This assessment checklist contains 2 sections:

- SECTION 1 (page 02 to 23) – Assessment checklist for Information Security Management System (ISMS)
- SECTION 2 (page 24 to 33) – Assessment checklist for Privacy Information Management System (PIMS)

If your organisation is applying for or is accredited to ISMS only, please complete SECTION 1.

If your organisation is applying for or is accredited to both ISMS and PIMS, please complete both SECTION 1 and SECTION 2.

Certification Body	:	
Address	:	
Date of Assessment	:	
Type of Assessment	:	
Team Leader/Assessor	:	

SECTION 1

ASSESSMENT CHECKLIST FOR INFORMATION SECURITY MANAGEMENT SYSTEM CERTIFICATION BODY - ISO/IEC 27006:2015 Amendment 1 2020 INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF INFORMATION SECURITY MANAGEMENT SYSTEMS

Legend: C – Complies, O – Observation, T – To Address at Audit, N – Nonconformity, N/A – Not Applicable, F – Further information required

Section	Requirements	**Comments** (Manual and/or procedure references)	Finding
5	**GENERAL REQUIREMENTS**		
5.1	**Legal and Contractual Matters**		
	Does the CB comply with the requirements given in Clause 5.1 of ISO/IEC 17021-1?		
5.2	**Management of Impartiality**		
	Does the CB comply with the requirements given in Clause 5.2 of ISO/IEC 17021-1?		
5.2.1	**IS 5.2 Conflicts of Interest** Does the CB ensure that it does not provide internal information security reviews of the client's ISMS subject to certification? Is the CB independent from the body or bodies (including any individuals) which provide the internal ISMS audit?		
5.3	**Liability and Financing**		
	Does the CB comply with the requirements given in Clause 5.3 of ISO/IEC 17021-1?		
6	**STRUCTURAL REQUIREMENTS**		
	Does the CB comply with the requirements given in Clause 6 of ISO/IEC 17021-1?		
7	**RESOURCE REQUIREMENTS**		
7.1	**Competence of Personnel**		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
7.1.1	**IS 7.1.1 General Considerations**		
7.1.1.1	**Generic Competence Requirements** Does the CB ensure that it has knowledge of the technological, legal and regulatory developments relevant to the clients' ISMS?		
	Are competence requirements defined for each certification function as referenced in Table A.1 of ISO/IEC 17021-1?		
	Does it take into account the requirements that are relevant for the ISMS technical areas as determined by the CB?		
7.1.2	**IS 7.1.2 Determination of Competence Criteria**		
7.1.2.1	**Competence Requirements for ISMS Auditing**		
7.1.2.1.1	**General Requirements**		
	Has the CB established criteria for verifying the background experience, specific training or briefing of audit team members that ensures at least: (a) knowledge of information security; (b) technical knowledge of activity to be audited; (c) knowledge of management systems; (d) knowledge of principles of auditing; (e) knowledge of ISMS monitoring, measurement, analysis and evaluation. (a) to (e) apply to auditors being part of the audit team, with the except of (b), which can be shared among auditors being part of the team.		
	Is the audit team competent to trace indications of information security incidents in the client's ISMS back to the appropriate elements of the ISMS?		
	Does the audit team have appropriate work experience and practical application of the items a) to e) mentioned above?		
7.1.2.1.2	**Information Security Management Terminology, Principles, Practices and Techniques**		
	Does the CB ensure that all members of the audit team, *collectively* have knowledge of:		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
	(a) ISMS specific documentation structures, hierarchy and interrelationships; (b) Information security management related tools, methods, techniques and their application; (c) Information security risk assessment and risk management; (d) processes applicable to ISMS; (e) the current technology where information security may be relevant or an issue. Every auditor shall fulfil (a), (c), (d).		
7.1.2.1.3	**Information Security Management System Standards and Normative Documents**		
	(a) Does the CB ensure that all ISMS auditors have knowledge of all requirements contained in ISO/IEC 27001? (b) Collectively, do all members of the audit team have knowledge of all controls contained in ISO/IEC 27002 and their implementation?		
7.1.2.1.4	**Business Management Practices**		
	Does the CB ensure that all ISMS auditors have knowledge of: (a) industry information security good practices and information security procedures; (b) policies and business requirements for information security; (c) general business management concepts, practices and inter-relationship between policy, objectives and results; (d) management processes and related terminology.		
7.1.2.1.5	**Client Business Sector**		
	Does the CB ensure that all ISMS auditors have knowledge of: (a) legal and regulatory requirements in the particular information security field, geography and jurisdiction(s); (b) information security risks related to business sector; (c) generic terminology, processes and technologies related to the client business sector; (d) relevant business sector practices. Criteria (a) may be shared amongst the audit team.		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
7.1.2.1.6	**Client Products, Processes and Organisation**		
	Collectively, do CB auditors have knowledge of: (a) the impact of organization type, size, governance, structure, functions and relationships on development and implementation of the ISMS and certification activities, including outsourcing; (b) complex operations in a broad perspective; (c) legal and regulatory requirements applicable to the product or service.		
7.1.2.2	**Competence Requirements for Leading the ISMS Audit Team**		
	In addition to requirements in 7.1.2.1, do audit team leaders fulfil the following requirements which are demonstrated in audits under guidance and supervision? (a) knowledge and skills to manage the certification audit process and audit team; (b) capability to communicate effectively, both orally and in writing.		
7.1.2.3	**Competence Requirements for Conducting Application Review**		
	Do personnel conducting the application review to determine audit team competence required, to select the audit team members and to determine the audit time have knowledge of:		
7.1.2.3.1	**Information Security Management System Standards and Normative Documents**		
	Relevant ISMS standards and other normative documents used in the certification process.		
7.1.2.3.2	**Client Business Sector**		
	Generic terminology, processes, technologies and risk related to the client business sector.		
7.1.2.3.3	**Client Products, Processes and Organisation**		
	Client products, processes, organisation types, size, governance, structure, functions and relationships on development and implementation of the ISMS and certification activities, including outsourcing functions.		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
7.1.2.4	**Competence Requirements for Reviewing Audit Reports and Making Certification Decisions**		
7.1.2.4.1	General		
	Do personnel reviewing audit reports and making certification decisions have knowledge that enables them to verify the appropriateness of the scope of certification as well as changes to the scope and their impact on the effectiveness of audit, in particular in continuing validity of the identification of interfaces and dependencies and the associated risks.		
	In addition, do the personnel have knowledge of: (a) management systems in general; (b) audit processes and procedures; (c) audit principles, practices and techniques;		
7.1.2.4.2	**Information Security Management Terminology, Principles, Practices and Techniques**		
	(a) ISMS specific documentation structures, hierarchy and interrelationships; (b) Information security risk assessment and risk management; (c) processes applicable to ISMS; (d) legal and regulatory requirements relevant to information security. (e)		
7.1.2.4.3	**Information security management system standards and normative documents**		
	Relevant ISMS standards and other normative documents used in the certification process		
7.1.2.4.4	**Client Business Sector**		
	Generic terminology, and risks related to the relevant business sector practices.		
7.1.2.4.5	**Client Products, Processes and Organisation**		
	Client products, processes, organisation types, size, governance, structure, functions and relationships.		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
7.2	**Personnel Involved in the Certification Activities**		
	Does the CB comply with the requirements given in Clause 7.2 of ISO/IEC 17021-1?		
7.2.1	**IS 7.2 Demonstration of Auditor Knowledge and Experiences**		
	Does the CB demonstrate that the auditors have knowledge and experience through: (a) recognized ISMS-specific qualifications; (b) registration as auditor where applicable; (c) participation in ISMS training courses and attainment of relevant personal credentials; (d) up to date professional development records; (e) ISMS audits witnessed by another ISMS auditor.		
7.2.1.1	**Selecting of Auditors**		
	In addition to clause 7.2.1.1, does the CB ensure that each auditor: (a) Has professional education or training to an *equivalent* level of university education; (b) Has at least four years full time practical workplace experience in information technology, of which at least two years are in a role of function relating to information security; (c) Has successfully completed at least five days of training, the scope of which covers ISMS audits and audit management; (d) Has gained experience of auditing ISMS prior to acting as an auditor performing ISMS audits. This experience shall be gained by performing as an auditor-in-training monitored by an ISMS evaluator (see ISO/IEC 17021-1:2015, Clause 9.2.2.1.4) in at least one ISMS initial certification audit (stage 1 and stage 2) or re-certification and at least one surveillance audit. This experience shall be gained in at least 10 ISMS on-site audit days and performed in the last 5 years. The participation shall include review of documentation and risk assessment, implementation assessment and audit reporting. (e) Has relevant and current experience; (f) Keeps current knowledge and skills in information security and auditing up to date through continual professional development. (g) Has competence in auditing an ISMS in accordance with ISO/IEC 27001.		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
	Do the technical experts comply with criteria a), b) and e) above?		
7.2.1.2	**Selecting Auditors for Leading the Team**		
	Does the CB criteria for selecting an audit team leader ensure that this auditor has actively participated in **all stages of at least 3 ISMS audits**, where the participation includes initial scoping and planning, review of documentation and risk assessment, implementation assessment and formal audit reporting?		
7.3	**Use of individual external auditors and external technical experts**		
	Does the CB comply with the requirements of clause 7.3 in ISO/IEC 17021-1?		
7.3.1	**IS 7.3 Using the external auditors or external technical experts as part of the audit team**		
	Do the technical experts work under the supervision of an auditor? (refer to 7.2.1.1 for the minimum requirements for technical experts)		
7.4	**Personnel Records**		
	Does the CB comply with the requirements of clause 7.4 in ISO/IEC 17021-1?		
7.5	**Outsourcing**		
	Does the CB comply with the requirements of clause 7.5 in ISO/IEC 17021-1?		
8	**INFORMATION REQUIREMENTS**		
8.1	**Public Information**		
	Does the CB comply with the requirements given in Clause 8.1 of ISO/IEC 17021-1?		
8.2	**Certification Documents**		
	Does the CB comply with the requirements given in Clause 8.2 of ISO/IEC 17021-1?		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
8.2.1	**IS 8.2 ISMS Certification Documents**		
	Are the certification documents signed by an officer who has been assigned such responsibility?		
	Does the CB include the version of Statement of Applicability in the certification documents? The certification documents may reference national and international standards as source(s) of control set for controls that are determined as necessary in the organization's Statement of Applicability in accordance with ISO/IEC 27001:2013, 6.1.3d. Is the reference on the certification documents clearly stated as being only a control set source for controls applied in the Statement of Applicability and not a certification thereof?		
8.3	**Reference to Certification and Use of Marks**		
	Does the CB comply with the requirements given in Clause 8.3 of ISO/IEC 17021-1?		
