CERTIFICATION PROCEDURE FOR INFORMATION SECURITY MANAGEMENT SYSTEM

1.PURPOSE

The purpose of this procedure is to determine the method and responsibilities to declare the ISMS certification prepared as per ISO/IEC 27006 standard, and to determine the competence of audits and to plan, realize and document the audits.

2. DEFINITIONS

ISMS: Information Security Management System

Information Security Management System: Part of all management system based on establishing, realizing, operating, tracing, reviewing, performing the information security and on the work risk approach.

Declaration of Applicability: Declaration documented to explain the applicable control purposes and controls related to the ISMS of the body.

3. RELATED DOCUMENTS AND REFERENCES

ISO/IEC 17021
ISO/IEC 27006
ISO/IEC 27001
BQYSEK.01 Quality Manual

4. PRINCIPLES

The provisions in clause 4 of the ISO/IEC 17021 standard are valid.

5. GENERAL REQUIREMENTS

5.1. Legal and contractual matters

ISO/IEC 17021 standard and provisions of Article 5.1 of Quality Manual are valid.

5.2. Management of impartiality

ISO/IEC 17021 standard and provisions of Article 5.2 of Quality Manual are valid. Furthermore, the special conditions of ISMS and guide below are applied.

5.2.1. IS 5.2 Conflicts of interest

ASCERT may perform the duties below in a way that it is not defined as consultancy and without causing any conflict of interest:

a) Organizing trainings or participating as trainer provided that it is open to general participation and general information is given, in case of the fact that training is related to information security management, relative management systems or audits (for example, provided that special advices conflicting with the provisions of section b below are not given),

b) Allowing to access the conditions of certification audit standard and information explaining the comment of ASCERT, and publishing them,

c) Activities performed before the audit in order to determine whether it is ready for certification audit or not (such activities cannot be resulted in advices conflicting with this paragraph, and ASCERT guarantees that such activities do not conflict with these requirements and are not used to cause a decrease on certification audit time),

d) Performing second and third party audits as per the standards or regulations out of the scope of accreditation,

e) Providing added value during the certification audits and surveillances (for example, determining opportunities for improvement incurred during the audit without offering special solutions).

ASCERT is independent from the organization(s) performing the internal audit of ISMS for the bodies subject to certifications (including any person), and does not provide such services.

5.3. Liability and Financing

ISO/IEC 17021 standard and provisions of Article 5.3 of Quality Manual are valid.

6. STRUCTURAL REQUIREMENTS

6.1. Organization Structure and Top Management

ISO/IEC 17021 standard and provisions of Article 6.1 of Quality Manual are valid.

6.2. Operational Control

ISO/IEC 17021 standard and provisions of Article 6.2 of Quality Manual are valid.

7. RESOURCE REQUIREMENTS

7.1. Competence of Personnel

ISO/IEC 17021 standard and provisions of Article 7.1 of Quality Manual and provisions in Management Procedure for Certification Personnel are valid.

ASCERT has determined and documented basic competences to perform ISMS certification, and the criteria to select and manage the competent personnel complying with the activities to be audited and the relative information security aspects according to the Management Procedure for Certification Personnel.

Additionally, the personnel competence conditions are indicated in Competency Charts of certification personnel.

7.1.1. IS 7.1.1 General considerations

7.1.1.1. Generic competence requirements

ASCERT has personnel, which has knowledge about the technological and legal developments related to ISMS of the customer body to be audit, or can reach if required.

ASCERT has determined and documented basic competencies to perform ISMS certification, and the criteria to select and manage the competent personnel complying with the activities to be audited and the relative information security aspects according to the Management Procedure for Certification Personnel and selects personnel accordingly.

7.1.2 IS 7.1.2 Determination of Competence Criteria

7.1.2.1 Competence requirements for ISMS auditing

7.1.2.1.1 General requirements

ASCERT has competent personnel or can reach, if required, to provide the followings:

a) Knowledge of information security

b) Technical details of activity to be audited

c) Information about management systems

d) Information about audit principles
e) Information about tracing, measuring, analyzing and evaluation.

Audit team has permit of tracing usage areas of information security events of customer.
The audit team is charged in a way that it has work experience related to the articles above and practices of these articles (It doesn't mean that an auditor has experience related to all fields in information security, but the audit teams need adequate recognition and experience as a whole).

When the Competent Personnel is being created, taking into account the requirements in the Competency Charts is formed. If the auditor's interview is completed and succeeded, the assignments are made if the field performances of the auditors are appropriate

7.1.2.1.2. Information Security Management Terminology, Principles, Practices and Techniques

ASCERT, established the following competency criteria for the training of audit teams and is specified in the Competency Charts:
a) ISMS-specific certification, hierarchy and relationships.
b) Tools, methods, techniques and practices related to information security management.
c) Information security risk assessment and risk management.
d) Applicable procedures for ISMS.
e) Current technology or a problem that may be related to information security.
These criteria are provided through trainings, personal records provided by the individual and auditor proficiency interview.

