MHM Advisory Ltd.

Client Certification Process for Security & Privacy Management Information Systems & CyberSecure Canada

Table of Contents

Version Control

Version	Date	Modified By	Reviewed By	Details
1.0	2023/2/23	Mark Mandel	Mark Mandel Jose Costa	Document creation and initial sign-off by MHM E-team
1.1	2023/07/04	Mark Mandel	Jose Costa	Minor edits and formatting
1.2	2023/11/25	Jose Costa	Jose Costa Mark Mandel	Reduced response time for customers to 10 days from 30 days.

Overview

This document outlines MHM Advisory Ltd.'s ("MHM") processes for performing certification audits related to Information Security Management System (ISMS), Privacy Information Management System (PIMS) and CyberSecure Canada's including processes for granting, refusing, maintaining, renewing, suspending, restoring or withdrawing certification or expanding or reducing the scope of certification. In addition, it provides an overview of:

- types of management systems and certification schemes in which MHM operates;
- the use of the certification body's name and certification mark or logo;
- MHM's processes for handling requests for information, complaints and appeals;
- MHM's policy on impartiality.

This document and all referenced documentation are reviewed at least annually, or every time there is a significant organizational, regulatory or operational change to the Security and Privacy Certification Services (SPCS) Practice and reviewed and approved by MHM's Executive team.

Management Systems And Certification Schemes Offered by MHM

MHM has established, documented and implemented a management system that is capable of supporting and demonstrating the consistent achievement of the requirements of ISO 17021-1:2015, ISO 27006:2015, ISO/IEC 27006-2:2015 and other applicable accreditation requirements.

MHM's E-team ensures that MHM's audit processes for performing certification audits and the related policies are available for staff involved in the certification process, implemented and understood. Responsibilities and authorities have been assigned for ensuring that (i) processes and procedures needed for the management system are

established, implemented and maintained, and (ii) reporting to top management on the performance of the management system and any need for improvement.

MHM has been authorized to perform certification audits of management systems by the Standards Council of Canada for the following schemes:

- ISO/IEC 27001
- ISO/IEC 27017
- ISO/IEC 27018
- ISO/IEC 27701
- CyberSecure Canada

In addition to providing the services described above, MHM also provides:

- SOC1 / SOC2 / SOC2+ / SOC3 audits[1]
- Privacy assessments (HIPAA, GDPR, etc.)
- Readiness assessments & support (SOC1/SOC2, PCI, etc.)
- IT Security Governance, Risk & Controls & Internal Audit

Accreditation Standards and Requirements

In order to provide above services, MHM complies with below accreditation standards and requirements:

- ISO 17021-1:2015
- ISO 27006:2015
- ISO/IEC 27006-2:2015
- Standards and Internal Accreditation Forum (IAF) requirements MD 5:2015

[1] Assurance Services governed by CPA Canada are provided by MHM Professional Corporation

- MHM's "Engagement and Quality Policy Manual"
- CPA Canada - Canadian Standard On Quality Management (CSQM 1) - Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements
- PIPEDA (Other federal and Provincial regulation applicable to MHM services)

Policy on Impartiality

All MHM's staff members and services offered are subject to MHM's principles related to independence, conflict of interest, impartiality and risk management. MHM does not engage with any clients or perform any services that would threaten its independence and impartiality, create any conflict of interest with the clients, vendors, contractors or business partners. These rules are in place to protect the MHM, its employees and its clients and are aligned to auditing and certification standards that it adheres to as well as MHM's ethical values.

MHM will not use staff, management or contractors to conduct certification activities if they have been involved in any consulting services (including internal audits) related to the organization's management system within two years of the end of the consulting engagement.

If MHM identifies an unacceptable risk to impartiality that cannot be mitigated to an acceptable level, MHM will notify the client or prospect that we can't perform the work.

MHM's has a defined process to assess and update the list of threats to impartiality as soon as they are identified and take immediate action to respond to any threats arising from employees, contractors, processes or the actions of other persons, bodies or organizations including comments received from the complaints process. The list of threats and safeguards is reviewed and signed off at least annually. In addition, MHM has a client acquisition process to evaluate impartiality or independence risks at an engagement level.

In addition, each staff member assigned to a new client project is expected to review the engagement letter and client acceptance information to assess if they have any personal independence conflicts (e.g. outside business relationships or significant work on a conflicting prior project). Any concerns are immediately brought to the attention of the lead principal and if necessary, the staff member is removed from the project prior to it starting. Each staff member is also required to attest, on an annual basis, that they are aware of MHM's independence policy and expectations and that there were no known conflicts during the year that were not already brought to the principal's attention. Records of this confirmation are stored in the employee personnel files.

MHM's Audit Processes

Pre-Certification Activities

Application

A discovery questionnaire will be the first step for MHM and an application organization to assess the audit scope, and key technical areas and to complete the Audit Days Calculation (ADC). A questionnaire form will be sent to the prospect or completed by MHM's personnel through a discovery conversation. The form shall be completed as comprehensively as possible and should include at least:

- The desired scope of the certification or details of the prospect's ISMS, PIMS or CyberSecure Canada scope statement
- Relevant details of the applicant organization as required by the specific certification scheme, 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
- Identification of outsourced processes used by the organization that will affect conformity to requirements

- The standards or other requirements for which the applicant organization is seeking certification
- Whether consultancy relating to the management system to be certified has been provided and, if so, by whom.
- Risk analysis and Statement of Applicability (SoA) if available
- Additional information should be gathered about the client's industry and business, usage and type of their IT infrastructure, number of end users and remote users, data that they collect and process, number of security and privacy personnel and their responsibilities.

Application review

As soon as a client's application certification, recertification or transfer of certification is received, MHM's engagement risk process will be triggered requiring documentation that includes (but not limited to) - Conflict of interest check, Completed Auditor Days Calculation (ADC) and budget, Proposed Audit Programme, Proposed audit team, Proposal and/or engagement letter

An Engagement Letter shall not be signed without signoff by an MHM principal of the engagement risk process.

