedürlerinin teyit edilmesi,
- Her bir rehber ve gözlemcinin durumu, görevi ve kimliklerinin teyit edilmesi,
- Denetim bulgularının herhangi bir sınıflaması dahil olmak üzere raporlama yöntemi,
- Denetimin zamanından önce sona erdirme koşulları hakkında bilgi verilmesi,
- CAS'yi temsil eden denetim ekibi ve denetim ekibi liderinin onayı ve denetim planı, denetim faaliyetleri ve denetim yolları da dahil olmak üzere denetimin yürütülmesi ve kontrolü,
- Uygun olan önceki gözden geçirme veya denetim bulgularının durumunun onaylanması,
- Örneklemeye dayalı denetim yapılması için kullanılacak prosedürler ve yöntemler,
- Denetim sırasında kullanılacak olan dilin onaylanması,
- Denetim sırasında, müşterinin denetimin ilerlemesi ve herhangi bir durumdan haberdar edileceğinin teyit edilmesi,
- Önceki Gözetim veya Diğer Denetim Bulgularının Onaylanması
- Müşteriye soru sorması için fırsat verilmesi.

Resmi bir açılış toplantısında, katılımcılar Katılım Formu ile kaydedilir ve imzalanır.

4.4.3 Denetim Esnasında İletişim

Denetim sırasında, denetim ekibi, denetimin oluşturulan plana göre ilerlemesini güvence altına almak amacı ile bilgi alış verişinde bulunur. Denetim ekip lideri, denetimin oluşturulan plandan sapması ve müşterinin herhangi bir endişesi ve/veya talebi durumunda, iletişim kurarak denetim ekibi üyelerinin arasındaki görev dağılımını yeniden düzenler.

Ulaşılamayan denetim hedefleri ya da acil ve önemli bir risk (örneğin, güvenlik) varlığını gösteren mevcut denetim kanıtlarının ortaya çıkması durumunda, denetim ekibi lideri uygun eylemi belirlemek için müşteriye ve mümkünse, CAS' a rapor eder. Bu tür eylemler, denetim hedeflerinin ya da denetim kapsamının değiştirilmesi ya da feshedilmesi, denetim planının değiştirilmesi veya yeniden teyit edilmesini içerir. Denetim ekibi lideri, alınan eylem sonucunu CAS' a rapor eder.

Denetim ekibi lideri, sahada yapılan denetim faaliyetlerinin ilerlemesinde ortaya çıkan denetim kapsamına yönelik herhangi bir değişikliği müşteri ile gözden geçirmekte ve bunu CAS' a rapor eder.

4.4.4 Bilginin Elde Edilmesi ve Doğrulanması

Denetim sırasında, denetim hedefleri, kapsamı ve kriterleri ile ilgili bilgiler (fonksiyonlar, faaliyetler ve prosesler arasındaki arabirimler ile ilgili bilgiler dahil) uygun örnekleme ile elde edilmekte ve denetim kanıtı olması için doğrulanır.

Bilgi toplama yöntemi aşağıdakileri içermektedir ancak bunlarla sınırlı değildir:

- Görüşmeler,
- Proses ve faaliyetlerin gözlemleri,
- Dokümantasyon ve kayıtların gözden geçirilmesi.

4.4.5 Denetim Bulgularının Belirlenmesi ve Kaydedilmesi

Uygunluğu özetleyen ve uygunsuzluğu detaylandıran denetim bulguları, bilinçli bir belgelendirme kararı alabilmek ya da sürdürülebilir belgelendirmeyi sağlayabilmek için raporlanmakta ve

kaydedilmektedir. Kayıtlar Düzeltici Faaliyet Formu ile yapılır.
İyileştirme fırsatları ve gözlemler, uygun durumlarda tanımlanır ve kaydedilir. Uygunsuzluk şeklinde tespit edilen denetim bulguları, minör veya majör olarak sınıflandırılıp Düzeltici Faaliyet Formuna kaydedilir.
Belirli bir şarta göre tespit edilen uygunsuzluk bulgusu kaydedilmekte ve uygunsuzluğun esas aldığı objektif kanıtı detaylı bir şekilde tanımlayan açık bir uygunsuzluk ifadesi içerir.
Uygunsuzluklar; uygunsuzlukların anlaşılmasını, kanıtın kesin ve doğru olmasını temin etmek için müşteri ile görüşülür. Ancak denetçi, uygunsuzlukların nedenini veya bunların çözümünü önermekten kaçınır.
Denetim ekibi lideri, denetim kanıtı veya bulguları ile ilgili müşteri ve denetim ekibi arasında farklılaşan görüşleri çözme girişiminde bulunmakta ve çözümlenmemiş hususları kayıt altına alır.

4.4.6 Denetim Sonuçlarının Hazırlanması

Denetim ekibi liderinin sorumluluğu altında, kapanış toplantısı öncesinde, denetim ekibi:

- Denetim hedefleri ve kriterlerine karşı, denetim sırasında toplanan denetim bulgularını ve diğer uygun bilgileri gözden geçirmeli ve uygunsuzlukları belirlemeli,
- Denetim prosesinin doğasında var olan belirsizliği göz önüne alarak, denetim sonuçları üzerinde mutabık kalmalı,
- Gerekli her türlü takip faaliyetlerinde anlaşılmalı,
- Denetim programının uygunluğunu onaylamalı veya gelecekteki denetimlerle ilgili istenen herhangi bir değişikliği (örneğin, belgelendirmenin kapsamı, denetim süresi veya tarihi, gözetim sıklığı, denetim ekibinin yeterliliği) tanımlamalıdır.

4.4.7 Kapanış Toplantısının Yapılması

Resmi bir kapanış toplantısında, katılımcılar Katılım Formu ile kaydedilir ve imzalanır. Toplantı, müşterinin yönetim otoritesi ve denetlenen prosesler veya fonksiyonlardan sorumlu uygun personelin katılımı ile gerçekleştirilir. Normal olarak denetim ekibi lideri tarafından yürütülen, kapanış toplantısının amacı, belgelendirme ile ilgili tavsiyeleri içeren denetim sonuçlarının sunulmasıdır. Her bir uygunsuzluk anlaşılır bir şekilde sunulmakta ve bunlara yanıt vermeleri için süre verilir.
Kapanış toplantısı aşağıdaki unsurları da içerir:

- Müşteriye, elde edilen kanıtın örnekleme bilgisine dayanarak elde edildiğinin ifade edilmesi ve böylelikle belirsizliğin ifadesi,
- Belgelendirme Kapsamının Teyidi
- Denetim bulgularının herhangi bir sınıflandırması da dahil, raporlama yöntemi ve süresi,
- Müşterinin belgelendirilme durumu ile ilgili herhangi bir sonuç da dahil, CAS' nin uygunsuzlukları ele alma prosesi,
- Denetim sırasında tespit edilen herhangi bir uygunsuzluğu düzeltme ve düzeltici faaliyeti yapmak için bir plan hazırlaması için müşteriye verilen süre,
- CAS' nin denetim sonrası faaliyetleri,
- Şikâyetlerin ele alınması ve itiraz prosesleri hakkında bilgiler.
- Logo Kullanım Kuralları (ürün, ambalaj, vb. belge sahibi olma ifadesi. Promosyon, marka kullanımının Talimat.01 Logo ve Sertifika Kullanım Talimatına uyumu)
- Sorular

Müşteriye soru sorma fırsatı verilir. Denetim ekibi ve müşteri arasında denetim bulguları veya sonuçları ile ilgili farklı görüşler tartışılmakta ve mümkünse bir karara bağlanır. Çözümlenmeyen farklı görüşler kayıt altına alınmakta ve CAS'a bildirilir.

