Annex II(F2)
Management System Checklist
(for ISMS certification)

The information security management system certification body shall complete the following checklist, which will be used for the assessment of the information security management system certification body's conformity with HKAS and HKCAS accreditation requirements.

This checklist consists of questions based on the requirements of ISO/IEC 27006-1: 2024 and HKCAS SC-08 (Issue No. 8). For further information, please refer to the corresponding document and clause as listed in the second column.

The information security management system certification body shall indicate in the 'QM Clause' column, for every question, the clause(s) in its management system manual, operation procedures or other related documentation which can demonstrate the information security management system certification body's conformity with the requirement.

The column headed 'OK' is for internal use of HKAS Executive.

A softcopy of this completed checklist shall be provided to HKAS Executive by email or other means.

ISO/IEC 27006-1: 2024 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
REQUIREMENTS FOR CERTIFICATION BODIES				
GENERAL REQUIREMENTS	5			
Management of impartiality	5.2			
Conflicts of interest	5.2.2			
Does your certification body provide internal information security reviews of the client's ISMS subject to certification?		☐		
Is your certification body independent from the body or bodies (including any individuals) which provide the internal ISMS audit of the client's ISMS subject to certification?		☐		
RESOURCE REQUIREMENTS	7			
Competence of Personnel	7.1			
Generic competence requirements	7.1.2			
Does your certification body define the competence requirements for each certification function as referenced in ISO/IEC 17021-1:2015, Table A.1.?		☐		
Does your certification body take into account all the requirements specified in ISO/IEC 17021-1 and 7.1.3 and 7.2.2 of ISO/IEC 27006-1 that are relevant for the ISMS technical areas as determined by your certification body?		☐		
Annex B provides further guides on competence.				
Does your certification body define the knowledge and skills that are required for certain functions in accordance with Annex A of ISO/IEC 27006-1?		☐		
Does your certification body apply additional specific criteria on competence requirements established in a specific standard, (e.g. ISO/IEC 27006-2)?		☐		

ISO/IEC 27006-1: 2024 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
Determination of competence criteria	7.1.3			
Competence requirements for ISMS auditing	7.1.3.1			
General requirements	7.1.3.1.1			
Does your certification body have criteria for verifying the competence of audit team members to ensure that they have at least the skills to apply their knowledge of the following?				
a) information security;		☐		
b) the technical aspects of the activity to be audited;		☐		
c) management systems;		☐		
d) the principles of auditing;		☐		
NOTE Further information on the principles of auditing can be found in ISO 19011.				
e) ISMS monitoring, measurement, analysis and evaluation.		☐		
Do the above requirements a) to e) apply to all auditors in the audit team (with the exception of b), which can be shared among auditors being part of the audit team)?		☐		
Do the audit team members, collectively, have skills appropriate to the requirements above, which can be demonstrated through experience of their application?		☐		
Are the audit team members, collectively, competent in tracing indications of information security incidents in the client's ISMS back to the appropriate elements of the ISMS?		☐		
Although individual auditors are not required to have a complete range of experience of all areas of information security, do the audit team as a whole have appropriate competence to cover the ISMS scope being audited?		☐		

ISO/IEC 27006-1: 2024 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
Information security management terminology, principles, practices and techniques	7.1.3.1.2			
Does each auditor in an ISMS audit team have knowledge of the following?				
a) ISMS specific documentation structures, hierarchy and interrelationships;		☐		
b) information security risk assessment and risk management;		☐		
c) processes applicable to ISMS.		☐		
Do the audit team members, collectively, have knowledge of the following?				
d) information security management related tools, methods, techniques and their application;		☐		
e) the current technology where information security may be relevant or an issue.		☐		
Information security management system standards and normative documents	7.1.3.1.3			
Does each auditor in an ISMS audit team have the knowledge of all requirements contained in ISO/IEC 27001?		☐		
Do the audit team members, collectively, have knowledge of all controls contained in ISO/IEC 27001:2022 Annex A and their implementation?		☐		
Business management practices	7.1.3.1.4			
Does each auditor in an ISMS audit team have knowledge of the following?				
a) industry information security good practices and information security procedures;		☐		
b) policies and business requirements for information security;		☐		

ISO/IEC 27006-1: 2024 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
c) general business management concepts, practices and the interrelationship between policy, objectives and results;		☐		
d) management processes and related terminology.		☐		
NOTE These processes also include human resources management, internal and external communication and other relevant support processes.				
Client business sector	7.1.3.1.5			
Does each auditor in an ISMS audit team have knowledge of the following?				
a) the legal and regulatory requirements in the particular information security field, geography and jurisdiction(s); *Note: Knowledge of legal and regulatory requirements does not imply a profound legal background.*		☐		
b) information security risks related to business sector;		☐		
c) generic terminology, processes and technologies related to the client business sector;		☐		
d) the relevant business sector practices.		☐		
The criteria a) may be shared amongst the audit team.				
Client products, processes and organisation	7.1.3.1.6			
Do the audit team members, collectively, have knowledge of the following?				
a) the impact of organisation 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.		☐		

ISO/IEC 27006-1: 2024 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
Competence requirements for conducting the application review	7.1.3.2			
Client business sector	7.1.3.2.1			
Do personnel conducting the application review to determine the audit team competence required, to select the audit team members and to determine the audit time have the knowledge of generic terminology, processes, technologies and risks related to the client business sector?		☐		
Client products, processes and organisation	7.1.3.2.2			
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 the following knowledge of the impact of client products, processes, organization types, size, governance, structure, functions and relationships on development and implementation of the ISMS and certification activities, including outsourcing functions?		☐		
Competence requirements for reviewing audit reports and making certification decisions	7.1.3.3			
General	7.1.3.3.1			
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 the audit, in particular the continuing validity of the identification of interfaces and dependencies and the associated risks?		☐		
Do personnel reviewing audit reports and making the certification decisions have knowledge of the following additionally?				
a) management systems in general;		☐		
b) audit processes and procedures;		☐		

ISO/IEC 27006-1: 2024 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
Information security management terminology, principles, practices and techniques	7.1.3.3.2			
Do personnel reviewing audit reports and making certification decisions have knowledge of the following?				
a) the items listed in 7.1.3.1.2 a), b) and c);		☐		
b) legal and regulatory requirements relevant to information security.		☐		
Client business sector	7.1.3.3.3			
Do personnel reviewing audit reports and making certification decisions have knowledge of generic terminology and risks related to the relevant business sector practices?		☐		
Client products, processes and organisation	7.1.2.4.5			
Do personnel reviewing audit reports and making certification decisions have knowledge of client products, processes, organization types, size, governance, structure, functions and relationships?		☐		
Personnel involved in the certification activities	7.2			
Demonstration of auditor knowledge and experience	7.2.2			
General considerations	7.2.2.1			
Does your certification body demonstrate that each auditor has knowledge and experience through each of the following?				
a) recognised ISMS-specific qualifications;		☐		
b) registration as auditor where applicable;		☐		
c) participation in ISMS training courses and attainment of relevant personal qualifications;		☐		
d) up-to-date professional development records;		☐		
e) ISMS audits witnessed by another ISMS auditor.		☐		

ISO/IEC 27006-1: 2024 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
Selecting auditors	7.2.2.2			
In addition to 7.1.3.1, does the process for selecting auditors ensure that each auditor comply with the following criteria?				
a) has professional education or training equivalent to university level;		☐		
b) has practical workplace experience in information technology and information security, which is sufficient to act as auditor for ISMS;		☐		
c) has received sufficient training regarding ISMS auditing, and demonstrated skills of auditing an ISMS according to ISO/IEC 27001. This experience shall be gained by performing as an auditor-in-training monitored by an ISMS evaluator (see ISO/IEC 17021-1:2015, 9.2.2.1.4) in at least one ISMS initial certification audit (stage 1 and stage 2) or re-certification audit 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 five years. The participation shall include document review; risk assessment and its implementation, and audit reporting;		☐		
d) maintains relevant and current knowledge and skills in information security and auditing.		☐		
NOTE 1 Skills maintenance can be demonstrated through continual professional development.				
NOTE 2 The certification body requires a competence criteria catalogue to match the above requirements and evidences (see ISO/IEC 17021-1:2015, 7.1.2.).				
Selecting technical experts	7.2.2.3			
Does the process for selecting technical experts ensure that each technical expert comply with the following criteria?				
e) has professional education or training equivalent to university level;		☐		
f) has practical workplace experience in information technology and information security sufficient to act as a technical expert;		☐		

ISO/IEC 27006-1: 2024 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
g) maintains relevant and current knowledge and skills in information security. *NOTE Skills maintenance can be demonstrated through continual professional development.*		☐		
Selecting auditors for leading the team	7.2.2.4			
In addition to 7.2.2.2, do criteria for selecting an auditor for leading the team ensure that the auditor has actively participated in all stages of at least three ISMS audits, of which the participation include initial scoping and planning, document review, review of risk assessment and its implementation, and formal audit reporting?		☐		
INFORMATION REQUIREMENTS	8			
Certification documents	8.2			
ISMS Certification documents	8.2.2			
Are certification documents signed by an officer who has been assigned such responsibility?		☐		
Is the version of the Statement of Applicability included in the certification documents? *NOTE A change to the Statement of Applicability which does not change the coverage of the controls in the scope of certification does not require an update of the certification documents.*		☐		
Where no activity of the organization within the scope of the certification is undertaken at a defined physical location at all, does the certification document(s) state that all activities of the organization are conducted remotely?		☐		

ISO/IEC 27006-1: 2024 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
Reference of other standards in the ISMS certification documents	8.2.3			
Does your certification body ensure that the following requirements are complied with when the certification documents reference national and international standards?				
a) the organization has compared all of its necessary controls with those in the reference control source(s), to determine that it has not inadvertently omitted any such reference control in accordance with ISO/IEC 27001:2022, 6.1.3 c);		☐		
b) a justification for excluded reference controls is stated in the Statement of Applicability (SoA) in accordance with ISO/IEC 27001:2022, 6.1.3 d).		☐		
The reference control standards can be based on ISO/IEC 27001:2022, Annex A, or be standards that include information security controls.				
Do the certification documents state that the control set(s) applied in the SoA is used only for referencing the relevance of the inclusion or exclusion of controls in the ISMS and not used for conformity assessment?		☐		
Confidentiality	8.4			
Access to organizational records	8.4.2			
Before conducting a certification audit, does your certification body ask the client to report if any ISMS related information (such as ISMS records or information about design and effectiveness of controls) cannot be made available for review by the audit team because it contains confidential or sensitive information?		☐		
Does your certification body determine whether the ISMS can be adequately audited in the absence of such information?		☐		
If your certification body concludes that it is not possible to adequately audit the ISMS without reviewing the identified confidential or sensitive information, does your certification body advise the client that the certification audit cannot take place until appropriate access arrangements are granted?		☐		

ISO/IEC 27006-1: 2024 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
PROCESS REQUIREMENTS	9			
Pre-certification activities	9.1			
Application	9.1.1			
Considerations for certification procedures	9.1.1.2			
Do your certification body's procedures not presuppose a particular manner of implementation of an ISMS or a particular format for documentation and records?		☐		
Do your certification procedures focus on confirming that a client's ISMS meets the requirements specified in ISO/IEC 27001 and the policies and objectives of the client?		☐		
NOTE It is possible for an organization to design its own necessary controls or to select them from any source, therefore it is possible that an organization is certified to ISO/IEC 27001 even though none of its necessary controls are those specified in ISO/IEC 27001:2022, Annex A.				
Audit programme	9.1.3			
General considerations	9.1.3.2			
Does your certification body take into account the determined information security controls when preparing an ISMS audit programme?		☐		
NOTE 1 The information security controls can be from ISO/IEC 27001:2022, Annex A, and/or other applicable standard(s) and/or self-designed.				
NOTE 2 Further guidance on auditing is given in ISO/IEC 27007.				
Deployment of remote audit	9.1.3.3			
Does your certification body define procedures to determine the level of remote audit activities ("remote audits") that can be applied to auditing a client's ISMS, when intending to conduct remote audit activities?				

