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 The accreditation criteria for information security management system certification include HKAS 002, HKCAS 003: 2015, ISO/IEC 27006, HKCAS SC-04, the relevant HKAS and HKCAS Supplementary Criteria, relevant IAF requirements as specified in IAF documents including Mandatory Documents and Resolutions, relevant PAC requirements as specified in PAC documents including Technical Documents and Resolutions, and the current edition of this document which serves to amplify the accreditation requirements in the above documents.

1.3 The normative documents listed in Appendix B form part of the accreditation requirements of this document. For dated references, only the edition cited applies. For undated references, the latest editions (including any amendments) apply.

1.4 HKAS operates its accreditation process in accordance with Annex AA of HKCAS 003: 2015 and Appendix A of this document. Applicant or accredited certification bodies should take note of the process applicable to them.

1.5 Details of the HKCAS accreditation for an accredited certification body are given in its current 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 Fees for application, assessment and other accreditation services are charged in accordance with HKCAS 006.

1.7 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 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 organisation'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" is used. It has the same meaning as the term "audit team leader" which is used in HKCAS 003: 2015 and ISO/IEC 27006.

3 GENERAL REQUIREMENTS

3.1 There shall be a contract signed between the client organisation and the certification body to confer the latter the authority to carry out its responsibility in accordance with HKCAS 003: 2015, ISO/IEC 27006 and this document.

4 RESOURCE REQUIREMENTS

4.1 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: 2015 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 such criteria through a proper appraisal system, and evidence of competence shall be kept.

4.2 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 evaluation for ISMS audit shall

be performed for every auditor and lead auditor 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 their competence.

4.3 A technical expert may be included in the audit team. He/she provides technical support to an auditor or the team. A technical expert needs not be trained on auditing techniques but must 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.

4.4 The audit team may include a trainee auditor who works under close supervision of a qualified lead auditor or auditor. The responsibility assigned to him/her should be less than the level for a qualified auditor.

5 INFORMATION REQUIREMENTS

5.1 An applicant or accredited certification body shall include all names and geographic locations of a certified client organisation 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 documents.

6 PROCESS REQUIREMENTS

6.1 An applicant or accredited certification body shall specify the information to be provided by a client organisation which applies for its certification such as relevant information of the client organisation, 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 organisation.

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

6.3 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 organisation before performing the application review. Details of the analysis and the outcome shall be recorded.

6.4 Stage 1 audit should take place at the site(s) of the client organisation. 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 organisation

6.5 An applicant or accredited certification body shall examine the implementation of a client organisation's ISMS in the stage 1 audit to determine whether and when the organisation 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 organisation. As in general, client organisations 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 stage 1 audit if changes to an client organisation's ISMS have rendered the information collected in the original stage 1 audit invalid.

6.6 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.

6.7 An applicant or accredited certification body shall evaluate whether the client organisation 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 organisation has applied appropriate risk assessment process and the repeated risk assessments performed by the client organisation produced consistent, valid and comparable results. An applicant or accredited certification body shall ensure that the levels or risk acceptance identified by the client organisation fulfil its business objectives. Reference to ISO/IEC 27005 which provides guidelines for information security risk management in an organisation may be made.

6.8 An applicant or accredited certification body shall ensure that the client organisation 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 make reference to applicable guideline standards in the ISO/IEC 27000 series, e.g. ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, ISO/IEC 27017, ISO/IEC 27018 or other recognised standards or guidelines on information security management controls and implementation.

6.9 An applicant or accredited certification body shall ensure that the client organisation defined the maximum interval between risk assessments. It shall also require the client organisation 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.

6.10 Where an applicant or accredited certification body offers multiple-site certification, the certification body shall have documented procedures for multiple-site sampling audit in accordance with ISO/IEC 27006 and IAF MD 1. The certification body shall record the justification for the sampling plan of a multiple-site sample audit.

6.11 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 an 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.

6.12 An applicant or accredited certification body shall ensure that the scope and boundaries of the ISMS are clearly defined by the client organisation and stated in the certification documents. The scope and boundaries defined by the client organisation shall fulfil and be consistent with its policies and objectives. The certification body shall evaluate if the client organisation 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 organisation's ability, and/or responsibility, to provide information security that meets the security requirements determined by risk assessment and applicable legal or regulatory requirements.

6.13 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

A1.1 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.

A1.2 To apply for accreditation, an applicant certification body shall complete an application form HKCAS 005 and provide the details of its organisation and its certification system to be accredited in HKCAS 019 application questionnaire. All supporting documents, including the quality manual, documents of the certification programme as required in HKCAS 019, and the appropriate application fee shall be provided together with the completed HKCAS 005 and HKCAS 019 to HKAS Executive.

Preliminary visit

A1.3 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: 2015 and ISO/IEC 27006 and if the certification body has not been accredited for certifications carried out in accordance with HKCAS 003: 2015, e.g. if the certification body is accredited only for product certification, the certification body is strongly recommended to request HKAS Executive to conduct a preliminary visit at an additional fee.

Initial assessment

A1.4 Assessments are conducted by HKAS assessment team(s). A HKAS assessment team usually consists of a team leader and where necessary, technical assessors and/or technical experts. The certification system of an applicant certification body will be assessed against the requirements in the HKCAS 003: 2015, ISO/IEC 27006, relevant HKAS and HKCAS Supplementary Criteria and this document.

Appendix B

NORMATIVE DOCUMENTS

1. HKAS 002, Regulations for HKAS accreditation
2. HKAS Supplementary Criteria No. 1 (HKAS SC-01), Use of HKAS accreditation symbols and claims of accreditation status
3. HKAS Supplementary Criteria No. 2 (HKAS SC-02), Non-conformities and their grading
4. HKCAS Supplementary Criteria No. 4 (HKCAS SC-04), Accreditation regulations specific for HKCAS – certification body
5. HKCAS 003: 2015, Technical Criteria of Accreditation of Management System Certification Bodies
6. ISO/IEC 27000: 2016, Information technology – Security techniques – Information security management systems – Overview and vocabulary
7. ISO/IEC 27001: 2013, Information technology – Security techniques – Information security management systems – Requirements
8. ISO/IEC 27006: 2015, Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems
9. IAF MD 1: 2007, IAF Mandatory Documents for the Certification of Multiple Sites Based on Sampling

INFORMATIVE DOCUMENTS

10. ISO/IEC 27002, Information technology – Security techniques – Code of practice for information security controls
11. ISO/IEC 27003, Information technology – Security techniques – Information security management system implementation guidance
12. ISO/IEC 27004, Information technology – Security techniques – Information security management – Measurement

13. ISO/IEC 27005, Information technology – Security techniques – Information security risk management

14. ISO/IEC 27017, Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

15. ISO/IEC 27018, Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors