CİCERT BELGELENDİRME HİZMETLERİ LTD.ŞTİ.

Yönetim Sistemi Belgelendirme Kılavuzu

Revizyon No	Revizyon Tarihi	Açıklama
A	06.02.2012	İlk Yayın
B	17.09.2012	İlk Belgelendirme Denetiminin Değerlendirilmesi; İlk Belgelendirme Kararının Verilmesi; Belgenin Sürdürülmesi Kararının Verilmesi; maddelerinde minör ve majör uygunsuzluklar için değişen şartlar düzenlendi Bölüm 9- Belge ve Logoların Kullanımı maddesinde belge geçerlilik süresi tanımı değiştirildi
C	12.10.2012	Bölüm 10- CICERT Yükümlülükleri son maddesinde akreditasyonun askıya alınması/iptali durumunda zararların tazmini ile ilgili açıklama getirildi
D	26.11.2012	Teklif ve Sözleşme Formu yerine Denetim ve Belgelendirme sözleşmesi ifadesi kullanıldı. Cıcert sorumluluklarına ekleme yapıldı.
E	31.12.2012	Belgelendirilmiş Kuruluş ve Cicert yükümlülüklerine ekleme yapıldı.
F	20.07.2015	ISO 27006:2011 şartları ilave edildi.
G	15.08.2016	EN ISO/IEC 17021-1:2015 ve ISO/IEC 27006:2015 revizyonu yapılmıştır.

Hazırlayan **Onaylayan**

AMAÇ

Bu kılavuzun amacı, CIcert tarafından gerçekleştirilecek EN ISO/IEC 17021-1:2015 ve ISO/IEC 27006:2015 kuralları çerçevesinde kuruluşların yönetim sistemlerinin denetlenerek değerlendirilmesi ve uygunluğunun belgelendirilmesi için yürütülen faaliyetlerin esaslarını tanımlamaktır.

KAPSAM

Bu prosedür, CIcert yönetim sistemi kapsamındaki yönetim sistemleri için başvurunun alınması, denetimlerin planlanması ve yürütülmesi, denetim sonuçlarının değerlendirilmesi, belgelendirilmesi, belgenin devamlılığı için gerekli şartları, askıya alma ve iptal halinde yapılacak işlemleri ile belge ve logo kullanım esaslarını kapsar.

TANIMLAR

Belgelendirilmiş Müşteri: Yönetim sistemi belgelendirilmiş olan kuruluş.
Tarafsızlık: Objektifliğin varlığı.
Not 1 - Objektiflik, belgelendirme kuruluşunun sonraki faaliyetlerini olumsuz şekilde etkilenmemesi için çıkar çatışmasının olmaması veya çözümlendiği anlamına gelir.
Not 2 - Tarafsızlık unsurunu bildirmek için faydalı diğer kelimelerden bazıları da "bağımsızlık", "çıkar çatışmasının olmaması", "kayırmacılık olmayan", "ön yargıdan uzaklık", "tarafsızlık", "adaletli", "açık fikirlilik", "aynı şekilde ele alma", "yansızlık" ve "dengeli olmak"tır.
Yönetim Sistemi Danışmanlığı: Yönetim sisteminin kurulması, uygulanması veya devamlılığının sağlanmasına katılım.
Örnek 1 – El kitapları veya prosedürlerin hazırlanması veya oluşturulması.
Örnek 2 – Bir yönetim sisteminin geliştirilmesi ve uygulanması esnasında özel tavsiyeler, talimatlar veya çözümlerin verilmesi.
Not 1 – Eğitimin yönetim sistemleriyle veya tetkikle ilgili olması ve kursta verilen bilgilerin genel bilgilerle sınırlı olması şartıyla, bir başka deyişle, eğitmenin müşteriye özgü çözümler sağlamaması kaydıyla, eğitimin düzenlenmesi ve eğitmen olarak katılım sağlanması, danışmanlık olarak değerlendirilmez.
Not 2 – Proseslerin veya sistemin gelişmesi için müşteriye özgü çözümler sağlamaması kaydıyla verilen genel bilgiler danışmanlık sayılmaz. Bu bilgiler aşağıdakileri içerebilir:
- Belgelendirme kriterinin anlamının ve amacının açıklanması,
- Geliştirme imkânlarının belirlenmesi,
- İlgili teoriler, yöntemler, teknikler ve araçların açıklanması,
- İlgili iyi uygulama örneklerinden gizli olmayan bilgilerin paylaşımı,
- Tetkik edilen yönetim sistemlerinde yer almayan diğer yönetim hususları.

Belgelendirme Kuruluşu: Sistemin gerektirdiği herhangi bir ek doküman ve yayınlanmış bulunan Yönetim sistemi standartlarına göre bir müşteri kuruluşun yönetim sistemini değerlendiren ve belgelendiren üçüncü taraf.
Belgelendirme Dokümanı-Sertifika: Bir müşteri kuruluşun Yönetim sisteminin, sistemin gerektirdiği herhangi bir ek dokümana ve belirli Yönetim Sistemi standartlarına uygun olduğunu gösteren doküman.
İşaret: İlgili ürün ya da kişilerin belirli bir standardın şartlarına uyduğunu ya da bir kuruluş tarafından işletilen sistemlere olan yeterli güvenin mevcut olduğunu gösteren ve bir belgelendirme kuruluşun ya da bir akreditasyon kuruluşun şartları gereğince verilmiş bulunan ve hukuki olarak tescilli ticari işaret ya da hukuki olarak korunan başka bir sembol.
Müşteri: Belgelendirme amacıyla yönetim sistemi tetkik edilen kuruluş.
Kuruluş: Şirketleşmiş, kamu ya da özel, kendi fonksiyonları ve idaresine sahip olan ve yönetim sistemi uygulanmasını sağlayabilen şirket, firma, girişim, kurum, enstitü ya da bunların birleşimi. Hedeflerine ulaşmak için sorumlulukları, yetki ve ilişkileri ile kendi fonksiyonlara sahiptir kişi veya grup.
Denetçi: Tetkiki gerçekleştiren kişi.
Yeterlilik: İstenen sonuçlara ulaşmak için bilgi ve becerileri uygulama kabiliyeti.
Rehber: Tetkik ekibine yardımcı olmak amacıyla müşteri tarafından görevlendirilen kişi.
Gözlemci: Tetkik ekibine eşlik eden, ancak tetkik yapmayan kişi.
Akreditasyon: Bir uygunluk değerlendirme kuruluşunun, belirli şartlara uygun olduğunun ve ilgili uygunluk değerlendirme faaliyetlerini gerçekleştirmek için yeterli olduğunun resmi olarak üçüncü taraf tarafından tanınması.
Belgelendirme Programı: Aynı belirlenen şartlar, belirlenmiş kurallar ve prosedürlerin uygulandığı, yönetim sistemlerinin uygunluk değerlendirme sistemi.
Belgelendirme Tetkiki: Müşterinin yönetim sistemini belgelendirmek amacıyla, müşteriden ve belgelendirmeye bel bağlayan taraflardan bağımsız bir tetkik kuruluşu tarafından gerçekleştirilen tetkik.
Not 1 – Takip eden terim ve tariflerde geçen "tetkik" ifadesi basitleştirmek amacı ile "üçüncü taraf belgelendirme tetkiki" ifadesi yerine kullanılmıştır.
Not 2 – Belgelendirme tetkikleri; gözetim, takip ve yeniden belgelendirme tetkikleri ile özel tetkikleri içerir.
Not 3 – Belgelendirme tetkikleri tipik olarak yönetim sistemi standard şartlarını yerine getiren kuruluşlara uygunluk sertifikası düzenleyen belgelendirme kuruluşlarının tetkik ekipleri tarafından yürütülür.

Not 4 – Ortak tetkik, tek bir müşterinin tetkikinin, iki veya daha fazla belgelendirme kuruluşunun birlikte yaptığı tetkiktir.
Not 5 – Birleşik tetkik, bir müşterinin iki veya daha fazla yönetim standardlarının şartlarına göre birlikte tetkik edildiği tetkiktir.
Not 6 – Entegre tetkik, bir müşterinin iki veya daha çok yönetim sistemi standardları şartlarının tek bir yönetim sistemi içine entegre edilmiş uygulamasının, bir standarddan daha fazlasına göre yaptığı tetkiktir.
Uygunsuzluk: Bir şartın karşılanmaması.
Majör Uygunsuzluk: Yönetim sisteminin amaçlanan sonuçlarına ulaşması yeteneğini etkileyen uygunsuzluk
Not 1 – Uygunsuzluk aşağıdaki durumlarda majör olarak sınıflandırılabilir:
- Etkin proses kontrol yapıldığına dair veya ürün ve hizmetlerin belirlenen özelliklere uygunluğuna dair önemli şüphe varsa;
- Bir şart veya konu ile sistematik bir eksiklik olabileceğini gösteren ve böylelikle bir majör uygunsuzluk oluşturan çok sayıda minör uygunsuzluk.

Minör Uygunsuzluk: Yönetim sisteminin amaçlanan sonuçlarına ulaşması yeteneğini etkilemeyen uygunsuzluk
Gözlem: Denetim ekibinin bir sonraki denetime de yardımcı olması amacıyla belgelendirmeye esas yönetim sistemi ile ilgili olumlu veya olumsuz yazılı görüşlerdir.
Düzeltici Faaliyet: Saptanmış bir uygunsuzluğun sebebinin veya istenmeyen diğer durumların ortadan kaldırılması için yapılan faaliyet.
Düzeltme: Saptanmış bir uygunsuzluğu gidermek için yapılan faaliyet.
Şikâyet: Özel veya tüzel kişilerin, itirazdan farklı olarak, CIcert'in belgelendirme faaliyetleri ile ilgili performansı, prosedürleri, politikaları, geçici veya sürekli personeli, belgelendirdiği bir kurumun belgelendirme kapsamında yaptığı faaliyetler veya CIcert ile ilgili herhangi bir konuya ilişkin yaptıkları sözlü veya yazılı memnuniyetsizlikleri.
İtiraz: Özel veya tüzel kişilerin, CIcert'in kendilerini ilgilendiren konularda aldığı kararları yeniden mütalaa etmesine yönelik talebi.
Belgelendirme Komitesi: Yönetim sistem belgeleri ile ilgili raporları değerlendirerek belgelendirme ile ilgili tüm kararları almaya yetkili komite. Denetim ekibinde yer alan kişiler komitede yer alamaz.
İtiraz Komitesi: Yönetim sistemlerinin belgelendirme faaliyetleri ve bu faaliyetler sonucu alınan belgelendirme komitesi kararları ile ilgili itirazları değerlendirerek karara bağlamaya yetkili komite.
Denetim Ekibi: Denetimlerin gerçekleştirilmesi için başvuruya esas standart/standartlar, kuruluşun faaliyet alanı, çalışan personel sayısı ve proseslerinin durumu göz önüne alınarak oluşturulan ekip. Denetim Ekibinde, her zaman bir baş denetçi ve belgelendirilecek kapsama uygun bir veya birkaç denetçi ile gerektiğinde teknik uzmanlar yer alır. Denetim ekibi oluşturulurken ekipte yer alan denetçilerin, mümkün ise aynı müşteri kuruluşta arka arkaya 3 yıldan fazla görev almaması sağlanır.
Belgelendirme Kararı: Belgelendirme Komitesi tarafından alınan ilk belgelendirme, belgenin sürdürülmesi, askıya alınması, askıdan indirilmesi, geri çekilmesi, iptal edilmesi veya kapsam değişikliği işlemleri ile ilgili kararlar.