ISO/IEC 27006-1: 2024 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
Do your procedures include analysis of the risks related to the use of remote auditing for the client, considering the following factors:				
a) available infrastructure of the certification body and the client;		☐		
b) sector in which the client operates;		☐		
c) type(s) of audit during the certification cycle from initial audit to recertification audit;		☐		
d) competence of the persons of the certification body and the client, who are involved in the remote audit;		☐		
e) previously demonstrated performance of remote audits for the client;		☐		
f) scope of the certification.		☐		
Is the analysis performed prior to performing any remote audit?		☐		
Are the analysis and the justification for use of remote audit during the certification cycle documented?		☐		
Do the audit plan and audit report include clear indications if remote audit activities have been performed?		☐		
Are remote audits not used if the risk assessment identifies unacceptable risks to the effectiveness of the audit process?		☐		
Is the risk assessment reviewed during the certification cycle to ensure its continued suitability?		☐		
NOTE In case the client uses virtual sites (i.e. location where an organization performs work or provides a service using an online environment allowing persons involved to execute processes irrespective of physical locations), remote audit techniques are a relevant part of the audit plan.				
General preparations for the initial audit	9.1.3.4			
Does your certification body require a client to make all necessary arrangements for the access to internal audit reports and reports of independent reviews of information security?		☐		

ISO/IEC 27006-1: 2024 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
Review periods	9.1.3.5			
Does your certification body certify an ISMS only when there is sufficient evidence to demonstrate that arrangements for management reviews and internal ISMS audits have been implemented, are effective, and will be maintained covering the scope of certification?		☐		
Scope of ISMS certification	9.1.3.6			
Does your audit team audit the ISMS of the client covered by the defined scope against all applicable certification requirements?		☐		
Does your certification body confirm, in the scope of the client ISMS, that clients address the requirements stated in ISO/IEC 27001:2022, 4.3?		☐		
Does your certification body 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 your certification body confirm that this is reflected in the client's scope of their ISMS and Statement of Applicability?		☐		
Does your certification body verify that there is a Statement of Applicability for the scope of certification?		☐		
Does your certification body 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?		☐		
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 organisations.				

ISO/IEC 27006-1: 2024 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
Determining audit time	9.1.4			
Audit time	9.1.4.2			
Does your certification body use Annex C to determine audit time?		☐		
NOTE Further guidance and examples on audit time calculation are provided in Annex D.				
Multi-site sampling	9.1.5			
Multiple sites	9.1.5.2			
Does your certification body consider using a sample-based approach to multiple-site certification audit when a client has a number of sites meeting the criteria from a) to c) below?	9.1.5.2.1			
a) all sites are operating under the same ISMS, which is centrally administered and audited and subject to central management review;		☐		
b) all sites are included within the client's internal ISMS audit programme;		☐		
c) all sites are included within the client's ISMS management review programme.		☐		
Does your certification body have procedures in place to ensure the following when using a sample-based approach:	9.1.5.2.2			
a) The initial contract review identifies, to the greatest extent possible, the difference between sites such that an adequate level of sampling is determined.		☐		
b) A representative number of sites have been sampled by the certification body, taking into account:		☐		

ISO/IEC 27006-1: 2024 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
1) the results of internal audits of the central office (if appropriate) and the sites;				
2) the results of management review;				
3) variations in the size of the sites;				
4) variations in the business purpose of the sites;				
5) complexity of the information systems at the different sites;				
6) variations in working practices;				
7) variations in activities undertaken;				
8) variations of design and operation of controls;				
9) potential interaction with critical information systems or information systems processing sensitive information;				
10) any differing legal requirements;				
11) geographical and cultural aspects;				
12) risk situation of the sites;				
13) information security incidents at the specific sites.				
c) A representative sample is selected from all sites within the scope of the client's ISMS; this selection shall be based upon judgmental choice to reflect the factors presented in item b) above as well as a random element.		☐		
d) Every site included in the ISMS which is subject to significant risks is audited by the certification body prior to certification.		☐		
e) The audit programme has been designed in the light of the above requirements and covers representative samples of the scope of the ISMS certification within the three-year period.		☐		
f) In the case of a nonconformity being observed at a single site, the corrective action procedure applies to all sites covered by the certificate.		☐		
Does the audit address the client's activities to ensure that a single ISMS applies to all sites and delivers central management at the operational level?		☐		

