REVİZYON TABLOSU */REVISION TABLE*		
Revizyon No ***Revision No***	**Revizyon Tarihi** ***Revision Date***	**Revizyon Nedeni** ***Reason For Revision***
00	25.03.2021	İlk Yayın /First broadcast
01	14.11.2022	Aşama 2 denetimine geçiş onayının verilmesine dair revizyon */Revision regarding the approval of transition to Stage 2 audit*
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 ve ISO/IEC 27006:2015 AMD.1 2020 standartları doğrultusunda, denetimlerin gerçekleştirilmesi için yöntem ve sorumlulukları belirlemektir.

/The purpose of this procedure is; To determine the methods and responsibilities for carrying out audits in line with ISO/IEC 27006:2015 and ISO/IEC 27006:2015 AMD.1 2020 standards.

2. TANIMLAR */DEFINITIONS*

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

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

Varlık: Kuruluş için değeri olan herhangi bir şey. [ISO/IEC 13335-1: 2004]

/Asset: Anything that has value to the organization. [ISO/IEC 13335-1:2004]

Kullanılabilirlik: Yetkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliği. [ISO/IEC 13335-1: 2004]

/Availability: The ability to be accessible and usable when requested by an authorized entity. [ISO/IEC 13335-1:2004]

Gizlilik: Bilginin yetkisiz kişiler, varlıklar ya da proseslere kullanılabilir yapılmama ya da açıklanmama özelliği. [ISO/IEC 13335-1: 2004]

/Confidentiality: The ability of information not to be made available or disclosed to unauthorized persons, entities or processes. [ISO/IEC 13335-1:2004]

Bilgi Güvenliği: Bilginin gizliliği, bütünlüğü ve kullanılabilirliğinin korunması. Ek olarak, doğruluk, açıkla edememe ve güvenilirlik gibi diğer özellikleri de kapsar. [ISO/IEC 17799: 2005]

/Information Security: Protecting the confidentiality, integrity and availability of information. Additionally, it includes other characteristics such as accuracy, inexplicability, and reliability. [ISO/IEC 17799:2005]

Bilgi Güvenliği Olayı: Olası bir bilgi güvenliği politikası açığı, koruyucuların başarısızlığı ya da güvenlikle ilgili olabilecek önceden bilinmeyen bir durumu belirten bir sistem, hizmet ya da ağ durumunun tanımlanan bir ortaya çıkışı. [ISO/IEC TR 18044: 2004]

/Information Security Incident: An identified occurrence of a system, service, or network condition that indicates a potential information security policy vulnerability, failure of safeguards, or a previously unknown condition that may be security-related. [ISO/IEC TR 18044:2004]

Bilgi Güvenliği İhlal Olayı: İş operasyonlarını tehlikeye atma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek istenmeyen ya da beklenmeyen bilgi güvenliği olayı. [ISO/IEC TR 18044: 2004]

/Information Security Breach Incident: A single unintended or unexpected information security event that is likely to compromise business operations and threaten information security. [ISO/IEC TR 18044:2004]

Bütünlük: Varlıkların doğruluğunu ve tamlığını koruma özelliği. [ISO/IEC 13335-1: 2004]

/Integrity: The ability to maintain the accuracy and completeness of assets. [ISO/IEC 13335-1:2004]

Artık Risk: Risk işlemeden sonra kalan risk.[ISO/IEC Guide 73]

/Residual Risk: The risk remaining after risk treatment.[ISO/IEC Guide 73]

Riskin Kabulü: Bir riski kabul etme kararı.

/Acceptance of Risk: The decision to accept a risk.

Risk Analizi: Kaynakları belirlemek ve riski tahmin etmek amacıyla bilginin sistematik kullanımı.[ISO/IEC Guide 73]

/ Risk Analysis: Systematic use of information to identify resources and estimate risk.[ISO/IEC Guide 73]

Risk Değerlendirme: Risk analizi ve risk derecelendirmesini kapsayan tüm proses. [ISO/IEC Guide 73]

/Risk Assessment: The entire process including risk analysis and risk rating. [ISO/IEC Guide 73]

Risk Derecelendirme: Riskin önemini tayin etmek amacıyla tahmin edilen riskin verilen risk kriterleri ile karşılaştırılması prosesi. [ISO/IEC Guide 73]

/Risk Grading: The process of comparing the estimated risk with the given risk criteria in order to determine the significance of the risk. [ISO/IEC Guide 73]