7.1.2.1.3. Information Security Management System Standards and Normative Documents

Auditors participating in the ISMS audit;
a) All requirements of ISO / IEC 27001
All members of the audit team shall have information about the following:
b) All controls contained in ISO / IEC 27002 (if required also according to sectoral standards) and their implementations are categorized:
1) Information security policies;
2) Organization of information security;
3) Human resources security;
4) Asset management;
5) Access control, including authorization;
6) Cryptography;
7) Physical and environmental safety;
8) Operational security including IT services;
9) Communication security including network security management and information transfer;
10) System acquisition, development and maintenance;
11) Supplier relationships, including outsourced services;
12) Information security event management;
13) Information security aspects of business continuity management, including dismissal;

14) Compatibility, including information security reviews

7.1.2.1.4. Business Management Practices

Auditors in the ISMS audit shall have the following information:

a) Industry information security best practices and information security procedures;

b) Information security policies and business requirements;

c) General business management concepts, practices and interrelationships between policy, objectives and outcomes;

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

7.1.2.1.5 Client business sector

Auditors in the ISMS audit shall have the following information:

a) Legal and regulatory requirements in the field of specific information security, geography and jurisdiction;

b) Information security risks related to the business sector;

c) General terminology, processes and technologies related to customer terminology;

d) The relevant business sector applications.

Criterion a) can be shared between the audit team.

7.1.2.1.6 Client products, processes and organization

Auditors participating in the ISMS audit shall have knowledge of the following:

a) The development and implementation of ISMS and certification activities, including the type, size, governance, structure, functions and outsourcing of relationships of the organization:

b) Complex operations in a broad perspective;

c) Legal and regulatory requirements applicable to the product or service.

7.1.2.2 Competence requirements for leading the ISMS audit team

In addition to the requirements of 7.1.2.1, the Chief Auditors shall comply with the following requirements, which shall be indicated in guidance and audits under audit:

a) Information and skills to manage certification audit process and audit team

b) Demonstration of effective oral and written communication skills.

7.1.2.3 Competence requirements for conducting the application review

7.1.2.3.1 Information security management system standards and normative documents

It is ensured that the practice reviewer has the knowledge of the following to determine the audit team competency, select the members of the audit team, and determine the audit time:

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

7.1.2.3.2 Client business sector

It is ensured that the practice reviewer has the knowledge of the following to determine the audit team competency, select the members of the audit team, and determine the audit time:

a) General terminology, processes, technologies and risks related to customer terminology.

7.1.2.3.3 Client products, processes and organization

It is ensured that the practice reviewer has the knowledge of the following to determine the audit team competency, select the members of the audit team, and determine the audit time:

a) Including customer products, processes, organizational types, dimensions, governance, structure, functions and relationships, outsourcing functions for the development and implementation of ISMS and certification activities.

7.1.2.4 Competence requirements for reviewing audit reports and making certification decisions

7.1.2.4.1 General

Personnel who review audit reports and make certification decisions should have the knowledge to verify the appropriateness of the scope of certification and its changes in scope and the effects on the audit activity, in particular the continuing validity of the identification of interfaces and dependencies.

In addition, personnel who reviews audit reports and makes certification decisions should know that::

a) Management systems in general;

b) Audit processes and procedures

c) Auditing principles, practices and techniques.

7.1.2.4.2. Information Security Management Terminology, Principles, Practices and Techniques

Personnel who reviews audit reports and makes certification decisions is ensured to have the following information:

a) The articles listed in 7.1.2.1.2 a), c) and d);

b) Legal and regulatory requirements related to information security.

7.1.2.4.3. Information Security Management System Standards and Normative Documents

Personnel who reviews audit reports and makes certification decisions is ensured to have the following information:

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

7.1.2.4.4 Client business sector

Personnel who reviews audit reports and makes certification decisions is ensured to have the following information:

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

7.1.2.4.5 Client products, processes and organization

Personnel who reviews audit reports and makes certification decisions is ensured to have the following information:

a) Customer products, processes, types of organization, size, governance, structure, functions and relationships.

7.2 Personnel involved in the certification activities

The provisions of ISO / IEC 17021, Quality Manual Article 7.2 and the Certification Personnel Management Procedure apply. In addition, special conditions and guidelines apply to the following ISMS.

7.2.1 IS 7.2 Demonstration of auditor knowledge and experience

ASCERT indicates that the auditors have the following knowledge and experience:
a) ISMS-specific characteristics;
b) Enroll as an auditor if possible;
c) Participation in ISMS training courses and obtaining relevant personal identification information;
d) Current professional development records;
e) ISMS audits that another ISMS auditor has witnessed.

7.2.1.1 Selecting auditors

In addition to 7.1.2.1, it is ensured that the Auditor selection criteria guarantee that each Auditor shall provide the following:
a) Professional education or training for an equivalent university education;
b) Full-time at least four years work experience in information technology; for at least two years there must be a role or function related to information security;
c) Successful completion of at least five days of training covering the scope ISMS audits and audit management;
d) Before working as an auditor performing ISMS audits, he/she should gain experience in ISMS auditing. This experience will be gained by performing as an auditor in training, monitored by an ISMS evaluator (see ISO/IEC 17021-1:2015, 9.2.2.1.4) in at least one ISMS initial certification audit (stage 1 and stage 2). or re-certification and at least one surveillance audit. This experience will be gained in at least 10 ISMS on-site audit days and will be carried out in the last 5 years. Participation will include documentation review and risk assessment, implementation assessment and audit reporting.
e) Having relevant and up-to-date experience;
f) Keeping current knowledge and skills up to date with continuous professional development.
g) Must have the competence to audit an ISMS in accordance with ISO/IEC 27001.
Technical Experts must comply with the criteria a), b) and e).

7.2.1.2 Selecting auditors for leading the team

In addition to 7.1.2.2 and 7.2.1.1, it is ensured that the Chief Auditor shall provide the following:
a) Active participation in all stages of at least 3 ISMS audits. Participation should include initial scoping and planning, review of certification and risk assessment, practice evaluation and formal audit reporting.

7.3 Use of individual external auditors and external technical experts

The provisions of ISO / IEC 17021, clause 7.3 of Quality Manual and the Certification Personnel Management Procedure apply.

7.3.1 IS 7.3 Using external auditors or external technical experts as part of the audit team

When ASCERT uses external auditors and external technical experts as part of the audit team, they ensure the followings with the contracts they have made and the up-to-date notifications they receive;

- These persons are competent and consistent with the applicable provisions of the ISO / IEC 27006 standard,
- They are not involved in the design, implementation or maintenance of an ISMS or related management systems, either directly or through employers, in violation of impartiality,

7.4. Personnel Records

The provisions of ISO / IEC 17021 and clause 7.4 of Quality Manual and Certification Procedures for Certification Personnel apply.

7.5 Outsourcing

The provisions of ISO / IEC 170215 and clause 7.5 of Quality Manual apply.

8. INFORMATION REQUIREMENTS

8.1. Public Information

The provisions of ISO / IEC 17021 and clause 8.1 of Quality Manual apply.

8.2. Certification Documents

The provisions of ISO / IEC 17021 and clause 8.2 of Quality Manual apply.

8.2.1. IS 8.2 ISMS Certification Documents

ASCERT, provides a certificate signed by the Certification Manager for each of the customer bodies certified by ISMS.

The amendment to the Applicability Statement that does not change the scope of the controls under the certificate does not require the certificate to be updated.

The certification documents may reference national and international standards as source(s) of control set for controls that are determined as necessary in the organization's Statement of Applicability in accordance with ISO/IEC 27001:2013, 6.1.3 d). The reference on the certification documents shall be clearly stated as being only a control set source for controls applied in the Statement of Applicability and not a certification thereof.

8.3. Reference to certification and use of marks

The provisions of ISO/IEC 17021, Quality Manual Article 8.3 and the Certificate and Logo Usage Instructions apply. In addition, special conditions and guidelines apply to the following ISMS.

8.4. Confidentiality

The provisions of ISO / IEC 17021 standard and clause 8.4 of Quality Manual apply. In addition, special conditions and guidelines apply to the following ISMS

8.4.1. IS 8.4 Access to organizational records

ASCERT requires that the customer body notify the audit team whether or not there is any record of the ISMS that cannot be presented for review because it contains confidential or sensitive information, prior to the certification audit.

ASCERT decides whether or not ISMS can be properly audited if these records are incomplete. If ASCERT decides that it is not possible to conduct an appropriate audit of the ISMS without reviewing any confidential or sensitive records found, it will inform the customer body that certification audits will not be performed until appropriate access arrangements are established.

8.5. Information Exchange between ASCERT and Its Clients

The provisions of ISO / IEC 17021 and clause 8.5 of Quality Manual apply.

9. PROCESS REQUIREMENTS

9.1. Pre-Certification Activities

9.1.1. Application

Customer bodies applying for ISMS certification are required to submit their applications through the Certification Application Form.

Before evaluation and review of the contract by the Planning Officer, for the following particulars, ISMS Certification Application Control Form is sent to customer bodies applying for ISMS certification and required to be returned to ASCERT by filling in the relevant fields;

1. To evaluate the competencies for the assessed needs,
2. To be informed about the appropriateness of the field proficiency analysis in operation and
3. To obtain Information on the verification of the exclusions specified

9.1.2. Application review

For customer body's applying for certification, a qualification analysis is carried out before the contract is reviewed and the ISMS Certification Application Control Form is signed by the authorized personnel, who is responsible to carry out this analysis.

After the completion of the reviewing of the contract, the offer to be given in line with the Certification Procedure shall be prepared and sent to the customer body.

A contract is signed in accordance with the Certification Procedure with the customer body accepting the offer.

9.1.3. Audit program

ISO/IEC 17021 standard and provisions of article 9.1.3 of Quality Manual are valid. In addition, following ISMS specific conditions and guidelines are applied.

9.1.3.1. IS 9.1.3 General

The Audit Program for ISMS audits is designed to take into account the determined information security controls.

9.1.3.2. IS 9.1.3 Audit Methodology

ASCERT has created and implemented the ISMS Audit Procedure for an audit application that demonstrates the customer body is planning ISMS internal audits and the programs and procedures are being implemented and can be implemented.

9.1.3.3. IS 9.1.3 General Preparations for Initial Audit

ASCERT, demands from a customer body to make all necessary arrangements to access internal audit reports and independent audit reports on information security.

At least during Stage 1 of the initial certification audit, the customer body is requested to provide the following information:

a) General information on ISMS and the activities it covers;

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

9.1.3.4. IS 9.1.3 Review periods

ASCERT, does not make ISMS certification unless there is at least one administrative audit and an internal audit covering the scope of certification.

9.1.3.5. IS 9.1.3 Scope of Certification

The audit team audits the ISMS of the customer body in the defined scope for the purposes of verifying that all requirements have been fulfilled. ASCERT, confirms that the customer fulfills the requirements of article 4.3 of ISO/IEC 27001 within the scope of the ISMS of the customer body.

ASCERT, confirms that the customer establishment has correctly performed the information security risk assessment processes within the boundaries of the activities defined in the certification. ASCERT, confirms that this is reflected within the scope of ISMS and the Applicability Declaration of the customer body. ASCERT, verifies that there is at least one Applicability Declaration per certification scope.

ASCERT, ensures that interfaces to services or activities not covered by the ISMS are dealt with within the ISMS scope, which is subjected to certification, and that the customer body is involved in information security risk assessment. An example of such a situation is that it involves deficiencies in sharing with other bodies (e.g. IT systems, databases and telecommunications systems or outsourcing of a business function).

9.1.3.6. IS 9.1.3 Certification Auditing Criteria

For the criteria for auditing ISMS of a customer body, ISMS standard ISO / IEC 27001 is taken as a reference.

9.1.4. Determining audit time

ISO/IEC 17021 standard and provisions of article 9.1.4 of Quality Manual are valid. In addition, following ISMS specific conditions and guidelines are applied.

The total number of persons doing work under the organization’s control for all shifts within the scope of the certification is the starting point for determination of audit time.

a) Determination of the audit period according to the number of people working under the control of the organization is indicated in the Audit timeline in Table 1. However, the factors contributing to the change must be taken into account.

Table1 Audit time chart

Number of persons doing work under the organization's control	ISMS audit time for initial audit (auditor days)	Additive and subtractive factors
1-10	5	See Table2
11-15	6	See Table2
16-25	7	See Table2
26-45	8.5	See Table2
46-65	10	See Table2
66-85	11	See Table2
86-125	12	See Table2
126-175	13	See Table2
176-275	14	See Table2
276-425	15	See Table2
426-625	16,5	See Table2
626-875	17,5	See Table2
876-1175	18,5	See Table2
1176-1550	19,5	See Table2
1551-2025	21	See Table2
2026-2675	22	See Table2
2676-3450	23	See Table2
3451-4350	24	See Table2
4351-5450	25	See Table2
5451-6800	26	See Table2
6801-8500	27	See Table2
8501-10700	28	See Table2
>10.700	Follow progression above	

b) The audit duration can be adjusted according to what was found during the stage 1 audit (for example, different assessment of the complexity of the ISMS scope or additional areas within the scope).

c) Persons working part-time under the control of the organization contribute in proportion to the number of hours worked compared to a person working full-time under the control of the organization.

d) "Audit time" referred to in the table is expressed in terms of "Auditor days" spent on the audit. The basis for the calculation of Table 1 is an 8-hour working day.

e) If BQS develops an audit plan in which remote audit activities represent more than 30% of the planned onsite audit time, BQS will justify the audit plan and obtain specific approval from the accreditation body prior to implementation.

f) Audit timeline is not used alone. For the specified time, the following factors related to the complexity of the ISMS and therefore the effort required to audit the ISMS are also taken into account.

g) It is expected that the calculated time for planning and report writing will not reduce to less than 70% of the total onsite inspection time. Where additional time is required for planning and/or report writing, this cannot be a justification for shortening the onsite inspection time. Auditor travel time is not included in this calculation and is in addition to the audit time specified in the chart.

h) The number of total on-site auditor days – as calculated for the scope– shall be distributed amongst the different sites based on the relevance of the site for the management system and the risks identified. The justification for the distribution shall be recorded by the certification body.
The total time expended on initial audit and surveillance is the total sum of the time spent at each site plus the central office and shall never be less than that which would have been calculated for the size and complexity of the operation if all the work had been undertaken at a single site (i.e. with all the employees of the company in the same site).

