1. OBJECTIVE

The purpose of this procedure is to define the ISMS documentation prepared in accordance with the ISO/IEC 27006-1:2024 standard, to determine auditor qualifications, and to define the methods and responsibilities for planning, conducting audits, and making certification decisions.

2. DEFINITIONS

ISMS: Information Security Management System

Information Security Management System: A part of the overall management system for establishing, implementing, operating, monitoring, reviewing, maintaining information security, and based on a business risk approach.

Statement of Applicability (SOA): A documented statement describing the applicable control objectives and controls related to the organization's ISMS .

3. RELATED DOCUMENTS

ISO/IEC 17021-1:2015
ISO/IEC 27001:2022
BQYSEK.01 Quality Manual

4. APPLICATION

ISO/IEC 17021-1:2015 standard And the provisions of section 4 of the Quality Manual apply.

5. GENERAL TERMS AND CONDITIONS

5.1. Legal and Contractual Matters

ISO/IEC 17021-1:2015 standard And the provisions of section 5.1 of the Quality Manual apply.

5.2. Managing Neutrality

ISO/IEC 17021-1:2015 standard And the provisions of section 5.2 of the Quality Manual apply.

5.2.2. Conflicts of Interest

ASCERT can add value during certification and surveillance audits (for example, by identifying areas for improvement that become apparent during the audit, without suggesting specific solutions) without being considered a consultancy or creating a potential conflict of interest.

the ISMS of its certified clients . Furthermore, ASCERT ensures that the internal ISMS audit is independent of any organization or entities (including any individuals) performing the audit.

5.3. Liabilities and Financing

ISO/IEC 17021-1:2015 standard and Quality Manual clause 5.3 apply.

6. STRUCTURAL REQUIREMENTS

ISO/IEC 17021-1:2015 standard and Quality Manual clause 6.1 apply.

7. SOURCE REQUIREMENTS

7.1 Staff Competence

7.1.1 General

ISO/IEC 17021-1:2015 standard The provisions of Article 7.1 of the Quality Manual and the Certification Personnel Management Procedure apply.

7.1.2. General Qualification Requirements

ASCERT has defined the qualification requirements for each certification function specified in Table A.1 of ISO/IEC 17021-1:2015 . ASCERT takes into account all requirements related to the ISMS technical areas defined by ASCERT, as specified in ISO/IEC 17021-1 and clauses 7.1.3 and 7.2.2 of ISO/IEC 27006-1:2024. Annex B provides further guidance on qualification.

ASCERT defines the knowledge and skills required for specific functions, in accordance with Annex A.

If additional specific criteria, including qualification requirements, are defined in a particular standard (e.g., ISO/IEC 27006-1), these shall be applied.

7.1.3 Determining the qualification criteria

7.1.3.1 Qualification requirements for ISMS audit

7.1.3.1.1 General requirements

ASCERT has qualified personnel on hand or available as needed to provide the following:

a) Information security;
b) Technical aspects of the activity to be audited;
c) Management systems;
d) Its principles;
Note: More detailed information about audit principles can be found in ISO 19011.
e) ISMS monitoring, measurement, analysis, and evaluation.

Items a) through e) above apply to all auditors on the audit team. However, item b) may be shared among audit team members.

The audit team members, collectively, must possess the skills outlined above and demonstrate these skills through practical experience.

The audit team members should be collectively competent in tracing the signs of information security incidents within the client's ISMS down to the relevant elements of the ISMS .

Auditors are not required to have comprehensive experience in all areas of information security; however, the audit team as a whole should have adequate competence to cover the scope of the ISMS being audited.

7.1.3.1.2 Information security management terminology, principles, practices and techniques

Each auditor on the ISMS audit team should be knowledgeable about the following:
a) Documentation structures, hierarchies, and relationships specific to the ISMS ;
b) Information security risk assessment and risk management;
c) Processes applicable to the ISMS (Information Security Management System).

The audit team members will collectively be informed about the following:
d) Tools, methods, techniques, and their applications related to information security management;
e) Current technology where information security may be important or a problem.

7.1.3.1.3 Information security management system standards and normative documents

must be knowledgeable about all requirements contained in ISO/IEC 27001 and the Quality Manual .

The audit team members, collectively, should be knowledgeable about all the controls listed in Annex A of ISO/IEC 27001:2022 and their implementation.

7.1.3.1.4 Business management practices

Each auditor on the ISMS audit team should be knowledgeable about the following:
a) Industrial information security best practices and information security procedures;
b) Policies and business requirements related to information security;
c) The relationship between the results;
d) Management processes and related terminology.
Note: These processes also include human resources management, internal and external communications, and other related support processes.

7.1.3.1.5 Customer business sector

Each auditor on the ISMS audit team should be knowledgeable about the following:
a) Legal and regulatory requirements in specific information security areas, geographies, and jurisdictions;
Knowledge of legal and regulatory requirements does not equate to having a deep legal background.
b) Information security risks related to the business sector;
c) General terminology, processes, and technologies related to the customer's business sector;
d) Relevant business sector practices.
Criterion a) can be shared among the audit team.

7.1.3.1.6 Customer products, processes and organization

The audit team members will collectively be informed about the following:

a) The impact of the organization's type, size, governance, structure, functions, and relationships, including outsourcing;
b) Complex operations from a broad perspective;
c) Legal and regulatory requirements applicable to the product or service.

7.1.3.2 Qualification requirements for conducting application reviews

7.1.3.2.1 Customer business sector

Personnel reviewing the application must be knowledgeable about the general terminology, processes, technologies, and risks relevant to the client's business sector in order to determine the competence of the audit team, select audit team members, and schedule the audit duration.

7.1.3.2.2 Customer products, processes and organization

Personnel reviewing the application must have knowledge of the impact of customer products, processes, organizational types, size, governance, structure, functions, and relationships on the development and implementation of ISMS and certification activities, including externally provided functions, in order to determine the necessary audit team qualifications, select audit team members, and determine the audit duration.

7.1.3.3 Competency requirements for reviewing audit reports and making certification decisions.

7.1.3.3.1 General

Personnel reviewing audit reports and making certification decisions must possess the knowledge to verify the appropriateness of the certification scope and any changes within the scope and their impact on the effectiveness of the audit, particularly the continued validity of the identification of interfaces and dependencies and associated risks.

In addition, personnel who review audit reports and make certification decisions should have knowledge of the following:

a) In general, management systems;
b) Audit processes and procedures.

7.1.3.3.2 Information security management terminology, principles, practices and techniques

Personnel reviewing audit reports and making certification decisions should be knowledgeable about the following:

a) Items listed in 7.1.3.1.2 a), b) and c);
b) Legal and regulatory requirements regarding information security.

7.1.3.3.3 Customer business sector

Personnel reviewing audit reports and making certification decisions must have knowledge of the general terminology and risks related to relevant industry practices.

7.1.3.3.4 Customer products, processes and organization

Personnel reviewing audit reports and making certification decisions must be knowledgeable about customer products, processes, organization types, size, governance, structure, functions, and relationships.

7.2. Personnel Involved in Certification Activities

7.2.1 General

ISO/IEC 17021-1:2015 standard , Quality Manual clause 7.2, and the Certification Personnel Management Procedure are applicable.

7.2.2 Demonstration of the auditor's knowledge and experience

7.2.2.1 General provisions

ASCERT demonstrates that each auditor possesses knowledge and experience in each of the following.

a) of the ISMS ;
b) If possible, register as an auditor;
c) Participation in ISMS training courses and acquisition of relevant personal competencies;
d) current professional development records;
e) ISMS audits witnessed by another ISMS auditor.

7.2.2.2 Selection of Auditors

In addition to section 7.1.3.1, ASCERT guarantees that each auditor meets the following criteria during the selection process:

a) Having professional education or training at the university level;
b) Possessing sufficient practical workplace experience in information technology and information security to serve as an auditor;
c) must have received adequate training in ISMS auditing and demonstrate the skills to audit an ISMS according to ISO/IEC 27001. This experience will be gained by participating in at least one ISMS initial certification audit (stage 1 and stage 2) or recertification audit and at least one surveillance audit as a training auditor monitored by an ISMS assessor (see ISO/IEC 17021-1:2015, Quality Manual 9.2.2.1.4). This experience will be gained and realized through at least 10 ISMS on-site audit days within the last five years. Participation will include document review, examination of risk assessment and implementation, and audit reporting.
d) It maintains current and relevant knowledge and skills in information security and auditing.

Note 1: Skill retention can be demonstrated through continuous professional development.
Note 1: The certification body has created a competency matrix that conforms to the above requirements and evidence.

7.2.2.3 Selection of technical experts

The process of selecting technical experts involves ensuring that each technical expert:

a) Having professional education or training at the university level;

b) To work as a technical expert, the candidate must have sufficient practical work experience in the field of information technology and information security.
c) Having relevant and up-to-date knowledge and skills in the field of information security.

Note: Skill retention can be demonstrated through continuous professional development.

7.2.2.4 Selection of supervisors to lead the team

In addition to section 7.2.2.2, the selection criteria for the auditor leading the team requires that the auditor actively participate in all phases of at least three ISMS audits. Participation should include initial scope definition and planning, document review, review of risk assessment and implementation, and formal audit reporting.

7.3 Use of individual external auditors and external technical experts

ISO/IEC 17021-1:2015 standard and Quality Manual clause 7.3 apply.

7.4 Personnel records

ISO/IEC 17021-1:2015 standard and Quality Manual clause 7.4 apply.

7.5 Outsourcing

ISO/IEC 17021-1:2015 standard and Quality Manual The provisions of article 7.5 apply.

8. INFORMATION REQUIREMENTS

8.1. Publicly Available Information

ISO/IEC 17021-1:2015 standard and Quality Manual The provisions of article 8.1 apply.