4.4.8 Denetim Raporu

Denetim ekibi tarafından hazırlanan denetim raporu ve ekleri aşağıdakilerden oluşmaktadır:
Aşama.1 Denetim Raporu
Aşama.2 Denetim raporu
Eki Açılış ve kapanış toplantı formu
Eki Uygunsuzluk Düzeltici faaliyet formu
Eki Denetim Planı

Atama Formu
Denetim Ekibinin hazırladığı rapor son karar olmayıp Belgelendirme Karar Komitesine görüş niteliğindedir.
Denetim sonrasındaki on beş gün içerisinde, denetim raporları CAS tarafından kuruluşlara iletilir.
Denetim raporlarında iyileşme fırsatlarından bahsedilmelidir fakat çözüm önerilerinde spesifik çözüm önerilerinde bulunulmamaktadır. Denetim raporunun sahibi CAS' tır.
Nihai denetim raporunu Baş denetçi tarafından yazılır. Denetim ekibi tarafından, baş denetçiye denetim bulgularını içeren denetim raporları iletilir. Baş denetçi tüm denetim ekibi bulgularını içeren nihai denetim raporunu hazırlar.
Denetim ekibi lideri, denetim raporunun hazırlanmasını güvence altın alır ve içeriğinden sorumludur. Denetim Raporu, bildirilecek belgelendirme kararına imkân verebilecek denetimin doğru, özlü ve net olmasını sağlamakta ve aşağıdakileri içermekte veya atıf yapmaktadır:

- CAS' nin tanımı,
- Müşteri ve müşteri yönetim temsilcisinin adı ve adresi,
- Denetimin tipi (örneğin başlangıç, gözetim veya yeniden belgelendirme denetimi ya da özel denetimler),
- Denetim kriterleri,
- Denetimin amaçları,
- Denetimin kapsamı, özellikle denetlenen kuruluşun organizasyon yapısı veya fonksiyonel birimlerin ya da proseslerin tanımlanması ve denetimin zamanı,
- Denetim planından herhangi bir sapma ve nedenleri,
- Denetim programını etkileyen önemli durumlar,
- Denetim ekibi lideri, denetim ekibi üyeleri ve beraberindeki kişilerin tanıtımı,
- Denetim faaliyetlerinin yapıldığı (saha veya saha dışı, kalıcı ve geçici mekanlar) yerler ve tarihleri,
- Denetim tipinin şartları ile tutarlı, kanıt ve sonuçlara referans veren denetim bulguları,
- Varsa, en son denetimden beri meydana gelen müşterinin yönetim sistemini etkileyen önemli değişiklikler,
- Tanımlanmışsa, çözümlenmemiş hususlar,
- Denetimin uygun olduğu takdirde, kombine, ortak veya entegre olması,
- Denetimin mevcut bilgilerin örneklemesi prosesi esas alınarak gerçekleştiğine dair ifade,
- Denetim ekibinin tavsiyesi,
- Denetlenen müşterinin uygun şekilde, belgelendirme dokümanları ve markalarının kullanımının kontrolü,
- Daha önceden belirlenen uygunsuzluklarla ilgili uygulanabilir düzeltici faaliyetlerin etkinliğinin doğrulanması.
- İklim değişikliği hususları

Rapor aşağıdakileri de kapsar:
Aşağıdakilerle ilgili kanıtların bir özeti ile birlikte, yönetim sisteminin uygunluğu ve etkinliği ile ilgili ifade:

- Yönetim sisteminin uygulanabilir şartlar ve beklenen çıktıları karşılama yeteneği,
- İç denetim ve yönetimin gözden geçirmesi prosesi,
- Belgelendirme kapsamının uygunluğu ile ilgili bir sonuç, BGYS/KVYS/ KVYS kapsamı
- Denetim amaçlarının karşılandığının teyidi.
- BGYS/KVYS İklim Değişikliği Hususlarının Etkisi

Organizasyonu ve bağlamını "Müşteri, iklim değişikliğinin ilgili bir konu olup olmadığını belirlemeli" İlgili tarafların ihtiyaç ve beklentileri "İlgili tarafların iklim değişikliğiyle ilgili gereksinimler"

4.4.9 Uygunsuzlukların Sebeplerinin Analizi

CAS, müşteriden, belirlenen zaman içerisinde, kök neden analizi yapmasını ve yapılan veya yapılması planlanan belirli düzeltme ve düzeltici faaliyetleri tanımlamasını, tespit edilen uygunsuzlukların ortadan kaldırılmasını ister.

4.4.10 Düzeltme ve Düzeltici Faaliyetlerin Etkinliği

CAS, müşteri tarafından tespit edilen düzeltmeleri, belirlenen sebepleri ve uygulanabilir düzeltici faaliyetleri gözden geçirir. CAS, gerçekleştirilen her bir düzeltme ve düzeltici faaliyetin etkinliğini doğrular. Uygunsuzlukların çözümünü desteklemek için elde edilen kanıt kayıt altına alınır. Müşteri, gözden geçirme ve doğrulama sonucundan haberdar edilir. Müşteri, etkin düzeltme ve düzeltici faaliyetlerin doğrulaması için ilave bir tam denetim, ilave bir sınırlı denetim veya dokümante edilmiş kanıt (gelecekteki denetimlerde teyit edilecek) gerekip gerekmediği konusunda bilgilendirilir.

ISO/IEC 17021-1:2015, Madde 9.4'ün gereklilikleri esas alındı.

BGYS/KVYS tetkikinin Özel Unsurları

CAS tetkik ekibi:

a) müşteriden, BGYS/KVYS kapsamındaki bilgi güvenliği ile ilişkili risk değerlendirmesinin BGYS/KVYS'nin işletimi için ilgili ve yeterli olduğunu kanıtlamasını talep eder;

b) müşterinin bilgi güvenliğine ilişkin risklerin tanımlanması, incelenmesi ve değerlendirilmesi için olan prosedürlerinin ve uygulanma sonuçlarının müşterinin politikası, amaçları ve hedefleri ile uyumlu olup olmadığını belirler.