When reviewing any application or engagement proposal, particular attention should be paid to the scope of the certification. The scope should be defined taking into consideration the organizations:

- Statement of Applicability (SOA) version (to be referenced in the scope statement)
- Organization's business activities
- Organizational boundaries (Departments, services or processes in scope as well as organizational structure supporting them)
- Geographical location/s

- Key assets and Information processed
- Technology, supporting infrastructure, system boundaries, platforms, applications
- Any outsourced activity
- Activities supporting the services in scope

If MHM declines an application for certification as a result of the review of application, the reasons for declining an application shall be documented and made clear to the prospect.

Audit Programme

A contract containing details of the audit programme for the full certification cycle will be drafted to clearly identify the audit activities required to demonstrate that the client's management system fulfils the requirements for certification to the selected standard(s). The audit programme for the certification cycle shall cover the complete management system requirements. MHM's contract will provide an indication of the prospect's ISMS, PIMS or CyberSecure Canada scope and how the audit time has been determined. MHM shall not certify an ISMS/PIMS unless it has been operated through at least one management review and one internal ISMS/PIMS audit covering the scope of certification.

Determination of audit time

According to ISO IEC 17021-1, the ADC is the time needed to plan and accomplish a complete and effective audit of the client organization's management system. The methodology implemented by MHM to calculate ADC is based on the requirements outlined in the ISO/IEC 27006:2015, Annex B, Table B.1 and ISO/IEC 17021-1:2015 and the Standards and Internal Accreditation Forum (IAF) requirements MD 5:2015 "Determination of Audit Time of Quality and Environmental Management Systems."

Multi-site audits

For multi-site audits, MHM will select a representative sample from all sites within the scope of the client's organization's ISMS, PIMS or CyberSecure Canada system. The audit shall address the client organization's head office activities to ensure that a single ISMS, PIMS or CyberSecure Canada program applies to all sites and delivers central management at the operational level. If a non-conformity is observed, either at the head office or a single site, the corrective action SOP will apply to the head office and all sites covered by the certificate. MHM will assess if the client would fall under the category of Multi-Site if the sites meet the pre-established criteria defined by MHM.

Integrated audits

Organizations seeking multiple certifications may request a joint or integrated assessment and maintenance assessment visits. In those cases, the following should be taken into consideration:

- Initial assessments should not be performed under an integrated audit or reliance should be kept to a minimum.
- Integrated auditor's competence and expertise
- Integrated audit plans scope
- Ensure that audit time is sufficient for a proper evaluation of the systems
- Documentation may be provided together (i.e. information related to a financial audit, health and safety audit, etc.) as long as the information is relevant to the scope of the audit
- A combined assessment with other management systems may be completed as long as the client can demonstrate meeting all the requirements for the audited system
- The auditor needs to ensure that the information provided and policies are in scope for the services, product or system in scope

Planning Audits

Determining audit objectives, scope and criteria

Audits operate on a three-year cycle (except CyberSecure Canada certifications that operate in a two-year cycle) and visits are normally scheduled within six months or annually. Reports and outcome from audits should provide a complete, accurate, concise and clear record of the audit and should include (but not limited to):

- The audit objectives, scope and schedule
- Identification of the audit client, Engagement Leader, team members
- The audit criteria (ISO27001, CyberSecure Canada, ISO27701, etc.)
- The type of audit (initial, maintenance, re-certification audit)
- The audit findings, evidence and conclusions, consistent with the requirements of the type of audit. The audit report may also include or refer to the following as appropriate
- The audit plan
- A list of client representatives
- Summary of the audit process and objectives
- Any unresolved diverging opinions or issues between the audit team and the client, if identified
- The distribution list of the audit report
- Identification of the certification body
- Clarification and information on nonconformities

- Assessment enquiries which have been followed, rationale for their selection, and methodology employed
- Recommendation by the assessment team on certification of the organization

Readers of the assessment report should be able to:

- Determining the degree of reliance that can be placed in the audit
- Determine from a summary, the most important observations, positive and negative, regarding the effectiveness of the management system
- Determine the conclusions reached by the assessment team

Both stage 1 and Stage 2 reports shall clearly specify what and how many controls within Annex A have been justifiably excluded and accepted by the assessment team. The version of the SOA shall be referenced within the documented scope of registration including both State 1 and Stage 2 reports.

Audit Team Selection

The audit team will be allocated considering the skills and expertise necessary. MHM will select the audit team taking into consideration the following:

- Audit objectives, scope, criteria and estimated audit time
- Whether the audit is a combined, joint or integrated
- The overall competence of the audit team needed to achieve the objectives of the audit
- Certification requirements (including any applicable statutory, regulatory or contractual
- requirements);
- Language and culture

The audit team leader, in consultation with the audit team, shall assign to each team member responsibility for auditing specific processes, functions, sites, areas or activities. Such assignments shall take into account the need for competence, and the effective and efficient use of the audit team, as well as different roles and responsibilities of auditors, auditors-in-training and technical experts. Changes to the work assignments may be made as the audit progresses to ensure achievement of the audit objectives.

The audit team, under no circumstances, will touch or operate any system to avoid possible disruption. The Engagement team leader and the client will agree on assigning a guide to facilitate the audit and address any questions that may arise. The responsibilities of a guide can include:

- Establishing contacts and timing for interviews
- Arranging visits to specific parts of the site or organization
- Ensuring that rules concerning site safety and security procedures are known and respected by the audit team members
- Witnessing the audit on behalf of the client
- Providing clarification or information as requested by an auditor

Audit Plan

MHM shall ensure that an audit plan is established prior to each audit identified in the audit programme to provide the basis for agreement regarding the conduct and scheduling of the audit activities.

The audit plan shall be appropriate to the objectives and the scope of the audit. The audit plan shall at least include or refer to the following:

- The audit objectives
- The audit criteria

- The audit scope, including identification of the organizational and functional units or processes to be audited
- The dates and sites where the on-site audit activities will be conducted, including visits to temporary sites and remote auditing activities, where appropriate
- The expected duration of on-site audit activities
- The roles and responsibilities of the audit team members and accompanying persons, such as observers or interpreters.

