Annex II(F1)
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: 2015 + A1: 2020 and HKCAS SC-08 (Issue No. 7). 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: 2015 + A1: 2020 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
REQUIREMENTS FOR CERTIFICATION BODIES				
IS 5.2 Conflicts of interest	5.2.1			
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?		☐		
7.1 Competence of Personnel				
IS 7.1.1 General consideration				
Generic competence requirements	7.1.1.1			
Does your certification body have knowledge of the technological, legal and regulatory developments relevant to the ISMS of the client which it assesses?		☐		
Does your certification body define the competence requirements for each certification function as referenced in Table A.1 of ISO/IEC 17021-1?		☐		
Does your certification body take into account all the requirements specified in ISO/IEC 17021-1 and 7.1.2 and 7.2.1 of ISO/IEC 27006 that are relevant for the ISMS technical areas as determined by your certification body?		☐		
NOTE Annex A provides a summary of the competence requirements for personnel involved in specific certification functions.				

ISO/IEC 27006: 2015 + A1: 2020 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
IS 7.1.2 Competence requirements for ISMS auditing				
Competence requirements for ISMS auditing	7.1.2.1			
General requirements	7.1.2.1.1			
Does your certification body have criteria for verifying the background experience, specific training or briefing of audit team members that ensures at least the following?				
a) knowledge of information security;		☐		
b) technical knowledge of the activity to be audited;		☐		
c) knowledge of management systems;		☐		
d) knowledge of the principles of auditing;		☐		
NOTE Further information on the principles of auditing can be found in ISO 19011.				
e) knowledge of ISMS monitoring, measurement, analysis and evaluation.		☐		
Do the above requirements a) to e) apply to all auditors being part of the audit team (with the exception of b), which can be shared among auditors being part of the audit team)?		☐		
Are your audit teams competent to trace indications of information security incidents in the client's ISMS back to the appropriate elements of the ISMS?		☐		
Do your audit teams have appropriate work experience of the items above and practical application of these items (this does not mean that an auditor needs a complete range of experience of all areas of information security, but the audit team as a whole shall have enough appreciation and experience to cover the ISMS scope being audited)?		☐		
Information security management terminology, principles, practices and techniques	7.1.2.1.2			

ISO/IEC 27006: 2015 + A1: 2020 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
Do all members of each audit team have the following knowledge collectively?				
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.		☐		
Does every auditor fulfil a), c) and d)?		☐		
Information security management system standards and normative documents	7.1.2.1.3			
Do auditors involved in ISMS auditing have the following knowledge?				
a) all requirements contained in ISO/IEC 27001.		☐		
Do all members of the audit team have the following knowledge collectively?				

ISO/IEC 27006: 2015 + A1: 2020 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
b) all controls contained in ISO/IEC 27002 (if determined as necessary also from sector specific standards) and their implementation, categorized as: 1) information security policies; 2) organisation of information security; 3) human resource security; 4) asset management; 5) access control, including authorisation; 6) cryptography; 7) physical and environmental security; 8) operations security, including IT-services; 9) communications security, including network security management and information transfer; 10) system acquisition, development and maintenance; 11) supplier relationships, including outsourced services; 12) information security incident management; 13) information security aspects of business continuity management, including redundancies; 14) compliance, including information security reviews.		☐		
Business management practices	7.1.2.1.4			
Do auditors involved in ISMS auditing have the following knowledge?				
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 the inter-relationship between policy, objectives and results;		☐		

ISO/IEC 27006: 2015 + A1: 2020 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
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	7.1.2.1.5			
Do auditors involved in ISMS auditing have the following knowledge?				
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	7.1.2.1.6			
Do auditors involved in ISMS auditing have the following knowledge collectively?				
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: 2015 + A1: 2020 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
Competence requirements for leading the ISMS audit team	7.1.2.2			
In addition to the requirements in 7.1.2.1, do audit team leaders fulfil the following requirements as demonstrated in audits under guidance and supervision?				
a) knowledge and skills to manage the certification audit process and the audit team;		☐		
b) demonstration of the capability to communicate effectively, both orally and in writing.		☐		
Competence requirements for conducting the application review	7.1.2.3			
Information security management system standards and normative documents	7.1.2.3.1			
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?				
a) relevant ISMS standards and other normative documents used in the certification process.		☐		
Client business sector	7.1.2.3.2			
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 following knowledge?				
a) generic terminology, processes, technologies and risks related to the client business sector.		☐		
Client products, processes and organisation	7.1.2.3.3			
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?				