REFRERANS DOKÜMANLAR

ISO/IEC 17021-1:2015
ISO/IEC 27006:2015
TÜRKAK Akreditasyon rehberleri
MD1, MD2, MD5, MD3
EA-7-05, EA-7-04
ISO 9001:2008
ISO 14001:2004
ISO 27001:2013

UYGULAMA

Bölüm 1- İlk Denetim ve Belgelendirme

Başvuru;
ISO 9001, ISO 14001 ve ISO 27001 Yönetim Sistemi belgelendirmesi yapmak isteyen kuruluşlar www.cicert.com.tr adresinden, e-mail veya telefon aracılığı ile başvuru ve belgelendirme için gerekli bilgileri temin edebilirler. Başvurunun resmi olarak alınabilmesi için ***Belgelendirme Başvuru formunun*** tam ve doğru olarak doldurulması gerekmektedir.
Cicert, denetim, belgelendirme ve eğitim hizmetlerimizi, tüm TÜRKİYE de gerçekleştirmektedir. ISO 14001 denetim başvurusunun tamamlanabilmesi için ***ÇYS Belgelendirme Başvuru Formunun***, ISO 27001 denetim başvurusunun tamamlanabilmesi için ***BGYS Belgelendirme Başvuru Formu***, Entegre sistem başvurusunun tamamlanabilmesi için ise ***Entegre Belgelendirme Başvuru Forumu***'nun doldurulması gerekmektedir.

Başvuran müşteri bilgileri; istenen belgelendirme kapsamı, Belirli bir belgelendirme programı için müracaat eden kuruluşla ilgili detaylı bilgi; kuruluşun adı, tesisin/tesislerinin adresi/adresleri, prosesleri ve işlemleri, insan ve teknik kaynakları,

fonksiyonları, ilişkileri ve ilgili herhangi bir yasal kısıtlama dahil belgelendirme programında istendiği şekilde, Şartlara uygunluğu etkileyecek, belgelendirilecek kuruluş tarafından kullanılan kuruluş dışında yaptırılan proseslerin belirtilmesi, Müracaat eden kuruluşun belgelendirme istediği standardlar veya diğer şartlar, Belgelendirme istenen yönetim sistemleri için danışmanlık alınıp alınmadığı, alındı ise kimden alındığı bilgiler, vardiyalı çalışma ile ilgili detaylar ***"Belgelendirme Başvuru Formu"*** ile alınır.

Başvurunun gözden Geçirilmesi;
Gelen Başvurular Cıcert tarafından Akreditasyon Kurumu rehberleri, ISO 17021-1 standardı ve ISO 27006 standardı doğrultusunda ***Başvuru Gözden Geçirme Formu*** ile gözden geçirilir.
Başvurunun onaylanabilmesi için;

- Başvuru formlarının ve istenen evrakların tam ve doğru olması
- Müracaat eden kuruluş ve yönetim sistemi ile ilgili bilginin bir tetkik programı gerçekleştirmek için yeterli olduğu (belgelendirme için gerekli olan ilgili Standard ve diğer dokümanlara uyan yazılı hale getirilmiş ve uygulanmakta olan bir Yönetim sistemine sahip olması ve min 2 ay uygulaması)
- Başvuran kuruluş ile CIcert arasında bulunan anlayış farklarının çözümlenmesi, (Bu kılavuz şartlarının başvuran kuruluş tarafından algılanması)
- Cıcert'in belgelendirme hizmeti verebilmesi için yeterlilik ve kabiliyete sahip olması (istenen belgelendirme kapsamı, EA kodu veya teknik alan, BGYS teknolojik alanları, akreditasyon talebi, yönetim sistemi, lokasyonları, denetim ekibi ile belgelendirme kararı için yetkinlikler)
- Başvurulan belgelendirme kapsamı, başvuran kuruluşun faaliyet alanları ve çoklu sahalarının ve geçici sahalarının sayısı ve kapsamları, mevsimlik çalışma alanları ve bunların her birinin çalışan sayıları,
- Tetkiklerin yapılması için gerekli olan süre ve belgelendirme faaliyetlerini etkileyen diğer hususlar (dil, güvenlik şartları, tarafsızlığa olan tehditler (danışman kuruluş ile çalışılmış olması, akrabalık ilişkileri) vb.),
- Varsa kapsam dışı bırakılan Standard maddeleri ve gerekçeleri,
- Mevcut bir yönetim sistem belgesinin varlığı, var ise son denetime ait raporlar, uygunsuzluk raporları ve kapatmaları, mevcut belgenin bir kopyası,
- Varsa dış kaynaklı prosesler,
- Kuruluş tarafından uyulması gereken yasal mevzuat şartları ve bunlar ile ilgili alınmış olan izin ve lisans belgeleri,
- Eğer ürün veya hizmetin gerçekleştirilmesi sırasında vardiyalı bir çalışma sistemi varsa, denetimin planı ve genişliği vardiyada yapılan işin niteliğine ve vardiyaların müşteri tarafından nasıl kontrol edildiğine göre değerlendirilir. Eğer vardiya denetimi yapılmayacaksa bunun haklı gerekçesi mutlaka başvurunun gözden geçirilmesi formunda açıklanmalıdır.

Yukarıdaki kriterleri uygun olarak başvuru değerlendirilir. Başvurunun kabul edilmemesi durumunda yazılı olarak başvuran kuruluşa durum ve kabul edilmeme nedeni bildirilir. Başvurunun onaylanması durumunda başvuran kuruluş için ***Başvuru ve Denetim Faaliyetleri Prosedürü*** ne uygun olarak ***CIBELP01/F04 sözleşme*** hazırlanır. Sözleşmenin her iki taraf tarafından imzalanması ile sözleşme yürürlüğe girer. Sözleşmede belgelendirilecek kuruluşun birden fazla belgelendirilecek sahası olduğunda, bütün sahaları bu sözleşmede belirtilecektir. Cıcert'in birden fazla adresi olması durumunda da tüm Cıcert adresleri sözleşme üzerinde belirtilmesi zorunludur. Denetimler, kuruluşun sözleşmede beyan edilen tüm saha adreslerinde gerçekleştirilir.
Sözleşmesinin imzalanması, bu Kılavuzda geçen tüm şartların kuruluş tarafından kabul edildiğini de gösterir.
Sözleşme ile ekinde belirtilen tüm doküman ve evrakların kuruluş tarafından Cıcert'e iletilmesi şarttır.

Belgelendirme tetkikinden önce Cicert, müşteri kuruluştan, gizli veya hassas bilgi içermesi nedeniyle tetkik ekibine incelenmek üzere sunulamayacak olan BGYS'ye ait herhangi bir kaydın olup olmadığını bildirmesini talep eder. Cicert, bu kayıtların eksik olması durumunda, BGYS'nin uygun bir şekilde tetkik edilip edilemeyeceğine karar verir. Cicert, tespit edilen gizli ya da hassas kayıtları incelemeden BGYS'nin uygun bir şekilde tetkikinin yapılmasının mümkün olmadığına karar verirse, uygun erişim düzenlemeleri sağlanana kadar belgelendirme tetkikinin gerçekleştirilemeyeceğini müşteri kuruluşa bildirir.

Müşteri kuruluş, BGYS iç tetkiklerini planladığını ve program ve prosedürleri işletip işletmediğini başvuru formu ile beyan etmelidir.

Kuruluş, başvuruda bulunduğu tarihten itibaren 6 ay içinde belgelendirme denetimini kabul etmeyerek erteler ise başvurusu iptal edilir. Başvurunun iptali kuruluş talebi ile de yapılabilir.

Tüm Denetimler Cıcert ***"Başvurunun Alınması ve Denetim Faaliyetleri Prosedürü"*** doğrultusunda, ***"Denetim Sürelerinin Belirlenmesi Talimatı"*** uygun olarak ***"Denetim Süresi hesaplama tablosu"*** hazırlanır ve belirlenen sürelerde planlanır ve ***"Denetim Kılavuzuna"*** uygun gerçekleştirilir.

İlk Belgelendirme Denetimi;
Yönetim sisteminin ilk belgelendirme tetkiki iki aşamada yapılır. Aşama 1 ve Aşama 2 olarak gerçekleştirilir. Denetimler ***"Denetim Kılavuzu"*** doğrultusunda gerçekleştirilir.

Aşama 1 Denetimi;
Aşama 1 tetkikinin amacı, müşteri kuruluşun Yönetim sistemi politika ve amaçları bağlamında ve özellikle tetkik için müşteri kuruluşun hazırlık durumu kapsamında Yönetim Sisteminin anlaşılması ve aşama 2 tetkiki planlaması için odaklanmanın sağlanmasıdır.
Aşama 1 denetiminde aşağıdaki hususlar yerine getirilir;

- Müşterinin yönetim sisteminde dokümante edilmiş bilgiyi gözden geçirmek,
- Müşteri mahallini ve sahaya özgü koşulları değerlendirmek ve Aşama 2 tetkikine 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 standart 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 tetkikine yönelik kaynak tahsisinin gözden geçirmek ve Aşama 2 tetkikinin 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 tetkikinin planlanmasına odaklanmak,
- İç tetkiklerin ve yönetimin gözden geçirmesinin planlanıp planlanmadığı ve gerçekleştirilip gerçekleştirilmediğinin değerlendirilmesi ve uygulanan yönetim sisteminin uygulama seviyesi ile müşterinin Aşama 2 tetkiki için hazır olup olmadığını değerlendirmek. Belgelendirme kapsamında yönetim sistemi ile ilgili en az bir yönetimin gözden geçirme ve iç denetim gerçekleştirmemiş kuruluş belgelendirilmez.