8.2. Documentation

8.2.1 General

ISO/IEC 17021-1:2015 standard and Quality Manual The provisions of article 8.2 apply. In addition, the following requirements and guidelines also apply: Sections 8.2.2 and 8.2.3 apply.

8.2.2 ISMS Certification Documents

ASCERT provides each of its client organizations whose ISMS has been certified with a certificate signed by the Certification Manager. A version of the Declaration of Applicability is included with the certificates.

NOTE: A change to the Declaration of Applicability that does not alter the scope of the controls covered by the certification does not require an update to the certificate.

If none of the organization's activities covered by the certification are conducted at a specific physical location, the certification document states that all of the organization's activities are conducted remotely.

8.2.3 References to other standards in ISMS certificates

References to national and international standards may only be made in certificates under the following circumstances:

a) The organization has determined, in accordance with ISO/IEC 27001:2022, 6.1.3 c), that it has compared all required checks with those at the reference control source and has not inadvertently omitted any such reference checks;

b) The rationale for excluding reference controls is stated in the Declaration of Applicability (SOA) in accordance with ISO/IEC 27001:2022, 6.1.3 d).

Reference control standards may be based on ISO/IEC 27001:2022 Annex A, or they may be standards that also include information security controls.

The certification documents must state that the set(s) of controls applied in the SOA are used solely to refer to the appropriateness of including or excluding controls in the ISMS and are not used for conformity assessment.

8.3. Reference to Certification and Use of Trademarks

ISO/IEC 17021-1:2015 standard and Quality Manual clause 8.3 apply.

8.4. Privacy

8.4.1 General

ISO/IEC 17021-1:2015 standard and Quality Manual clause 8.4 apply. Furthermore, the requirements and guidelines in 8.4.2 shall also apply.

8.4.1. BG 8.4 Access to Corporate Records

ASCERT requires the client organization to inform the audit team prior to the certification audit whether there are any ISMS records that, due to containing confidential or sensitive information (such as ISMS records or information about the design and effectiveness of controls), cannot be submitted for review .

the ISMS can be properly audited if these records are missing . If ASCERT determines that a proper audit of the ISMS is not possible without reviewing the identified confidential or sensitive records, it will inform the client organization that the documentation audit cannot be performed until appropriate access arrangements are in place.

8.5. Information Exchange Between ASCERT and Its Customers

ISO/IEC 17021-1:2015 standard and Quality Manual clause 8.5 apply.

9. PROCESS REQUIREMENTS

9.1. Pre-Certification Activities

9.1.1. Application

9.1.1.1 General

ISO/IEC 17021-1:2015 standard and Quality Manual clause 9.1.1 apply. Furthermore, the requirements and guidelines in 9.1.1.2 shall also apply.

9.1.1.2 Matters relating to certification procedures

ASCERT procedures do not presuppose a specific implementation style for an ISMS or a particular format for documentation and records. The certification procedures focus on confirming that a customer's ISMS meets the requirements specified in ISO/IEC 27001 and the customer's policies and objectives.

Note: Since an organization can design its own necessary controls or select them from any source, it is possible for an organization to be certified to ISO/IEC 27001 even if none of its necessary controls are specified in ISO/IEC 27001:2022 Annex A.

9.1.2. Review of the Application

ISO/IEC 17021-1:2015 standard and Quality Manual clause 9.1.2 apply.

9.1.3. Audit Program

9.1.3.1 General

of ISO/IEC 17021-1:2015 standard and Quality Manual clause 9.1.3 apply. In addition, the requirements and guidelines in clauses 9.1.3.2, 9.1.3.3, 9.1.3.4, 9.1.3.5 and 9.1.3.6 shall also apply.

9.1.3.2 General provisions

The Audit Program for ISMS audits is created taking into account the specified information security controls.

Note 1: Information security controls may consist of ISO/IEC 27001:2022, its Annex and/or other applicable standards and/or standards designed by the company itself.
Note 2: Further information regarding the audit is provided in ISO/IEC 27007.

9.1.3.3 Deployment of remote control

ASCERT has developed the BQP.18 Remote Audit Procedure to determine the level of remote audit activities (remote audits) that can be applied to the audit of the client's ISMS .
This procedure involves analyzing the risks associated with the use of remote monitoring for the client and takes the following factors into account:

a) ASCERT and the client's existing infrastructure;
b) The sector in which the client operates;
c) s) of audit(s) during the certification cycle, from initial audit to recertification audit ;
d) The competence of ASCERT and the client's personnel participating in the remote audit;
e) Having previously demonstrated remote monitoring performance;
f) Scope of certification.

The analysis will be conducted before the remote audit takes place. The rationale for using remote audits during the analysis and certification cycle must be documented.

The audit plan and audit report include clear indications as to whether remote audit activities were carried out.

Remote auditing will not be used if the risk assessment identifies unacceptable risks in terms of the effectiveness of the audit process.

The risk assessment will be reviewed throughout the certification cycle to ensure continued compliance.
NOTE: If the client uses virtual spaces (i.e., where an organization conducts business or provides services using an online environment that allows it to run processes independently of physical locations), remote audit techniques are a relevant part of the audit plan.

9.1.3.4 General preparations for the initial audit

ASCERT requires the client to make all necessary arrangements to provide access to internal audit reports and independent review reports related to information security.

9.1.3.5 Review periods

an ISMS unless there is sufficient evidence demonstrating that the regulations relating to management reviews and internal ISMS audits are being implemented, are effective, and will be maintained to cover the scope of certification .

9.1.3.6 Scope of ISMS certification

The audit team audits the customer's ISMS within the defined scope according to all applicable certification requirements. ASCERT confirms that the customer's ISMS meets the requirements specified in ISO/IEC 27001:2022, 4.3.

ASCERT ensures that the client's information security risk assessment and risk management accurately reflect their operations and encompass the operational boundaries as defined within the scope of the certification. ASCERT confirms that this is reflected in the client's ISMS and SOA scope. ASCERT verifies that there is an SOA for the certification scope.

ASCERT ensures that interfaces related to services or activities not fully covered by the ISMS are addressed within the scope of the certified ISMS and included in the client's information security risk assessment. An example of such a situation is the sharing of facilities (e.g., IT systems, databases and telecommunication systems, or the outsourcing of a business function) with other organizations.

9.1.4. Determining the Audit Period

9.1.4.1 General

ISO/IEC 17021-1:2015 standard and Quality Manual clause 9.1.4 apply. Furthermore, the requirements and guidelines in 9.1.4.2 shall also apply.

9.1.4.2 Inspection period

The calculation of inspection periods is specified in Appendix C.

Note: Further guidance and examples regarding audit duration calculations are included in Appendix D.

9.1.5 Multi- site sampling

9.1.5.1 General

ISO/IEC 17021-1:2015 standard and Quality Manual clause 9.1.5 apply. Furthermore, the requirements and guidelines in 9.1.5.2 shall also apply.

9.1.5.2 Multiple fields

9.1.5.2.1 If a client has more than one facility that meets criteria a) to c) below, ASCERT uses a sample-based approach for the multiple facility certification audit.

a) All facilities operate under the same ISMS, which is centrally managed, supervised, and subject to central management review;

b) All sites are included in the client's internal ISMS audit program;

c) All sites have been included in the client's ISMS management review program.

9.1.5.2.2 Multiple site audits are conducted according to the principles given below and the BQP.02 Certification Procedure:

a) During the initial contract review, differences between sites are identified to ensure that the broadest possible scope and adequate sampling can be carried out.

b) ASCERT conducts representative field sampling, taking the following into consideration.

1) Internal audit results of the head office (where applicable) and facilities;
2) The results of the management review are as follows:
3) Differences in the size of the fields ;
4) Differences regarding the scope of work of the sites ;
5) of the ISMS ;
6) The complexity of information systems in different fields;
7) Differences in working methods;
8) Differences in design and operational control.
9) Potential interactions with critical information systems or information systems processing sensitive information;
10) Changing legal requirements;
11) Geographical and cultural aspects;
12) Risk status of the sites;
13) Information security incidents in specific regions.

c) the client organization's ISMS ; this selection is determined by a random choice based on a decision that also reflects the factors mentioned in item (b) above.

d) All sites facing significant risks within the scope of the ISMS are audited by ASCERT before certification.

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

f) If a nonconformity is observed at the head office or at a single site, the corrective action procedure is applied to the head office and all sites covered by the certification.

will review the client's activities to ensure the implementation of a single ISMS across all sites and the provision of centralized management at the operational level. The audit will address all of the aforementioned issues.

9.1.6 Multiple management systems

9.1.6.1 General

ISO/IEC 17021-1:2015 standard and Quality Manual clause 9.1.6 apply. In addition, the requirements and guidelines in 9.1.6.2 and 9.1.6.3 shall also apply.

9.1.6.2 Integration of ISMS and other management system documentation

The customer organization may consolidate documentation for the ISMS and other management systems (such as quality, health and safety, and environment), provided that the appropriate interfaces to the ISMS and other systems are clearly defined.

9.1.6.3 Integration of Management System Audits

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

9.2. Planning of Audits

9.2.1. Determining the Purpose, Scope and Criteria of the Audit

9.2.1.1 General

ISO/IEC 17021-1:2015 standard and Quality Manual clause 9.2.1 apply. In addition, the requirements and guidelines in 9.2.1.2 and 9.2.1.3 shall also apply.

9.2.1.2 Audit objectives

Audit objectives will include the following:

a) Determining the effectiveness of the management system;
b) To ensure the client identifies the necessary controls based on their risk assessment; and
c) Determining that the stated information security objectives have been achieved.

9.2.1.3 Audit criteria

a client's ISMS to be audited, the criteria should include ISO/IEC 27001.

