REVİZYON TABLOSU /REVISION TABLE		
Revizyon No ***/Revision Number***	**Revizyon Tarihi** ***/ Revision Date***	**Revizyon Nedeni** ***/ Reason for Revision***
00	25.03.2021	İlk Yayın */ First broadcast*
01	18.11.2021	Türkak Kapsam Genişletme Denetimi Oluşan Uygunsuzluktan Dolayı */ Türkak Scope Expansion Audit Due to Nonconformity*
02	17.07.2023	ISO 27001:2022 geçişinden dolayı revizyon */ Revision due to ISO 27001:2022 transition*

1. AMAÇ */PURPOSE*

Bu prosedürün amacı; ISO/IEC 27006:2015/AMD 1 2020 standardı doğrultusunda hazırlanan BGYS dokümantasyonunun açıklanması, Denetçi yeterliliklerinin belirlenmesi, denetimlerin planlanması, gerçekleştirilmesi ve belgelendirme kararının alınması için yöntem ve sorumlulukları belirlemektir.

/ The purpose of this procedure is; To explain the ISMS documentation prepared in line with the ISO/IEC 27006:2015/AMD 1 2020 standard, to determine the methods and responsibilities for determining auditor qualifications, planning and carrying out audits and taking certification decisions.

2. TANIMLAR */ DEFINITIONS*

BGYS: Bilgi Güvenliği Yönetim Sistemi

*/ **ISMS:** Information Security Management System*

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

*/ **Information Security Management System:** It is a part of the entire management system based on establishing, realizing, operating, monitoring, reviewing, maintaining information security and business risk approach.*

Uygulanabilirlik Beyanı (SOA): Kuruluşun BGYS'si ile ilgili ve uygulanabilir kontrol amaçlarını ve kontrolleri açıklayan dokümante edilmiş beyan.

/ Statement of Applicability (SOA): Documented statement describing the control objectives and controls relevant to the organization's ISMS and applicable.

3. PRENSİPLER */ PRINCIPLES*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı madde 4'teki hükümler geçerlidir.

/ The provisions of the ISO/IEC 17021-1:2015 standard and article 4 of the ISO/IEC 17021-1 System Certification Handbook apply.

4. GENEL ŞARTLAR */ GENERAL CONDITIONS*

4.1. Yasal ve Sözleşmeyle İlgili Hususlar */ Legal and Contractual Considerations*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı ve Bilgi Güvenliği El Kitabı madde 5.1'deki hükümler geçerlidir.

/ The provisions of the ISO/IEC 17021-1:2015 standard and ISO/IEC 17021-1 System Certification Handbook and Information Security Handbook article 5.1 are valid.

4.2. Tarafsızlığın Yönetilmesi */ Managing Impartiality*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı ve Bilgi Güvenliği El Kitabı madde 5.2'deki hükümler geçerlidir. Ayrıca aşağıdaki BGYS'ye özel şartlar ve kılavuz uygulanmaktadır.

/ The provisions of the ISO/IEC 17021-1:2015 standard and ISO/IEC 17021-1 System Certification Handbook and Information Security Handbook article 5.2 are valid. In addition, the following ISMS-specific conditions and guidance apply.

4.2.1. BG 5.2 Çıkar Çatışmaları */ IS 5.2 Conflicts of Interest*

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

/ AVACERT may perform the following tasks without being considered consultancy or creating a potential conflict of interest:

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

/ a) Trainings; Organizing training or participating as a trainer, provided that it is open to general participation and limited to the provision of general information, where it is related to information security management, relevant management systems or auditing (for example, provided that it does not provide specific recommendations to the organization that conflict with the requirements of paragraph b) below),

b) Belgelendirme denetim standartlarının şartlarının, AVACERT'in yorumunu açıklayan bilgilerin, talep üzerine erişime açılması veya yayınlanması,

/ b) Making the information explaining AVACERT's interpretation of the terms of the certification audit standards accessible or published upon request,

c) Belgelendirme denetimi için hazır olunup olunmadığını belirlemek için denetimden önce yapılan faaliyetler (bu tür faaliyetler, bu maddeyle çelişen tavsiyelerin sağlanmasıyla sonuçlanamaz ve AVACERT, bu tür faaliyetlerin, bu gereklerle çelişmediğini ve bunların belgelendirme denetim süresinde bir azalmaya neden olacak şekilde kullanılmadığını garanti eder),

/ c) Activities carried out before the audit to determine readiness for the certification audit (such activities may not result in the provision of recommendations that conflict with this clause and AVACERT guarantees that such activities do not conflict with these requirements and are not used in a way that would result in a reduction in the certification audit time);

d) Akreditasyon kapsamında bulunanların haricindeki standartlara veya düzenlemelere göre ikinci ve üçüncü taraf denetimlerin yapılması,

/ d) Conducting second and third party audits according to standards or regulations other than those within the scope of accreditation,

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

/ e) Providing added value during certification audits and audits (for example, identifying opportunities for improvement revealed during the audit without recommending special solutions).

AVACERT, belgelendirmeye tabi kuruluşun BGYS'nin BGYS iç denetimini gerçekleştiren kuruluş veya kuruluşlardan (herhangi bir birey de dâhil olmak üzere) bağımsızdır ve bu hizmetleri kendisi sunmamaktadır.

/ AVACERT is independent from the organization or organizations (including any individual) that perform the ISMS internal audit of the ISMS of the organization subject to certification and does not provide these services itself.

4.3. Yükümlülük ve Finansman */ Liability and Financing*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı ve Bilgi Güvenliği El Kitabı madde 5.3'deki hükümler geçerlidir.

/ The provisions of the ISO/IEC 17021-1:2015 standard and ISO/IEC 17021-1 System Certification Handbook and Information Security Handbook article 5.3 are valid.

5. YAPISAL ŞARTLAR */ STRUCTURAL CONDITIONS*

5.1. Organizasyon Yapısı ve Üst Yönetim */ Organizational Structure and Senior Management*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı madde 6.1'deki hükümler geçerlidir.

/ The provisions of the ISO/IEC 17021-1:2015 standard and article 6.1 of the ISO/IEC 17021-1 System Certification Manual apply.

5.2. Operasyonel Kontrol / *Operational Control*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı madde 6.2'deki hükümler geçerlidir.

/ The provisions of the ISO/IEC 17021-1:2015 standard and article 6.2 of the ISO/IEC 17021-1 System Certification Manual apply.

6. KAYNAK ŞARTLARI / *WELDING CONDITIONS*

6.1. Personelin Yeterliliği / *Competence of Personnel*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı ve Bilgi Güvenliği El Kitabı madde 7.1 ile PR-11 Personel Atama ve Performans Değerlendirme Prosedüründeki hükümler geçerlidir.

/ The provisions of the ISO/IEC 17021-1:2015 standard and article 7.1 of the ISO/IEC 17021-1 System Certification Handbook and Information Security Handbook and the PR-11 Personnel Appointment and Performance Evaluation Procedure are valid.

AVACERT, BGYS belgelendirmesinin yapılabilmesi için gereken temel yetkinlikleri, denetlenecek faaliyetlere ve ilgili bilgi güvenliği konularına uygun olan yeterliliğe sahip personeli seçmek ve yönetmek için kriterleri, PR-11 Personel Atama ve Performans Değerlendirme Prosedürü doğrultusunda belirlemiş ve dokümante etmiştir.

/ AVACERT has determined and documented the basic competencies required for ISMS certification and the criteria for selecting and managing competent personnel suitable for the activities to be audited and relevant information security issues, in line with the PR-11 Personnel Assignment and Performance Evaluation Procedure.

6.1.1. BG 7.1.1 Genel Değerlendirmeler / *IS 7.1.1 General Evaluations*

6.1.1.1. Genel Yeterlilik Şartları / *General Qualification Requirements*

AVACERT, denetleyeceği müşteri kuruluşun BGYS'si ile ilgili teknolojik ve yasal gelişmelere dair bilgi birikimine sahip personel bulundurmaktadır veya ihtiyaç olunca ulaşabilmektedir.

/ AVACERT employs personnel with knowledge of technological and legal developments regarding the ISMS of the customer organization it audits, or can be reached when needed.

AVACERT, BGYS belgelendirmesinin yapılabilmesi için gereken temel yetkinlikleri, denetlenecek faaliyetlere ve ilgili bilgi güvenliği konularına uygun olan kabiliyet ve yetkinliğe sahip bireyleri seçmek, temin etmek ve yönetmek için kriterleri, PR-11 Personel Atama ve Performans Değerlendirme Prosedürü doğrultusunda belirlemiş ve dokümante etmiş olup buna uygun personeli seçmektedir.

/ AVACERT has determined and documented the basic competencies required for ISMS certification, the criteria to select, provide and manage individuals with the ability and competence suitable for the activities to be audited and relevant information security issues, in line with the PR-11 Personnel Appointment and Performance Evaluation Procedure, and selects personnel.

ISO/IEC 27001 belgelendirme faaliyetleri için AVACERT tarafından belirlenmiş olan teknik alanlar ve alt teknik alanlar, aşağıda yer alan tabloda verilmiştir:

/ The technical areas and sub-technical areas determined by AVACERT for ISO/IEC 27001 certification activities are given in the table below:

Teknik Alan *technical area*	**Teknik Alan Kodu** *technical area code*	**Alt Teknik Alan Kodu** *lower technical area code*	**Alt Teknik Alan** *lower technical area*
Üretim Sektörü */ Production Sector*	A	A.01	01 Tarım, Ormancılık */01 Agriculture, Forestry* 03 Gıda Ürünleri İmalatı */03 Food Products Manufacturing* 30 Otel İşletmeleri ve Restoran */30 Hotels and Restaurants*
		A.02	02 Madencilik */02 Mining* 15 Metalik olmayan ürünler */15 Non-metallic products* 16-Beton, çimento, kireç, alçı, sıva vb */16-Concrete, cement, lime, plaster, plaster etc.*
		A.03	04 Tekstil Ürünleri */04 Textile Products* 05 Deri Ürünleri */05 Leather Products* 06 Ağaç Ürünleri */06 Wood Products* 14 Plastik ve Kauçuk Ürünleri */14 Plastic and Rubber Products* 23 Sınıflandıramamış diğer ürünlerin üretimi */23 Production of other unclassified products*
		A.04	07 Kağıt ve Kağıt Ürünleri */07 Paper and Paper Products* 08 Yayıncılık */08 Publishing* 09 Matbaacıtık ve Basım */09 Printing and Printing*
		A.05	10 Petrol Ürünleri */10 Petroleum Products* 12 Kimyasalların İmalatı */12 Manufacturing of Chemicals* 13 İlaç */13 Medicine*
		A.06	17 Metal ürünleri İmalatı */17 Manufacturing of metal products* 18 Makine ve Teçhizat */18 Machinery and Equipment* 19 Elektrik ve Optik ürünler */19 Electrical and Optical products* 20 Gemi */20 Ships* 22 Ulaşım Araçları İmalatı */22 Transportation Vehicles Manufacturing*
		A.07	25 Elektrik Temini */25 Electricity Supply* 26 Gaz Temini */26 Gas Supply* 27 Su Temini */27 Water Supply*
		A.08	24 Geri Dönüşüm */24 Recycling*
		A.09	28 İnşaat */28 Construction*
Hizmet Sektörü */ Service Sector*	B	B.01	29 Toptan ve Perakende Ticaret */29 Wholesale and Retail Trade*
		B.02	31 Ulaşım, Depolama, İletişim */31 Transportation, Storage, Communication*
		B.03	34 Mühendislik Hizmetleri */34 Engineering Services*
		B.04	35 Diğer Hizmetler */35 Other Services* 39 Diğer Sosyal Hizmetleri */39 Other Social Services*
Özel Sektörler */ Special Sectors*	C	C.01	33 Bilgi Teknolojileri */33 Information Technologies*
		C.02	36 Kamu Yönetimi */36 Public Administration*
		C.03	37 Eğitim */37 Education*
		C.04	32 Finansal Hizmetler */32 Financial Services*
		C.05	38 Sağlık */38 Health*
		C.06	21 Havacılık ve Uzay */21 Aerospace*
		C.07	31 Telekomünikasyon */31 Telecommunications*
		C.08	39 Yardım Dernekleri */39 Charities*

6.1.2. BG 7.1.2 Yeterlilik Kriterlerinin Belirlenmesi */ IS 7.1.2 Determination of Qualification Criteria*

6.1.2.1. BGYS Denetimi İçin Yeterlilik Şartları */ Qualification Requirements for ISMS Audit*

6.1.2.1.1. Genel Şartlar */ General conditions*

AVACERT, aşağıdakileri sağlamak için yetkin personel bulundurmaktadır veya ihtiyaç olunca ulaşabilmektedir:

/ AVACERT employs competent personnel or is available when needed to ensure the following:

a) Bilgi güvenliği bilgisi;

/ a) Information security information;

b) Denetlenecek faaliyetin teknik bilgisi;

/ b) Technical knowledge of the activity to be audited;

c) Yönetim sistemleri bilgisi

/ c) Knowledge of management systems

d) Denetim ilkeleri hakkında bilgi;

/ d) Information about auditing principles;

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

/ e) Information on monitoring, measuring, analyzing and evaluating.

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

/ The audit team has permission to monitor the customer's use of information security incidents.

Denetim ekibi, yukarıdaki maddelere ilişkin uygun iş tecrübesine ve bu maddelerin pratik uygulamasına sahip olacak şekilde (Bu bir denetçinin bilgi güvenliği alanlarının tamamına ilişkin deneyim tecrübesine ihtiyacı olduğu anlamına gelmez, ancak denetim ekibinin bir bütün olarak yeterli bilgi ve deneyime sahip olması gerekir) görevlendirilmektedir.

/ The audit team is assigned to have appropriate work experience regarding the above items and the practical application of these items (This does not mean that an auditor needs experience in all areas of information security, but the audit team as a whole must have sufficient knowledge and experience).

