1. AMAÇ

Bu prosedürün amacı; CAS tarafından yürütülen ISO/IEC 27001:2022 AMD 1:2024, ISO/IEC 27701 sistemi belgelendirme faaliyetleri içerisinde yer alan CAS çalışanlarının ve denetimde görev alacak denetim ekibi personelinin gerekli yetkinliklerini ISO/IEC 17021-1, ISO/IEC 27006-1:2024 Standartlarına göre belirlemek değerlendirmektir.

2. TANIMLAR

BGYS: Bilgi Güvenliği Yönetim Sistemi
Bilgi Güvenliği Yönetim Sistemi: Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası.
Uygulanabilirlik Beyanı (SoA): Kuruluşun BGYS'si ile ilgili ve uygulanabilir kontrol amaçlarını ve kontrolleri açıklayan dokümante edilmiş beyan.
KVYS: kişisel Verileri Yönetim Sistemi
Üst Düzey bilgi / beceri: Bilgi ve beceri kriteri ile ilgili ortalama üstünde derin yetkinlik.
Baş denetçi: Denetimde görev alan denetim ekibine liderlik yapan denetim ekibi personeli
Denetçi: Denetimde, denetim görevinde bulunan denetim ekibi personeli
Teknik Uzman: Denetim ekibinde, müşterinin faaliyet gösterdiği alanda sektör, ürün, proses ve organizasyon bilgisi olan ve teknik alanda yetkin denetim ekibi personeli.
Gözlemci: Denetim ekibinin dışında, denetim ekibini ve gerçekleştirilen denetimi gözlemlemek amacı ile görevlendirilen kişi. Gözlemci, denetim yapılan standartta baş denetçi olmalı, ayrıca CAS tarafından yapılan değerlendirmede yetkin görülen kişilerden seçilir. (Gözlemci, denetim tecrübesi, önceki katıldığı denetimler, denetim bilgisi, akreditasyon bilgisi, tanık denetim tecrübesi vb. kriterlerin bir veya birkaçına yönelik yetkinliği bulunan kişilerden seçilir.)
Değerlendirilen Denetçi (DD): CAS' da İlk defa denetime giden ve yetkinlik değerlendirilmesi için, baş denetçi veya gözlemci refakatinde denetime iştirak eden, denetim adam günü hesaplamasına dahil edilmeyen denetim ekibi personeli.
Belgelendirme Kararı Alan Personel: Gerçekleştirilecek denetim sonrasında, gerçekleşen denetimin CAS prosedürlerine uygunluğunu ve denetim raporunu değerlendirerek belgelendirme ile ilgili karar alan, belgelendirme kurulu personeli.
Alanda Yetkinlik: Personelin, müşterilerin faaliyet gösterdiği alanlarda sahip oldukları sektör ve ürün, proses, organizasyon, teknolojik alan, yasal şartları konusunda bilgi sahibi olmasıdır. Alandaki yetkinlik atamaları, ISO/IEC 27001 2022 AMD 1:2024 belgelendirmelerinde Türkak R.40.01 dokümanında belirtilen EA/NACE kodlarına ve bu prosedürde anlatılan yöntemlere göre yapılır. ISO/IEC 27001 2022 AMD 1:2024 belgelendirmelerinde ISO/IEC 27006-1 standardında karmaşıklık kriterlerine ve risk seviyelerine göre belirlenmiştir.
Denetim Ekibi Personeli: Denetimde görev alan Denetçi, Baş denetçi ve teknik uzmanlar.
Ofis Personeli: Denetim ekibi görevlileri ve belgelendirmeyi onaylayan personel haricindeki, CAS ofisinde görev alan çalışanları.
Rehber: Denetimin kolaylaşması için denetim ekibindeki her denetçi için kuruluş tarafından bir rehber atanır.
Rehberlerin görevleri; görüşme için iletişim ve zamanlamayı sağlar, kuruluşun sahalarına ziyaretlerin düzenlenmesi sağlar, kuruluş içerisindeki güvenlik ve emniyet prosedürlerini bilir ve denetim ekibinin bu kurallara uymasını sağlar, kuruluş adına denetime tanıklık tapar, denetçiye gerek duyduğu bilgi ve açıklamaları sağlar.

3. İLGİLİ DOKÜMANLAR

F011 BD D TU Değerlendirme Formu-Müşteri
F013 Başdenetçi Değerlendirme Formu
F041 Personel Ön Değerlendirme Formu
F042 Başdenetçi/ Denetçi/ Teknik Uzman Atama Formu
F067 Eğitim Katılım Formu
M003 Personel Yetkinlik Matrisi
T008 BGYS Yeterlilik Analizi Değerlendirme Talimatı
P001 Doküman Kontrol Prosedürü
P008 Personel Atama ve Performans Değerlendirme Prosedürü

P005 Düzeltici Önleyici Faaliyet Prosedürü
P002 Kayıtların Kontrolü Prosedürü
P009 Belgelendirmenin Askıya Alınması ve Geri Çekilmesi Prosedürü
TÜRKAK R.40.01, TÜRKAK R.40.02, TÜRKAK R.40.05, TÜRKAK R.40.06
ISO/IEC 17021-1:2015
ISO/IEC 27006-1:2024

4 Prensipler

ISO/IEC 17021-1:2015,Madde 4'ün gereklilikleri esas alındı.

5 Genel Gereklilikler

5.1 Hukuki ve Sözleşmeyle İlgili Maddeler

ISO/IEC 17021-1:2015,Madde 5.1.'in gereklilikleri esas alındı.

5.2 Tarafsızlık Yönetimi

5.2.1 Genel

ISO/IEC 17021-1:2015,Madde 5.2'nin gereklilikleri esas alındı.

Çıkar Çatışmaları

CAS, danışmanlık olarak değerlendirilmeksizin veya potansiyel bir çıkar çatışması oluşturmadan, belgelendirme ve gözetim tetkikleri sırasında (örneğin; tetkik esnasında belirli çözümler önermeden iyileştirme fırsatlarını belirleyerek) değer katar.

CAS, müşterilerin belgelendirmeye tabi BGYS'lerine ilişkin dâhilî bilgi güvenliği gözden geçirmelerini sağlar. Ayrıca CAS, BGYS iç tetkikini gerçekleştiren kuruluş veya kuruluşlardan (herhangi bir kişi de dâhil) bağımsızdır. Belgelendirme yaptığı müşteriye iç tetkik vb. eğitimler vermez. Denetim ekibi ile yapılan Sözleşmeler ve Atama Formu ile güvence altına alınır. Ayrıca Denetim Ekibinde belirli periyotlarda eğer yapıyor ise danışmanlık ve eğitim verdiği kuruluşlar hakkında yazlı olarak bilgi Yönetim Temsilcisi tarafından temin edilerek kayıtlar saklanır.

ISO/IEC 27006-1:2024,Madde 5.2.2'nin gereklilikleri esas alındı.

5.3 Yükümlülükler ve finansman

ISO/IEC 17021-1:2015,Madde 5.3.'ün gereklilikleri esas alındı.

6 Yapısal gereklilikler

ISO/IEC 17021-1:2015,Madde 6'nın gereklilikleri esas alındı.

7 Kaynak gereklilikleri

7.1 Yönetimin ve personelin yeterliliği

Genel hususlar

CAS, uygun personelin, faaliyet alanları ve çalışmakta olduğu coğrafi alanlardaki yönetim sistemleriyle örneğin bilgi güvenliği yönetim sistemi Kişisel Verilerin Korunması Yönetim Sistemi ilgili uygun bilgiye sahip olmalarını sağlayacak prosesleri oluşturmuş ve uygular.

Yeterlilik kriterlerinin belirlenmesi

CAS, belgelendirme, denetimlerin performansı ile yönetiminde içinde olduğu personel için yeterlilik kriterlerini belirleyen dokümante edilmiş bir prosese sahiptir. Yeterlilik kriterleri, belgelendirme prosesindeki her fonksiyon için, her teknik alan için ve yönetim sistem standard veya şartnamenin her bir tipi ile ilgili şartlar için belirlenmiştir. Prosesin çıktısında, istenen sonuçlara erişilebilmesi için denetim ve belgelendirmeyi etkileyen bütün görevlerin yerine getirilebilmesini sağlayacak bilgi ve becerileri de kapsayan Personel Yetkinlik Matrisinde dokümante edilmiş, kriterler oluşturulmuştur. CAS, Personel Yetkinlik Matrisinde belirlediği bilgi ve becerileri aşağıda verilen referansları dikkate almak suretiyle oluşturmuştur: BGYS için ISO/ IEC 27006, IAF MD Dokümanları

Değerlendirme prosesi

CAS, belirlenen yeterlilik kriterlerini uygulayarak denetim ve belgelendirme performansı ile yönetim içindeki tüm personelin performans ve yetkinliğini izlemek için, Personel Atama ve Performans Değerlendirme Prosedürünü oluşturmuş ve uygulamaktadır.

Diğer değerlendirmeler

CAS, çalışmakta olduğu teknik alanlar, yönetim sistemi tipleri ve coğrafi alanlarda önemli sektörlerin belgelendirmesiyle doğrudan ilgili konular hakkında tavsiyeler için gerekli görülen teknik uzmanlığa erişebilir durumdadır. Bu tip tavsiyeler CAS'nin tam zamanlı personeli veya sözleşmeli personel tarafından sağlanır.

ISO/IEC 17021-1:2015,Madde 7.1.'in gereklilikleri esas alındı.

Genel yetkinlik gereklilikleri

CAS, ISO/IEC 17021-1 Çizelge A.1'de gösterildiği gibi, her bir belgelendirme işlevi için yetkinlik gerekliliklerini bu prosedür ve Personel Yetkinlik Matrisinde tanımlamıştır.

CAS, kendisinin belirlediği BGYS teknik alanlarıyla alakalı bu Uluslararası Standartta Madde 7.1.3 ve Madde 7.2.2'de ve ISO/IEC 17021-1:2015'de belirtilen bütün gereklilikleri göz önüne alır. Ek B, yetkinlik konusunda daha ayrıntılı kılavuzluk sunmaktadır.

CAS, Ek A ile uyumlu olarak belirli fonksiyonlar için gerekli bilgi ve becerileri tanıölamıştır. Yeterli gereklilikler de dahil olmak üzere, ek özel kriterlerin belirli bir standartta (örneğin; ISO/IEC 27006-2) belirlenmiş olması durumunda bunlar uygulanır.

ISO/IEC 27006-1:2024,Madde 7.1.2'nin gereklilikleri esas alındı.

ISO/IEC 17021-1:2015 Çizelge A.1 Bilgi ve Beceriler esas alındı.

Çizelge A.1 - Bilgi ve becerilerin çizelgesi

Bilgi ve beceriler	**Belgelendirme fonksiyonları**		
	Tetkik ekibi üyelerinin seçilmesi ve tetkik ekibinin gerekli yeterliliğinin belirlenmesi için yapılan başvurunun gözden geçirilmesi	Tetkik raporlarının gözden geçirilmesi ve belgelendirme kararının verilmesi	Tetkikin gerçekleştirilmesi ve tetkik ekibinin liderliği
İş yönetim uygulamalarının bilgisi			X (bk. Madde A.2.1)
Tetkik prensip, uygulama ve tekniklerinin bilgisi		X (bk. Madde A.3.1)	X (bk. Madde A.2.2)
Belirli yönetim sistem standardları/hüküm ifade eden dokümanların bilgisi	X (bk. Madde A.4.1)	X (bk. Madde A.3.2)	X (bk. Madde A.2.3)
Belgelendirme kuruluşunun proseslerinin bilgisi	X (bk. Madde A.4.2)	X (bk. Madde A.3.3)	X (bk. Madde A.2.4)
Müşterinin yaptığı iş sektörü bilgisi	X (bk. Madde A.4.3)	X (bk. Madde A.3.4)	X (bk. Madde A.2.5)
Müşterinin ürün, proses ve kuruluşunun bilgisi	X (bk. Madde A.4.4)		X (bk. Madde A.2.6)
Müşteri kuruluşundaki bütün seviyelerde uygun lisan becerileri			X (bk. Madde A.2.7)
Not alma ve rapor yazma becerileri			X (bk. Madde A.2.8)
Sunum becerileri			X (bk. Madde A.2.9)
Görüşme becerileri			X (bk. Madde A.2.10)
Tetkik-yönetim becerileri			X (bk. Madde A.2.11)
Not – Risk ve karmaşıklık, bu fonksiyonların her biri için ihtiyaç duyulan uzmanlık seviyesine karar verilmesinde dikkate alınacak diğer hususlardır.			