Risk Yönetimi: Bir kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetler. [ISO/IEC Guide 73]

/Risk Management: Coordinated activities used to control and direct an organization regarding risk. [ISO/IEC Guide 73]

Risk İşleme: Riski değiştirmek için alınması gerekli önlemlerin (kontrollerin) seçilmesi ve uygulanması prosesi. [ISO/IEC Guide 73]

/Risk Treatment: The process of selecting and implementing the measures (controls) necessary to change the risk. [ISO/IEC Guide 73]

Uygulanabilirlik Beyanı (SOA): Müşteri kuruluşun BGYS'si ile ilgili ve uygulanabilir kontrol amaçlarını ve kontrolleri açıklayan dokümante edilmiş beyan (Kontrol amaçları ve kontroller, risk değerlendirme ve risk işleme proseslerinin sonuçları ve çıkarımlarını, yasal ve düzenleyici gereksinimleri, anlaşma yükümlülüklerini ve kuruluşun bilgi güvenliği için iş gereksinimlerini temel alır).

/Statement of Applicability (SOA): Documented statement describing the control objectives and controls applicable to the client organization's ISMS (Control objectives and controls include the results and implications of risk assessment and risk treatment processes, legal and regulatory requirements, contractual obligations, and the organization's information security). based on business requirements).

SORUMLULUKLAR ve UYGULAMALAR */RESPONSIBILITIES AND PRACTICES*

2.1. Genel */General*

BGYS denetimleri, Denetim Prosedüründe belirlenen denetim uygulamaları doğrultusunda gerçekleştirilir.

/ISMS audits are carried out in line with the audit practices determined in the Audit Procedure.

BGYS denetimleri, Denetim Prosedüründe belirlenen denetim uygulamaları dışında, aşağıda verilen esaslar dikkate alınarak gerçekleştirilir.

/ISMS audits are carried out by taking into account the principles given below, apart from the audit practices specified in the Audit Procedure.

2.2. BGYS Denetim Şartları */ISMS Audit Conditions*

Belgelendirme denetiminden önce müşteri kuruluşa denetim ekibinin görmesini istemedikleri gizli ya da hassas bilgi içeren kayıtları olup olmadığı sorulur. Sonrasında AVACERT denetim ekibi, bu kayıtların yokluğunda BGYS'nin yeterince denetlenip denetlenemeyeceğine karar verir. Eğer bu kayıtların yokluğunda denetim yapılamayacağına karar verirse müşteri kuruluşa erişim için gerekli düzenlemeler yapılmadan denetim yapılamayacağı bildirilir.

/ Before the certification audit, the client organization is asked whether it has records containing confidential or sensitive information that they do not want the audit team to see. Afterwards, the AVACERT audit team decides whether the ISMS can be adequately audited in the absence of these records. If it decides that an audit cannot be performed in the absence of these records, the customer is informed that the audit cannot be performed without making the necessary arrangements for access to the organization.

2.2.1. Denetim Kriterleri */Audit Criteria*

Bir müşterinin BGYS denetimi ile ilgili kriterler; BGYS standardı ISO/IEC 27001'de belirtilenler ve ilgili faaliyetler için oluşturulan dokümanlardan oluşmaktadır.

/Criteria for a customer's ISMS audit; The ISMS standard consists of documents created for those specified in ISO/IEC 27001 and related activities.

2.2.2. Belgelendirme Kapsamı */Scope Of Certification*

AVACERT denetim ekibi, müşteri kuruluşu, uygulanabilir bütün BGYS gereklilikleri kapsamında denetleyecektir. AVACERT denetim ekibi, müşteri kuruluşunun BGYS' nin kapsamının ve sınırlarının işin, kuruluşun, yerinin, varlıklarının ve teknolojinin özellikleri açısından açıkça tanımlanmış olduğunu garanti edecektir. AVACERT denetim ekibi, ISO/IEC 27001, Madde 1.2'de belirtilen gereklere müşteri kuruluşunun uyduğuna dair hususları, BGYS' nin kapsamında teyit edecektir.

/AVACERT audit team will audit the customer organization within the scope of all applicable ISMS requirements. AVACERT audit team will ensure that the scope and boundaries of the client organization's ISMS are clearly defined in terms of the characteristics of the business, organization, location, assets and technology. AVACERT audit team will confirm within the scope of the ISMS that the customer organization complies with the requirements specified in ISO/IEC 27001, Article 1.2.