6.1.2.1.2. Bilgi Güvenliği Yönetim Terminolojisi, İlkeleri, Uygulamaları ve Teknikleri / Information Security Management Terminology, Principles, Practices and Techniques

AVACERT, denetim ekiplerinin eğitimi için aşağıdakileri temin eden yetkinlik kriterleri oluşturmuştur:

/ AVACERT has established competency criteria for the training of audit teams that ensure:

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

/ a) ISMS-specific documentation structures, hierarchy and relationships;

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

/ b) Tools, methods, techniques and applications related to information security management;

c) Bilgi güvenliği risk değerlendirmesi ve risk yönetimi;

/ c) Information security risk assessment and risk management;

d) BGYS için uygulanabilir işlemler;

/ d) Applicable procedures for ISMS;

e) Bilgi güvenliği ile ilgili olabilecek güncel teknoloji veya bir sorun

/ e) Current technology or a problem that may be related to information security

6.1.2.1.3. Bilgi Güvenliği Yönetim Sistemi Standartları ve Normatif Dokümanlar / Information Security Management System Standards and Normative Documents

BGYS denetimine katılan denetçiler;

/ Auditors participating in the ISMS audit;

a) ISO/IEC 27001'de yer alan tüm gereklilikleri

/ a) All requirements in ISO/IEC 27001

Denetim ekibinin tüm üyeleri aşağıdakiler hakkında bilgi sahibi olacaktır:

/ All members of the audit team will have knowledge of:

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

/ b) All controls included in ISO/IEC 27002 (if necessary and also determined according to sectoral standards) and their implementation are categorized as:

1) Bilgi güvenliği politikaları;

/1) Information security policies;

2) Bilgi güvenliğinin organizasyonu;

/2) Organization of information security;

3) İnsan kaynakları güvenliği;

/3) Human resources security;

4) Varlık yönetimi;

/4) Asset management;

5) Yetkilendirme de dahil olmak üzere erişim kontrolü;

/5) Access control, including authorization;

6) Kriptografi;

/6) Cryptography;

7) Fiziksel ve çevresel güvenlik;

/7) Physical and environmental security;

8) IT hizmetleri de dahil olmak üzere operasyon güvenliği;

/8) Operational security, including IT services;

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

/9) Communication security, including network security management and information transfer;

10) Sistem edinimi, geliştirilmesi ve bakımı;

/10) System acquisition, development and maintenance;

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

/11) Supplier relationships, including outsourced services;

12) Bilgi güvenliği olay yönetimi;

/12) Information security incident management;

13) İş sürekliliği yönetiminin, işten çıkarmalar da dahil olmak üzere bilgi güvenliği yönleri;

/13) Information security aspects of business continuity management, including layoffs;

14) Bilgi güvenliği incelemeleri de dahil uyumluluk

/14) Compliance, including information security reviews

6.1.2.1.4. İşletme Yönetimi Uygulamaları ***/ Business Management Applications***

BGYS denetiminde yer alan Denetçiler şu bilgilere sahip olacaktır:

/ Auditors involved in the ISMS audit will have the following information:

a) Sanayi bilgi güvenliği iyi uygulamaları ve bilgi güvenlik prosedürleri;

/ a) Industry information security good practices and information security procedures;

b) Bilgi güvenliği politikaları ve iş gereksinimleri;

/ b) Information security policies and business requirements;

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

/ c) General business management concepts, practices and the interrelationship between policy, objectives and results;

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

/ d) Management processes (including human resources management, internal and external communication and other relevant support processes) and related terminology.

6.1.2.1.5. Müşteri Sektörü Uygulamaları ***/ Customer Industry Applications***

BGYS denetiminde yer alan Denetçiler bilgisine sahip olacaktır:

/ Auditors involved in the ISMS audit will have knowledge of:

a) Belirli bilgi güvenliği alanında, coğrafyasında ve yargılama alanındaki yasal ve düzenleyici gereklilikler;

/ a) Legal and regulatory requirements in the particular information security field, geography and jurisdiction;

b) İşletme sektörüyle ilgili bilgi güvenliği riskleri;

/ b) Information security risks related to the business sector;

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

/ c) General terminology, processes and technologies for customer use;

d) İlgili işletme sektörü uygulamaları.

/ d) Relevant business sector applications.

Kriter a) denetim ekibi arasında paylaşılabilir.

/ Criterion can be shared among the a) audit team.

6.1.2.1.6. Müşteri Ürünleri, Prosesleri ve Organizasyonu ***/ Customer Products, Processes and Organization***

BGYS denetimine katılan Denetçiler aşağıdakilerin bilgisine sahip olacaklardır:

/ Auditors participating in the ISMS audit will have knowledge of the following:

a) Organizasyonun türü, boyutu, yönetişimi, yapısı, işlevleri ve ilişkilerinin dış kaynak kullanımını da içeren BGYS ve belgelendirme faaliyetlerinin geliştirilmesi ve uygulanması;

/ a) Development and implementation of ISMS and certification activities, including outsourcing of the type, size, governance, structure, functions and relationships of the organization;

b) Geniş bir perspektif içinde karmaşık operasyonlar;

/ b) Complex operations in a broad perspective;

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

/ c) Legal and regulatory requirements that apply to the product or service.

6.1.2.2. BGYS Denetim Ekibinin Yönetilmesi İçin Yetkinlik Şartları */ Competency Requirements for Managing the ISMS Audit Team*

Baş denetçiler, Bilgi Güvenliği El Kitabı madde 7.1.2.1'deki gerekliliklere ek olarak, rehberlik ve denetim altında denetimlerde gösterilecek olan aşağıdaki gereklilikleri yerine getirmelidir:

/ In addition to the requirements in clause 7.1.2.1 of the Information Security Handbook, lead auditors must meet the following requirements, which will be demonstrated in guided and supervised audits:

a) Belgelendirme denetim prosesini ve denetim ekibini idare edebilecek bilgi ve beceriler

/ a) Knowledge and skills to manage the certification audit process and audit team

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

/ b) Demonstration of the ability to communicate effectively verbally and in writing.

6.1.2.3. Başvurunun İncelenmesi İçin Yetkinlik Şartları */ Competency Requirements for Application Review*

6.1.2.3.1. Bilgi Güvenliği Yönetim Sistemi Standartları ve Normatif Dokümanlar */ Information Security Management System Standards and Normative Documents*

Denetim ekibi yetkinliğini belirlemek, denetim ekibi üyelerini seçmek ve denetim zamanını belirlemek için uygulama gözden geçirme görevlisi aşağıdakilerin bilgisine sahip olması sağlanmaktadır:

/ To determine audit team competency, select audit team members, and schedule the audit, the practice reviewer must have knowledge of:

a) İlgili BSYS standartları ve sertifikasyon prosesinde kullanılan diğer normatif dokümanlar.

/ a) Relevant ISMS standards and other normative documents used in the certification process.

6.1.2.3.2. Müşteri İş Sektörü */ Customer Business Sector*

Denetim ekibinin yetkinliğini belirlemek, denetim ekibi üyelerini seçmek ve denetim zamanını belirlemek için uygulama gözden geçirme görevlisi aşağıdakilerin bilgisine sahip olması sağlanmaktadır:

/ To determine the competency of the audit team, select audit team members, and schedule the audit, the application review officer must have knowledge of:

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

/ a) General terminology, processes, technologies and risks for customer use.

6.1.2.3.3. Müşteri Ürünleri, Prosesleri ve Organizasyonu */ Customer Products, Processes and Organization*

Denetim ekibi yeterliliğini belirlemek, denetim ekibi üyelerini seçmek ve denetim zamanını belirlemek için uygulama gözden geçirme görevlisi aşağıdakilerin bilgisine sahip olması sağlanmaktadır:

/ To determine audit team competency, select audit team members, and schedule the audit, the application review officer must have knowledge of:

a) BGYS ve belgelendirme faaliyetlerinin geliştirilmesi ve uygulanmasına ilişkin müşteri ürünleri, prosesler, organizasyon türleri, boyut, yönetişim, yapı, fonksiyonlar ve ilişkiler, dış kaynak fonksiyonları dahil.

/ a) Including customer products, processes, organization types, size, governance, structure, functions and relationships, outsourcing functions regarding the development and implementation of ISMS and certification activities.

6.1.2.4. Denetim Raporlarının Gözden Geçirilmesi ve Belgelendirme Kararlarının Verilmesi İçin Yetkinlik Şartları */ Competency Requirements for Reviewing Audit Reports and Making Certification Decisions*

6.1.2.4.1. Genel */ General*

Denetim raporlarını gözden geçiren ve belgelendirme kararları veren personel, belgelendirme kapsamının uygunluğunu ve bunların kapsamındaki değişiklikleri ve denetim etkinliği üzerindeki etkilerini, özellikle ara yüzlerin ve bağımlılıkların tanımlanmasının devam eden geçerliliğini doğrulamasını sağlayacak bilgi sahibi olmalıdır.

/ Personnel reviewing audit reports and making certification decisions should have knowledge that will enable them to verify the appropriateness of the scope of certification and changes in its scope and their impact on audit activity, particularly the continued validity of the identification of interfaces and dependencies.

Buna ek olarak, denetim raporlarını gözden geçiren ve belgelendirme kararlarını veren personel aşağıdaki hususları bilmelidir:

/ In addition, personnel who review audit reports and make certification decisions must know the following:

a) Genel olarak yönetim sistemleri;

/ a) Management systems in general;

b) Denetim prosesleri ve usulleri;

/ b) Audit processes and procedures;

c) Denetim ilke, uygulama ve teknikleri.

/ c) Audit principles, practices and techniques.

6.1.2.4.2. Bilgi Güvenliği Yönetim Terminolojisi, İlkeleri, Uygulamaları ve Teknikleri ***/ Information Security Management Terminology, Principles, Practices and Techniques***

Denetim raporlarını gözden geçiren ve belgelendirme kararlarını veren personelin, aşağıdaki bilgilere sahip olması sağlanmaktadır:

/ It is ensured that the personnel who review the audit reports and make certification decisions have the following information:

a) Bilgi Güvenliği El Kitabı madde 7.1.2.1.2 a), c) ve d) 'de listelenen maddeler;

/ a) Substances listed in Information Security Handbook article 7.1.2.1.2 a), c) and d);

b) Bilgi güvenliği ile ilgili yasal ve düzenleyici gereklilikler.

/ b) Legal and regulatory requirements regarding information security.

6.1.2.4.3. Bilgi Güvenliği Yönetim Sistemi Standartları ve Normatif Dokümanlar ***/ Information Security Management System Standards and Normative Documents***

Denetim raporlarını gözden geçiren ve belgelendirme kararları veren personelin, aşağıdaki bilgilere sahip olması sağlanmaktadır:

/ It is ensured that personnel who review audit reports and make certification decisions have the following information:

a) İlgili BGYS standartları ve sertifikasyon prosesinde kullanılan diğer normatif dokümanlar.

/ a) Relevant ISMS standards and other normative documents used in the certification process.

6.1.2.4.4. Müşteri İş Sektörü ***/ Customer Business Sector***

Denetim raporlarını gözden geçiren ve belgelendirme kararları veren personelin, aşağıdaki bilgilere sahip olması sağlanmaktadır:

/ It is ensured that personnel who review audit reports and make certification decisions have the following information:

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

/ a) Risks related to general terminology and relevant business sector practices.

6.1.2.4.5. Müşteri Ürünleri, Prosesleri ve Organizasyonu ***/ Customer Products, Processes and Organization***

Denetim raporlarını gözden geçiren ve belgelendirme kararları veren personelin, aşağıdaki bilgilere sahip olması sağlanmaktadır:

/ It is ensured that personnel who review audit reports and make certification decisions have the following information:

a) Müşteri ürünleri, prosesler, organizasyon türleri, boyut, yönetişim, yapı, işlevler ve ilişkiler.

/ a) Customer products, processes, organizational types, size, governance, structure, functions and relationships.

6.2. Belgelendirme Faaliyetlerinde Görev Alan Personel */ Personnel Involved in Certification Activities*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı ve Bilgi Güvenliği El Kitabı madde 7.2 ile PR-11 Personel Atama ve Performans Değerlendirme Prosedüründeki hükümler geçerlidir. Ayrıca aşağıdaki BGYS'ye özel şartlar ve kılavuz uygulanır.

/ The provisions of the ISO/IEC 17021-1:2015 standard and ISO/IEC 17021-1 System Certification Handbook and Information Security Handbook article 7.2 and PR-11 Personnel Appointment and Performance Evaluation Procedure are valid. In addition, the following ISMS-specific conditions and guidance apply.

6.2.1. BG 7.2 Denetçinin Bilgi ve Tecrübesinin Gösterilmesi */ IS 7.2 Demonstration of Auditor's Knowledge and Experience*

AVACERT, Denetçilerin, aşağıdaki bilgi ve tecrübeye sahip olduklarını göstermektedir:

/ AVACERT shows that Auditors have the following knowledge and experience:

a) BGYS'ye özgü nitelikleri

/ a) ISMS-specific features

b) Mümkün ise denetçi olarak kayıt;

/ b) Registration as an auditor, if possible;

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

/ c) Participation in ISMS training courses and obtaining relevant personal identification information;

d) Güncel mesleki gelişim kayıtları;

/ d) Current professional development records;

e) Başka bir BGYS denetçisinin tanık olduğu BGYS denetimleri

/ e) ISMS audits witnessed by another ISMS auditor

6.2.1.1. Denetçi Seçimi */ Auditor Selection*

Bilgi Güvenliği El Kitabı madde 7.1.2.1'e ek olarak, Denetçileri seçme kriterleri her Denetçinin aşağıdakileri sağlayacağını garanti etmesi sağlanmaktadır:

/ In addition to Article 7.1.2.1 of the Information Security Handbook, the criteria for selecting Auditors are provided to ensure that each Auditor:

a) Eşdeğer bir üniversite eğitimine yönelik profesyonel eğitim veya öğretim;

/ a) Professional education or training leading to an equivalent university education;

b) Bilgi teknolojisinde tam zamanlı en az dört yıl iş deneyimi; bunlardan en az iki yıl bilgi güvenliği ile ilgili bir rol veya işlevde olmalı;

/ b) At least four years of full-time work experience in information technology; Of these, at least two years must have been in an information security-related role or function;

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

/ c) Successfully completing at least five days of training covering ISMS audits and audit management;

d) BGYS denetimlerini gerçekleştiren bir denetçi olarak hareket etmeden önce BGYS' yi denetim deneyimi kazanmıştır. Bu deneyim, en az bir BGYS ilk belgelendirme denetiminde (Aşama 1 ve Aşama 2) veya yeniden belgelendirme ve en az bir gözetim denetiminde bir BGYS değerlendiricisi (bkz. ISO / IEC 17021-1: 2015, 9.2.2.1.4) tarafından izlenen eğitimde denetçi olarak gerçekleştirilerek kazanılmalıdır. Bu deneyim en az 10 BGYS yerinde denetim gününde kazanılmalı ve son 5 yıl içinde gerçekleştirilmelidir. Katılım, dokümantasyon ve risk değerlendirmesinin gözden geçirilmesi, uygulama değerlendirmesi ve denetim raporlamasını içermelidir.

