BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ UYUM DENETİMİ YAPAN FİRMALAR İÇİN DENETİM ŞARTLARI

No	Firma Denetim Şartları
1	Firma, IAF üyesi bir akreditasyon kuruluşu tarafından akredite edilmiş bir belgelendirme kuruluşunca verilen ve geçerliliği devam etmekte olan ISO/IEC 27001 belgesine sahip olmalıdır.
2	Firmada, Belgelendirme Programı Madde 5.1.1'i sağlayan en az 1 (bir) D1 veya D2 tipi denetçinin tam zamanlı çalışıyor olmalıdır. Belirtilen denetçilerin haricinde Belgelendirme Programı Madde 5.1.2'yi sağlayan en az 1 (bir) başdenetçi firmada tam zamanlı çalışıyor olmalıdır. Firmada tam zamanlı olarak çalışan denetçiler aynı anda başka bir firmada denetçi olarak istihdam edilemez.
3	Firma, denetim çalışmalarını etkin bir şekilde yürütebilecek düzeyde organizasyon, mekân, teknik altyapı ve donanım, belge ve kayıt düzenine sahip olmalıdır.
4	Firmanın, BİG Rehber denetimlerini nasıl gerçekleştireceğine yönelik üst seviye bilgi içeren bir kalite kontrol ya da metodoloji içeren politika, prosedürü olmalıdır.
5	Denetimler firma veya firmada çalışan denetçiler tarafından sözleşme tarihinden önceki iki yıl içerisinde rehber uyum faaliyetleri konusunda danışmanlık hizmeti verilmemiş olan kurumlara gerçekleştirilmelidir.
6	Firma aynı kuruma art arda üçten fazla denetim hizmeti vermemiş olmalıdır.
7	Denetim öncesinde denetim yaptıran kurum ile firma arasında hizmet alım sözleşmesi ve gizlilik sözleşmesi imzalanmalıdır. Hizmet alım sözleşmesinde; • Denetimin amacı, kapsamı, • Sözleşmenin feshine ilişkin şartlar, • İhtiyaç olunan uzmanlık alanındaki denetçi bilgileri • Denetim kapsamında hazırlanması gereken rapor, çalışma formları gibi belgelerin format ve özellikleri, • BİG Rehberinde yer alan "Tedarikçi İlişkileri Güvenliği" başlığı altındaki tedbirler, • Firma ve denetim ekibinde yer alacak tüm personelin gizlilik taahhütnamesi imzalayacağı hususunda hükümler yer almalıdır.
8	Firmanın denetim kapsamı değişikliği durumları için standart bir formu bulunmalıdır. Denetim esnasında denetim kapsamına yapılabilecek olası eklemeler ve güncellemeler için gelen talepler bu standart form üzerinden yapılmalıdır. Denetim kapsamının dışına kuruluşun yazılı izni olmadan çıkılmamalıdır.
9	Aşağıda belirtilen dokümanlar firmanın doküman yapısında bulunmalı ve denetim faaliyetlerinde kullanılmalıdır; • Ek – A: Denetim Ekibi Bilgisi • Ek – B: Varlık Grupları Ve Denetim Kapsamı • Ek – C: Denetim Programı

	• Ek – D: Çalışma Formu • Ek – E: Rehber Uygulama Süreci Etkinlik Durumu • Ek – F: Tedbir Etkinlik Durumu • Ek – G: Bulgu Tablosu • Ek – H: Denetim Görüşü • Ek – I: Gizlilik Taahhütnamesi • Ek – J: Tarafsızlık Taahhütnamesi
10	Firma, denetime başlamadan önce kuruluşunun irtibat noktasını tekrar bilgilendirmelidir.
11	Firma, denetim raporunu aşağıdaki başlıkları içerecek şekilde hazırlamalıdır; • Rapor Kapağı: Kurum adı, denetim tarihi ve raporu hazırlayan denetçi bilgilerini içerir. • Yönetici Özeti: Denetimin yapılma amacını, kapsamını, kapsam dışı bırakılan hususlar var ise bu hususların kapsam dışı bırakılma nedenlerini, denetim gerçekleştirilirken uygulanan metodolojiyi, Kurumun Rehbere uyum durumunu, elde ettiği bulguların Kurum bilgi güvenliğinde yaratacağı risklerin kısa bir özetini içerir. • İçindekiler: Rapor içeriğine ilişkin dizin bilgisini içerir. • Tanımlar ve Kısaltmalar: Denetim raporunda yer alan ve tanımlanmasının raporun anlaşılması açısından faydalı olacağı değerlendirilen kavramlar ile raporda yer alan kısaltmaların açık haline yönelik bilgiyi içerir. • Giriş: Kurumun bilgi güvenliği kapsamında uyum sağlaması gereken yasal düzenlemeler, bilgi güvenliğine yönelik organizasyon yapısı, bilişim sistemleri kapsamında iç ve dış paydaşlara hizmet veren sistem, uygulama ve altyapısı hakkında genel bilgiyi içerir. • Denetim Kapsamına İlişkin Bilgi: Kurum bilişim sistemlerinde yer alan varlık gruplarından hangilerinin denetim kapsamına dâhil edilip edilmediğine yönelik bilgiyi içerir. • Denetim Görüşü: EK – H'de yer alan şablonun, denetim görüşünü yansıtacak şekilde denetim ekibi tarafından doldurularak ekipte yer alan tüm denetçiler ve Kurum Üst Yöneticisi tarafından imzalanması sonucu oluşturulan dokümandır. Ekler: Denetim kapsamındaki varlık grupları, denetim ekibi bilgisi, bulgu tablosu, denetim görüşü ile denetçinin rapor içeriğinde bahsettiği ve ek olarak sunmak istediği diğer bilgi, belge ve dokümanı içerir.
12	Denetim raporu denetimde görev alan denetçiler tarafından doldurulmalıdır. Denetim raporunun gözden geçirilmesi /onaylanması farklı kişiler tarafından yapılmalıdır.

13	Firma ve denetçiler, denetim çalışmalarını yürütürken kurum kaynakları dışında herhangi bir uygulama, cihaz vb. araç kullandığı durumda, denetim çalışmalarını tamamladıktan sonra bu araçlar üzerindeki kuruma ait her tür bilgiyi kurum gözetiminde geri döndürülemeyecek şekilde silmeli veya mümkünse imha işlemini gerçekleştirerek yapılan işlemleri tutanak altına almalı ve söz konusu tutanak kayıtları en az 3 (üç) yıl süreyle saklanmalıdır. Süreci tanımlayan prosedürler oluşturulmalı ve uygulanmalıdır.
14	Her bir denetim çalışmasına ilişkin tüm belgelerin ekleriyle birlikte **elektronik ortamda** denetim dosyası haline getirilmesi zorunludur. Denetim dosyasının **denetim sürecinde** oluşturulması esastır. Firma, denetim raporunun imzalandığı tarih itibarıyla bahsi geçen bilgi, belge ve kayıtların bütünlüğünü sağlayacak mekanizmayı tesis etmekle mükelleftir. Örnek HASH bilgisinin kayıt edilmesi.
15	Denetim raporunu oluşturan belgelerin her sayfası ekler dâhil denetim ekibinde yer alan denetçiler tarafından 5070 sayılı Elektronik İmza Kanunu hükümlerine göre oluşturulan güvenli elektronik imza ile imzalanarak rapor nihai haline getirilmelidir. Firmanın denetim raporlarını e-imza ile imzalama sistemi olmalı ve uygulamalıdır.
16	Denetim faaliyetleri ile ilgili gerek kurum/kuruluş tarafından doldurulan anket, form vb. dokümanlar gerekse firma tarafından üretilen denetim raporu ve ekleri gibi dokümanlar gizlilik derecesine sahip dokümanlardır. Bu tür dokümanlar üretim, kullanım, saklama, aktarım ve imha aşamalarında hassasiyetle ele alınmalı; çalınma, yetkisiz erişim, kaybolma vb. risklere karşı yetkilendirilmiş firma tarafından korunmalıdır. Bu dokümanlara gizlilik derecesini belirten işaret konmalıdır.
17	Denetim sonunda firma tarafından hazırlanan Denetim Dosyası ve özet (hash) bilgisi kurumlara elektronik ortamda şifreli bir medya halinde denetim öncesinde anlaşma yapılan kuruluş yetkilisine (Denetim Dosyasının bütünlüğünün bozulmasını önleyecek yöntemler kullanılarak) teslim edilmelidir ve teslim edildiğine dair kayıtlar (tutanak, email vs) tutulmalıdır.
18	Firma ve denetçiler saklama süresi dolan bilgi, belge ve dokümanları geri döndürülemeyecek şekilde imha edebilir. İmha sürecinde yapılan işlemler tutanak ile kayıt altına alınmalı ve söz konusu tutanak kayıtları en az 3 (üç) yıl süreyle saklanmalıdır. Süreci tanımlayan prosedürler oluşturulmalı ve kayıtlar tutulmalıdır.
19	Firma tarafında sadece denetim kapsamını, kurum / kuruluşa teslim edilen denetim dosyasının boyutunu, dosyanın özet (hash) bilgisini ve teslim edilme tarihini içeren bilgiler taraflarca tutanak altına alınarak elektronik ortamda saklanmalıdır. Firma bu bilgileri en az 3 (üç) yıl süre ile güvenli ortamlarda saklamalıdır. Bu tür bilgiler, örnek mahiyetinde kullanılmak amacıyla belirli verileri anonim hale getirilse dahi üçüncü taraflarla paylaşılmamalıdır. Denetim ekibi bunların dışında herhangi bir belge, doküman veya sair bilgiyi Kurum dışına çıkarmamalıdır.