  BGYS denetimlerinde ayrıca;
  - ISO 27001 tarafından istenen BGYS tasarımında kullanılan dokümanların elde edilmesi
  - Kuruluşun Aşama 2 denetimine hazır olup olmadığını ölçmek için bilgi güvenliği politikası ve hedefleri, risk analizi ve değerlendirmesi (belirtilen kontroller dahil), kuruluş bağlamına göre BGYS tasarımını anlamak

Aşama 1 denetimi kuruluşun yönetim sistemini uygulamaya başlamasından en erken iki ay sonra gerçekleştirilebilir.
Kalite ve Çevre Yönetim sistemi Aşama 1 denetimi, kuruluş sahasında ya da masa başında yapılabilir. Bu durum TÜRKAK R 40.05 rehberindeki NACE kodlarına göre belirlenen risk faktörü tablosu çerçevesinde belirlenir. Her iki durum içinde yukarıda belirtilen hususlar dikkate alınır. Bilgi güvenliği yönetim sistemi aşama 1 denetimler mutlaka kuruluş sahasında gerçekleştirilir.
Aşama 1'in amaçlarının karşılanması ve Aşama 2 için hazırlıkla ilgili dokümante edilmiş sonuçlar (Aşama 2 tetkiki esnasında uygunsuzluk olarak sınıflandırılabilecek) müşteriye bildirilir. Aşama 1 denetimi sonuçunda rapor hazırlanır. Aşama 2 denetiminin yürütülmesi kararı ve aşama 2 denetim ekibi yeterliliği için uygunluk değerlendirmesi için Belgelendirme komitesi tarafından gözden geçirilir.
1. ve 2. asama denetimi arasındaki süre, müşterinin ihtiyaçları ve gerekli çözümleri bulmak için zaman ihtiyacı esas alınarak belirlenir.
Aşama 1 denetimi ile Aşama 2 denetimi arasındaki süre Aşama 1 denetimindeki sonuçlara bağlı olarak belirlenir. Bu süre 6 ayı geçemez.
Aşama 1'de bulunan uygunsuzluklar ile ilgili olarak gerçekleştirilecek düzeltici faaliyetler, belgelendirme denetimi/ Aşama 2 öncesinde tamamlanmalıdır. Düzeltici faaliyetlerin gerçekleştirildiği doğrulanmadan belgelendirme/ Aşama 2 denetimi yapılmaz.
Aşama 1 denetimi sonrasında denetim raporu müşteri kuruluşa gönderilir. Cicert, müşteri kuruluşunu, aşama 2 tetkiki sırasında detaylı inceleme için gerekli olabilecek daha fazla farklı türde bilgi ve kayıt hakkında bilgilendirecektir.

Cicert, Aşama 2 için düzenlemelerini revize etme ihtiyacı da duyabilir. Yönetim sistemini etkileyecek önemli değişiklikler olursa, Cicert tamamının veya Aşama 1'in tekrarını değerlendirecektir. Müşteri, Aşama 1'in sonuçlarının Aşama 2'yi ertelemeye veya iptal etmeye yol açabileceği konusunda bilgilendirilir.

Aşama 2 Denetimi;
Aşama 2 denetimin amacı, müşterinin yönetim sisteminin etkinliği de dahil olmak üzere uygulamalarının yeterliliğinin ölçülmesidir. Aşama 2 denetimi, kuruluşun bütün alanlarında yapılır. Ancak kuruluş çoklu alan özelliği gösteriyor ise denetim, Çoklu Alan Denetim Talimatı doğrultusunda gerçekleştirilir. Aşama 1 tetkik raporunda dokümante edilmiş bulgulara dayalı olarak, Cicert, aşama 2 tetkikinin yürütülmesi için taslak bir tetkik planı hazırlar ve müşterisine gönderir.

Aşama 2 denetiminde aşağıdaki hususlar yerine getirilir;

- Uygulanabilir yönetim sistem standardı veya diğer hüküm ifade eden dokümanların şartlarına uygunluk hakkındaki bilgi ve kanıt,
- Kilit performans hedefleri ve amaçlarına yönelik (uygulanabilir yönetim sistem standardı veya diğer hüküm ifade eden dokümanlarındaki beklentilerle tutarlı) performansın izlenmesi, ölçülmesi, kayıt altına alınması ve gözden geçirilmesi,
- Müşterinin yönetim sistemi kabiliyeti ve uygulanabilir statüsel, düzenleyici ve sözleşme şartların karşılanması ile ilgili performansı,
- Kuruluş proseslerinin operasyonel kontrolü,
- İç tetkik ve yönetimin gözden geçirmesi, (yılda en az bir kez)
- Kuruluş politikaları için yönetimin sorumluluğu,

Bilgi Güvenliği Yönetim sistemi denetimlerinde yukarıdakilere ek olarak;

- Müşteri kuruluşun kendi politikaları, hedefleri ve prosedürlerine bağlı kaldığının teyit edilmesi,
  Bunu yapmak için, tetkik sırasında, müşteri kuruluşu ile ilgili olarak aşağıdakilere odaklanılır:
  a) müşteri kuruluşun politika ve hedeflerini ile ilgili üst yönetimin liderliği ve taahhüdü
  b) ISO/IEC 27001'de istenen dokümantasyon şartları
  c) Bilgi güvenliği ile ilgili risklerin değerlendirilmesi ve değerlendirmenin karşılaştırılabilir ve tekrarlanabilir sonuçlar üretmesi,
  d) Kontrol amaçlarının ve risk değerlendirme ve risk işleme proseslerine dayanan kontrollerin seçimi,
  e) BGYS'nin etkinlik gözden geçirmeleri ve bilgi güvenliği kontrollerinin etkinliğinin ölçümleri, raporlama ve BGYS amaçlarının gözden geçirilmesi,
  f) Seçilmiş ve uygulanmış kontroller, Uygulanabilirlik bildirgesi ve risk değerlendirme ve risk işleme prosesinin sonuçları ve BGYS politikası ve amaçlarının aralarındaki ilişki,
  g) Kontrollerin uygulanıp uygulanmadığına ve belirtilen amaçları sağlayacak şekilde etkin olup olmadığını belirlemek için, kuruluş tarafından bilgi güvenliği prosesleri ve kontrolleri izleme, ölçme ve analiz etme, iç ve dış bağlam ve ilgili riskleri ele alarak kontrollerin uygulanması,
  h) Programlar, prosesler, prosedürler, kayıtlar, iç tetkikler ve BGYS etkinliğinin gözden geçirmelerinin yönetim kararları ve BGYS politikaları ve hedeflerine izlenebilir olmalarının sağlanması.

Bilgi Güvenliği Yönetim sistemi Denetimleri için Cicert;

a) Müşteri kuruluşun bilgi güvenliği ile ilgili risklerin değerlendirmesinin, müşteri kuruluşun faaliyeti için uygun ve yeterli olduğunu göstermesini şart koşar.

b) Müşteri kuruluşun varlıklara yönelik bilgi güvenliği ile ilgili tehditlerin, açıklıkların ve etkilerin tespit edilmesi, incelenmesi ve değerlendirilmesi için prosedürlerin ve bunların uygulama sonuçlarının müşteri kuruluşun politikası, hedefleri ve amaçları ile tutarlı olup olmadığını teyit eder.

Cicert, önem analizinde kullanılan prosedürlerin mantıklı olduğunu ve doğru şekilde uygulandığını da denetler. Müşteri kuruluşunda, varlıklara yönelik bir bilgi güvenliği ile ilgili tehdit, bir zafiyet veya etki önemli olarak tespit edilir ise, BGYS dâhilinde yönetir

Yasa ve düzenleyicilerle uyumluluğun sürdürülmesi ve değerlendirilmesi müşteri kuruluşun sorumluluğudur. Cicert, BGYS'nin bu yönde işlediğine dair güven oluşturmak için kontroller ve örneklerle kendisini garanti altına alır.

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

İlk Belgelendirme Denetiminin Sonuçları;

Denetim ekibi aşama 1 ve aşama 2 denetiminde toplanan tüm bilgi ve objektif deliller denetim bulgularını gözden geçirmek ve denetim sonucuna karar verebilmek için değerlendirir.

Majör Uygunsuzluklar ile ilgili düzeltici faaliyetler yerine getirilmeden ve takip denetimi yapılarak doğrulanmadan ve/veya doküman ve kayıtların incelenmesi ile de kontrol edilmeden belge verilmesi yönünde tavsiye kararı alınamaz.

Minör uygunsuzlukların giderilip giderilmediği takip eden bir sonraki denetimde yerinde kontrol edilerek doğrulaması yapılır. Her bir minör uygunsuzluk için etkin bir düzeltme-düzeltici faaliyet planlanması durumunda belge verilmesi yönünde tavsiye verilir.

Gözlemler belgelendirme tavsiyesi yapılmasına engel değildir.

Uygunsuzlukların kapatılmasına müteakip baş denetçi denetim dosyasını belgelendirme komitesine iletir. Takip denetim kararı tavsiyesi verilmiş ise takip denetiminin yapılması ile ilgili karar için rapor Belgelendirme komitesine iletilir.

İlk Belgelendirme Kararının Verilmesi;

Denetim ekibi tarafından denetim bilgileri (Denetim raporları, varsa uygunsuzluklar ve bunlar ile ilgili müşteri tarafından gerçekleştirilen düzeltme ve düzeltici faaliyetler, Başvuru aşamasındaki bilgilerin teyidi, denetim amaçlarına ulaşıldığının teyidi ve herhangi bir şart veya gözlemle birlikte, belgelenin verilip verilmemesine ilişkin tavsiye) belgelendirme kararı alınabilmesi için Cıcert'e ulaştırılır.

Belgelendirme ile ilgili tüm kararlar Cıcert tarafından atanmış Belgelendirme Komitesi tarafından alınır. Belgelendirme Komitesi denetim bulgularını ve sonuçlarını ve varsa ilgili diğer bilgileri değerlendirerek son kararı verir.
Aşama 2'de bulunan majör uygunsuzluklar ile ilgili olarak gerçekleştirilecek düzeltici faaliyetlerin gerçekleştirildiği doğrulanmadan belgelendirme yapılmaz. Minör uygunsuzluklar için planlanan faaliyetler uygun bulunursa bir sonraki denetimde yerinde doğrulanmak üzere belgelendirme kararı alınır.

Belgelendirme kararı, yukarıda tanımlanan gerekliliklere ve denetim raporunda yer alan denetim ekibi belgelendirme tavsiyesi üzerine verilir.Belgelendirme kararını alan Cicert Belgelendirme Komitesi, normal olarak tetkik ekibinin olumsuz bir tavsiyesini geri çevirmemesi esastır. Bu tür bir durum gerçekleşir ise, belgelendirme kuruluşu tavsiyenin geri çevrilmesi kararının temelini yazılı hale getirmeli ve gerekçelendirmelidir.