/ d) Gained ISMS audit experience before acting as an auditor performing ISMS audits. This experience must be demonstrated in training followed by an ISMS assessor (see ISO/IEC 17021-1:2015, 9.2.2.1.4) in at least one ISMS initial certification audit (Phase 1 and Phase 2) or re-certification and at least one surveillance audit It must be earned by performing as an auditor. This experience must be gained in at least 10 ISMS on-site audit days and must be carried out within the last 5 years. Participation should include review of documentation and risk assessment, implementation evaluation and audit reporting.

e) İlgili ve güncel deneyime sahip;

/ e) Have relevant and current experience;

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

/ f) Keeps current knowledge and skills up to date through continuous professional development.

g) ISO/IEC 27001 uyarınca bir BGYS'yi denetleme yeterliliğine sahiptir.

/ g) Has the competence to audit an ISMS in accordance with ISO/IEC 27001.

Teknik Uzmanların a), b) ve e) kriterlerine uyması yeterlidir.

/ It is sufficient for Technical Experts to comply with criteria a), b) and e).

6.2.1.2. Baş denetçi Seçimi / Selection of chief auditor

Bilgi Güvenliği El Kitabı madde 7.1.2.2 ve 7.2.1.1'e ek olarak, Baş denetçinin aşağıdakileri sağlayacağını garanti etmesi sağlanmaktadır:

/ In addition to Articles 7.1.2.2 and 7.2.1.1 of the Information Security Manual, the Chief auditor shall ensure that:

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

/ a) Actively participating in all stages of at least 3 ISMS audits. Engagement should include initial scoping and planning, review of documentation and risk assessment, implementation evaluation, and formal audit reporting.

6.3. Kuruluş Dışı Denetçilerin ve Teknik Uzmanların Kullanımı / Use of External Auditors and Technical Experts

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı ve Bilgi Güvenliği El Kitabı madde 7.3 ve PR-11 Personel Atama ve Performans Değerlendirme Prosedüründeki hükümler geçerlidir.

/ The provisions of the ISO/IEC 17021-1:2015 standard and ISO/IEC 17021-1 System Certification Handbook and Information Security Handbook article 7.3 and PR-11 Personnel Appointment and Performance Evaluation Procedure are valid.

6.3.1. BG 7.3 Denetim Ekibinin Bir Parçası Olarak Dış Denetçilerin ve Dış Teknik Uzmanların Kullanımı */ IS 7.3 Use of External Auditors and External Technical Experts as Part of the Audit Team*

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

/ AVACERT uses external Auditors and external Technical Experts as part of the audit team;

- Bu kişilerin yeterli olduklarından ve ISO/IEC 27006:2015 standardının uygulanabilir hükümleri ile uyumlu olduklarından,

/ - They are competent and comply with the applicable provisions of the ISO/IEC 27006:2015 standard,

- Tarafsızlığı ihlal edecek şekilde doğrudan veya işvereni üzerinden, bir BGYS veya ilgili yönetim sistemlerinin tasarımı, uygulaması veya sürdürülmesinde yer almış olmadıklarından,

/ - They have not been involved, directly or through their employer, in the design, implementation or maintenance of an ISMS or related management systems in a way that would violate impartiality,

yaptığı sözleşmeler ve aldığı güncel bildirimler ile emin olmaktadır.

/ It is assured with the contracts it makes and the up-to-date notifications it receives.

6.4. Personel Kayıtları */ Personnel Records*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı madde 7.4 ve PR-11 Personel Atama ve Performans Değerlendirme Prosedüründeki hükümler geçerlidir.

/ The provisions of the ISO/IEC 17021-1:2015 standard and ISO/IEC 17021-1 System Certification Handbook article 7.4 and PR-11 Personnel Appointment and Performance Evaluation Procedure are valid.

6.5. Dışarıdan Temin / *Outsourcing*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı madde 7.5'de yer alan hükümler geçerlidir.

/ The provisions of the ISO/IEC 17021-1:2015 standard and article 7.5 of the ISO/IEC 17021-1 System Certification Handbook are valid.

7. BİLGİ ŞARTLARI / *INFORMATION TERMS*

7.1. Kamuya Açık Bilgiler / *Public Information*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı madde 8.1'de yer alan hükümler geçerlidir. Ayrıca aşağıdaki BGYS'ye özel şartlar ve kılavuz uygulanır.

/ The provisions of the ISO/IEC 17021-1:2015 standard and article 8.1 of the ISO/IEC 17021-1 System Certification Handbook are valid. In addition, the following ISMS-specific conditions and guidance apply.

7.2. Belgelendirme Dokümanları / *Certification Documents*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı ve Bilgi Güvenliği El Kitabı madde 8.2 maddesinde yer alan hükümler geçerlidir. Bunlara ek olarak aşağıdaki BGYS'ye özel şartlar ve kılavuz uygulanır.

/ The provisions of the ISO/IEC 17021-1:2015 standard and ISO/IEC 17021-1 System Certification Handbook and Information Security Handbook article 8.2 are valid. In addition, the following ISMS-specific conditions and guidance apply.

7.2.1. BG 8.2 BGYS Belgelendirme Dokümanları / IS 8.2 ISMS Certification Documents

AVACERT, BGYS'si belgelendirilen müşteri kuruluşlarının her birine, AVACERT Genel Müdürü tarafından imzalanan bir sertifika sunmaktadır.

/ AVACERT offers a certificate signed by the AVACERT General Manager to each of the customer organizations whose ISMS is certified.

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

/ A change to the Declaration of Applicability that does not change the scope of controls within the scope of the Certificate does not require updating the Certificate.

Belgelendirme dokümanları, kuruluşun ISO / IEC 27001: 2022, 6.1.3 d) uyarınca Uygulanabilirlik Bildirgesinde gerekli olduğu belirlenen kontroller için kontrol seti kaynağı / kaynakları olarak ulusal ve uluslararası standartlara atıfta bulunabilir. Belgelendirme dokümanlarındaki atıfların, Uygulanabilirlik Bildirgesinde uygulanan kontroller için sadece bir kontrol seti kaynağı olduğu ve dolayısıyla atıfların belgelendirmesinin olmadığı açıkça belirtilmelidir.

/ Certification documents may refer to national and international standards as control set source(s) for controls identified as necessary in the organization's Declaration of Applicability in accordance with ISO/IEC 27001:2022, 6.1.3 d). It should be made clear that references in certification documents are merely a source of control sets for the controls applied in the Declaration of Applicability and therefore there is no documentation of references.

7.3. Belgelendirmeye Atıf ve Markaların Kullanımı / *Reference to Certification and Use of Trademarks*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı madde 8.3 ve TL-02 Logo ve Belge Kullanım Talimatındaki hükümler geçerlidir. Ek olarak aşağıdaki BGYS'ye özel şartlar ve kılavuz uygulanır.

/ The provisions of ISO/IEC 17021-1:2015 standard and ISO/IEC 17021-1 System Certification Handbook article 8.3 and TL-02 Logo and Document Usage Instruction are valid. In addition, the following ISMS-specific conditions and guidance apply.

7.4. Gizlilik / *Security*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı madde 8.4'de yer alan hükümler geçerlidir. Ek olarak aşağıdaki BGYS'ye özel şartlar ve kılavuz uygulanır.

/ The provisions of the ISO/IEC 17021-1:2015 standard and article 8.4 of the ISO/IEC 17021-1 System Certification Handbook are valid. In addition, the following ISMS-specific conditions and guidance apply.

7.4.1. BG 8.5 Kurumsal Kayıtlara Erişim */ IS 8.5 Access to Corporate Records*

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

/ Before the certification audit, AVACERT requests the client organization to inform whether there are any records of the ISMS that cannot be presented to the audit team for review because they contain confidential or sensitive information.

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

/ AVACERT decides whether the ISMS can be audited appropriately if these records are missing. If AVACERT decides that it is not possible to conduct an appropriate audit of the ISMS without reviewing the detected confidential or sensitive records, it will notify the customer organization that the certification audit cannot be carried out until appropriate access arrangements are provided.

7.5. AVACERT ile Müşterileri Arasındaki Bilgi Alışverişi */ Information Exchange Between AVACERT and Its Customers*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı ve Bilgi Güvenliği El Kitabı madde 8.5'da yer alan hükümler geçerlidir.

/ The provisions of the ISO/IEC 17021-1:2015 standard and ISO/IEC 17021-1 System Certification Handbook and Information Security Handbook article 8.5 are valid.

8. PROSES ŞARTLARI */ PROCESS CONDITIONS*

8.1. Belgelendirme Öncesi Faaliyetler */ Pre-certification Activities*

8.1.1. Başvuru */ Application*

BGYS belgelendirmesi için başvuran müşteri kuruluşlardan başvurularını, FRB-01 Başvuru Formu ve FRB-01 Ek-2 ISO 27001 Başvuru ek Bilgilendirme Formu ile iletmeleri istenir.

/ Customer organizations applying for ISMS certification are asked to submit their applications with the FRB-01 Application Form and FRB-01 Annex-2 ISO 27001 Application additional Information Form.

Planlama Sorumlusu tarafından, BGYS belgelendirme başvurusunda bulunan müşteri kuruluşlara, sözleşmeyi gözden geçirip değerlendirmeden önce;

/ Before reviewing and evaluating the contract, the Planning Officer will inform the customer organizations that have applied for ISMS certification;

1. Değerlendirilen ihtiyaçlara karşın yetkinlikleri değerlendirmek,
/ 1. Evaluating competencies against assessed needs,
2. Faaliyet gösterdiği alanda yeterlilik analizinin uygunluğu ve
/ 2. The suitability of competency analysis in the field of activity and
3. Belirttiği hariç tutmaların doğrulamasının yapılması amacıyla bilgi edinmek üzere,
/ 3. To obtain information for the purpose of verifying the exclusions specified,

FRB-02 Başvuru Gözden Geçirme Formu gönderilir ve ilgili alanlarının doldurarak AVACERT'ye geri gönderilmesi istenir.

/ The FRB-02 Application Review Form is sent and the relevant fields are requested to be filled in and sent back to AVACERT.

8.1.2. Başvurunun Gözden Geçirilmesi */ Review of Application*

Belgelendirme için başvuran müşteri kuruluşlar için, sözleşmenin gözden geçirilmesinden önce, Bilgi Güvenliği El Kitabı madde 9.1.2 'de yer alan tablolar da dikkate alınarak, bir yeterlilik analizi yapılır ve FRB-02 Başvuru Gözden Geçirme Formu, bu analizin yapıldığına dair gözden geçirmeyi yapan yetkili personel tarafından imzalanır.

/ For customer organizations applying for certification, before reviewing the contract, a proficiency analysis is carried out, taking into account the tables in Article 9.1.2 of the Information Security Handbook, and the FRB-02 Application Review Form is submitted by the reviewing officer to confirm that this analysis has been carried out. signed by the staff.

Sözleşmenin gözden geçirilmesinin tamamlanmasından sonra, PR-08 BGYS Belgelendirme Prosedürü doğrultusunda verilecek teklif hazırlanır ve müşteri kuruluşa gönderilir.

/ After the review of the contract is completed, the offer to be submitted in line with the PR-08 ISMS Certification Procedure is prepared and sent to the customer organization.

Teklifi kabul eden müşteri kuruluş ile PR-08 BGYS Belgelendirme Prosedürü doğrultusunda sözleşme imzalanır.

/ A contract is signed with the customer organization that accepts the offer in line with the PR-08 ISMS Certification Procedure.

8.1.3. Denetim Programı */ Audit Program*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı ve Bilgi Güvenliği El Kitabı madde 9.1.3'deki hükümler geçerlidir. Ek olarak aşağıdaki BGYS'ye özel şartlar ve kılavuz uygulanır.

/ The provisions of the ISO/IEC 17021-1:2015 standard and ISO/IEC 17021-1 System Certification Handbook and Information Security Handbook article 9.1.3 are valid. In addition, the following ISMS-specific conditions and guidance apply.

8.1.3.1. BG 9.1.3 Genel */ IS 9.1.3 General*

BGYS denetimleri için FRB-27 EK-E Denetim Programı, belirlenen bilgi güvenlik kontrollerini dikkate alacak şekilde oluşturulmaktadır.

/ FRB-27 ANNEX-E Audit Program for ISMS audits is created to take into account the determined information security controls.

8.1.3.2. BG 9.1.3 Denetim Metodolojisi */ IS 9.1.3 Audit Methodology*

AVACERT, müşteri kuruluşun, BGYS iç denetimlerinin planlandığını, program ve prosedürlerin uygulanmakta olduğunu ve uygulanabildiğini gösterebilen bir denetim uygulaması için, PR-09 BGYS Denetim Prosedürü oluşturmuş ve uygulamaktadır.