ISO/IEC 27006-1:2024 Ek A BGYS tetkiki ve belgelendirmesi için bilgi ve beceriler

A.1 Genel Bakış

Çizelge A.1, ISO/IEC 17021-1 gerekliliklerine ek olarak, bir belgelendirme kuruluşunun belirli sertifikasyon fonksiyonları için tanımlaması gereken bilgi ve becerileri belirtir. "X", belgelendirme kuruluşunun bilgi ve becerilerin kriterlerini ve derinliğini tanımlaması gerektiğini belirtir. Çizelge A.1'de belirtilen bilgi ve beceri gereklilikleri, Madde 7'de daha ayrıntılı olarak açıklanmış ve Çizelge A.1'de parantez içinde çapraz referans verilmiştir.

Başvuru aşamasında çalışan sayısı, adres, kapsam, süreç bilgisi doğrulama mekanizması olusturullmuştur. Başvuru formuyla kayıt altına alınmaktadır.

ISO/IEC 27006-1:2024 Çizelge A.1-BGYS tetkiki ve belgelendirmesi için bilgi ve becerilerin çizelgesi

TABLO 4	**ISO/IEC 27001:2022 AMD 1:2024 & ISO/IEC 27701 Temel İhtiyaçlar Matrisi**		
Bilgi ve beceriler	Tetkik ekibinin yetkinliğini belirlemek, tetkik ekibinin üyelerini seçmek ve tetkik zamanını belirlemek için başvuru değerlendirmesini yürütme	Tetkik raporlarını değerlendirme ve belgelendirme kararı verme	Tetkik ve tetkik ekibini yönetme
Bilgi güvenliği yönetimi terminolojisi, prensipleri, uygulamaları ve teknikleri	-	X (7.1.3.3.2)	X (7.1.3.1.2)

Bilgi güvenliği yönetim sistemi standartlar/bağlayıcı dokümanlar	-	-	X (7.1.3.1.3)
İş yönetimi uygulamaları	-	-	X (7.1.3.1.4)
Müşteri iş sektörü	X (7.1.3.2.1)	X (7.1.3.3.3)	X (7.1.3.1.5)
Müşteri ürünleri, süreçleri ve organizasyonu	X (7.1.3.2.2)	X (7.1.3.3.4)	X (7.1.3.1.6)
*** ISO/IEC 27001:2022 AMD 1:2024 & ISO/IEC 27701 faaliyetlerinde görev alan personellerin yukardaki konular hakkında bilgi sahibi olması beklenir.**			

ISO/IEC 27001 Bilgisi, ISO/IEC 27006-1:2024 EK A kontrolleri, Aşağıdaki, BGYS denetimiyle bağlantılı olarak tipik bilgiyi tanımlamaktadır. ISO/IEC 27001 deki kontrol alanlarına ek olarak ISO/IEC 27006-1:2024 EK A listelenen tablo ile denetçiler 27000 ailesindeki diğer standartlardan da haberdar olmalıdır.

Bilgi güvenliği için düzenlemeler ve iş gereklilikleri için bilgi ve tecrübe	Güvenlik politikası
İş prosesleri, uygulamaları ve organizasyon yapılarıyla ilgili genel bilgi ve tecrübe	Bilgi güvenliğinin organizasyonu
Varlık değerleme, yatırım, sınıflandırma ve kabul edilebilir kullanım düzenlemeleri için bilgi	Varlık yönetimi
insan kaynakları departmanının kullandığı prosedürler ve prosesler hakkında genel bilgi	İnsan kaynakları güvenliği
Fiziksel ve çevresel güvenlik faktörlerinin bilgisi	Fiziksel ve çevresel güvenlik
Yönetim ölçümleri ve belirli bir teknik uzmanlık seviyesini de dahil ederek bilgi güvenliği için kullanılan standartların, proseslerin, tekniklerin ve metotların güncel bilgisi ve tecrübesi	İletişim ve operasyon yönetimi
	Erişim kontrolü
	Bilgi sistemleri kazanımı, gelişimi ve muhafazası
Vaka yönetimiyle ilgili proses ve prosedürlere ilişkin güncel bilgi ve tecrübe	Bilgi güvenliği olay yönetimi
Standartlar, prosesler planlar ve iş için test prosedürleriyle ilgili güncel bilgi	İş devamlılığı yönetimi
Kontratlarla ilgili ve BGYS' ile bağlantılı kanuni düzenlemelere, düzenleyici gereksinimlere ilişkin güncel bilgi	Uygunluk
Bilgi güvenliği risk değerlendirme ve risk yönetimi	Risk
BGYS' nin kapsamının da ve sınırlarında teknolojik bilgi	Bilgi Teknolojisi

A.2 Standart ile Bağlantılı Tipik Bilgi

Denetçilerin aşağıdaki denetim ve BGYS,KVYS başlıklarıyla ilgili bilgisi ve kavrayışı olmalıdır:

- Denetim programlama ve planlama
- Denetim tipi ve metodolojileri
- Denetim riski
- Bilgi güvenliği prosesleri analizi
- Devamlı gelişim için PDCA döngüsü
- Bilgi güvenliği için iç denetim
- Bilgi Güvenliği -Kişisel Veri Yönetimi, Hizmet Yönetimi terminoloji, prensipleri, pratikleri ve teknikleri

Denetçilerin aşağıdaki düzenleyici gerekliliklerle ilgili bilgisi ve kavrayışı olmalıdır:

- Telif hakları
- Organizasyon kayıtlarının fihristi, korunması ve muhafazası
- Bilgi koruması ve gizlilik
- Kriptografik kontrollerin düzenlenmesi
- Elektronik ticaret
- Elektronik ve dijital imzalar
- Çalışma yeri gözetimi
- Telekomünikasyon tevkifi ve bilginin yönetimi (ör: e-mail)
- Bilgisayar tacizi
- Elektronik kanıt toplama
- Penetrasyon testi
- Uluslararası ya da milli sektöre özel uygulamalar (örn. bankacılık)

Denetçilerin aşağıdaki yönetim gerekliliklerıyle ilgili bilgisi ve kavrayışı olmalıdır:

- Bilgi güvenliği riskine yaklaşım
- Bilgi ve iletişim teknolojilerinde dış kaynak kullanımında güvenlik riskleri
- Tedarik zinciri bilgi güvenliği riskleri

ISO/IEC 27006-1:2024 Ek B Diğer yetkinlik hususları

B.1 Genel yetkinlik hususları

Tetkikçilerin bilgi ve deneyimlerini kanıtlayabilecekleri çeşitli yollar vardır. Bilgi ve beceriler; örneğin, tanınmış nitelikler kullanılarak değerlendirilir. Aynı şekilde personel belgelendirme şemaları altındaki tescil kayıtları da istenen bilgi ve deneyimi değerlendirmede kullanılabilir. Tetkik ekibi için istenen yetkinlik düzeyinin, kuruluşun endüstri/teknolojik alanı ve BGYS'nin karmaşıklığına uygun olarak belirlenmesi esastır.

B.2 Belirli bilgi birikimi ve deneyim hususları

B.2.1 BGYS ile ilgili tipik bilgi

Madde 7.1.3'deki gerekliliklere ek olarak aşağıda belirtilenler göz önünde bulundurulması esastır. Denetçilerin aşağıda belirtilen tetkik ve BGYS konularında bilgi ve kavrayış sahibi olması esastır:

- tetkik programlaması ve planlaması;
- tetkik tür ve metodolojileri;
- tetkik riski;
- bilgi güvenliği süreç analizi;
- sürekli iyileştirme;
- bilgi güvenliğinin iç tetkiki.

Denetçiler aşağıda belirtilen düzenleyici gereklilikleri bilmeleri ve anlamaları esastır:

- fikrî mülkiyet;
- kurumsal kayıtların içeriği, korunması ve tutulması;
- verilerin korunması ve gizliliği;
- kriptografik kontrollerin düzenlenmesi;
- elektronik ticaret;
- elektronik ve dijital imzalar;
- işyeri gözetimi;
- haberleşme verilerinin dinlenmesi ve izlenmesi (ör. e-posta);
- bilgisayarların kötüye kullanımı;
- elektronik kanıt toplama;
- sızma testleri;
- sektörlere özgü uluslararası ve ulusal gereklilikler (ör. bankacılık).

Belirli bir sektör için bilgi ve anlayışın belirli bir standartta (örneğin ISO/IEC 27006-2) yerleşmiş olması mümkündür.

Yetkinlik kriterlerinin belirlenmesi

BGYS tetkiki yapmak için yetkinlik gereklilikleri

Genel gereklilikler (7.1.3.1.1)

CAS; tetkik ekibi üyelerinin aşağıdaki hususları garanti eden belirli kriterlere sahip olduklarından emin olmak için yetkinliklerini doğrulama kriterlerine sahiptir:

a) bilgi güvenliği;
b) tetkik edilecek faaliyetin teknik yönleri;
c) yönetim sistemleri;
d) tetkik prensipleri;
e) NOT Tetkik prensipleriyle ilgili daha fazla bilgi ISO 19011'de bulunabilir.
f) BGYS izleme, ölçme, analiz etme ve değerlendirme.

Yukarıda a) ile e) gereklilikleri, tetkik ekibindeki tüm tetkikçiler için geçerlidir. Ancak, b) gereklilikleri tetkik ekibi üyeleri arasında paylaşılır.

Tetkik ekibi üyeleri, toplu olarak, yukarıdaki gerekliliklere uygun becerilere sahip olup ve bu beceriler, uygulama deneyimleri aracılığıyla kanıtlanır.

Tetkik ekibi üyeleri, toplu olarak, müşterinin BGYS'sindeki bilgi güvenliği ihlal olaylarının belirtilerini

BGYS'nin ilgili unsurlarına kadar izleme konusuna yetkindir.
Bireysel olarak tetkikçilerin bilgi güvenliğinin tüm alanlarında kapsamlı deneyime sahip olması gerekmez, ancak bir bütün olarak bakıldığında tetkik ekibi tetkiki yapılan BGYS kapsamını kapsayacak yetkinliğe sahiptir.

Bilgi güvenliği yönetimi terimleri, prensipleri, uygulamaları ve yöntemleri (7.1.3.1.2)

BGYS tetkik ekibindeki her denetçi aşağıdaki konularda bilgi sahibi olmalıdır:

a) BGYS'ye özgü dokümantasyon yapısı, hiyerarşisi ve karşılıklı ilişkileri,
b) bilgi güvenliği risk değerlendirmesi ve risk yönetimi;
c) BGYS'ye uygulanabilen süreçler,
d) Tetkik ekibi üyeleri, toplu olarak, aşağıdaki konularda bilgi sahibi olmalıdır:
e) bilgi güvenliği yönetimiyle ilgili araçlar, yöntemler, teknikler ve bunların uygulamaları,
f) bilgi güvenliğiyle alakası olabilecek ya da bir konusunu teşkil edebilecek mevcut teknoloji.

Bilgi güvenliği yönetim sistemleri standartları ve bağlayıcı dokümanlar (7.1.3.1.3)

BGYS tetkikinde yer alan her denetçi, ISO/IEC 27001:2022'deki bütün gereklilikler hakkında bilgi sahibidir.
Tetkik ekibi üyeleri, toplu olarak, ISO/IEC 27001:2022, Ek A'da yer alan tüm kontroller ve bunların uygulanması hakkında bilgi sahibidir.

İş yönetimi uygulamaları (7.1.3.1.4)

BGYS tetkik ekibindeki her denetçi aşağıdaki konularda bilgi sahibidir:

a) endüstriyel bilgi güvenliği iyi uygulamaları ve bilgi güvenliği prosedürleri,
b) bilgi güvenliği için politikalar ve iş gereklilikleri,
c) genel iş yönetimi konuları, uygulamaları ile politika, hedef ve sonuçlar arası ilişkiler,
d) yönetim süreçleri ve ilgili terminoloji.

NOT Bu süreçler ayrıca insan kaynakları yönetimi, dâhilî ve harici iletişim ve diğer ilgili destek süreçlerini de içerir.