Yönetimin gözden geçirmesi ve YS iç denetimleri için düzenlemelerin yapılmadığı, etkin olduğu ve sürdürüleceğinin gösterilmesine dair yeterli delil olmadığı sürece, müşteri kuruluşla belgelendirme yapılmaz.

Bölüm 2-Belgenin Sürdürülmesi
Gözetim Faaliyetleri
Gözetimin amacı, onaylanmış YS'nin uygulamasının sürdürüldüğünün doğrulanması, müşteri kuruluşun işletimindeki değişikliklerin sonucunda başlatılan sistemdeki değişikliklerin sonuçlarının dikkate alınması ve belgelendirme şartları (ilgili standart) ile sürekli uyumluluğun sahada doğrulanmalıdır.
Cıcert, belgeli kuruluşların yönetim sistemi kapsamına giren alanları, fonksiyonları ve kuruluşta ve yönetim sisteminde oluşabilecek değişiklikleri düzenli olarak takip edilmek her yıl gözetim denetimi uygular. Gözetim Denetimlerinin sayısı kuruluş talebi, ulaşan müşteri şikâyetleri, gözetim denetimi sırasında bulunan uygunsuzluğun derecesine göre veya denetim ekibinin belirttiği şekilde artırılabilir. Gözetim tetkiklerinin sıklığı belirlenirken, mevsim veya yönetim sistemleri belgelendirmesinin belirli bir süre için olması (örneğin, geçici inşaat alanı gibi) gibi hususları dikkate alınır.
Gözetim denetimleri için Kuruluşlardan gelen erteleme talepleri Belgelendirme Komitesi tarafından değerlendirilerek mücbir durumlar için (örneğin sezonluk ürün/hizmetlerde, doğal afetler, genel ekonomik kriz vb. durumlarda) en fazla 6 aya kadar erteleme yapılabilir. Belirtilen durumlar haricindeki erteleme talepleri, Sistem Belgelendirme Müdürü tarafından değerlendirilerek maksimum (1) bir ayı geçmeyecek şekilde ertelenir. Erteleme durumunda yapılan gözetim denetimine ait tarih bir sonraki tetkik tarihini bağlamaz.
Gözetim denetimi, belgelendirilmiş kuruluşun belgelendirilen Standard şartlarının yerine getirilip getirilmediğinin doğrulanması amacı ile müşteri sahasında gerçekleştirilir. Ayrıca aşağıdakileri de içerebilir;

- Müşteriye belgelendirme ile ilgili hususlar hakkında sorular sorulmasını,
- Müşterinin işlemleri hakkında beyanlarının gözden geçirilmesini (promosyon malzemeleri, web sayfası gibi),
- Müşteriden dokümanların ve kayıtların (kâğıt ve elektronik ortamda) sağlamasının istenmesi,
- Belgelendirilmiş müşterinin performansının diğer yollarla izlenmesini.

Gözetim Denetimi;
Bir belge kullanma döneminde (3 yıl) en az 2 gözetim denetimi Kuruluş sahasında yapılır. Fakat sistemin tümüyle denetimini gerektirmez. Bu süre içinde referans standardın tüm maddeleri en az 1 kez incelenir. İnceleme yönetim sisteminin tümünü veya bölümlerini kapsayabilir. Her gözetim denetiminde belgelendirilmiş yönetim sistemi standardının şartlarını karşıladığına olan güven sürdürülmelidir.

Gözetim denetiminde aşağıdaki hususlar yerine getirilir.

- Kuruluş, referans standardın Yönetimin Gözden Geçirmesi ve İç Denetim maddeleri ile ilgili uygulamalarını yılda en az bir kez yapmakla yükümlü olup, Denetim Ekibine bu uygulamalara ait kayıtları Gözetim Denetimlerinde ibraz etmek zorundadır,
- Bir önceki denetimde tespit edilmiş ve yerinde doğrulama yapılmadan kapatılmış uygunsuzlukların yerinde doğrulaması,
- Şikâyetlerin ele alınması,
- Kuruluşun amaçlarının gerçekleştirmesi ve ilgili yönetim sisteminin/sistemlerinin amaçları bakımından yönetim sisteminin etkinliğini,
- Sürekli iyileştirmede amaçlanan planlı faaliyetlerdeki gelişmeler,
- Sürdürülen operasyonel kontrol,
- Sistemdeki her değişikliğin gözden geçirilmesi
- Marka kullanımı/belgelendirmeye yapılan atıflar,
- Düzeltici ve önleyici faaliyetler olmak üzere sistemin sürdürülmesine yönelik unsurlar,
- Değişikliğe tabi olan alanlar,
- Yönetim Sistemi standardının seçilen unsurları,
- Seçilen diğer uygun alanlar.

BGYS denetimlerinde yukarıdakilere ek olarak;

- Bilgi güvenliği risk analizi ve kontroller, BGYS iç denetimi, YGG ve düzeltici faaliyetler gibi sistem elemanlarının gözden geçirilmesi
- ISO/IEC 27001 ve belgelendirme için gerekli olan diğer dokümanların gerektirdiği dış taraflarla olan iletişim
- BGYS'nin müşteri kuruluşun bilgi güvenliği politikasının amaçlarını başarmak doğrultusunda etkinliği,
- Periyodik değerlendirme için prosedürlerin işleyişi ve ilgili bilgi güvenliği yasa ve düzenlemeleri ile uyumluluğun gözden geçirilmesi,
- Belirlenen kontrollerdeki değişiklikler ve buna bağlı olarak SOA'daki değişiklikler
- Denetim programına göre uygulama ve kontrollerin etkinliği

Gözetim tetkikleri, yeniden belgelendirme yılı hariç her takvim yılında bir kez yapılır. İlk belgelendirmeden sonra yapılacak ilk gözetim tetkiki, belgelendirme tarihinden itibaren 12 ayı geçmemelidir. İlk gözetim denetimi tarihi, belgeli kuruluşun Aşama 2 denetim tarihinin son günü temel alınarak 12 ay içerisinde gerçekleştirilmelidir.
Denetimin gerçekleştirilmesi, raporlanması ve uygunsuzlukların kapatılması ve takibi Denetim Kılavuzunda belirtildiği şekilde gerçekleştirilir. Denetim dosyası Baş denetçi tarafından Cıcert iletilir.

Bir önceki denetimde tespit edilmiş ve yerinde doğrulama yapılmadan kapatılmış uygunsuzlukların yerinde doğrulaması, marka ve sertifika kullanımının kontrolü, gözetim denetimi sırasında gerçekleştirilir. Yerinde doğrulama sonucu uygunsuzluk bulunursa denetim ekibi tarafından uygunsuzluk raporunda majör uygunsuzluk olarak değerlendirilir ve kuruluş uygunsuzlukla ilgili takip denetimine bırakılır. Takip denetiminde, anlaşılan süre içerisinde yapılmaz ise, belgelendirme kapsamı daraltılacak veya belge askıya alınacak veya geri çekilecektir. Düzeltici faaliyetin uygulanması için izin verilen süre, uygunsuzluğunun ve belirli şartları karşılayan müşteri kuruluşun ürün ve hizmetlerinin güvencesine yönelik riskin şiddeti ile tutarlı olacaktır.

Gözetim tetkikleri esnasında, Cicert daha önceden gelen itiraz ve şikâyet ve herhangi bir uygunsuzluk veya belgelendirmenin şartlarını karşılayamama durumu varsa, müşteri kuruluşun kendi YS'ni ve prosedürlerini araştırarak ve uygun düzeltici faaliyetleri gerçekleştirdiğine dair kayıtları kontrol eder.
Gözetim raporları, özellikle daha önce belirlenen uygunsuzlukların giderildiğine dair bilgileri içermelidir.

Belgenin Sürdürülmesi Kararının Verilmesi;
Belgenin sürdürülüp sürdürülmemesi kararı gözetim denetim dosyasının Belgelendirme Komitesi tarafından incelenmesi sonucu verilir. Belgeli kuruluşun yönetim sistem Standard şartlarını sürekliliğinin yerine getirilip getirilmediği kontrol edilir.
Denetim sonucuna göre belgenin askıya alınması, kapsamın daraltılması veya geri çekilmesi söz konusu olabilir. Uygunsuzlukların, belirtilen tarih aralıkları içerisinde kapatılamaması (bir önceki denetimde bulunan minör uygunsuzlukların kapatıldığının doğrulanamaması) durumunda kuruluşun belgesi Belgelendirme Komitesinin kararı ile askıya alınır. Kuruluşa durum yazı ile bildirilir.
Majör uygunsuzlukları belirtilen tarih aralıklarında kapatan kuruluşların belgelerinin geçerliliklerinin devamına belgelendirme komitesi tarafından karar verilir.
Minör uygunsuzluklar için kuruluş tarafından planlanan düzeltme ve düzeltici faaliyet planları yeterli bulunması durumunda belgenin devamlılığına karar verilir.

Belge Yenileme

Belge Yenileme Denetiminin Planlanması;
Belge yenileme denetimleri ilgili yönetim sistem Standard şartlarının karşılandığının sürekliliğini takip etmek amacıyla planlanır ve gerçekleştirilir. Belge Yenileme denetiminin amacı yönetim sisteminin uygunluğunun ve etkililiğinin bir bütün olarak devam ettirildiğini ve belgelendirme kapsamı için ilginin ve uygulanabilirliğin sürdürüldüğünü teyit etmektir.
Belge Yenileme denetimleri, önceki gözetim denetim raporlarının gözden geçirilmesinde dâhil olmak üzere belgelendirme periyodu boyunca yönetim sistem performansının değerlendirmesini kapsar.
Belge Yenileme faaliyetlerinde, yönetim sisteminde, müşteride veya yönetim sisteminin çalıştığı kapsamda (mevzuattaki değişiklikler gibi) önemli bir değişiklik olduğunda, ayrı bir Aşama 1 tetkiki gerekebilir. Bu durum Cicert tarafından belge yenileme denetimi öncesi incelenerek raporlanır.
Her belge Yenileme öncesi bölüm 1'de anlatıldığı gibi başvuru tekrar alınarak değerlendirilir ve denetim planlaması yapılır.
Çoklu saha denetimleri veya birden çok yönetim sisteminin belgelendirilmesi durumunda, etkin bir denetim yapılabilmesi için Denetim Sürelerinin Belirlenmesi Talimatı ve Çoklu Alan Denetimleri Talimatına göre denetim süresi hesaplanır ve uygulanır.
Belge yenileme denetimi, sistem belgesinin geçerlilik süresi (3 yıl) sona ermeden kuruluşları yeniden belgelendirmek için yapılan denetimlerdir. İlk belgelendirme denetimi ve yeniden belgelendirme denetimi arasındaki veya iki yeniden belgelendirme denetimi arasındaki zaman aralığı 3 yılı geçmemelidir. Kuruluş, burada belirtilen süreler içerisinde cevap vermez ya da belge devamını talep etmez ise, belge geçerlilik süresi sonunda belge geçerliliğini kaybeder.