CAS aynı zamanda risk değerlendirme sırasında kullanılmış olan prosedürlerin sağlıklı ve doğru uygulanmış olduğunu belirler.

ISO/IEC 27006-1:2024,Madde 9.4.2'nin gereklilikleri esas alındı.

Tetkik Raporu

Tetkik raporu aşağıdaki bilgileri ya da onlara yapılan atıfları verilir:

- a) müşterinin bilgi güvenliği risk analizinin belgelendirme tetkikine dair bir açıklama,
- b) kuruluş tarafından, ISO/IEC 27001:2022, Madde 6.1.3 c) gereğince karşılaştırma amacıyla kullanılan herhangi bir bilgi güvenliği kontrol seti.

Tetkik raporu belgelendirme kararını kolaylaştırıcı ve destekleyici olacak şekilde detaylı olur.

Rapor aşağıdakileri içerir:

- izlenen önemli tetkik adımları ve kullanılan yöntemler.
- Uygulanabilirlik Bildirgesi sürümüne yapılan atıf ve uygulanabilir ise, müşterinin daha önceki belgelendirme tetkiklerinin sonuçları ile işe yarayabilecek karşılaştırmalar.

Tamamlanmış anketler, kontrol listeleri, gözlemler, kayıtlar ya da tetkikçi notları tetkik raporunun ayrılmaz bir parçasını oluşturur. Bu yöntemler kullanılmışsa, bu dokümanlar CAS'a belgelendirme kararını destekleyici kanıt olarak sunulur. Tetkik sırasında değerlendirilmiş olan örneklemlerin bilgileri tetkik raporunda ya da bir başka belgelendirme dokümanında bulunur.

Uzaktan tetkik yöntemlerinin kullanıldığı durumlarda, raporda bu yöntemlerin tetkikin yürütülmesinde ne ölçüde kullanıldığı ve tetkik hedeflerine ulaşmadaki etkinliği belirtilir.

Kuruluşun faaliyetleri belirli bir fiziksel konumda yürütülmüyorsa ve bu nedenle kuruluşun tüm faaliyetleri uzaktan yürütülüyorsa, tetkik raporunda kuruluşun tüm faaliyetlerinin uzaktan yürütüldüğü belirtilir.

Rapor, BGYS/KVYS'de güvenilirlik sağlanması için müşterinin benimsediği iç düzen ve prosedürlerin yeterliliğini göz önünde bulundurulur.

Raporda, BGYS/KVYS gereklilikleri ve bilgi güvenliği kontrollerinin uygulanması ve etkinliğine ilişkin olumlu ya da olumsuz, en önemli gözlemlerin bir özeti yer alır.

ISO/IEC 27006-1:2024,Madde 9.4.3'ün gereklilikleri esas alındı.

4.5 Belgelendirme Kararı

4.5.1 Genel

CAS, belgelendirmeyi verme veya reddetme, belgelendirme kapsamının genişletilmesi veya daraltılması, belgelendirmenin askıya alınması veya geri çekilmesi, belgelendirmenin iptali veya yenilenmesi kararlarını veren kişilerin veya komitelerin denetimleri yapanlardan farklı olmalarını güvence altına alır. Bunun için belgelendirme komitesi oluşturulmuş, Belgelendirme kararı vermek üzere atanan kişilerin uygun yeterliliğe sahip olması sağlanır. Belgelendirme Komitesinin üyelik yapısı, çalışma esasları, sorumluluk ve yetkileri Personel Yetkinlik Matrisi ve Yönetim Sistemi El Kitabı, belgelendirme komitesi yetki sorumluluk ve görev tanımlarında belirtilen gerekliliklere göre gerçekleştirilir.

CAS tarafından belgelendirme kararı vermek üzere atanan kişiler denetim ekibinden bağımsız,

tarafsızlık riski bulunmayan, standart tarafından öngörülen teknik yeterliliğe sahip, etkin inceleme gerçekleştirilebilecek komite üyelerinden oluşmaktadır. Komite üyeleri tam zamanlı çalışan, kısmi zamanlı çalışan, dış kaynaklı uzman, sözleşmeli teknik uzman veya bağımsız komite üyesi olabilir. Belgelendirme komite üyelerinin Belgelendirme Komitesi Üyelik Sözleşmesi ile atamaları yapılır. CAS altındaki çalışan veya sözleşmeli personel, ISO/IEC 17021-1 ile diğer standartların şartlarını sağlar.
CAS, denetim ekibi ve diğer kaynaklardan (ek teknik görüş veya uzman bilgisi) gelen ilave bilgi veya açıklamalar dahil, her bir belgelendirme kararını göz önüne alır.

4.5.2 Karar Vermeden Önce Yapılacaklar

CAS, belgelendirmenin verilmesi, belgelendirme kapsamının genişletilmesi veya daraltılması, belgelendirmenin yenilenmesi, askıya alınması, geri çekilmesi, iptal edilmesi kararlarından birini vermeden önce etkin bir gözden geçirmeyi gerçekleştirmek için aşağıdakileri içeren BGYS/KVYS Belgelendirme Prosedürüne sahiptir:

- Denetim ekibi tarafından sağlanan bilgi, belgelendirme şartları ve belgelendirme kapsamına göre yeterliliği.
- Her hangi bir majör uygunsuzluk için düzeltme veya düzeltici faaliyetin gözden geçirilmesi, kabul edilmesi ve doğrulanması,
- Her hangi bir minör uygunsuzluk için düzeltme veya düzeltici faaliyetin gözden geçirilmesi, kabul edilmesi ve doğrulanması.

4.5.3 İlk Belgelendirme Kararı Verilmesi İçin Bilgi

Belgelendirme kararı için denetim ekibi tarafından CAS'a en az aşağıdaki bilgiler sağlanır:

- Denetim raporu,
- Uygunsuzluklar ve uygun olduğu takdirde denetlenen kuruluş tarafından yapılan düzeltme ve düzeltici faaliyetler hakkındaki yorumlar,
- Başvurunun gözden geçirilmesinde kullanılmak üzere CAS' ye sağlanan bilginin teyidi,
- Denetim amaçlarına ulaşıldığının teyidi,
- Herhangi bir şart veya gözlemle birlikte, belgelendirmenin verilip verilmemesine ilişkin tavsiye.

