HKCAS Supplementary Criteria No. 8

Accreditation Programme for Information Security Management System (ISMS) Certification

1 INTRODUCTION

1.1 HKAS accreditation for information security management system certification is provided under Hong Kong Certification Body Accreditation Scheme (HKCAS) and is open for voluntary application from any certification body offering third-party certification service on information security management system as described in ISO/IEC 27001 or information security management system in respect of a certification scheme. The certification scheme shall satisfy the criteria set out in HKCAS SC-11.

1.2 Specific accreditation criteria for information security management system certification include HKCAS 003, ISO/IEC 27006 and HKCAS SC-08.

1.3 The normative documents listed in Appendix B form part of the accreditation requirements of this document.

1.4 Applicant or accredited certification bodies should take note of the accreditation procedure stated in HKCAS IN001 and Appendix A of this document.

1.5 Details of the HKCAS accreditation are given in an accredited certification body's scope of accreditation. For an accredited certification body offering certification service(s) in respect of certification scheme(s), the details include identification of the certification scheme(s), a brief description of each scheme such as certification criteria, normative references, evaluation and surveillance regime.

1.6 Accreditation of a certification body for a particular management system certification is an attestation that the certification body is competent in offering third-party certification service on that management system certification for which it is accredited

in accordance with the accreditation criteria. An accredited certification body shall comply with the relevant accreditation criteria at all times for maintaining accreditation. Nevertheless, accreditation is not a guarantee that an accredited certification body will carry out its accredited activities in accordance with the accreditation criteria all the time. Furthermore, accreditation is not a guarantee that any organisation certified by an accredited certification body is in conformity with all certification requirements. HKAS does not endorse, sanction or approve in any way, any organisation certified by any accredited certification body. Conversely, failure to obtain certification from an accredited certification body does not imply that HKAS has refused to endorse, sanction or approve in any way the applicant organisation to be certified.

2 TERMS AND DEFINITIONS

2.1 For the purpose of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 27001 and ISO/IEC 27006 apply.

2.2 Throughout this document, the term “assessment” refers to the process in which HKAS Executive assesses the competence of a certification body while the term “audit” refers to the process in which a certification body evaluates the conformity of an organisation with certification criteria.

Note: Where the term “risk assessment” appears in this document, it refers to the client’s information security risk assessment and the definition in ISO/IEC 27001 applies.

2.3 The term “shall” is used throughout this document to indicate those provisions which are mandatory. The term “should” is used to indicate guidance which, although not mandatory, is provided by HKAS as a recognised means of meeting the requirements.

2.4 In this document, the term “lead auditor” has the same meaning as the term “audit team leader” which is used in HKCAS 003 and ISO/IEC 27006.

3 RESOURCE REQUIREMENTS

3.1 An applicant or accredited certification body shall 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. The requirements in Annex A of HKCAS 003 and Sections 7.1.2 and 7.2.1 of ISO/IEC 27006 shall be applied. An applicant or accredited certification body shall demonstrate that its personnel comply with HKAS accreditation criteria through operating a proper appraisal system and keeping sufficient evidence of competence.

3.2 An applicant or accredited certification body shall implement a system to monitor the performance of its personnel involved in the ISMS audit, including lead auditors, auditors and technical experts. On-site performance of each ISMS leader auditor and auditor shall be evaluated at least once every three years. The evaluation shall cover all aspects of the activities that the auditors have been authorised by the certification body to perform. Corrective actions shall be taken if there is any doubt on the competence of an auditor.

3.3 A technical expert may be included in the audit team to provide technical support to the team. A technical expert does not need any training on auditing techniques but shall have the required qualification, experience and technical knowledge on the activities to be audited. During an ISMS audit, technical experts shall work under the direction and close supervision of a qualified auditor or a lead auditor.

3.4 The audit team may include a trainee auditor who works under close supervision of a qualified lead auditor or auditor and who is assigned less responsibility than that of a qualified auditor.

4 INFORMATION REQUIREMENTS

4.1. An applicant or accredited certification body shall include all names and geographic locations of a certified client covered by a certification in the certification document. The activities carried out in each geographic location covered by a certification shall also be clearly specified in the certification document.

5 PROCESS REQUIREMENTS

5.1. An applicant or accredited certification body shall 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. To ensure that essential information will not be missed out, the certification body should design an application form which lists all the information required from the client.

5.2. Upon receiving an application, an applicant or accredited certification body shall review and check whether sufficient information has been provided by the client and ask for supplementary information if necessary.

5.3. An applicant or accredited certification body shall 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. Such competence analysis shall be conducted by the certification body for each client before performing the application review. Details of the analysis and the outcome shall be recorded.

5.4. Stage 1 audit should take place at the site(s) of the client. Otherwise, an applicant or accredited certification body shall 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.

5.5. An applicant or accredited certification body shall 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. The certification body shall determine the interval between stage 1 and stage 2 audits and shall 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. The interval between stage 1 and stage 2 audits and its justification shall be recorded. The certification body should repeat the stage 1 audit if changes to a client's ISMS have rendered the information collected in the original stage 1 audit invalid.

5.6. An applicant or accredited certification body shall 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. Determination of audit duration shall meet the requirements specified in Annex B of ISO/IEC 27006. In addition, the guidelines for calculation of audit time given in Annex C of ISO/IEC 27006 should be followed as far as applicable. The audit duration determined by the certification body and the justification for the determination shall be recorded.

5.7. An applicant or accredited certification body shall 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. An applicant or accredited certification body shall 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. An applicant or accredited certification body shall 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.

5.8. An applicant or accredited certification body shall ensure that the client has selected

and implemented appropriate controls to ensure risks are reduced to an acceptable level. It shall 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.

5.9. An applicant or accredited certification body shall ensure that the client defined the maximum interval between risk assessments. It shall also require the client to define an appropriate time interval for conducting ISMS internal audit and management review. The certification body shall record the justification for accepting the time intervals.

5.10. Where an applicant or accredited certification body offers multiple-site certification, the certification body shall have documented procedures for multi-site sampling of audit. The certification body shall record the justification for the sampling plan of a multi-site audit.

5.11. The ISMS audit can be combined with audits of other management systems, for example, quality management system (QMS) and environment management system (EMS) provided that the applicant or accredited certification body can demonstrate that the ISMS audit complies with all requirements as specified in ISO/IEC 27006 and with all relevant HKAS accreditation criteria.

5.12. An applicant or accredited certification body shall ensure that the scope and boundaries of the ISMS are clearly defined by the client and stated in the certification document. The scope and boundaries defined by each client shall be consistent with the policies and objectives of the client. The certification body shall evaluate if the client applies appropriate controls over the scope and boundary before conducting the stage 2 audit. Any exclusion of controls applicable to the scope boundary is 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.

5.13. Certification decisions may be made by a staff member or a committee. In case the certification decision is made by a committee, the applicant/accredited certification body shall ensure that the committee members who make the decision on granting/withdrawing a certification shall have a level of knowledge and experience sufficient for making a sound decision based on the results or information obtained from the auditing processes. The certification body shall also have documented procedures and criteria for the committee to make certification decisions and the committee members shall be trained on the decision criteria. Detailed records of the factors considered by the committee and the deliberation shall be kept.

Appendix A
(Informative)

HKAS Assessment Process for ISMS Certification Bodies

A1. The purpose of a HKAS assessment is to determine whether the subject certification body has the competence and reliability to provide ISMS certification. Emphasis will be given to whether the certification body has the necessary expertise in information security management system such as technical knowledge relevant to ISMS, knowledge of legislative and regulatory requirements relevant to information security, knowledge of information security related threats to assets, vulnerabilities and impacts, risk assessment and risk management, ISMS controls and implementation, ISMS effectiveness review and measurement of controls, and the robustness of its auditing process.

A2. HKAS Executive will conduct a preliminary visit to an applicant certification body which has not been accredited previously under HKCAS. If an applicant certification body has already been accredited for another certification field under HKCAS, e.g., QMS or EMS, the application for accreditation of ISMS certification will be treated as an application for extension of accreditation and no preliminary visit will be conducted. However, as ISMS certification is to be carried out in accordance with HKCAS 003 and ISO/IEC 27006, if the certification body has not been accredited for certifications carried out in accordance with HKCAS 003, e.g. the certification body is accredited for product certification only, the certification body is strongly recommended to request HKAS Executive to conduct a preliminary visit at an additional fee.

Appendix B

NORMATIVE DOCUMENTS

1. HKCAS 003: 2015, Technical Criteria of Accreditation of Management System Certification Bodies
2. HKCAS Supplementary Criteria No. 11 (HKCAS SC-11), HKAS Policy on Product and Management System Certification Schemes
3. ISO/IEC 27000: 2018, Information technology – Security techniques – Information security management systems – Overview and vocabulary
4. ISO/IEC 27001: 2022, Information security, cybersecurity and privacy protection – Information security management systems – Requirements
5. ISO/IEC 27006: 2015 + A1: 2020, Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems

Note: For dated references, only the edition cited applies. For undated references, the latest editions (including any amendments) apply.