Müşteri iş sektörü (7.1.3.1.5)

BGYS tetkik ekibindeki her denetçi aşağıdaki konularda bilgi sahibidir.

a) belirli bilgi güvenliği alanı, coğrafyası ve yargı alan(lar)ı hakkında yasal ve düzenleyici gereklilikler;

NOT Yasal ve düzenleyici gerekliliklerin bilinmesi kapsamlı bir hukuki arka plana sahip olunduğu anlamına gelmez.

b) iş sektörüyle bağlantılı bilgi güvenliği riskleri;
c) müşteri iş sektörüyle bağlantılı genel terminoloji, süreçler ve teknolojiler;
d) ilişkili iş sektörü uygulamaları;

Kriter a) tetkik ekibi arasında paylaştırılır.

Müşteri ürünleri, süreçler ve teşkilat (7.1.3.1.6)

Tetkik ekibi üyeleri, toplu olarak, aşağıdaki konularda bilgi sahibidir.

a) dış kaynak kullanımı dahil BGYS'nin geliştirilmesi ve uygulamaya konulması ile belgelendirme faaliyetleri üzerine kuruluş türünün, büyüklüğünün, yönetiminin, işlevlerinin ve ilişkilerinin etkisi,
b) geniş bir perspektifte karmaşık işlemler;
c) ürüne veya hizmete uygulanabilir yasal ve düzenleyici gereklilikler.

Başvuru değerlendirilmesinin yürütülmesinde yetkinlik gereklilikleri (7.1.3.2.1)

Müşteri iş sektörü

Başvuru değerlendirmesini yapan personel, tetkik ekibinin gerekli yetkinliklerini belirlemek, tetkik ekibi üyelerini seçmek ve tetkik süresini belirlemek için; müşterinin iş sektörüyle ilgili genel terminoloji, süreçler, teknolojiler ve riskler hakkında bilgi sahibi ve eğitimlidir.

Müşteri ürünleri, süreçler ve teşkilat (7.1.3.2.2)

Başvuru değerlendirmesini yapan personel, gerekli tetkik ekibi yetkinliğini belirlemek, tetkik ekibi üyelerini seçmek ve tetkik süresini belirlemek için; dış kaynak kullanımı dâhil BGYS ve'nin geliştirilmesi ve uygulamaya konulması ile belgelendirme faaliyetleri üzerine müşteri ürünleri, süreçler, kuruluş türleri, büyüklük, yönetişim, yapı, işlevler ve ilişkiler hakkında bilgi sahibidir.

Tetkik raporlarını gözden geçirmek ve belgelendirme kararlarını vermek için yetkinlik gereklilikleri (7.1.3.3/7.1.3.3.1)

Tetkik raporlarını gözden geçiren ve belgelendirme kararlarını veren personel, belgelendirmenin

kapsamının uygunluğunu doğrulamalarını, kapsamdaki değişiklikleri ve bunların tetkikin etkinliğine olan etkisini görmelerini, özellikle de arayüzlerin tanımlamalarının devam eden geçerliliğini, bağlılıkları ve bağlantılı riskleri anlamalarını sağlamak için gerekli bilgi düzeyine sahiptir.
Buna ek olarak, tetkik raporlarını gözden geçiren ve belgelendirme kararlarını veren personel şunları
Bilir ve eğitimlidir:

a) genel olarak yönetim sistemleri;
b) tetkik süreçleri ve yöntemleri.

Bilgi güvenliği yönetimi terimleri, prensipleri, uygulamaları ve yöntemleri (7.1.3.3.2)
Tetkik raporlarını gözden geçiren ve belgelendirme kararlarını veren personel aşağıdaki bilgilere sahibidir:

a) "Bilgi güvenliği yönetimi terimleri, prensipleri, uygulamaları ve yöntemleri" altındaki listelenen a), b), c) ögeleri;
b) bilgi güvenliği ile ilişkili yasal ve düzenleyici gereklilikler.

Müşteri iş sektörü (7.1.3.3.3)
Tetkik raporlarını gözden geçiren ve belgelendirme kararlarını veren personel, ilgili iş sektörü uygulamalarına dair genel terminoloji ve riskler hakkında bilgi sahibidir.
Müşteri ürünleri, süreçler ve teşkilat (7.1.3.3.4)
Tetkik raporlarını gözden geçiren ve belgelendirme kararlarını veren personel, müşteri ürünleri, süreçler, teşkilat türleri, büyüklük, yönetişim, yapı, işlevler ve ilişkiler hakkında bilgi sahibidir.
ISO/IEC 27006-1:2024,Madde 7.1.3'ün gereklilikleri esas alındı.

7.1.4 Denetim Ekibi Yetkinliği

Gözetim faaliyetleri için sadece planlanan gözetimle ilgili aktiviteler uygulanır. Aşağıdaki gereklilikler denetim ekibinin ekibinin tümüne uygulanır.
Belge süresi dolmuş müşteriler askı iptal sürecine göre değerlendirilmektedir. F101 Müşteri Dosyaları Değerlendirme Analiz Raporu ile aylık Planlama Sorumlusu tarafından kontrol edilecektir.
Süre hesaplama ve başvuru verisi doğrulama kontrol noktaları artırılmış başvuru gözden geçirme formuyla kayıt altına alınmaktadır.
Aşağıdaki alanların her biri için en az bir denetleme ekibi üyesi CAS Belgelendirmenin sorumluluk alma kriterini gerçekleştirmek üzere görevlendirilir;

- Ekibi yönetmek
- BGYS, KVYS' ye uygulanabilecek yönetim sistemleri ve prosesler
- Bilgi Güvenliği Yönetim Sistemi -Kişisel Veri Yönetim Sistemi ilgili kanuni ve düzenleyici gerekliliklerin bilgisi
- Bilgi Güvenliği Yönetim Sistemi –Kişisel Veri Yönetim Sistemine bağlantılı tehditlerin ve vaka trendlerinin belirlenmesi
- Müşteri organizasyonun zayıflıklarının belirlenmesi ve bunların istismarı, organizasyona etkisi, etkilerin hafifletilme ve kontrolü için olası yapılabileceklerin anlaşılması
- BGYS/ KVYS kontrolü ve uygulamalarının bilgisi
- BGYS/ KVYS etkinliği gözden geçirmesi ve kontrol ölçümlerinin bilgisi
- İlgili ya da bağlantılı BGYS/ KVYS standartları, endüstri pratikleri, güvenlik düzenlemeleri
- Vaka inceleme metotları ve iş devamlılığına ilişkin bilgi
- Somut ve soyut bilgi varlıklarının ve etki analizinin bilgisi
- Güvenlikle bağlantılı olabilecek mevcut teknoloji bilgisi
- Risk yönetimi proses ve metotlarının bilgisi

Denetim ekibi, BGYS/ KVYS'nin uygun bileşenlerine göre müşteri kuruluşunun yönetim sistemi desteği kapsamında güvenlik olaylarının belirtilerini izleme yeteneğine sahiptir. Denetleme ekibi yukarıdaki maddelerin hepsini karşılayabilecek çalışma deneyimi ve pratik uygulamaya sahiptir. (Bu bir denetçinin Bilgi Güvenliği Yönetim Sistem-Kişisel Veri Yönetim Sistemi ile ilgili bütün alanlarda bilgi sahibi olmasını gerektirmez, ancak denetleme ekibi bütün olarak denetlenmekte olan BGYS/KVYS kapsamını değerlendirebilecek tecrübeye ve bilgiye sahiptir.

Denetim ekibi, belgelendirilmesi istenilen BGYS/KVYS kapsamı dahilindeki faaliyetler ve uygun olması halinde bu faaliyetler ile ilgili prosedürler, potansiyel bilgi güvenliği riskleri ve bu riskler ile ilgili teknik bilgi birikimine sahiptir. (Teknik uzmanlar ile de bu yeterlilik sağlanabilir)
Denetim ekibi, güvenilebilir bir BGYS/KVYS denetimi yapmak için müşteride kurulan BGYS/KVYS' nin kapsamını ve içeriğini, faaliyet gösterdiği sektörü, ürün ve hizmetlerini standart açısından değerlendirebilecek yeterli bilgi ve tecrübeye sahip kişilerden oluşur.
Denetim ekibi, müşteri kuruluşun sahip olduğu BGYS, KVYS' ye uygun yasal ve düzenleyici gereksinimlerinin neler olabileceğini doğru anlayabilen kişilerden oluşur.
Denetleme ekibi, eğer ilgili kişi yukardaki kriterleri sağlıyorsa tek bir kişiden de oluşur.

7.1.4.1 Denetçi Yeterliliğinin Gösterilmesi

Denetçiler, yukarıda belirtildiği üzere aşağıdakiler vasıtasıyla bilgi ve deneyimlerini gösterebilmektedir.

a) Kabul edilmiş BGYS/KVYS özel nitelikleri;
b) Denetçi olarak tescil;
c) Onaylanmış BGYS/KVYS eğitim kursları;
d) Güncel ve sürekli mesleki gelişim kayıtları;
e) Gerçek müşteri sistemlerine ilişkin BGYS/KVYS denetim süreci vasıtasıyla denetçiler tarafından uygulamalı ispat.
f) BGYS/KVYS eğitimleri almış olduğuna dair kimlik bilgilerini içeren kayıtlar

7.1.4.2 Genel Yeterlilik Değerlendirmeleri

Denetçinin kendi bilgi ve tecrübesini kanıtlayabileceği birkaç yol vardır. Bilgi ve tecrübe, farkında olunan nitelikler gösterilerek ispatlanabilir. Bilgi ve Deneyimi değerlendirilir. CAS Belgelendirme yeterliliği kendi atadığı ve aşağıda 3.a ve b'de belirtilen konulara haiz kişiler aracılığı ile sağlar. Atamalar PR.15 BGYS-KVYS Belgelendirme Prosedüründe belirtilen değerlendirme doğrultusunda yapılır.

7.2 Belgelendirme faaliyetlerinde görev alan personel

CAS, kuruluş bünyesinde, denetim programları ve yapılan diğer belgelendirme işinin yönetim tipi ve çeşitliliği için yeterli yetkinliğe sahip olan personele sahiptir.
CAS, bütün faaliyetlerini kapsayacak ve yapılan denetim işini yürütecek yeterli sayıda başdenetçi, denetçi ve teknik uzman istihdam etmekte veya bunlara erişir.
CAS, her bir personelinin görevlerini, sorumluluklarını ve yetkilerini açık bir şekilde Yönetim Sistemi El Kitabı bölüm 4'de belirlemiş ve dokümante etmiştir
CAS, belgelendirme faaliyetlerinde yer alacak olan denetçiler ve teknik uzmanları seçme, eğitme, resmî olarak yetkilendirmek ve izlemek için Personel Atama ve Performans Değerlendirme Prosedürünü oluşturmuş ve uygular.
Bu prosedür doğrultusunda bir denetçinin ilk yeterlilik değerlendirmesi, denetimler esnasında uygulanabilir kişisel nitelikleri ile gerekli bilgi ve beceriyi uygulama kabiliyetinin belirlenmesini ve yetkin bir değerlendirici tarafından yapılan bir saha denetimini kapsar.
CAS, kullandığı denetçilerin ve başdenetçilerin hem genel denetim bilgi ve becerisine, hem de özel teknik alanların denetlenmesi için uygun bilgi ve beceriyi sağlamak için Personel Yetkinlik Matrisi ve Personel Atama ve Performans Değerlendirme Prosedürünü oluşturmuş ve uygular.
CAS, denetçilerin (ve ihtiyaç duyulduğunda teknik uzmanların) belgelendirme şartları, denetim şartları ve ilgili diğer şartlar hakkında bilgi sahibi olmalarını sağlar.
CAS, denetçilerin ve teknik uzmanların, denetim talimatları ve belgelendirme faaliyetleri hakkındaki tüm bilgileri içeren Denetim Prosedürlerini oluşturmuş ve uygular. İlgili tüm tarafların bu prosedürlerin güncel bir setine erişimini ve uygulamalarını sağlar.
CAS, belgelendirme faaliyetlerinde yer alan denetçilerini, teknik uzmanlarını ve diğer personeli yerine getirdikleri fonksiyonlarda yeterli kılmak için eğitim ihtiyaçlarını belirlemekte, bunları vermekte veya verilmesini sağlar. Bu amaçla Personel Eğitim Prosedürü oluşturulmuş ve uygular.
CAS, belgelendirmenin verilmesi, reddedilmesi, sürdürülmesi, belgelendirmenin kapsamının genişletilmesi veya daraltılması, yenileme, askıya alma veya askıya alma sonrasında eski durumuna getirme veya belgelendirmeyi geri çekme kararını alan komite veya kişilerin, uygulanan standardı ve belgelendirme şartlarını anladığını, denetim proseslerini ve denetim ekibinin ilgili tavsiyelerini değerlendirmeye yönelik yeterli bilgi ve tecrübeye sahip olmasını sağlamak için kriterler Personel