CAS, Aşama.2 'nin son gününden sonra 6 ay içerisinde herhangi bir majör uygunsuzluk için gerçekleştirilecek düzeltme ve düzeltici faaliyetin yerine getirildiğini doğrulayamazsa, belgelendirme tavsiyesinden önce yeni bir Aşama.2 denetimi gerçekleştirir.
Belgelendirmenin, bir CAS'tan taşınması durumunda (transfer), CAS belgelendirme kararı almak için yeterli bilginin elde edilmesi için Transfer Belgelendirme Prosedürü ve BGYS/KVYS Belgelendirme Prosedürünü oluşturmuş ve uygulamaktadır.

4.5.4 Yeniden Belgelendirme İçin Bilgi

CAS, belgelendirmeyi yenileme hakkındaki kararlarını, yeniden belgelendirme denetimi sonuçlarına, belgelendirme periyodu boyunca sistemin gözden geçirilmesine ve belgelendirme kullanıcılarından alınan şikâyetlere dayanarak verir.

Belgenin Düzenlenmesi

ISO 27001 BGYS/KVYS sertifikasından SoA uygulanabilirlik bildirgesi güncel tarihi ile birlikte sertifika üzerine yazılır.
Uygulanabilirlik bildirgesindeki kontroller için kuruluş başka bir kaynak (PCIDSS-Tisax-Cobit vb.) kullanmışsa sertifikasyonda bu kaynağa atıfta bulunulması durumda bunun bir referans kaynak olduğu, bir sertifikasyon olmadığı açıkça belirtilir.
Belgelendirme dokümanları, kuruluşun ISO/IEC 27001:2022, 6.1.3 d)uyarınca Uygulanabilirlik Bildirgesinde gerekli olduğu belirlenen kontroller için kontrol seti kaynağı / kaynakları olarak ulusal ve uluslararası standartlara atıfta bulunabilir. Belgelendirme dokümanlarındaki atıfların, Uygulanabilirlik Bildirgesinde uygulanan kontroller için sadece bir kontrol seti kaynağı olduğu ve dolayısıyla atıfların belgelendirmesinin olmadığı açıkça belirtilmelidir.
ISO/IEC 17021-1:2015, Madde 9.5'in gereklilikleri esas alındı.

Belgelendirme Kararı

Belgelendirme kararı, tetkik ekibi tarafından sağlanan belgelendirme tetkiki raporundaki

belgelendirme tavsiyesini temel alır.
Yönetimin gözden geçirmeleri ve iç BGYS/KVYS tetkikleri için gerekli düzenlemelerin uygulandığı, etkin olduğu ve sürdürüleceğini ispatlayacak kanıtlar olmadan müşteriye belgelendirme yapılmaz.
ISO/IEC 27006-1:2024,Madde 9.5.2'nin gereklilikleri esas alındı.

4.6 Belgelendirmenin Sürdürülmesi

4.6.1 Genel

CAS, müşterinin yönetim sistemi standardının şartlarını sağlamayı sürdürdüğünü göstermesini esas alarak belgelendirmenin sürdürülmesine karar verir. Aşağıdakilerin olması şartıyla, CAS, ilave bağımsız gözden geçirme ve karar olmadan, denetim ekibi liderinin olumlu sonucunu esas alarak müşterinin belgelendirmesinin devamına karar verir:

- Herhangi bir majör uygunsuzluk veya belgelendirmenin askıya alınması veya geri çekilmesine sebep olabilecek bir durumda, CAS'ın belgelendirmenin sürdürülmesine karar vermesini tayin için denetimi gerçekleştirenden farklı yeterli personel tarafından bir gözden geçirmeyi başlatması ihtiyacını denetim ekibi liderinin CAS'a rapor etmesi için bir sisteme sahip olması,
- Belgelendirme faaliyetlerinin etkin bir şekilde gerçekleştirileceğini teyit etmek için CAS'ın, gözetim faaliyetlerini izleyebilmesi için yeterli personel.

ISO/IEC 17021-1:2015, Madde 9.6.1'in gereklilikleri esas alındı.

4.6.2 Gözetim Faaliyetleri

CAS, gözetim faaliyetlerini, yönetim sisteminin kapsamında yer alan saha ve fonksiyonların temsilini düzenli aralıklarla, belgelendirilmiş müşteri ve yönetim sistemindeki değişiklikleri dikkate alarak gerçekleştirmektedir.
Gözetim faaliyetleri, belgelendirilmiş müşterinin yönetim sisteminin, belgelendirmenin sağlandığı standardın belirlenmiş şartlarını sağlamasının sahada denetimini içermektedir. Diğer gözetim faaliyetleri aşağıdakileri içerir:

- Belgelendirme hususlarında, CAS'ın belgelendirilmiş kuruluşa yönelttiği sorular,
- Belgelendirilmiş müşteri kuruluşun işlemleri hakkındaki beyanların gözden geçirilmesi (örneğin, promosyon malzemeleri, internet sayfası),
- Belgelendirilmiş müşteriden dokümante edilmiş bilgi verme istekleri (kağıt veya elektronik ortamda),
- Belgelendirilmiş müşterinin performansının izlenmesi için diğer araçlar.

Gözetim Denetimi

Gözetim denetimleri, İlk belgelendirmeyi takip eden ilk gözetim tarihi, Aşama.2 denetiminin son gününden 12 ay sonrasını geçmeyecek şekilde yılda en az 1 kez gerçekleştirilir. Gözetim denetimi, denetim süresinin en az üçte birini oluşturmalıdır ve Denetim süresi, toplam denetim süresinin %80'inden az olmamalıdır
Gözetim denetimleri, yukarıda belirlenen prensip doğrultusunda, kuruluşların Aşama.2 denetimini takiben, Deneti Raporu Eki Denetim Programı ile izlenmek üzere planlanır. Düzenlemelerden sonra en az 1 gün olmalıdır;
Gözetim denetimleri için, Planlama Sorumlusu tarafından, 12 aylık periyodun dolmasından en az (1) bir ay önce denetim tarihi ve denetim ekibi belirlenerek Atama Formu ile görevlendirmesi yapılır, ilgili kuruluşa Atama Formu ile denetim bildirilir.
Gözetim denetimi şunları kapsamalıdır.