AVACERT, müşterinin bilgi güvenliği risk değerlendirmesinin ve risk karşısındaki davranışının ISO/IEC 27001 BGYS standardının kapsamını içeren aktivitelerle uyumlu olduğunu temin etmektedir. AVACERT denetim ekibi, buna ilişkin ifadelerin BGYS ve Uygunluk Beyanında açıkça yansıtıldığını teyit edecektir.

/AVACERT ensures that the customer's information security risk assessment and risk response are compatible with the activities that include the scope of the ISO/IEC 27001 ISMS standard. AVACERT audit team will confirm that the relevant statements are clearly reflected in the ISMS and Declaration of Conformity.

AVACERT denetim ekibi, müşteri kuruluşun belgelendirmesine konu olan BGYS' nde ve bilgi güvenliği risk değerlendirmesinde BGYS' nin direkt kapsamında olmayan hizmet ve aktivitelerin de gerekli yerlerde işaret edildiğini garanti altına alacaktır.

AVACERT audit team will ensure that the services and activities that are not directly within the scope of the ISMS, which are the subject of the customer organization's certification, and in the information security risk assessment, are also marked where necessary.

2.2.3. Çok Sahalı Kuruluşların Denetimi */Audit Of Multi-site Organizations*

Çok sahalı kuruluşların denetiminde, aşağıdaki şartların yerine getirildiği incelenmelidir: */ The audit of multi-site organizations should examine whether the following conditions are met:*

- Sistem dokümantasyonu ve sistem değişiklikleri, */System documentation and system changes,*
- Yönetimin gözden geçirmesi, */management review,*
- Şikâyetler */Complaints*
- Düzeltici/önleyici faaliyetlerin değerlendirilmesi, */Evaluation of corrective/preventive actions,*
- İç denetimlerin planlanması ve sonucun değerlendirilmesi. */Planning internal audits and evaluating the results.*

Çok sahalı kuruluşlarda, tespit edilen uygunsuzluklar için gerçekleştirilen takip denetimlerinde, merkez büro veya sahaların en azından birinde, ilgili yönetim sisteminde ve/veya uygulamasında devam eden uygunsuzluklar tespit edilmesi durumunda, belgelendirme yapılmaz veya mevcut belgelendirme iptal edilir.

/In multi-site organizations, if ongoing non-conformities are detected in the relevant management system and/or application in at least one of the head office or fields during the follow-up audits carried out for detected non-conformities, certification will not be made or the existing certification will be cancelled.

2.3. Denetim Metodolojisi */Audit Methodology*

BGYS denetimlerinde; Denetim Raporu kullanılarak, sistemin ISO/IEC 27001 standardı gereklerine uygun olarak kurulmuş, dokümante edilmiş ve etkin olarak uygulanmakta olduğu incelenir.

/In ISMS audits; Using the Audit Report, it is examined whether the system is established, documented and effectively implemented in accordance with the requirements of the ISO/IEC 27001 standard.

Denetim ekibi üyeleri tarafından, denetim süresince yapılan inceleme ve gözlemlere ilişkin pozitif ve negatif bulgu ve gözlemler, FRB-27-1 / 2 Denetim Raporuna kaydedilir.

/Positive and negative findings and observations regarding the examinations and observations made by the audit team members during the audit are recorded in the FRB-27-1 / 2 Audit Report.

2.4. Belgelendirme Denetimi Raporu */Certification Audit Report*

AVACERT;

a) Denetim ekibi müşteri kuruluştan ayrılmadan önce, aşağıda belirtilenleri görüşmek üzere, müşteri kuruluşun yönetimi ile denetim ekibi arasında bir toplantının yapılmasını, */Before the audit team leaves the client organization, a meeting is held between the management of the client organization and the audit team to discuss the following,*

1) Belirli belgelendirme şartlarına göre müşteri kuruluşunun BGYS' nin uygunluğuna ilişkin yazılı ya da sözlü bir beyan, */A written or verbal statement regarding the conformity of the customer organizations ISMS according to certain certification conditions*

2) Bulgular ile bunların gerekçesi hakkında sorular sormak üzere müşteri kuruluş için bir fırsat; */An opportunity for the client organization to ask questions about the findings and their rationale*

b) Denetim ekibi tarafından, müşteri kuruluşunun BGYS'nin belgelendirme şartlarının tamamına uygunluğu hususunda elde ettiği bulgularına ilişkin bir denetim raporunun AVACERT' e sunulmasını / Submission of an audit report to AVACERT by the audit team regarding the findings of the customer organization regarding compliance with all ISMS certification requirements.