Belge Yenileme Denetimi;
Belge yenileme denetimleri kuruluşun sahasında gerçekleştirilmeli ve denetiminde aşağıdaki hususlar yerine getirilir.

- iç ve dış değişiklikleri ve belgelendirme kapsamı devamlı olarak uygunluğu ve uygulanabilirliği ışığında bütünüyle yönetim sisteminin etkinliğini
- Toplam performansını arttırmak için yönetim sisteminin etkinliğinin ve iyileştirilmesi korunması için kararlılık
- Belgelendirilmiş müşterinin amaçlarına ulaşma ve ilgili yönetim sistemi/ sistemlerinin amaçlanan sonuçları bakımından yönetim sisteminin etkinliğini
- Marka ve Logo kullanımı uygunluğu

Belge yenileme denetimi, Belge Bitiş süresine 2-3 ay kala gerçekleştirilir. Böylece denetim sırasında ortaya çıkabilecek uygunsuzluklar için kuruluşa düzeltme ve düzeltici faaliyetleri gerçekleştirecek bir zaman bırakılır. Cicert, belgenin geçerlilik süresinden önce, yeniden belgelendirme tetkikini tamamlayamazsa veya herhangi bir majör uygunsuzluk için düzeltme ve düzeltici faaliyetin yerine getirildiğini doğrulayamazsa, yeniden belgelendirme önerilmez ve belgenin geçerliliği uzatılmaz. Müşteri bilgilendirilir. Ancak, haklı gerekçe belirtmek koşulu ile belge geçerlilik süresi bitimi tarihinden itibaren 6 ay içerisinde belge yenileme denetimi yapılabilir. Aksi takdirde en azından bir Aşama 2 yapılır.
Denetimin gerçekleştirilmesi, raporlanması ve uygunsuzlukların kapatılması ve takibi Denetim Kılavuzunda belirtildiği şekilde gerçekleştirilir. Denetim dosyası Baş denetçi tarafından Cıcert iletilir.
Düzeltici faaliyetin uygulanması için izin verilen süre, uygunsuzluğunun ve bilgi güvenliği riskinin şiddeti ile tutarlı olmalıdır.

Belge Yenileme Kararının Verilmesi;
Belge Yenileme Kararı Belgelendirme Komitesi tarafından denetim raporlarının incelenmesi, belgelendirme periyodu boyunca sistem gözden geçirme sonuçları ve gelen şikâyetlerin değerlendirilmesi sonucu verilir.

Transfer Denetimleri;
IAF MLA üyesi olan bir akreditasyon kurumu tarafından akredite edilmiş başka bir belgelendirme kuruluşu
tarafından verilen yönetim sistem belgesinin CIcert'e transferinin sağlanması için yapılan denetimlerdir. Belge geçişinin transfer denetimi statüsünde değerlendirilmesi aşağıdaki koşullara bağlıdır.

- Transfer denetimi yapılabilmesi için belgenin halen aktif olması gerekir. Askıda bulunan belgeler için transfer denetimleri gerçekleştirilemez.
- Transfer denetimlerinin gerçekleştirilmeden önce kuruluş tarafından daha önceki belgelendirme firması tarafından bildirilen uygunsuzlukların kapatılmış olması gerekir.
- Transfer başvurusu yapan kuruluşun son denetim tarihi transfer denetim tarihinden en fazla 12 ay önce gerçekleştirilmiş olmalıdır.

Transfer denetimi başvuruları, belgelendirme denetimindekine benzer şekilde yapılır. Belgelendirme denetimi öncesi istenilen dokümanlara (kalite el kitabı, prosedür vb.) ek olarak diğer belgelendirme kuruluşunda gerçekleşen tüm denetimlere ait raporlar (herhangi bir uygunsuzluğa uygulanan düzeltici faaliyetlere ait raporlar ve dokümantasyon gibi yeterli kanıtlar) incelenir.
Belgelendirme öncesi aşağıda belirtilen konular incelenir.

- Kuruluşun transfer sebebi
- Gerçekleştirilmiş son denetim süre ve tarihleri
- Kuruluş kapsamının CIcert kapsamına uygunluğu
- Belgenin doğruluğu, geçerliliği, belge üzerindeki adreslerin ve istenilen adreslerin belgelendirme kapsamında olup olmadığı ve geçerliliği,
- Halen kapatılmamış uygunsuzlukların durumu ve mümkünse kapatılan uygunsuzlukların daha önceki belgelendirme kuruluşu tarafından doğrulanması
- Önceki denetim raporları ve gözlemler
- Elde edilen bilgiyi esas alarak, var olan tetkik programındaki herhangi bir değişikliği ve önceki uygunsuzluklarla ilgili düzeltici faaliyetlerin takibini doğrular ve ***"Başvurunun Gözden Geçirilmesi Formu"*** na kayıt eder.
- Alınan şikâyet ve gerçekleştirilen faaliyetler.
- Yasal mercilerle herhangi bir anlaşmazlığın mevcudiyeti

Transfer denetiminde Aşama 1 denetimi uygulanmaz. Tüm Denetimler Cıcert ***"Başvurunun Alınması ve Denetim Faaliyetleri Prosedürü"*** doğrultusunda denetim kılavuzuna uygun olarak planlanır ve gerçekleştirilir. Transfer denetimi sonrası alınacak belgelendirme kararı ***"Belgelendirme Kararlarının Alınması Prosedürü"*** ne göre gerçekleştirilir. Belge periyodu önceki belgelendirme kuruluşunun vermiş olduğu belge yayın tarihinden son kullanma tarihine kadardır.

Takip Denetimleri
Denetimler esnasında ortaya çıkan majör uygunsuzlukların giderilmiş, bunlara ilişkin düzeltici faaliyetlerin etkin bir şekilde uygulanmakta olduğunun belirlenmesi amacıyla gerçekleştirilen ilave tam denetim veya ilave sınırlı denetimlerdir.

Entegre Denetimler;
Kalite Yönetim Sistemi(KYS), Çevre Yönetim Sistemini(ÇYS) ve Bilgi Güvenliği Yönetim Sistemini (BGYS) paralel yürüten kuruluşlarda aşağıda belirtilen bir veya daha fazla şart mevcut olduğunda gerçekleştirilen eş zamanlı denetimlerdir. Entegre

Denetimler Cıcert ***"Başvurunun Alınması ve Denetim Faaliyetleri Prosedürü"*** doğrultusunda denetim kılavuzuna uygun olarak planlanır ve gerçekleştirilir.
Organizasyonun entegrasyon seviyesi aşağıdaki kriterler bazında değerlendirilir.

- Tüm iş stratejisi ve planı içeren yönetim Gözden geçirme,
- Entegre iç denetimler (İç denetçiler her iki standart da kalifiye olmuş denetçiler tarafından yürütülmeli),
- Entegre Politika ve hedefler
- Entegre proses yaklaşımı
- İş talimatlarını da içeren entegre dokümantasyon
- Entegre iyileştirme mekanizması (Düzeltici ve Önleyici faaliyetler; ölçme ve sürekli iyileştirme)
- İşletme çapında risk yönetimi yaklaşımları iyi kullanımı ile entegre planlama yaklaşımı
- Entegre Yönetim desteği ve Sorumlulukları

Değişiklik Kaynaklı Denetimler
Kuruluşun Kapsam değişikliği, Şube veya tesis eklenmesi, adres değişikliği veya diğer büyük çapta değişikler veya belgelendirmesinin temelini etkileyebilecek diğer değişikliklerinden dolayı ile gerçekleştirilen denetimlerdir. Değişiklik talebi kanıtları doğrultusunda gözden geçirilir. Yönetim sistemi yapısını etkilemeyecek yasal ve ticari değişiklikler söz konusu ise denetim gerektirmez ve Belgelendirme Komitesinde değerlendirilir. Denetim gerektiren durumlarda faaliyetler, değişiklik mahiyetini kapsayacak şekilde yürütülür. Denetim raporları, Belgelendirme Komitesi tarafından değerlendirilir. Belge değişikliklerinde kuruluşun mevcut belge geçerlilik süresi değişmez.

Özel Denetimler
Kapsam Genişletme;
Kapsam genişletme talepleri yazılı olarak veya başvuru formunun doldurulması ile alınır. Cıcert, hâlihazırda verilmiş olan belgelendirmenin kapsamına yönelik bir genişletme başvurusuna cevaben, başvurunun gözden geçirmesini yapar ve genişletmenin yapılıp yapılamayacağına karar vermek için gerekli tetkik faaliyetlerini belirler. Kapsam genişletme denetimleri gözetim denetimleri ile birlikte yapılabilir.
Kapsam değişikliği denetimi, kuruluşun yönetim sisteminin, talep ettiği yeni kapsam doğrultusunda, referans standardın ilgili maddelerinin uygulamalarının incelenmesidir.
Kapsam değişikliği denetimlerinde, kapsama ilave edilecek ilgili standart maddeleri Baş Denetçi tarafından incelenir.

Kısa Süreli Haberli Denetim;
Kısa süreli haberli denetim, Belgelendirilmiş müşterilerin şikâyetlerinin araştırılması, yönetim sistem standardı veya belgelendirme kuruluşun kurallarında değişiklik olması durumunda veya askıya almanın kaldırılmasını takip için gerçekleştirilebilir.
Kısa süreli haberli denetimin kapsamı ile doğru orantılı olarak Belgelendirme Müdürü tarafından denetimin nasıl gerçekleştirileceğine karar verilir.
Bu tür denetimlerde kuruluşun mevcut durumu değiştirmesine imkân vermeyecek bir süre önce (en fazla 2 gün önce) kuruluşa haber verilir ve denetim gerçekleştirilir.
Denetimi gerçekleştirecek denetim ekibi atanırken Belgelendirme Müdürü bir önceki denetim ekibinden farklı ve şikâyet konusunu yorumlayabilecek yeterlilikte bir denetim ekibini görevlendirir.
Kuruluşun denetimi kabul etmemesi halinde belgesi belgelendirme komitesi kararı ile askıya alınır ve durum kuruluşa yazı ile bildirilir.