- İç denetim, yönetim incelemesi ve önleyici ve düzeltici faaliyet olan sistem devamlılığı bileşenleri;
- BGYS/KVYS standardı ISO/IEC 27001 & ISO/IEC 27701 ve belgelendirme için gerekli olan diğer dokümanlar tarafından gerekli olan harici taraflardan alınan iletişim
- Dokümante edilmiş sistemdeki değişiklikler
- Değişime konu olan alanlar
- ISO/IEC 27001 & ISO/IEC 27701'in seçilen bileşenleri;
- Uygun şekilde seçilen diğer alanlar
- CAS tarafından yapılan gözetimler en az aşağıdakileri gözden geçirmelidir:

- Müşteri organizasyonun, politikalarının hedeflerine ulaşabilmesi hususunda kullanılan BGYS/KVYS' nin etkinliği
- Periyodik değerlendirme için prosedürlerin işleyişleri ve bağlı bilgi güvenliği düzenlemelerine uygunluğunun gözden geçirilmesi
- En son denetlemede tespit edilen uygunsuzluklar için alınan aksiyonlar
- Belirlenen kontrollerdeki değişiklikler ve buna bağlı olarak uygulanabilirlik bildirgesindeki değişiklikler.
- Denetim programına göre uygulama ve kontrollerin etkinliği

Ek olarak, aşağıdaki hususlar göz önüne alınmalıdır:

- Sertifikasyon kuruluşu gözetim programını, varlıkları, güvenlik açıkları ve müşteri organizasyona olan etkileriyle bağlantılı bilgi güvenliği sistemi konularına adapte edebilmeli ve programın yürüdüğünü ispat edebilmelidir.
- Sertifikasyon kuruluşunun gözetim programı yine sertifikasyon kuruluşu tarafından belirlenecektir. Sertifikasyon almış müşteri organizasyonla belirli ziyaret günleri konusunda anlaşmaya varılabilir.
- Gözetim denetlemeleri diğer yönetim sistemlerinin denetimleriyle birleştirilebilir. Raporlama her bir yönetim sistemiyle bağlantılı durumları açıkça içerecektir.
- BGYS/KVYS İklim Değişikliği Hususlarının Etkisi
- Organizasyonu ve bağlamını "Müşteri, iklim değişikliğinin ilgili bir konu olup olmadığını belirlemeli"

  İlgili tarafların ihtiyaç ve beklentileri "İlgili tarafların iklim değişikliğiyle ilgili gereksinimler"

Sertifikasyon kuruluşu sertifikasyonun düzgün kullanımını denetlemek zorundadır.
Gözetim denetimleri sonucunda, baş denetçi tarafından Gözetim için hazırlanan Denetim Raporu ve Eki Açılış Kapanış Toplantı formu, varsa uygunsuzluk için düzeltici faaliyet formu Belgelendirme Müdürlüğüne ve bu yolla kuruluşa iletilir.
Gözetim denetimlerinde SoA, BGYS/KVYS kontrolleri ve değişikliklerin değerlendirilmesi denetim raporu ile garanti altına alınır.
Gözetim denetimlerinde bulunan küçük uygunsuzluklar ile ilgili düzeltici faaliyet planları (30) otuz gün içinde giderilerek, CAS' ye bildirilmelidir.
Bir önceki denetimde tespit edilen ve doküman veya kayıt incelenmesi ile kapatılan küçük uygunsuzluklar giderilmemiş ise büyük uygunsuzluğa çevrilerek denetim raporu (Tüm sistemlerde Denetim Raporu) düzenlenir.
Gözetim denetiminde büyük uygunsuzluk tespit edilirse, uygunsuzluğun/uygunsuzlukların durumu dikkate alınarak 8.maddede açıklandığı şekliyle belge askıya alınabilir.
ISO/IEC 17021-1:2015, Madde 9.6.2'nin gereklilikleri esas alındı.
Gözetim tetkiki prosedürleri, bu dokümanda da belirtildiği gibi müşterinin BGYS/KVYS'nin belgelendirme
tetkiklerine yönelik prosedürlerin bir alt kümesini teşkil eder.
Gözetimin amacı ise, onaylanmış BGYS/KVYS'nin uygulamada kalmasını ve müşterinin değişen çalışma yaklaşımları sonucu sistemde yapılan değişikliklerin olası sonuçlarının dikkate alınmasını ve bunların belgelendirme gereklilikleriyle uyumlu olduğunu doğrular. Gözetim tetkikleri asgari aşağıdakileri kapsar:

- bilgi güvenliği risk değerlendirme ve kontrolün sürdürülmesi, iç BGYS/KVYS tetkikleri, yönetim gözden geçirmesi ve düzeltici eylemler gibi sistem devamlılığının unsurları;
- ISO/IEC 27001 ve belgelendirme için gerekli olan diğer dokümanların gerektirdiği şekilde dış taraflardan gelen iletişimler.

ISO/IEC 27006-1:2024,Madde 9.6.2.2'nin gereklilikleri esas alındı
CAS tarafından yapılacak her gözetim asgari olarak aşağıdakileri gözden geçirir:

- müşterinin bilgi güvenliği politikası amaçlarına ulaşma açısından BGYS/KVYS'nin etkinliğini;
- ilgili bilgi güvenliği mevzuatı ve düzenlemeleri açısında düzenli değerlendirme ve uyum gözden geçirmeleri için prosedürlerin işleyişini;

- ❖ belirlenmiş kontrollerde yapılan değişiklikleri ve sonucunda SoA'da oluşan değişiklikleri;
- ❖ tetkik programına göre kontrollerin uygulanmasını ve etkinliğini.

ISO/IEC 27006-1:2024,Madde 9.6.2.3'ün gereklilikleri esas alındı

CAS, gözetim faaliyetleri programını, müşteriye ilişkin bilgi güvenliği konularıyla ilgili riskler ve etkiler doğrultusunda uyarlayabilmeli ve bu programı gerekçelendirir.

Gözetim tetkikleri, diğer yönetim sistemlerinin tetkikleriyle birlikte yapar. Tetkik raporları, her yönetim sistemiyle ilgili hususları açıkça belirtir.

Gözetim tetkikleri sırasında CAS, kendisine iletilmiş itiraz ve şikâyetlerin kayıtlarını kontrol eder. Herhangi bir uygunsuzluk veya belgelendirme gerekliliklerinin karşılanmaması durumunda, CAS, müşterinin kendi BGYS/KVYS'sini ve prosedürlerini inceleyip incelemediğini ve uygun düzeltici önlemleri alıp almadığını kontrol eder.

Gözetim raporu özellikle daha önceden belirlenmiş uyuşmazlıkların giderilmiş olduğu bilgisi ile SoA'nın güncel sürümünü ve önceki tetkikten sonra yapılmış önemli değişiklikleri içerir.

Gözetimden kaynaklanan raporlar asgari olarak yukarıda belirtilen gerekliliklerin tümünü kapsayacak şekilde oluşturulur.

ISO/IEC 27006-1:2024,Madde 9.6.2.4'ün gereklilikleri esas alındı

4.6.3 Yeniden Belgelendirme

Yeniden belgelendirme denetimlerinin tarihi, belge geçerlilik süresi baz alınarak belirlenir.