9.2.2 Selection and appointment of the audit team

9.2.2.1 General

ISO/IEC 17021-1:2015 standard and Quality Manual clause 9.2.2 apply.

9.2.3 Audit plan

9.2.3.1 General

ISO/IEC 17021-1:2015 standard and Quality Manual clause 9.2.3 apply. In addition, the requirements and guidelines in 9.2.3.2 and 9.2.3.3 shall also apply.

9.2.3.2 General provisions

The audit plan for ISMS audits is created taking into account the specified information security controls.

Note: It is good practice for ASCERT to agree with the audited organization on the audit schedule to best reflect the full scope of the organization. Where appropriate, factors such as season, month, day/date and shift may be taken into consideration.

9.2.3.3 Remote monitoring techniques

The aim of remote audit techniques should be to increase audit effectiveness and efficiency and to support the integrity of the audit process.

The audit plan will refer to the tools used to assist with remote auditing.

9.3 Initial Certification

9.3.1 General

ISO/IEC 17021-1:2015 standard and Quality Manual clause 9.3 apply. In addition, the requirements and guidelines in 9.3.2 shall also apply.

9.3.2 Initial certification audit

9.3.2.1 Stage 1

At this stage of the audit, the certification body will obtain documentation relating to the ISMS design, including the documentation required by ISO/IEC 27001.

During the first stage of the certification audit, the customer will provide at least the following information:

a) General information about the ISMS and the activities it covers;
b) A copy of the required ISMS documentation as specified in ISO/IEC 27001 and any other related documentation as needed.

ASCERT must have sufficient knowledge of the client's ISMS design in the context of the client's organization, risk assessment and management (including defined controls), information security policy and objectives, and especially the client's readiness for the audit. This information should be used in planning the Phase 2 audit.

A written report is prepared for the results of Phase 1. ASCERT reviews the Phase 1 audit report before deciding whether to proceed to Phase 2. ASCERT confirms that the members of the Phase 2 audit team possess the necessary qualifications. This can be done by the auditor who led the Phase 1 audit team, if deemed competent and appropriate.

Note: Having a person not involved in the audit, but appointed by ASCERT, review the report and confirm the audit team members' qualifications for Stage 2 by making a decision to proceed, provides some mitigation for these risks. However, other risk mitigation measures may already be in place to achieve the same objective.

ASCERT informs the client about other types of information and records that may be required for a detailed review in Stage 2.

9.3.2.2 Stage 2

Based on the findings documented in the Phase 1 audit report, ASCERT is developing an audit plan for the organization to execute Phase 2. In addition to assessing the effective implementation of the ISMS , the purpose of Phase 2 is to confirm that the client complies with its own policies, objectives, and procedures.

The client will focus on the following issues:

a) Senior management leadership and commitment to information security objectives;

b) The assessment of information security risks should also ensure that the audit, if repeated, produces consistent, valid and comparable results;

c) Identifying controls based on their processes;

d) Information security performance and the effectiveness of the ISMS , and their evaluation against information security objectives;

e) The alignment between the defined controls, the Statement of Applicability, the results of the information security risk assessment, the risk treatment process, and the information security policy and objectives;

f) Implementing controls taking into account the internal and external context and relevant risks (see Appendix E for examples of audit controls) and monitoring, measuring and analyzing the organization's information security processes and controls to determine whether the controls declared to be implemented are actually implemented and whether they are effective as a whole;

g) Programs, processes, procedures, records, internal audits, and reviews regarding the effectiveness of the ISMS to ensure traceability to top management decisions and information security policy and objectives .

9.4 Conducting audits

9.4.1 General

ISO/IEC 17021-1:2015 standard and Quality Manual clause 9.3 apply. In addition, the requirements and guidelines in clauses 9.4.2 and 9.4.3 shall also apply.

9.4.2 Specific elements of ISMS audit

ASCERT audit team:

a) Requesting the customer to demonstrate that the assessment of information security risks within the scope of the ISMS is appropriate and sufficient for the ISMS operation;

b) To determine whether the customer's procedures for identifying, investigating, and assessing information security risks, and the results of their implementation, are consistent with the customer's policy, goals, and objectives.

ASCERT also determines whether the procedures used in risk assessment are robust and properly implemented.

9.4.3 Audit report

9.4.3.1 The audit report shall include the following information or a reference to it:

a) An account relating to the audit of the client's information security risk analysis;

b) Any information security control set used by the organization for comparison purposes as required by ISO/IEC 27001:2022, 6.1.3 c).

9.4.3.2 The audit report should be detailed enough to facilitate and support the certification decision. The report should include the following:

a) Key audit trails monitored and audit methodologies used (see 9.1.1.2);
b) A reference to the version of the Declaration of Applicability and, where applicable, a useful comparison of the results of the client's previous certification audits.

Completed questionnaires, checklists, observations, records, or auditor notes may be an integral part of the audit report. If these methods are used, these documents must be submitted to ASCERT as evidence to support the certification decision . Relevant information regarding samples evaluated during the audit will be included in the audit report or other certification documents.

Where remote audit methods were used, the report should specify the extent to which these methods were used in conducting the audit and how effective they were in achieving the audit objectives.

If the organization's operations are not conducted in a specific physical location and therefore all of its activities are carried out remotely, the audit report must state that all of the organization's activities are conducted remotely.

The report will consider the adequacy of the internal organization and procedures that will ensure the customer's trust in the ISMS .

The report will include a summary of the key observations, both positive and negative, regarding the implementation and effectiveness of ISMS requirements and information security controls.

9.5 Certification decision

9.5.1 General

ISO/IEC 17021-1:2015 standard and Quality Manual clause 9.5 apply. Furthermore, the requirements and guidelines in 9.5.2 shall also apply.

9.5.2 Certification decision

The certification decision is based on the certification recommendation included in the audit team's audit report.

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

9.6 Maintaining the Certificate

9.6.1 General

ISO/IEC 17021-1:2015 standard and Quality Manual clause 9.6 apply.

9.6.2 Surveillance activities

9.6.2.1 The provisions of ISO/IEC 17021-1:2015 standard and Quality Manual clause 9.6.2 apply. In addition, the requirements and guidelines in 9.6.2.2, 9.6.2.3 and 9.6.2.4 shall also apply.

9.6.2.2 Surveillance audit procedures will be a subset of the procedures for the customer's ISMS certification audit, as described in this document.

The purpose of the monitoring is to verify that the approved ISMS continues to be implemented, to assess the impact of changes initiated in the ISMS as a result of changes in the customer's operational practices , and to confirm continued compliance with the documentation requirements.

Surveillance and inspection programs should include at least the following:

a) Information security risk assessment and control, internal ISMS audit, management review, and corrective actions are elements demonstrating that the ISMS is being maintained;
b) Communications from external parties as required by the ISO/IEC 27001 standard and other documents necessary for certification.

9.6.2.3 ASCERT examines at least the following in each surveillance audit:

a) of the ISMS in terms of achieving the objectives of the customer's information security policy ;
b) The procedures for the periodic assessment and review of compliance with regulations;
c) Changes in the defined controls and changes occurring in the SOA ;
d) Implementation and effectiveness of the controls specified in the audit program.

9.6.2.4 ASCERT is able to adapt and justify its surveillance activity program to reflect information security concerns related to the risks and impacts on the customer.

Surveillance audits may be combined with audits of other management systems. Audit reports should clearly detail matters related to each management system.

During surveillance audits, ASCERT reviews records of objections and complaints submitted to it. If any non-conformity or failure to meet documentation requirements is identified, ASCERT will check whether the client has reviewed its own ISMS and procedures and taken appropriate corrective actions.

A surveillance report should include information, in particular, on the redress of previously identified nonconformities, the version of the SOA , and any significant changes made since the previous audit . Reports resulting from surveillance should be formulated to fully cover at least the requirements of 9.6.2.2 and 9.6.2.3.

9.6.3 Recertification

9.6.3.1 General

ISO/IEC 17021-1:2015 standard and Quality Manual clause 9.6.2 apply. Furthermore, the requirements of 9.6.3.2 shall also apply.

9.6.3.2 Recertification audits

Recertification audit procedures will be a subset of the procedures for the client's ISMS initial certification audit, as described in this procedure.

The time allowed for implementing corrective action should be consistent with the severity of the nonconformity and the associated information security risk.

9.6.4 Special audits

ISO/IEC 17021-1:2015 standard and Quality Manual clause 9.6.4 apply.

9.6.5 Suspension, withdrawal or reduction of scope of certification

ISO/IEC 17021-1:2015 standard and Quality Manual clause 9.6.5 apply.

9.7 Objections

ISO/IEC 17021-1:2015 standard and Quality Manual clause 9.7 apply.

9.8 Complaints

9.8.1 General

ISO/IEC 17021-1:2015 standard and Quality Manual clause 9.8 apply.

9.8.2 Complaints

Complaints indicate a potential incident and a possible misconduct.

9.9 Customer records

ISO/IEC 17021-1:2015 standard and Quality Manual clause 9.9 apply.

10. Management system requirements for certification bodies.

10.1 Options

ASCERT has chosen to meet the requirements of clauses 5 through 9, as well as implement the general management system requirements (Option A). (Clause 10.2)

Appendix A
Knowledge and skills for ISMS audit and certification.

A.1 Overview

Table A.1 specifies the knowledge and skills that a certification body must define for specific certification functions, in addition to the requirements of ISO/IEC 17021-1 and the Quality Manual. X indicates that the certification body must define the criteria and depth of knowledge and skills. The knowledge and skills requirements specified in Table A.1 are described in more detail in Clause 7 and cross-referenced in parentheses in Table A.1.

Table A.1 – Knowledge and skills table for ISMS audit and certification.