Yetkinlik Matrisinde belirlenir.
CAS, denetim ve belgelendirme faaliyetlerinde yer alan personelin performansının tatmin edici bir performans göstermesini sağlar. Faaliyetlerdeki kullanım sıklığı ve faaliyetleriyle bağlantılı risk seviyesine göre, görev alan bütün kişilerin performansını izlemek için Personel Atama ve Performans Değerlendirme Prosedürünü oluşturmuş ve uygular. CAS, eğitim ihtiyacını belirlemek için, performanslarına göre personelin yeterliliğini gözden geçirir.
CAS, denetçinin yetkin olduğu kabul edilen her bir yönetim sistemi türünü dikkate alarak her bir denetçiyi izler. Denetçiler için izleme prosesi; saha değerlendirme, denetim raporlarının gözden geçirilmesi ve müşterilerin geribildiriminin bir kombinasyonunu içermekte ve kayıtları tutulur.
Bu izleme, özellikle müşterinin bakış açısından, belgelendirme proseslerine zararı en aza indirecek şekilde tasarlanır.
CAS, her denetçinin performansını periyodik olarak değerlendirir. Sahada değerlendirme sıklığı belirlenirken, mevcut izleme bilgileri doğrultusunda belirlenen ihtiyaçları temel alır.
ISO/IEC 17021-1:2015,Madde 7.2'nin gereklilikleri esas alındı.

Denetçi bilgi birikimi ve deneyiminin gösterilmesi

CAS, denetçilerin bilgi birikimi ve deneyime sahip olduğunu aşağıdaki yollardan gösterir:

a) tanınmış BGYS'ye özgü nitelikler;
b) geçerli olduğu durumda denetçi olarak kayıt olma;
c) BGYS eğitim kurslarına katılım ve konuyla ilişkili kişisel niteliklerin kazanılması;
d) güncel mesleki gelişim kayıtları;
e) başka bir BGYS denetçisi tarafından şahitlik edilen BGYS tetkikleri.

Denetçilerin seçilmesi

Ek olarak denetçi seçim kriterleri her denetçinin aşağıdaki şartları sağlamasını gerektirir:

a) Üniversite eğitimine eş değer seviyede mesleki eğitim veya öğrenime sahip olmalı;
b) BGYS denetçisi olarak görev yapmak için yeterli düzeyde bilgi teknolojileri ve bilgi güvenliği alanında pratik iş yeri deneyimine sahip olmalı,
c) BGYS denetimi konusunda yeterli eğitim almış olmak ve ISO/IEC 27001'e göre bir BGYS'yi denetleme becerilerini göstermek. Bu deneyim, bir BGYS değerlendiricisi (bkz. ISO/IEC 17021-1:2015, Madde 9.2.2.1.4) tarafından izlenen eğitim aşamasındaki denetçi olarak en az bir BGYS ilk belgelendirme denetiminde (aşama1 ve aşama2) veya yeniden belgelendirme ve en az bir gözetim tetkikinde görev alarak kazanılmalıdır.
d) Bu deneyim, son beş yıl içinde en az 10 BGYS yerinde tetkik gününde kazanılmalı ve gerçekleştirilmelidir. Katılım, belge incelemesini, risk değerlendirmesinin ve uygulanmasının gözden geçirilmesini ve tetkik raporlamasını kapsamalıdır,
e) bilgi güvenliği ve tetkiki konusundaki mevcut bilgi ve becerilerini güncel tutar. (referanslar, audit log vb.)

a) Aşama 1 tetkik raporlarında Aşama 2 tetkik ekibi uygunluğu denetim ekibinden bağımsız teknik gözden geçirme sürecinde kontrol edilecektir. Yapılan denetim ekibinden bağımsız teknik gözden geçirme belgelendirme karar alıcılarından biri veya yetkin teknik gözden geçiren tarafından doğrulanacaktır.

b) BGYS/KVYS ilk belgelendirme müşteri dosyaları incelenecek ve Aşama 1 tetkik raporlarında Aşama 2 tetkik ekibi uygunluğu kayıtlarının bulunduğu doğrulanacaktır.

NOT1 Becerilerin sürdürülmesi, sürekli mesleki gelişimle gösterilebilir. (kongre, konferans vb.)
NOT2 CAS, yukarıdaki gereklilik ve kanıtlara uygun bir yetkinlik kriterleri (referanslar, audit log vb.) talep eder. (ISO/IEC 17021-1:2015, Madde 7.1.2.).

Teknik uzmanların seçilmesi

Teknik uzman seçme süreci, her teknik uzmanın aşağıdaki niteliklere sahip olmasını sağlar:

a) Üniversite eğitimine eş değer seviyede mesleki eğitim veya öğrenime sahip olmalı,
b) teknik uzman olarak görev yapabilecek düzeyde bilgi teknolojileri ve bilgi güvenliği alanında pratik iş yeri deneyimine sahip olmalı,
c) bilgi güvenliği ve tetkiki konusundaki mevcut bilgi ve becerilerinin devamlılığını sağlamalı.

NOT Becerilerin devamlılığı, sürekli mesleki gelişim yoluyla gösterilebilir. (kongre, konferans vb.)

Ekibe liderlik edecek denetçilerin seçilmesi

Madde 7.2.2.2'ye ek olarak, ekibe liderlik bir denetçinin seçilmesinde uyulması gereken kriterler, denetçinin en az üç BGYS tetkikinin tüm aşamalarına etkin olarak katılmış olmalıdır. Bahsedilen katılım, başlangıç kapsamının belirlenmesi ve planlanması, dokümantasyonun gözden geçirilmesi, risk değerlendirmesinin ve uygulanmasının gözden geçirilmesi ve resmi tetkik raporlamasını içermelidir.

ISO/IEC 27006-1:2024,Madde 7.2.2'nin gereklilikleri esas alındı.

7.3 Dış kaynaklı bireysel denetçilerin ve teknik uzmanların kullanımı

CAS, dış kaynaklı denetçiler ve teknik uzmanlarla, belirlemiş olduğu politikalara ve prosedürlere uyacaklarının taahhüdünü içeren Başdenetçi/Denetçi Sözleşmesi ve Teknik Uzman Sözleşmesi yapar.

Sözleşmeler, gizlilik ve tarafsızlığa ilişkin hususları ele almakta, ayrıca dış kaynaklı denetçilerden ve teknik uzmanlardan, denetim için görevlendirilebilecekleri her bir kuruluşla mevcut olan veya önceki ilişkisini, CAS'ye bildirmelerini ister.

ISO/IEC 17021-1:2015,Madde 7.3'ün gereklilikleri esas alındı.

7.4 Personel kayıtları

CAS, ilgili yetkinlikler, eğitim, tecrübe, bağlantıları, mesleki durum ve yetkinlik dahil olmak üzere personelin kayıtlarını güncel tutar. Belgelendirme faaliyetlerini yerine getirenlere ilave olarak, yönetim ve idarede bulunan personel de bu duruma dâhildir.

ISO/IEC 17021-1:2015,Madde 7.4'ün gereklilikleri esas alındı.

7.5 Dış kaynak kullanımı

CAS, belgelendirmenin verilmesi, reddedilmesi, sürdürülmesi, belgelendirmenin kapsamının genişletilmesi veya daraltılması, yenileme, askıya alma veya askıya alma sonrasında eski durumuna getirme veya belgelendirmeyi geri çekme kararını, dış kaynaklı hizmet sağlayan hiç bir kuruluşa bırakmaz.

ISO/IEC 17021-1:2015,Madde 7.5'in gereklilikleri esas alındı.

7.6 İş tecrübelerinin Değerlendirilmesi:

ISO/IEC 27001:2022 AMD 1:2024 & ISO/IEC 27701 sistemleri için; tam zamanlı ve yarı zamanlı çalışmalar değerlendirilir. Denetçiler içinde her hangi bir kişinin pozisyonu değiştiğinde, değerlendirme yöntemleri tekrardan uygulanır. Değerlendirme metotları Tablo 1'de verilmiştir.

TABLO 1: DEĞERLENDİRME METODLARI TABLOSU

Değerlendirme Yöntemi	Uygulanan yöntemin amaçları	Değerlendirilmeye tabi tutulacaklar	İlgili kayıtlar/Açıklamamlar
Kayıtların kontrol edilmesi	Değerlendirilenin sunduğu cv veya bilgi formundaki bilgiler değerlendirilmesi. Verilen bilgiler ile diğer kayıtların (Diploma, sertifika, referans, denetim tecrübesi vb.) tutarlılığının kontrol edilmesi, yazılı ve sözlü doğrulamalar yapılması. (İş tecrübelerinin doğrulanmasında, doğrulama bilgileri formunda doğrulama bölümüne kaydedilir.)	Denetçi, Baş denetçi, Teknik Uzman, Belgelendirme karar alma personeli, BGYS-KVYS Planlama sorumlusu,	Personel Ön Değerlendirme Formu E BD D TU Atama Formu CV, Sertifika ve referanslar
Yazılı Sınav	Değerlendirilenin ilgili olduğu standart ve teknik alan bilgisinin değerlendirilmesi	Denetçi, Baş denetçi, Belgelendirme karar alma personeli,	Bilgi Güvenliği Yönetim Sistemi Başdenetçi/ Denetçi Sınav Formu BGYS Denetçi Adayı Yazılı Değerlendirme Sınavı KVYS Denetçi Adayı Yazılı Değerlendirme Sınavı YETKİNLİK ATAMA SINAVI CEVAP ANAHTARI Not: Denetçi ve baş denetçiler için eğer ilgili kişinin sahip olduğu sertifika bünyemizde açılan bir eğitimden alınmış ise tekrar yazılı veya sözlü

			bir değerlendirme yapılmayabilir.
Sözlü Sınav	Değerlendirilenin ilgili olduğu standartlardaki bilgisinin değerlendirilmesi Değerlendirilenin teknik alan bilgisinin değerlendirilmesi Değerlendirenin belgelendirme süreci bilgisinin değerlendirilmesi	Denetçi, Baş denetçi, Teknik Uzman, Belgelendirme karar alma personeli BGYS-KVYS Planlama sorumlusu, Belgelendirme Sorumlusu, Belgelendirme Müdürü	BGYS&KVYS Denetçi Adayı Sözlü Sınav Kontrol Formu Not: Denetçi ve baş denetçiler için eğer ilgili kişinin sahip olduğu sertifika bünyemizde açılan bir eğitimden alınmış ise tekrar yazılı veya sözlü bir değerlendirme yapılmayabilir.
Bire bir görüşme	Değerlendirilenin geçmiş iş tecrübeleri ile ilgili bilgilerin detaylandırmak. Spesifik konularda, bilgi ve beceriyi değerlendirmek. İşletme yönetimi ile ilgili değerlendirme yapmak.	Denetçi, Baş denetçi, Teknik Uzman, Belgelendirmeyi onaylayan personel	Personel Ön Değerlendirme Formu E BD D TU Atama Formu CV, Sertifika ve referanslar
Gözlem	Değerlendirilenin görev almak istediği pozisyonda, çalışma süresince bilgi ve beceri ve yetkinliğinin gözlemlenerek değerlendirilmesi	Denetçi, Baş denetçi, Teknik Uzman	BD-Denetçi Değerlendirme Formu (BGYS-KVYS) Baş Denetçi/ Denetçi
Geri Bildirimler	Değerlendirilenin, geçmiş iş referanslarının alınması. Müşterilerden gelen geri bildirimlerin (Anket, şikayet, beğeni vb.) değerlendirilmesi. Geçmişte beraber çalıştığı kişilerin yorumlarının değerlendirilmesi.	Denetçi, Baş denetçi, Teknik Uzman	BD-Denetçi Değerlendirme Formu (BGYS-KVYS) Şikâyet / İtiraz Formu

*ISO/IEC 27001:2022 AMD 1:2024 & ISO/IEC 27701 denetim ekibi personelinin sahip olması gereken yeterlilikler aşağıdaki tabloda yer almaktadır,

TABLO 2: ISO/IEC 27001:2022 AMD 1:2024 & ISO/IEC 27701 DENETİM EKİBİ GÖREVLİSİ YETKİNLİK TABLOSU
ISO/IEC 17021-1:2015, Madde 7.2'deki ve ISO/IEC 27006-1:2024 Madde 7.2.2' deki gereklilikler ve kılavuz da geçerlidir.