MHM procedures shall not presuppose a particular manner of implementation of a Management System or a particular format for documentation and records. Certification procedures shall focus on establishing that a client's Management System meets the requirements specified in the standard and the policies and objectives of the client.

MHM will communicate the tasks and roles for each of the audit team members. The audit team is required to:

- Examine and verify the structure, policies, processes, procedures, records and related documents of the client relevant to the management system standard
- Determine that these meet all the requirements relevant to the intended scope of certification
- Determine that the processes and procedures are established, implemented and maintained effectively, to provide a basis for confidence in the client's management system
- Communicate to the client, for its action, any inconsistencies between the client's policy, objectives and targets.

The audit Plan, proposed audit dates and Team composition will be provided to the client and shall be agreed upon in advance. The client has the right to object to the

appointment of any particular team member and MHM will work with the client to reconstitute the team in response to any valid objection.

Initial Certification

The initial certification audit of a management system shall be conducted in two stages: stage 1 and stage 2

Document and readiness review - Stage 1

When an organization believes they are ready for the certification process to begin, MHM will perform a document and readiness review (DRR) of the organization to determine if its management system is defined and functional. The assessment team will be assessing whether the management system has been implemented for a long enough period of time for there to be an adequate amount of objective evidence of its operation. A minimum operation period of three months will typically be required.

The objective of stage 1 is to gain a sufficient understanding of the design of the ISMS and/or PIMS in the context of the client's organization, the risk assessment and risk treatment (controls) determined, and information security and privacy policies and objectives. In particular, the preparedness for the Stage two Assessment. Additionally, the DRR shall be the input to determine and or confirm that the appropriate audit team is selected and the on-site schedule is prepared to audit the implementation and effectiveness of the ISMS and/or PIMS.

Generally, Stage 1 audits are performed as on-site document reviews. The stage 1 audit may be performed off-site or extended beyond a document review wherever appropriate for the specific client or scope of certification.

The client shall be requested to provide a copy of their organization chart, SOA, Risk Assessment Methodology and the completed Risk Assessment, Risk Treatment Plan, Internal Audit Report and the documented ISMS and/or PIMS policies and procedures. Before inspecting the documentation provided, the Lead Auditor shall ensure that the SOA is appropriate for the scope of the certification and there is at least once SOA per

scope of certification. Details of the client's IT infrastructure and contractual relationships with partner organizations and other remote access arrangements should also be obtained.

Recommendation to proceed to Stage 2 should not be provided if the ISMS and/or PIMS have not been fully implemented for at least 3 months and an internal audit and management review have not been completed or planned to be completed prior to Stage 2.

The DRR assessment will include a review of available system documentation, augmented with some interviews of key management and operations personnel, as required. The assessment team will sample all of the available management system documentation, complete the interviews, evaluate the assessment evidence and prepare a report of the system nonconformities and opportunities for improvement. The audit team will advise the client whether, in the opinion of the Engagement Leader, the organization is ready for the implementation assessment (Stage 2). If the organization is not ready for the Stage 2 assessment, the system shortcoming will be documented in an assessment report presented to the application.

The DRR Assessment will be performed to

- Review the client's management system documented information
- Evaluate the client's site-specific conditions and to undertake discussions with the client's personnel to determine the preparedness for Stage 2
- Review the client's status and understanding regarding requirements of the standard, in particular with respect to the identification of key performance or significant aspects, processes, objectives and operation of the management system
- Collect the necessary information regarding the scope of the management system, including:
    - The client's site(s)

  - Processes and equipment used
  - Levels of controls established (Particularly in the case of multisite clients)
  - Applicable statutory and regulatory requirements

- Provide an opportunity for immediate feedback to the organization
- Plan and allocate resources for further document review where required at Stage 2
- Confirm that an internal audit and management reviews are being planned and performed and that the level of implementation of the management system substantiates that the client is ready for Stage 2.
- Agree with the organization on the details of the Stage 2 assessment

The Engagement Leader will agree with the Client and determine when and where the DRR assessment will take place. For a DRR assessment, the team will obtain, at a minimum, the following information from the client:

- System documentation including procedures (And preferably, a cross-reference list linking the documentation to the related requirements of the applicable Standard)
- A description of the organization and its processes
- The means by which the concept of continual improvement is realized
- An overview of the applicable regulations (Including licenses/permits) and any agreements with regulatory agencies
- Internal audit programs and reports
- Reports of independent review of information security and privacy

- Records (including any records of incidents, breaches of regulation or legislation and relevant correspondence with authorities) on which the organization based its internal audit of compliance with regulatory requirements
- Details of any internally identified nonconformities together with details of relevant corrective and preventive actions taken in the previous 12 months (or since commencement of the system implementation if this is less than 12 months)

During Stage 1, the following documents shall be prepared, and wherever appropriate, released to the client representative:

- Audit Cycle planning - Identifying the significant departments, processes or activities and the related standard requirements within the ADC
- Audit checklist or protocol - The audit checklist is a mandatory record during both Stage 1 and Stage 2. The key ISMS and/or PIMS requirements shall be recorded on stage 1 and Stage 2 individual or combined Audit Reports.
- Stage 1 Audit report – Representing the results of the Stage 1 document review. The report shall be forwarded to the client for any necessary changes prior to the Stage 2 audit.

The DRR assessment will follow the relevant guidelines defined in the applicable Standards.