Knowledge and skills	**Documentation function**		
	The application review process aims to determine the competence of the audit team, select the audit team members, and determine the audit duration.	**Review of audit reports and making certification decisions.**	**Supervision and management of the audit team.**
Information security management terminology, principles, practices, and techniques.		X (see 7.1.3.3.2)	X (see 7.1.3.1.2)
Information security management system standards/normative documents			X (see 7.1.3.1.3)
Business management practices			X (see 7.1.3.1.4)
Customer business sector	X (see 7.1.3.2.1)	X (see 7.1.3.3.3)	X (see 7.1.3.1.5)
Customer products, processes and organization	X (see 7.1.3.2.2)	X (see 7.1.3.3.4)	X (see 7.1.3.1.6)

Further details are included in Annex B.

Appendix B
Further competency considerations

B.1 General competency aspects

Auditors have various ways to demonstrate their knowledge and experience. Knowledge and experience can be assessed, for example, using recognized qualifications. Records from a staff certification program can also be used to assess the necessary knowledge and experience. The required competency level for the audit team should be determined to reflect the organization's sector/technology field and the complexity of the ISMS .

B.2 Specific knowledge and experience considerations

B.2.1 Typical information regarding ISMS

In addition to the requirements in 7.1.3, the following should also be considered. Auditors should have knowledge and understanding of the following audit and ISMS topics:

- Audit programming and planning;
- Types and methodologies of audits;
- Audit risk;
- Information security process analysis;
- Continuous improvement;
- Internal audit of information security.

Auditors should have knowledge and understanding of regulatory requirements regarding the following:

- Intellectual property;
- Content, preservation, and storage of corporate records;
- Data protection and privacy;
- Regulation of cryptographic controls;
- Electronic commerce;
- Electronic and digital signatures;
- Workplace surveillance;
- Interception and monitoring of telecommunications data (e.g., email);
- Computer misuse;
- Electronic evidence collection;
- Penetration test;
- International and national sector-specific requirements (e.g., banking).

For a particular sector, knowledge and understanding may be established within a specific standard (e.g., ISO/IEC 27006-1).

Appendix C
Audit time

C.1 General

This annex contains additional requirements related to ISO/IEC 17021-1:2015 and Quality Manual 9.1.4. It provides minimum requirements and guidance for a certification body to develop its own procedures to determine the time required for certifying ISMS scopes of varying size and complexity across a wide range of activities.

Certification bodies must allow auditors sufficient time to conduct all activities related to the initial audit, surveillance audit, or recertification audit. The calculation of total audit time should include sufficient time for audit reporting.

Certification bodies must determine the audit time to be spent on initial certification, surveillance, and recertification for each client and certified ISMS. Using this additional audit during the planning phase ensures a consistent approach in determining the appropriate audit duration. Furthermore, the audit duration can be adjusted according to issues identified during the audit, particularly in Phase 1 (e.g., differing assessments of the complexity of the ISMS scope or additional sites within the scope).

This annex contains the following:

- Concepts used in calculating the audit period (C.2);
- Requirements regarding procedures for determining the audit duration for different stages of the initial audit (C.3);
- Audit duration requirements for surveillance (C.4) and recertification audit (C.5);
- Requirements relating to multiple facility audits (C.6);
- Audit time requirements for scope extensions (C.7).

To illustrate the application of this annex, examples of calculating the inspection period are given in Annex D.

The basic assumption of the approach in this appendix is that a calculation scheme for determining the audit duration should be as follows:

a) Consider only the qualities that can be assessed objectively;
b) It should be simple enough for certification bodies to implement and to obtain valid, comparable and repeatable results;
c) Become sophisticated enough to ensure that changes in attribute values lead to comparable changes during the audit period.

The audit period will be determined based on the numbers in Table C.1, taking into account the factors contributing to the change.

The approach to determining the audit duration set by the certification body should be reviewed regularly to verify whether it is adequate for the complexity of the ISMS .

C.2 Concepts

Number of people working under the organization's control

The audit duration is determined based on the total number of people working under the organization's control in all shifts covered by the certification.

Note: Individuals working under the organization's control include all personnel (whether or not they are members of the organization) who are required to work according to ISMS requirements and are within the scope of certification.

Part-time employees working under the organization's supervision contribute to the number of people working under the organization's supervision in proportion to the number of hours worked compared to a full-time employee working under the organization's supervision. This determination will depend on the number of hours worked compared to a full-time employee.

When a high percentage of persons working under certification within the organization's control perform specific identical activities, a reduction in the number of persons is permitted before using Table C.1 for calculating the audit duration. Certification bodies should use the factors given in C.3.4 and determine how to reduce the number of persons under certification, taking into account the impact of the activities on information security risk. Repeatable and consistent procedures should be documented on a company-by-company basis.

C.2.2 Auditor's Day

The audit duration specified in Table C.1 is expressed in terms of the number of days the auditor spent on the audit. This appendix is based on an eight-hour workday.

C.2.3 Temporary site

A temporary facility covered by certification is a location outside the facilities specified in the certification document where activities covered by certification are performed for a specific period. These facilities can range from large project management facilities to small service/installation facilities. The need to visit these facilities and the scope of sampling should be based on an assessment of the risks to meeting information security objectives of the activities performed at this temporary facility. Selected facility examples should represent the scope of the organization's competency needs and service diversity, in light of the size and types of activities and the various phases of ongoing projects. For general sampling, see section 9.1.5.2.

C.3 Procedure for determining the audit period for the initial audit

C.3.1 General

The certification body must have and follow a documented procedure for calculating the audit duration.

C.3.2 Methods of conducting remote monitoring

If remote audit methods such as interactive web-based collaboration, web meetings, teleconferences, and/or electronic verification of the organization's processes are used to interact with the organization, these activities should be identified in the audit plan (see 9.2.3) and may be considered to partially contribute to the total on-site audit time.

Note : On-site inspection time refers to the on-site inspection time allocated for each site. Electronic inspections of remote sites are considered remote inspections, even if the electronic inspections are physically performed at the organization's facilities.

C.3.3 Calculation of audit period

The audit duration schedule presented in Table C.1 establishes the starting point for the average number of initial audit days. [In this appendix and Appendix D, this number includes the initial audit days (Stage 1 and Stage 2).] It has been shown to be appropriate for an ISMS scope where a certain number of people work under the organization's control. Furthermore, experience has shown that for ISMS scopes of similar size, some require more time than others.

The following audit timeline provides the framework to be used for audit planning. The starting point is based on the total number of people working under the organization's control for all shifts. The number of auditor days is adjusted according to the significant factors applicable to the ISMS scope being audited, and an additive or subtractive weighting is applied to modify the base figure for each factor. The audit timeline in Table C.1 should be used taking into account the contributing factors and allowable deviation restrictions (see C.3.5 and C.3.6). The terms used in Table C.1 are explained in C.2. Appendix D provides examples of how the calculation method of this appendix can be applied.

C.3.4 Determining the initial number of people

Certification bodies will request information from the client regarding the number of individuals performing specific, identical activities. This information includes:

- Number of people participating in the activity;
- The type of activity or process.

Examples of factors that can reduce the number of people performing the same activities and are used in the calculation include:

- Individuals who have read-only access to information to perform their duties;
- Within the scope of the ISMS, individuals who do not have access to the organization's information processing facilities;
- Within the scope of the ISMS, individuals have specific and verifiable restricted access to the company's information processing facilities;
- Individuals whose activities are subject to strict restrictions to limit information disclosure (for example, measures prohibiting the bringing of personal belongings and devices into the work area).
- Individuals whose activities are subject to strict restrictions to limit the disclosure of information (for example, measures prohibiting the bringing of personal belongings and equipment into the work area).

The reduction in the number of people performing the same activities is based on the risk associated with the tasks. The square root of the number of people performing each identical activity can be used to determine the effective number of people used in audit duration calculations, and rounded up to the next whole number. This number will be the maximum allowed reduction in the number of people.

The nature of the tasks, legal requirements, and the importance of the information accessible to individuals may limit mitigation.

The number of people determined after this procedure is the starting point in Table C.1.
Note: The table is structured in the same way as IAF MD5(9).

Table C.1 Audit time schedule

Number of people working under the organization's control	Quality management system audit period for the initial audit.	Environmental management system audit period for the initial audit.	ISMS audit period for the first audit	Additive and indirect factors	Total audit duration
1-10	1.5-2	2.5-3	5	See section C.3.5.	
11-15	2.5	3.5	6	See section C.3.5.	
16-25	3	4.5	7	See section C.3.5.	
26-45	4	5.5	8.5	See section C.3.5.	
46-65	5	6	10	See section C.3.5.	
66-85	6	7	11	See section C.3.5.	
86-125	7	8	12	See section C.3.5.	
126-175	8	9	13	See section C.3.5.	
176-275	9	10	14	See section C.3.5.	
276-425	10	11	15	See section C.3.5.	
426-625	11	12	16.5	See section C.3.5.	
626-875	12	13	17.5	See section C.3.5.	
876-1175	13	15	19.5	See section C.3.5.	
1176-1550	14	16	19,5	C.3.5'e bakın	
1551-2025	15	17	21	C.3.5'e bakın	
2026-2675	16	18	22	C.3.5'e bakın	
2676-3 450	17	19	23	C.3.5'e bakın	
3451-4350	18	20	24	C.3.5'e bakın	
4351-5450	19	21	25	C.3.5'e bakın	
5451-6800	20	23	26	See section C.3.5.	
6801-8500	21	25	27	See section C.3.5.	
8501-10700	22	27	28	See section C.3.5.	
>10 700	Follow the progress above.	Follow the progress above.	Follow the progress above.	See section C.3.5.	