Table2 - Classification of factors for calculating audit time

Factors	Impact on effort		
	Reduced effort	Normal effort	Increased effort
a) complexity of the ISMS: • information security requirements [confidentiality, integrity and availability, (CIA)] • number of critical assets • number of processes and services	• Only little sensitive or confidential information, low availability requirements • Few critical assets (in terms of CIA) • Only one key business process with few interfaces and few business units involved	• Higher availability requirements or some sensitive / confidential information • Some critical assets • 2–3 simple business processes with few interfaces and few business units involved	• Higher amount of sensitive or confidential information (e.g. health, personally identifiable information, insurance, banking) or high availability requirements • Many critical assets • More than 2 complex processes with many interfaces and business units involved
b) the type(s) of business performed within scope of the ISMS	• Low risk business without regulatory requirements	• High regulatory requirements	• High risk business with (only) limited regulatory requirements
c) previously demonstrated performance of the ISMS	• Recently certified • Not certified but ISMS fully implemented over several audit and improvement cycles, including documented internal audits, management reviews and effective continual improvement system	• Recent surveillance audit • Not certified but partially implemented ISMS: Some management system tools are available and implemented; some continual improvement processes are in place but partially documented	• No certification and no recent audits • ISMS is new and not fully established (e.g. lack of management system specific control mechanisms, immature continual improvement processes, ad hoc process execution)
d) extent and diversity of technology utilized in the implementation of the various components of the ISMS (e.g. number of different IT platforms, number of segregated networks)	• Highly standardized environment with low diversity (few IT-platforms, servers, operating systems, databases, networks, etc.)	• Standardized but diverse IT platforms, servers, operating systems, databases, networks	• High diversity or complexity of IT (e.g. many different segments of networks, types of servers or databases, number of key applications)
e) extent of outsourcing and third party arrangements used within the scope of the ISMS	• No outsourcing and little dependency on suppliers, or • Well-defined, managed and monitored outsourcing arrangements • Outsourcer has a certified ISMS • Relevant independent assurance reports are available	• Several partly managed outsourcing arrangements	• High dependency on outsourcing or suppliers with large impact on important business activities, or • Unknown amount or extent of outsourcing, or • Several unmanaged outsourcing arrangements
f) extent of information system development	• No in-house system development • Use of standardized software platforms	• Use of standardized software platforms with complex configuration/ parameterization • (Highly) customized software • Some development activities (in-house or outsourced)	• Extensive internal software development activities with several ongoing projects for important business purpose
g) number of sites and number of Disaster Recovery (DR) sites	• Low availability requirements and no or one alternative DR site	• Medium or High availability requirements and no or one alternative DR site	• High availability requirements e.g. 24/7 services • Several alternative DR sites • Several Data Centers
h) for surveillance or re-certification audit: The amount and extent of change relevant to the ISMS in accordance with ISO/IEC 17021-1, 8.5.3	• No changes since last re-certification audit	• Minor changes in scope or SoA of ISMS, e.g. some policies, documents, etc. • Minor changes in the factors above	• Major changes in scope or SoA of ISMS, e.g. new processes, new business units, areas, risk assessment management methodology, policies, documentation, risk treatment • Major changes in the factors above

i) To ensure that effective audits are carried out and to provide reliable and comparable results, the audit time specified in the audit timetable cannot be reduced by more than 30%.

j) The calculated time for planning and report writing should not be less than 70% of the time shown in the audit time sheet.
k) Appropriate reasons for deviation should be identified and documented.
l) For surveillance audits, About 1/3 of the time allocated for certification audit, For re-certification audits; 2/3 of it should be separated.
m) Stage 1 audit should be a maximum of 30% of the total audit time.

Example for audit time calculation
The following example shows how you can use the factors outlined in Table2 to calculate the audit time. In the example below, the calculation of the inspection time is done as follows.

Step 1: Identifying business and organizational factors (other than IT): Determine the appropriate grade for each of the categories given in Table 3 and aggregate the results.

Step 2: Identifying factors related to the IT environment: Determine the appropriate grade for each of the categories given in Table4 and aggregate the results.

Step 3: Based on the results of steps 1 and 2 above, select the appropriate location in Table 5 to determine the impact of factors on the audit duration.

Factors related to business and organization (other than IT)
(Table3)

Category	Grade
Type(s) of business and regulatory requirements	1. Organization works in non-critical business sectors and non-regulated sectors* 2. Organization has customers in critical business sectors* 3. Organization works in critical business sectors*
Process and tasks	1. Standard processes with standard and repetitive tasks; lots of persons doing work under the organization's control carrying out the same tasks; few products or services 2. Standard but non-repetitive processes, with high number of products or services 3. Complex processes, high number of products and services, many business units included in the scope of certification (ISMS covers highly complex processes or relatively high number or unique activities)
Level of establishment of the MS	1. ISMS is already well established and/or other management systems are in place 2. Some elements of other management systems are implemented, others not 3. No other management system implemented at all, the ISMS is new and not established

* Critical business sectors are sectors that may affect critical public services that will cause risk to health, security, economy, image and government ability to function that may have a very large negative impact to the country.