Belge geçerlilik süresi bitecek kuruluşlar için, Planlama Sorumlusu tarafından, belge geçerlilik süresi bitmeden (3) üç ay önce Gözetim-Yeniden Belgelendirme Teyit Formu ile güncel bilgiler alınır ve Atama Formu ile bildirilir. Firma yeniden belgelendirme ister ise belge yenileme sözleşmesi yapılması için satış ve pazarlama bölümüne bildirilir. Yenileme talebi olan kuruluşlardaki değişikliklerin değerlendirilmesi ve firma bilgilerinin kontrolü için yeniden başvuru formu doldurmaları talep edilir. Yeni sözleşmeyi takiben, yeniden belgelendirme denetimi tarihi ve denetim ekibi belirlenerek, teyit edilmesi amacı ile ilgili kuruluşa Atama Formu gönderilir.

Daha sonra üzerinde uzlaşılan denetim tarihi için, denetim ekibi belirlenerek, teyit edilmesi amacıyla, genel olarak denetimden önce, Atama Formu, Teklif ve Sözleşme Formu ile ilgili kuruluşa bildirilir.

Yeniden belgelendirme denetimlerinin süresi ilk belgelendirme denetiminde harcanan sürenin 2/3 ü kadardır ve Yeniden belgelendirme denetimleri için ayrılan denetim süresi, düzenlemelerden sonra en az 2 gün olmalıdır. Yeniden belgelendirme denetimleri ilk belgelendirme denetimlerinin ikinci aşama denetimi gibi planlanır ve gerçekleştirilir.

Ancak aşağıdaki değişikliklerin kuruluşta oluştuğunun tespit edilmesi durumunda 1. aşama denetimde teklif edilir, planlanır ve uygulanır.

a) Kuruluşun proses, yönetim sisteminde ve personelinde en son yapılan ara denetimden sonra çok önemli değişiklikler olmuş ise,
b) Kuruluşun belgelendirildiği standartlar veya uygulanabilir yasal şartlarda çok önemli değişiklikler oluşmuş ise.

Eğer denetim birinci ve ikinci aşama olarak birlikte planlanacak ise denetim süresi bu prosedüre uygun olarak hesaplanır.

Yeniden belgelendirme denetimlerinde denetim ekibi bir önceki 3 yıllık belgelendirme süresi içerisinde kuruluşun yönetim sisteminin performans bilgisini inceleyerek denetimlerini bu bilgiler ışığında planlar ve gerçekleştirir. Bu performans bilgisine ara denetim raporlarından veya varsa kuruluşun ofiste bulunan dosyasından erişilir.

Belge yenileme denetiminden önce denetim ekibi tarafından firmanın dokümanları, geçmiş denetim ve gözetim raporları, tespit edilen uygunsuzluklar ve kapatmaları incelenir.

Belge yenileme denetimi, bütün geçmiş bulguların ışığında, kuruluşun geçmiş performansı ve zayıf noktaları da dikkate alınarak, standardın bütün şartlarını karşılandığı değerlendirmek üzere belgelendirme denetimlerinde incelenen tüm konular incelenecek şekilde planlanır ve gerçekleştirilir.

Ayrıca sistemde revize edilen veya kapsama dâhil edilen dokümanlar gözden geçirilerek uygulamaları denetlenir.

Kuruluşun belge ve logo kullanımı gözden geçirilir.
Belge yenileme denetimleri aşama.2 denetimi gibi yapılmalıdır.
Yeniden belgelendirme denetimleri sırasında büyük veya küçük olarak derecelendirilebilecek herhangi bir uygunsuzluk tespit edilmiş ise bu uygunsuzluklar kapatılmadan yeniden belgelendirme kararı verilmez.
Uygunsuzlukların kapatılması için maksimum süre 3 aydır. Bu süreyi aşması durumunda prosedür tekrar ilk belgelendirme denetimi gibi devam eder.
Yeniden belgelendirme denetimlerinde tespit edilen uygunsuzlukların kapatılması aşağıdaki şekilde olabilir.

a) Takip denetimi yapılması
b) Uygunsuzlukların kapatıldığının kanıtlarının alınması
c) Uygunsuzluklar ile ilgili kuruluş yönetimi tarafından onaylı uygulama planının alınması

Uygunsuzluklar ancak Baş Denetçi-denetim ekibi denetçisi ve Belgelendirme Müdürünün olumlu onayı ile kapatılabilir.
Yeniden belgelendirme tetkiklerinde müşteri kuruluşun düzeltici faaliyet süresi uygunsuzluğun ve BGYS/KVYS riskinin şiddeti ile tutarlı olarak belirlenir.
Yeniden Belgelendirme Kararı; Kuruluşun yeniden belgelendirme kararı, denetim sonuçlarına göre denetim ekibinin tavsiyesi doğrultusunda denetim raporunun gözden geçirilmesi ile ve Belgelendirme Kararı verebilecek yeterliliğe sahip kişi tarafından verilir.
ISO/IEC 17021-1:2015, Madde 9.6.3'ün gereklilikleri esas alındı.

Yeniden Belgelendirme Tetkikleri

Yeniden belgelendirme tetkik prosedürleri, bu dokümanda belirtildiği üzere müşterinin BGYS/KVYS'nin ilk belgelendirme tetkikine yönelik prosedürlerin bir alt kümesini teşkil eder.
Düzeltici eylemi uygulanması için verilecek süre, uygunsuzluğun önem derecesi ve ilişkili bilgi güvenliği riskiyle tutarlı olmaktadır.
ISO/IEC 27006-1:2024,Madde 9.6.3.2'nin gereklilikleri esas alındı.

4.6.4 Özel Denetimler

Kapsam Genişletme

CAS, hâlihazırda verilmiş olan belgelendirmenin kapsamına yönelik bir genişletme başvurusuna cevaben, başvurunun gözden geçirmesini yapmakta ve genişletmenin yapılıp yapılamayacağına karar vermek için gerekli denetim faaliyetlerini belirler. Bu denetim, uygun durumlarda bir gözetim denetimi ile bağlantılı olarak yapılır.

Kısa Süreli Denetimler

CAS, şikâyetleri soruşturmak veya değişiklikleri ele almak veya askıya alınan müşterileri takip etmek veya habersiz denetimler için belgelendirilmiş müşterisini kısa süre içerisinde denetime tabi tutması gerekebilir. Bu gibi durumlarda CAS;

- a) Bu kısa süreli ziyaretleri hangi şartlar altında gerçekleştireceğini belirlemekte ve bu husus hakkında belgelendirilmiş müşterisini önceden bilgilendirmektedir.
- b) Denetim ekibinin atanmasına, müşterinin ekip üyelerine itiraz fırsatı bulunmayacağını göz önünde bulundurarak, azami önem göstermektedir.