DENETİM EKİBİ GÖREVLİSİ	DENETÇİ		BAŞDENETÇİ		TEKNİK UZMAN	
YETKİNLİK KRİTERİ	GEREKLİ YETKİNLİK	YETKİNLİK GÖSTERGESİ	GEREKLİ YETKİNLİK	YETKİNLİK KRİTERİ	GEREKLİ YETKİNLİK	YETKİNLİK GÖSTERGESİ
Öğrenim	Üniversite eğitimine eş değer seviyede mesleki eğitim veya öğrenime sahip olmalı	Diploma	Denetçi ile aynı	Diploma	Üniversite eğitimine eş değer seviyede mesleki eğitim veya öğrenime sahip olmalı	Diploma
Temel İş Tecrübesi	3 yıl/4 yıl en az iş tecrübesi **Yüksek Okul (ön lisans) ve/veya 4 yıllık Üniversite (lisans) öğrenimi için 3 yıllık iş tecrübesi**	Mevcut İş Tecrübe Kayıtları	Denetçi ile aynı	Denetçi ile aynı	3 yıl/4 yıl İlgili teknik alanda en az	Mevcut İş Tecrübe Kayıtları
Bilgi Teknolojileri, Bilgi güvenliği, Kişisel veri KVKK, İş sürekliliği, Hizmet yönetimi alanındaki iş tecrübesi	BGYS için, Bilgi Teknolojileri alanda tecrübe en az 2 yılı Diğer herhangi bir alanda en az 1 yıl, Yukarıdaki sağlanıyor ise KVYS, alanında en az 6 ay	Mevcut İş Tecrübe Kayıtları	Denetçi ile aynı	Mevcut İş Tecrübe Kayıtları	- 3 yıl/4 yıl İlgili teknik alanda en az Yukarıdaki sağlanıyor ise KVYS, alanında en az 6 ay	Mevcut İş Tecrübe Kayıtları
Denetçi Eğitimi	Uluslararası kabul görmüş geçerli bir yönetim sistemi Denetçi eğitimini (ilk 40 saatlik, ilave YS için 24 saat) başarı ile tamamlamış olmak.	Baş Denetçi/ Denetçi Eğitim Sertifikası	Uluslararası kabul görmüş geçerli bir yönetim sistemi Denetçi eğitimini (ilk 40 saatlik, ilave YS için 24 saat) başarı ile tamamlamış olmak.	Baş Denetçi/ Denetçi Eğitim Sertifikası	--	--
Denetim Tecrübesi	Denetim ekibi lideri veya bir denetçinin yönlendirmesi ve rehberliğinde eğitim gören (aday) denetçi olarak en az 1 tam denetim (Aşama.1 ve Aşama.2 veya Yeniden Belgelendirme ve en az bir Gözetim denetim tecrübesi. Bu deneyim, son beş yıl içinde en az 10 BGYS yerinde tetkik gününde kazanılmalı ve gerçekleştirilmelidir. Katılım,	Denetim kayıtları	Yetkin bir denetim ekibi liderinin yönlendirmesi ve rehberliğinde (aday) denetim ekibi lideri rolü üstlenerek en az 3 BGYS tetkikinin tüm aşamalarına etkin olarak katılmış olmalıdır. Bahsedilen katılım, başlangıç kapsamının belirlenmesi ve planlanması, dokümantasyonun gözden geçirilmesi, risk değerlendirmesinin ve	Denetim kayıtları	İlk denetiminde baş denetçi tarafından teknik uzman değerlendirmesine tabi tutularak başarılı bulunmalıdır. Tetkik raporu yeterliliği; • objektif delil • örnekleme • kapsam uygunluğu • hariç tutulan maddelerin doğruluğu	--

	belge incelemesini, risk değerlendirmesinin ve uygulanmasının gözden geçirilmesini ve tetkik raporlamasını kapsamalıdır, İlave YS' lerin her biri için denetim ekibi lideri veya bir denetçinin yönlendirmesi ve rehberliğinde (aday) denetçi olarak toplam en az 2 tam denetim ve 10 gün süreli denetim tecrübesi. Denetimler ardışık son 3 yıl içinde tamamlanmış olmalıdır.		uygulanmasının gözden geçirilmesi ve resmi tetkik raporlamasını içermelidir. İlave YS' lerde denetim ekibi liderliği için ayrıca adaylık süreci aranmayacaktır. ISO/IEC 27001, ISO/IEC 27701, standartlarında daha önce başka bir UDK' dan atanmış olan Baş Denetçi(ler) CAS' den 1 tam denetim izlemesi tecrübesi ile ataması yapılır.		• gözlem/iyileştirme alanlarının yeterliliğine göre değerlendirilecektir.	

DENETİM EKİBİ GÖREVLİSİ	**DENETÇİ**		**BAŞDENETÇİ**		**TEKNİK UZMAN**	
YETKİNLİK KRİTERİ	**GEREKLİ YETKİNLİK**	**YETKİNLİK GÖSTERGESİ**	**GEREKLİ YETKİNLİK**	**YETKİNLİK KRİTERİ**	**GEREKLİ YETKİNLİK**	**YETKİNLİK GÖSTERGESİ**
İş yönetim uygulamaları	Endüstride iyi bilgi güvenliği uygulamaları Bilgi güvenliği politikaları ve iş gereksinimleri Genel işletme yönetimi kavramları, uygulamaları ve arasındaki ilişki Yönetim politikası, hedefleri ve sonuçları süreçleri ve ilgili terminoloji, Bilgi güvenliği ve mahremiyeti (Kişisel Veri Yönetim Sistemi) ile ve hizmet yönetimine özel dokümantasyon yapıları, hiyerarşi ve karşılıklı ilişkiler, Bilgi güvenliği ve mahremiyeti (Kişisel Veri Yönetim Sistemi) ile ve hizmet yönetimine özel ile ilgili araçlar, yöntemler, teknikler ve bunların uygulamalar, Bilgi güvenliği ve mahremiyeti (Kişisel Veri Yönetim Sistemi) ile ve hizmet yönetimine özel risk değerlendirmesi ve risk yönetimi, Bilgi güvenliği ve mahremiyeti(Kişisel Veri Yönetim Sistemi) ile ve hizmet yönetimine özel bilgisi yönetimi için geçerli süreçler, Bilgi güvenliği ve mahremiyeti (Kişisel Veri Yönetim Sistemi) ile ve hizmet yönetimine özel muhtemelen ilgili veya bir sorun olabilecek mevcut teknoloji,	Referanslar İlgili BGYS Rehberi - Eğitimi BGYS Kategori sınavları Birebir görüşmede başarılı olunması Personel Ön Değerlendirme Formu Referanslar Eğitimi KVYS Yetkinlik sınavları Birebir görüşmede başarılı olunması Personel Ön Değerlendirme Formu KVYS)	Endüstride iyi bilgi güvenliği uygulamaları Bilgi güvenliği politikaları ve iş gereksinimleri Genel işletme yönetimi kavramları, uygulamaları ve politikası, hedefleri ve sonuçları arasındaki ilişki Yönetim süreçleri ve ilgili terminoloji Bilgi güvenliği ve mahremiyete özel dokümantasyon yapıları, hiyerarşi ve karşılıklı ilişkiler, Bilgi güvenliği ve mahremiyet bilgi yönetimi (Kişisel Veri Yönetim Sistemi) ile ilgili araçlar, yöntemler, teknikler ve bunların uygulamalar, Bilgi güvenliği ve mahremiyet risk değerlendirmesi ve risk yönetimi, Bilgi güvenliği ve mahremiyet bilgisi yönetimi için geçerli süreçler, Bilgi güvenliği ve mahrem bilgilerinin korunmasında muhtemelen ilgili veya bir sorun olabilecek mevcut teknoloji,	Referanslar İlgili BGYS Rehberi Eğitimi BGYS Kategori sınavları Birebir görüşmede başarılı olunması Personel Ön Değerlendirme Formu Referanslar Eğitimi KVYS Yetkinlik sınavları Birebir görüşmede başarılı olunması Personel Ön Değerlendirme Formu KVYS)	Endüstride iyi bilgi güvenliği uygulamaları Bilgi güvenliği politikaları ve iş gereksinimleri Genel işletme yönetimi kavramları, uygulamaları ve politikası, hedefleri ve sonuçları arasındaki ilişki Yönetim süreçleri ve ilgili terminoloji Bilgi güvenliği ve mahremiyete özel dokümantasyon yapıları, hiyerarşi ve karşılıklı ilişkiler, Bilgi güvenliği ve mahremiyet bilgi yönetimi (Kişisel Veri Yönetim Sistemi) ile ilgili araçlar, yöntemler, teknikler ve bunların uygulamalar, Bilgi güvenliği ve mahremiyet risk değerlendirmesi ve risk yönetimi, Bilgi güvenliği ve mahremiyet bilgisi yönetimi için geçerli süreçler, Bilgi güvenliği ve mahrem bilgilerinin korunmasında muhtemelen ilgili veya bir sorun olabilecek mevcut teknoloji	Referanslar İlgili BGYS Rehberi - Eğitimi Birebir görüşmede başarılı olunması
Tetkik Prensipleri, Uygulamaları ve Teknikleri bilgisi	CAS prosedürlerine ve 27001 /27701 gerekliliklerine uygun olarak tetkik yapabilme kabiliyeti,	İlgili standartta CAS Yazılı sınavları Başarı ile tamamlamak (%70 başarı) ISO/IEC 27001 Baş denetçi olmak ISO/IEC 27701 Baş denetçi olmak DP Değerlendirme Formu (tanık denetim)	CAS prosedürlerine ve 27001 /27701 gerekliliklerine uygun olarak tetkik yapabilme kabiliyeti,	İlgili standartta CAS Sözlü sınavını Başarı ile tamamlamak (%70 başarı) ISO/IEC 27001 Baş denetçi olmak ISO/IEC 27701 Baş denetçi olmak DP Değerlendirme Formu (tanık denetim)	Yeterli teknik bilgiyi denetçiye aktarabilmeli	---
Bilgi Güvenliği dahil kişisel veri yönetim sistemi, iş sürekliliği ve hizmet Yönetim Sistemleri, Standartları ve ilgili normatif dokümanlar hakkındaki bilgisi	IAF MD serisi dokümanları, ISO 27000 Bilgi Güvenliği Yönetim Sistemi (BGYS) temeller, tanımlar, terimler, ISO 27003 - Kurulum yönergesi, ISO 27004 – BGYS ölçümler yönergesi, ISO 27005 - Risk yönetimi, ISO 27007 - Bilgi Teknolojisi – Güvenlik Teknikleri	KVYS Denetçi Adayı Yazılı Değerlendirme Soruları BGYS Denetçi Adayı Yazılı Değerlendirme Soruları (%70 başarı) ve Eğitim sertifikaları	IAF MD serisi dokümanları, ISO 27000 Bilgi Güvenliği Yönetim Sistemi (BGYS) temeller, tanımlar, terimler, ISO 27003 - Kurulum yönergesi, ISO 27004 – BGYS ölçümler yönergesi, ISO 27005 - Risk yönetimi, ISO 27007 - Bilgi Teknolojisi	Bilgi Güvenliği Yönetim Sistemi Başdenetçi/Denetçi Sınav Formu Değerlendirme Sınavı BGYS Denetçi Adayı Yazılı Değerlendirme Sınavı KVYS Denetçi Adayı Yazılı Değerlendirme	---	---