/ AVACERT has created and implemented PR-09 ISMS Audit Procedure for an audit practice that can show that the customer organization's ISMS internal audits are planned, programs and procedures are implemented and can be implemented.

8.1.3.3. BG 9.1.3 İlk Denetim İçin Genel Hazırlıklar */ IS 9.1.3 General Preparations for the First Audit*

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

/ AVACERT requires a client organization to make all necessary arrangements to access internal audit reports and independent review reports regarding information security.

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

/ At least during Phase 1 of the initial certification audit, the customer organization is requested to provide the following information:

a) BGYS ve kapsadığı faaliyetlerle ilgili genel bilgi;

/ a) General information about ISMS and the activities it covers;

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

/ b) A copy of the required ISMS documentation specified in ISO/IEC 27001 and relevant documents where necessary.

8.1.3.4. BG 9.1.3 Gözden Geçirme Sıklığı */ IS 9.1.3 Review Frequency*

AVACERT, en az bir yönetim gözden geçirmesi ve belgelendirme kapsamını kapsayan bir iç denetimi yapılmadığı sürece, BGYS belgelendirmesi yapmamaktadır.

/ AVACERT does not provide ISMS certification unless an internal audit covering the scope of at least one management review and certification is carried out.

8.1.3.5. BG 9.1.3 Belgelendirme Kapsamı */ IS 9.1.3 Scope of Certification*

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

/ The audit team audits the customer organization's ISMS within the defined scope to verify that all requirements are met. AVACERT confirms that, within the scope of the customer organization's ISMS, customers fulfill the conditions specified in ISO/IEC 27001 article 4.3.

AVACERT, müşteri kuruluşun belgelendirme kapsamında tanımlanan faaliyetlerinin sınırlarını içinde, bilgi güvenliği risk değerlendirmesi işlemlerini doğru bir şekilde gerçekleştirdiğini teyit eder. AVACERT bunun, müşteri kuruluşun BGYS ve Uygulanabilirlik Beyanı kapsamına yansıtıldığını teyit eder. AVACERT, belgelendirme kapsamı başına en az bir Uygulanabilirlik Beyanı bulunduğunu doğrular.

/ AVACERT confirms that the customer organization has carried out information security risk assessment processes correctly, within the limits of its activities defined within the scope of certification. AVACERT confirms that this is reflected in the client organization's ISMS and Declaration of Applicability. AVACERT verifies that there is at least one Declaration of Applicability per scope of certification.

AVACERT, BGYS kapsamına girmeyen hizmetler veya faaliyetlerle olan ara yüzlerin, belgelendirmeye tabi BGYS kapsamında ele alınmasını ve müşteri kuruluşun bilgi güvenliği risk değerlendirmesinde yer almasını sağlar. Böyle bir durumun bir örneği, diğer kuruluşlarla paylaşımdaki aksaklıkları (örneğin IT sistemleri, veri tabanları ve telekomünikasyon sistemleri veya bir işletme işlevinin dış kaynak kullanımı) içermesidir.

/ AVACERT ensures that interfaces with services or activities that are not within the scope of ISMS are handled within the scope of ISMS subject to certification and are included in the information security risk assessment of the customer organization. An example of such a situation involves disruptions in sharing with other organizations (for example, IT systems, databases and telecommunications systems, or outsourcing a business function).

8.1.3.6. BG 9.1.3 Belgelendirme Denetimi Kriterleri */ ISBG 9.1.3 Certification Audit Criteria*

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

/ For the criteria for auditing a customer organization's ISMS, ISMS standard ISO/IEC 27001 is taken as reference.

8.1.4. Denetim Zamanının Belirlenmesi */ Determining Audit Time*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı ve Bilgi Güvenliği El Kitabı madde 9.1.4'de yer alan hükümler geçerlidir. Ek olarak aşağıdaki BGYS'ye özel şartlar ve kılavuz uygulanır.

/ The provisions of the ISO/IEC 17021-1:2015 standard and ISO/IEC 17021-1 System Certification Handbook and Information Security Handbook article 9.1.4 are valid. In addition, the following ISMS-specific conditions and guidance apply.

8.1.4.1. BG 9.1.4 Denetim Zamanı */ IS 9.1.4 Audit Time*

AVACERT, denetim ekibine, ilk belgelendirme denetimi, gözetim denetimi ya da yeniden belgelendirme denetiminde bütün faaliyetleri tamamlamaları için yeterli süreyi verecek şekilde planlama yapmaktadır.

/ AVACERT plans to give the audit team sufficient time to complete all activities in the initial certification audit, surveillance audit or re-certification audit.

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

/ The calculation of overall audit time includes sufficient time for audit reporting.

AVACERT, denetim zamanını belirlemek için ISO/IEC 27006:2015 ve Ek B ve EK C'yi ve ISO/IEC 27006:2015 AMD.1 2020 kullanmaktadır.

/ AVACERT uses ISO/IEC 27006:2015 and Annex B and Annex C and ISO/IEC 27006:2015 AMD.1 2020 to determine the audit timing.

Belgelendirme kapsamındaki tüm vardiyalar için kuruluşun kontrolü altında çalışan toplam kişi sayısı dikkate alınarak denetim süresinin belirlenir.

/ The audit period is determined by taking into account the total number of people working under the control of the organization for all shifts within the scope of certification.

Planlama ve rapor yazma için hesaplanan sürenin, genellikle toplam yerinde 'denetim süresini' Ek B' ye göre hesaplanan sürenin%70'inden daha aza indirilemez. Planlama ve /veya rapor yazımı için ek süre gerekli olduğunda, bu, yerinde denetim süresini azaltmak için bir gerekçe olamaz. Denetçi seyahat süresi bu hesaplamaya dahil edilmez ve çizelgede belirtilen denetim süresine ilave edilir.

/ The time calculated for planning and report writing cannot generally be reduced to less than 70% of the total on-site 'audit time' calculated in accordance with Annex B. Where additional time is required for planning and/or report writing, this is not a justification for reducing on-site audit time. Auditor travel time is not included in this calculation and is added to the audit time specified in the schedule.

Ek B' de ki şartlara Ek olarak kapsam için hesaplanan toplam yerinde denetçi günlerinin sayısı, sahanın yönetim sistemi için uygunluğuna ve belirlenen risklere bağlı olarak farklı sahalar arasında dağıtılır. Dağıtımın gerekçesi, AVACERT Planlama bölümü tarafından kayıt altına alınır.

/ In addition to the requirements in Annex B, the total number of on-site auditor days calculated for the scope is distributed among the different sites depending on the suitability of the site for the management system and the identified risks. The justification for the distribution is recorded by the AVACERT Planning department.

İlk belgelendirme denetimi ve gözetim için harcanan toplam süre, her bir sahada harcanan süre artı merkez ofiste harcanan toplam sürenin toplamıdır. Tüm işin tek bir sahada kuruluşu tüm çalışanları ile yapılması halinde, hiçbir zaman operasyonun boyutu ve karmaşıklığı için hesaplanacak olan süreden daha az olmamaktadır.

/ Total time spent on initial certification audit and surveillance is the sum of time spent at each site plus total time spent at head office. If the entire work is done on a single site with all employees, the time is never less than that which would be calculated for the size and complexity of the operation.

Denetim zamanı, aşağıda verilen tablo 1 doğrultusunda belirlenir:
/ The audit time is determined in accordance with table 1 below:

Çalışan Sayısı / Number of Employees	İlk belgelendirme için BGYS adam/gün / ISMS man/day for initial certification			Arttırıcı ya da azaltıcı faktörler / Increasing or decreasing factors
	Toplam /Total	Aşama 1 / Stage 1	Aşama 2 / Stage 2	
1-10	5	1.5	3.5	ISO/IEC 27006:2015 Annex B.3.4'e bakın / See ISO/IEC 27006:2015 Annex B.3.4
11-15	6	2	4	ISO/IEC 27006:2015 Annex B.3.4'e bakın / See ISO/IEC 27006:2015 Annex B.3.4
16-25	7	2,5	4,5	ISO/IEC 27006:2015 Annex B.3.4'e bakın / See ISO/IEC 27006:2015 Annex B.3.4
26-45	8.5	3	5.5	ISO/IEC 27006:2015 Annex B.3.4'e bakın / See ISO/IEC 27006:2015 Annex B.3.4
46-65	10	3,5	6,5	ISO/IEC 27006:2015 Annex B.3.4'e bakın
66-85	11	3,5	7,5	ISO/IEC 27006:2015 Annex B.3.4'e bakın / See ISO/IEC 27006:2015 Annex B.3.4
86-125	12	4	8	ISO/IEC 27006:2015 Annex B.3.4'e bakın / See ISO/IEC 27006:2015 Annex B.3.4
126-175	13	4,5	8,5	ISO/IEC 27006:2015 Annex B.3.4'e bakın / See ISO/IEC 27006:2015 Annex B.3.4
176-275	14	4,5	9	ISO/IEC 27006:2015 Annex B.3.4'e bakın / See ISO/IEC 27006:2015 Annex B.3.4

Çalışan Sayısı / Number of Employees	İlk belgelendirme için BGYS adam/gün / ISMS man/day for initial certification			Arttırıcı ya da azaltıcı faktörler / Increasing or decreasing factors
	Toplam /Total	Aşama 1 / Stage 1	Aşama 2 / Stage 2	
276-425	15	5	10	ISO/IEC 27006:2015 Annex B.3.4'e bakın / See ISO/IEC 27006:2015 Annex B.3.4
426-625	16,5	5.5	11	ISO/IEC 27006:2015 Annex B.3.4'e bakın / See ISO/IEC 27006:2015 Annex B.3.4
626-875	17,5	6	11.5	ISO/IEC 27006:2015 Annex B.3.4'e bakın / See ISO/IEC 27006:2015 Annex B.3.4
876-1175	18,5	6	12.5	ISO/IEC 27006:2015 Annex B.3.4'e bakın / See ISO/IEC 27006:2015 Annex B.3.4
1176-1550	19,5	6.5	13	ISO/IEC 27006:2015 Annex B.3.4'e bakın / See ISO/IEC 27006:2015 Annex B.3.4
1551-2025	21	7	14	ISO/IEC 27006:2015 Annex B.3.4'e bakın / See ISO/IEC 27006:2015 Annex B.3.4
2026-2675	22	7,5	14,5	ISO/IEC 27006:2015 Annex B.3.4'e bakın / See ISO/IEC 27006:2015 Annex B.3.4
2676-3450	23	7.5	15.5	ISO/IEC 27006:2015 Annex B.3.4'e bakın / See ISO/IEC 27006:2015 Annex B.3.4
3451-4350	24	8	16	ISO/IEC 27006:2015 Annex B.3.4'e bakın / See ISO/IEC 27006:2015 Annex B.3.4
4351-5450	25	8.5	16.5	ISO/IEC 27006:2015 Annex B.3.4'e bakın / See ISO/IEC 27006:2015 Annex B.3.4
5451-6800	26	8.5	17.5	ISO/IEC 27006:2015 Annex B.3.4'e bakın / See ISO/IEC 27006:2015 Annex B.3.4
6801-8500	27	9	18	ISO/IEC 27006:2015 Annex B.3.4'e bakın / See ISO/IEC 27006:2015 Annex B.3.4
8501-10700	28	9.5	18.5	ISO/IEC 27006:2015 Annex B.3.4'e bakın / See ISO/IEC 27006:2015 Annex B.3.4
>10.700	Yukarıdaki ilerlemeyi izleyin / Watch the progress above	Yukarıdaki ilerlemeyi izleyin / Watch the progress above	Yukarıdaki ilerlemeyi izleyin / Watch the progress above	

AVACERT, ilk belgelendirme denetiminde, gözetim ve yeniden belgelendirme denetimlerinde kullanılan zamanı gerekçelendirmekte ya da bu zamanı sağlamak üzere gerektiği şekilde hazırlık yapmaktadır.

/ AVACERT justifies the time used in the initial certification audit, surveillance and recertification audits, or prepares as necessary to ensure this time.

Geçiş denetimlerinde gözetimler için 1 adam gün , yeniden belgelendirme denetimlerinde 0,5 adam gün eklenir.

/ In transition audits, 1 man day is added for audits, and in recertification audits, 0.5 man days are added.

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

/ The following factors (ISO/IEC 27006:2015 Annex B.3.4) are taken into account for the time allocated:

a) BGYS kapsamının büyüklüğü (Ör: kullanılan bilgi sistemlerinin sayısı, çalışan sayısı),
/ a) Size of ISMS scope (e.g. number of information systems used, number of employees),

b) BGYS' nin karmaşıklığı (Ör: bilgi sistemlerinin kritikliği, BGYS' nin risk durumu), ayrıca ISO/IEC 27006:2015 Ek A'ya göre aşağıdaki tablo dikkate alınır:
/ b) The complexity of the ISMS (e.g. criticality of information systems, risk status of the ISMS), as well as the following table according to ISO/IEC 27006:2015 Annex A, are taken into account:

c) BGYS kapsamında gerçekleştirilen iş tipleri,
/ c) Types of work carried out within the scope of ISMS,

d) BGYS' nin çeşitli bileşenlerinin uygulanmasında kullanılan teknolojinin kapsamı ve çeşitliliği (uygulanan kontroller, dokümantasyon ve/veya proses kontrol, düzeltici/önleyici faaliyet, vb. gibi),
/ d) The scope and diversity of technology used in the implementation of various components of the ISMS (such as applied controls, documentation and/or process control, corrective/preventive action, etc.),

e) Saha sayısı,
/ e) Number of fields,

f) BGYS' nin daha önce gösterdiği performans,
/ e) Number of fields,

g) BGYS kapsamı dâhilinde kullanılan dış kaynak kullanımı ve üçüncü taraf düzenlemelerinin kapsamı,
/ g) Scope of outsourcing and third party arrangements used within the scope of ISMS,

h) Belgelendirmeye dair standartlar ve düzenlemeler.
/ h) Standards and regulations regarding certification.