ISO/IEC 27006: 2015 + A1: 2020 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
a) client products, processes, organisation 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	7.1.2.4			
General	7.1.2.4.1			
Do personnel reviewing audit reports and making certification decisions have the 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 the following knowledge additionally?				
a) management systems in general;		☐		
b) audit processes and procedures;		☐		
c) audit principles, practices and techniques.		☐		
Information security management terminology, principles, practices and techniques	7.1.2.4.2			
Do personnel reviewing audit reports and making the certification decisions have the following knowledge?				
a) the items listed in 7.1.2.1.2 a), c) and d);		☐		
b) legal and regulatory requirements relevant to information security.		☐		
Information security management system standards and normative documents	7.1.2.4.3			

ISO/IEC 27006: 2015 + A1: 2020 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
Do personnel reviewing audit reports and making certification decisions have the following knowledge?				
a) relevant ISMS standards and other normative documents used in the certification process.		☐		
Client business sector	7.1.2.4.4			
Do personnel reviewing audit reports and making certification decisions have the following knowledge?				
a) 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 the following knowledge?				
a) client products, processes, organisation types, size, governance, structure, functions and relationships.		☐		
IS 7.2 Demonstration of auditor knowledge and experience	7.2.1			
Does your certification body demonstrate that the auditors have knowledge and experience through the following?				
a) recognised 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.		☐		

ISO/IEC 27006: 2015 + A1: 2020 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
Selecting auditors	7.2.1.1			
In addition to 7.1.2.1, does your certification body ensure that each auditor comply with the following criteria?				
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 or 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, 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 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.		☐		
Do technical experts comply with criteria a), b) and e).		☐		
Selecting auditors for leading the team	7.2.1.2			
In addition to 7.1.2.2 and 7.2.1.1, do criteria for selecting an auditor for leading the team ensure the following for the auditor?				

ISO/IEC 27006: 2015 + A1: 2020 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
a) has actively participated in all stages of at least three ISMS audits. The participation shall include initial scoping and planning, review of documentation and risk assessment, implementation assessment and formal audit reporting.		☐		
IS 7.3 Using external auditors or external technical experts as part of the audit team	7.3.1			
Do technical experts work under the supervision of an auditor?		☐		
Do they satisfy the minimum requirements for technical experts as listed in 7.2.1.1?		☐		
IS 8.2 ISMS Certification documents	8.2.1			
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?		☐		
For a certification document which makes reference to national and international standards as source(s) of control set for controls that are determined as necessary in the organisation's Statement of Applicability in accordance with ISO/IEC 27001, 6.1.3 d), is the reference on the certification document clearly stated as being only a control set source for controls applied in the Statement of Applicability and not a certification thereof?		☐		
IS 8.4 Access to organisational records	8.4.1			
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?		☐		

ISO/IEC 27006: 2015 + A1: 2020 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
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?		☐		
IS 9.1.1 Application readiness	9.1.1.1			
Does your certification body require the client to have a documented and implemented ISMS which conforms to ISO/IEC 27001 and other documents required for certification?		☐		
9.1.3 Audit Programme				
IS 9.1.3 General	9.1.3.1			
Does your certification body take into account the determined information security controls when preparing an ISMS audit programme?		☐		
IS 9.1.3 Audit Methodology	9.1.3.2			
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 establishing that a client's ISMS meets the requirements specified in ISO/IEC 27001 and the policies and objectives of the client?		☐		

ISO/IEC 27006: 2015 + A1: 2020 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
IS 9.1.3 General preparations for the initial audit	9.1.3.3			
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?		☐		
Does your certification body require a client to provide the following during stage 1 of the certification audit?				
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.		☐		
IS 9.1.3 Review periods	9.1.3.4			
Does your certification body certify an ISMS only when it has been operated through at least one management review and one internal ISMS audit covering the scope of certification?		☐		
IS 9.1.3 Scope of certification	9.1.3.5			
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, 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 at least one Statement of Applicability per scope of certification?		☐		

ISO/IEC 27006: 2015 + A1: 2020 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
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) with other organisations.*		☐		
IS 9.1.3 Certification audit criteria	9.1.3.6			
Is the ISMS of your clients audited against the criteria in the ISMS standard ISO/IEC 27001? *Note: Other documents may be required for certification relevant to the function performed.*		☐		
IS 9.1.4 Audit time	9.1.4.1			
Does your certification body allow auditors sufficient time to undertake all activities relating to an initial audit, surveillance audit or re-certification audit?		☐		
Does the calculation of overall audit time include sufficient time for audit reporting?		☐		
Does your certification body use Annex B to determine audit time?		☐		
IS 9.1.5 Multiple sites				
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?	9.1.5.1.1			
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;		☐		

