Accreditation Services Branch

SCC Requirements and Guidance for the Accreditation of CyberSecure Canada Certification Bodies

2020-12-17

Standards Council of Canada

Open a world of possibilities.

Canada

Standards Council of Canada
55 Metcalfe St., Suite 600
Ottawa, ON K1P 6L5

Telephone: + 1 613 238 3222
Fax: + 1 613 569 7808
accreditation@scc.ca
www.scc.ca

Permission to Reproduce

Aussi offert en français sous le titre *Exigences et lignes directrices – Exigences et lignes directrices du CCN – Accréditation des organismes de certification de CyberSécuritaire Canada*

Table of Contents

Introduction

The purpose of this document is to outline the accreditation requirements for Certification Bodies operating the CyberSecure Canada certification program. These requirements are based on a combination of those previously used by CyberNB and fundamental requirements from ISO/IEC 17021-1. The numbers in the reference columns in the requirements and guidance tables that follow are aligned with the similar clause in ISO/IEC 17021-1.

1. Scope

The document encompasses the requirements for organizations transitioning from the CyberNB program to obtain SCC-recognized Certification Body status for the CyberSecure Canada Program.

2. References

The following referenced documents provide background for the application of this document but are not to be considered additional mandatory documents.

- SCC Accreditation Services - Accreditation Program Overview
- CyberSecure CB Handbook
- ISO/IEC 17021-1:2015 Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements

3. Definitions

All definitions as defined in all normative reference documents apply.

3.1 Audit Programme is the set of one or more audits planned for a specific time frame, the audit cycle, and directed towards s specific purpose, example year one, initial audit, year two surveillance audit, and so on to the next recertification audit.

3.2 Certified Client
Organization whose management system has been certified.

3.3 Impartiality
The presence of objectivity or that conflict of interest does not exist.

3.4 Management System Consultancy
Participation in establishing, implementing or maintaining a management system. Refer to ISO 17021-1:2015 clause 4.2.

3.5 Competence
Competence of all personnel involved in certification activities.

3.6 Responsibility
The certified client, and not the certification body, has the responsibility for consistently achieving the intended results of implementation of the management system and conformity with the requirements for certification.

3.7 Openness
A certification body shall provide public access to, or disclosure of, appropriate and timely information about its audit, certification and certification status processes.

3.8 Confidentiality
The certification body does not disclose any confidential information.

3.9 Responsiveness to Complaints
Effective responsiveness to complaints against errors, omissions or unreasonable behaviour.

3.10 Risk-based Approach
Certification bodies need to take into account the risks associated with providing competent, consistent and impartial certification.

4. Principles

Reference	Requirement & Guidance
4.2 Impartiality	
4.2.1	The certification body shall have a documented process to manage risks to impartiality and for carrying out its certification activities, managing conflict of interest and ensuring objectivity of its certification activities, including any conflicts arising from its relationships or from the relationships of its personnel.
4.2.2	The certification body shall undertake certification activities impartially by not allowing commercial, financial or other pressures to compromise impartiality, and demonstrate a commitment to impartiality in assessment activities.
4.2.3	When an unacceptable risk to impartiality is identified and which cannot be mitigated to an acceptable level, then certification shall not be provided.
4.2.4 b)	In case the certification body is linked to an organization offering consultancy, the certification body shall be able to demonstrate a clear separation of duties and responsibilities between personnel providing consultancy and certification auditing services. Personnel providing consultancy services shall not participate in certification services for the same customer for a minimum period of 2 years before the date of the certification decision.

4.3 Competence	
4.3.3	The certification body shall have an implemented process for the establishment of competence criteria for the personnel involved in the audit and other certification activities and perform evaluation of personnel against the competence criteria.
4.6 Confidentiality	
4.6	The certification body shall not disclose to a third party any confidential information that was obtained due to the privileged access to information that was needed to assess conformity to requirements.
4.7 Responsiveness to Complaints	
4.7	The certification body shall have a documented process for receiving, evaluating and making decisions on complaints. The certification body shall be responsible for all decisions at all levels of the documented complaints handling process.
4.8 Risk Based Approach	
4.8	The certification body shall consider risks and opportunities that may impact impartiality of the certification process and shall plan actions to address risks and opportunities, integrate these actions into the certification body processes and shall evaluate the effectiveness of these actions.

5. General Requirements

Reference	Requirement & Guidance
5.1 Legal and contractual matters	
5.1.1	The certification body shall be a legal entity or a defined part of a legal entity such that it may be accountable for its activities, enter contracts or agreements, incur and pay back debts, be sued and sue other entities, and assume legal obligations.
5.1.2	A legally enforceable arrangement is required between the certification body and its client for the provision of certification activities. The certification body shall ensure that there is a legally enforceable agreement that covers all its client's sites within the scope of the certification.
5.2 Managing Impartiality	
5.2.3	The certification body shall have a process to manage the risks related to conflict of interests arising from its certification activities on an ongoing basis.

	This shall include the identification, analysis, evaluation, treatment, monitoring, and recording of risks to impartiality.
5.2.8	Outsourcing of audits to organizations that provide consultancy is not permitted. This does not apply to individuals contracted as auditors covered in 7.5.1.
5.2.10	To avoid any potential conflict of interest, certification body personnel who have provided consultancy to a client, shall comply with clause 4.2.4 (b) above.
5.2.13	In its process to manage the risks related to conflict of interests, certification bodies shall require all personnel involved in the certification process to disclose any situation known to them that can be perceived as a conflict of interest. This information shall be used by the certification body in its identification of potential risks to impartiality.
5.2.14	The certification body shall provide feedback to the CyberSecure Canada program owner at ISED on the CyberSecure Canada program.

6. Structural Requirements

Reference	Requirement & Guidance
6.1 Organizational structure and top management	
6.1.1	The certification body shall maintain a representation of its organizational structure and document the duties, responsibilities and authorities all personnel involved in the certification process.
6.2 Operational control	
6.2.1	The certification body shall have a process for the management of certification activities performed at all locations and by all personnel.
6.2.2	The certification body shall demonstrate control of its certification activities including its processes, competence of personnel, reporting and remote access to operations including records.

7. Resource Requirements

Reference	Requirement & Guidance
7.1 Resources	
7.1.1	The certification body shall have a process to manage the competence of its personnel, including the determination of necessary knowledge and skills required to operate the CyberSecure Canada certification program.
7.1.2	The certification body shall determine and document the competence criteria for personnel involved in the conduct of certification audits and other certification activities.
7.1.3	The certification body shall have records of the initial competence evaluation, and ongoing monitoring of competence and performance of all personnel involved in the certification activities.
7.2 Personnel involved in the certification activities	
7.2.1	The certification body shall maintain a sufficient and competent roster of personnel to support the initial and ongoing audit program for the CyberSecure Canada certification program.
7.2.3	The certification body shall inform each person of their duties, responsibilities and authorities.
7.2.7	The certification body shall ensure its auditors, technical experts and other personnel involved in certification activities are competent for their roles by identifying training needs and close any gaps.
7.2.8	The decision to grant, refuse, maintain, renew, suspend, restore, or withdraw certification shall be undertaken by individual(s) with an understanding of the certification requirements, and shall have competence to evaluate the outcomes of the audit processes including related recommendations of the audit team.
7.2.10	The certification body shall monitor each auditor to verify competency. The monitoring process shall include a review of audit reports and feedback from clients. This monitoring shall be designed in such a way as to minimize disturbance to the normal processes of certification, especially from the client's viewpoint.
7.2.11	The certification body shall evaluate the performance of each auditor. The evaluations shall be conducted at intervals determined from all monitoring information available.