Karmaşıklık Faktörleri / Complexity Factors	Risk Sınıfı / Risk Class			Önem / Importance
1-BGYS Karmaşıklık Faktörleri /1-ISMS Complexity Factors	Yüksek /High	Orta /Medium	Düşük /Low	
1.1 Çalışan Sayısı +Sözleşmeli Personel /1.1 Number of Employees +Contracted Personnel	≥ 250 (3 Puan) /≥ 250 (3 Points)	≥ 50 (2 Puan) /≥ 50 (2 Points)	< 50 (1 Puan) /< 50 (1 Point)	*BGYS uygulamasının ölçeği /*Scale of ISMS application *Bilgi sisteminin yönetimi /*Information system management *Üretim/Hizmet yönetimi ile ilgili sistemler /*Production/Service management related systems *Satış/dağıtım/genel servisle ilgili sistemler /*Sales/distribution/general service related systems *Bilgi teknolojisi/bilgi hizmetleriyle ilgili hizmetler /*Information technology/information services related services *İnşaat/gemi yapımı/fabrika /*Construction/shipbuilding/factory
1.2 Yasal uygunluğa verilen önem /1.2 Importance given to legal compliance	Kurala uymama durumunda muhtemel cezai yaptırıma sebep olması (3 Puan)	Kurala uymama durumunda önemli finansal yaptırıma sebep olması (2 Puan)	Kurala uymama durumunda önemsiz finansal yaptırıma sebep olması (1 Puan)	İlgili mevzuat, kılavuzlar ve ilkeler ISO/IEC 27001 A. 5.19 / Relevant legislation, guidelines and principles

Karmaşıklık Faktörleri / Complexity Factors	Risk Sınıfı / Risk Class			Önem / Importance
1-BGYS Karmaşıklık Faktörleri /1-ISMS Complexity Factors	Yüksek /High	Orta /Medium	Düşük /Low	
	/ Possible criminal sanctions in case of non-compliance with the rule (3 points)	/ Failure to comply with the rule causes significant financial sanctions (2 Points)	/ Causing insignificant financial sanctions in case of non-compliance with the rule (1 Point)	ISO/IEC 27001 A. 5.19
1.3 Sektöre özel risklerin uygulanabilirliği /1.3 Applicability of sector-specific risks	Öze yasa ve yükümlülüklerin uygulanması durumu (3 Puan) / Status of implementation of specific laws and obligations (3 Points)	Sektöre özel yasa ve düzenleme uygulanamaz ancak önemli derecedeki sektöre özel risk uygulanması durumu (2 Puan) / Sector-specific laws and regulations cannot be applied, but significant sector-specific risks apply. (2 Points)	Özel yasa ya da düzenlemede sektöre özel risk de uygulanamaz durumu (1Puan) / Sector-specific risk is also not applicable in a special law or regulation. (1Point)	*BGYS uygulamasının ölçeği /*Scale of ISMS application *İlgili mevzuat, kılavuzlar ve ilkeler /*Relevant legislation, guidelines and principles ISO/IEC 27001 A. 5.19
1.4 Ağ bağlantısı şifreleme teknolojisi /1.4 Network connection encryption technology	Dış veriler şifrelenmiş internet bağlantısı dijital imza PKI gereklilikleri durumu (3 Puan) / External data encrypted internet connection digital signature PKI requirements status (3 Points)	Dışsal veriler şifrelenmiş internet bağlantısı dijital imza olmadan durumu (2 Puan) / External data encrypted internet connection status without digital signature (2 Points)	Dış veriler şifresiz internet bağlantısı sayısal imza/PKI gereksinimleri durumu (1 Puan) / External data, unencrypted internet connection, digital signature/PKI requirements status (1 Point)	* Telekomünikasyon ve operasyon yönetimi ISO/IEC 27001 A. 8.24 /* Telecommunications and operations management ISO/IEC 27001 A. 8.24 *Erişim Kontrolü ISO/IEC 27001 A. 5.15 /*Access Control ISO/IEC 27001 A. 5.15
1.5 Risk durumu ve değerlendirilen kritik bilgilerin hacmi /1.5 Risk status and volume of critical information evaluated	≥ 50 (3 Puan) /≥ 50 (3 Points)	≥ 10 (2 Puan) /≥ 10 (2 Points)	< 10 (1 Puan) /< 10 (1 Point)	
1.6 Projelerinin sayısı ve büyüklüğü /1.6 Number and size of projects	≥ 7 (3 Puan) /≥ 7 (3 Points)	≥ 3 (2 Puan) /≥ 3 (2 Points)	< 3 (1 Puan) /< 3 (1 Point)	
1.7 Uzaktan çalışmanın kapsamı /1.7 Scope of remote working	≥ 25% (3 Puan) /≥ 25% (3 Points)	≥ 10% (2 Puan) /≥ 10% (2 Points)	< 10% (1 Puan) /< 10% (1 Point)	
1.8 BGYS Belgelendirme kapsamı /1.8 Scope of ISMS Certification	Karmaşık (3 Puan) / Complex (3 Points)	Normal (2 Puan) / Normal (2 Points)	Basit (1 Puan) / Simple (1 Point)	
2- BGYS kapsamının büyüklüğü ile ilgili faktörler /2- Factors related to the size of the ISMS scope				
2.1 Kullanılan bilgi sistemi sayısı (Program	≥10 (3 Puan) /≥10 (3 Points)	≥5 (2 Puan) /≥5 (2 Points)	< 5 (1 Puan) /< 5 (1 Point)	

Karmaşıklık Faktörleri / Complexity Factors	Risk Sınıfı / Risk Class			Önem / Importance
1-BGYS Karmaşıklık Faktörleri /1-ISMS Complexity Factors	Yüksek /High	Orta /Medium	Düşük /Low	
sayısı) /2.1 Number of information systems used (Number of programs)				
2.2 Kullanıcı sayısı /2.2 Number of users	≥ 100 bin (3 Puan) /≥ 100 thousand (3 Points)	≥ 50 bin (2 Puan) /≥ 50 thousand (2 Points)	< 50 bin (1 Puan) /< 50 thousand (1 Point)	
2.3 İmtiyazlı kullanıcı sayısı /2.3 Number of privileged users	≥50 (3 Puan) /≥ 50 (3 Points)	≥10 (2 Puan) /≥10 (2 Points)	<10 (1 Puan) /<10 (1 Point)	
2.4 İşletim sistemi platform sayısı /2.4 Number of operating system platforms	≥3 (3 Puan) /≥3 (3 Points)	≥2 (2 Puan) /≥2 (2 Points)	< 2 (1 Puan) /< 2 (1 Point)	
2.5 Ağ bağlantısı sayısı ve boyutu /2.5 Number and size of network connections				
Server sayısı / Number of servers	≥20 (3 Puan) /≥20 (3 Points)	≥10 (2 Puan) /≥10 (2 Points)	< 5 (1 Puan) /< 5 (1 Point)	
Çalışma istasyonu +PC +laptop / Workstation +PC +laptop	≥300 (3 Puan) /≥300 (3 Points)	≥50 (2 Puan) /≥50 (2 Points)	< 50 (1 Puan) /< 50 (1 Point)	
3-Kulanılan teknolojinin kapsamı ve çeşitliliği /3-Scope and diversity of technology used				
3.1 Proseslerin ve dokümanların kontrolleri /3.1 Controls of processes and documents	Yetersiz (3 Puan) / Insufficient (3 Points)	Normal (2 Puan) / Normal (2 Points)	Mükemmel (1 Puan) / Excellent (1 Point)	
3.2 Düzeltici ve Önleyici Faaliyet /3.2 Corrective and Preventive Action	Yetersiz (3 Puan) / Insufficient (3 Points)	Normal (2 Puan) / Normal (2 Points)	Mükemmel (1 Puan) / Excellent (1 Point)	
3.3 Bilgi sistemleri /3.3 Information systems				
3.3.1) Şebeke /3.3.1) Network	Wireless (3 Puan) /Wireless (3 Points)	Mobile (2 Puan) / Mobile (2 Points)	Sabit (1 Puan) / Fixed (1 Point)	
3.3.2) Lokasyon /3.3.2) Location	Harici (3 Puan) / External (3 Points)	Dahili (2 Puan) / Internal (2 Points)		
4. BGYS kapsamı içinde /Within the scope of ISMS				
4.1 Alan sayısı /4.1 Number of fields	≥ 5FarklıBenzer (3 Puan) /≥ 5DifferentSimilar (3 Points)	≥ 2FarklıBenzer (2 Puan) /≥ 2DifferentSimilar (2 Points)	1FarklıBenzer (1 Puan) /1DifferentSimilar (1 Point)	
4.2 Denetim alanları /4.2 Control areas	Tüm alan (3 Puan) / Whole field (3 Points)	Örnek alan (2 Puan) / Sample area (2 Points)	-	
5- Bu hizmetlere bağlılık ve BGYS'nin kapsamında kullanılan dış kaynak kullanımının ve üçüncü taraf anlaşmalarının kapsamı /5- Commitment to these services and the scope of outsourcing and third party agreements used within the scope of ISMS				
5.1 Dış kaynak kullanımı	Evet (3 Puan) / Yes (3 Points)	Hayır (1 Puan) / No (1 Point)		

Karmaşıklık Faktörleri / Complexity Factors	Risk Sınıfı / Risk Class			Önem / Importance
1-BGYS Karmaşıklık Faktörleri /1-ISMS Complexity Factors	Yüksek /High	Orta /Medium	Düşük /Low	
/5.1 Outsourcing				
5.2 BGYS kapsamında dış kaynak kullanımının oransal büyüklüğü /5.2 Proportional size of outsourcing within the scope of ISMS	≥ 50% (3 Puan) /≥ 50% (3 Points)	≥ 20% (2 Puan) /≥ 20% (2 Points)	< 20% (1 Puan) /< 20% (1 Point)	
5.3 Bu hizmetlere bağlılık /5.3 Commitment to these services	Düşük (3 Puan) / Low (3 Points)	Orta (2 Puan) / Medium (2 Points)	Yüksek (1 Puan) / High (1 Point)	
6. Belgelendirmeye uygulanan standardlar /6. Standards applied to certification				
6.1 Diğer standardlar /6.1 Other standards	Hayır (3 Puan) / No (3 Points)	-	Evet (1 Puan) / Yes (1 Points)	
6.2 Mevzuat ve düzenlemeler /6.2 Legislation and regulations	Hayır (3 Puan) / No (3 Points)	-	Evet (1 Puan) / Yes (1 Points)	
6.3 Uygulanabilen sektöre ilişkin diğer gereklilikler /6.3 Other applicable industry requirements	Hayır (3 Puan) / No (3 Points)	-	Evet (1 Puan) / Yes (1 Points)	

Arttırma/ Azaltma Yüzdesi / Increase/Decrease Percentage	Artırma/ Azaltma Miktarı / Increase/Decrease Amount	Risk Sınıfı / Risk Class	
91~100	+ 30 %	Yüksek /High	- Toplam adam/gün sayısı, tablodaki karmaşıklık faktörleri ve bunlarla ilgili mevcut alt yapı göz önünde bulundurularak hesaplanır. / - The total number of man/days is calculated by taking into account the complexity factors in the table and the existing infrastructure related to them. - Arttırma/Azaltma Yüzdesi = Toplam Puan X (100/78) / - Increase/Decrease Percentage = Total Score X (100/78)
86~90	+ 20 %		
76~85	+ 10 %	Orta /Medium	
66~75	0 %		
61~65	- 10 %		
56~60	- 20 %	Düşük /Low	
50~55	- 30 %		

Tablo 3 */Table 3* Sektör */Sector*	Sektör Grubu / *Sector Group*	İlgili Teknik Kapsam / *Relevant Technical Scope*	Alt Sektör Alan / *Subsector Area*
Üretim Sektörü / *Production sector*	**A**	**01-Tarım, Ormancılık** */01-Agriculture, Forestry* **03-Gıda Ürünleri İmalatı** */03-Food Products Manufacturing* **30-Otel İşletmeleri ve Restoran** */30-Hotel Management and Restaurant*	**A.01**
		02-Madencilik */02-Mining* **15-Metalik olmayan Ürünler** */15-Non-metallic Products*	**A.02**
		04-05-Tekstil ve Deri Ürünleri */04-05-Textile and Leather Products* **06-Ağaç Ürünleri** */06-Wood Products* **14-Plastik Ve Kauçuk Ürünler** */14-Plastic and Rubber Products*	**A.03**
		07-Kağıt ve Kağıt Ürünleri */07-Paper and Paper Products* **08-09-Matbaacılık ve Basım** */08-09-Printing and Printing*	**A.04**
		10-Petrol Ürünleri */10-Petroleum Products* **12-Kimyasalların İmalatı** */12-Manufacture of Chemicals*	**A.05**
		17-Metal Ürünleri İmalatı */17-Metal Products Manufacturing* **18-Makine ve Teçhizat** */18-Machinery and Equipment* **19-Elektrik ve Optik ürünler** */19-Electrical and Optical products* **22-Ulaşım Araçları İmalatı** */22-Transportation Vehicles Manufacturing*	**A.06**
		25-26-27-Elektrik-Gaz ve Su temini */25-26-27-Electricity-Gas and Water supply*	**A.07**
		24-Geri Dönüşüm */24-Recycling*	**A.08**
		28-İnşaat */28-Construction*	**A.09**
Hizmet Sektörü / *Service industry*	**B**	**29-Toptan Ve Perakende Ticaret** */29-Wholesale and Retail Trade*	**B.01**
		31-Ulaşım, Depolama, İletişim */31-Transportation, Storage, Communication*	**B.02**
		34-Mühendislik Hizmetleri */34-Engineering Services*	**B.03**
		35-Diğer Hizmetler	**B.04**

		/35-Other Services	
Özel Sektörler	C	33-Bilgi Teknolojileri /33-Information Technologies	C.01
		36-Kamu Yönetimi /36-Public Administration	C.02
		37-Eğitim /37-Education	C.03
		32-Finansal Hizmetler /32-Financial Services	C.04
		38-Sağlık /38-Health	C.05
		21-Havacılık ve Uzay /21-Aviation and Space	C.06
		33-Telekomünikasyon /33-Telecommunication	C.07
		39-Yardım Dernekleri kar amacı gütmeyen kuruluşlar /39-Charities non-profit organizations	C.08