C.3.5 Factors related to adjusting the audit duration

Table C.1 should not be used in isolation. The time allocated should also consider the following factors relating to the complexity of the ISMS and therefore the effort required to audit it :

a) of the ISMS (e.g., information criticality, risks associated with the ISMS, etc.);
b) Type(s) of work performed within the scope of the ISMS;
c) The previous performance of the ISMS ;
d) The scope and variety of technology used in the implementation of the various components of the ISMS (e.g., the number of different IT platforms, the number of dedicated networks);
e) The scope of outsourcing and third-party arrangements used within the scope of the ISMS;
f) The scope of information system development;
g) Number of sites and number of Disaster Recovery (DR) sites;
h) After the first stage, the certification body will consider the number and complexity of the checks;
i) For surveillance or recertification audits: the amount and scope of changes to the ISMS according to ISO/IEC 17021-1:2015 and Quality Manual 8.5.3.

Appendix D provides examples of how these different factors can be taken into account when calculating the audit duration.

Examples of factors that necessitate adding audit time include:

- Complex process logistics encompassing multiple buildings or locations within the scope of the ISMS;
- The staff speaking multiple languages (necessary for interpreters or hindering the independent work of individual auditors) or the provision of documents in multiple languages;
- Management system certification activities that require visiting temporary sites to verify the operations of permanent sites subject to certification.
- There are numerous standards and regulations applied to BGYD .

Examples of factors that allow for the exclusion of the audit period include:

- Risk-free or low-risk processes
- Processes that involve a single overall activity (e.g., service only);
- The organization's prior knowledge (for example, whether the organization has previously been certified by the same certification body according to another standard);
- High customer readiness for certification (e.g., already certified or recognized by another third-party scheme);
- The management system must have a high level of maturity.

Where a customer or certified organization provides its products or services in temporary locations, it is important that assessments of such locations are included in certification audit and monitoring programs.

Adjustments can be made for the factors listed above. Factors requiring the addition or subtraction of audit time may balance each other out. In all cases where adjustments are made to the periods specified in Table C.1, sufficient evidence and records must be kept to justify the change.

3.6 Limiting the deviation of the audit period

To ensure effective audits are conducted and reliable and comparable results are obtained, the audit duration specified in the audit timeline cannot be reduced by more than 30%.
Appropriate reasons for deviations should be identified and documented.

C.3.7 On-site inspection period

The time allocated for planning and report writing should not result in less than 70% of the time calculated according to sections C.3.3, C.3.4, and C.3.5. The need for additional time for planning and/or report writing should not justify reducing the on-site audit time. Auditor travel time is not included in this calculation and is added to the audit time specified in the table.

Note 1: This is a factor based on experience gained from 70% ISMS audits.

Note 2: The term "physical/remote" means that "on-site" inspections (for the customer's physical locations or electronic facilities) can be performed physically or remotely (see 9.2.3 and C.3.2). For "on-site" inspections, also see ISO/IEC 17021-1:2015 and Quality Manual 9.4.1.

C.4 Audit duration for surveillance audits

For the initial certification audit cycle, the surveillance time for a given organization should be proportional to the time spent on the initial audit, and the total time spent on surveillance annually should be approximately one-third of the time spent on the initial audit. The planned surveillance time should be reviewed periodically to account for changes that may affect the audit duration. The time spent on surveillance audits should be increased to allow for the auditing of changes in the ISMS (such as auditing new or modified information security controls, processes, and services).

C.5 Audit duration for recertification audit

The total time spent on conducting the recertification audit will depend on the results of the previous audit, as defined in sections 9.4.3 and ISO/IEC 17021-1:2015 and Quality Manual 9.6.3. The audit time required for the recertification audit must be at least two-thirds, but proportionate, to the audit time required for the initial certification audit of the same organization during the recertification audit.

C.6 Multiple site audit period

Generally, the total audit time for an on-site audit is calculated by taking into account the total number of people working under the organization's control, regardless of their positions.

Alternatively, for justifiable reasons requiring documentation, the combined audit periods, calculated separately for each facility, may be longer than the period defined in the first paragraph of this article. Discounts may be applied to account for parts of the audit that are not related to the central office or local facilities (if any). The justification for these discounts shall be recorded by the certification body.
C.3.3 and C.3.4 , will be distributed to different sites taking into account the importance of the site in terms of the management system, the activities carried out on-site, and the risks identified. The justification for the allocation will be recorded by the certification body.

Any reductions must be implemented before comparing the reduced audit duration to the overall audit duration.

C.7 Review period for scope expansions
an ISMS should be calculated taking into account factors such as the following:

a) Type of expansion:
b) The activity(s) of the current certification;
c) Number of locations where the activity(s) were carried out;
d) Information security risks related to the activity(s);
e) The number of controls related to the expansion;
f) Under the new framework, the number of people working under the organization's control is; and
g) Time required to review the integration of the expanded scope into the ISMS .

Certification bodies need to have procedures in place that provide a consistent approach to expanding scope.
The timeframe for the initial audit of the new coverage will be calculated based on the number of individuals and sites added to the existing coverage, using sections C.3.3, C.3.4, and C.3.5.

the customer's ISMS . This additional time will be at least as follows:

1) If the scope expansion audit is conducted together with a surveillance audit or recertification audit, the rate is 0.5 man-days.
2) If the scope expansion audit is conducted as a separate audit, the cost is 1.0 man-day.

Appendix D
Methods for calculating audit duration

D.1 General

This appendix provides further guidance on developing a formula for calculating audit duration. Section D.2 gives an example of classifying factors that can be used as a basis for calculating audit duration, and Section D.3 gives an example of calculating audit duration.

Note: The concepts in this appendix begin after the implementation of the reduction in the number of people performing specific identical activities, as described in section C.3.4.

D.2 Classification of factors in calculating the audit period

Table D.1, C.3.5, a) to i) provides examples of the classification of key factors in calculating audit duration. This classification can be used by certification bodies to derive an audit duration calculation scheme in accordance with 9.1.4.2.

Table D.1 Classification of factors in calculating the audit period.

Factors (see section 3.5)	Its effect on effort		
	Reduced effort	Normal effort	Increased effort
a) of the ISMS : - Information security requirements [confidentiality, integrity, and availability, (CIA)] - Number of critical assets - Number of processes and services	- Very little sensitive or confidential information, low availability requirements. - Several critical assets (from the CIA's perspective) - Only one core business process with a small number of interfaces and a small number of business units involved.	- Higher availability requirements or certain sensitive/confidential information - Some critical assets - 2-3 simple business processes with a small number of interfaces and a small number of business units.	- More sensitive or confidential information (e.g., health, personally identifiable information, insurance, banking) or high accessibility requirements. - Many critical assets - More than two complex processes involving numerous interfaces and business units.
b) Type(s) of work performed within the scope of ISMS	- Low-risk business without regulatory requirements	- High regulatory requirements	- High-risk jobs with (only) limited regulatory requirements.
c) Previously demonstrated performance of the ISMS .	- Recently approved. - It is not certified, but the ISMS has been fully implemented throughout various audit and improvement cycles, including documented internal audits, management reviews, and an effective continuous improvement system.	- Last surveillance inspection - ISMS that is not certified but partially implemented: Some management system tools are available and implemented; some continuous improvement processes are in place but only partially documented.	- There is no certification and no recent audit. - The ISMS is new and not fully established (e.g., lack of system-specific control mechanisms, immature continuous improvement processes, special process execution)
d) The scope and variety of technology used in the implementation of the various components of the ISMS (e.g., the number of different IT platforms, the number of dedicated networks)	- Highly standardized environment; High 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 network segments, server or database types, number of key applications)

e) Scope of outsourcing and third-party arrangements used within the scope of the ISMS	- There is no outsourcing and very little dependence on suppliers, - Well-defined, managed, and monitored outsourcing arrangements. - The outsourcing provider has a certified ISMS. - Relevant independent assurance reports are available.	- Several partially managed outsourcing arrangements	- High dependence on outsourcing or suppliers that has a major impact on important business activities or - The unknown amount or scope of outsourcing or - Several unmanaged outsourcing arrangements
f) The scope of information system development	- No in-house system development. - Use of standardized software platforms	- The use of standardized software platforms with complex configuration/parameterization. - (Highly) customized software - Some development activities (in-house or external)	- Extensive internal software development activities with several ongoing projects for important business purposes.
g) Number of sites and disaster recovery (DR) sites	- Low usability requirements and no or no DR site.	- Medium or high availability requirements and no or no DR site.	- High availability requirements (e.g., 24/7 services) - Several DR sites - Several data centers
h) Number and complexity of controls	- Fewer controls than usual, with some common control areas not included – for example, no system development controls or physical controls.	- Typical number and complexity of checks	- More detailed and complex controls than ever before, for example, many controls related to network protocols or cryptography.
i) For surveillance or recertification audits: Amount and scope of changes to the ISMS in accordance with ISO/IEC 17021-1:2015, 8.5.3.	- There have been no changes since the last recertification audit.	- to the scope or SOA of the ISMS , for example, some policies, documents. - Minor changes in the above factors	- the scope or SOA of the ISMS , such as new processes, new business units, areas, risk assessment management methodology, policies, documentation, risk treatment. - Major changes in the above factors

D.3 Example of calculating audit duration

The following example shows how a certification body can use the factors given in C.3 to calculate audit duration . In the following example, the calculation of audit duration works as follows:

Step 1: Identifying business and organizational factors (excluding IT): Assign the appropriate score for each category given in Table D.2 and sum the results.

Step 2: Identifying IT environment factors: Assign the appropriate score for each category given in Table D.3 and sum the results.

Step 3: Based on the results of steps 1 and 2 above, determine the impact of the factors on the control period by selecting the appropriate entry in Table D.4.

