1. PURPOSE

The purpose of this procedure is to determine the methods and responsibilities in accordance with ISO/IEC 27006 standard for the audits to be performed.

2. DEFINITIONS

Information Security Management System (ISMS): It is a part of whole management system based on creating, actualizing, operating, monitoring, reviewing, maintaining of information security and business risk approach.
Asset: Anything worth for the institution.[ISO/IEC 13335-1: 2004]
Availability: The feature of being accessible and available when requested by an authorized entity.[ISO/IEC 13335-1: 2004]
Confidentiality: The feature of non-availability or non-disclosure of the information for unauthorized persons, entities or processes. [ISO/IEC 13335-1: 2004]
Information Security: The protection of confidentiality, integrity and availability of the information. [ISO/IEC 17799: 2005]
Information Security: A system that identifies a possible information security policy, a guardian's failure, or an unknown situation that may be related to security, service or emergence of network status determined. [ISO/IEC TR 18044: 2004]
Information Security Violation: Undesired or unexpected information security that is likely to jeopardize business operations and threaten information security.[ISO/IEC TR 18044: 2004]
Integrity: The feature of protection of the accuracy and integrity of assets. [ISO/IEC 13335-1: 2004]
Residual Risk: Remaining risk after the processing.[ISO/IEC Guide 73]
Risk Acceptance: Decision of acceptance of a risk.
Risk Analysis: The systematic use of the information on the purpose of determining the sources and estimating risk.[ISO/IEC Guide 73]
Risk Assessment: Whole process which involves risk analysis and risk rating. [ISO/IEC Guide 73]
Risk Rating: The process of comparing the estimated risk with the given risk criteria in order to determine the significance of risk. [ISO/IEC Guide 73]
Risk Management: The coordinated activities used in order to control and guide an institution about risk. [ISO/IEC Guide 73]
Risk Processing: The process of selection and implementation of required measures (controls) to be taken to change the risk. [ISO/IEC Guide 73]
Statement of Applicability (SOA): A documented statement which describes the control objectives and controls of the customer body related to the ISMS (This is based on the results and inferences of the control objectives and controls, risk assessment and risk processing processes, legal and regulatory requirements, agreement liabilities and business requirements for information security of the body).

3. RELATED DOCUMENTS and REFERENCES

ISO/IEC 17021-1:2015
ISO/IEC 27006:2015
BQYSEK.01 Quality Manuel
BQF.44 Stage 1 Audit Report
BQF.45 Audit Report
BQF.102 ISMS Certification Application Control Form
BQF.28 Application Form of Certification

4. RESPONSIBILITIES and APPLICATIONS

4.1. General

The ISMS audits are carried out in accordance with the audit applications specified in the Audit Procedure and pursuant to the principles given below.

4.2. The Conditions of ISMS Audit

Prior to the audit of certification, the customer body is asked in the ISMS Certification Application Control Form whether they have records which contain confidential or sensitive information they do not want the audit team to see.

Thereafter, the audit team of ASCERT decides whether the ISMS is adequately checked or not in the absence of these records. If it is decided that the audit cannot be made in the absence of these records, the customer body is notified that the audit cannot be made without the necessary arrangements for access.

4.2.1. Audit Criteria

The criteria related to the ISMS audit of a customer body; is consisted of the facts specified in ISMS standard ISO/IEC 27001 and the documents which were consisted for the related activities.

4.2.2. The Scope of Certification

The Customer Body determines the Scope of ISMS in the Certification Application Form, the audit team of ASCERT guarantees that the scope and restrictions of ISMS are clearly described in accordance with the context of the body through taking account of the place of body, its assets and technological features.

4.2.3. The Audit of Bodies with Many Fields

In the audit of bodies with many fields, it is observed that the following conditions are fulfilled:

- System certification and system changes,
- Review of the management,
- Complaints,
- Assessment of nonconformity and corrective actions,
- Planning of internal audits and the assessment of the result.

In the bodies with many fields, in case of the fact that on-going nonconformities are detected in the central office or at least one of the fields, management system and / or implementation in the follow-up audits carried out for the nonconformities determined, the certification is not made or the present certification is cancelled.

4.2.4. Audit Methodology

In the ISMS audits; it is examined that the system is set up in accordance with the requirements of ISO/IEC 27001 standard, is documented and is effectively applied through Audit report.

The audit team of ASCERT confirms the following;

- The customer body complies with the requirements specified in the ISO/IEC 27001 within the scope of ISMS,
- The information security risk assessment and attitude against the risk of the customer body complies with the requirements specified in ISO/IEC 27001 and the statements with regard to that are clearly reflected in the ISMS and the Declaration of Applicability,
- The attachment points to the services or actions which are not included within the scope of ISMS are determined within the scope of ISMS subject to the certification and the customer body are included in the information security risk assessment.

4.3. The Audit of First Certification

4.3.1. Stage 1

In Stage 1, the audit team of ASCERT, investigates the documentation related to the system in the standard of ISO/IEC 27001 via Stage 1 audit report in such a way that will also involve the requested certification.

The purpose of Stage 1 is to ensure that ISMS is understood in the context of ISMS policies and objectives, and specifically in the context of customer body readiness for audit and the focusing is done for Stage 2 planning.

The Stage 1 involves the review of document, however, it is not restricted with this. ASCERT, reaches a mutual agreement with the customer body on when and where to conduct the review. In all circumstances, the review of the document is completed before the beginning of the Stage 2.

The results of Stage 1 are documented in the Stage 1 Audit report. Before the ASCERT, decides whether the audit should be continued or not with the Stage 2, it reviews the Stage 1 audit report for Stage 2 team members who have necessary requirements to be selected.

The ASCERT, notifies the customer body of further different types of information and record that may be required for detailed review during Stage 2.

The results of stage 1 shall be documented in a written report. The certification body shall review the stage 1 audit report before deciding on proceeding with stage 2 and shall confirm if the stage 2 audit team members have the necessary competence; this may be done by the auditor leading the team that conducted the stage 1 audit if deemed competent and appropriate.

NOTE Independent review (i.e. by a person from the certification body not involved in the audit) is one measure to mitigate the risks involved when deciding if and with whom to proceed to stage 2. However, other risk mitigation measures can already be in place achieving the same goal.

4.3.2. Stage 2

The Stage 2 is always carried out in the field of the customer. ASCERT, prepares an audit plan for the execution of Stage 2, based upon the findings documented in the audit report of Stage 1.

The purposes of Stage 2 are as follows:

a) Confirmation that the customer body depends on its own policies, objectives and procedures.

The Stage 2 focuses on the following regarding the customer body :

a) The leadership of top management and information security policy and safety objectives of information commitment;
b) Certification requirements which are required in ISO/IEC 27001,
c) Assessment of information security and relevant risks and the consistent, valid and comparable results of the assessments,
d) On the basis of the assessment of information security and the relevant risks, the selection of controls based upon the control purposes and risk operation processes,
e) The review of information security performance, information security objectives and the efficiency of ISMS,
f) The relation of selected and implemented controls, Applicability Declaration and the results of risk assessment and risk operation and ISMS policy and purposes,
g) Through taking consideration of external and inner context in order to determine whether the implementation of controls are effective or not to ensure the specified objectives; the monitoring, measuring and analyzing of information security, processes and controls made by customer body, the determination of the controls whether they are implemented and carried out or effective and the implementation of controls with taking consideration of the efficiency measurements of the controls,
h) The review of programs, processes, procedures, records, internal audits and ISMS efficiency, and ensuring that these are traceable to senior management decisions and to the ISMS policy and objectives.

4.3.3. Information for First Certification

The ASCERT, explicitly requests the Audit Report which provides sufficient information from the audit team to reach this decision in order to ensure a basis regarding the certification decision.

4.4. Surveillance Audits

The purpose of surveillance audits is to confirm that the approved ISMS continues to be implemented, to evaluate the results of inceptive changes due to the change of operations of the customer body and to observe continuous compliance with the certification requirements. The surveillance audits normally include these:

a) The factors for continuation of the system including ISMS internal audit, review of management, non-compliance and corrective actions,
b) The communication with exterior sides required by ISO / IEC 27001 standard and other documents required for certification,
c) Changes on system documented,
d) Areas subject to change,
e) Selected factors of ISO/IEC 27001,
f) Other selected appropriate areas.

In the surveillance audits made by ASCERT, at least the following are considered:
a) The activity of ISMS in order to achieve the objectives of the information security policy of the customer organization,
b) The review of compliance with the operation of procedures and the relevant information security law and regulations for periodic assessment,
c) The transactions related to the nonconformities detected in the previous audit.

In addition to the points required for the surveillance audit in ISO/IEC 17021, the following subjects are also included in the surveillance audits :
a) The ASCERT, harmonizes its own surveillance program on information security subjects related to threats to assets, customer body's publicities and effects, and provides justification for the program.
b) The surveillance program is determined by ASCERT. Agreement is reached with documented customer body on specific visiting dates.
c) The surveillance audits can be associated with audits of other management systems. Reporting clearly specifies aspects regarding each management system.
d) The ASCERT, checks issue relating to appropriate use of certificate**.**

During surveillance audits, in case of a previous complaint and any nonconformity or failure to meet the requirements of the certification, ASCERT, checks the records related to the ISMS and procedures investigated and appropriate corrective actions made by the customer body.

A surveillance report involves in particular information on the elimination of previously identified nonconformities. As a minimum, the reports from surveillance are added on condition a) above.

4.5. Recertification Audits

It is examined that the consistency of ISMS applications of the customer body is sustainable in accordance with ISO / IEC 27001 standard in recertification audits.

4.6. Specific Audits

If the certified customer body makes fundamental changes related to the system or if other changes that may affect the basis of the certification occur, the customer body is required to notify ASCERT of these circumstances. In such circumstances, specific audits are carried out.

4.7. Specific Factors of ISMS Audit

The role of ASCERT is to make procedures in order to for identifying, reviewing and evaluating the effects of threats related to information security oriented assets, explicitness on customer body and it provides maintenance and consistency. ASCERT shall carry out the following:

a) It obliges that the analyses of threats regarding the safety of customer body are required to be appropriate and it requires that the customer body demonstrate that it is enough to operate.

b) It detects whether the procedures belonging to the customer body comply with the policy, objectives and purposes of the customer body for assessment, examination and determination of threats regarding information security despite the presence of assets, vulnerabilities and their consequences relating to implementation.

ASCERT also determines whether the procedures used in significant analyzes are correct and if they are being applied appropriately. In case of the information security threats related to the assets, vulnerability or effect belonging to the customer body are significantly determined, this is handled in ISMS.

4.8. Audit Report

The Audit Report includes the following information or references are shown for reaching information:

a) An assessment of the audit which also includes the summary of the document review,

b) An assessment of information security risk analysis of the customer body,

c) Deviations from audit plan (for instance, more or less wasted time in specific scheduled activities),

d) Scope of ISMS,

e) Relevant assessment related to specific standard according to business sector of Customer Body.

The Audit Report must also include sufficient detail mentioned below in order to facilitate and support the certification decision

a) Significant audit solutions and audit methodologies used,

b) Both observations as positive (eg. Remarkable features) and also negative (eg. potential non-conformities),

c) The remarks which include the definition of the nonconformity or the conformity of the customer body's ISMS with the certification requirements, any useful comparison with the results of previous certification audits of the customer body where a reference to the current version of the Applicability Declaration can be applied.

An integrant part of audit report can be consisted by filled surveys, control lists, observations, logs or auditor notes. If these methods are used, these documents are given as evidence to ASCERT to support the certification decision.

The information on evaluated samples during audit is included in the audit report.

To ensure the adequacy of the internal organization of the customer body and the confidence of the customer body's ISMS, the Audit Report should include the following:

- A summary of the most significant positive and negative observations regarding the efficiency and implementation of ISMS,
- The recommendation of audit team about the issuance or non-issuance of the certification related to the customer body's ISMS and the information to support this recommendation.

4.9. The Suspension and Withdrawal of Certification

In ISMS surveillance audits, in case of the conditions below occur, it is recommended that the certification should be suspended:

- The availability of major nonconformities as a result of audits carried out,
- The presence of the minor nonconformities detected in previous audits during the considered periods,
- Detection of non-fulfillment of legal requirements,
- Failure to comply with the certification rules.

During the follow-up audit of customer bodies that have been suspended from the ISMS certification, if the determined nonconformities have been removed, the validation of the certification should be continued, if these nonconformities have not been removed, it is recommended that the certification should be suspended.

5. REVISION INFORMATION

Rev. Date	Rev. No	Item No	Rev. Descriptions
20.08.2022	02	-	ISO/IEC 27006:2015 transition was made.

Hazırlayan	Onaylayan
Yönetim Temsilcisi	*Genel Müdür*