Askıya Alma, Geri Çekme ve Kapsam Daraltma

CIcert, kuruluşun yönetim sistem belgesi kullanımını, Belgelendirme Komitesi'nin kararına göre, belirli bir süre için askıya alabilir. Belgenin askıda kalma süresi en fazla 6 aydır. Belgelendirilen kuruluşun verilen süre içerisinde sorunları çözememesi durumunda kuruluşun belgesi belgelendirme komitesi tarafından iptal edilir ya da kapsamı daraltılır.
Askıya alma nedenleri;

- Kuruluşun belgelendirilmiş yönetim sistemi sürekli veya ciddi olarak, yönetim sisteminin etkinliği için gereklilikleri de dahil olmak üzere, sertifikasyon gereklilikleri karşılamada başarısız olması.
- Kuruluşun gözetim denetimini veya belge yenileme denetimini belirlenen periyotlar dahilinde kabul etmemesi
- Kuruluşun kendi isteği,
- Kuruluşun sözleşme hükümlerini yerine getirmemesi

Kuruluş, belgenin askıya alınma kararının tebliğinden itibaren belge ve logo kullanımını durdurur. Askıya alma süresince, kuruluş belgeye ait haklardan faydalanamaz. Askıya alınma durumunda, müşterinin yönetim sistemi belgesi geçici olarak geçersizdir. CIcert belgenin askıya alınmasına dair kararları web sitesinde yayınlama hakkına sahiptir. Bu nedenle askıya alınan belgelendirme durumunu web sitesi aracılığı ile kamunun erişimine açar.
Askı süresi boyunca kuruluş problemlerini çözemez ise Cıcert tarafından belge iptal edilebilir veya kapsam daraltılabilir.
Belgenin askıya alınma nedeninin giderildiği (denetimlerde, doküman inceleme ile vb.) kanıtlandığında, Belgelendirme Komitesi kararı ile belge askıdan kaldırılır.

Kuruluş belgelendirme kapsamının bir kısmı için belgelendirme şartlarını karşılamada devamlı veya ciddi başarısızlık gösterdiğinde, Cıcert, kuruluşun belgelendirme kapsamını, şartları karşılamayan kısım dışarıda kalacak şekilde daraltır. Bu tip bir daraltma, belgelendirme için kullanılan standardın şartlarıyla uyumlu olmalıdır. Belgelendirme kapsamı daraltıldığında, buna göre bütün reklam malzemeleri kuruluş tarafından değiştirilmelidir.
Kuruluşun yönetim sistem belgesinin kullanımına dair sözleşmesi, Cıcert Belgelendirme Komitesi'nin kararına göre iptal edilebilir.
Sözleşmenin iptali ve belgenin geri alınmasının nedenleri;

- Verilen askı süresi sonuna kadar kuruluşun denetimin gerçekleştirilmesine müsaade etmemesi
- Askıya alınma gereklerini yerine getirmemesi (ödeme, marka kullanımı, belge kullanımı, vb)
- Askı halinin kaldırılması için gerçekleştirilen faaliyetlerde (denetim, doküman inceleme vb) kuruluşun uygunsuzluklarını öngörülen sürelerde kapatmaması,
- Kuruluşun iflası veya belge kapsamındaki faaliyete son vermesi,
- Kuruluşun, yönetim sistem belgesini kapsamında belirtilen ürün veya hizmetten farklı alanlarda kullanması,
- Kuruluşun denetimler sırasında eksik, yanıltıcı ve/veya gerçeğe aykırı bilgi vermesi,
- Belgenin yanıltıcı ve haksız kullanımı,
- Cıcert tarafından tahakkuk ettirilen ücretlerin fatura edilmesini takip eden 15 gün içerisinde ödenmemesi,
- Belgenin geçerlilik süresi içinde, yapılan denetimlerde kuruluşun yönetim sisteminin uygunluğunu tamamen yitirdiğinin tespit edilmesi,
- Kuruluşun belgede belirtilen tesis adresinde bulunmaması,
- Kuruluşa ait tüzel kişiliğin değişmesi,
- Kuruluşun belge ve ekleri üzerinde tahrifat yapması,
- Herhangi bir sebepten dolayı Kuruluşun, Cıcert tarafından bildirilen gözetim/takip denetim tarihini süre belirtilmeksizin erteleme talebinde bulunması veya gözetim/takip denetiminin iptali talebinde bulunması,
- Kuruluş talebi

Belgenin iptal kararının tebliğinden itibaren kuruluş, belge, belgeye atıfta bulunan her türlü doküman ve tanıtım malzemesi ve logo kullanımını durdurmakla yükümlüdür. Cıcert belgenin geri alınması ve sözleşmenin feshine dair kararları web sitesinde yayınlama hakkına sahiptir. Bu nedenle iptal edilen belgelendirme durumunu web sitesi aracılığı ile kamunun erişimine açar.
Kuruluş, tebliğ tarihinden itibaren en geç 15 gün içerisinde belgenin orijinalini Cıcert'e iade etmek ve imzalanan Sözleşmeden kaynaklanan tüm mali ve hukuki yükümlülüklerini yerine getirmekle sorumludur.
Sözleşmesi ve belgesi iptal edilen kuruluşların yeniden başvuruları en az 30 gün sonra işleme alınabilir. Yeniden başvuru yapıldığında ilk müracaattaki belgelendirme işlemleri uygulanır.

Bölüm 3- İtirazlar

İtirazlar, CIcert "***İtiraz ve Şikayetlerin Ele Alınması Prosedürü"*** doğrultusunda ele alınır. İtiraz ile ilgili form ve prosedürlere www.cicert.com.tr sitesinden ulaşılabilir. Cıcert itirazları ele almanın bütün seviyelerindeki bütün kararlardan sorumludur.
Herhangi bir kişi ya da kuruluş tarafından yapılan itirazlar İtiraz/Şikayet Değerlendirme Formu ile kayıt altına alınır. İtiraz, söz konusu karar tebliğ tarihinden itibaren 30 gün içerisinde yazılı olarak yapmalıdır.
Gelen tüm itirazlar niteliği açısından değerlendirilir ve CIcert itiraz komitesine iletilerek gerekli bilgilendirme yapılır. Değerlendirmeyi ve faaliyetleri gerçekleştiren kişilerin şikâyete veya itiraza konu olan hususlara dâhil olmayan kişilerden (denetim yapan veya belgelendirme kararı alan) olması sağlanır.
İtirazların kabulü, soruşturması ve kararı, itiraz edene karşı ayrımcı bir uygulamaya yol açmaz. İtiraz başvurusunun yapılmasından sonra Cıcert, itirazın alındığını, ilerleme raporlarını ve sonucu ile ilgili itiraz sahibine bilgilendirme yapar.

Bölüm 7- Şikâyetler
Şikâyetler, CIcert ***"İtiraz ve Şikayetlerin Ele Alınması Prosedürü"*** doğrultusunda ele alınır. Şikayet ile ilgili form ve prosedürlere www.cicert.com.tr sitesinden ulaşılabilir. Cıcert şikâyetleri ele almanın bütün seviyelerindeki bütün kararlardan sorumludur.
Herhangi bir kişi ya da kuruluş tarafından yapılan şikâyetler İtiraz/Şikayet Değerlendirme Formu ile kayıt altına alınır.
Gelen tüm şikayetler niteliği açısından değerlendirilir ve gerekli bilgilendirme yapılır. Şikayet belgelendirme faaliyetleriyle ilgiliyse şikayet Cıcert tarafından ele alınır. Şikayet, belgelendirilmiş bir müşteriyle ilgiliyse şikayetin sorgulanmasında belgelendirilmiş yönetim sisteminin etkililiği dikkate alınır ve belgelendirilmiş müşteriye yönlendirilir. Gelen şikayetler gizlilik prensipleri doğrultusunda değerlendirilir.
Gelen tüm şikayetler araştırılır ve geçerli kılmak için gerekli olan bütün bilgilerin toplanması ve doğrulanması sağlanır. Cıcert tarafında şikayetin alınmasından sonra her aşamada şikayet sahibine geri bildirimler yapılmaktadır.
Değerlendirmeyi ve faaliyetleri gerçekleştiren kişilerin şikâyete veya itiraza konu olan hususlara dâhil olmayan kişilerden (denetim yapan veya belgelendirme kararı alan) olması sağlanır.
Cıcert, şikayet konusu ve bunun çözümünün kamuoyuna verilip verilmeyeceği, verilecekse ne kapsamda verileceği konusunu, müşteri ve şikayet sahibi ile birlikte belirler.

Bölüm 8- Denetimlerin Gerçekleştirilmesi

Belgelendirme Denetimi ve diğer tüm denetimler, ***"Denetim Sürelerinin Belirlenmesi Talimatı"*** doğrultusunda planlanır. Eğer kuruluş birden fazla alanda faaliyet gösteriyorsa ***"Çoklu Alan Denetim Talimatı"*** dikkate alınır ve kuruluşa bilgisi verilir.
Tetkik ekibi, ***"Başvurunun Alınması ve Denetim Faaliyetleri Prosedürü"*** ve ***"Denetim Kılavuzu"*** çerçevesinde resmi olarak görevlendirilir ve uygun çalışma dokümanları ekibe sağlanır. Tetkikin planı ve tarihi konusunda müşteri kuruluşu ile mutabakata varılır. Tetkik ekibine verilen görev, açıkça tanımlanır, müşteri kuruluşu bununla ilgili olarak bilgilendirilir ve tetkik ekibinin müşteri kuruluşun yapısı, politikaları ve prosedürlerini incelemesi sağlanır. Bu hususların belgelendirmenin kapsamına uygun tüm şartları karşıladığını, prosedürlerin uygulandığını ve bu prosedürlerin müşteri kuruluşun YS'sine güven sağlayan mahiyette olduğunu teyit edilir.

Denetim Ekibinin veya taslak denetim planının kabul görmemesi durumunda, kuruluş nedenlerini yazılı olarak açıklar. Kuruluşun gerekçeleri değerlendirilir. Gerekçelerin haklı bulunması durumunda, Denetim Ekibinde değişiklik yapılır. Gerek duyulduğunda üzerinde anlaşma sağlanan denetim tarihleri de her iki tarafında talebiyle değiştirile bilinir.

Bilgi Güvenliği Yönetim sistemi denetimlerinde;

Cicert tetkik ekibi, tanımlanan kapsama sahip müşteri kuruluşun BGYS'sini uygulanabilir tüm belgelendirme şartlarına göre tetkik eder. Cicert, müşteri kuruluşun BGYS'nin kapsamının ve sınırlarının işin, kuruluşun, yerinin, varlıklarının ve teknolojisinin özellikleri açısından açıkça tanımlanması için başvuru formları kullanmaktadır. Cicert, müşteri kuruluşların BGYS'nin kapsamında, ISO/IEC 27001 şartları karşıladığını yapılan denetimler doğrulanır.