Implementation Assessment - Stage 2

The objectives of the Stage 2 audit are:

- Confirm that the client adheres to its policies, objectives and procedures
- Confirm that the ISMS and/or PIMS conforms to all the requirements of the ISMS and/or PIMS standards and is achieving the organization's policy objectives
- Evaluate the adequacy of the identification, examination, evaluation, and management of the ISMS and/or PIMS controls and their associated risks

- Determine whether the ISMS and/or PIMS is capable and designed to “Achieve continuous compliance with regulatory requirements applicable to the information security risks or privacy risks from its activities, products and services”
- Determine whether the ISMS and/or PIMS is capable and designed to achieve “continual improvement and reduction of risk”

The audit plan for the Stage 2 audit shall be prepared considering the information gathered during Stage 1 and shall be organized around the departments, processes and/or activities and sites based on the ADC. It is important for the audit team to ensure the timing of the audit which will best demonstrate the full scope of the organization. The audit plan will be provided to the client representative before the audit and will not include any suggestion or guidance to the client for implementing any processes.

Key considerations:

- Interview of top management, management representative
- Top management leadership to information security and privacy
- Documentation requirements listed in the standards
- Assessment of information security and/or privacy related risks and that the assessments procedure consistent, valid and comparable results if repeated
- Addressing of interfaces which services or activities are not completely within the scope of the certification e.g. occurring on the same site
- Determination of control objectives and controls based on the risk assessment and risk treatment process
- Performance and effectiveness of ISMS/PIMS against organization objectives
- Communication within the organization with contractors and third parties including communication in emergency situation

- Correspondence between the determined controls, the SOA and the results of the risk assessment and risk treatment process as well as the organization policies and objectives
- Implementation of controls, taking into account the external and internal context and related risks to the organization's monitoring, measurement and analysis of organizations processes and controls, to determine whether controls are implemented and effective and meet their stated objectives.
- Programs, processes, procedures, records, internal audit reviews and ISMS/PIMS effectiveness to ensure that there traceable to top management decisions and the organization's policies and objectives
- Training, awareness and competence of personnel
- Internal audit including audit schedule, auditor independence and competency, audit procedure and methodology, references and standards, resources and organization, check and verifications performed, audit findings, reports and records, and effectiveness of corrective actions.
- Management review (At least one management review must be conducted prior to Stage 2 certification audit)
- Maintenance and evaluation of legal and regulatory compliance in regard to ISMS/PIMS risks and the client's action taken in case of non-compliance
- The client's procedures for evaluating compliance with legislation

The Stage 2 report and supporting audit records shall be used to provide sufficient detail to facilitate and support the certification decisions. The report shall contain:

- Date(s) of the audit(s)
- Assessment team, observers, accreditation witness auditors if applicable
- Identification of entities audited

- The assessed scope of certification or reference to it, including reference to the standard or other normative document applied
- Assessment methodologies
- If the objectives of the audit were met and if there were any exceptions
- An account of the audit (Stages 1 and 2) including a summary with findings of the two stages
- An account of the certification assessment of the client's risk analysis
- Deviations from the assessment plan (e.g. more or less time spent on certain scheduled activities)
- A summary of the most important observations, positive as well as negative, regarding the implementation effectiveness of the ISMS/PIMS
- The effectiveness of the organization's ISMS/PIMS together with a summary of the evidence with regards to the capability of the ISMS/PIMS to meet its compliance obligations
- Comments on the conformity of the client's ISMS/PIMS with the certification requirements with a clear statement of nonconformity, a reference to the version of the SOA and, where applicable, any useful comparison with the results of previous certification audits of the client
- The conclusions reached by the assessment team
- Recommendations by the assessment team and granting of certification or continued certification

Before the assessment is completed, a meeting will take place with the organization's management team to provide an indication regarding the conformity of the organization's management system. The meeting will be an open forum where members of the organization can ask questions about the findings and their basis. Nonconformities and Opportunities for Improvement will be presented to the

organization in written form and the organization will be able to comment/respond and to describe the specific actions taken, or planned to be taken within a defined time. Major nonconformities, minor nonconformities and opportunities for improvement addressed within 60 days, to remedy any nonconformity with the certification requirements identified during the assessment.

Conducting Audits

Network-assisted audits and use of ICT

Although most of our customers operate in virtual environments and virtual sites and the use of Information Communication Technology (ICT) has become more sophisticated and widely used globally, considerations should be taken prior to conducting a virtual/remote audit using ICT to determine audit feasibility and ensure a consistent approach.

This process is based on IAF MD4 Mandatory Document for the use of Information Communication Technology (ICT) for Auditing Purposes.

Network-assisted auditing techniques may include teleconferencing, web meeting, interactive web-based communications and remote electronic access to the documentation and process to obtain objective evidence. After reviewing the prospect's acceptance documents, understanding the environment, infrastructure and organizational structure of the prospect as well as the scope of the certification. The engagement Leader will discuss with the client the feasibility of performing a virtual/remote audit, what ICT will be used to perform the audit and identify any potential risks of not meeting all the specific requirements necessary to perform an effective and efficient audit. If there are no issues identified, the decision to perform a remote/virtual audit will be agreed upon with the client in the Engagement Letter and reflected in all the planning documentation and communication.

MHM's approved ICT tools and methods will be used to ensure confidentiality and security during remote audits. ICT methods will be discussed and agreed upon with

the client and MHM will be open to discussing ICT methods requested by their clients. (i.e. video conferencing technology or document sharing sites, etc.).

In cases where the ICT plan could not be fulfilled, and the audit objective could not be met, this will be documented in the working papers and report. An alternate method to complete the audit shall be determined and approved by the Engagement Leader and agreed to with the client with documented evidence.

Automated vulnerability Assessment Tools in CyberSecure Canada Assessments

MHM shall use a combination of tools and manual processes to perform audits as per the CyberSecure Canada program requirements. If required, Automated vulnerability Assessment Tools shall support all mainstream operating systems and produce repeatable and comparable results as well as auditable findings that may be used in dispute resolution with customers.

Opening meetings

The purpose of the opening meeting is 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. During the opening meeting, top management should provide a brief introduction of the organization's structure and a brief description of the product/services and primary markets as well as the history and structure of their management system.