8.4	**Confidentiality**		
	Does the CB comply with the requirements given in Clause 8.4 of ISO/IEC 17021-1?		
8.4.1	**IS 8.4 Access to organisational records**		
	Before the certification audit, does the CB request the client to report if any ISMS related information that cannot be made available for review by the audit team because it contains confidential or sensitive information before the certification audit?		
	Does the CB determine whether the ISMS can be adequately audited in the absence of such information?		
	Does the CB advise the client that the certification audit cannot take place until appropriate access arrangements are granted, when the CB		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
	concludes that it is not possible to adequately audit the ISMS without reviewing the identified confidential or sensitive information.		
8.5	**Information Exchange Between a Certification Body and its Clients**		
	Does the CB comply with the requirements given in Clause 8.5 of ISO/IEC 17021-1?		
9	**PROCESS REQUIREMENTS**		
9.1	**Pre-Certification Activities**		
9.1.1	**Application**		
	Does the CB comply with the requirements given in Clause 9.1.1 of ISO/IEC 17021?		
9.1.1.1	**IS 9.1.1 Application Readiness** Does the CB require the client to have a documented and implemented ISMS which conforms to ISO/IEC 27001 and other documents required for certification.		
9.1.2	**Application Review**		
	Does the CB comply with the requirements given in Clause 9.1.2 of ISO/IEC 17021?		
9.1.3	**Audit Programme**		
	Does the CB comply with the requirements given in Clause 9.1.3 of ISO/IEC 17021?		
9.1.3.1	**IS 9.1.3 General**		
	Does the audit programme for ISMS audits take in account the determined information security controls?		
9.1.3.2	**IS 9.1.3 Audit Methodology**		
	Does the CB ensure that their procedures do not presuppose a particular manner of implementation of an ISMS or a particular format of documentation and records?		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
	Do the certification procedures focus on establishing that a client's ISMS meets the requirements specified in ISO/IEC 27001 and the policies and objectives of the client?		
9.1.3.3	**IS 9.1.3 General Preparations for the Initial Audit**		
	Does the CB require that a client makes all necessary arrangements for the access to internal audit reports and reports of independent review of information security? Does the information provided by the client during stage 1 of the certification audit includes: (a) general information concerning the ISMS and the activities it covers; (b) a copy of the required ISMS documentation specified in ISO/IEC 27001 and, where required, associated documentation?		
9.1.3.4	**IS 9.1.3 Review Periods**		
	Does the CB ensure that it does not certify an ISMS unless it has been operated through at least one management review and one internal ISMS audit covering the scope of certification?		
9.1.3.5	**IS 9.1.3 Scope of Certification**		
	Does the audit team audit the ISMS of the client covered by the defined scope against all applicable certification requirements? Does the CB confirm, in the scope of the client ISMS, that the client address the requirements stated in clause 4.3 of ISO/IEC 27001?		
	Does the CB ensure that the client's information security risk assessment and risk treatment properly reflects its activities and extends to the boundaries of its activities as defined in the scope of certification? Does the CB confirm that this is reflected in the client's scope of their ISMS and Statement of Applicability? Does the CB verify that there is at least one Statement of Applicability per scope of certification?		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
	Does the CB ensure that interfaces with services or activities that are not completely within the scope of the ISMS are addressed within the ISMS subject to certification and are included in the client's information security risk assessment?		
9.1.3.6	**IS 9.1.3 Certification Audit Criteria**		
	Is the criteria against which the ISMS of the client audited be the ISMS standard ISO/IEC 27001?		
9.1.4	**Determining Audit Time**		
	Does the CB comply with the requirements given in Clause 9.1.4 of ISO/IEC 17021?		
9.1.4.1	**IS 9.1.4 Audit Time**		
	Does the CB allow auditors sufficient time to undertake all activities relating to an initial audit, surveillance audit or re-certification audit? Does the calculation of the overall audit time include sufficient time for audit reporting? Does the CB use Annex B of ISO/IEC 27006:2015 Amd 1:2020 to determine the audit time? Note: Annex C provides further guidance on audit time calculations		
9.1.5	**Multi-site Sampling**		
	Does the CB comply with the requirements given in Clause 9.1.5 of ISO/IEC 17021?		
9.1.5.1	**IS 9.1.5 Multi Sites**		
9.1.5.1.1	Does the CB use a sample-based approach for multiple-site certification audit, where a client has a number of sites meeting the criteria below: (a) all sites are operating under the same ISMS, which is centrally administrated and audited and subject to central management review; (b) all sites are included within the client's internal ISMS audit programme;		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
	(c) all sites are included within the client's internal ISMS management review programme? (d)		
9.1.5.1.2	When a sample based approach is used, does the CBs have procedures in place to ensure the following: (a) The initial contract review has identified, to the greatest extent possible, the difference between sites such that an adequate level of sampling is determined; (b) A representative number sites is sampled by taking into account various factors listed in the standard; (c) A representative sample is selected from all sites within the scope of the client's ISMS, and the selections based upon judgmental choice to reflect the factors above, as well as a random element; (d) Every site included in the ISMS which is subject to significant risks is audited by the CB prior to certification; (e) The audit programme has been designed in light of above requirements and covers representative samples of the scope of ISMS certification within the three-year period; (f) In case of nonconformity being observed, either at head office or at single site, the corrective action procedure applies to the head office and all sites covered by the certificate.		
	Does the audit address the client's head office activities to ensure that a single ISMS applies to all sites and delivers central management at operational level?		