sağlar. */provides.*

Denetim raporu aşağıdaki bilgileri içermektedir: */ The audit report includes the following information:*

a) Doküman incelemesinin bir özeti, */A summary of the document review*

b) Müşteri kuruluşun bilgi güvenliği risk analizini, */Information security risk analysis of the customer organization,*

c) Doküman incelemesi, risk analizi değerlendirmesi, yerinde denetim ve denetim raporlamasında harcanan sürenin detayı ve kullanılan toplam denetim süresi, */Details of the time spent on document review, risk analysis evaluation, on-site audit and audit reporting and the total audit time used,*

d) Yapılan seçimin gerekçesi, takip edilen denetim sorguları ve kullanılan metodoloji. */Justification for the selection made, audit queries followed and methodology used.*

Denetim raporu, ayrıca aşağıdakileri içerebilir: */The audit report may also include:*

a) Kullanılan denetim metodolojileri ve takip edilen önemli denetim yöntemleri dahil olmak üzere denetimde kapsanan alanlar (Ör. Belgelendirme şartları ve denetlenen sahalar); */Areas covered in the audit, including audit methodologies used and significant audit methods followed (e.g. certification requirements and sites audited);*

b) Yapılan olumlu gözlemler (ör: dikkate değer özellikler) ve olumsuz gözlemler (potansiyel uygunsuzluklar) */Positive observations made (e.g. notable features) and negative observations (potential nonconformities)*

c) Objektif kanıtlarla desteklenmiş ve ilgili BGYS standardı ISO/IEC 27001:2022'i ya da belgelendirme için gerekli başka bir dokümanı referans göstererek belirlenen uygunsuzlukların detayları */Details of the nonconformities identified, supported by objective evidence and referring to the relevant ISMS standard ISO/IEC 27001:2022 or another document required for certification.*

d) Uygulanabildiği durumda müşteri kuruluşunun önceki belgelendirme denetimlerinin sonuçları ile faydalı bir karşılaştırma, Uygulanabilirlik Beyanının referansı, uygunsuzluğun açık bir beyanına ilişkin belgelendirme şartlarına müşteri kuruluşunun BGYS' nin uygunluğuna ilişkin yorumlar. */Where applicable, a useful comparison with the results of the client organization's previous certification audits, reference to the Declaration of Applicability, comments on the compliance of the client organization's ISMS with the certification requirements, a clear statement of non-conformity.*

Denetim Raporu, şunları da kapsayabilir: */The Audit Report may also include:*

a) Takip edilen önemli denetim logları ve kullanılan denetim metodolojileri (bk. Madde BG 9.1.5) de dâhil olmak üzere denetim tarafından kapsanan alanlar (örneğin, belgelendirme şartları ve tetkik edilen yerleşkeler), */Areas covered by the audit (for example, certification conditions and campuses audited), including significant audit logs followed and audit methodologies used (see Article BG 9.1.5),*

b) Hem olumlu (örneğin, kayda değer özellikler), hem de olumsuz (örneğin, potansiyel uygunsuzluklar) olarak yapılan gözlemler, */Observations made both positive (e.g. noteworthy features) and negative (e.g. potential nonconformities),*

c) Objektif delil ve ISO/IEC 27001'in veya belgelendirme için gereken diğer dokümanların şartları ile olan uygunsuzluklara yapılan bir atıf ile desteklenen, tespit edilen tüm uygunsuzlukların detayları, */Details of all detected*

non-conformities, supported by objective evidence and a reference to non-conformities with the requirements of ISO/IEC 27001 or other documents required for certification;

d) Müşteri kuruluşun BGYS'nin, uygunsuzluğun açık bir beyanını içeren belgelendirme şartları ile uygunluğuna ilişkin yorumlar, Uygulanabilirlik Beyanının sürümüne bir atıf ve uygulanabildiği durumda müşteri kuruluşun önceki belgelendirme denetimlerinin sonuçları ile herhangi bir faydalı karşılaştırma. */Comments on the compliance of the client organization's ISMS with the certification requirements, including a clear statement of non-conformity, a reference to the version of the Declaration of Applicability and, where applicable, any useful comparison with the results of the client organization's previous certification audits.*

Doldurulmuş anketler, kontrol listeleri, gözlemler, loglar veya denetçi notları, denetim raporunun bütünleyici bir parçasını oluşturabilir. Bu yöntemler kullanılırsa, bu dokümanlar, belgelendirme kararını desteklemek üzere belgelendirme kuruluşuna delil olarak verilmektedir. Denetim sırasında değerlendirilmiş örnekler hakkında bilgiler, denetim raporuna veya diğer belgelendirme dokümantasyonuna dâhil edilmektedir.

/Completed questionnaires, checklists, observations, logs or auditor's notes may form an integral part of the audit report. If these methods are used, these documents are given as evidence to the certification body to support the certification decision. Information about samples evaluated during the audit is included in the audit report or other certification documentation.

Rapor, müşteri kuruluşun dahili prosedürlerinin ve müşteri kuruluş tarafından BGYS'ye güven sağlamak için uyum sağlanan prosedürlerin yeterliliğini dikkate almaktadır.

/ The report takes into account the adequacy of the client organization's internal procedures and the procedures adopted by the client organization to ensure confidence in the ISMS.

Denetim Raporu, aşağıdakileri kapsamalıdır: */The Audit Report should cover the following:*

- BGYS iç denetimleri ve yönetimin gözden geçirmelerine olan güvenin derecesi, */Degree of confidence in ISMS internal audits and management reviews*
- BGYS' nin etkinliğine ve uygulanmasına ilişkin en önemli olumlu ve olumsuz gözlemlerin bir özeti, */A summary of the most important positive and negative observations regarding the effectiveness and implementation of the ISMS,*
- Müşteri kuruluşun BGYS'nin, belgelendirilip belgelendirilmemesine dair denetim ekibinin tavsiyesi ve bu tavsiyenin desteklenmesi için bilgiler. */The recommendation of the audit team on whether the customer organization's ISMS should be certified or not, and information to support this recommendation.*

2.5. İlk Belgelendirme Denetimi */First Certification Audit*

2.5.1. Aşama 1 Denetimi */Stage 1 Audit*

Aşama 1 denetimleri müşterinin yerinde yapılır.

/Stage 1 inspections are performed at the customer's site.

Aşama 1 denetiminde AVACERT denetim ekibi, sistemle ilgili dokümantasyonu ISO/IEC 27001 standardında istenen dokümantasyonu da kapsayacak şekilde inceler.

/In the Stage 1 audit, the AVACERT audit team examines the system-related documentation, including the documentation required in the ISO/IEC 27001 standard.

Aşama 1 denetimin amacı, müşteri kuruluşun BGYS' ni düzenlemesi ve amaçları doğrultusunda anlayarak, müşteri kuruluşun Aşama 2 denetimine hazır olma derecesine bir bakış açısı sağlamaktır.

/The purpose of the Stage 1 audit is to provide a perspective on the customer organization's readiness for the Stage 2 audit by understanding the customer organization's ISMS in line with its regulation and purposes.

Aşama 1 denetiminin sonuçları yazılı bir raporla dokümante edilir. AVACERT, Aşama 2'ye devam etmeye karar vermeden önce Aşama 1 denetim raporunu gözden geçirir ve aşama 2 denetim ekibi üyelerinin gerekli yeterliliğe sahip olup olmadığını teyit etmektedir. Bu, Aşama 1 denetimini gerçekleştiren Baş denetçi tarafından yapılır.

/The results of the Stage 1 audit are documented in a written report. AVACERT reviews the Phase 1 audit report and confirms whether the phase 2 audit team members have the necessary competence before deciding to proceed with Phase 2. This is done by the Lead auditor who performs the Stage 1 audit.

Baş Denetçi, yazmış olduğu rapordaki uygunsuzluk ve/veya gözlemi iki nüsha şeklinde çıktı alır. Mutabakata varılan uygunsuzluk ve/veya gözlemlerden sonra formu, önce baş denetçi daha sonrasında firma yetkilisi imzalar.

/The Chief Auditor prints out the nonconformity and/or observation in the report he wrote in two copies. After the agreed nonconformities and/or observations, the form is signed first by the chief auditor and then by the company official.

Firma uygunsuzlukların kök sebebini ve tekrarını engelleyecek şekilde düzeltici faaliyet planlamalıdır.

/The company must plan corrective action to identify the root cause of nonconformities and prevent their recurrence.

Düzeltici faaliyetler gerçekleştirilip ve gerçekleştiğine dair objektif deliller baş denetçiye FRB-27-EK-C Düzeltici Faaliyet Formu ile birlikte hard copy veya e-posta ile iletilmelidir.

/Objective evidence that corrective actions have been carried out should be submitted to the chief auditor by hard copy or e-mail together with the FRB-27-EK-C Corrective Action Form.

Baş denetçi tarafından uygunsuzlukların giderildiğinin kabulü sonrasında rapor ve ekleri AVACERT ofise gönderilir. Rapor Belgelendirme Müdürü veya Yönetim Temsilcisi tarafından gözden geçirilir durum kayıt altına alınır.

/After the chief auditor accepts that the non-conformities have been resolved, the report and its annexes are sent to the AVACERT office. The report is reviewed by the Certification Manager or Management Representative and the situation is recorded.

Aşama 2 denetimi öncesinde aşama 1 denetim raporunun ve aşama 1 denetiminin uygunluğunun incelenmesi ve aşama 2 denetimine geçiş onayının verilmesi; o dosya için görevlendirilen baş denetçi/denetçi dışında bir baş denetçiden onay alınmaktadır.

/Before the stage 2 audit, examining the suitability of the stage 1 audit report and the stage 1 audit and granting approval for the transition to the stage 2 audit; Approval is obtained from a lead auditor other than the lead auditor/auditor assigned for that file.

2.5.2. Aşama 2 Denetimi */Stage 2 Audit*

Aşama 1 ve aşama 2 denetimleri arasındaki aralığın makul bir şekilde 6 aydan uzun olmaması bekleniyor. Daha uzun bir aralık gerekirse aşama 1 denetimi tekrarlanmalıdır. Aşama 2 denetimin Aşama 2 denetimi her zaman müşterinin yerinde gerçekleştirilir.

/The interval between stage 1 and stage 2 inspections is reasonably expected to be no longer than 6 months. If a longer interval is required, the stage 1 inspection should be repeated. Stage 2 inspection Stage 2 inspection always takes place at the customer's location.

Amaçları şunlardır: */Their purposes are:*

a) Müşterinin kendi düzenlemeleri, amaçları ve prosedürlerine bağlandığını teyit etmek. */Confirming that the client adheres to its regulations, objectives and procedures.*

b) BGYS' nin, ISO/IEC 27001'ün bütün gerekliliklerine uygun olduğunu ve müşterinin kural hedeflerine uyum sağladığını teyit etmek. */To confirm that the ISMS complies with all requirements of ISO/IEC 27001 and complies with the customer's rule objectives.*

Bütün bunları yapmak için denetim müşteri kuruluşun aşağıdaki noktalarına odaklanır: */To do all this, the audit focuses on the following aspects of the client organization:*

a) Bilgi güvenliğiyle ilgili risklerin değerlendirilmesi ve bu değerlendirmelerin kıyaslanabilir ve üretken sonuçlar üretmesi, */Assessing risks related to information security and ensuring that these assessments produce comparable and productive results,*

b) ISO/IEC 27001 standardında istenen dokümantasyon gereklilikleri, */Documentation requirements required in the ISO/IEC 27001 standard,*

c) Risk değerlendirme ve risk yaklaşımı proseslerine göre kontrol hedeflerinin ve kontrol noktalarının seçilmesi, */Selecting control targets and control points according to risk assessment and risk approach processes,*

d) BGYS' nin etkinliğinin gözden geçirilmesi ve bilgi güvenliği kontrollerinin, raporlamasının ve yeniden gözden geçirmesinin BGYS hedefleri karşısında etkinliğinin ölçülmesi dair, */Reviewing the effectiveness of the ISMS and measuring the effectiveness of information security controls, reporting and review against ISMS objectives,*

e) BGYS iç denetimleri ve yönetim gözden geçirmeleri, */ISMS internal audits and management reviews,*

f) Bilgi güvenliği politikasıyla ilgili yönetimin sorumluluğu */Management's responsibility regarding the information security policy*

g) Seçilen ve ifade edilen kontroller, uygulanabilirlik beyannamesi ve risk değerlendirmesi risk yaklaşımı ve BGYS kuralları ve hedefleri arasındaki bağlantı, */The connection between the selected and expressed controls, the declaration of applicability and the risk assessment risk approach and ISMS rules and objectives,*