The audit team shall consider the following topics:

- Introduction of the participants, including an outline of their roles;
- Confirmation of the scope of certification;
- Confirmation of the audit plan (including type and scope of audit, objectives and criteria), 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;

- Confirmation of formal communication channels between the audit team and the client;
- Confirmation that the resources and facilities needed by the audit team are available;
- Confirmation of matters relating to confidentiality;
- Confirmation of relevant work safety, emergency and security procedures for the audit team;
- Confirmation of the availability, roles and identities of any guides and observers;
- The method of reporting, including any grading of audit findings;
- Information about the conditions under which the audit may be prematurely terminated;
- 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;
- Confirmation of the status of findings of the previous review or audit, if applicable;
- Methods and procedures to be used to conduct the audit based on sampling;
- Confirmation of the language to be used during the audit;
- Confirmation that, during the audit, the client will be kept informed of audit progress and any concerns;
- Opportunity for the client to ask questions.

In addition to the Opening meeting checklist the following items need to be confirmed:

- The latest version of the SOA
- Confirmation that any security clearance requirement for the audit team has been obtained.
- Confirmation that the audit team, under no circumstances, will touch or operate any system to avoid possible disruption.

Communication during the audit

MHM will communicate with the client about the status of the audit and discuss any concerts with the client. If any audit activity indicates that the audit objectives are unattainable or suggests the presence of an immediate and significant risk, the Engagement Leader shall report this to the client and, if possible, to the MHM E-Team to determine appropriate action. Such action may include reconfirmation or modification of the audit plan, changes to the audit objectives or audit scope, or termination of the audit. Suggested changes to the audit scope will also be communicated to SPCS Practice Leader for discussion before taking appropriate action.

During the audit, the audit team shall periodically assess audit progress and exchange information. The Engagement leader shall reassign work as needed between the audit team members and periodically communicate the progress of the audit and any concerns to the client.

Obtaining and verifying information

MHM will request and review information relevant to the audit objectives, scope and criteria (including information relating to interfaces between functions, activities and processes). Information shall be obtained by appropriate sampling and verified to become audit evidence. Methods to obtain information shall include, but are not limited to:

- Interviews;

- Observation of processes and activities;
- Review of documentation and records.

IDENTIFYING AND RECORDING AUDIT FINDINGS AND PREPARING AUDIT CONCLUSIONS

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.

Opportunities for improvement may be identified and recorded, unless prohibited by the requirements of a management system certification scheme. Audit findings, however, which are nonconformities, shall not be recorded as opportunities for improvement.

A finding of nonconformity shall be recorded against a specific requirement, and shall contain a clear statement of the nonconformity, identifying in detail the objective evidence on which the nonconformity is based. Nonconformities shall be discussed with the client to ensure that the evidence is accurate and that the nonconformities are understood. The auditor however shall refrain from suggesting the cause of nonconformities or their solution.

The Engagement Leader shall attempt to resolve any diverging opinions between the audit team and the client concerning audit evidence or findings, and unresolved points shall be recorded. Prior to the closing meeting, the audit team shall:

- Review the audit findings, and any other appropriate information obtained during the audit, against the audit objectives and audit criteria and classify the nonconformities
- Agree upon the audit conclusions, taking into account the uncertainty inherent in the audit process
- Agree any necessary follow-up actions;

- Confirm the appropriateness of the audit programme or identify any modification required for future audits (e.g. scope of certification, audit time or dates, surveillance frequency, audit team competence).

Closing Meeting

MHM will perform a formal closing meeting after every audit with client's management and, where appropriate, those responsible for the functions or processes audited. The purpose of the closing meeting is to present the audit conclusions, including the recommendation regarding certification. Any nonconformities shall be presented in such a manner that they are understood, and the timeframe for responding shall be agreed. The client shall be given an opportunity for questions. Any diverging opinions regarding the audit findings or conclusions between the audit team and the client shall be discussed and resolved where possible. If any diverging opinions are not resolved, they shall be recorded and discussed with the MHM E-Team for appropriate action.

The closing meeting shall also include the following elements where the degree of detail shall be consistent with the familiarity of the client with the audit process:

- Advising the client that the audit evidence obtained was based on a sample of the information; thereby introducing an element of uncertainty;
- The method and timeframe of reporting, including any grading of audit findings;
- The certification body's process for handling nonconformities including any consequences relating to the status of the client's certification;
- The timeframe for the client to present a plan for correction and corrective action for any nonconformities identified during the audit;
- The certification body's post audit activities;
- Information about the complaint and appeal handling processes.

Audit report

MHM will provide a written report for each audit to the client. The audit team may identify opportunities for improvement but shall not recommend specific solutions. The 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:

- Identification of the certification body;
- The name and address of the client and the client's representative;
- The type of audit (e.g. initial, surveillance or recertification audit or special audits);
- The audit criteria;
- The audit objectives including audit methodologies utilized;
- The audit scope, particularly identification of the organizational or functional units or processes audited and the time of the audit;
- An account of the audit including a summary of the document review;
- An account of the certification audit of the client's information security risk analysis;
- Any deviation from the audit plan and their reasons;
- Any significant issues impacting on the audit programme;
- Identification of the audit team leader, audit team members and any accompanying persons;
- The dates and places where the audit activities (on site or offsite, permanent or temporary sites) were conducted;
- Audit findings, reference to evidence and conclusions, consistent with the requirements of the type of audit;

- Significant changes, if any, that affect the management system of the client since the last audit took place;
- Any unresolved issues, if identified;
- Where applicable, whether the audit is combined, joint or integrated;
- A disclaimer statement indicating that auditing is based on a sampling process of the available information;
- Recommendation from the audit team
- The audited client is effectively controlling the use of the certification documents and marks, if applicable;
- Verification of effectiveness of taking corrective actions regarding previously identified nonconformities, if applicable.
- 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;
- A conclusion on the appropriateness of the certification scope;
- Confirmation that the audit objectives have been fulfilled.