Factors related to IT environment (Table4)	
Category	Grade
IT infrastructure complexity	1. Few or highly standardized IT platforms, servers, operating systems, databases, networks, etc. 2. Several different IT platforms, servers, operating systems, databases, networks 3. Many different IT platforms, servers, operating systems, databases, networks
Dependency on outsourcing and suppliers, including cloud services	1. Little or no dependency on outsourcing or suppliers 2. Some dependency on outsourcing or suppliers, related to some but not all important business activities 3. High dependency on outsourcing or suppliers, large impact on important business activities
Information System development	1. None or a very limited in-house system/application development 2. Some in-house or outsourced system/application development for some important business purposes 3. Extensive in-house or outsourced system/application development for important business purposes

Table5		IT complexity		
		Low (3-4)	Medium (5-6)	High (7-9)
Business complexity	High (7-9)	(+ %5) – (+%20)	(+%10) – (+%50)	(+%20) – (+%100)
	Medium (5-6)	(-%5) – (-%10)	%0	(+%10) – (+%50)
	Low (3-4)	(-%10) – (-%30)	(-%5) – (-%10)	(+%5) – (+%20)

9.1.4.1. IS 9.1.4 Audit Time

ASCERT, is planning to provide sufficient time for the audit team to complete all activities in the initial certification audit, surveillance audit or re-certification audit.

Calculation of the overall audit time also includes sufficient time for audit reporting.

ASCERT, uses ISO / IEC 27006 Annex B and Annex C to determine audit time.

ASCERT, makes justification for the period used in the initial certification audit, surveillance and re-certification audits, or prepares as necessary to ensure this period.

The following factors (ISO / IEC 27006 Annex B.3.4) are taken into consideration for the period of separation:

a) Size of ISMS scope (e.g. number of information systems used, number of employees)
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 Annex A:
c) The types of work carried out under ISMS,
d) The scope and diversity of the technology used to implement the various components of the ISMS (such as applied controls, certification and/or process control, corrective/preventive action, etc.)
e) Number of fields,
f) The ISMS's previously performance,
g) Outsourcing used within ISMS scope and scope of third party regulations,
h) Certification standards and regulations.

9.1.5. Multi-site sampling

Sampling decisions for multiple fields for ISMS certifications are more complex than for the quality management systems. In the cases that the customer body has fields that meet the criteria from a) through to c) below, ASCERT, evaluates the audits in the following manner;

a) All the fields must be operated under the same ISMS, centrally managed, audited and subject to centralized management review,
b) All fields must be included in the ISMS internal audit program of the customer body,
c) All fields must be included in the review program of the ISMS management of the customer body.

Multiple field audits are carried out according to the following guidelines and the following table:

a) In order to determine the level of sufficient sampling at the first review of the contract, the differences between the fields are defined in the most comprehensive way possible.
b) Taking into account the following by ASCERT, representative number of fields are sampled:
    1) The internal audit results of the head office and the fields,
    2) The results of the management review,
    3) Differences in size of field/s
    4) Differences in the scope of the field/s
    5) ISMS's complexity,
    6) The complexity of information systems in different fields,
    7) Differences in working patterns,
    8) Differences in design and operation control
    9) Potential interactions with critical information systems or information systems that process sensitive information,
    10) Changing legal conditions.
    11) Geographical and cultural aspects;
    12) Risk situation of facilities
    13) Information security events in specific facilities
c) An example is selected from among all the fields within the scope of the ISMS of the customer body; this selection is determined randomly based on a decision to reflect the factors mentioned in article b) above.
d) ASCERT, audits all the fields that face major risks within the scope of the ISMS prior to certification.
e) The audit program is designed in the light of the above requirements and covers representative examples of the scope of ISMS certification within three years.
f) When an inconvenience is observed in the head office or a single field, corrective action procedure applies to all campuses covered by head office and certification.

The audit described below addresses the activities of the head office of the customer body to ensure that a single ISMS is fully implemented in the field and to be certain about the centralized management at the operational level.

At least 25% of the sample fields are randomly selected. The remainder is selected from among the fields with a certain degree of quality difference for a given time period.

9.1.6. Multiple Management Systems

The provisions which are included in ISO/IEC 17021 standard and Article 9.1.6 in Quality Manual are valid. In addition, the special conditions and guide are applied to the ISMS below.

9.1.6.1. IS 9.1.6 The Integration of ISMS Documentation with Other Management Systems

The customer establishment may combine the 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 determinable.
The ASCERT may recommend the certification of other management systems in association with the ISMS certification or may only offer the ISMS certification.

9.1.6.2. IS 9.1.6 Combining management system audits

The ISMS audit may be combined with the audits of other management systems. This combination is possible as long as it is demonstrable that the audit complies with the requirements of the ISMS certification. All factors which are significant for an ISMS must be clearly seen in audit reports and must be directly detected. The quality of audit must not be affected from the combination of the audits.

9.2. Planning audits

9.2.1. Determining audit objectives, scope and criteria

The provisions which are included in ISO/IEC 17021 standard and Article 9.1.6 in Quality Manual are valid. In addition, the special conditions and guide are applied to the ISMS below.

9.2.1.1. IS 9.2.1 Audit objectives

The objective of the audit is determined to include the determination of the effectiveness of the management system that the client organization implements applicable controls based on risk assessment and achieves the established information security objectives.