7.3	Use of individual external auditors and external technical experts
7.3	The certification body shall have a written agreement with its external auditors and external technical experts by which the external resource commits themselves to comply with applicable policies and implement processes as defined by the certification body.
7.5	**Outsourcing**
7.5.1	Other than organizations mentioned in 5.2.8, the certification body may outsource (subcontract to another organization) part of the certification activity with a legally enforceable agreement covering the necessary arrangements, including confidentiality and conflicts of interests, with each body that provides outsourced services. The certification body shall have a documented process to describe the conditions where outsourcing may be considered.
7.5.4	If outsourcing is used, the certification body shall have a process for the approval and monitoring of all organizations that provide outsourced services used for certification activities and shall maintain records of the competence of all personnel involved in certification activities.

8. Information Requirements

Reference	Requirement & Guidance
8	**Information Requirements**
8.0	The certification body shall endeavour to notify the customer of significant changes to the CyberSecure Canada program.
8.1	**Public Information**
8.1.1	The certification body shall publish information about: a) the certification process; b) a description of the process for granting, refusing, maintaining, renewing, suspending, restoring and withdrawing certification; c) the use of the certification body's name and certification mark or logo; d) processes for handling requests for information, complaints and appeals; e) policy on impartiality.
8.1.2	The certification body shall respond to third party requests for: a) geographical areas in which it operates; b) the status of a given certification; c) the name, scope and geographical location for a specific certified client.
8.2	**Certification Documents**
8.2.2	The certification body shall include the following in its certification documents:

	a) the name and geographical location of each certified client; b) the effective date of granting, or renewing certification; c) the expiry date or recertification due date consistent with the recertification cycle; d) a unique reference code; e) the revision date or number of the standard used for audit of the certified client; f) the type of activity, product or service provided by the certified client; g) the name and address of the certification body; other marks (e.g. accreditation symbol, client's logo) may be used provided they are not misleading or ambiguous; and h) any other information required by the standard and/or other normative document used for certification.
8.4 Confidentiality	
8.4.1	The certification body, and any external bodies or individuals acting on its behalf shall keep all information obtained or created during the performance of certification activities confidential.
8.4.2	The certification body shall inform the client, in advance, of the information it intends to place in the public domain.
8.4.4	The certification body may be required by law or authorized by contractual arrangements (such as with the accreditation body) to release confidential information. In these cases, the certification body shall notify the client, unless prohibited by law, of the information provided.
8.4.7	The certification body shall ensure the secure handling of confidential information.
8.5 Information Exchange between a certification body and its clients	
8.5.1	The certification body shall provide information and update its clients on the following: a) a detailed description of the initial and continuing certification activity; b) changes to the requirements for certification; c) information about the fees for application, initial certification and continuing certification; d) the certification body's requirements for clients to: 1) comply with certification requirements; 2) make all necessary arrangements for the conduct of the audits, including provision for examining documentation and the access to all processes and areas, records and personnel for the purposes of initial certification, surveillance, recertification and resolution of complaints; 3) make provisions, where applicable, to accommodate the presence of observers (e.g. accreditation assessors or trainee auditor); e) documents describing the rights and duties of certified clients, including requirements, when making reference to its certification in communication of any kind in line with the requirements in 8.3; f) information on processes for handling complaints and appeals.

8.5.2	The certification body shall give its certified clients advanced notice of any changes to the requirements for certification. The certification body shall verify that each certified client complies with the new requirements.

9. Process Requirements

Reference	Requirement & Guidance
9.1 Pre-certification activities	
9.1.1	The certification body shall require an applicant organization to provide the necessary information to enable it to establish the following: a) relevant details of the applicant organization as required by the CyberSecure Canada certification program, including its name and the address(es) of its site(s), its processes and operations, human and technical resources, functions, relationships and any relevant legal obligations; b) identification of outsourced processes used by the organization that will affect conformity to requirements; c) whether consultancy relating to the management system to be certified has been provided and, if so, by whom.
9.1.2.1	The certification body shall conduct a review of the application and supplementary information for certification to ensure that: a) the information about the applicant organization and its management system is sufficient to develop an audit programme (see 9.1.3.1); b) any known difference in understanding between the certification body and the applicant organization is resolved; c) the certification body has the competence and ability to perform the certification activity; d) the site(s) of the applicant organization's operations, time required to complete audits and any other points influencing the certification activity are taken into account (language, safety conditions, threats to impartiality, etc.).
9.1.3.1	An audit programme for the full certification cycle shall be developed to clearly identify the audit activities required to demonstrate that the client's management system fulfils the requirements for certification. The audit programme for the certification cycle shall cover the complete set of requirements outlined in this document.
9.1.3.2	The audit programme for the initial certification shall include a surveillance activity in the year following the certification decision, and a recertification audit in the second year prior to expiration of certification. This two-year certification cycle begins with the certification decision. Subsequent cycles begin with the recertification decision. The determination of the audit programme and any subsequent adjustments shall consider the size of the client, the scope and complexity of its

	management system, products and processes as well as demonstrated level of management system effectiveness and the results of any previous audits.
9.1.3.3	Surveillance activities shall be conducted mid way between the certification/recertification audits plus or minus 3 months. i.e. The date of the surveillance activity following certification shall not be more than 15 months from the certification decision date, and not before 9 months form the certification decision date.
9.2 Planning audits	
9.2.1.1	The certification body shall inform the client of the audit objectives, scope and criteria, including any changes.
9.2.1.3	The audit scope shall describe the extent and boundaries of the audit, such as sites, organizational units, activities and processes to be audited. Where the initial or re-certification process consists of more than one audit (e.g. covering different sites), the scope of an individual audit may not cover the full certification scope, but the totality of audits shall be consistent with the scope in the certification document.
9.4 Conducting audits	
9.4.1 a)	The certification body shall use a combination of tools and manual processes to enable it to perform audits as per the program requirements.
9.4.1 b)	If required, Automated vulnerability Assessment Tools shall support all mainstream operating systems.
9.4.1 c)	Automated vulnerability Assessment Tools, if used shall produce repeatable and comparable results and shall produce auditable findings that may be used in dispute resolution with customers.
9.4.2	The certification body shall conduct an opening meeting with the auditee to provide a short explanation of how the audit activities will be undertaken. The degree of detail shall be consistent with the familiarity of the client with the audit process and shall consider the following: a) introduction of the participants, including an outline of their roles; b) confirmation of the scope of certification; c) confirmation of the audit plan including any changes, and other relevant arrangements with the client, such as the date and time for the closing meeting, interim meetings between the audit team and the client's management; d) confirmation of formal communication channels between the audit team and the client; e) confirmation that the resources and facilities needed by the audit team are available; f) confirmation of matters relating to confidentiality;

	g) confirmation of relevant work safety, emergency and security procedures for the audit team; h) confirmation of the availability, roles and identities of any guides and observers; i) the method of reporting, including any grading of audit findings; j) information about the conditions under which the audit may be prematurely terminated; k) confirmation that the audit team leader and audit team representing the certification body is responsible for the audit and shall be in control of executing the audit plan including audit activities and audit trails; l) confirmation of the status of findings of the previous review or audit, if applicable; m) methods and procedures to be used to conduct the audit based on sampling; n) confirmation of the language to be used during the audit; o) confirmation that, during the audit, the client will be kept informed of audit progress and any concerns; p) opportunity for the client to ask questions.
9.4.5.1	Audit findings summarizing conformity and detailing nonconformity shall be identified, classified and recorded to enable an informed certification decision to be made or the certification to be maintained.
9.4.6	In preparing the audit conclusions prior to the closing meeting, the audit team leader shall: a) review the audit findings, and any other appropriate information obtained during the audit, against the audit objectives and audit criteria and classify the nonconformities; b) agree upon the audit conclusions, taking into account the uncertainty inherent in the audit process; c) agree any necessary follow-up actions; d) confirm the appropriateness of the audit programme or identify any modification required for future audits.
9.4.7.1	At the end of the audit, a closing meeting shall be convened between the audit team and the client. Both parties shall sign the findings report and discuss what the next steps are.
9.4.7.2	The closing meeting shall also include the following elements: a) advising the client that the audit evidence obtained was based on a sample of the information; thereby introducing an element of uncertainty; b) the method and timeframe of reporting, including any grading of audit findings; c) the certification body's process for handling nonconformities including any consequences relating to the status of the client's certification; d) the timeframe for the client to present a plan for correction and corrective action for any nonconformities identified during the audit; e) the certification body's post audit activities; f) information about the complaint and appeal handling processes.