ISO/IEC 27006-1: 2024 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
Does the audit address all the issues outlined above?		☐		
Multiple management systems	9.1.6			
Integration of ISMS and other management system documentation	9.1.6.2			
Where documentation is combined (e.g. for information security, quality, health and safety and environment), does your certification body require the client to clearly identify the ISMS which has appropriate interfaces to other management systems?		☐		
Combining management system audits	9.1.6.3			
When combining an ISMS audit with audits of other management systems, does your certification body demonstrate that the audit satisfies all requirements for certification of the ISMS?		☐		
Do all the elements important to an ISMS appear clearly, and be readily identifiable, in the audit reports?		☐		
Does your certification body ensure that the quality of the audit is not adversely affected by the combination of the audits?		☐		
Planning audits	9.2			
Determining audit objectives, scope and criteria	9.2.1			
Audit objectives	9.2.1.2			
Do audit objectives include the following?				
a) determination of the effectiveness of the management system;		☐		
b) ensuring that the client, based on the risk assessment, has implemented applicable controls and		☐		
c) determining that the established information security objectives have been achieved.		☐		

ISO/IEC 27006-1: 2024 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
Audit plan	9.2.3			
General considerations	9.2.3.2			
Does each audit plan for ISMS audits take the determined information security controls into account?		☐		
NOTE It is good practice for a certification body to agree on the timing of the audit with the organization being audited to best demonstrate the full scope of the organization. Considerations can include season, month, day/dates and shifts, as appropriate.				
Remote audit techniques	9.2.3.3			
Is the objective of remote auditing techniques to enhance audit effectiveness and efficiency, and to support the integrity of the audit process?		☐		
Does the audit plan reference tools that are used to assist remote auditing?		☐		
Initial certification	9.3			
Initial certification audit	9.3.2			
Stage 1	9.3.2.1			
In this stage of the audit, does your certification body obtain documentation on the design of the ISMS covering the documentation required in ISO/IEC 27001?		☐		
Does our client provide the following information during stage 1 of the certification audit as a minimum?				
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, other associated documentation.		☐		

ISO/IEC 27006-1: 2024 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
Does your certification body obtain sufficient understanding of the design of the ISMS in the context of the client's organisation, risk assessment and treatment (including the controls determined), information security policy and objectives and, in particular, of the client's preparedness for the audit?		☐		
Does your certification body use the above information in planning stage 2 audit?		☐		
Are the results of stage 1 documented in a written report?		☐		
Does your certification body review the stage 1 audit report before deciding on proceeding with stage 2 and confirming if the stage 2 audit team members with the necessary competence? *The review may be done by the auditor leading the team that conducted the stage 1 audit if deemed competent and appropriate.* *NOTE Having a person from the certification body who is not involved in the audit reviewing the report, and who decides to proceed and confirms the competence of the audit team members for stage 2, offers a degree of mitigation for the risks involved. However, other risk mitigation measures can already be in place to achieve the same goal.*		☐		
Does your certification body make the client aware of the further types of information and records that may be required for detailed examination during the stage 2?		☐		
Stage 2	9.3.2.2			
Does your certification body develop an audit plan for the conduct of stage 2 on the basis of findings documented in the stage 1 audit report?		☐		
In addition to evaluating the effective implementation of the ISMS, is the the objective of the stage 2 to confirm that the client adheres to its own policies, objectives and procedures?		☐		
Does the audit focus on the following?	9.3.1.2.2			
The client's:				
a) top management leadership and commitment to the information security objectives;		☐		