9.2.2. Audit team selection and assignments

The provisions which are included in ISO/IEC 17021 standard and Article 9.2.2 in Quality Manual are valid. In addition, the special conditions and guide are applied to the ISMS below.

9.2.2.1. IS 9.2.2 Audit Team

The audit team must be officially appointed and they must have appropriate employment certificates. The duty shall be clearly defined to the audit team and the customer shall be notified of this.
An audit team may consist of a person providing that the person complies with all the criteria set out in 7.1.2.1

9.2.2.2. IS 9.2.2 Audit team competence

The conditions listed in 7.1.2 are valid. For the surveillance and specific audit activities, the factors related to only planned surveillance activity and specific audit activity are applied.

When selecting and managing the audit team to be appointed for a particular audit, the ASCERT, guarantees that each team member appointed has the competency mentioned below:

a) The team member has appropriate technical knowledge about security risks (Technical Specialists can carry out this function) and specific activities within the scope of the ISMS, as well as the procedures and potential information required for certification;

b) Having a comprehension of the customer establishment which is sufficient to make a safe certification audit that provides the scope and context of the ISMS in order to manage the information security aspect related to its activities, products and services of the ISMS;

c) Providing that the legal and regulatory requirements implemented to the ISMS of the customer establishment are properly understood.

9.2.3. Audit Plan

The provisions which are included in ISO/IEC 17021 standard and Article 9.2.3 in Quality Manual are valid. In addition, the special conditions and guide are applied to the ISMS below.

9.2.3.1. IS 9.2.3 General

The audit plan for ISMS audits is created in order to take the information security controls which are set into consideration.

9.2.3.2. IS 9.2.3 Network Assisted Audit Techniques

If it is required to be applied, the audit plan for network-assisted audit techniques conveniently determines the network-assisted audit techniques to be used during the audit.

The network-assisted audit techniques may involve teleconference, web interview, interactive web-based communication and remote electronic access to ISMS documentation and / or ISMS processes. The aim of such techniques is to increase the efficiency of audit and productivity and to support the integrity of the audit.

The customer establishment is responsible for maintaining and evaluating the compliance with laws and regulations. The ASCERT, investigates the controls and samples to develop trust with regard to that the ISMS operates in this direction. The ASCERT, confirms that it has a management system which will provide compliance with the laws and regulations applicable to the information security risks and effects of the customer establishment.

9.2.3.3. IS 9.2.3 Timing of Audit

The ASCERT confirms timing of audit with the customer establishment to be audited and the audit can be conducted in accordance with the season, month, date and shift.

9.3. Initial certification

For the application of ISMS audits, the ISMS Audit Procedure has been created and applied.

9.3.1. IS 9.3.1 Initial certification audit

The provisions which are included in ISO/IEC 17021 standard and Article 9.2 in Quality Manual are valid. In addition, the special conditions and guide are applied to the ISMS below.

9.3.1.1. IS 9.3.1.1 Stage 1

For the application of ISMS audits, the ISMS Audit Procedure has been created and applied.

9.3.1.2. IS 9.3.1.2 Stage 2

For the application of ISMS audits, the ISMS Audit Procedure has been created and applied.

9.4. Conducting audits

The provisions which are included in ISO/IEC 17021 standard and Article 9.4 in Quality Manual are valid. In addition, the special conditions and guide are applied to the ISMS below.

9.4.1. IS 9.4 General

For the application of ISMS audits, the ISMS Audit Procedure has been created and applied.

9.4.2. IS 9.4 Specific elements of the ISMS audit

For the determination of specific factors of ISMS audits, the ISMS Audit Procedure has been created and applied.

9.4.3. IS 9.4 Audit Report

For the content and use of ISMS certification audit reports, the ISMS Audit Procedure has been created and applied.

9.5. Certification Decision

The ASCERT, requests obvious and clear audit reports, which provide the sufficient information to take decision for the purpose of ensuring the basis for the certification decision, from audit team.

9.5.1. IS 9.5 Certification Decision

The decisions related to issuance / withdrawal of the ISMS certification are taken by the decision maker in accordance with the certification procedure.

The decision maker shall be constituted of person / persons with accumulation of knowledge and experience at a specific level in all areas sufficient for the assessment of the concerned recommendations made by the audit processes and the audit team.

The decision on the ISMS certification and non-certification of a customer establishment is taken by the ASCERT relying on the information collected in the certification process and all other relevant information. The persons who have taken the certification decision are the person / persons who are not involved in the audit. This decision is based on the ASCERT and all other explicit relevant knowledge with the findings and certification recommendation of the audit team according to the certification submitted in the audit report (see also Article IS 9.4.3).

It is essential that the decision maker should normally not refuse a negative recommendation of the audit team. In case of such a circumstance occurs, the ASCERT puts the recommendation regarding refusal down in black and white and gives justification.

No certification is given to the customer establishment unless there is sufficient evidence to demonstrate that the review of management and the arrangements for ISMS internal audits are conducted, they are active and sustainable.