9.4.8.1	The certification body shall provide a written report for each audit to the client. The audit team may identify opportunities for improvement but shall not recommend specific solutions. Ownership of the audit report shall be maintained by the certification body.
9.4.8.2	The audit team leader shall ensure that the audit report is prepared and shall be responsible for its content. The audit report shall provide an accurate, concise and clear record of the audit to enable an informed certification decision to be made and shall include or refer to the following: a) identification of the certification body; b) the name and address of the client and the client's representative; c) the type of audit (e.g. initial, surveillance or recertification audit or special audits); d) the audit criteria; e) the audit objectives; f) the audit scope, particularly identification of the organizational or functional units or processes audited and the time of the audit; g) any deviation from the audit plan and their reasons; h) any significant issues impacting on the audit programme; i) identification of the audit team leader, audit team members and any accompanying persons; j) the dates and places where the audit activities (on site or offsite, permanent or temporary sites) were conducted; k) audit findings, reference to evidence and conclusions, consistent with the requirement of the type of audit; l) significant changes, if any, that affect the management system of the client since the last audit took place; m) any unresolved issues, if identified; n) where applicable, whether the audit is combined, joint or integrated; o) a disclaimer statement indicating that auditing is based on a sampling process of the available information; p) recommendation from the audit team; q) the audited client is effectively controlling the use of the certification documents and marks, if applicable; r) verification of effectiveness of taken corrective actions regarding previously identified nonconformities, if applicable.
9.4.8.3	The report shall also contain: a) a statement on the conformity and the effectiveness of the management system together with a summary of the evidence relating to: — the capability of the management system to meet applicable requirements and expected outcomes; — the internal audit and management review process; b) a conclusion on the appropriateness of the certification scope; c) confirmation that the audit objectives have been fulfilled.

9.5 Certification decision	
9.5.1.1	The certification body shall ensure that the person(s) that make the decisions for granting or refusing certification, suspending or restoring certification, withdrawing certification or renewing certification are different from those who carried out the audits. The individual(s) appointed to conduct the certification decision shall have appropriate competence.
9.5.2	The certification body shall have a process to conduct an effective review prior to making a decision for granting certification, renewing, suspending or restoring, or withdrawing of certification, including, that: a) the information provided by the audit team is sufficient with respect to the certification requirements and the scope for certification; b) for any major nonconformities, it has reviewed, accepted and verified the correction and corrective actions; c) for any minor nonconformities it has reviewed and accepted the client's plan for correction and corrective action.
9.6 Maintaining certification	
9.6.2.1.2	Surveillance activities shall include auditing of the certified client's management system's fulfilment of specified requirements with respect to the standard to which the certification is granted. Other surveillance activities may include: a) enquiries from the certification body to the certified client on aspects of certification; b) reviewing any certified client's statements with respect to its operations (e.g. promotional material, website); c) requests to the certified client to provide documented information (on paper or electronic media); d) other means of monitoring the certified client's performance.
9.6.3.2.1	The recertification audit shall include an audit that addresses the following: a) the effectiveness of the management system in its entirety in the light of internal and external changes and its continued relevance and applicability to the scope of certification; b) demonstrated commitment to maintain the effectiveness and improvement of the management system in order to enhance overall performance; c) the effectiveness of the management system with regard to achieving the certified client's objectives and the intended results of the respective management system(s).
9.6.5.1	The certification body shall have a policy and documented procedure(s) for suspension, withdrawal or reduction of the scope of certification, and shall specify the subsequent actions by the certification body.
9.6.5.2	The certification body shall suspend certification in cases when, for example:

	— the client's certified management system has persistently or seriously failed to meet certification requirements, including requirements for the effectiveness of the management system; — the certified client does not allow surveillance or recertification audits to be conducted at the required frequencies; — the certified client has voluntarily requested a suspension.
9.8 Complaints	
9.8.1	The certification body shall be responsible for all decisions made in its complaints handling process.
9.8.6	The certification body's complaints-handling process shall include at least the following elements and methods: a) an outline of the process for receiving, validating, investigating the complaint, and for deciding what actions need to be taken in response to it; b) tracking and recording complaints, including actions undertaken in response to them; c) ensuring that any appropriate correction and corrective action are taken.
9.9 Client records	
9.9.1	The certification body shall maintain records on the audit and other certification activities for all clients, including all organizations that submitted applications, and all organizations audited, certified, or with certification suspended or withdrawn.
9.9.3	The certification body shall keep the records on applicants and clients secure to ensure that the information is kept confidential. Records shall be transported, transmitted or transferred in a way that ensures that confidentiality is maintained.

10. Management System Requirements for Certification Bodies

Reference	Requirement & Guidance
10.2 General Management system requirements	
10.2.3	Control of documents Documents include the written process descriptions required by this document, the policies that its clients shall to adhere to, and the criteria for evaluation and selection of auditors. The certification body shall establish procedures to control the documents (internal and external). The procedures shall define the controls needed to: a) approve documents for adequacy prior to issue;

	b) review and update where necessary and re-approve documents; c) ensure that changes and the current revision status of documents are identified; d) ensure that relevant versions of applicable documents are available at points of use; e) ensure that documents remain legible and readily identifiable; f) ensure that documents of external origin are identified, and their distribution controlled; g) prevent the unintended use of obsolete documents, and to apply suitable identification to them if they are retained for any purpose.
10.2.5.1	Management Review The certification body's top management shall establish procedures to review its management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness, including the stated policies and objectives. These reviews shall be conducted at least once a year.
10.2.5.2	Review inputs The input to the management review shall include information related to: a) results of internal and external audits; b) feedback from clients and interested parties; c) safeguarding impartiality; d) the status of corrective actions; e) the status of actions to address risks; f) follow-up actions from previous management reviews; g) the fulfilment of objectives; h) changes that could affect the management system; i) appeals and complaints.
10.2.5.3	Review outputs The outputs from the management review shall include decisions and actions related to: a) improvement of the effectiveness of the management system and its processes; b) improvement of the certification services related to the fulfilment of these requirements; c) resource needs; d) revisions of the organization's policy and objectives.
10.2.6.2	The certification body shall establish an internal audit programme to verify that it fulfils the requirements of this document and legal requirements, and that the management system is effectively implemented and maintained.
10.2.6.3	Internal audits shall be performed at least once every 12 months.

10.2.6.4	Internal audits shall be conducted by competent personnel knowledgeable in certification, auditing and the requirements of this certification program. The certification body shall ensure that: a) auditors do not audit their own work; b) personnel responsible for the area audited are informed of the outcome of the audit; c) any actions resulting from internal audits are taken in a timely and appropriate manner; d) any opportunities for improvement are identified.
10.4 Process for continual improvement	
10.4	The certification body shall have a process for continual improvement, development and maintenance of the CyberSecure Canada program.
10.5 Key Performance Indicators (KPIs)	
10.5	The certification body shall ensure records relating to performance are gathered and maintained and that remedial actions are taken for activities that fail to meet the following Key Performance Indicators: a) Process more than 90% of all activities within agreed timescales; b) Ensure that at least 95% of certificates issued by the certification body are correct; c) Ensure that less than 5% of certificates are issued with incorrect information; d) Close (following completed investigation and corrective action) more than 95% of customer appeals and complaints within agreed timescales.
10.6 Data privacy and protection	
10.6	The certification body shall document and retain supporting analysis of evaluation activities in line with the requirements of the Personal Information Protection and Electronic Documents Act (PIPEDA) and other applicable regulations.

- End of Document -