9.1.6	**Multiple Management Systems**		
	Does the CB comply with the requirements given in Clause 9.1.6 of ISO/IEC 17021?		
9.1.6.1	**IS 9.1.6 Integration of ISMS Documentation with that for other Management Systems**		
	The CB may accept documentation that is combined as long as the ISMS can be clearly identified together with the appropriate interfaces to the other systems.		
9.1.6.2	**IS 9.1.6 Combining Management System Audits**		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
	Are all elements important to an ISMS appear clearly and be readily identifiable in audit reports? Does the CB ensure that the quality of ISMS audit is not adversely affected by the combination of other management system audits?		
9.2	**Planning Audits**		
9.2.1	**Determining Audit Objectives, Scope and Criteria**		
	Does the CB comply with the requirements given in Clause 9.2.1 of ISO/IEC 17021-1?		
9.2.1.1	**IS 9.2.1 Audit Objectives**		
	Do the audit objectives include the determination of the effectiveness of the management system to ensure that the client, based on the risk assessment, has implemented applicable controls and achieved the established information security objectives?		
9.2.2	**Audit Team Selection and Assignments**		
	Does the CB comply with the requirements given in Clause 9.2.2 of ISO/IEC 17021-1?		
9.2.2.1	**IS 9.2.2 Audit Team**		
	Is the audit team are formally appointed and provided with the appropriate working documents? Is the mandate given to the audit team clearly defined and made known to the client?		
9.2.2.2	**IS 9.2.2 Audit Team Competence**		
	When selecting and managing the audit team to be appointed for a specific certification audit, does the CB ensure that the competencies brought to each assignment are appropriate? Does the audit team have: (a) Appropriate technical knowledge of specific activities within the scope of ISMS for which certification is sought and, where relevant, with associated procedures and their potential information security risks;		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
	(b) Understanding of the client sufficient to conduct a reliable certification audit of its ISMS given the ISMS' scope and context within the organization in managing the information security aspects of its activities, products and services; (c) Appropriate understanding of the legal and regulatory requirements applicable to the client's ISMS.		
9.2.3	**Audit Plan**		
	Does the CB comply with the requirements given in Clause 9.2.3 of ISO/IEC 17021-1?		
9.2.3.1	**IS 9.2.3 General**		
	Does the audit plan take into account the determined information security controls?		
9.2.3.2	**IS 9.2.3 Network-assisted Techniques**		
	Does the audit plan identify the network-assisted auditing techniques that will be utilised during the audit, as appropriate?		
9.2.3.3	**IS 9.2.3 Timing of Audit**		
	Has the CB agreed with the organisation to be audited the timing of the audit which will best demonstrate the full scope of the organisation? Considerations could include season, month, day/dates and shift as appropriate.		
9.3	**Initial Certification**		
	Does the CB comply with the requirements given in Clause 9.3 of ISO/IEC 17021-1?		
9.3.1.1	**IS 9.3.1.1 Stage 1**		
	Does the CB obtain documentation on the design of the ISMS covering the documentation required in ISO/IEC 27001 during the stage 1 audit?		
	Does the CB obtain a sufficient understanding of the design of the ISMS in the context of the client's organisation, risk assessment and treatment,		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
	information security policy and objectives and, in particular, of the client's preparedness for the audit?		
	Are results of the stage 1 audit documented in a written report?		
	Does the CB review the stage 1 audit report before deciding on proceeding with stage 2 and confirm if the stage 2 audit team members have the necessary competence; this may be done by the auditor leading the team that conducted the stage 1 audit if deemed competent and appropriate.		
	Does the CB make the client aware of the further types of information and records that may be required for detailed examination during stage 2?		
9.3.1.2	**IS 9.3.1.1 Stage 2**		
9.3.1.2.1	Does the CB develop an audit plan for the conduct of stage 2 on the basis of findings documented in the stage 1 audit report?		
	Are the objectives of stage 2 audit to: (a) Evaluate the effective implementation of the ISMS; (b) Confirm that the client adheres to its own policies, objectives and procedures?		
9.3.1.2.2	Does the stage 2 audit focus on the client's: (a) Top management leadership and commitment to information security policy and objectives; (b) Documentation requirements listed in ISO/IEC 27001; (c) Assessment of information security related risks and that the assessments produce consistent, valid and comparable results if repeated; (d) Determination of control objectives and controls based on the information security risk assessment and risk treatment processes; (e) Information security performance and effectiveness of the ISMS, evaluating against the information security objectives (f) Correspondence between the determined controls, the Statement of Applicability and the results of the information security risk assessment, treatment process and policy and objectives;		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
	(g) Implementation of controls (refer to Annex D of ISO/IEC 27006), taking into account the external and internal context and related risks, the organization's monitoring, measurement and analysis of information security processes and controls, to determine whether controls are implemented and effective and meet their stated information security objectives; (h) Programmes, process, procedures, records, internal audits and reviews of ISMS effectiveness to ensure that these are traceable to top management decisions and the information security policy and objectives.		
9.4	**Conducting Audits**		
	Does the CB comply with the requirements given in Clause 9.4 of ISO/IEC 17021-1?		
9.4.1	**IS 9.4 General**		
	Does the CB have documented procedures for:		
	(a) Initial certification of a client's ISMS, in accordance with the provisions of ISO/IEC 17021-1?		