Takip Denetimi

Aşama.2, gözetim ve yeniden belgelendirme denetimleri neticesinde, kuruluşun belge almaya hak kazanamaması veya belgesinin askıya alınması durumunda gerçekleştirilen denetimdir.
Takip denetimlerinde, bir önceki denetim raporunda belirtilen büyük uygunsuzluklar ve bu uygunsuzluklarla ilgili olarak baş denetçinin uygun göreceği diğer Standart maddeleri dikkate alınır.

Transfer Denetimi

CAS, transfer başvurularını kabul etmemektedir.
Belgelendirmenin, bir belgelendirme kuruluşundan CAS'a taşınması durumunda, CAS, transfer denetimi yapmamaktadır. Böyle bir durumda başvuru yeni kabul edilerek belgelendirme süreçleri takip edilir.

Ön Denetim

Sistem Belgelendirme hazırlıklarını tamamlayan ve bu hazırlıkların yeterliliğini kontrol etmek

isteyen kuruluşların talepleri doğrultusunda, Belgelendirme denetimleri öncesinde yapılan denetimdir.
Ön denetimler, belgelendirme denetiminden bağımsızdır ve belgelendirme denetim gün sayısını hiçbir şekilde etkilemez.
Ön denetimlerin süresi, kuruluşun büyüklüğü ne olursa olsun (1) bir gün ile sınırlıdır.
Ön denetimlerde, aşağıda verilen konular özellikle dikkate alınmalıdır:

- Yönetimin gözden geçirmesi,
- İç denetimler,
- Düzeltici/Önleyici faaliyetler,
- Müşteri şikâyetleri,
- Risk değerlendirme metodolojisinin tanımı, risk değerlendirme raporu, risk işleme planı ihtiyaç duyulan prosedür ve kontrollerin etkinliğinin nasıl ölçüleceğini tanımlama, bu standart tarafından gerek duyulan kayıtlar, uygulanabilirlik bildirgesini içermeli,
- Sürdürülebilirliğinin sağlanması
- BGYS/KVYS İklim Değişikliği Hususlarının Etkisi

Organizasyonu ve bağlamını "Müşteri, iklim değişikliğinin ilgili bir konu olup olmadığını belirlemeli" İlgili tarafların ihtiyaç ve beklentileri "İlgili tarafların iklim değişikliğiyle ilgili gereksinimler"
Ön denetim sonrasında, denetim ekibi tarafından iki nüsha olarak "Ön Denetim Raporu" hazırlanır bir nüshası kuruluşa gönderilir. Bir nüshası, kuruluş dosyasında saklanır.
ISO/IEC 17021-1:2015, Madde 9.6.4'ün gereklilikleri esas alındı.

4.6.5 Belgelendirmenin Askıya Alınması, Geri Çekilmesi veya Kapsamının Daraltılması

CAS, belgelendirmeyi askıya alma, geri çekme veya kapsamı daraltma için Belgelendirmenin Askıya Alınması ve Geri Çekilmesi Prosedürü oluşturmuş ve uygulamaktadır.
CAS, bunlarla sınırlı olmamak kaydıyla aşağıdaki durumlarda belgelendirmeyi askıya alır:

- Müşterinin belgelendirilmiş yönetim sisteminin, yönetim sisteminin etkili olmasına yönelik şartları dâhil olmak üzere, belgelendirme şartlarını karşılamada devamlı ve ciddi şekilde başarısız olması,
- Belgelendirilmiş müşterinin gözetim veya yeniden belgelendirme denetimlerinin gerekli sıklıkta yapılmasına izin vermemesi,
- Belgelendirilmiş müşterinin, gönüllü olarak geçici askıya alma talebinde bulunması.
- Askıya alınma durumunda, müşterinin yönetim sistemi belgesi geçici olarak geçersizdir.

CAS, askıya alma işlemini doğuran sorun çözümlendiği takdirde, askıya alınan belgelendirmeyi eski durumuna getirir. CAS, askıya alınma ile sonuçlanan konunun verilen süre içerisinde çözümlenmemesi durumunda, belgelendirmeyi geri çeker veya belgelendirme kapsamını daraltır.
Müşteri belgelendirme kapsamının bir kısmı için belgelendirme şartlarını karşılamada devamlı veya ciddi başarısızlık gösterdiğinde, CAS, müşterinin belgelendirme kapsamının şartlarını karşılamayan kısmı dışarıda tutacak şekilde daraltır. Bu tip bir daraltma, belgelendirme için kullanılan standardın şartlarıyla uyumludur.
ISO/IEC 17021-1:2015, Madde 9.6.5'in gereklilikleri esas alındı.

4.7 İtirazlar

CAS itirazları alma, değerlendirme ve bunlar hakkında karar vermek için İtiraz ve Şikayet Prosedürünü oluşturmuş ve uygulamaktadır.
CAS itirazları ele almanın bütün seviyelerindeki kararlardan sorumludur. CAS, itirazları ele alma proseslerinde yer alan kişilerin, belgelendirme kararını verenler ve denetimi yapanlardan farklı olmasını, güvence altına alır.
İtirazların kabulü, soruşturması ve kararı, itiraz edene karşı ayrımcı herhangi bir faaliyetle sonuçlanmaması, güvence altına alır.
İtirazı ele alma prosesi aşağıdaki unsurları ve yöntemleri kapsar:

- Daha önceki benzer itirazlar dikkate alınarak, itirazları; alma, geçerli kılma ve soruşturma ile bunlara cevap olarak yapılacak faaliyetlere karar vermeye yönelik prosesin ana hatlarını,
- İtirazları çözümlemek için yapılan faaliyetler dâhil olmak üzere, itirazların izlenmesini ve kayıt altına alınmasını,

- ❖ Yapılacak uygun düzeltmenin ve düzeltici faaliyetin sağlanmasını.

CAS, itirazı aldıktan sonra, itirazın geçerli olması için bütün gerekli bilgiyi toplamakta ve doğrulanmasını yapar.
CAS itirazın alındığını, ilerleme raporlarını ve sonucu, itiraz sahibine bildirir.
İtiraz sahibine iletilecek olan karar, itiraza konuyla daha önce ilgili olmayan kişi/ler tarafından verilmekte veya gözden geçirilmekte ve onaylar.
CAS, itirazı ele alma prosesi sonucunun resmî bildirimini, itiraz sahibine yapar.
ISO/IEC 17021-1:2015, Madde 9.7'nin gereklilikleri esas alındı.

4.8 Şikayetler

CAS, şikâyetleri ele almanın bütün aşamalarındaki kararlardan sorumludur.
Şikâyetlerin kabulü, soruşturması ve kararı, şikâyet edene karşı ayrımcı herhangi bir faaliyetle sonuçlanmaması, güvence altına alınır.
Şikâyetin alınması üzerine, CAS şikâyetin kendisinin sorumlu olduğu belgelendirme faaliyetleriyle ilgili olup olmadığını, teyit etmektedir. Şikâyet, belgelendirme faaliyetleriyle ilgiliyse şikâyeti ele almaktadır. Şikâyet, belgelendirilmiş bir müşteri kuruluşla ilgiliyse, şikâyetin sorgulanmasında belgelendirilmiş yönetim sisteminin etkinliği dikkate alınır.
Belgelendirilmiş müşteri kuruluş hakkındaki herhangi bir şikâyet, CAS tarafından sözü edilen belgelendirilmiş müşteri kuruluşa zamanında yönlendirilir.
CAS şikâyetleri alma, değerlendirme ve hakkında karar vermek için İtiraz ve Şikayet Prosedürünü oluşturmuş ve uygulamaktadır. Bu proses, şikayet sahibi ve şikayet konusuyla ilgili olduğundan, gizlilikle ilgili şartlara tâbidir.
Şikâyetleri ele alma prosesi aşağıdaki unsurları ve yöntemleri kapsar:

- ❖ Şikâyeti alma, geçerli kılma ve soruşturma ile bunlara cevap olarak yapılacak faaliyetlere karar vermek için gereken prosesin ana hatlarını,
- ❖ Şikâyetleri çözümlemek için yapılan faaliyetler dâhil olmak üzere, şikâyetlerin izlenmesi ve kayıt altına alınmasını,
- ❖ Yapılacak uygun düzeltmenin ve düzeltici faaliyetin güvence altına alınmasını.
- ❖ CAS, şikâyeti aldıktan sonra, şikâyeti geçerli kılmak için gerekli olan bütün bilgilerin toplanmasından ve doğrulanmasından sorumludur.

CAS, mümkün olduğu durumlarda, şikâyet sahibine şikâyetin alındığını bildirmekte ve ilerleme raporlarını ve sonucu iletir.
Şikâyet sahibine iletilecek olan kararın, şikâyete konu olan hususlara önceden müdâhil olmamış kişi/ler tarafından verilmekte veya gözden geçirilmekte ve onaylanmaktadır.
CAS, mümkün olan durumlarda, şikâyet sahibine şikâyeti ele alma prosesinin sonucunu resmi olarak bildirir.
CAS, şikâyet konusunu ve bunun çözümünün kamuoyuna verilip verilmeyeceği, verilecekse ne kapsamda verileceği konusunu, müşteri ve şikâyet sahibi ile birlikte belirler.
Şikayetler, potansiyel ihlal olayı ve muhtemel uyumsuzluğun bir göstergesidir.
ISO/IEC 17021-1:2015, Madde 9.8'in gereklilikleri esas alındı.

4.9 Müşteri Kayıtları

CAS, başvuru yapan müşteri kuruluşlar ile denetlenen, belgelendirilen veya belgelendirmesi geri çekilen ve askıya alınan bütün müşteri kuruluşlar dâhil olmak üzere, bütün müşteri kuruluşlar için denetim ve diğer belgelendirme prosesleri hakkındaki kayıtları Back Up Talimatına göre muhafaza eder.
Belgelendirilmiş müşteri kuruluşlar ile ilgili kayıtlar aşağıdakileri içerir:

- ❖ Başvuru bilgileri ve ilk, gözetim ve yeniden belgelendirme denetim raporlarını,
- ❖ Belgelendirme anlaşmasını,
- ❖ Örnekleme için kullanılan yönteminin gerekçelendirilmesini (uygun olduğu takdirde),
- ❖ Denetim zamanını belirlemenin gerekçelendirmesini,
- ❖ Düzeltme ve düzeltici faaliyetlerin doğrulanmasını,
- ❖ İtirazlar ve şikâyetler ile bunları takip eden düzeltme ve düzeltici faaliyetlerin kayıtlarını,
- ❖ Uygulanabilir olduğunda, komite tutanakları ve kararlarını,

- Belgelendirme kararlarının dokümantasyonunu,
- Ürün, proses veya uygulanabilir olduğunda hizmet ile ilgili olarak belgelendirme kapsamı dâhil olmak üzere belgelendirme dokümanlarını,
- Belgelendirmenin güvenilirliğini sağlamak için denetçilerin ve teknik uzmanların yeterlilik kanıtı gibi, gerekli olan ilgili kayıtlarını,
- Denetim programlarını.

CAS, başvuruda bulunan ve belgelendirilmiş olan müşteri kuruluş hakkındaki kayıtları, bilgilerin gizliliğini güvence altına almak için koruma altında tutar. Kayıtların, gizliliğinin sürdürülmesini temin edecek şekilde taşınmasını, aktarılmasını veya nakledilmesini sağlar.
CAS, kayıtların tutulması hakkında Kayıtların Kontrolü Prosedürünü oluşturmuş ve uygulamaktadır. Belgelendirilmiş müşteri kuruluş ile daha önceden belgelendirilmiş müşteri kuruluşların kayıtları, mevcut çevrim süresine ilave olarak, tam bir belgelendirme çevrimi boyunca saklanır.
ISO/IEC 17021-1:2015, Madde 9.9'un gereklilikleri esas alındı.

5 Belgelendirme Kuruluşları İçin Yönetim Sistemi Gereklilikleri

5.1 Seçenekler

ISO/IEC 17021-1:2015, Madde 10.1'in gereklilikleri esas alındı.

BGYS/KVYS Uygulaması

CAS'ın ISO/IEC 27001 uyarınca BGYS/KVYS'ni uygulaması tavsiye edildiği için uygulanmaktadır.
ISO/IEC 27006-1:2024,Madde 10.1.2'nin gereklilikleri esas alındı.

5.2 Seçenek A: Genel yönetim sistemi gereklilikleri

Uygulanmamaktadır.
ISO/IEC 17021-1:2015, Madde 10.2'nin gereklilikleri esas alındı.

5.3 Seçenek B: ISO 9001 uyarınca yönetim sistemi gereklilikleri

Uygulanmaktadır.
ISO/IEC 17021-1:2015, Madde 10.3'ün gereklilikleri esas alındı.

REVİZYON BİLGİLERİ		
Rev.No	**Revizyon Tarihi**	**Revizyon Açıklaması**
0	05.01.2022	İlk yayın.
1	04.08.2023	Madde 7.5 ekleme yapıldı ve değiştirildi.
2	02.12.2024	ISO 27001:2022 AMD 1:2024 iklim değişikliği ile ilgili ekleme yapıldı
3	01.01.2025	İçerik Düzeltme ve Unvan değişikliği

HAZIRLAYAN:	**ONAYLAYAN:**
YÖNETİM TEMSİLCİSİ	GENEL MÜDÜR