ISO/IEC 27006-1: 2024 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
b) assessment of information security related risks; the audit shall also ensure that the assessments produce consistent, valid and comparable results if repeated;		☐		
c) determination of control controls based on the information security risk assessment and risk treatment processes;		☐		
d) information security performance and the effectiveness of the ISMS, evaluating these against the information security objectives;		☐		
e) correspondence between the determined controls, the Statement of Applicability and the results of the information security risk assessment, the risk treatment process and the information security policy and objectives;		☐		
f) implementation of controls (see Annex E of ISO/IEC 27006-1: 2024 for examples on auditing controls), taking into account the external and internal context and related risks, and the organisation's monitoring, measurement and analysis of information security processes and controls, to determine whether controls declared as being implemented are actually implemented and effective as a whole;		☐		
g) programmes, processes, procedures, records, internal audits and reviews of the ISMS effectiveness to ensure that these are traceable to top management decisions and the information security policy and objectives.		☐		
Conducting audits	9.4			
Specific elements of the ISMS audit	9.4.2			
Does your certification body 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?		☐		

ISO/IEC 27006-1: 2024 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
Does your certification body also establish whether the procedures employed in risk assessment are sound and properly implemented?		☐		
Audit report	9.4.3			
Do your audit reports provide the following information or a reference to it?	9.4.3.1			
a) an account of the audit of the client's information security risk analysis;		☐		
b) any information security control sets used by the organization for comparison purposes as required by ISO/IEC 27001:2022, 6.1.3 c).		☐		
Do your audit reports contain sufficient detail to facilitate and support the certification decision?	9.4.3.2	☐		
Do your reports contain the following?				
a) the significant audit trails followed and audit methodologies utilised (see 9.1.3.2 of ISO/IEC 27006-1:2024);		☐		
b) 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.		☐		
Completed questionnaires, checklists, observations, logs, or auditor notes may form an integral part of the audit report. If these methods are used, are these documents submitted to your certification body as evidence to support the certification decision?		☐		
Do your audit reports or other certification documentations include information about the samples evaluated during the audit?		☐		
Where remote audit methods have been used, do your reports indicate the extent to which they have been used in carrying out the audit and their effectiveness in achieving the audit objectives?		☐		
Where the activities of the organization are not undertaken at a defined physical location and therefore all activities of the organization are conducted remotely, do your audit reports state that all activities of the organization are conducted remotely?		☐		

ISO/IEC 27006-1: 2024 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
Do your reports consider the adequacy of the internal organisation and procedures adopted by the client to give confidence in the ISMS?		☐		
Do your reports include a summary of the most important observations, positive as well as negative, regarding the implementation and effectiveness of the ISMS requirements and information security controls?		☐		
Certification decision	9.5			
Certification decision	9.5.2			
Is the certification decision based on the certification recommendation of the audit team as provided in their certification audit report?		☐		
Does your certification body 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?		☐		
Maintaining certification	9.6			
Surveillance activities	9.6.2			
Are surveillance audit procedures a subset of those for the certification audit of the client's ISMS as described in ISO/IEC 27006-1:2024?	9.6.2.2	☐		
The purpose of surveillance is to verify that the approved ISMS continues to be implemented, to consider the implications of changes to that system initiated as a result of changes in the client's operational practices and to confirm continued compliance with certification requirements. Does your certification body's surveillance audit programmes cover at least the following: a) the ISMS maintenance elements such as information security risk assessment and control maintenance, internal ISMS audit, management review and preventive and corrective action; b) communications from external parties as required by ISO/IEC 27001 and other documents required for certification;		☐ ☐		

ISO/IEC 27006-1: 2024 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
Does your certification body review the following, as a minimum, in every surveillance audit?	9.6.2.3			
a) the 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.		☐		
Does your certification body adapt your programme of surveillance activities to reflect the information security issues related to risks and impacts on the client and justify this programme?	9.6.2.4	☐		
Surveillance audits may be combined with audits of other management systems. In such cases, does the audit report clearly indicate the aspects relevant to each management system?		☐		
During surveillance audits, does your certification body check the records of appeals and complaints brought before the certification body and, where any nonconformity or failure to meet the requirements of certification is revealed, that the client has investigated its own ISMS and procedures and taken appropriate corrective action?		☐		
Does a surveillance report contain, in particular, information on clearing of nonconformities revealed previously and the version of the SoA and important changes from the previous audit?		☐		
Do your reports arising from surveillance, as a minimum, build up to cover in totality the requirements of 9.6.2.2 and 9.6.2.3 of ISO/IEC 27006-1: 2024?		☐		