20	Firma kuruluşa yapacağı denetimde, en az 1 adet denetçi ve en az 1 adet başdenetçiyi görevlendirmelidir. Firma, bir denetim öncesinde o denetimde yer alacak denetçileri resmi olarak belirlemeli ve atamalıdır.
21	Denetim hizmeti veren firma, denetim ekibinde yer alan denetçi ve uzmanların tamamına EK – I Gizlilik Taahhütnamesi ve EK – J Tarafsızlık Taahhütnamesini imzalatmalıdır.
22	Denetçiler, denetim öncesinde kuruluş tarafından değerlendirilmeli ve onaylanmalıdır.
23	Firma, hangi personelinin hangi denetimlerde görev aldığını dair kayıtları tutmalı ve en az 3 yıl süre ile bu kayıtları saklamalıdır.
24	<u>Denetçi/Başdenetçi personel değişikliği:</u> • Firma, TSE tarafından belgeli bir denetçi/başdenetçi personel firmadan ayrıldığında veya firmada göreve başladığında bu durumu 15 takvim günü içerisinde TSE'ye bildirmelidir. • Firmadan ayrılan personel, firmanın belgelendirmesinde değişikliğe neden oluyor ise ayrılış tarihini müteakip iki (2) ay içerisinde eşdeğer yetkinliğe sahip bir personel istihdam edilmelidir. Bu süre içerisinde yetkinlik şartı sağlanamadığından dolayı belgeli firma belgelendirme programı kapsamında Bilgi ve İletişim Güvenliği Uyum Denetimleri gerçekleştiremez, yapılan denetimler ise geçersiz sayılır. Firmanın yetkilendirilmesinde değişikliğe neden olan personelin ayrılış tarihini müteakip iki (2) ay içerisinde eşdeğer yetkinliğe sahip bir personel istihdam edilememesi durumunda firmanın denetim yapma yetkisi askıya alınır. Süreci tanımlayan prosedürler oluşturulmalı ve uygulanmalıdır.
25	Firma yaptığı denetimler esnasında kuruluş çalışanlarının kişisel bilgilerine ulaşması durumunda, bu bilgileri üçüncü taraflarla paylaşmamalı, denetim sonuç raporuna eklememeli ve bir kopyasını kendisine almamalıdır. Süreci tanımlayan prosedürler oluşturulmalı ve uygulanmalıdır.
26	Firma faaliyetlerinin yasal olarak sonlandığı durumda, saklama süresi dolan bilgi, belge ve dokümanlar geri döndürülemeyecek şekilde imha edilmelidir. İmha sürecinde yapılan işlemler tutanak ile kayıt altına alınmalı ve söz konusu tutanak kayıtları en az 3 (üç) yıl süreyle saklanmalıdır. Firma bu süreci kendi prosedürlerinde tanımlamalıdır. Güvenli ve geri döndürülemez imha yöntemleri prosedürlerde tanımlanmalı ve ihtiyaç durumunda kullanılmalıdır.

- Denetim hizmeti verecek firma, Soru listesinde belirtilen şartların dışındaki BİG Rehberi ve BİG Denetim Rehberindeki tüm şartları sağlamalıdır.
- TSE saklanması zorunlu tutulan bilgi ve belgenin hangi ortamlarda tutulduğuna yönelik, firmadan bilgi ve inceleme talebinde bulunduğu takdirde; firma gerekli bilgiyi TSE'ye ibraz etmek ve inceleme çalışmalarına uygun ortam sağlamakla yükümlüdür.