h) Kontrollerin ifade edilmesi (ISO/IEC 27006:2015 Annex D), müşteri kuruluşun kontrol etkinliğini ölçüm şekli de gözetilerek, kontrollerin belirlenen hedefleri başarmakta etkin olup olmadığını belirtmek, */Expressing the controls (ISO/IEC 27006:2015 Annex D), indicating whether the controls are effective in achieving the determined objectives, taking into account the way the customer organization measures control effectiveness,*

i) Prosesler, programlar, prosedürler, kayıtlar, iç denetimler ve BGYS etkinliği gözden geçirmesi gibi enstrümanları kullanarak bunların yönetim kararları ve BGYS kuralları ve hedefleri için etkin olması. */Using instruments such as processes, programs, procedures, records, internal audits and ISMS effectiveness review to ensure that they are effective for management decisions and ISMS rules and objectives.*

2.5.3. İlk Belgelendirme İçin Bilgi */Information For Initial Certification*

AVACERT, belgelendirme kararına ilişkin bir esas sağlamak amacıyla denetim ekibinden, bu karara varmak için yeterli bilgiyi sağlayan açık anlaşılır raporları talep etmektedir.

/In order to provide a basis for the certification decision, AVACERT requests clear reports from the audit team that provide sufficient information to reach this decision.

2.6. Gözetim Denetimleri */Surveillance Inspections*

Gözetim denetimlerinin amacı, onaylanmış BGYS'nin uygulanmaya devam ettiğini onaylamak, müşteri kuruluşun operasyonlarının değişmesi nedeniyle başlayan değişimlerin sonuçlarını değerlendirmek ve belgelendirme gerekliliklerine sürekli uyumun devam ettiğini görmektir. Gözetim denetimleri normalde şunları kapsamaktadır:

/The purpose of surveillance audits is to confirm that the approved ISMS continues to be implemented, to evaluate the results of changes initiated due to changes in the operations of the customer organization, and to ensure continued compliance with certification requirements. Surveillance audits normally include:

a) BGYS iç denetçisi, yönetim gözden geçirmesi ve önleyici-düzeltici faaliyet gibi sistem koruma unsurları */System protection elements such as ISMS internal auditor, management review and preventive-corrective action*

b) BGYS standardı ISO/IEC 27001'ün istediği şekilde dış taraflarla etkileşimler ve belgelendirme için gerekli diğer dokümanlar */Other documents required for interactions and certification with external parties as required by the ISMS standard ISO/IEC 27001*

c) Dokümante edilmiş sistemdeki değişiklikler */Changes in the documented system*

d) Değişime konu olan alanlar */Areas subject to change*

e) ISO/IEC 27001'ün seçilmiş unsurları */Selected elements of ISO/IEC 27001*

f) Uygun şekilde seçilen diğer alanlar */Other suitably selected areas*

AVACERT tarafından yapılan gözetimde en az aşağıdakileri gözden geçirilmektedir: */Under the supervision carried out by AVACERT, at least the following are reviewed:*

a) Müşteri kuruluşun bilgi güvenliği politikalarının hedeflerine ulaşabilmesi hususunda kullanılan BGYS'nin etkinliği, */ The effectiveness of the ISMS used in achieving the objectives of the customer organization's information security policies,*

b) Periyodik değerlendirme için prosedürlerin işleyişleri ve bağlı bilgi güvenliği düzenlemelerine uygunluğunun gözden geçirilmesi, */Reviewing the operation of the procedures for periodic evaluation and their compliance with the relevant information security regulations,*

c) En son denetimde tespit edilen uygunsuzluklar için alınan aksiyonlar. */Actions taken for nonconformities detected in the last audit.*

2.7. Yeniden Belgelendirme */Recertification*

Yeniden belgelendirme denetimlerinde, müşteri kuruluşun BGYS uygulamalarının, ISO/IEC 27006:2015 standardı ile tutarlılığının sürdürülebilir olduğu incelenir.

/During recertification audits, the sustainability of the customer organization's ISMS practices with the ISO/IEC 27006:2015 standard is examined.

2.8. Özel Denetimler */Special Inspections*

Belgelendirilmiş müşteri kuruluş, sisteme ait büyük değişiklikler yaparsa ya da belgelendirmenin temelini etkileyebilen başka değişiklikler meydana gelirse bu durumlardan AVACERT'i haberdar etmesi istenmektedir. Böyle durumlarda, özel denetimler gerçekleştirilir.

/If the certified customer organization makes major changes to the system or other changes that may affect the basis of certification, it is requested to inform AVACERT of these situations. In such cases, special inspections are carried out.