ISO/IEC 27006-1: 2024 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
Re-certification	9.6.3			
Re-certification audits	9.6.3.2			
Are re-certification audit procedures a subset of those for the initial certification audit of the client's ISMS as described in ISO/IEC 27006-1:2024?		☐		
Is the time allowed to implement corrective action consistent with the severity of the nonconformity and the associate information security risk?		☐		
Complaints	9.8			
Complaints	9.8.2			
Does your certification body consider that complaints represent a potential incident and an indication to possible nonconformity?		☐		
MANAGEMENT SYSTEM REQUIREMENTS FOR CERTIFICATION BODIES	10			
Options	10.1			
ISMS implementation	10.1.2			
It is recommended that certification bodies implement an ISMS in accordance with ISO/IEC 27001. Does your certification body implement an ISMS in accordance with ISO/IEC 27001?		☐		

Regulations for HKAS Accreditation	Clause	OK	QM/Procedure Clause	Remarks / Questions to be asked at certification body
RESOURCES REQUIREMENTS				
Does your certification body define the competence criteria for personnel responsible for each certification function?	HKCAS SC-08 3.1	☐		
Does your certification body apply the requirements specified in Annex A of HKCAS 003 and Sections 7.1.3 and 7.2.2 of ISO/IEC 27006-1?		☐		
Is your certification body able to demonstrate that your personnel comply with HKAS accreditation criteria through operating a proper appraisal system and keeping sufficient evidence?		☐		
Does your certification body implement a system to monitor the performance of its personnel involved in the ISMS audit, including lead auditors, auditors and technical experts?	HKCAS SC-08 3.2	☐		
Is the on-site performance of each ISMS auditor and lead auditor evaluated at least once every three years?		☐		
Does the evaluation cover all aspects of the activities that the auditors have been authorised by your certification body to perform?		☐		
Does your certification body take corrective actions if there is any doubt on the competence of an auditor?		☐		
A technical expert may be included in the audit team to provide technical support to the team. Although a technical expert does not need any training on auditing techniques, does your certification body ensure a technical expert has the required qualification, experience and technical knowledge on the activities to be audited? During an ISMS audit, do technical experts work under the direction and close supervision of a qualified auditor or a lead auditor?	HKCAS SC-08 3.3	☐		
The audit team may include a trainee auditor who is assigned less responsibility than that of a qualified auditor. Does your certification body ensure the trainee auditor works under close supervision of a qualified lead auditor or auditor?	HKCAS SC-08 3.4	☐		

Regulations for HKAS Accreditation	Clause	OK	QM/Procedure Clause	Remarks / Questions to be asked at certification body
INFORMATION REQUIREMENTS				
Are activities carried out in each geographic location covered by a certification clearly specified in the certification documents?	HKCAS SC-08 4.1	☐		
PROCESS REQUIREMENTS				
Does your certification body specify the information to be provided by a client which applies for its certification such as relevant information of the client, desired scope and boundaries of the certification, documented statements of the information security policy and objectives, description of the risk assessment process, the statement of applicability, all outsourced processes, information concerning the use of consultancy relating to the management system?	HKCAS SC-08 5.1	☐		
To ensure that essential information will not be missed out, does your certification body design an application form which lists all the information required form the client?		☐		
Upon receiving an application, does your certification body review and check whether sufficient information has been provided by the client and ask for supplementary information if necessary?	HKCAS SC-08 5.2	☐		
Does your certification body have an effective system for the analysis of their own competencies in information security management to ensure that it has the competence and ability required for each technical area in the certification process?		☐		
Does your certification body conduct such competence analysis for each client before performing the application review?		☐		
Does your certification body record details of the analysis and the outcome?		☐		
Does stage 1 audit take place at the site(s) of the client? Does your certification body record the justification if it has determined that the stage 1 audit is not required to be conducted at the sites(s) of the client?	HKCAS SC-08 5.3	☐		