CAUSE ANALYSIS OF NONCONFORMITIES AND EFFECTIVENESS OF CORRECTIONS AND CORRECTIVE ACTIONS

In general, a nonconformity shall be considered minor if:

- It is a temporary lapse
- It is unusual / non-systemic

- The impacts of the nonconformity are limited in their temporal and organization scale
- It does not result in a fundamental failure to achieve the objective of the relevant requirement

A nonconformity shall be considered major if, either alone or in combination with further non-conformities, it results in, or is likely to result in a fundamental failure to achieve the objective of the relevant requirement (i.e. completion of internal audit and or to management review during an initial new certification) in a management system assessment. Such fundamental failures shall be indicated by nonconformities which:

- Continue over a long period of time
- Are repeated or systematic
- Affect a wide range of the service, customers or employees
- Are not corrected or adequately addressed by the organization once they have been identified

Any major nonconformity discovered during the certification assessment may result in a delay of the certification of the application. The application must conform with all requirements of the applicable standards for certification in order to successfully complete the assessment. Corrective action for nonconformities will be required by and reviewed thoroughly by the MHM assessment team in accordance with the requirements below. Major nonconformities are required to be closed before certification or re-certification audit activities are completed (i.e. before the report is issued and/or the certification is granted). Minor nonconformities may be left open without a client response during maintenance assessments for the purpose of timely final report issuance. All minor nonconformities should be closed within one year of detection and may be left open longer under justified circumstances to be determined by the Engagement Leader. It is anticipated that a minor nonconformity would not remain open for more than two audits.

To ensure that nonconformities are addressed, the engagement team will complete a documented form with the nature of the nonconformities and provide them to the applicant to provide a written response describing the mitigating factors that they plan to implement and a proposed date for the completion of the mitigating factors. The applicant must complete the corrective action response section and return a copy of the form to the engagement team along with any supporting documentation or evidence showing that the nonconformity has been addressed. The MHM assessment team will assess the action plan developed and actions taken to correct the nonconformity(s) either through a review of documentation or a site visit as appropriate.

Once the nonconformity has been addressed, the Engagement Leader will review the assessment findings, action plan to address the findings, and report. If the assessment findings, action plan and report fulfill the appropriate requirements, the Engagement Leader will sign off the report and approve the recommendation for certification.

The corrective action requests timelines commence on the last day of the audit or the time the findings are formally presented to the client and should have the following timeframes:

- Minor nonconformity should be corrected within a period of one year (under exceptional and justified circumstances, the timeline may be extended to two years) and the time limit should be 30 days for responding to the minor nonconformities.

- Major nonconformities should be corrected within three months. In the event the Major nonconformity cannot be effectively corrected in three months then the Major nonconformity may be downgraded to a Minor nonconformity and left open for up to an additional 6 months if the client provides and acceptable action plan and can demonstrate that the action plan requires a longer timeframe to implement.

Action(s) taken to correct a major nonconformity may continue over a period of time which is longer than the three months, however, action must be taken within the specificized period which is sufficient to prevent new instances of nonconformities within the scope of the certification. Rationale for extending timelines should be on an exception basis and documented. They may only be approved by the Engagement Leader. It is important to note that it is not uncommon for action(s) to adequately address a major nonconformity to continue over a period of time which is longer than two months. However, each of the client's actions must be taken within the specified timeline and documented in the corrective action response which is sufficient to prevent new instances of nonconformity or recurrence. The assessment team will be reasonable and take due care when assessing and accepting the Client's responses and associated timelines for the actions.

MHM shall determine whether corrective action requests have been appropriately implemented within their time frames. If the action taken is not considered adequate then a Minor nonconformity shall be escalated to a Major nonconformity and addressed as noted above and if a Major nonconformity is not addressed as above, it may lead to immediate suspension of the certificate.

MHM shall not issue, re-issue or lift suspension without reasonable cause of a certificate that has open major nonconformities. As a guide, the occurrence of five or more major nonconformities in a maintenance audit should be considered as a breakdown of the company's management system, and the Engagement Leader shall consider if the certification should be suspended immediately. This shall be discussed with MHM's E-Tem prior to a final decision.

CyberSecure Canada Directions on Nonconformities

For CyberSecure Canada certifications, minor nonconformities can have the corrective action reviewed at the annual surveillance audit and major nonconformities shall have the corrective action review within ninety days.

Certification Decisions

MHM will not delegate its authority for granting, maintaining, extending, suspending or withdrawing certification to an outside person or body.

Procedures for issuing, retaining, suspending, withdrawing or reducing the scope of the certification are discussed below. The engagement leader will request an application for amendment to certification in the case of material changes in products, ownership of the client organization, application structure or management, or any relevant information. Any application for amendment to the scope of a certification shall be reviewed by MHM's E-Team. The Engagement Leader will decide what, if any, assessment procedure(s) is/are appropriate to determine whether or not the amendment should be granted and if necessary, assign the assessment procedure(s) to an audit team.

The final review and certification decision is confirmed by MHM's E-Team. The certification decision shall incorporate a level of knowledge and experience sufficient to evaluate the verification processes, working papers and associated evidence and recommendations made by the audit team. The leader of the SPCS Practice shall approve the integrity of the review procedures, including the review of the final audit report, ensuring that the procedures documented in the BMS manual are followed, ensuring that MHM specific procedures or policies are followed by the assessment team, ensuring all working papers files tasks are completed , ensuring that the Engagement team has addressed and resolved all outstanding issues in the client file, and, for integrated management system audits, if a nonconformity found for the management system may have an impact on the other audits. Certification shall not be 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.

If the decision is to not grant a certification, the Engagement Leader will notify the client of the decision and identify the reasons for the decision. If MHM is not able to verify the implementation of corrections and corrective actions of any major

nonconformity within 6 months after the last day of stage 2, another stage 2 audit shall be conducted prior to recommending certification.

MHM will follow the same process for renewing certifications based on the results of the recertification audit, as well as the results of the review of the system over the period of certification and complaints received from users of certification.