Tablo 4 /Table 4 Sektör / Sector	Sektör Grubu / Sector Group	İlgili Teknolojik Alan / Related Technological Field	Teknolojik alan kodu / Technological area code
Üretim Sektörü /Hizmet/Özel Kategori / Production Sector / Service / Special Category	A/B/C ve alt gruplar Ortak / A/B/C and subgroups partner	Sunucu ve Masaüstü İşletim Sistemleri / Server and Desktop Operating Systems	TA-01
		Ağ ve Ağ Sistemleri / Network and Network Systems	TA-02
		Teknik Açıklık Analizi (Özellikle dışarıya açık olan hiz.) / Technical Vulnerability Analysis (Especially the services that are open to the outside.)	TA-03
		Uygulama Platformları / Application Platforms	TA-04
		Veri Tabanı Sistemleri (Müşteri Dataları, Üretim Dataları, Satış Dataları, vatandaş vb.) / Database Systems (Customer Data, Production Data, Sales Data, citizens, etc.)	TA-05
		Fiziki Güvenlik Tedbirleri / Physical Security Measures	TA-06
		Mesajlaşma Güvenliği / Messaging Security	TA-07
		Kriptografik kontrollerin düzenlenmesi / Regulation of cryptographic controls	TA-08
		Elektronik ticaret / Electronic trade	TA-09
Üretim / Production	A	Otomasyon Sistemi / Automation System	TA-10
Üretim / Production	A	Üretim aşamalarında alınan bilgi güvenliği tedbirleri (Çizimler vs.)	TA-11

		/ *Information security measures taken during production stages (Drawings, etc.)*	
Hizmet / *Service*	**B**	**Hizmet aşamalarında alınan bilgi güvenliği tedbirleri (Müşteri bilgileri vs.** / *Information security measures taken during service stages (Customer information, etc.*	**TA-12**
Özel Kategori / *Special Category*	**C 01**	**Yazılım kodlama Teknikleri** / *Software coding Techniques*	**TA-13**
		E-Fatura / *E-Invoice*	**TA 14**
		E-Arşiv / *E-Archive*	**TA 15**
		E-Defter / *E-Ledger*	**TA 16**

TABLO 5: */Table 5*

Düzenleyici Gereksinimler / *Regulatory Requirements*	**Düzenleyici Gereksinim kodu** / *Regulatory Requirement code*
Fikri Mülkiyet / *Intellectual property*	**DG-01**
Kurumsal kayıtların İçerikleri, korunması ve saklanması / *Contents, protection and storage of corporate records*	**DG-02**
Veri koruma ve mahremiyet / *Data protection and privacy*	**DG-03**
Kriptografik kontrollerin düzenlenmesi / *Regulation of cryptographic controls*	**DG-04**
Elektronik ve sayısal imzalar / *Electronic and digital signatures*	**DG-05**
İşyeri izlemesi / *workplace monitoring*	**DG-06**
Telekomünikasyon dinleme ve verinin izlenmesi / *Telecommunications interception and monitoring of data*	**DG-07**
Bilgisayarı kötüye kullanma / *computer abuse*	**DG-08**
Elektronik delil toplama / *Electronic evidence collection*	**DG-09**
Sızma testi / *Penetration testing*	**DG-10**
Uluslararası ve ulusal sektöre özgü şartlar / *International and national sector-specific conditions*	**DG-11**
Diğer / *Other*	**DG-12**

AVACERT; aşağıdaki gereklilikleri yerine getirmektedir,
/ AVACERT; It meets the following requirements,
a) Kuruluşun bilgi güvenliği risklerinin önemini ve bunların etkilerini dile getirişinin makul ve anlaşılır olup olmadığını denetlemek,
/ a) To check whether the organization's expression of the importance of information security risks and their effects is reasonable and understandable,
b) Uygunluk (bütün ilgili kanuni şartlar ve BGYS'ye uygunluk gösteren diğer şartlar) göstermek üzere tasarlanmış sistemin bunu yapabildiğini teyit ederek bu sistemin yerine getirildiğini ve korunduğunu belirtmek,
/ b) Confirming that the system designed to demonstrate compliance (all relevant legal requirements and other requirements that comply with the ISMS) is able to do so, and stating that this system is fulfilled and maintained,
c)Kontrol hedeflerinin ve kontrollerin doğru olarak seçilip belirlendiğinin teyit edilerek etkinliklerin ölçüldüğünün ve "güvenlik zaaflarını önleme ve doğru karşılık verme" hususunu başarma üzere oluşturulan prosesin uygun ve katılımcı olduğunun belirlenmesi,
/ c) Confirming that the control targets and controls are correctly selected and determined, determining that the activities are measured and that the process created to achieve "preventing security vulnerabilities and responding correctly" is appropriate and participatory,
d)Kuruluşun BGYS'si ile ilgili doküman gerekliliklerinin yerine getirildiğinin teyidi,
/ d) Confirmation that the document requirements regarding the organization's ISMS are met,
e) Aşama1 denetimden kaynaklanan artan talebin karşılanması
/ e) Meeting the increasing demand resulting from Stage 1 audit

BGYS denetim süresi Tablo 2'ye göre belirlenir ancak Denetleme süresi belirlenirken yukarıda belirtilen tüm faktörler dikkate alınmaktadır. Her bir belgelendirme için harcanan süredeki değişiklik işletmenin büyüklüğü, kapsamı organizasyon karmaşıklığı ve yukardaki faktörlere bağlı olarak değişiklik gösterebilir.
/ ISMS audit period is determined according to Table 2, but all the factors mentioned above are taken into account when determining the audit period. The change in time taken for each certification may vary depending on the size of the business, its scope, organizational complexity and the above factors.
Ek denetim süresi isteyen örnek etkenler;
/ Example factors that require additional audit time:
* BGYS kapsamında birden fazla bina veya lokasyonu içeren karmaşık lojistik
/ Complex logistics involving more than one building or location within the scope of ISMS*
* Birden fazla dilde konuşan çalışan (çevirmen isteyen veya bireysel denetçileri bağımsız çalışmaktan engelleyen)
/ Employee speaking multiple languages (requiring a translator or preventing individual supervisors from working independently)*
* Çok fazla düzenlemenin olması
/ Too much regulation*
* BGYS fazla karmaşık prosesleri veya göreceli olarak yüksek sayılı veya tek aktiviteleri kapsıyorsa
/ If the ISMS covers very complex processes or a relatively high number of or single activities*
* Prosesler donanım, yazılım, proses ve servislerin kombinasyonundan oluşuyorsa.
/ If the processes consist of a combination of hardware, software, processes and services.*
* Belgelendirmeye konu olan ana merkezlerin aktivitelerini teyit edecek geçici yerleri ziyaret etmeyi gerektiren aktiviteler (aşağıdaki not1'e bakınız)
/ Activities that require visiting temporary locations to confirm the activities of the main centers subject to certification (see note 1 below)*

Daha az denetim süresine izin verecek etkenler;
/ Factors that will allow less audits time:
* Risksiz ya da düşük risk içeren ürünler/prosesler
/ Risk-free or low-risk products/processes*
* Kuruluşun önceden bilinmesi (örneğin, eğer kuruluş AVACERT tarafından başka bir standardda belgelendirilmişse)
/ Knowing the organization in advance (for example, if the organization is certified by AVACERT in another standard)*
* Kuruluşun belgelendirme için hazır olması (örneğin, başka bir belgelendirme kuruluşu tarafından belgelendirilmiş ya da başka bir üçüncü parti danışmanlığı tarafından organize edilmiş),
/ The organization is ready for certification (e.g. certified by another certification body or organized by another third party consultancy),*
* Prosesler tek bir genel aktivite içeriyorsa (yalnızca hizmet),
/ If the processes contain a single general activity (service only),*
* Faaliyetteki yönetim sisteminin olgunluğu,
/ Maturity of the management system in operation,*
* Yüksek oranda kişinin aynı basit işleri yapıyor olması,
/ A high percentage of people are doing the same simple tasks,*

Not 1: Kuruluş veya belgelendirilmiş kuruluşun geçici yerlerde hizmet verdiği ya da üretim yaptığı durumlarda bu yerlerin değerlendirmesinin belgelendirme ve gözetim denetlemesinin içine alındığına dikkat edilmektedir.
/ Note 1: It is noted that in cases where the organization or certified organization provides services or produces in temporary locations, the evaluation of these places is included in the certification and surveillance audit.

BGYS kapsamına yapılan bütün atıflar, prosesler ve ürün/hizmetler değerlendirilmeli ve bu faktörler için adil bir düzeltme yapılarak daha fazla ya da az denetleme süresi etkin bir denetim için dahil edilmelidir. Aşağıdaki grafik denetleme zamanını arttırıcı ya da azaltıcı faktörlerin potansiyel etkileşimlerini göstermektedir.
/ All references to the ISMS scope, processes and products/services should be evaluated and a fair adjustment should be made for these factors and more or less audit time should be included for an effective audit. The graph below shows the potential interactions of factors that increase or decrease audit time.

BGYS kapsamının karmaşıklığı belirlenirken FRB-01 Başvuru Formu dikkate alınmaktadır. Karmaşıklık kriterleri denetim sürelerinin belirlenmesinde artırıcı veya azaltıcı faktörleri tespit etmede kullanılmaktadır.
/ FRB-01 Application Form is taken into consideration when determining the complexity of the ISMS scope. Complexity criteria are used to identify increasing or decreasing factors in determining audit times.

8.1.5. Çoklu Saha Örneklemesi */ Multi-Site Sampling*

BGYS belgelendirmeleri için birden fazla sahanın örnekleme kararları, kalite yönetim sistemleri için aynı kararlardan daha karmaşıktır. Müşteri kuruluşun aşağıda a) ile c) arasında olan kriterleri karşılayan sahaları olduğu durumlarda AVACERT, denetimlerde aşağıda verilen yaklaşımla değerlendirme yapmaktadır;

/ Sampling decisions for multiple sites for ISMS certifications are more complex than the same decisions for quality management systems. In cases where the customer organization has sites that meet the criteria between a) and c) below, AVACERT evaluates the audits with the approach given below;

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

/ a) All sites are centrally managed, supervised and operated under the same ISMS, which is subject to central management review,

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

/ b) All sites are included in the customer organization's ISMS internal audit program,

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

/ c) All sites are included in the customer organization's ISMS management review program.

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

/ Multi-site audits are carried out according to the principles given below and the table given below:

Sahaların sayısı (merkez ofis hariç) */ Number of sites (excluding head office)* (1)	İlk denetim için örnekleme sayısı */ Sampling number for first audits* (2)	Gözetim denetimi için örnekleme sayısı* */ Number of samples for surveillance audit** (3)	Belge yenileme denetimi için örnekleme sayısı */ Sampling number for document renewal audit* (4)
1-2	%100 (hepsi*/ All*)	Hepsi */ All*	Hepsi */ All*
3-4	2	2	2
5-9	3	2	3
10-25	4-5	3	4
26-36	6	4	5
37-49	7	5	6
50-64	8	5	7
65-100	9-10	6	8
101-121	11	7	9

122-144	12	8	10
145-169	13	8	11
170-225	14-15	9	12
226-256	16	10	13
257-289	17	11	14
290-324	18	11	15
325-400	19-20	12	16
> 400	en az 21 */ at least 21*	en az 13*/ at least 13*	en az 17*/ at least 17*

a) Sözleşmenin ilk gözden geçirmesinde, yeterli örnekleme seviyesinin belirlenebilmesi için, sahalar arasındaki farkları, mümkün olan en kapsamlı şekilde tanımlanır.

/ a) In the initial review of the contract, differences between sites are described in the most comprehensive manner possible to determine an adequate sampling level.

b) AVACERT tarafından aşağıdakiler dikkate alınarak, temsil edici sayıda saha seçilir:

/ b) A representative number of sites are selected by AVACERT, taking into account the following:

1) Merkez ofis ve sahaların iç denetim sonuçları,
/ 1) Internal audit results of the head office and fields,
2) Yönetimin gözden geçirmesi sonuçları,
/ 2) Management review results,
3) Saha/ların büyüklüklerindeki farklılıklar,
/ 3) Differences in the size of the field/s,
4) Saha/ların iş kapsamıyla ilgili farklılıklar,
/ 4) Differences regarding the work scope of the field/s,
5) BGYS'nin karmaşıklığı,
/ 5) The complexity of ISMS,
6) Farklı sahalardaki bilgi sistemlerinin karmaşıklığı,
/ 6) The complexity of information systems in different fields,
7) Çalışma şekillerindeki farklılıklar,
/ 7) Differences in working methods,
8) Tasarım ve operasyon kontrolündeki farklar
/ 8) Differences in design and operational control
9) Kritik bilgi sistemleri veya hassas bilgiyi işleyen bilgi sistemleriyle potansiyel etkileşimler,
/ 9) Potential interactions with critical information systems or information systems that process sensitive information,
10) Değişen yasal şartlar.
/ 10) Changing legal conditions.
11) Coğrafi ve kültürel yönler;
/ 11) Geographical and cultural aspects;
12) Tesislerin risk durumu
/ 12) Risk status of the facilities
13) Belirli tesislerde bilgi güvenliği olaylar
/ 13) Information security incidents at certain facilities

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

/ c) A representative sample is selected from all fields within the scope of the customer organization's ISMS; This selection is determined by a random selection based on the decision to be made reflecting the factors mentioned in b) above.

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

/ d) All sites facing significant risks within the scope of ISMS are audit by AVACERT before certification.

e) Denetim programı, yukarıdaki şartların ışığında tasarlanır ve BGYS belgelendirme kapsamının üç yıllık süre içinde temsili örneklerini kapsar.