2.9. BGYS Denetiminin Özel Unsurları */Special Elements of ISMS Audit*

AVACERT'in rolü, müşteri kuruluşların, varlıklara yönelik bilgi güvenliği ile ilgili tehditlerin, açıklıkların ve müşteri kuruluş üzerindeki etkilerinin tespit edilmesi, incelenmesi ve değerlendirilmesi için prosedürleri oluştururken ve sürdürürken tutarlı olmasını sağlamaktır. AVACERT:

/AVACERT's role is to ensure that client organizations are consistent in establishing and maintaining procedures for detecting, examining and evaluating information security-related threats, vulnerabilities to assets and their impact on the client organization. AVACERT:

a) Müşteri kuruluşunun, güvenliğe ilişkin tehditlerin analizinin uygun olduğunu ve müşteri kuruluşunun çalışması için yeterli olduğunu göstermesini zorunlu kılmaktadır. */Requires the customer organization to demonstrate that the analysis of security threats is appropriate and sufficient for the customer organization's operation.*

Not- Müşteri kuruluşu, müşteri kuruluşunun bilgi güvenliğine ilişkin risklerin hangisinin önemli olarak tanımlandığına dair kriterlerin belirlenmesinden ve bunu gerçekleştirmek için de prosedürün/prosedürlerin geliştirilmesinden sorumludur.

/Note- The customer organization is responsible for determining the criteria for which risks related to the information security of the customer organization are defined as significant and for developing the procedure(s) to achieve this.

b) Varlıklar, açıklıklar ve bunların uygulanmasının sonuçlarına karşın bilgi güvenliğine ilişkin tehditlerin değerlendirilmesi, incelenmesi ve belirlenmesi için müşteri kuruluşunun prosedürlerinin, müşteri kuruluşunun politikası, amaçları ve hedeflerine uygun olup olmadığını tespit etmektedir. */Determines whether the customer organization's procedures for assessing, examining and identifying threats to information security against assets, vulnerabilities and the consequences of their implementation are in accordance with the customer organization's policy, objectives and goals.*

AVACERT ayrıca, önemli analizde kullanılan prosedürlerin doğru olup olmadığını ve uygun bir şekilde uygulanıp uygulanmadığını belirlemektedir. Müşteri kuruluşa ait varlıklara, açıklığa ya da etkisine ilişkin bilgi güvenliği tehditleri, önemli olarak belirlenirse, BGYS içinde ele alınmaktadır.

/AVACERT also determines whether the procedures used in the significant analysis are correct and have been appropriately implemented. If information security threats related to assets, vulnerability or impact of the customer organization are determined to be significant, they are addressed within the ISMS.

2.10. Belgelendirmeyi Askıya Alma veya Geri Çekme */Suspending or Withrawing Certification*

BGYS gözetim denetimlerinde, aşağıdaki şartların oluşması söz konusu olursa belgelendirmenin askıya alınması yönünde, öneride bulunulacağı ifade edilir:

/It is stated that in ISMS surveillance audits, if the following conditions occur, a recommendation will be made to suspend the certification:

- Gerçekleştirilen denetimler sonucunda majör uygunsuzluklar bulunması, */Finding major nonconformities as a result of the audits carried out,*
- Önceki denetimlerde tespit edilen minör uygunsuzlukların, belirlenmiş sürelerde giderilmemesi, */Minor nonconformities detected in previous audits are not resolved within the specified periods,*
- Yasal şartların yerine getirilmediğinin tespiti, */Determination that legal requirements are not met,*
- Belgelendirme kurallarına uyulmaması. */Failure to comply with certification rules.*

BGYS belgelendirmesi askıya alınmış müşteri kuruluşların takip denetiminde, belirlenen uygunsuzluklar kapatılmış ise belgelendirmenin geçerliliğinin devamı, kapatılmamış ise belgelendirmenin geri çekilmesi yönünde, öneride bulunulacağı ifade edilir.

/It is stated that in the follow-up audit of customer organizations whose ISMS certification has been suspended, if the identified nonconformities are closed, a recommendation will be made to continue the validity of the certification, if not, to withdraw the certification.

3. İLGİLİ DOKÜMANLAR ve REFERANSLAR */Related Documents and Referances*

ISO/IEC 27006:2015

ISO/IEC 27006:2015 AMD.1 2020

ISO/IEC 27001

FRB-27-1/2 Denetim Raporu */FRB-27-1/2 Audit Report*