Step 4: Final calculation: The number of days determined by applying the audit duration schedule in Table D.1 is multiplied by the factor obtained in Step 3. When using multicenter sampling, the calculated audit days are increased according to the effort required to execute the multicenter sampling plan.

This result represents the final number of audit days.

Table D.2 Business and organizational factors (excluding IT)

Category	Level
Job type(s) and regulatory requirements	1. operates in non-critical business sectors and unregulated sectors · 2. $^{\text{critical}}$ business sectors . 3. $^{\text{critical}}$ business sectors .
Processes and tasks	1. Standard processes with standard tasks; a small number of products or services. 2. Standard but non-repetitive processes, with a large number of products or services. 3. Complex processes, numerous products and services, many business units included in the scope of certification (ISMS covers highly complex processes or a relatively large number of unique activities)
Organizational level of the management system	1. The ISMS is already well-established and/or other management systems are in place. 2. Some elements of other governance systems are implemented, others are not. 3. No other management system has been implemented; the ISMS is new and not yet established.
[a.] Critical business sectors are those that can affect critical public services, posing risks to health, safety, the economy, reputation, and the ability of government to function, and having significant negative impacts on countries.	

Table D.3 Factors related to the IT environment

Category	Level
Complexity of IT infrastructure	1. A small number of 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
Dependence on outsourcing and suppliers, including cloud services.	1. There is little or no dependence on outsourcing or suppliers. 2. Some degree of reliance on outsourcing or suppliers, related to, but not all, important business activities. 3. High reliance on outsourcing or suppliers has a significant impact on key business operations.
Information system development	1. No or very limited in-house system/application development 2. Developing in-house or outsourced systems/applications for key business purposes. 3. Comprehensive in-house or outsourced system/application development for critical business objectives.

Table D.4 Effect of factors on control period

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

Example 1: The organization to be audited has 700 employees, therefore, according to Table C.1, the initial audit requires 17.5 days. The organization does not operate in a critical business sector, has highly standardized and repetitive tasks, and has recently implemented an ISMS . According to Table D.2 , this reveals a 1+1+3=5 factor related to the business and organization. The organization has very few IT platforms and databases but heavily relies on outsourcing. Software development is neither done in-house nor outsourced. According to

Table D.3, this reveals a 1+3+1 = 5 factor related to the IT environment. Using Table D.4, no adjustment is needed for the audit duration.

Example 2: Using the same organization as in Example 1, but with several management systems already in place and an already well-established ISMS , will change the calculation according to Table D.2 to 1+1+1 = 3. According to Table D.4, this will result in a 5% to 10% reduction in audit time, meaning a decrease of 1 to 1.5 days, and a total reduction of 16 to 16.5 days.

Appendix E
Guidelines for reviewing the implemented ISO/IEC 27001:2022, Annex A controls.

E.1 Objective

In accordance with the requirement in clause 9.3.2.2 f), the implementation of controls determined by the customer to be necessary for the ISMS (in accordance with the Declaration of Applicability) will be reviewed during the second phase of the initial audit and during surveillance or recertification activities. The reviews aim to determine whether the controls have been implemented and are effective, and whether they meet the stated information security objectives.

Typically, after an auditor visits an organization, the certification body learns what the organization's required controls are or whether they are defined using the same control text as in ISO/IEC 27001:2022, Annex A. The certification body also does not know the relationship between information security controls or the relationship between information security controls and the organization's processes. Therefore, while the initial audit may be limited to auditing individual controls, subsequent audits may adopt a more effective approach, such as auditing controls within the context of the organization's processes and the risk treatment plans to which they are implemented.

However, certification bodies are aware that organizations must compare their required controls with those in ISO/IEC 27001:2022, Annex A, and therefore there is a relationship between the organization's required controls and those in ISO/IEC 27001:2022, Annex A. The guidance given in Table E.1 aims to support the certification body in developing audit plans to meet the required controls determined by the client, taking into account the relationship with the controls in ISO/IEC 27001:2022, Annex A.

E.2 How to use Table E.1
E.2.1 General

Table E.1 provides an example guideline for reviewing required controls. The table uses controls listed in ISO/IEC 27001:2022, Annex A; however, auditors should use the relationship between these controls and the organization's required controls when interpreting the audit evidence gathering guidance provided in Table E.1, which demonstrates the effectiveness of the controls.

Note: Table E.1 is not intended to provide guidance on reviewing controls unrelated to those in Annex A of ISO/IEC 27001:2022.

Most controls involve organizational aspects that can be evidenced through reviewing the client's documentation regarding controls, processes, or procedures, through interviews, or through observation.

Many controls are based on rules established by the client organization. These rules may take the form of subject-specific policies, requirements in processes or procedures, or other types of rules communicated to personnel. Table E.1 uses the general term "rules" to specify such requirements or expectations as defined by the client organization's management.

Many controls can be tested through sampling, that is, by examining a sample of the outputs of the control activity.

E.2.2 "System Test" column

Many controls in Annex A of ISO/IEC 27001:2022 are implemented as technological controls, for example through specific system settings, configurations, or technology functions. Evidence of the performance of technological controls can often be obtained through system testing or the use of specialized audit or reporting tools. System testing means the direct examination of information systems: the auditor may examine system settings and configurations or evaluate the results of test tools. If the client uses tools known to the auditor, these may also be used to support the audit, or the auditor may review the results of an assessment performed by the client.

The "system testing" column in Table E.1 provides guidance for examining technological controls:

- "Empty" system testing generally means that it is not applicable or necessary in an ISMS audit;
- The term "possible" means that system testing is generally feasible for evaluating control implementation, but may not be necessary in an ISMS audit;
- The term "recommended" means that system testing is generally required in an ISMS audit.

E.2.3 "Visual examination" column

Other controls in Annex A of ISO/IEC 27001:2022 can be examined through an on-site "visual inspection" to assess their implementation and effectiveness. Since reviewing relevant documentation on paper or through interviews is not sufficient, the auditor must assess the verification of the control at the location where it is implemented.

Note: On-site visual inspection can also be conducted using remote inspection techniques, such as having a person on-site providing the inspector with a real-time video stream.

The "Visual examination" column in Table E.1 provides guidance for examining the physical evidence of the controls:

- "Blank" visual inspection generally means that it is not applicable or necessary in an ISMS audit;
- "Possible" visual inspection generally means that it is possible for evaluating the control application, but may not be necessary in an ISMS audit;

- The phrase "recommended recommendation" means that visual inspection is generally required in ISMS audits.

E.2.4 Possible evidence regarding the design and implementation of controls.

"Potential evidence regarding the design and implementation of controls " column provides guidance on evidence that may assist an auditor in assessing compliance with ISO/IEC 27001:2022, 8.3 (the need to implement a risk treatment plan and therefore the necessary controls). The various items in this column are not requirements and do not constitute an exhaustive list. Because they are derived from the control text in Annex A of ISO/IEC 27001:2022, they are not necessarily applicable to an organization's relevant required control(s). In this case, other forms of evidence should be used. The organization's Statement of Applicability and related ISMS documentation should be used as the specification of the organization's required controls. The organization's Statement of Applicability includes the required controls, the rationale for their inclusion, whether they are implemented, and the rationale for any controls excluded from Annex A of ISO/IEC 27001:2022.

Table E.1 — Evaluation of controls

Controls in Annex ^{A} of ISO/IEC 27001:2022.	System test	Visual inspection	Possible evidence regarding the design and implementation of controls.
5. Corporate controls			
5.1 Information security policies			- Information security policy - Information security-specific policies as deemed necessary by the organization. - Communicating policies to relevant personnel and stakeholders.
5.2 Information security roles and responsibilities			- Assigned roles and responsibilities for the implementation, operation, and management of information security.
5.3 Separation of Duties			- It defined overlapping tasks or areas of responsibility and the corresponding rules for distinguishing between them.
5.4 Management responsibilities			- Management statements and support for information security objectives, policies, procedures, etc. - Specifying the personal responsibility of personnel regarding information security.
5.5 Communication with authorities			- Defined contact points with the relevant authorities - Rules for reporting incidents - Content of information flow from and to the relevant authorities.
5.6 Communication with special interest groups			- Membership in special interest groups or other forums and associations and defined points of contact [e.g., Computer Emergency Response Teams, cybersecurity agencies] - Rules about what can be discussed in such organizations - The content of information flowing from and to such organizations.
5.7 Threat intelligence			- The approach to gathering relevant threat intelligence. - Analysis of threat intelligence related to the organization and its communication to relevant parties.
5.8 Information security in project management			- Ensuring information security in project management throughout the project lifecycle, for example, requirements definition, testing. - For example projects, identified information security risks and corresponding risk management.

5.9 Inventory of information and other related assets	Possible		- Inventories of information and other related assets maintained by the ISMS - Maintaining ownership of assets in asset inventories - Rules regarding ownership duties for assets, such as classification.
5.10 Acceptable use of information and other related assets			- Documented guidelines regarding the acceptable use of information and other related assets. - Procedures for processing information and other related assets.
5.11 Return of assets			- Rules for returning the organization's assets, for example, checklists for employment, contract or agreement modification or termination. - Examples of documented return records.
5.12 Classification of Information			- For example, in a subject-specific policy, there are rules and schemes for classifying information. - Examples of information from various sources that need to be classified.
5.13 Labeling Information		Possible	- Rules for labeling information and other related assets - Procedures for labeling specific types of information and other related assets.
5.14 Information transfer	Possible		- Rules regarding information transfer, for example in a subject-specific policy. - The ISMS defines the use cases for information transfer and includes relevant rules, procedures, or agreements, for example, physical, electronic, or oral transfer. - Examples of implemented information transfer procedures or agreements
5.15 Access control	Possible		- Rules for controlling physical and logical access to information and other related assets, for example, a subject-specific policy regarding access control. - Summaries (examples) where access rights for high-risk physical or logical access to information and other assets are checked for compliance with the above rules.
5.16 Identity management			- Procedures for managing identities assigned to individuals or non-human entities throughout their life cycle.
5.17 Authentication Information	Recommended		- A description of a process for allocating and managing identity verification information. - Instructions for users on how to properly process information used for identity verification. - Where passwords are used, the security settings of password management systems (e.g., length, complexity, return)
5.18 Access rights	Recommended		- Access control rules, for example, the subject of access control, are detailed in a specific policy (physical and logical). - Description of the process for assigning, updating, or revoking access rights. - Rules and procedures for the regular review of access rights. - Access rights assigned to the identity document - Results of the investigations conducted regarding access rights

5.19 Information security in supplier relationships			- A topic-based policy regarding the use of the supplier's products and services. - Information security in supplier relationships: processes or procedures for managing these relationships throughout their lifecycle. - Results obtained from supplier evaluations [e.g., Information and Communication Technology (ICT) infrastructure components, services] - Results obtained from monitoring compliance with defined information security requirements (for example, as an example regarding supplier relationships)
5.20 Addressing information security within the scope of supplier contracts			- Recording agreements with external parties, depending on the type of supplier relationship. - Supplier contracts including relevant information security requirements and Service Level Agreements (example)
Management of information security in the information and communication technology supply chain			- Rules for handling information security when purchasing products or services. - IT supply chain information security risk management practices - The results of the risk analysis performed, i.e., mitigating controls for a specific IT supply chain example.
5.22 Monitoring, reviewing and change management of supplier services			- Supplier information security practices and processes for managing changes in service delivery. - Plans for regularly monitoring, reviewing, and evaluating supplier information security practices (e.g., through service reports, supplier audits) - Results from monitoring and review activities, including action plans.
5.23 Information security for the use of cloud services			- A specific policy regarding the use of cloud services. - List of cloud services used by the organization - Processes for managing information security risks associated with the use of cloud services. - Specific provisions regarding the protection of the organization's data and the availability of services, if the cloud service agreements do not cover the organization's confidentiality, integrity, availability, and information processing requirements.
5.24 Information security incident management planning and preparation			- Processes, plans, roles, and responsibilities for handling information security incidents. - Reporting procedures for information security incidents and examples of such reports.
5.25 Assessment and decision-making regarding information security incidents			- Criteria for evaluating information security incidents. - Categorization and prioritization scheme for information security incidents.
5.26 Responding to information security incidents			- Information security incident response procedures - Records of events and corresponding event responses.
5.27 Learning lessons from information security incidents			- Records of information security incidents that occurred, including their types, volumes, and resulting costs. - Lessons learned from the analysis of information security incidents, for example, improving the incident management plan, enhancing controls, and raising awareness.
5.28 Gathering evidence			- Procedures for dealing with evidence related to information security incidents, such as identifying, collecting, acquiring, and preserving evidence.
5.29 Information security during outages			- Plans for maintaining appropriate levels of information security during the outage. - Integrating information security requirements into business continuity management planning and

			processes.
5.30 IT preparedness for business continuity			- IT continuity requirements derived from business impact analysis. - IT continuity plans - Results of regular IT continuity tests
5.31 Legal, regulatory, and contractual requirements			- List of relevant countries in which the organization operates or uses its products and services, which could affect the organization's information security. - Specified external requirements, including legal, regulatory, or contractual requirements relating to information security, particularly concerning the use of cryptography in any form.
5.32 Intellectual property rights			- For example, rules regarding the management of intellectual property rights in a subject-specific policy. - Procedures for processing inventories relating to document copyrights, design rights, trademarks, patents, and source code licenses.
5.33 Record keeping	Recommended		- For example, in a subject-specific policy, records management rules are linked to applicable laws, regulations, and contractual requirements. - Procedures for record keeping, chain of custody management, storage and destruction. - Configuring data storage systems to enable record management requirements (e.g., protection, retention).
5.34 Privacy and protection of personally identifiable information			- For example, rules regarding the processing of personally identifiable information (PII) in a subject-specific policy. - with which the organization does business or uses products and services that may affect the confidentiality and protection of PII . - Specified external requirements, including legal, regulatory or contractual requirements, for the protection of privacy and the protection of personal data. - Analyses carried out by the processing responsible parties show that PII requirements are met through appropriate technical and organizational measures.
5.35 Independent review of information security			- Plans to conduct independent information security reviews - Reporting the results of independent reviews (sampling) to senior management. - Corrective actions were taken when the organization's approach to managing information security was found to be inadequate.
5.36 Compliance with information security policies, rules and standards			- The organization's information security policy includes plans for reviewing compliance with issue-based policies, rules, and standards. - Results of such reviews (example) and corrective actions taken.
5.37 Documented operating procedures			- Information security aspects of the operating procedures of the relevant information processing facilities.
6 people checked			
6.1 Scanning			- Rules and procedures for background checks, taking into account applicable laws, regulations, and ethical guidelines. - Background checks are performed on the sample applicable to both new hires and existing staff (e.g., promotions, sensitive job profiles).

6.2 Employment terms and conditions			- General rules or general terms and conditions relating to information security responsibilities, such as codes of conduct. - Acceptance of information security terms and conditions by personnel. - Examples of specific information security responsibilities accepted by personnel in critical roles (e.g., access to sensitive information or privileged access to systems)
6.3 Information security awareness, training and education			- Information security awareness, education, and training program with specific content for key target groups. - List of participants in the information security trainings held. - Responses regarding expected behaviors from interviews conducted with a sample of participants.
6.4 Disciplinary process			- The formal disciplinary process communicated to staff and other relevant parties.
6.5 Responsibilities following termination or job change			- Signed acceptance by the employee of specific responsibilities and duties that will be effective upon leaving the company or changing jobs.
6.6 Confidentiality or non-disclosure agreements			- Confidentiality agreements signed by personnel and other relevant parties.
6.7 Remote work	Possible		- Remote working rules, for example, a subject-specific policy. - Examples of physical and communication security measures. - Design of permitted secure computing devices [laptops]
6.8 Information security incident reporting			- Mechanism for reporting information security incidents that can be identified by personnel. - Instructions or communications to raise awareness about reporting information security incidents.
7. Physical checks			
7.1 Physical security environments		Possible	- Regulations regarding the construction of safe zones and the strength of physical barriers. - Physical security perimeter and secure area design for each relevant location.
7.2 Physical entrance	Possible	Recommended	- Access authorization system (physical or electronic) for entry points to secure areas. - Access logs to track the entry of staff and visitors. - Physical design of delivery and loading areas and related process descriptions.
7.3 Ensuring the security of offices, rooms and facilities		Possible	- Physical security design and implementation for offices and facilities where sensitive information is processed.
7.4 Physical security monitoring	Possible	Possible	- Designing physical surveillance systems to detect unauthorized physical access. - Protection of monitoring systems - Records resulting from the operation of physical surveillance systems.
7.5 Protection against physical and environmental threats		Recommended	- Results of risk assessments regarding physical and environmental threats. - Designing appropriate protection measures against physical and environmental threats.

7.6 Working in safe areas		Possible	- Rules for working in safe areas (specifying specific safety precautions) - Security measures were implemented for safe areas.
7.7 Clean desk and clean screen		Recommended	- For example, in a subject-specific policy, there might be clean desk and clean screen rules. - Spot checks for clean desk and clean screen behaviors (e.g., workspaces and printers).
7.8 Equipment placement and protection		Possible	- Placement and protection rules - On-site checks regarding equipment placement and protection.
7.9. Security of assets outside the facility			- Rules regarding the use of assets outside the organization's facilities - Results of interviews or surveys conducted among personnel using assets outside the organization's facilities.
7.10 Storage medium	Possible		- Rules regarding the use of removable storage media can be outlined, for example, in a specific policy. - Device configurations (including encryption) to restrict or protect the transfer of information from removable storage media. - Safe disposal processes and records obtained from these processes.
7.11 Supporting services		Recommended	- Especially in data centers, installation protection measures (e.g., temperature, electricity supply, water) - Emergency provisions relating to the interruption of electricity, water, gas or other services.
7.12 Cabling safety		Possible	- Physical routing and protection of cabling.
7.13 Equipment maintenance			- Procedures for maintaining different types of equipment. - Equipment maintenance records
7.14 Safe disposal or reuse of equipment	Possible	Possible	- Rules regarding the disposal or reuse of equipment containing storage media. - Records relating to the physical or logical destruction of information or equipment.
8. Technological controls			
8.1 User endpoint devices	Possible		- Rules for secure configuration and processing of user endpoint devices, for example, a subject-specific policy. - End-user awareness activities covering security requirements and procedures for protecting user endpoint devices. - Where applicable, rules regarding the separation and protection of commercial information on private devices. - Design of secure computing devices that are permitted for remote use (e.g., laptops)
8.2 Privileged access rights	Possible		- For example, rules regarding the restricted allocation, use, and monitoring of privileged access rights in a subject-specific policy. - Authorization and review processes for managing privileged access rights.
8.3 Restrictions on access to information	Recommended		- Rules regarding restricting access to information and other related assets, for example, a subject-specific policy. - Access management techniques and processes for protecting access to sensitive information throughout its lifecycle (i.e., creation, processing, storage, transmission, destruction).
8.4 Access to source code	Recommended		- Procedures for managing read and write access to source code, development tools, and software libraries.