	(b) Surveillance and Re-Certification audits for a client's ISMS in accordance with ISO/IEC 17021-1 on a periodic basis for continuing conformity with relevant requirements and for verifying and recording that a client takes corrective action on a timely basis to correct all nonconformities.		
9.4.2	**IS 9.4 Specific elements of the ISMS audit**		
	Does the CB, represented by the audit team: (a) Require the client to demonstrate that the assessment of information security related risks is relevant and adequate for the ISMS operation within the ISMS scope; (b) Establish whether the client's procedures for the identification, examination and evaluation of information security related risks and the results of their implementation are consistent with the client's policy, objectives and targets.		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
	Does the CB also establish whether the procedures employed in risk assessment are sound and properly implemented?		
9.4.3	**IS 9.4 Audit Report**		
9.4.3.1	In addition to the requirements in clause 9.4.8 of ISO/IEC 17021-1, do the audit reports provide the following information of a reference to it? (a) An account of the audit including a summary of the document review; (b) An account of the certification audit of the client's information security risk analysis; (c) Deviations from the audit plan; (d) The ISMS' scope		
9.4.3.2	Are audit reports of sufficient detail to facilitate and support the certification decision?		
	Do audit reports contain the following: (a) Significant audit trails followed and audit methodologies utilized; (b) Observations made, both positive and negative; (c) Comments on the conformity of the client's ISMS with the certification requirements with a clear statement of nonconformity, a reference to the version of the Statement of Applicability and, where applicable, any useful comparison with the results of previous certification audits of the client.		
	Are completed questionnaires, checklists, observations, logs or auditor notes submitted to the CB as evidence to support the certification decision?		
	Do the audit reports (or other certification documents) include information about the samples evaluated?		
	Do the audit reports consider the adequacy of the internal organization and procedures adopted by the client to give confidence in the ISMS?		
	Do the audit reports cover:		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
	(a) A summary of the most important observations, positive as well as negative, regarding the implementation and effectiveness of the ISMS requirements and IS controls; (b) Audit team's recommendation as to whether the client's ISMS should be certified or not, with information to substantiate this recommendation.		
9.5	**Certification Decision**		
	Does the CB comply with the requirements given in Clause 9.5 of ISO/IEC 17021-1?		
9.5.1	**IS 9.5 Certification Decision**		
	Are certification decisions based, in addition to the requirements of ISO/IEC 17021-1, on the certification recommendation of the audit team as provided in their certification audit report (see 9.4.3).		
	When a person or committee takes the decision on granting certification which overturns a negative recommendation of the audit team, does the CB document and justify the basis for the decision to overturn the recommendation?		
	Does the CB ensure that certification is not granted to the client until there is sufficient evidence to demonstrate that arrangements for management reviews and internal ISMS audits have been implemented, are effective and will be maintained?		
9.6	**Maintaining Certification**		
9.6.1	**General**		
	Does the CB comply with the requirements given in Clause 9.6.1 of ISO/IEC 17021-1?		
9.6.2	**Surveillance activities**		
	Does the CB comply with the requirements given in Clause 9.6.2 of ISO/IEC 17021-1?		
9.6.2.1.1	**IS 9.6.2 Surveillance Activities**		
	Are the surveillance audit procedures consistent with those concerning the certification audit of the client's ISMS as described in this standard?		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
	Do surveillance audit programmes cover at least:		
	(a) The system maintenance elements such as information security risk assessment and control maintenance, internal ISMS audit, management review and corrective action;		
	(b) Communications from external parties as required by ISO/IEC 27001 and other documents required for certification;		
	(c) Changes to the documented system;		
	(d) Areas subjected to change;		
	(e) Selected requirements of ISO/IEC 27001;		
	(f) Other selected areas as appropriate.		
9.6.2.1.2	As a minimum, does the CB review the following at every surveillance?		
	(a) Effectiveness of the ISMS with regard to achieving the objectives of the client's information security policy;		
	(b) The functioning of procedures for the periodic evaluation and review of compliance with relevant information security legislation and regulations;		
	(c) Changes to the controls determined, and resulting changes to the SoA;		
	(d) Implementation and effectiveness of controls according to the audit programme.		
9.6.2.1.3	Is the CB able to adapt its surveillance programme to the information security issues related to risks and impacts on the client and justify this programme?		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
	If surveillance audits are combined with audits of other management systems, does the reporting clearly indicates the aspects relevant to each management system?		
	Does the CB check the records of appeals and complaints brought before the CB and, where any nonconformity or failure to meet the requirements of certification is revealed, and that the client has investigated its own ISMS and procedures and taken appropriate corrective action?		
	Do the surveillance reports contain, in particular, information on clearing of nonconformities revealed previously and the version of the SoA and important changes from the previous audit?		
	Do the surveillance reports, as a minimum, build up to cover in totality the requirements of 9.6.2.1.1 and 9,6.2.1.2 above?		
9.6.3	**Re-certification**		
	Does the CB comply with the requirements given in Clause 9.6.3 of ISO/IEC 17021-1?		
9.6.3.1	**IS 9.6.3 Re-certification Audits**		
	Are re-certification audit procedures consistent with those concerning the certification audit of the client's ISMS as described in this standard?		
	Is the time allowed to implement corrective action consistent with the severity of the nonconformity and the associated information security risk?		
9.6.4	**Special Audits**		
	Does the CB comply with the requirements given in Clause 9.6.4 of ISO/IEC 17021-1?		
9.6.4.1	**IS 9.6.4 Special Cases**		
	Are activities necessary to perform special audits subjected to special provisions, if a client with a certified ISMS makes major nonconformities to its system or if other changes take place which could affect the basis of its certification?		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
9.6.5	**Suspending, Withdrawing or Reducing the Scope of Certification**		
	Does the CB comply with the requirements given in Clause 9.6.5 of ISO/IEC 17021-1?		
9.7	**Appeals**		
	Does the CB comply with the requirements given in Clause 9.7 of ISO/IEC 17021-1?		
9.8	**Complaints**		
	Does the CB comply with the requirements given in Clause 9.8 of ISO/IEC 17021-1?		
9.8.1	**IS 9.8 Complaints**		
	Complaints represent a potential incident and an indication to possible nonconformity.		
9.9	**Client Records**		
	Does the CB comply with the requirements given in Clause 9.9 of ISO/IEC 17021-1?		
10	**Management system requirements for certification bodies**		
10.1	**Options**		
	Does the CB comply with the requirements given in Clause 10.1 of ISO/IEC 17021-1?		
10.1.1	**IS 10.1 ISMS Implementation**		
	It is *recommended* that the CB implement an ISMS in accordance with ISO/IEC 27001.		
10.2	**Option A: General Management System Requirements**		
	Does the CB comply with the requirements given in Clause 10.2 of ISO/IEC 17021-1?		
10.3	**Option B: Management System Requirements in Accordance with ISO 9001**		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
	Does the CB comply with the requirements given in Clause 10.3 of ISO/IEC 17021-1?		

SECTION 2

ASSESSMENT CHECKLIST FOR PRIVACY INFORMATION MANAGEMENT SYSTEM CERTIFICATION BODY - ISO/IEC TS 27006-2:2021 - REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF INFORMATION SECURITY MANAGEMENT SYSTEMS – PART 2: PRIVACY INFORMATION MANAGEMENT SYSTEMS

Legend: C – Complies, O – Observation, T – To Address at Audit, N – Nonconformity, N/A – Not Applicable, F – Further information required

Section	Requirements	**Comments** (Manual and/or procedure references)	Finding
5	**GENERAL REQUIREMENTS**		
5.1	**Legal and Contractual Matters**		
	Does the CB comply with the requirements given in Clause 5.1 of 27006:2015 Amendment 1 2020?		
	PS 5.1 Normative basis for this document		
	All requirements from ISO/IEC 27006 apply unless otherwise specified.		
5.2	**Management of Impartiality**		
	Does the CB comply with the requirements given in Clause 5.2 of ISO/IEC 27006:2015 Amendment 1 2020?		
	PS 5.2 Conflicts of Interest		
	Does the CB ensure that it does not provide management system consultancy related to PIMS (e.g. services as external data protection officer, process reviews or data protection reviews)?		
5.3	**Liability and Financing**		
	Does the CB comply with the requirements given in Clause 5.3 of ISO/IEC 27006:2015 Amendment 1 2020?		
6	**STRUCTURAL REQUIREMENTS**		
	Does the CB comply with the requirements given in Clause 6 of 27006:2015 Amendment 1 2020?		
7	**RESOURCE REQUIREMENTS**		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
7.1	**Competence of Personnel**		
7.1.1	**PS 7.1.1 General Considerations**		
	Does the CB comply with the requirements given in Clause 7.1.1 of 27006:2015 Amendment 1 2020?		
7.1.2	**PS 7.1.2 Determination of Competence Criteria**		
	Does the CB comply with the requirements given in Clause 7.1.2 of 27006:2015 Amendment 1 2020?		
7.1.2.1.1	**PS 7.1.2.1 Competence requirements for PIMS auditing**		
	Has the CB established criteria for verifying the background experience, specific training or briefing of audit team members that ensures auditors have knowledge of: (a) privacy information management including ISO/IEC 27701 (b) identification and handling of personally identifiable information (PII); (c) privacy by design and by default; (d) PIMS monitoring, measurement, analysis and evaluation; (e) information security risks related to privacy information management and processing of PII; (f) policies and business requirements for privacy information management.		
7.1.2.1.2	**Information Security Management Terminology, Principles, Practices and Techniques**		
	Does the CB ensure that all members of the audit team, *collectively* have knowledge of: (a) privacy information management and processing of PII related tools, methods, techniques and their application; (b) tracing privacy incidents; (c) privacy information risk assessment, privacy impact assessment and the related methods and risk management; (d) processes applicable to PIMS; (e) the current technology where privacy may be relevant or an issue; (f) all controls contained in ISO/IEC 27701 and their implementation;		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
	(g) the legal requirements that apply to privacy information management and/or processing of PII (e.g. sector specific laws and local privacy laws); (h) industry privacy good practices and privacy procedures.		
7.1.2.2	**PS 7.1.2.4 Competence requirements for reviewing audit reports and making certification decisions**		
	Does the CB ensure that personnel reviewing audit reports and making certification decisions have knowledge of: (a) the privacy framework presented in ISO/IEC 29100; (b) ISO/IEC 27701; (c) legal and regulatory requirements relevant to privacy; (d) scope definition for management systems according to ISO/IEC 27701 (in particular in terms of PII controllers and PII processors) to be able to verify the appropriateness of the scope as well as changes to the scope. Does the CB ensure that personnel reviewing audit reports and making certification decisions have general understanding of: (a) privacy information risk assessment, privacy impact assessment and risk management; (b) processes applicable to PIMS.		
7.2	**Personnel Involved in the Certification Activities**		
	Does the CB comply with the requirements given in Clause 7.2 of 27006:2015 Amendment 1 2020?		
7.2.1	**PS 7.2 Demonstration of auditor knowledge and experience**		
	Does the CB demonstrate that the auditors have necessary knowledge and experience through (where applicable): (a) recognized PIMS-specific qualifications; (b) participation in PIMS training courses and attainment of relevant personal credentials; (c) PIMS audits witnessed by another PIMS auditor.		
7.2.2	**PS 7.2.1.1 Selecting auditors**		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
	In addition to clause 7.1.2.1, does the CB ensure that each PIMS auditor: (a) has at least four years full-time practical workplace experience in information technology, of which at least two years was in a role or function relating to privacy; (b) has completed at least one onsite audit in the field of PIMS; (c) keep current knowledge and skills in privacy information management up to date through continual professional development.		
	Do the technical experts comply with criteria (a) above?		
7.3	**Use of individual external auditors and external technical experts**		
	Does the CB comply with the requirements of clause 7.3 of 27006:2015 Amendment 1 2020?		
7.4	**Personnel Records**		
	Does the CB comply with the requirements of clause 7.4 of 27006:2015 Amendment 1 2020?		
7.5	**Outsourcing**		
	Does the CB comply with the requirements of clause 7.5 of 27006:2015 Amendment 1 2020?		
8	**INFORMATION REQUIREMENTS**		
8.1	**Public Information**		
	Does the CB comply with the requirements given in Clause 8.1 of 27006:2015 Amendment 1 2020?		
8.2	**Certification Documents**		
	Does the CB comply with the requirements given in Clause 8.2 of ISO/IEC 27006:2015 Amendment 1 2020?		
8.2.1	**PS 8.2 PIMS Certification documents**		
	Do the certification documents identify that the organization is either or both a PII controller and a PII processor within the scope of the certification?		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
	Does the CB include the version of Statement of Applicability for ISO/IEC 27001 on which the ISO/IEC 27701 certification is based and that the organization conforms to ISO/IEC 27701? If issued separately, the SoA for ISO/IEC 27701 shall be included in the certification documents. The effective date of ISO/IEC 27701 certification shall not exceed the date of the ISO/IEC 27001 certification on which it is based. Do the Certification documents include the following: (a) the words privacy information management system; (b) the role of the organization for each activity, product or service in scope (i.e. if the organization acts as PII controller and/or PII processor); (c) the fact that the certified organization fulfils both ISO/IEC 27001 and ISO/IEC 27701.		
8.3	**Reference to Certification and Use of Marks**		
	Does the CB comply with the requirements given in Clause 8.3 of ISO/IEC 27006:2015 Amendment 1 2020?		
8.4	**Confidentiality**		
	Does the CB comply with the requirements given in Clause 8.4 of ISO/IEC 27006:2015 Amendment 1 2020?		
8.5	**Information Exchange Between a Certification Body and its Clients**		
	Does the CB comply with the requirements given in Clause 8.5 of ISO/IEC 27006:2015 Amendment 1 2020?		
9	**PROCESS REQUIREMENTS**		
9.1	**Pre-Certification Activities**		
9.1.1	**Application**		
	Does the CB comply with the requirements given in Clause 9.1.1 of ISO/IEC 27006:2015 Amendment 1 2020?		
9.1.2	**Application Review**		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
	Does the CB comply with the requirements given in Clause 9.1.2 of ISO/IEC 27006:2015 Amendment 1 2020?		
9.1.3	**Audit Programme**		
	Does the CB comply with the requirements given in Clause 9.1.3 (except 9.1.3.6) of ISO/IEC 17021?		
9.1.3.1.1	**PS 9.1.3 Scope of certification**		
	Does CB ensure that the scope of the ISO/IEC 27701 certification is within or identical to the scope of the ISO/IEC 27001 certification, and also ensure that the scope of certification to ISO/IEC 27701 is included within boundaries of the activities of the client as defined in the scope of the PIMS?		
9.1.3.1.2	**Specific elements of the PIMS audit**		
	Does the audit programme for PIMS audit identify the role of the client as a PII controller and/or PII processor? Does the CB confirm in the scope of the client PIMS, that PII processing is in the scope? Does the CB ensure that the client's information security and privacy risk assessment and risk treatment properly reflect its activities and extend to the boundaries of its activities as defined in the scope of the PIMS. Certification bodies shall confirm that this is reflected in the client's scope of their PIMS and statement of applicability.		
9.1.3.2	**PS 9.1.3 Certification audit criteria**		
	Does the CB ensure that the criteria against which the PIMS of a client shall be ISO/IEC 27001 extended by ISO/IEC 27701?		
9.1.4	**Determining Audit Time**		
	Does the CB comply with the requirements given in Clause 9.1.4 of ISO/IEC 27006:2015 Amendment 1 2020?		
9.1.4	**PS 9.1.4 Audit time**		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
	Does the CB identify additional audit time to be spent on ISO/IEC 27701 certification audits audits (including initial certification, surveillance and re-certification)? Is the audit time needed for PIMS-specific aspects at least; - 30% of audit time if client is a PII controller; - 20% of audit time if client is a PII processor; - 50% of audit time if client is both PII controller and processor; calculated for the identical ISO/IEC 27001 certification scope, based on ISO/IEC 27006:2015, 9.1.4 and Annex B of ISO/IEC 27006:2015 Amd 1:2020? Is the additional time for an initial PIMS audit at least 2.5 days for PII processors, 3 days for PII controllers or 3.5 days for both, if the values calculated from the previous paragraph are lower? In the case that the organisation has already been certified to ISMS (ISO/IEC 27001) and a PIMS initial audit is conducted separately from ISMS audits (i.e. ISMS surveillance audit or ISMS recertification audit), is there at least 0.5 audit days added to the audit time in order to verify if the ISMS (especially its management system aspects such as internal audit and management review) is extended to include PIMS perspectives as specified in ISO/IEC 27701? Does the calculation of the overall audit time include sufficient time for audit reporting?		
9.1.5	**Multi-site Sampling**		
	Does the CB comply with the requirements given in Clause 9.1.5 of ISO/IEC 27006:2015 Amendment 1 2020?		
9.1.6	**Multiple Management Systems**		
	Does the CB comply with the requirements given in Clause 9.1.6 of ISO/IEC 27006:2015 Amendment 1 2020?		
9.2	**Planning Audits**		
9.2.1	**Determining Audit Objectives, Scope and Criteria**		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
	Does the CB comply with the requirements given in Clause 9.2.1 of ISO/IEC 27006:2015 Amendment 1 2020?		
9.2.2	**Audit Team Selection and Assignments**		
	Does the CB comply with the requirements given in Clause 9.2.2 of ISO/IEC 27006:2015 Amendment 1 2020?		
9.2.3	**Audit Plan**		
	Does the CB comply with the requirements given in Clause 9.2.3 of ISO/IEC 27006:2015 Amendment 1 2020?		
9.2.3	**PS 9.2.3 General**		
	Does the audit plan take into account the PIMS controls?		
9.3	**Initial Certification**		
	Does the CB comply with the requirements given in Clause 9.3 of ISO/IEC 27006:2015 Amendment 1 2020?		
9.4	**Conducting audits**		
9.4.1	**IS 9.4 General**		
	Does the CB comply with the requirements given in Clause 9.4.1 of ISO/IEC 27006:2015 Amendment 1 2020?		
9.4.2	**IS 9.4 Specific elements of the ISMS audit**		
	Does the CB comply with the requirements given in Clause 9.4.2 of ISO/IEC 27006:2015 Amendment 1 2020?		
9.4.3	**IS 9.4 Audit Report**		
	Does the CB comply with the requirements given in Clause 9.4.3 of ISO/IEC 27006:2015 Amendment 1 2020?		
	PS IS 9.4 Audit Report		
	Do audit reports contain the following: (a) The role of the client (PII controller, PII processor or both) shall be described in the audit report.		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
	(b) The audit report shall provide the overview of the audit of the client's privacy impact assessment, or a reference to it.		
9.5	**Certification Decision**		
	Does the CB comply with the requirements given in Clause 9.5 of ISO/IEC 27006:2015 Amendment 1 2020?		
	PS 9.5 Certification decision		
	Does the CB consider the impact that a nonconformity found for ISO/IEC 27701 requirements will affect on the conformity for ISO/IEC 27001, and report accordingly?		
9.6	**Maintaining Certification**		
9.6.1	**General**		
	Does the CB comply with the requirements given in Clause 9.6.1 of ISO/IEC 27006:2015 Amendment 1 2020?		
9.6.2	**Surveillance activities**		
	Does the CB comply with the requirements given in Clause 9.6.2 of ISO/IEC 27006:2015 Amendment 1 2020?		
9.6.3	**Re-certification**		
	Does the CB comply with the requirements given in Clause 9.6.3 of ISO/IEC 27006:2015 Amendment 1 2020?		
9.6.4	**Special Audits**		
	Does the CB comply with the requirements given in Clause 9.6.4 of ISO/IEC 27006:2015 Amendment 1 2020?		
9.6.5	**Suspending, Withdrawing or Reducing the Scope of Certification**		
	Does the CB comply with the requirements given in Clause 9.6.5 of ISO/IEC 27006:2015 Amendment 1 2020?		
	PS 9.6.5 Suspending, withdrawing or reducing the scope of certification		

Section	Requirements	Comments (Manual and/or procedure references)	Finding
	Does the CB also suspend, withdraw or reduce the scope of certification of ISO/IEC 27701 where its base ISO/IEC 27001 certification is suspended, withdrawn or its scope (which includes the scope of ISO/IEC 27701 certification) is reduced?		
9.7	**Appeals**		
	Does the CB comply with the requirements given in Clause 9.7 of ISO/IEC 27006:2015 Amendment 1 2020?		
9.8	**Complaints**		
	Does the CB comply with the requirements given in Clause 9.8 of ISO/IEC 27006:2015 Amendment 1 2020?		
9.9	**Client Records**		
	Does the CB comply with the requirements given in Clause 9.9 of ISO/IEC 27006:2015 Amendment 1 2020?		
10	**Management system requirements for certification bodies**		
10.1	**Options**		
	Does the CB comply with the requirements given in Clause 10.1 of ISO/IEC 27006:2015 Amendment 1 2020?		
10.2	**Option A: General Management System Requirements**		
	Does the CB comply with the requirements given in Clause 10.2 of ISO/IEC 27006:2015 Amendment 1 2020?		
10.3	**Option B: Management System Requirements in Accordance with ISO 9001**		
	Does the CB comply with the requirements given in Clause 10.3 of ISO/IEC 27006:2015 Amendment 1 2020?		