İş sürekliliği Bilgisi	standartlarına hakim olmalı		– Güvenlik Teknikleri standartlarına hakim olmalı	Sınavı Değerlendirme Sınavı (%70 başarı) ve Eğitim sertifikaları		
Müşterinin Ürünü/Hizmeti Prosesleri, Organizasyonu Hakkındaki Bilgisi	İlgili alanda ürün/ Hizmet proses, organizasyon bilgisi	İlgili BGYS Rehberi Eğitimi BGYS Kategori sınavları KVYS Yetkinlik Yazılı Sınavı Referans Yazıları DP Değerlendirme Formu	İlgili alanda ürün/ Hizmet proses, organizasyon bilgisi	İlgili BGYS Rehberi Eğitimi BGYS Kategori sınavları KVYS Yetkinlik Yazılı Sınavı Referans Yazıları DP Değerlendirme Formu (tanık denetim)	İlgili alanda ürün/ Hizmet proses, organizasyon bilgisi	İlgili BGYS Rehberi Eğitimi Referans Yazıları
Sunum Becerisi ve görüşme becerileri	Kişisel özellikler ile bilgi ve becerileri uygulama kabiliyetinin etkinliğinin değerlendirilmesi	DP Değerlendirme Formu (tanık denetim) Müşterinin Başdenetçi/ denetçi Değerlendirme Formu	Kişisel özellikler ile bilgi ve becerileri uygulama kabiliyetinin etkinliğinin değerlendirilmesi	DP Değerlendirme Formu (tanık denetim) Müşterinin Başdenetçi/ denetçi Değerlendirme Formu	--	--
Not Tutma ve Rapor Yazma Becerisi	Not tutma ve rapor yazma konusunda becerili olmalı	DP Değerlendirme Formu (tanık denetim) Müşterinin Başdenetçi/ denetçi Değerlendirme Formu	Not tutma ve rapor yazma konusunda becerili olmalı	DP Değerlendirme Formu (tanık denetim) Müşterinin Başdenetçi/ denetçi Değerlendirme Formu	--	--
CAS Proses Bilgisi	Kuruluşun kültürü içinde, kuruluş ve raporlama yapısı içinde etkin olarak çalışabilme Kabiliyeti	Oryantasyon eğitimi ortak portal kullanımı ve atama dosyası	Kuruluşun kültürü içinde, kuruluş ve raporlama yapısı içinde etkin olarak çalışabilme Kabiliyeti	Oryantasyon eğitimi ortak portal kullanımı ve atama dosyası	Kuruluşun kültürü içinde, kuruluş ve raporlama yapısı içinde etkin olarak çalışabilme Kabiliyeti	Oryantasyon eğitimi ortak portal kullanımı ve atama dosyası
Müşteri kuruluşundaki bütün seviyelerinde uygun lisan becerileri	Kuruluşun her seviyesindeki personel ile uygun terimler, ifade ve konuşma kullanarak etkin bir şekilde iletişim kurma becerisi olmalı.	İlgili BGYS Rehberi Eğitimi DP Değerlendirme Formu (tanık denetim) Müşterinin Başdenetçi/ denetçi Değerlendirme Formu	Kişisel dil becerileri yoluyla veya tercüman vasıtasıyla etkin şekilde iletişim kurma kabiliyetlerine sahip olmalı	İlgili BGYS Rehberi Eğitimi DP Değerlendirme Formu (tanık denetim) Müşterinin Başdenetçi/ denetçi Değerlendirme Formu	--	--
Bilgi güvenliği kişisel bilgi yönetimi, iş sürekliliği ve hizmet yönetimi terminolojisi, ilkeler, uygulamalar ve teknikleri hakkındaki bilgisi	BGYS/KVYS ait özel terminoloji uygulamalara ve tekniklere sahip olmalı BGYS VE KVYS özel dokümantasyon yapıları, hiyerarşi ve ilişkiler; Bilgi güvenliği yönetim kişisel bilgi yönetimi ve hizmet yönetimi ile ilgili araç, yöntem, teknik ve uygulamaları; Bilgi güvenliği kişisel bilgi yönetimi ve hizmet yönetimi risk değerlendirme ve risk yönetimi; BGYS VE KVYS'e uygulanabilir süreçlerini (proseslerini) Mevcut teknolojilerle alakalı nerede bilgi güvenliği sorunları olabileceğini bilmeli (İlgili teknolojik alana sahip ise)	ISO/IEC 27001 ve ISO 27000 Serisi Standartları Eğitimi DP Değerlendirme Formu (tanık denetim) Müşterinin Başdenetçi/ denetçi Değerlendirme Formu	BGYS/KVYS ait özel terminoloji uygulamalara ve tekniklere sahip olmalı BGYS VE KVYS özel dokümantasyon yapıları, hiyerarşi ve ilişkiler; Bilgi güvenliği yönetim kişisel bilgi yönetimi ve hizmet yönetimi ile ilgili araç, yöntem, teknik ve uygulamaları; Bilgi güvenliği kişisel bilgi yönetimi ve hizmet yönetimi risk değerlendirme ve risk yönetimi; BGYS/KVYS uygulanabilir süreçlerini (proseslerini) Mevcut teknolojilerle alakalı nerede bilgi güvenliği sorunları olabileceğini bilmeli (İlgili teknolojik alana sahip ise)	ISO/IEC 27001 ve ISO 27000 Serisi Standartları Eğitimi DP Değerlendirme Formu (tanık denetim) Müşterinin Başdenetçi/ denetçi Değerlendirme Formu	BGYS/KVYS ait özel terminoloji uygulamalara ve tekniklere sahip olmalı Mevcut teknolojilerle alakalı nerede bilgi güvenliği sorunları olabileceğini bilmeli	İlgili BGYS Rehberi Eğitimi
Müşteri iş sektörü	-Yasal ve düzenleyici gereksinimler hakkında bilgi sahibi olmalı (sektör koduna sahip ise) -Sektörün bilgi güvenliği	İlgili BGYS Rehberi Eğitimi BGYS Kategori sınavları	-Yasal ve düzenleyici gereksinimler hakkında bilgi sahibi olmalı (sektör koduna sahip ise) - Sektörün bilgi güvenliği	İlgili BGYS Rehberi İlgili BGYS Rehberi Eğitimi BGYS Kategori sınavları	-Yasal ve düzenleyici gereksinimler hakkında bilgi sahibi olmalı (sektör koduna sahip ise)	İş tecrübesi kayıtları Yeterli iş tecrübesine sahip olmak.

	/mahremiyet /hizmet yönetim riskleri -Sektöre özgü terminoloji, varlıkları, proses ve teknolojileri -Sektör uygulamaları	KVYS Yetkinlik Yazılı Sınavları Yazılı Sınavı Referans Yazıları DP Değerlendirme Formu (tanık denetim)	/mahremiyet /hizmet yönetim riskleri -Sektöre özgü terminoloji, varlıkları, proses ve teknolojileri -Sektör uygulamaları	KVYS Yetkinlik Yazılı Sınavları Referans Yazıları DP Değerlendirme Formu (tanık denetim)	- Sektörün bilgi güvenliği /mahremiyet /hizmet yönetim riskleri -Sektöre özgü terminoloji, varlıkları, proses ve teknolojileri - Sektör uygulamaları	İlgili BGYS Rehberi Eğitimi
Bilgi Teknolojisi Güvenlik Teknikleri - Bilgi Güvenliği Kontrolleri İçin Uygulama Prensipleri bilgisi (ISO IEC 27002)	Denetimlerine ilişkin standardına uygun sorgulama yetkinliğine sahip olmalı	Eğitim kaydı /sertifikası Baş Denetçilerin BD-Denetçi Değerlendirme Formu (tanık denetim)	Denetimlerine ilişkin standardına uygun sorgulama yetkinliğine sahip olmalı	Eğitim kaydı /sertifikası Baş Denetçilerin BD Denetçi Değerlendirme Formu (tanık denetim)		
(TEKNOLOJİK ALAN) ALT YAPI BİLGİSİ Ağ yönetimi Sistem yönetimi Güvenlik yönetimi	Aşağıdaki alt yapı uygulamalar hakkında bilgi sahibi olmalı ; SİSTEM YÖNETİMİ: Sunucular, Storage Yedeklilik Sistemleri (load balancer gibi), Veri merkezleri (iklimlendirme, kesintisiz güç sistemleri gibi), Sunucu İşletim Merkezleri, Masaüstü yönetimi, Sanallaştırma, Bulut bilişimi AĞ YÖNETİMİ; Yerel ağlar, Geniş alan ağları, İletişim Teknolojileri (mobil ağ, Karasal Ağ gibi), Kablosuz Ağ Teknolojileri GÜVENLİK YÖNETİMİ; Güvenlik Sistemleri (Firewall, proxy, IPS, IDS gibi), Log yönetimi, TEKNİK AÇIKLIK ANALİZİ; (kısıtlamalar, tarama testleri, penetrasyon testleri, zafiyet değerlendirmeleri) KRİPTOGRAFİ; (SSL, VPN gibi)	Teknolojik alan sınavı Baş Denetçilerin BD-Denetçi Değerlendirme Formu (tanık denetim) Referans yazısı	Aşağıdaki alt yapı uygulamalar hakkında bilgi sahibi olmalı; SİSTEM YÖNETİMİ: Sunucular,Storage ,Yedeklilik Sistemleri (load balancer gibi), Veri merkezleri (iklimlendirme, kesintisiz güç sistemleri gibi), Sunucu İşletim Merkezleri, Masaüstü yönetimi, Sanallaştırma, Bulut bilişimi AĞ YÖNETİMİ; Yerel ağlar, Geniş alan ağları, İletişim Teknolojileri (mobil ağ, Karasal Ağ gibi), Kablosuz Ağ Teknolojileri GÜVENLİK YÖNETİMİ; Güvenlik Sistemleri (Firewall, proxy, IPS, IDS gibi), Log yönetimi, TEKNİK AÇIKLIK ANALİZİ; (kısıtlamalar, tarama testleri, penetrasyon testleri, zafiyet değerlendirmeleri) KRİPTOGRAFİ; (SSL, VPN gibi)	Teknolojik alan sınavı DP Değerlendirme Formu (tanık denetim) (tanık denetim) Referans yazısı	Aşağıdaki alt yapı uygulamalar hakkında bilgi sahibi olmalı ; SİSTEM YÖNETİMİ: Sunucular,Storage ,Yedeklilik Sistemleri (load balancer gibi), Veri merkezleri (iklimlendirme, kesintisiz güç sistemleri gibi), Sunucu İşletim Merkezleri, Masaüstü yönetimi, Sanallaştırma, Bulut bilişimi AĞ YÖNETİMİ; Yerel ağlar, Geniş alan ağları, İletişim Teknolojileri (mobil ağ, Karasal Ağ gibi), Kablosuz Ağ Teknolojileri GÜVENLİK YÖNETİMİ; Güvenlik Sistemleri (Firewall, proxy, IPS, IDS gibi), Log yönetimi, TEKNİK AÇIKLIK ANALİZİ; (kısıtlamalar, tarama testleri, penetrasyon testleri, zafiyet değerlendirmeleri) KRİPTOGRAFİ; (SSL, VPN gibi)	DP Değerlendirme Formu (tanık denetim) (tanık denetim) Referans yazısı
(TEKNOLOJİK ALAN) Yazılım Ve Uygulama Temini Bilgisi	Aşağıdaki yazılım ve uygulama temini hakkında bilgi sahibi olmalı, Uygulama (Software) Geliştirme Özelleştirilmiş Yazılım Temini Paket Programları Mobil uygulamalar Web tabanlı uygulamalar	Teknolojik alan sınavı DP Değerlendirme Formu (tanık denetim) (tanık denetim) Referans yazısı	Aşağıdaki yazılım ve uygulama temini hakkında bilgi sahibi olmalı, Uygulama (Software) Geliştirme Özelleştirilmiş Yazılım Temini Paket Programları Mobil uygulamalar Web tabanlı uygulamalar	Teknolojik alan sınavı DP Değerlendirme Formu (tanık denetim) (tanık denetim) Referans yazısı	Aşağıdaki yazılım ve uygulama temini hakkında bilgi sahibi olmalı, Uygulama (Software) Geliştirme Özelleştirilmiş Yazılım Temini Paket Programları Mobil uygulamalar Web tabanlı uygulamalar	Teknolojik alan sınavı DP Değerlendirme Formu (tanık denetim) (tanık denetim) Referans yazısı
(TEKNOLOJİK ALAN) Yazılım Ve Veri Uygulama Yönetimi Bilgisi	Aşağıdaki Yazılım Ve Veri Uygulama Yönetimi hakkında bilgi sahibi olmalı ; YAZILIM VE VERİ UYGULAMA YÖNETİMİ; Elektronik mesajlaşma (E-posta, Kurumsal Anlık Mesajlaşma) Tasarım ve modelleme uygulamaları (CAD-CAM) (Örneğin autocad, 3Dmax portal uygulamaları gibi) VERİ YÖNETİMİ; • Veri tabanları sistemleri (DBA) • Veri yönetimi teknikleri (Büyük veri, veri	Teknolojik alan sınavı DP Değerlendirme Formu (tanık denetim) (tanık denetim) Referans yazısı	Aşağıdaki Yazılım Ve Veri Uygulama Yönetimi hakkında bilgi sahibi olmalı ; YAZILIM VE VERİ UYGULAMA YÖNETİMİ; Elektronik mesajlaşma (E-posta, Kurumsal Anlık Mesajlaşma) Tasarım ve modelleme uygulamaları (CAD-CAM) (Örneğin autocad, 3Dmax portal uygulamaları gibi) VERİ YÖNETİMİ; • Veri tabanları sistemleri (DBA) • Veri yönetimi teknikleri (Büyük veri, veri	Teknolojik alan sınavı DP Değerlendirme Formu (tanık denetim) (tanık denetim) Referans yazısı	Aşağıdaki Yazılım Ve Veri Uygulama Yönetimi hakkında bilgi sahibi olmalı ; YAZILIM VE VERİ UYGULAMA YÖNETİMİ; Elektronik mesajlaşma (E-posta, Kurumsal Anlık Mesajlaşma) Tasarım ve modelleme uygulamaları (CAD-CAM) (Örneğin autocad, 3Dmax portal uygulamaları gibi) VERİ YÖNETİMİ; • Veri tabanları sistemleri (DBA) • Veri yönetimi	Teknolojik alan sınavı DP Değerlendirme Formu (tanık denetim) (tanık denetim) Referans yazısı