ISO/IEC 27006: 2015 + A1: 2020 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
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:	9.1.5.1.2			
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:		☐		
1) the results of internal audits of the head office 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.		☐		

ISO/IEC 27006: 2015 + A1: 2020 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
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, either at the head office or at a 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 the operational level?		☐		
Does the audit address all the issues outlined above?		☐		
IS 9.1.6 Integration of ISMS documentation with that for other management systems	9.1.6.1			
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?		☐		
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?		☐		
IS 9.2.1 Audit objectives	9.2.1.1			
Do 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?		☐		

ISO/IEC 27006: 2015 + A1: 2020 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
IS 9.2.2 Audit team	9.2.2.1			
Are audit teams formally appointed and provided with the appropriate working documents?		☐		
Is the mandate given to the audit team clearly defined and made known to your clients?		☐		
When an audit team only consist of one person, does the person meet all the criteria set out in 7.1.2.1?		☐		
IS 9.2.2 Audit team competence	9.2.2.2			
When selecting and managing the audit team to be appointed for a specific certification audit, does your certification body ensure that the competences brought to each assignment are appropriate?		☐		
Does each team meet the following requirements?				
a) have appropriate technical knowledge of the specific activities within the scope of the ISMS for which certification is sought and, where relevant, with associated procedures and their potential information security risks (technical experts may fulfil this function);		☐		
b) have understanding of the client sufficient to conduct a reliable certification audit of its ISMS given the ISMS' scope and context within the organisation in managing the information security aspects of its activities, products and services;		☐		
c) have appropriate understanding of the legal and regulatory requirements applicable to the client's ISMS.		☐		
NOTE Appropriate understanding does not imply a profound legal background.				
IS 9.2.3 General	9.2.3.1			
Does each audit plan for ISMS audits take the determined information security controls into account?		☐		

ISO/IEC 27006: 2015 + A1: 2020 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
IS 9.2.3 Network-assisted audit techniques	9.2.3.2			
Does each audit plan identify the network-assisted auditing techniques that will be utilised during the audit, as appropriate?		☐		
Network assisted auditing techniques may include, for example, teleconferencing, web meeting, interactive web-based communications and remote electronic access to the ISMS documentation or ISMS processes. The focus of such techniques should be to enhance audit effectiveness and efficiency and should support the integrity of the audit process.				
IS 9.2.3 Timing of audit	9.2.3.3			
Does your certification body agree with the organisation to be audited the timing of the audit which will best demonstrate the full scope of the organisation?		☐		
The consideration could include season, month, day/dates and shift as appropriate.				
IS 9.3.1.1 Initial certification audit	9.3.1			
IS 9.3.1.1 Stage 1	9.3.1.1			
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 your certification body obtain a 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?		☐		
This allows planning for stage 2.				
Are the results of stage 1 documented in a written report?		☐		

ISO/IEC 27006: 2015 + A1: 2020 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
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?		☐		
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?		☐		
IS 9.3.1.2 Stage 2	9.3.1.2			
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?		☐		
Is the following the objectives of the stage 2?				
a) 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 information security policy and the information security 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 the 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 and risk treatment process and the information security policy and objectives;		☐		

ISO/IEC 27006: 2015 + A1: 2020 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
g) implementation of controls (see Annex D of ISO/IEC 27006: 2015), taking into account the external and internal context and related risk, the organisation'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, 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.		☐		
9.4 Conducting audits				
IS 9.4 General	9.4.1			
Does your certification body have documented procedures for the following:				
a) the initial certification audit of a client's ISMS, in accordance with the provisions of ISO/IEC 17021-1;		☐		
b) surveillance and re-certification audits of 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.		☐		
IS 9.4 Specific elements of the ISMS audit	9.4.2			
Does your certification body, 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?		☐		

ISO/IEC 27006: 2015 + A1: 2020 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?		☐		
IS 9.4 Audit report	9.4.3			
In addition to the requirements for reporting in ISO/IEC 17021-1, 9.4.8, do your audit reports provide the following information or a reference to it?	9.4.3.1			
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 (e.g. more or less time spent on certain scheduled activities);		☐		
d) the ISMS' scope.		☐		
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) significant audit trails followed and audit methodologies utilised (see 9.1.3.2);		☐		
b) observations made, both positive (e.g. noteworthy features) and negative (e.g. potential nonconformities);		☐		
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.		☐		
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?		☐		

ISO/IEC 27006: 2015 + A1: 2020 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?		☐		
In addition to the requirements for reporting in ISO/IEC 17021-1, 9.4.8, do your reports cover the following?				
- a summary of the most important observations, positive as well as negative, regarding the implementation and effectiveness of the ISMS requirements and IS controls;		☐		
- the audit team's recommendation as to whether the client's ISMS should be certified or not, with information to substantiate this recommendation.		☐		
IS 9.5 Certification decision	9.5.1			
Is the certification decision based, additionally 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)?		☐		
The persons or committees that take the decision on granting certification should not normally overturn a negative recommendation of the audit team. If such a situation arises, does your certification body document and justify the basis for the decision to overturn the recommendation?		☐		
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?		☐		
IS 9.6.2 Surveillance activities	9.6.2.1			
Are surveillance audit procedures consistent with those concerning the certification audit of the client's ISMS as described inISO/IEC 27006?	9.6.2.1.1	☐		

ISO/IEC 27006: 2015 + A1: 2020 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
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 operation and to confirm continued compliance with certification requirements. Does your certification body's surveillance audit programmes cover at least the following:				
a) the system 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 the ISMS standard ISO/IEC 27001 and other documents required for certification;		☐		
c) changes to the documented system;		☐		
d) areas subject to change;		☐		
e) selected requirements of ISO/IEC 27001;		☐		
f) other selected areas as appropriate.		☐		
Does your certification body review the following, as a minimum, in every surveillance?	9.6.2.1.2			
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 surveillance programme to the information security issues related to risks and impacts on the client and justify this programme?	9.6.2.1.3	☐		

ISO/IEC 27006: 2015 + A1: 2020 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
Surveillance audits may be combined with audits of other management systems. In such cases, does the reporting 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 9.6.2.1.1 and 9.6.2.1.2 above?		☐		
IS 9.6.3 Re-certification audits	9.6.3.1			
Are recertification audit procedures consistent with those concerning the initial certification audit of the client's ISMS as described in ISO/IEC 27006?		☐		
Is the time allowed to implement corrective action consistent with the severity of the nonconformity and the associate information security risk?		☐		
IS 9.6.4 Special cases	9.6.4.1			
Are the activities necessary to perform special audits subject to special provision if a client with a certified ISMS makes major modifications to its system or if other changes take place which could affect the basis of its certification?		☐		
IS 9.8 Complaints	9.8.1			
Does your certification body consider that complaints represent a potential incident and an indication to possible nonconformity?		☐		

ISO/IEC 27006: 2015 + A1: 2020 Requirements	Clause	OK	QM/ Procedure Clause	Remarks / Questions to be asked at certification body
IS 10.1 ISMS implementation 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?	10.1.1	☐		

Regulations for HKAS Accreditation	Clause	OK	QM/Procedure Clause	Remarks / Questions to be asked at certification body
Does your certification body define the competence criteria for personnel responsible for each function in the management and performance of audits and certification, such as conducting application review, selecting and verifying the competence of ISMS auditors, briefing and arranging training of ISMS auditors, auditing, leading the audit team, reviewing audit reports and making certification decisions?	HKCAS SC-08 3.1	☐		
Does your certification body apply the requirements in Annex A of HKCAS 003 and Sections 7.1.2 and 7.2.1 of ISO/IEC 27006? 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 eachISMS 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
Does your certification body include all names and geographic locations of a certified client covered by a certification in the certification document?	HKCAS SC-08 4.1	☐		
Are activities carried out in each geographic location covered by a certification clearly specified in the certification documents?		☐		
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?	HKCAS SC-08 5.3	☐		
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 5.4	☐		

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 5.5	☐		
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 5.6	☐		
Does the determination of audit duration meet the requirements specified in Annex B of ISO/IEC 27006?				
Does your certification body certification body follow the guidelines for calculation of audit time given in Annex C of ISO/IEC 27006?		☐		
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 5.7	☐		
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 5.8	☐		
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 5.9	☐		
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 5.10	☐		
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 5.11	☐		
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 5.12	☐		
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?		☐		
Certification decisions may be made by a staff member or a committee. In case the certification decision is made by a committee, does your certification body ensure that the committee members who make the decision on granting/withdrawing a certification have a level of knowledge and experience sufficient for making a sound decision based on the results or information obtained from the auditing processes?	HKCAS SC-08 5.13	☐		

Regulations for HKAS Accreditation	Clause	OK	QM/Procedure Clause	Remarks / Questions to be asked at certification body
Does your certification body have documented procedures and criteria for the committee to make certification decisions? Are the committee members trained on the decision criteria? Are detailed records of the factors considered by the committee and the deliberation kept?		☐ ☐		