9.6. Maintaining certification

9.6.1. General

The provisions which are included in ISO/IEC 17021 standard and Article 9.6.1 in Quality Manual are valid.

9.6.2. Surveillance Activities

The provisions which are included in ISO/IEC 17021 standard and Article 9.6.2 in Quality Manual are valid.

9.6.2.1. IS 9.6.2. Surveillance Activities

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

The purpose of the surveillance is to confirm that the implementation of the certified ISMS is maintained, to take into consideration the consequences of the changes in the system initiated as a result of the changes in the operation of the customer body and to confirm the compatibility with the certification requirements.

9.6.3. Recertification

The provisions which are included in ISO/IEC 17021 standard and Article 9.4 in Quality Manual are valid.

9.6.3.1 IS 9.6.3 Re-certification audits

For the implementation of ISMS recertification audits, the ISMS Audit Procedure has been established and implemented.

9.6.4. Special Audits

The provisions which are included in ISO/IEC 17021 standard and Article 9.5 in Quality Manual are valid.

9.6.4.1. IS 9.6.4. Special Cases

In case that the customer body which has certified ISMS makes any changes in great measure in its system or makes any other changes that will affect the basis of the certification (such as changes in SOA), the customer body is required to notify the ASCERT of these situations. In these situations, the special audits are carried out.

9.6.5. Suspending, withdrawing or reducing the scope of certification

The provisions which are included in ISO/IEC 17021 standard, Article 9.6 in Quality Manual and The Procedure of Suspension, Withdrawal of Certification are valid.

9.7. Appeals

The provisions which are included in ISO/IEC 17021 standard, Article 9.7 in Quality Manual and The Procedure of Complaint and Objection are valid.

9.8. Complaints

The provisions which are included in ISO/IEC 17021 standard, Article 9.8 in Quality Manual and The Procedure of Complaint and Objection are valid. In addition, the following provisions and guide which are specific to the ISMS are applied.

9.8.1. IS 9.8 Complaints

ASCERT, stipulates in accordance with the conditions of ISO/IEC 27001 that each customer body that the ISMS is certified must have all complaints and records of corrective actions carried out ready to be examined when requested in the certification contract.

9.9. Client Records

The provisions which are included in ISO/IEC 17021 standard, Article 9.9 in Quality Manual and The Procedure of Records Control are valid.

10. MANAGEMENT SYSTEM REQUIREMENTS FOR CERTIFICATION BODIES

The conditions which are included in ISO/IEC 17021 standard and Article 10.3 in Quality Manual are applied. In addition, the following conditions and guide which are specific to the ISMS are applied.

It is carried out in compliance with the following the ASCERT management system procedures prepared in accordance with ISO / IEC 17021:

- Document Control Procedure
- Records Control Procedure
- Procedure of Review of Management
- Internal Audit Procedure
- Procedure of Corrective Action

Annex-A

Technical field classification

Sector	Group of sectors	Relevant Technical Scope	Sub Sector Area	Technological Field
Production sector	**A**	01-Agriculture, fishing 03-Food products, beverages and tobacco 30-Hotels and restaurants	**A-01**	**TA1-TA2-TA3-TA4-TA5-TA6-TA7-TA8-TA9-TA10-TA11**
		02-Mining and quarrying 15-Non-metallic mineral products 16-Concrete, cement, lime, plaster etc.	**A-02**	
		04-Textiles and textile products 05- Leather and leather products 06-Wood and wood products 14-Rubber and plastic products 23-Manufacturing not elsewhere classified	**A-03**	
		07-Pulp, paper and paper products 08-Publishing companies 09-Printing companies	**A-04**	
		10-Manufacture of coke and refined petroleum products 12-Chemicals, chemical products and fibers 13-Pharmaceuticals	**A-05**	
		17-Basic metals and fabricated metal products 18-Machinery and equipment 19-Electrical and optical equipment 20-Shipbuilding 22-Other transport equipment	**A-06**	
		25-Electricity supply 26-Gas supply 27-Water supply	**A-07**	
		24-Recycling	**A-08**	
		28-Construction	**A-09**	
Service industry	**B**	29- Wholesale and retail trade; Repair of motor vehicles, motorcycles and personal and household goods	**B.01**	**TA1-TA2-TA3-TA4-TA5-TA6-TA7-TA8-TA9-TA12**
		31- Transport, storage and communication	**B.02**	
		34-Engineering services	**B.03**	
		35-Other services 39-Other social services	**B.04**	
Special sector	**C**	33-Information technology	**C.01**	**TA1-TA2-TA3-TA4-TA5-TA6-TA7-TA8-TA9-TA13-TA14-TA15-TA16**
		36-Public administration	**C.02**	**TA1-TA2-TA3-TA4-TA5-TA6-TA7-TA8-TA9**
		37-Education	**C.03**	
		32-Financial intermediation; real estate; renting	**C.04**	
		38-Health and social work	**C.05**	
		21-Aerospace	**C.06**	

11. REVISION INFORMATION

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