/ e) The audit program is designed in the light of the above conditions and covers representative examples of the ISMS certification scope within a three-year period.

f) Merkez ofis veya tek bir sahada, bir uygunsuzluğun gözlemlendiği durumda, düzeltici faaliyet prosedürü merkez ofise ve belgelendirmenin kapsadığı tüm yerleşkelere uygulanır.

/ f) In case a nonconformity is observed in the head office or a single site, the corrective action procedure is applied to the head office and all campuses covered by the certification.

Aşağıda tarif edilen denetim, tek bir BGYS' nin tüm sahalara uygulanmasından ve işletim seviyesinde merkezden yönetim sağlandığından emin olunması için müşteri kuruluşun merkez ofis faaliyetlerini ele alır.

/ The audit described below addresses the client organization's head office activities to ensure that a single ISMS is applied to all sites and centralized management is achieved at the operational level.

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

/ At least 25% of the sample fields are selected randomly. The rest is selected from fields that show as much difference in quality as possible for a certain period of time.

8.1.6. Çoklu Yönetim Sistemi Standartları */ Multiple Management System Standards*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı ve Bilgi Güvenliği El Kitabı madde 9.1.6'da yer alan hükümler geçerlidir. Ek olarak aşağıdaki BGYS' ye özel şartlar ve kılavuz uygulanır.

/ The provisions of the ISO/IEC 17021-1:2015 standard and ISO/IEC 17021-1 System Certification Handbook and Information Security Handbook article 9.1.6 are valid. In addition, the following ISMS-specific conditions and guidance apply.

8.1.6.1. BG 9.1.6 BGYS Dokümantasyonunun Diğer Yönetim Sistemleri ile Entegrasyonu */ IS 9.1.6 Integration of ISMS Documentation with Other Management Systems*

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.

/ The client organization may combine documentation for the ISMS and other management systems (such as quality, health and safety and environment) as long as the appropriate interfaces to the ISMS and other systems are clearly identifiable.

AVACERT, BGYS belgelendirmesi ile bağlantılı olan diğer yönetim sistemleri belgelendirmesini önerebilir veya sadece BGYS belgelendirmesini teklif edebilir.

/ AVACERT may recommend other management systems certification in connection with ISMS certification or may offer only ISMS certification.

8.1.6.2. BG 9.1.6 Yönetim Sistemi Denetimlerini Birleştirilmesi */ IS 9.1.6 Combining Management System Controls*

BGYS denetimi, başka yönetim sistemlerinin denetimleri ile birleştirilebilir. Bu birleştirme, denetimin, BGYS belgelendirmesinin tüm şartlarını yerine getirdiği gösterilebilir olduğu sürece mümkündür. Bir BGYS için önemli olan tüm unsurlar, denetim raporlarında, açıkça görülmeli ve doğrudan tespit edilebilir olmalıdır. Denetimin kalitesi, denetimlerin birleştirilmesinden olumsuz yönde etkilenmemelidir.

/ ISMS audit can be combined with audits of other management systems. This combination is possible as long as it can be shown that the audit meets all the requirements of ISMS certification. All elements important for an ISMS should be clearly visible and directly detectable in audit reports. The quality of the audit should not be adversely affected by combining audits.

Entegre denetimlerin süresi, PR-07 Denetim Prosedürü baz alınarak belirlenir.

/ The duration of integrated audits is determined based on the PR-07 Audit Procedure.

8.2. Denetimlerin Planlanması */ Planning Audits*

8.2.1. Denetimin Amaç, Kapsam ve Kriterlerinin belirlenmesi */ Determining the Purpose, Scope and Criteria of the Audit*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı ve Bilgi Güvenliği El Kitabı madde 9.2.1'de yer alan hükümler geçerlidir. Ek olarak aşağıdaki BGYS' ye özel şartlar ve kılavuz uygulanır.

/ The provisions of the ISO/IEC 17021-1:2015 standard and ISO/IEC 17021-1 System Certification Handbook and Information Security Handbook article 9.2.1 are valid. In addition, the following ISMS-specific conditions and guidance apply.

8.2.1.1. BG 9.2.1 Denetimin Amacı */ IS 9.2.1 Purpose of Audit*

Denetimin amacı, müşteri kuruluşu, risk değerlendirmesine dayalı olarak uygulanabilir kontrolleri uyguladığı ve kurulu bilgi güvenlik amaçlarını gerçekleştirdiğine dair yönetim sisteminin etkililiğinin belirlenmesini içerecek şekilde belirlenir.

/ The objective of the audit is determined to include determining the effectiveness of the management system that the client organization has implemented applicable controls based on its risk assessment and achieved its established information security objectives.

8.2.2. Denetim Ekibinin Seçimi ve Atanması */ Selection and Appointment of the Audit Team*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı ve Bilgi Güvenliği El Kitabı madde 9.2.2'de yer alan hükümler geçerlidir. Ek olarak aşağıdaki BGYS' ye özel şartlar ve kılavuz uygulanır.

/ The provisions of the ISO/IEC 17021-1:2015 standard and ISO/IEC 17021-1 System Certification Handbook and Information Security Handbook article 9.2.2 are valid. In addition, the following ISMS-specific conditions and guidance apply.

8.2.2.1. BG 9.2.2 Denetim Ekibi */ IS 9.2.2 Audit Team*

Denetim ekibi resmen atanmalı ve uygun çalışma belgeleri olmalıdır. Denetleme ekibine verilen görev açıkça tanımlanacak ve müşteriye bildirilecektir.

/ The audit team must be formally appointed and have appropriate working documentation. The task assigned to the inspection team will be clearly defined and communicated to the client.

Bir denetim ekibi, kişinin Bilgi Güvenliği El Kitabı madde 7.1.2.1'de belirtilen tüm kriterleri karşılaması koşuluyla bir kişiden oluşabilir.

/ An audit team may consist of one person, provided that the person meets all the criteria specified in Article 7.1.2.1 of the Information Security Handbook.

8.2.2.2. BG 9.2.2 Denetim Ekibi Yeterliliği */ IS 9.2.2 Audit Team Competence*

Bilgi Güvenliği El Kitabı madde 7.1.2'de listelenen şartlar geçerlidir. Gözetim ve özel denetim faaliyetleri için, sadece planlanmış gözetim faaliyeti ve özel denetim faaliyeti ile ilgili olan unsurlar uygulanır.

/ The conditions listed in Article 7.1.2 of the Information Security Handbook apply. For surveillance and special audit activities, only those elements relevant to the planned surveillance activity and special audit activity apply.

Belli bir denetimi için atanacak olan denetim ekibini seçerken ve yönetirken, AVACERT, görevlendirilen her ekip üyesinin aşağıda belirtilen yetkinliği sağlandığını garanti etmektedir:

/ When selecting and managing the audit team to be assigned for a particular audit, AVACERT ensures that each assigned team member has the following competencies:

a) Belgelendirme için aranan ve ilgili prosedürler ve potansiyel bilgileri güvenlik riskleri ile (Teknik Uzmanlar bu işlevi yerine getirebilir) BGYS kapsamındaki spesifik faaliyetlere ilişkin uygun teknik bilgiye sahiptir;

/ a) Has appropriate technical knowledge of the specific activities within the scope of the ISMS sought for certification and related procedures and potential information about security risks (Technical Experts can perform this function);

b) BGYS' yi, faaliyetleri, ürünleri ve hizmetleri ile ilgili bilgi güvenliği yönünü yönetmek için BGYS' nin kapsam ve bağlamını sağlayan bir güvenilir belgelendirme denetimi yapmak için yeterli olan müşteri kuruluşun anlayışına sahip olmak;

/ b) have an understanding of the client organization sufficient to conduct a reliable certification audit that provides the scope and context of the ISMS to manage the information security aspect of its ISMS, activities, products and services;

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

/ c) Ensuring a proper understanding of the legal and regulatory requirements applicable to the client organization's ISMS.

Teknik Alan Kodu */ Technical Area Code*	**Teknik Alan / Technical Area**	**Alt Teknik Alan Kodu / Sub Technical Area Code**	**Alt Teknik Alan / Sub-Technical Field**
A	Finansal Hizmetler / Financial Services	A.1	Bankalar */ Banks*
		A.2	Sigorta şirketleri */ insurance companies*
B	Bilgi Teknolojileri-Geliştirme/Hizmetler, Telekom */ Information Technologies-Development/Services, Telecom*	B.1	Yazılım Hizmetleri */ Software Services*
		B.2	Donanım Hizmetleri */ Hardware Services*
		B.3	İnternet Servis Sağlayıcı/Server Hizmetleri */ Internet Service Provider/Server Services*
		B.4	BT-Danışmanlığı */ IT-Consultancy*
		B.5	IT-Consultancy */ IT-Consultancy*
		B.6	Tamir ve Bakım (Teknik Servis) Hizmetleri */ Repair and Maintenance (Technical Service) Services*
C	Sağlık ve Eğitim */ Health and Education*	C.1	Hastaneler */ Hospitals*
		C.2	Okullar */ Schools*
D	Kamu/Devlet Kurumları */ Public/Government Institutions*	D.1	Kamu Otoritesi */ Public Authority*
		D.2	Kamu Hizmeti */ Public service*
		D.3	Eğitim Öğretim Hizmetleri */ Educational Services*
		D.4	Askeriye */ The military*
E	Otomotiv/Havacılık */ Automotive/Aviation*	E.1	Otomotiv Üreticisi/Tedarikçisi */ Automotive Manufacturer/Supplier*
		E.2	Uçak/Uzay Sanayi */ Aircraft/Aerospace Industry*
F	Çeşitli sanayi */ Various industries*	-	

8.2.3. Denetim Planı ***/ Audit Plan***

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı ve Bilgi Güvenliği El Kitabı madde 9.2.3'de yer alan hükümler geçerlidir. Ek olarak aşağıdaki BGYS'ye özel şartlar ve kılavuz uygulanır.

/ The provisions of the ISO/IEC 17021-1:2015 standard and ISO/IEC 17021-1 System Certification Handbook and Information Security Handbook article 9.2.3 are valid. In addition, the following ISMS-specific conditions and guidance apply.

8.2.3.1. BG 9.2.3 Genel ***/ IS 9.2.3 General***

BGYS denetimleri için denetim planı, belirlenen bilgi güvenlik kontrollerini dikkate alacak şekilde oluşturulmaktadır.

/ The audit plan for ISMS audits is created to take into account the determined information security controls.

8.2.3.2. BG 9.2.3 Ağ Destekli Denetim Teknikleri ***/ IS 9.2.3 Network Assisted Control Techniques***

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

/ If necessary, the audit plan for network-assisted audit techniques is determined in accordance with the network-assisted audit techniques to be used during the audit in question.

Ağ destekli denetim teknikleri, örneğin, telekonferans, web görüşmesi, etkileşimli web tabanlı iletişim ve BGYS dokümantasyonuna ve/veya BGYS proseslerine uzaktan elektronik erişimi içerebilir. Bu tür tekniklerin hedefi, denetim etkinliğini ve verimliliğini arttırması ve denetimin bütünlüğünü desteklemesidir.

/ Network-enabled audit techniques may include, for example, teleconferencing, web conferencing, interactive web-based communication, and remote electronic access to ISMS documentation and/or ISMS processes. The goal of such techniques is to increase audit effectiveness and efficiency and support audit integrity.

Yasalar ve düzenleyicilerle uyumluluğun sürdürülmesi ve değerlendirmesi, müşteri kuruluşun sorumluluğudur. AVACERT, BGYS'nin bu yönde işlediğine dair güven oluşturmak için kontroller ve örnekleri incelemektedir. AVACERT, müşteri kuruluşun bilgi güvenliği riskleri ve etkilerine uygulanabilir olan yasa ve düzenleyicilerle uyumluluğu sağlayacak bir yönetim sistemine sahip olduğunu doğrulamaktadır.

/ It is the client organization's responsibility to maintain and evaluate compliance with laws and regulators. AVACERT examines controls and examples to create confidence that the ISMS operates in this direction. AVACERT confirms that the client organization has a management system to ensure compliance with laws and regulators applicable to information security risks and impacts.

8.2.3.3. BG 9.2.3 Denetimin Zamanlaması ***/ IS 9.2.3 Timing of Audit***

AVACERT, denetlenecek müşteri kuruluşla, denetimin zamanlaması konusunda teyitleşmekte ve denetim sezona, aya, tarihe ve vardiyaya uygun olarak yapılabilmektedir.

/ AVACERT confirms the timing of the audit with the customer organization to be audited, and the audit can be carried out in accordance with the season, month, date and shift.

8.3. İlk Belgelendirme ***/ Initial Certification***

BGYS denetimlerinin uygulaması için, PR-09 BGYS Denetim Prosedürü oluşturulmuş ve uygulanmaktadır.

/ For the implementation of ISMS audits, PR-09 ISMS Audit Procedure has been created and implemented.

8.3.1. BG 9.3.1 İlk Belgelendirme Denetimi ***/ IS 9.3.1 Initial Certification Audit***

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı ve Bilgi Güvenliği El Kitabı madde 9.3'de yer alan hükümler geçerlidir. Ek olarak aşağıdaki BGYS' ye özel şartlar ve kılavuz uygulanır.

/ The provisions of the ISO/IEC 17021-1:2015 standard and ISO/IEC 17021-1 System Certification Handbook and Information Security Handbook article 9.3 are valid. In addition, the following ISMS-specific conditions and guidance apply.

8.3.1.1. Aşama 1 /Stage 1

BGYS denetimlerinin uygulaması için, PR-09 BGYS Denetim Prosedürü oluşturulmuş ve uygulanmaktadır.

/ For the implementation of ISMS audits, PR-09 ISMS Audit Procedure has been created and implemented.

8.3.1.2. Aşama 2 / Stage 2

BGYS denetimlerinin uygulaması için, PR-09 BGYS Denetim Prosedürü oluşturulmuş ve uygulanmaktadır.

/ For the implementation of ISMS audits, PR-09 ISMS Audit Procedure has been created and implemented.

8.4. Denetimin Gerçekleştirilmesi */ 8.4. Performing the Audit*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı ve Bilgi Güvenliği El Kitabı madde 9.4'de yer alan hükümler geçerlidir. Ek olarak aşağıdaki BGYS' ye özel şartlar ve kılavuz uygulanır.

/ The provisions of the ISO/IEC 17021-1:2015 standard and ISO/IEC 17021-1 System Certification Handbook and Information Security Handbook article 9.4 are valid. In addition, the following ISMS-specific conditions and guidance apply.

8.4.1. BG 9.4 Genel */ IS 9.4 General*

BGYS denetimleri için, PR-09 BGYS Denetim Prosedürü oluşturulmuş ve uygulanmaktadır.

/ For ISMS audits, PR-09 ISMS Audit Procedure has been created and implemented.

8.4.2. BG 9.4 BGYS Denetiminin Özel Unsurları */ IS 9.4 Special Elements of ISMS Audit*

BGYS denetimlerinin özel unsurlarının belirlenmesi için, PR-09 BGYS Denetim Prosedürü oluşturulmuş ve uygulanmaktadır.

/ In order to determine the special elements of ISMS audits, PR-09 ISMS Audit Procedure has been created and implemented.

8.4.3. BG 9.4 Denetim Raporu */ IS 9.4 Audit Report*

BGYS belgelendirme denetim raporlarının içeriği ve kullanımı için, PR-09 BGYS Denetim Prosedürü oluşturulmuş ve uygulanmaktadır.

/ PR-09 ISMS Audit Procedure has been created and implemented for the content and use of ISMS certification audit reports.

8.5. Belgelendirme Kararı */ Certification Decision*

AVACERT, denetim ekibinden, belgelendirme kararına esas sağlamak amacıyla, kararı alabilmek için yeterli bilgileri sağlayan açık ve anlaşılır denetim raporları talep etmektedir.

/ AVACERT requests clear and understandable audit reports from the audit team that provide sufficient information to make the decision, in order to provide the basis for the certification decision.

8.5.1. BG 9.5 Belgelendirme Kararı */ IS 9.5 Certification Decision*

BGYS belgelendirmenin verilmesi/geri çekilmesi kararları, PR-06 Belgelendirme Prosedürü doğrultusunda, AVACERT bünyesinde oluşturulmuş Belgelendirme Komitesi tarafından alınır.

/ Decisions on granting/withdrawing ISMS certification are made by the Certification Committee established within AVACERT, in line with the PR-06 Certification Procedure.

Belgelendirme Komitesi, denetim proseslerinin ve denetim ekibi tarafından yapılan ilgili önerilerin değerlendirilmesi için yeterli olan tüm alanlarda belirli seviyede bilgi birikimi ve tecrübeye sahip, kişi/kişilerden oluşturulur.

/ The Certification Committee is composed of person(s) who have a certain level of knowledge and experience in all areas sufficient to evaluate the audit processes and the relevant recommendations made by the audit team.

Bir müşteri kuruluşun BGYS'sinin belgelendirmesi veya belgelendirilmemesi kararı, AVACERT tarafından, belgelendirme prosesinde toplanan bilgiler ve diğer tüm ilgili bilgilere dayanılarak alınır. Belgelendirme kararını verenler, denetimde yer almamış kişi/kişiler olmaktadır. Bu karar, denetim raporunda (bk. madde BG 9.4.3) sunulduğu üzere denetim ekibinin bulguları ve belgelendirme önerisi ile AVACERT'ye açık diğer tüm ilgili bilgilere dayanır.

/ The decision to certify or not to certify a client organization's ISMS is made by AVACERT based on the information collected during the certification process and all other relevant information. Those who make the certification decision are the person(s) who were not involved in the audit. This decision is based on the audit team's findings and certification recommendation as presented in the audit report (see clause IS 9.4.3) and any other relevant information available to AVACERT.

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

/ It is essential that the Certification Committee does not normally reject a negative recommendation from the audit team. If such a situation occurs, AVACERT will put in writing and justify the decision to reject the recommendation.

Yönetimin gözden geçirmesi ve BGYS iç denetimleri için düzenlemelerin yapıldığı, etkin olduğu ve sürdürüleceğinin gösterilmesine dair yeterli delil olmadığı sürece, müşteri kuruluşa belgelendirme verilmez.

/ Certification is not given to the client organization unless there is sufficient evidence to show that arrangements for management review and ISMS internal audits have been made, are effective and will be maintained.

8.6. Belgelendirmenin Sürdürülmesi */ Maintaining Certification*

8.6.1. Genel */General*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı ve Bilgi Güvenliği El Kitabı madde 9.6.1'de yer alan hükümler geçerlidir.

/ The provisions of the ISO/IEC 17021-1:2015 standard and ISO/IEC 17021-1 System Certification Handbook and Information Security Handbook article 9.6.1 are valid.

8.6.2. Gözetim Faaliyetleri */ Surveillance Activities*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı ve Bilgi Güvenliği El Kitabı madde 9.6.2'de yer alan hükümler geçerlidir.

/ The provisions of the ISO/IEC 17021-1:2015 standard and ISO/IEC 17021-1 System Certification Handbook and Information Security Handbook article 9.6.2 are valid.

8.6.2.1. Gözetim Faaliyetleri */ Surveillance Activities*

BGYS gözetim denetimlerinin uygulaması için, PR-09 BGYS Denetim Prosedürü oluşturulmuş ve uygulanmaktadır.

/ For the implementation of ISMS surveillance audits, PR-09 ISMS Audit Procedure has been created and implemented.

Gözetimin amacı, onaylanmış BGYS'nin uygulamasının sürdürüldüğünün doğrulanması, müşteri kuruluşun işletimindeki değişikliklerin sonucunda başlatılan sistemdeki değişikliklerin sonuçlarının dikkate alınması ve belgelendirme şartları ile sürekli uyumluluğun doğrulanmasıdır.

/ The purpose of the surveillance is to verify that the implementation of the approved ISMS is maintained, to take into account the consequences of changes in the system initiated as a result of changes in the operation of the customer organization, and to verify ongoing compliance with the certification requirements.

8.6.3. Yeniden Belgelendirme */ Recertification*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı ve Bilgi Güvenliği El Kitabı madde 9.6.3'de yer alan hükümler geçerlidir.

/ The provisions of the ISO/IEC 17021-1:2015 standard and ISO/IEC 17021-1 System Certification Handbook and Information Security Handbook article 9.6.3 are valid.

8.6.3.1. Yeniden Belgelendirme Denetimleri */ Recertification Audits*

BGYS yeniden belgelendirme denetimlerinin uygulaması için,PR-09 BGYS Denetim Prosedürü oluşturulmuş ve uygulamaktadır.

/ For the implementation of ISMS re-certification audits, PR-09 ISMS Audit Procedure has been created and implemented.

8.6.4. Özel Denetimler */Special Audits*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı ve Bilgi Güvenliği El Kitabı madde 9.6.4'de yer alan hükümler geçerlidir.

/ The provisions of the ISO/IEC 17021-1:2015 standard and ISO/IEC 17021-1 System Certification Handbook and Information Security Handbook article 9.6.4 are valid.

8.6.4.1. Özel Durumlar / Exceptions

Belgelendirilmiş bir BGYS'ye sahip müşteri kuruluş, sistemindeki büyük çapta değişiklik yaparsa veya belgelendirmenin temelini etkileyebilecek diğer değişiklikler gerçekleştirirse (SOA üzerinden yapılan değişiklikler gibi) bu durumlardan AVACERT'yi haberdar etmesi istenmektedir. Böyle durumlarda, özel denetimler gerçekleştirilir.

/ If the customer organization with a documented ISMS makes major changes in its system or other changes that may affect the basis of certification (such as changes made through SOA), it is requested to inform AVACERT of these situations. In such cases, special inspections are carried out.

8.6.5. Belgelendirmenin Askıya Alınması, Geri çekilmesi veya Kapsamının Daraltılması */ Suspension, Withdrawal or Reduction of Scope of Certification*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı ve Bilgi Güvenliği El Kitabı madde 9.6.5'da ve PR-06 Belgelendirme Prosedüründe yer alan hükümler geçerlidir.

/ The provisions of the ISO/IEC 17021-1:2015 standard and the ISO/IEC 17021-1 System Certification Handbook and Information Security Handbook article 9.6.5 and the PR-06 Certification Procedure are valid.

8.7. İtirazlar */ Objections*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı ve Bilgi Güvenliği El Kitabı madde 9.7'de ve PR-12 İtiraz ve Şikâyet Prosedüründe yer alan hükümler geçerlidir.

/ The provisions of the ISO/IEC 17021-1:2015 standard and the ISO/IEC 17021-1 System Certification Manual and Information Security Manual article 9.7 and the PR-12 Objection and Complaint Procedure are valid.

8.8. Şikâyetler */ Complaints*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı ve Bilgi Güvenliği El Kitabı madde 9.8'de ve PR-12 İtiraz ve Şikâyet Prosedüründe yer alan hükümler geçerlidir. Ek olarak BGYS'ye özel aşağıdaki hükümler ve kılavuz uygulanır.

/ The provisions of the ISO/IEC 17021-1:2015 standard and the ISO/IEC 17021-1 System Certification Manual and Information Security Manual article 9.8 and the PR-12 Objection and Complaint Procedure are valid. In addition, the following provisions and guidance specific to ISMS apply.

8.8.1. BG 9.8 Şikâyetler */ IS 9.8 Complaints*

AVACERT, BGYS'si belgelendirilmiş her bir müşteri kuruluşa, ISO/IEC 27001:2013'in şartları doğrultusunda tüm şikâyetlerin ve gerçekleştirilen düzeltici faaliyetlerin kayıtlarının istendiğinde incelemeye hazır bulundurulmasını, belgelendirme sözleşmesinde şart koşmaktadır.

/ AVACERT stipulates in the certification contract that each customer organization whose ISMS is certified shall have the records of all complaints and corrective actions taken, available for review when requested, in line with the requirements of ISO/IEC 27001:2013.

8.9. Müşteri Kayıtları */ Customer Records*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı madde 9.9'da PR-01 Dokümanların ve Kayıtların Kontrolü Prosedüründe yer alan hükümler geçerlidir.

/ The provisions of the ISO/IEC 17021-1:2015 standard and the PR-01 Control of Documents and Records Procedure in article 9.9 of the ISO/IEC 17021-1 System Certification Handbook are valid.

9. BELGELENDİRME KURULUŞLARI İÇİN YÖNETİM SİSTEMİ ŞARTLARI */ MANAGEMENT SYSTEM REQUIREMENTS FOR CERTIFICATION BODIES*

ISO/IEC 17021-1:2015 standardı ve ISO/IEC 17021-1 Sistem Belgelendirme El Kitabı madde 10.2'da yer alan şartlar uygulanır. Ek olarak, aşağıdaki BGYS ye özel şartlar ve kılavuz uygulanır.

/ The conditions set out in article 10.2 of the ISO/IEC 17021-1:2015 standard and the ISO/IEC 17021-1 System Certification Handbook apply. In addition, the following ISMS-specific terms and guidance apply.

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

/ It is carried out according to the AVACERT management system procedures given below, prepared in accordance with the ISO/IEC 17021-1:2015 standard:

- PR-01 Dokümanların ve Kayıtların Kontrolü prosedürü */ - PR-01 Control of Documents and Records procedure*
- PR-02 Yönetim Gözden Geçirme Prosedürü */ - PR-02 Management Review Procedure*
- PR-03 İç Tetkik Prosedürü */ - PR-03 Internal Audit Procedure*
- PR-04 Düzeltici Faaliyet Prosedürü */ - PR-04 Corrective Action Procedure*

**geçiş süreci tamamlanana kadar , 3 kasım 2023 tarihinden itibaren ilk belgelendirme veya yeniden belgelendirme yapılamaz. Gözetim ise; 25 ekim 2025 tarihine kadar bitiş tarihi olabilmektedir.
*/**Initial certification or re-certification cannot be made as of November 3, 2023, until the transition process is completed. Surveillance is; The expiry date may be up to October 25, 2025.*

10. İLGİLİ DOKÜMANLAR ve REFERANSLAR */ RELATED DOCUMENTS and REFERENCES*

ISO/IEC 17021-1:2015
ISO/IEC 27006:2015 AMD.1 2020
ISO/IEC 27001:2022
ISO/IEC 27002:2017
Sistem Belgelendirme El Kitabı */ System Certification Handbook*
Bilgi Güvenliği El Kitabı / Information Security Handbook
FRB-01 Başvuru Formu */ FRB-01 Application Form*
FRB-01 EK-2 ISO 27001 Başvuru Ek Bilgilendirme Formu */ FRB-01 APPENDIX-2 ISO 27001 Application Additional Information Form*
FRB-02 Başvuru Gözden Geçirme Formu */ FRB-02 Application Review Form*
PR-01 Dokümanların ve Kayıtların Kontrolü prosedürü */ PR-01 Control of Documents and Records procedure*
PR-11Personel Atama ve Performans Değerlendirme Prosedürü */ PR-11Personnel Appointment and Performance Evaluation Procedure*
PR-12 İtiraz ve Şikâyet Prosedürü */ PR-12 Objection and Complaint Procedure*
PR-03 İç Tetkik Prosedürü */ PR-03 Internal Audit Procedure*
PR-02 Yönetim Gözden Geçirme Prosedürü */ PR-02 Management Review Procedure*
PR-04 Düzeltici Faaliyet Prosedürü */ PR-04 Corrective Action Procedure*
PR-06 Belgelendirme Prosedürü */ PR-06 Certification Procedure*
PR-07 Denetim Prosedürü */ PR-07 Audit Procedure*
PR-08 BGYS Belgelendirme Prosedürü */ PR-08 ISMS Certification Procedure*
PR-09 BGYS Denetim Prosedürü */ PR-09 ISMS Audit Procedure*
TL-02 Logo ve Belge kullanım Talimatı */ TL-02 Logo and Document Usage Instruction*