8.5 Secure authentication	Recommended		- Rules regarding authentication technologies and access control procedures, for example, in a subject-specific policy. - Implementing risk-based decisions and corresponding login procedures for systems or applications. - The use of strong or multi-factor authentication for critical information systems.
8.6 Capacity management	Possible		- Current and expected capacity requirements - Measurements of resource utilization, for example, computing facilities, human resources, offices, and other facilities. - Procedures for ensuring sufficient capacity or reducing capacity requirements
8.7 Protection against malware	Recommended		- Rules for protecting against malware. - Risk-based coverage of assets and the relevant configuration of malware detection software. - Other procedures and measures to protect information and other resources against malware. - End-user awareness activities regarding malware.
8.8 Managing technical security vulnerabilities	Recommended		- Gathering and managing information regarding technical vulnerabilities in the information systems used. - Results of vulnerability scans (performed regularly) or penetration tests - Assessment of the organization's vulnerability to technical vulnerabilities and planned mitigation measures. - The software update process ensures the installation of the most up-to-date approved patches and application updates.
8.9 Configuration management	Recommended		- Rules relating to the configuration of hardware, software, services, and networks, including security configurations. - Managing, implementing, or applying configurations, monitoring, and reviewing processes. - Standard templates for secure configuration (i.e., hardening) of hardware, software, services, and networks.
8.10 Deleting Information			- Rules for the timely deletion of information stored in information systems, devices, or other storage media, for example, according to a data retention-specific policy. - Procedures for securely deleting sensitive information from systems, applications, and services. - Third-party agreements where third parties store the organization's information and which include provisions for data deletion.
8.11 Data Masking			- Data masking rules, for example, according to the organization's subject-specific policy regarding access control. - The results of analyses conducted to identify where protecting sensitive information (e.g., PII) requires techniques such as data masking, aliasing, or anonymization. - Techniques used for data masking, aliasing, or anonymization.
8.12 Preventing data leakage	Possible		- Rules relating to data leakage prevention measures to be applied to systems, networks, and other devices that process, store, or transmit sensitive information. - Defined information requiring protection against leakage. - Leak channels were identified, along with measures including monitoring to prevent leaks. - Configuring the data loss prevention system.

8.13 Data backup	Recommended		- Rules for backing up information, software, and systems, for example, a policy specific to backup procedures. - Backup plans based on the organization's established business requirements. - Operational procedures for monitoring the timely and accurate execution of backups and troubleshooting failures. - Backup and restore tests are performed at regular intervals.
8.14 Redundancy of information processing facilities			- Determining the requirements regarding the availability of business services and information systems. - Architecture of high-requirement systems that provide adequate redundancy. - Results of the takeover tests conducted.
8.15 Login Records	Recommended		- Rules regarding the purpose for which log entries are created, the data collected, and specific requirements for processing log entries (e.g., a logging-specific policy) - A list of security entries and measures to ensure they are protected against unauthorized manipulation. - Procedures for performing systematic analysis and interpretation of incoming events, such as identifying unusual activities or abnormal behavior. - Configuration of input systems
8.16 Monitoring activities	Possible		- Rules for monitoring networks, systems, and applications for abnormal behavior. - The baselines of normal behavior were established, and criteria were derived to trigger warnings. - Monitoring logs kept for defined retention periods. - Results of the analysis conducted to identify abnormal behaviors.
8.17 Time synchronization	Possible		- List of reference time sources used by the organization - Clock synchronization methods and handling time differences.
8.18 Use of privileged utility programs	Possible		- List of utility programs used that may override system and application controls. - Processes, procedures, and other methods used to restrict and tightly control such utility programs.
8.19 Installing software on operating systems	Possible		- Procedures and precautions used to manage software installation on operating systems, including inventories of installed software along with their versions. - Rules regarding what types of software users can install. - Restrictions on software installation by persons other than trained administrators.
8.20 Network security	Recommended		- Rules for ensuring information security on networks and protecting connected services against unauthorized access. - Security measures and features implemented to protect information on networks support information processing facilities, such as configuration templates, configuration of cryptographic controls, gateway rule sets, and configuration examples of network devices. - Network architecture documentation (diagrams, configuration files, breakdown) - Rules for verifying network system connections
8.21 Network service security			- Rules regarding the secure use of networks and network services. - List of networks and network services used, along with security mechanisms and service levels. - Assurance obtained from network service providers.

8.22 Network Separation			- For example, rules for separating network areas according to trust, criticality and sensitivity levels, and issue-specific policy regarding access control. - Network topology (including wireless) and zone separation with a description of purposes and rules. - Definitions of security perimeters of network domains - Processes for managing security perimeters and firewall rules of network domains.
8.23 Web filtering	Possible		- Rules for the safe and appropriate use of online resources, including restrictions on unwanted or inappropriate websites. - Measures implemented to reduce exposure to malicious content on external websites (e.g., filtering rules) - All staff are provided with awareness and training activities on the safe and appropriate use of online resources.
8.24 The Use of Cryptography	Recommended		- Rules for the effective use of cryptography, including acceptable ciphers and key management, for example, in a topic-based policy on cryptography. - List of cryptographic techniques used by the organization - Standards, procedures, and methods for key management, including the creation, storage, archiving, retrieval, distribution, retrieval, and destruction of cryptographic keys.
8.25 Secure development lifecycle	Possible		- Secure software development guidelines to ensure information security is designed and implemented throughout the secure software development lifecycle. - The distinction between development, testing, and production environments. - Security processes and checkpoints that ensure information security requirements are adequately met throughout the entire software development process. - When software development is outsourced, assurance is obtained that information security requirements are properly addressed.
8.26 Application security requirements			- The process of defining application security requirements based on specific risk assessment. - Application risk assessments were conducted, identifying specific information security requirements. - Specifically, the requirements defined for a sample of the latest application developments/implementations for transactional services, electronic ordering and payment applications.
8.27 Secure system architecture and engineering principles			- Architectural and security engineering principles are created to ensure that information systems are designed, implemented, and operated securely throughout their development lifecycle. - Integration of safety engineering principles into software development. - An example of an application-specific safety practice that validates the use of the engineering principles above. - Where applicable, safe engineering principles embedded in outsourced development contracts.

8.28 Secure coding	Possible		- Rules regarding safe coding principles used in both new developments and reuse scenarios. - Processes to ensure the application of safe coding principles during planning and before coding, during coding, and during inspection and maintenance. - Applying specific secure coding principles to examples of recent development activities, including code scanning techniques. - Protection mechanisms for the code, including access restrictions.
8.29 Safety tests during development and acceptance phases	Recommended		- Security testing rules are used to verify that information security requirements are met when applications or code are deployed to a production environment. - Examples of requirements sets actually used for security testing and their corresponding test results. - Output and tracking from automated testing tools (e.g., code analysis tools, vulnerability scanners, functional tests).
8.30 External Development			- In outsourced system development, there are guidelines on how an organization should implement the information security measures it needs. - Procedures applied to direct, monitor, and review activities related to outsourced system development. - The result of monitoring or reviewing suppliers to ensure expectations are met.
8.31 Separation of development, testing and production environments	Possible		- Rules regarding the level of separation between production, testing, and development environments, including specific requirements for different development environments. - The distinction between development, testing, and production environments. - Protecting test and production environments (e.g., access restrictions, network isolation, ensuring that sensitive production information is not used)
8.32 Change management	Recommended		- Rules for managing changes to protect information security. - Change control procedures include, for example, documentation, specifications, testing, quality control, and managed implementation. - An example of a implemented change showing how the changes were tested, approved, and deployed.
8.33 Test information	Possible		- Rules for the proper selection, use, protection, and management of test data. - Procedures for protecting operational information during testing purposes (e.g., masking) - Examples of deleting data from test environments.
8.34 Protecting information systems during audit tests	Possible		- List of requests for audit tests or other assurance activities involving the evaluation of operational systems. - Examples of audit tests performed and how they were decided upon and conducted.
$^{\text{this}}$ column correspond to the control numbers in ISO/IEC 27001.2022, Annex A.			

Appendix F – Sector Group for Information Security Management System

Sector	Sector Group	Relevant Technical Scope	Sub-sector Area	Technological Field
Manufacturing Sector	**A**	01-Agriculture, Forestry 03-Food Products Manufacturing 30-Hotel Businesses and Restaurants	**A-01**	**TA1-TA2-TA3-TA4-TA5-TA6-TA7-TA8-TA9-TA10-TA11**
		02-Mining 15-Non-metallic products 16- Concrete, cement, lime, gypsum, plaster, etc.	**A-02**	
		04-05-Textile and Leather Products 06-Wood Products 14-Plastic and Rubber Products 23- Production of other unclassified products	**A-03**	
		07-Paper and Paper Products 08-09-Printing and Publishing	**A-04**	
		10-Petroleum Products 12-Manufacturing of Chemicals 13-Medicine	**A-05**	
		17-Manufacturing of Metal Products 18-Machinery and Equipment 19-Electrical and Optical Products 20- Shipbuilding 22-Manufacturing of Transportation Vehicles	**A-06**	
		25-26-27-Electricity, Gas and Water Supply	**A-07**	
		24-Recycling	**A-08**	
		28-Construction	**A-09**	
Service Sector	**B**	29-Wholesale and Retail Trade	**B.01**	**TA1-TA2-TA3-TA4-TA5-TA6-TA7-TA8-TA9-TA12**
		31-Transportation, Storage, Communication	**B.02**	
		34-Engineering Services	**B.03**	
		35-Other Services 39- Other social services	**B.04**	
Private Sectors	**C**	33-Information Technologies	**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 Services	**C.04**	
		38-Health	**C.05**	
		21-Aviation and Space	**C.06**	

11. REVISION INFORMATION

Revision Date	Revision No	Item No.	Explanation of the Revisions Made
01.03.2021	01	-	A major revision has been made.
August 20, 2022	02	-	The transition to ISO/IEC 27006:2015 has been completed.
08.11.2025	03	-	Transition to ISO/IEC 27006:2024 standard

Preparer	Approved
Management Representative	*General manager*