Certification transfer

Before accepting a certification transfer, the following matters should be addressed:

- Prospect will undergo the same risk and scoping procedures as any new client
- Prospect should provide a valid accredited certificate issued by the previous Certification Body (CB), and there shall be an Accreditation Mark on the Certificate to represent the specific Accreditation Body (AB)
- The prospect shall provide their last two audit reports issued by the previous CB and a valid accredited certificate. MHM shall notify the previous CB requesting and confirming if the Certificate is valid and if the client is in good standing.
- Status of open or closed non-conformities from the previous CB which may lead to a certificate suspension or withdrawal.
- Corrective actions from previous non-conformities
- Latest SOA
- Consideration shall be given to carrying out a document review to allow the audit team to familiarize themselves with the client's environment in order to prepare the Engagement Plan for the following audit.

When an existing, valid certificate was granted by a different accredited certification body, it will be recognized by MHM. MHM can issue our own certification to replace the pre-existing certificate. This transfer function enables clients to switch certification bodies without the need for an extra full implementation or Maintenance assessment.

After a transfer assessment is completed, the certificate will then be valid for the same length of time as the pre-existing certificate, and the existing assessment schedule will be maintained as agreed by MHM and the client.

A transfer certification could also be triggered by a client looking to switch to another certification body. A client initiated transfer is dealt with in the same way as a client initiated withdrawal.

Only certificates that are covered by a recognized international multilateral recognition agreement (MLA) will be eligible for transfer. Certificates held by organizations that are not part of an MLA will be treated by MHM as new certifications.

Transfer will be normally completed only for current, valid, accredited certificates. In cases where the existing certification body has ceased business or their accreditation has expired, suspended or withdrawn, MHM may, at the discretion of MHM's E-Team, transfer the certificate. In this case, MHM will obtain agreement from the SCC prior to transferring the registration.

Certificates which are known to have been suspended or under threat or suspension will not be accepted for transfer prior to completion of a full certification assessment.

For transferring certificates to MHM, the Engagement Leader will advise the client verbally and, in our proposal, that seeking transfer of its certification will require termination of the current certification agreement. The client will be advised that this should be completed in accordance with the requirements described in the Terms & Conditions of the existing registration contract and that certificates may be transferred only once in a 3 year period. Suspended certificates will not be transferred in.

MHM proposals will suggest that, following the proposed certification Transfer Assessment, and a successful transfer of the certification, that the client should return the original certification certificate with a request to remove the certified organization's name from the register maintained by the current certification body.

For MHM to assume an existing certification, the Engagement Leader will complete (i) a review of the existing management system process documentation (Document

review) within the scheduled maintenance period, and (ii) an assessment of the degree of effective implementation of the management system. In assuming an existing certification, MHM would rely on the certification work completed by the existing certification body up to the time of transfer. To assess the degree of effective implementation of the management system process prior to transfer, the Engagement Leader would review the following items:

- Presence of a valid certificate and an accurate scope of certification
- Reasons for seeking a transfer of certification
- The most recent initial assessment, re-assessment and maintenance assessment reports, and resolution of any outstanding nonconformities
- Assessment documentation such as assessment protocols, checklists, and other working papers provided to the client by the existing certification body
- Legal disputes, if any, with regulatory agencies
- Any complaints received and action taken

The document and readiness review section of the BMS manual (Stage 1 assessment) and the Implementation assessment section of the BMS manual (Stage 2 assessment) will be used to guide the assessment process required for the transfer.

The Engagement Leader may also contact the existing certification body if practical and ask to confirm the status of outstanding major and minor nonconformities, the status of the existing certificate, and existence of any other circumstance of concern, including fraud or illegal activity. If outstanding nonconformities are not closed out by the previous certification body, they will be reviewed and their status re-assessed by MHM in order to close them out.

Where doubt exists about the effectiveness of the management system following the transfer assessment, the Engagement Leader may decide to (i) contact the organization and complete an assessment contracting on specific problem areas, or (ii) Treat the application for transfer as a new certification. This decision will be based on the nature

and extent of the issues identified during the Transfer assessment, and the justification for the decision documented and retained in the working paper files.

After a successful transfer assessment, a certificate would be issued. The schedule of maintenance assessment and certification assessments established by the existing certification body would be followed by MHM unless the transfer has been completed as an initial certification assessment.

For transferring out certifications, the following requirements is in the engagement letter signed by MHM and the client:

> "Discontinue its use of all advertising materials that contain reference to certification by MHM and return any certification documents requested by MHM, in the event that the certification is suspended or withdrawn by MHM or the Company"

Therefore, when a client initiates a transfer to another certifying body or initiates withdrawal, MHM will request or send a communication to the client requesting return of the certificates and to no longer refer to MHM as their certifying body in any internal/external documents or websites. MHM's internal system must also be updated to reflect that the client is no longer active.

Maintaining certification

MHM shall maintain certification based on demonstration that the client continues to satisfy the requirements of the management system standard. It may maintain a client's certification based on a positive conclusion by the Engagement leader without further independent review and decision, provided that:

- For any major nonconformity or other situation that may lead to suspension or withdrawal of certification, MHMy has a system that requires the Engagement Leader to report to the the need to initiate a review by competent personnel, different from those who carried out the audit, to determine whether certification can be maintained;

- Competent personnel of MHM monitor its surveillance activities, including monitoring the reporting by its auditors, to confirm that the certification activity is operating effectively.

Surveillance Activities

The registration certificate provided by the certifying body for management system standards is valid for a period of three years after the certification decision date, and for a three year period thereafter, as long as the Maintenance Assessment results are satisfactory. For a three-year certificate at least two maintenance assessments shall take place before the certificate expires. Certificate expiration dates may not be extended. The re-assessment can be completed and the certification decision date can be completed within 6 months of the certification expiration date; however, the new certificate expiration date will remain within the three years of the previous certificate date.

As with the other audits. Surveillance audits shall take into consideration the scope of the certification, skills and expertise necessary and industry sector qualifications of the audit team.