Cicert, müşteri kuruluşun bilgi güvenliği risk değerlendirmesi ve risk tedavisinin faaliyetlerini doğru bir şekilde yansıttığını ve BGYS standardı ISO/IEC 27001'de tanımlandığı üzere faaliyetlerinin sınırlarını kapsadığını denetimler doğrultusunda teyit eder. Böylece, Cicert, bu hususun müşteri kuruluşun BGYS'nin kapsamında ve Uygulanabilirlik Bildirgesinde ele alındığını onaylar.

Cicert, tam olarak BGYS kapsamında bulunmayan hizmet ya da faaliyetlerle olan bağlantı noktalarının, belgelendirmeye tabi BGYS kapsamında belirtilmesini ve müşteri kuruluşun bilgi güvenliği risk değerlendirmesinde yer almasını denetler. Örneğin, BT sistemleri, veri tabanları ve telekomünikasyon sistemlerinin başka bir organizasyonla ortak kullanımını gösterebiliriz.

Denetimler; açılış toplantısı, denetimin gerçekleştirilmesi, denetim ekibi değerlendirme toplantısı ve kapanış toplantısı aşamalarından oluşur ve denetim programına göre yürütülür.

Açılış Toplantısında; ISO/IEC 17021-1:2015 ve ISO 27006:2015 standartlarına uygun (denetimin amacı, kapsamı, kullanılacak metot ve prosedürler, taslak denetim programı, vb) konular görüşülür.

Denetimin gerçekleştirilmesi; kuruluş yönetim sisteminin müracaat edilen standarda, kapsama ve oluşturulan dokümantasyona göre kabul edilebilir bir şekilde uygulanıp uygulanmadığının teyidi için karşılıklı görüşmeler, dokümanların ve kayıtların örnekleme metoduyla incelenmesi, ilgili alanlarda çalışmaların ve şartların gözlemlenmesi suretiyle yapılır.
Denetim Ekibi, denetim sonucunda elde edilen bulguları denetim kriterleri ve referans dokümanlara göre gözden geçirir ve değerlendirir. Standard şartlarından ve kuruluş dokümantasyonundan kaynaklanan uygunsuzluklar tespit edilir ise her bir uygunsuzluğu tanımlayan ayrı ayrı uygunsuzluk raporu hazırlanır. Uygunsuzluk raporlarında tespit edilen uygunsuzluğun sınıfı belirtilir. Denetim Ekibi, uygunsuzlukları Majör (Büyük) ve Minör (Küçük) olmak üzere iki sınıfta değerlendirebilir. Ayrıca denetim ekibi gözlemlerini de raporlar.
Denetimi gerçekleştirmenin güçlüğü anlaşılırsa, baş denetçi bunun nedenlerini kuruluş Yönetim Temsilcisine bildirir ve denetimi durdurarak tutanak düzenler. Uygunsuzluk raporları kuruluş yönetim temsilcisi tarafından uygunsuzlukların kabul edildiğini göstermek üzere karşılıklı imzalanır. Kuruluşun imzadan imtina etmesi durumunda baş denetçi kendi imzası ile bir tutanak hazırlayarak denetim sonucu görüşünü ihtiva eden raporu Belgelendirme Komitesine sunar. Konuyla ilgili Belgelendirme Komitesi kararı, Başvuru Formunda belirtilen faks numarasına veya iadeli taahhütlü mektupla veya noter aracılığıyla Sözleşmesinde geçen adresine tebliğ edilir. Kuruluşun karara itirazı, takip eden 30 gün içerisinde yapılırsa itiraz değerlendirilmek üzere ilgili İtiraz Komitesine sunulur.
Denetimde tespit edilen uygunsuzluklara yönelik olarak kuruluşun gerçekleştireceği düzeltici faaliyetleri, kuruluş, 15 gün içinde sebep sonuç analizi ve düzeltici faaliyet planını içerecek şekilde uygunsuzluk raporu ile bildirmekle yükümlüdür.
Denetim raporlarındaki uygunsuzluklar için verilen düzeltici faaliyet süresi 3 aydan uzun tutulamaz.
Takip denetimi için kuruluşa verilen sürede (Maksimum 3 ay içinde) kuruluş hazırlıklarını tamamlayamaz ise belgelendirme komitesi kararı ile maksimum 3 ay daha süre verilir. Toplam 6 ay içerisinde uygunsuzlukların giderilmediği gözlenirse veya takip denetimi yapılması için teyit verilmez ise kuruluşun belgesi iptal edilir, eğer Aşama 2/Belge Yenileme denetimi ise yeniden gerçekleştirilir.
Düzeltme ve düzeltici faaliyetlerin etkinliğini doğrulamak için ilave bir denetimin veya dökümante edilmiş delilin gerekli olup olmayacağı Baş Denetçi tarafından uygunsuzluk raporu üzerinde Takip denetimi işaretlenerek belirtilir. Bu durumda rapor

hazırlanarak belgelendirme komitesine iletilir. Takip denetimi gerekli olması durumunda düzeltici faaliyetler, verilen termin süresi sonunda sahada yapılacak ilave bir tam denetim yâda ilave sınırlı bir denetim ile; Takip denetimi gerekli değil ise faaliyetlere yönelik beyan edilen dokümante edilmiş delillerin gözden geçirilmesi ile doğrulanır. Kuruluş tarafından gerçekleştirilen düzeltici faaliyetler etkin ve yeterli bulunmaz ise Baş Denetçi tarafından komiteye bu durum raporlar ile birlikte sunulur. Komite kararı ile ilave tetkik yapılmasına karar verilebilir. Bu durum müşteriye yazılı olarak bildirilir.

Kapanış Toplantısı, denetim sonunda, denetim ekibi ile kuruluşun üst yönetimi, yönetim temsilcisi ve/veya ilgili birimlerin sorumluları ile yapılır. Toplantıda baş denetçi tarafından denetimin olumlu ve/veya olumsuz sonuçları, varsa uygunsuzluk raporuna kaydedilen uygunsuzluklar anlaşılacak şekilde sunulur ve ISO/IEC 17021-1:2015 ve ISO 27006:2015 standartlarına uygun diğer konular görüşülür. Müşteri kuruluş için, bulgular ve dayanakları hakkında sorular sorabilmesi için bir fırsat sunulur.

Denetim ekibinin hazırladığı rapor son karar olmayıp Belgelendirme Komitesine görüş niteliğindedir. Belgelendirme Komitesi tarafından alınan karar gereği işlemler yerine getirilir. Kuruluşa, Belgelendirme Komitesinin onayından geçmiş denetim raporu gönderilir.

Bölüm 9- Belge ve Logoların Kullanımı

Başvuruda bulunan kuruluşun denetim sonucunun yönetim sistemi standardında belirtilen şartlara uygun bulunması ve Belgelendirme Komitesinin belgelendirme kararı vermesinden sonra kuruluş yönetim sistemi belgesi almaya hak kazanır. Belge, denetim raporları ile birlikte kuruluşa ulaştırılır.
Belgenin geçerlilik süresi gözetim denetimlerinin başarılı olması kaydı ile üç (3) yıldır. Belge geçerlilik süresi ilk belgelendirme kararının alındığı komite tarihi dikkate alınarak belirlenir. Belge değişikliklerinde ilk belge tarihi baz alınır ve belge geçerlilik süresinde herhangi bir değişiklik yapılmaz. CICERT, markanın ve belge kullanımının kontrolünü, yürütmüş olduğu denetimler sırasında yapmaktadır.
Belge ve logoların kullanımında kuruluş, genel olarak aşağıdaki yükümlülükleri yerine getirmelidir:

- Belgelendirilmiş müşteriler bu tip markaları kullandıklarında, markaya veya beraberinde olan metinde, belgelendirilen husus ve hangi belgelendirme kuruluşunun belgeyi verdiği hakkında belirsizlik olmamalıdır. Bu marka ürün üzerinde veya tüketici tarafından görülen ürün ambalajı üzerinde veya başka bir şekilde ürün uygunluğunu temsil ettiği şekilde yorumlanabilecek biçimde kullanılmamalıdır.
- Cıcert markaların laboratuar testlerine, kalibrasyon, muayene ve deney rapor ve sertifikalarında uygulanmasına, bu tip rapor ve sertifikalarında bu bağlamdaki ürünler olarak varsayılacağı anlamı vereceği için, izin verilmez.
- İnternet, dokümanlar, broşürler veya reklâm gibi iletişim ortamlarında belgelendirme statüsüne atıfta bulunurken, CIcert şartlarına uymalıdır.
- Belgelendirmesine ilişkin herhangi bir yanıltıcı beyanatta bulunmamalı veya buna müsaade etmemelidir.
- Belgelendirme dokümanını ve bunun herhangi bir kısmını yanıltıcı bir tarzda kullanmamalı veya kullanımına müsaade etmemelidir.
- Cıcert tarafından belgelendirmesinin geri çekilmesi veya iptal edilmesi üzerine belgelendirmeye olan bir atfı kapsayan bütün reklâm işini, belge, belgeye atıfta bulunan her türlü doküman ve tanıtım malzemesi ve logo kullanımını durdurmalıdır.
- Cicert, akreditasyonunun TÜRKAK tarafından iptal edilmesi halinde, Cicert markasını kullanım hakkı vermiş olduğu kuruluşların tanıtım ve sarf malzemesi, reklam, etiket ve ambalajları üzerinde TÜRKAK Akreditasyon Markasının kullanımını derhal durdurmalıdır.
- Belgelendirme kapsamı daraltıldığında, buna göre bütün reklâm malzemelerini değiştirmelidir.
- Belgelendirme dokümanını ve bunun herhangi bir kısmını, kuruluşun bir ürününü (hizmet dâhil olmak üzere) ya da prosesini belgelendirdiği izlenimini verecek şekilde kullanmamalıdır.
- Belgelendirmenin, belgelendirme kapsamı ve adresleri dışındaki faaliyetlere uygulandığı izlenimini vermemelidir.
- Almış olduğu belgeyi, CIcert'e veya belgelendirme sisteminin itibarına gölge düşürecek, ticari itibarını sarsacak, zedeleyecek ve kamu güvenini kaybettirecek tarzda kullanmamalıdır.
- Belgenin yayınlanma hakkı CICert'e ait olup, CIcert onaylamadıkça farklı bir şekilde çoğaltılamaz ve kopya edilemez.
- Belgelendirmenin delili olarak kuruluşlara verilebilmesi için tek renkli fotokopiye izin verilir.
- Belge almaya hak kazanan kuruluş Cıcert yönetim sistemi belgelendirme Logosunu/ Logolarını belgenin ürüne değil yönetim sistemine verildiğinin belirtilmesi kaydıyla CIBELT04 Logo Kullanım Talimatında tanımlandığı şekilde kullanabilir. ***"Logo Kullanım Talimatına"*** www.cicert.com.tr web sitesinden ulaşılabilir.

Bölüm 10- CICERT Yükümlülükleri

- Kuruluş ile ilgili tüm bilgi ve belgeleri prosedürleri gereği gizli tutmakla, gizlilik hükümlerini içeren sözleşmeyi belgelendirme personeline, denetim görevlilerine, komitelere ve uzmanlara imzalatmakla yükümlüdür.
- Belgelendirme kuruluşundan, gizlilik arz eden bilgiyi kanuni olarak veya yetkililerle yapılan sözleşme düzenlemeleri (örneğin akreditasyon kuruluşları ile yapılan sözleşme gibi) ile verilmesi istendiği durumda, kanunla yasaklanmamışsa ilgili müşteri veya kişiye, sağlanan bilgi hakkında bildirimde bulunulmalıdır.
- Belirli bir belgelendirilmiş müşteri veya kişi ile ilgili bilgi, ilgili belgelendirilmiş müşterinin veya kişinin yazılı izni dışında, üçüncü bir tarafa açıklanmaz.
- Müşteri haricindeki kaynaklardan sağlanan müşteri hakkındaki bilgiler (örneğin, şikayetçiler, düzenleyiciler), Cicert'in politikasıyla tutarlı şekilde gizli olarak ele alınır.
- Komite üyeleri dâhil olmak üzere, personel, yükleniciler, Cicert adına faaliyet gösteren dış kaynaklı kuruluşların personeli veya bireysel tetkikçiler, faaliyetlerinin yapılması sırasında elde edilen veya oluşturulan bütün bilgileri, kanuni bir zorunluluk dışında gizli tutmalıdır.
- Kuruluşa sunulan sistem belgelendirmesi ile ilgili uygulama dokümanlarında; belgelendirme sistemi ile ilgili standartlar ve kurallarda meydana gelebilecek önemli değişiklikleri, belgeli ve başvuru aşamasındaki kuruluşlara duyurmakla yükümlüdür. Bu amaçla web sayfası, e-posta vb. kullanılabilir.
  CIcert, belgelendirme şartlarında değişiklik yapma hakkına sahiptir. Ancak değişiklik tarihi esas alınarak uygulamalar başlatılır ve değişiklikten önceki kazanılmış haklar geçerliliğini korur.
  Belgelendirmenin esas alındığı Standard şartlarındaki değişiklikler belgeli kuruluşlara bildirilir. Cıcert, kuruluşların yeni şartları uygulayabilmesi için mevzuat hükümlerine aykırı olmamak ve haksız bir rekabet ortamı yaratmamak kaydıyla uygun bir geçiş süresi tanımaya yetkilidir ve geçiş süresi sonuna kadar belgenin geçerliliği devam eder.
- CIcert belgeli, belgesi askıda bulunan ve belgesi iptal edilen kuruluşların bir listesini tutarak web sayfasında yayınlamak ve güncellemekle sorumludur. Web sitesinde bulunan Kamuya açık bilgi; belgenin verilmesi, sürdürülmesi, genişletilmesi, yenilenmesi, daraltılması, askıya alınması veya geri çekilmesi için denetim ve belgelendirme faaliyetleri, yönetim sistemlerinin tipleri ve çalıştığı coğrafi alanları hakkındaki bilgileri içerir.
- CIcert yönetim sistemi belgelendirmesi kapsamında gerçekleştirdiği faaliyetlerle ilgili olarak kuruluşlara ait tüm kayıtları saklamakla yükümlüdür.
- CIcert denetim ve belgelendirme faaliyetleri kapsamında zarara neden olabilecek ya da sonuçlanabilecek risklere karşı "Mesleki Sorumluluk Sigortası'na sahiptir. Üçüncü kişiler ya da müşteri kuruluşlarda Cicert denetim ve belgelendirme faaliyetleri nedeni ile oluşabilecek zararlar bu sigortada belirlenen limitler oranında karşılanacaktır. Bu limitler yıllık periyotlarda güncellenmektedir. Düzenlenen belgelerin, 3. taraflarca tanınmaması durumunda CIcert'in hiçbir sorumluluğu bulunmamaktadır.
- Cıcert'in kendi isteği ile akreditasyonundan vazgeçmesi veya akreditasyon kurumu tarafından akreditasyonunun iptal edilmesi durumunda; belgelendirilmiş kuruluşlar IAF üyesi bir akreditasyon kurumuna bağlı bir belgelendirme kuruluşuna transfer edilir.
- Cıcert, kalite, çevre ve bilgi güvenliği yönetim sistemi denetlenmesi ve belgelendirmesi hizmetinin kusurlu olması (akreditasyonunun askıya alması/iptal edilmesi gibi) sebebi ile husule gelebilecek zarar ve ziyandan doğan tazminat taleplerini mesleki sorumluluk sigortası poliçesinde belirtilen şartlar dâhilinde teminat altına alınmıştır.
- Cicert, denetim sonucunu Belgelendirme Komitesi kararı sonrası denetim raporları denetlenen kuruluşa iletmekten sorumludur.

Bölüm 11- Belgelendirilmiş Kuruluşun Yükümlülükleri

- Kuruluş Yönetim sistem standartlarına uygun bir yönetim sisteminin oluşturulması, sürekliliğinin sağlanması ve belgelendirme şartlarına uygunluğun sağlanması sorumluluğundadır.
- Kuruluş, dokümantasyonu inceleme ve bütün proseslere ve alanlara, birinci aşama belgelendirme, gözetim, yeniden belgelendirme ve şikayetlerin çözümü için kayıtlara ve personele ve kayıtlara erişim dahil, tetkiklerin gerçekleşmesi için bütün gerekli düzenlemelerin yapılması; hükümleri dâhil olmak üzere, tetkiklerin gerçekleştirilmesi ve bütün alanları, kayıtları, birinci aşama belgelendirme, gözetim, yeniden değerlendirme ve şikayetleri çözümleme amaçlı personeli değerlendirmesi için gerekli olan bütün düzenlemeleri yapmayı kabul eder.
- Belgelendirilmiş kuruluşlar, bu kılavuz ve içeriğindeki diğer dokümanlar ile belgelendirmeye esas alınan yönetim sistem standardı ve/veya zorunlu hüküm ifade eden şartlarına uymak ve yükümlülüklerini yerine getirmek zorundadırlar.
- CIcert tarafından güncellenen belgelendirme uygulamaları ile ilgili dokümanlardaki değişiklikleri www.cicert.com.tr den takip etmek ve uymakla yükümlüdür.
- Sözleşmeye esas alınan Referans Standard veya Belgelendirme şartlarındaki değişiklikler belgeli kuruluşlara bildirildikten sonra kuruluş geçiş süresi içerisinde gerekli değişiklikleri yapmak ve uygulamakla yükümlüdür.
- Kuruluş Yönetim Sistemi uygulamalarındaki (ana politikalar, prosedürler, prosesler, vb.) büyük değişiklikleri, Kuruluş ve yönetim (kilit yönetici, karar alma ve teknik kadro gibi) değişiklikleri, unvan değişikliklerini, adres değişikliklerini, Yasal, ticari, kurumsal durum veya mülkiyeti değişiklikleri, İletişim adresi ve sahalar ile ilgili değişiklikler, Belgelendirilmiş yönetim sistemi altındaki işlemlerin kapsamı değişiklikleri ve Başvuru Formunda yer

alan bilgilerden herhangi birindeki her türlü değişikliği değişiklik yapıldığı tarihten itibaren 1 ay içerisinde Cıcert'e yazılı olarak bildirmek zorundadır.

- Kuruluşun denetlenmesi esnasında akreditasyon kurumunun gerek gördüğü hallerde akreditasyon kurumunun temsilcileri de bulunabilir. Kuruluş, Akreditasyon kurumunun temsilcileri tarafından denetim ile ilgili ihtiyaç duyulan her türlü yazılı ve sözlü bilgiyi vermekle yükümlüdür.
- Uygulanabilir olduğunda gözlemci ve aday denetçilerin denetimlerde yer almasını kabul eder.
- Kuruluş denetim esnasında her bir denetçiye bir rehberin eşlik etmesini sağlamalıdır.
- Kuruluş kurmuş olduğu sistemin uygulanması ve sürekliliğinin sağlanması amacı ile bir temsilcisi belirler, çalışma saatlerinde denetim ekibinin gerekli tüm alanlara girişine olanak sağlamakla, belge kapsamında yer alan ürüne ilişkin yönetim sistem standardı dışında, mevcut yasal gereksinimlerin sağlandığını garanti altına almakla yükümlüdür.
- Kuruluş, yönetim sistem dokümanlarının bir kopyasını denetimlerinden önce CIcert' e ulaştırmakla yükümlüdür.
- Belge ve Logoları, CIcert'in ticari itibarını sarsacak, zedeleyecek, yetkisiz kılacak veya herhangi bir anlaşmazlığa düşürecek şekilde kullanamaz. Belge ve marka kullanımı da dahil yer alan şartlara uyan her tip iletişimde, belgelendirmesine atıflar yapma şartları dâhil bu kılavuza uygun şekilde kullanmakla yükümlüdür.
- Kuruluş, Yönetim Sistemindeki uygunsuzluklardan kaynaklanan ürün, hizmet, proses ve varsa servislerinin performansı ile ilgili müşteri şikayetlerinin kayıtlarını tutacak ve gerek duyulduğunda CIcert'e ibraz edecektir.
- Kuruluş, Yönetim Sistem Belgelendirmesiyle ilgili ücretleri, "***Ücret Belirleme Talimatı"*** ve Sözleşmesinde belirtildiği şekilde fatura edilmesini takip eden 15 gün içerisinde ödemekle yükümlüdür. İlk belgelendirme ücreti veya yeniden belgelendirme ücreti ödeninceye kadar belgeler yayınlanmaz. Gözetim ücretleri ödenmediğinde belge askıya alınır veya geriye çağrılır.
- İtiraz ve şikâyetlerini bu kılavuzda açıklandığı şekilde uygulamalıdır.
- Sözleşmesinde yer almayan belgelendirme faaliyetlerine yönelik ekstra maliyetler, plansız ziyaretler, kalite yönetim sisteminin uygulamada yeterliliğini sürdürdüğünün doğrulanması için yapılan ilave denetimlerle ilgili ücretlerde faturalandırılır.