	madenciliği, İş zekası) • Doküman Yönetim Sistemi • CRM Kurumsal Kaynak Planlama (ERP) ÜRETİM YAZILIM UYGULAMA; Endüstriyel kontrol sistemleri Elektronik devre tasarımları		madenciliği, İş zekası) • Doküman Yönetim Sistemi • CRM Kurumsal Kaynak Planlama (ERP) ÜRETİM YAZILIM UYGULAMA; Endüstriyel kontrol sistemleri Elektronik devre tasarımları		teknikleri (Büyük veri, veri madenciliği, İş zekası) • Doküman Yönetim Sistemi • CRM Kurumsal Kaynak Planlama (ERP) ÜRETİM YAZILIM UYGULAMA; Endüstriyel kontrol sistemleri Elektronik devre tasarımları	
(TEKNOLOJİK ALAN) E-hizmet yönetimi hakkında bilgi	E-Uygulamalar; E-fatura Elektronik Ticaret (Online ödeme sistemleri) E-arşiv E-defter E-imza	Teknolojik alan sınavı DP Değerlendirme Formu (tanık denetim) (tanık denetim) Referans yazısı	E-Uygulamalar; E-fatura Elektronik Ticaret (Online ödeme sistemleri) E-arşiv E-defter E-imza	Teknolojik alan sınavı DP Değerlendirme Formu (tanık denetim) (tanık denetim) Referans yazısı	E-Uygulamalar; E-fatura Elektronik Ticaret (Online ödeme sistemleri) E-arşiv E-defter E-imza	Teknolojik alan sınavı DP Değerlendirme Formu (tanık denetim) (tanık denetim) Referans yazısı

TABLO 3: ISO/IEC 27001:2022 AMD 1:2024 & ISO/IEC 27701 PLANLAMA SORUMLUSU – BELGELENDİRME KARARI ALAN PERSONEL YETKİNLİK TABLOSU

YETKİNLİK KRİTERİ	PLANLAMA SORUMLUSU		BELGELENDİRME KARARI ALAN PERSONEL	
	GEREKLİ YETKİNLİK	YETKİNLİK GÖSTERGESİ	GEREKLİ YETKİNLİK	YETKİNLİK GÖSTERGESİ
Öğrenim	Min. Ön Lisans	Diploma	En az Ön Lisans Mezunu olmak gereklidir	Diploma
Toplam iş Tecrübesi	En az 1 yıl	Mevcut İş Tecrübe Kayıtları	3 yıl/4 yıl en az iş tecrübesi **Yüksek Okul (ön lisans) ve/veya 4 yıllık Üniversite (lisans) öğrenimi için 3 yıllık iş tecrübesi**	Mevcut İş Tecrübe Kayıtları
Bilgi Teknolojileri, Bilgi güvenliği, Kişisel veri KVKK, İş sürekliliği, Hizmet yönetimi alanındaki iş tecrübesi	Diğer yönetim sistemleri de dahil en az 2 yıl	Mevcut İş Tecrübe Kayıtları	BGYS için, Bilgi Teknolojileri alanda tecrübe en az 2 yılı Diğer herhangi bir alanda en az 1 yıl, Yukarıdaki sağlanıyor ise KVYS en az 6 ay	Mevcut İş Tecrübe Kayıtları
Denetçi Eğitimi	---	--	Uluslararası kabul görmüş geçerli bir yönetim sistemi Denetçi eğitimini (ilk 40 saatlik, ilave YS için 24 saat) başarı ile tamamlamış olmak.	Eğitim Sertifikası
Denetim Tecrübesi	---	---	Denetim ekibi lideri veya bir denetçinin yönlendirmesi ve rehberliğinde eğitim gören (aday) denetçi olarak en az 1 tam denetim (Aşama.1 ve Aşama.2 veya Yeniden Belgelendirme ve en az bir Gözetim denetim tecrübesi. Bu deneyim, son beş yıl içinde en az 10 BGYS yerinde tetkik gününde kazanılmalı ve gerçekleştirilmelidir. Katılım, belge incelemesi, risk değerlendirmesinin ve uygulanmasının gözden geçirilmesini ve tetkik raporlamasını kapsar, Tetkik raporu yeterliliği; •objektif delil •örnekleme •kapsam uygunluğu •hariç tutulan maddelerin doğruluğu •gözlem/iyileştirme alanlarının yeterliliğine göre değerlendirilecektir.	Denetim kayıtları
Tetkik Prensipleri, Uygulamaları ve Teknikleri bilgisi	CAS prosedürleri ve 27001:2022 AMD 1:2024/ 27701 Denetim gereklilikleri hakkında bilgi sahibi olması	Planlama sorumlusu Yetkinlik Performans değerlendirmesi	CAS prosedürlerine ve 27001:2022 AMD 1:2024/27701 gerekliliklerine uygun tetkik proseslerini bilmesi	İlgili standartta CAS Yazılı sınavları Başarı ile tamamlamak (%70 başarı) 27001:2022 AMD 1:2024 /227701 denetçisi olmak DP Değerlendirme Formu (tanık denetim)

Bilgi Güvenliği dahil kişisel veri yönetim sistemi İş sürekliliği Yönetim Sistemi ve hizmet Yönetim Sistemleri, Standartları ve ilgili normatif dokümanlar hakkındaki bilgisi	BGYS eğitimleri, IAF MD serisi dokümanları, ISO 27000 Bilgi Güvenliği Yönetim Sistemi temeller, tanımlar, terimler, ISO 27002 - BGYS en iyi pratikler yönergesi, ISO 27003 - Kurulum yönergesi, ISO 27004 - BGYS ölçümler yönergesi, ISO 27005 - Risk yönetimi, ISO 27007 - Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri Denetimi için kılavuz, standartlarına	Eğitim kayıtları ve sertifikaları	BGYS eğitimleri, IAF MD serisi dokümanları, ISO 27000 Bilgi Güvenliği Yönetim Sistemi temeller, tanımlar, terimler, ISO 27002 - BGYS en iyi pratikler yönergesi, ISO 27003 - Kurulum yönergesi, ISO 27004 - BGYS ölçümler yönergesi, ISO 27005 - Risk yönetimi, ISO 27007 - Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri Denetimi için kılavuz, standartlarına	Eğitim kayıtları BGYS Yazılı Sınavı KVYS Yazılı Sınavı (%70 başarı)
Müşterinin ürünü, süreçleri ve organizasyonu ile ilgili bilgi	BGYS/KVYS ve belgelendirmede organizasyon türü, boyutu, yönetim, yapı, işlev ve geliştirme ve dış kaynak kullanımı gibi faaliyetlerin uygulanmasına ilişkin ilişkilerin etkisi; Geniş bir perspektif içinde karmaşık işlemler; Ürün veya hizmet için geçerli olan yasal ve düzenleyici gereksinimleri Hakkında bilgi sahibi olmalı (Gerekli bilginin mevcudiyeti teknik destek ile sağlanabilir)	İlgili alanda teknik yetkinliği olan denetim ekibi üyelerinden destek alabilmeli Planlama sorumlusu yetkinlik performans değerlendirme listesi Referans yazıları Rehber eğitimi	BGYS/KVYS ve belgelendirmede organizasyon türü, boyutu, yönetim, yapı, işlev ve geliştirme ve dış kaynak kullanımı gibi faaliyetlerin uygulanmasına ilişkin ilişkilerin etkisi; Geniş bir perspektif içinde karmaşık işlemler; Ürün veya hizmet için geçerli olan yasal ve düzenleyici gereksinimlerini bilmeli (Gerekli bilginin mevcudiyeti teknik destek ile sağlanabilir)	Baş Denetçilerin BD-Denetçi Değerlendirme Formu (tanık denetim) Denetim Ekibi Üyesi Mülakat Formu Denetim Ekibi Üyesi - Komite Üyesi Uygunluk Mülakat-Değerlendirme Formu (BGYS-KVYS) Rehber eğitimi Referans yazıları BGYS Kategori sınavları
Müşteri iş sektörü	BGYS ait özel terminoloji uygulamalara ve tekniklere sahip olmalı BGYS özel dokümantasyon yapıları, hiyerarşi ve ilişkiler; bilgi güvenliği yönetim ile ilgili araç, yöntem, teknik ve uygulamaları; bilgi güvenliği risk değerlendirme ve risk yönetimi; BGYS'nin uygulanabilir süreçlerini (proseslerini) Bilgi güvenliği ve mahremiyeti(Kişisel Veri Yönetim Sistemi) ile ve hizmet yönetimine özel dokümantasyon yapıları, hiyerarşi ve karşılıklı ilişkiler, Bilgi güvenliği ve mahremiyeti(Kişisel Veri Yönetim Sistemi) ile ve hizmet	İlgili alanda teknik yetkinliği olan denetim ekibi üyelerinden destek alabilmeli Planlama sorumlusu yetkinlik performans değerlendirme listesi Referans yazıları Rehber eğitimi	BGYS ait özel terminoloji uygulamalara ve tekniklere sahip olmalı BGYS özel dokümantasyon yapıları, hiyerarşi ve ilişkiler; bilgi güvenliği yönetim ile ilgili araç, yöntem, teknik ve uygulamaları; bilgi güvenliği risk değerlendirme ve risk yönetimi; BGYS'nin uygulanabilir süreçlerini (proseslerini) Bilgi güvenliği ve mahremiyeti(Kişisel Veri Yönetim Sistemi) ile ve hizmet yönetimine özel dokümantasyon yapıları, hiyerarşi ve karşılıklı ilişkiler, Bilgi güvenliği ve mahremiyeti(Kişisel Veri Yönetim Sistemi) ile ve hizmet yönetimine özel ile ilgili araçlar, yöntemler, teknikler ve bunların uygulamalar, Bilgi güvenliği ve mahremiyeti(Kişisel Veri Yönetim Sistemi) ile ve hizmet yönetimine özel risk değerlendirmesi ve risk yönetimi, Bilgi güvenliği ve mahremiyeti(Kişisel Veri Yönetim Sistemi) ile ve hizmet yönetimine özel bilgisi yönetimi için geçerli süreçler, Bilgi güvenliği ve mahremiyeti(Kişisel Veri Yönetim Sistemi) ile ve hizmet yönetimine özel muhtemelen ilgili veya bir sorun olabilecek mevcut teknoloji Mevcut teknolojilerle alakalı nerede bilgi güvenliği sorunları olabileceğini bilmeli (Gerekli bilginin mevcudiyeti teknik destek ile	Baş Denetçilerin BD-Denetçi Değerlendirme Formu (tanık denetim) Denetim Ekibi Üyesi Mülakat Formu Denetim Ekibi Üyesi - Komite Üyesi Uygunluk Mülakat-Değerlendirme Formu (BGYS-KVYS) Rehber eğitimi Referans yazıları BGYS Kategori sınavları KVYS Yetkinlik Yazılı Sınavı