Regulations for HKAS Accreditation	Clause	OK	QM/Procedure Clause	Remarks / Questions to be asked at certification body
Does your certification body examine the implementation of a client's ISMS in the stage 1 audit to determine whether and when the client is ready for the stage 2 audit?	HKCAS SC-08 5.4	☐		
Does your certification body determine the interval between stage 1 and stage 2 audits and only conduct stage 2 audit after the findings identified in the stage 1 audit have been adequately resolved by the client? As in general, a client will need some time to adequately resolve findings identified in the stage 1 audit, scheduling the stage 1 and stage 2 audits back to back is not recommended.		☐		
Is the interval between stage 1 and stage 2 audits and its justification recorded?		☐		
Does your certification body repeat the stage 1 audit if changes to a client's ISMS have rendered the information collected in the original stage 1 audit invalid?		☐		
Does your certification body have documented procedures for determining the amount of time required for any initial audit (stage 1 and stage 2), surveillance audit and re-certification audit?	HKCAS SC-08 5.5	☐		
Does the determination of audit duration meet the requirements specified in Annex C of ISO/IEC 27006-1?				
Does your certification body certification body follow the guidelines for calculation of audit time given in Annex D of ISO/IEC 27006-1?		☐		
Is the audit duration determined by your certification body and the justification for the determination recorded?		☐		

Regulations for HKAS Accreditation	Clause	OK	QM/Procedure Clause	Remarks / Questions to be asked at certification body
Does your certification body evaluate whether the client has relevant and sound analysis of information security related threats to information assets, vulnerabilities to and the likelihood of a threat materialising to information assets and the potential impact of any information security incident on information assets and whether appropriate procedures are properly implemented within the ISMS to manage the findings?	HKCAS SC-08 5.6	☐		
Does your certification body ensure that the client has applied appropriate risk assessment process and the repeated risk assessments performed by the client produced consistent, valid and comparable results?				
Does your certification body ensure that the levels or risk acceptance identified by the client fulfil its business objectives?		☐		
Reference to ISO/IEC 27005 which provides guidelines for information security risk management in an organisation may be made.				
Does your certification body ensure that the client has selected and implemented appropriate controls to ensure risks are reduced to an acceptable level?	HKCAS SC-08 5.7	☐		
Does your certification body evaluate whether the selected controls can mitigate risks as required by the risk treatment plan?		☐		
An applicant or accredited certification body is recommended to refer to applicable guideline standards in the ISO/IEC 27000 series or other recognised standards or guidelines on information security management controls and implementation.				
Does your certification body ensure that the client defined the maximum interval between risk assessments and an appropriate time interval for conducting ISMS internal audit and management review?	HKCAS SC-08 5.8	☐		
Does your certification body record the justification for accepting the time intervals?		☐		

Regulations for HKAS Accreditation	Clause	OK	QM/Procedure Clause	Remarks / Questions to be asked at certification body
Where your certification body offers multiple-site certification, does your certification body have documented procedures for multi-site sampling of audit?	HKCAS SC-08 5.9	☐		
Does your certification body record the justification for the sampling plan of a multi-site audit?		☐		
Where the ISMS audit is to be combined with audits of other management systems, for example, quality management system (QMS) and environment management system (EMS), is your certification body able to demonstrate that the ISMS audit complies with all requirements as specified in ISO/IEC 27006 and with all relevant HKAS accreditation criteria?	HKCAS SC-08 5.10	☐		
Does your certification body ensure that the scope and boundaries of the ISMS are clearly defined by the client and stated in the certification documents?	HKCAS SC-08 5.11	☐		
Does your certification body ensure that the scope and boundaries defined by each client are consistent with the policies and objectives of the client?		☐		
Does your certification body evaluate if the client applies appropriate controls over the scope and boundary before conducting the stage 2 audit?		☐		
Is exclusion of controls applicable to the scope boundary not allowed unless such exclusion does not affect the client's ability, and/or responsibility, to provide information security that meets the security requirements determined by risk assessment and applicable legal or regulatory requirements?		☐		
Does your certification body have documented procedures and criteria for the committee to make certification decisions?	HKCAS SC-08 5.12	☐		
Are the committee members trained on the decision criteria? Are detailed records of the factors considered by the committee and the deliberation kept?		☐		