	yönetimine özel ile ilgili araçlar, yöntemler, teknikler ve bunların uygulamalar, Bilgi güvenliği ve mahremiyeti(Kişisel Veri Yönetim Sistemi) ile ve hizmet yönetimine özel risk değerlendirmesi ve risk yönetimi, Bilgi güvenliği ve mahremiyeti(Kişisel Veri Yönetim Sistemi) ile ve hizmet yönetimine özel bilgisi yönetimi için geçerli süreçler, Bilgi güvenliği ve mahremiyeti(Kişisel Veri Yönetim Sistemi) ile ve hizmet yönetimine özel muhtemelen ilgili veya bir sorun olabilecek mevcut teknoloji, Mevcut teknolojilerle alakalı nerede bilgi güvenliği sorunları olabileceği hakkında bilgi sahibi olmalı (Gerekli bilginin mevcudiyeti teknik destek ile sağlanabilir)		sağlanabilir)	
Bilgi güvenliği ve mahremiyeti (Kişisel Veri Yönetim Sistemi) ile ve hizmet yönetim terminolojisi, ilkeler, uygulamalar ve teknikler			BGYS/KVYS özel dokümantasyon yapıları, hiyerarşi ve ilişkileri BGYS/KVYS risk değerlendirme ve risk yönetimi BGYS/KVYS uygulanabilir proseslerini BGYS/KVYS ile ilgili mevcut teknolojiler	Baş Denetçilerin BD-Denetçi Değerlendirme Formu (tanık denetim) Rehber eğitimi Referans yazıları BGYS Kategori sınavları KVYS Yetkinlik Yazılı Sınavı
İş Yönetim Uygulamaları			Endüstride iyi BGYS/KVYS uygulamaları BGYS/KVYS politikaları ve iş gereksinimleri Genel işletme yönetimi kavramları, uygulamaları ve politikası, hedefleri ve sonuçları arasındaki ilişki Yönetim süreçleri ve ilgili terminoloji	Baş Denetçilerin BD-Denetçi Değerlendirme Formu (tanık denetim) Rehber eğitimi Referans yazıları BGYS Kategori sınavları KVYS Yetkinlik Yazılı Sınavı

TABLO 4. TEKNOLOJİK ALANLAR-ISO/IEC 270012022 AMD 1:2024 & ISO/IEC 27701

TA 1.ALT YAPI	TA.1.1 SİSTEM YÖNETİMİ	TA.1.2 AĞ YÖNETİMİ	TA.1.3 GÜVENLİK YÖNETİMİ
	• Sunucular • Storage • Yedeklilik Sistemleri (load balancer gibi) • Veri merkezleri (iklimlendirme, kesintisiz güç sistemleri gibi) • İşletim Merkezleri • Masaüstü yönetimi • Sanallaştırma • Bulut Bilişim	• Yerel ağlar • Geniş alan ağları • İletişim Teknolojileri (mobil ağ, Karasal Ağ gibi) • Kablosuz Ağ Teknolojileri	• Güvenlik Sistemleri (Firewall, proxy, IPS, IDS gibi) • Log yönetimi **TA.1.4 TEKNİK AÇIKLIK ANALİZİ** • Kısıtlamalar, tarama testleri, penetrasyon testleri, zafiyet değerlendirmeleri **TA.1.5 KRİPTOGRAFİ** • SSL, VPN

TA.2 YAZILIM VE UYGULAMA TEMİNİ	**TA.2.1 YAZILIM VE UYGULAMA TEMİNİ** • Uygulama (Software) Geliştirme • Özelleştirilmiş Yazılım Temini • Paket Programları • Mobil uygulamalar • Web tabanlı uygulamalar		
TA.3 YAZILIM VE VERİ UYGULAMA YÖNETİMİ	**TA.3.1 YAZILIM VE VERİ UYGULAMA YÖNETİMİ** • Elektronik mesajlaşma (E-posta, Kurumsal Anlık Mesajlaşma) • Tasarım ve modelleme uygulamaları (CAD-CAM) (Örneğin autocad, 3Dmax portal uygulamaları gibi)	**TA.3.2 VERİ YÖNETİMİ** • Veri tabanları sistemleri (DBA) • Veri yönetimi teknikleri (Büyük veri, veri madenciliği, iş zekası) • Doküman Yönetim Sistemi • CRM • Kurumsal Kaynak Planlama (ERP)	**TA.3.3 ÜRETİM YAZILIM UYGULAMA** • Endüstriyel kontrol sistemleri • Elektronik devre tasarımları
TA.4 HİZMET YÖNETİMİ	**TA.4.1 E-UYGULAMALAR** • E-fatura • Elektronik Ticaret (Online ödeme sistemleri) • E-arşiv • E-defter • E-imza		

7.7 Denetim Ekibi Personeli ve belgelendirmeyi komitesi Personelinin Yetkinlik Alanında Atanması

BGYS ve KVYS alanında yetkinlik atamaları denetim ekibi personelinin ilgili alandaki yetkinliğini için yeterli iş tecrübesi, bilgisi, denetçi eğitimi ve denetim deneyimine göre değerlendirilir. TABLO 2' de yer alan yeterlilikleri karşıladığı taktirde, Tablo 5'de yer alan iş tecrübeleri ve teknik alanları dikkate alınarak sektör kategorilerine göre atamaları gerçekleştirir.

Tablo 5: Sektör Gruplarına Göre Çalışma Tecrübesi Belirleme Tablosu

Teknik Alan	Teknik Alan Kodu	Alt Teknik Alan Kodu	Alt Teknik Alan
Üretim & Hizmet Sektörü	A	A.01	Tarım, ormancılık, gıda ürünleri imalatı, otel işletmeleri ve restoran
		A.02	Madencilik, metalik olmayan ürünler, beton, çimento, kireç, alçı, sıva vb
		A.03	Tekstil, Deri, Ağaç, Plastik ve Kauçuk ürünleri ile sınıflandıramamış diğer ürünlerin üretimi
		A.04	Yayıncılık, Matbaacılık ve Basım
		A.05	Kağıt, Petrol ürünleri, İlaç ve Kimyasalların imalatı
		A.06	Metal ürünleri, Makine, Teçhizat, Elektrik, Optik ürünler, Gemi, Havacılık, Uzay ve Ulaşım Araçları imalatı
		A.07	Elektrik, Gaz ve Su temini
		A.08	Geri Dönüşüm, Taşımacılık, Depolama, Diğer Sosyal Hizmetler
		A.09	İnşaat ve Mühendislik Hizmetleri
		A.10	Toptan ve Perakende Ticaret; Motorlu Araçlar, Motosiklet, Kişisel Eşyalar ve Ev Eşyalarının Tamiri, Finansal Aracılık; Arsa ve Emlakçılık; Kiralama, Bilgi Teknolojileri, Kamu Yönetimi, Eğitim, Sağlık, Sosyal İşler ve Diğer Hizmetler
-Planlamacı tarafından ,EA Listesinden sektör tespit edilip Tablo 5'de eşleşen sektör kodlarından birini barındıran ve ilgili teknolojik alan yeterliliği olan - Sektör Gruplarına Göre Çalışma Tecrübesi Belirleme Tablosu; ISO/IEC 27001, ISO/IEC 27701 için geçerlidir.			

8 Bilgi gereklilikleri

8.1 Halkla ilişkiler

ISO/IEC 17021-1:2015,Madde 8.1'in gereklilikleri esas alındı.

8.2 Belgelendirme dokümanı

ISO/IEC 17021-1:2015,Madde 8.2'nin gereklilikleri esas alındı.

BGYS Belgelendirme dokümanları

Belgelendirme dokümanları, bu sorumluluğa atanmış bir görevli ve/veya Genel Müdür tarafından imzalanır. Belgelendirme dokümanlarında SOA Uygulanabilirlik Beyanının sürüm bilgisini içerir.
NOT SOA Uygulanabilirlik Beyanında yapılacak bir değişiklik, belgelendirme kapsamında ki kontrollerin içeriğini değiştirmiyorsa belgelendirme dokümanlarında güncelleme gerekmez.
Kuruluşun belgelendirme kapsamındaki faaliyetlerinden hiçbiri belirli bir fiziksel konumda yürütülmüyorsa, belgelendirmede kuruluşun tüm faaliyetlerinin uzaktan yürütüldüğünü belirtir.
ISO/IEC 27006-1:2024,Madde 8.2.2'nin gereklilikleri esas alındı.

BGYS belgelendirme dokümanlarında diğer standartlara atıflar

Belgelendirme dokümanları, ulusal ve uluslararası standartlara yalnızca aşağıdaki durumlarda atıfta bulunabilir:

a) Kuruluş, ISO/IEC 27001:2022, Madde 6.1.3 c)'ye uygun olarak, gerekli tüm kontrollerini referans kontrol kaynağındaki kontrollerle karşılaştırarak, bu kontrollerden herhangi birini farkında olmadan hariç tutmadığını belirlemişse;
b) ISO/IEC 27001:2022, Madde 6.1.3 d)'ye uygun olarak, hariç tutulan referans kontrollerin gerekçesi Uygulanabilirlik Beyanı (SoA) içinde belirtilmişse.

Referans kontrol standartları, ISO/IEC 27001:2022, Ek A'ya dayalı olabilir veya bilgi güvenliği kontrollerini içeren standartlardır.
Belgelendirme dokümanlarında, SoA'da uygulanan kontrol setinin/setlerinin yalnızca BGYS'deki kontrollerin dahil edilmesi veya hariç tutulmasının uygunluğuna atıfta bulunmak için kullanıldığı ve uygunluk değerlendirmesi için kullanılmadığı belirtir.
ISO/IEC 27006-1:2024,Madde 8.2.3'ün gereklilikleri esas alındı.

8.3 Belgelendirmeye atıflar ve işaretlerin kullanımı

ISO/IEC 17021-1:2015,Madde 8.3'ün gereklilikleri esas alındı.

8.4 Gizlilik

ISO/IEC 17021-1:2015,Madde 8.4'ün gereklilikleri esas alındı.

Kurumsal kayıtlara erişim

Belgelendirme tetkikinden önce, CAS gizli veya hassas bilgiler içermesi sebebiyle tetkik ekibinin gözden geçirmesine açamayacağı BGYS'e ilişkin bilgilerin (BGYS kayıtları veya kontrollerin tasarımı ve etkinliği ile ilgili BGYS kayıtları veya bilgiler gibi) var olup olmadığını müşteriden bildirmesini ister.
CAS, bu tarz bilginin eksikliği halinde BGYS'nin yeterli bir şekilde tetkik edilip edilemeyeceğine karar verir. Bir yetersizlik olma durumunda denetim ve belgelendirme gerçekleşmez. Müşterinin gerekli tedbirleri alması ve eksiklerin giderilmesi beklenir.
CAS, BGYS'nin tanımlanan gizli veya hassas bilgi olmadan yeterli bir şekilde tetkikinin mümkün olmadığı sonucuna varırsa, müşteriye, gerekli erişim düzenlemeleri yapılmadan belgelendirme tetkikinin yapılamayacağını bildirir. Aksi durumda ise Belgelendirme faaliyetlerine deva medilir.
ISO/IEC 27006-1:2024,Madde 8.4.2'nin gereklilikleri esas alındı.

8.5 Belgelendirme kuruluşu ve müşterileri arasında bilgi alışverişi

ISO/IEC 17021-1:2015,Madde 8.5'in gereklilikleri esas alındı.

REVİZYON BİLGİLERİ		
Rev. No	**Revizyon Tarihi**	**Revizyon Açıklaması**
0	05.01.2022	İlk yayın.
1	04.08.2023	Madde 3.İlgili Dokümanlar başlığı altında olan gereksiz bilgiler çıkartıldı. Madde 4.2' den çıkartmalar yapıldı.
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
4	26.02.2026	BGYS süreç kontrol mekanizması artıtıldı.

HAZIRLAYAN:	ONAYLAYAN:
YÖNETİM TEMSİLCİSİ	GENEL MÜDÜR