Surveillance audit programs shall cover at least:

- The system maintenance elements such as risk assessment and controls maintenance, internal ISMS/PIMS audit, management review and corrective actions
- References to certification and use of certification marks
- Effectiveness of the ISMS/PIMS to meet organizational objectives
- Continual improvement
- Security/Privacy incidents
- Changes to the controls determined and resulting changes to the SOA

- Implementations and effectiveness of controls in accordance with the audit programme
- Records of risk assessment
- Communications from external parties as required by the ISMS/PIMS and other documents required for certification
- The information security and/or privacy issues related to risks and impacts on the clients
- Changes to the ISMS/PIMS documented system
- Selected requirements of standards in the scope
- Planned arrangements for changes in processes and systems
- Actions taken as a result of nonconformities identified during past audits

The audit team should also check the records of appeals and complaints. The areas to be assessed during the maintenance visit will be influenced by the structure of the client's operations. The auditor shall ensure that the client has maintained resources, working practices and an environment appropriate for the product or service being offered.

CyberSecure Canada Surveillance audits

Surveillance audit activities for CyberSecure Canada certifications, will consist of a review of the client's environment to identify changes which are relevant to the scope of certification, along with a review of all controls and updated documentation. Follow up on nonconformities will also be performed.

Re-certification and certification expiry

MHM will make every effort to initiate the planning process for the re-certification assessment to allow for reasonable time to complete the re-certification assessment prior to the expiry of the existing certificate. Considerations for reasonable time to

enable a successful recommendation and decision for example, may include risks associated with logistics, availability or competent assessors, verify implementation of corrective actions associated with major nonconformity to either close them or to the review of an acceptable corrective action plan, including partial implementation of the plan which would enable the assessment team to downgrade the major to a minor nonconformity.

When recertification activities are successfully completed prior to the expiry date, the expiry date of the new certification can be based on the expiry date of the existing certification. The issue date on a new certificate shall be on or after the re-certification decision.

In cases where the re-certification assessment activities extend past the expiry date or where the Engagement leader has been unable to verify the implementation of corrections and corrective actions for any major nonconformity, the re-certification will not be recommended and the certificate shall not be extended. However, the certification can be restored within 6 months of the expiration provided the outstanding re-certification activities are completed, otherwise a Stage 2 assessment will be completed.

In such cases the certificate issue date on the new certificate(s) shall commence on or after the re-certification decision date, approved by the MHM E-Team, and shall expire based on the prior certification cycle (e.g. within 3 years of the previous anniversary expiration date)

Re-certification assessments may be conducted in place of a Maintenance assessment and or prior to the existing certificate expiry date. In the event of an early re-certification assessment the expiry date on the certificate shall be within 3 years of the re-certification decision date. The regular 12 months maintenance assessment cycles will commence from this date forward.

The re-certification assessment will involve:

- A review of management system documentation

- A review of past implementation and continuing maintenance (including complaints received from users of the certification) of the management system over the period of certification.

The re-certification assessment will at least ensure:

- The effective interaction between all elements of the management system
- The overall 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 the certification
- Demonstrated commitment to maintaining the effectiveness and improvement of the management system in order to enhance overall performance
- The effectiveness of the management system with regard to achieving the certified client's objectives and the intended results of the respective management systems(s)

The assessment methodology for the re-certification will follow the procedures outlined under the certification assessment section of this manual. Steps 1 (application form) and 2 (proposals) described in these procedures will not be completed during the re-certification unless the project is subject to re-proposal. Other steps such as a separate DRR, may not be performed if the Engagement Leader determines that there have not been significant enough changes to warrant it.

Special audit

In cases where MHM learns and or is notified – Through formal or informal channels – of major changes in the certification scope, site location and infrastructure. The Engagement Leader will determine whether a site visit is required and inform the client accordingly. Refusal of the client to cooperate may lead to immediate suspension of the certificate.

Recertification due to management system scope change

The decision to extend or reduce the scope of a certification will be determined by the client in conjunction with the Engagement Leader. Both parties must agree to any changes in the scope of the certification.

Scope change requests will be treated as new requests and will require completion of all the scoping documentation. The following should be considered:

- The client has reassessed the risks to cover the new service/product systematically
- The risk treatment plan has been proposed on the risk assessment result
- If any high-risk activity is involved in the scope change
- If any new technology is involved in the scope change
- Whether the client internal system covers the scope change

Any extension or reduction of the scope of certification will require that amendments are made to the existing Engagement Letter for the specific engagement in question. Amendments must be documented and cannot be verbal. The wording of the amendments must be approved by both the client and the Engagement Leader.

MHM can decide to re-assess an organization's management system in the event that significant changes occur that affect the activity or operation of the organization. These events may include, and are not limited to:

- Change of ownership
- Change of key personnel
- Change of key pieces of operating equipment
- Change of legislation/regulation
- Change of product/services

- Change in the certification standard
- Change of legal, commercial or organizational status
- Change of contract address
- Change of scope of operations under the certified management system
- Changes to the management system and processes
- In the event of an analysis of a complaint or any other information indicating that the certified organization is no longer complying with our certification requirements

The determination of whether the organization must be re-assessed will be at the discretion of the Engagement Leader and the MHM's E-Team.

The following steps will be used to complete a recertification:

- Re-certification contract
    - Establish cost, time and other resources required
- Determination of the effects of the change
    - Which areas of the business are affected by the change
    - What new aspects and impacts may be created by the change
    - What is the level of significance of these new aspects and impacts
- Development of the recertification plan (Assessment plan)
- Re-certification assessment
    - Only areas affected by the change will be assessed
    - Opening meeting
    - Collection of evidence

    - Determination of findings
    - Closing meeting
- Re-certification report
    - Draft report
    - Report distribution
- Certification
    - Issuance of a new certificate of certification

The conditions for MHM to change the scope of a certificate shall include the following requirements:

- The change of scope shall not include or result in an extension of the certificate's expiry date beyond the time period for which it was originally issued
- The certification boy shall reserve the right to inspect the site of the certified operations or related documentation to the management system before deciding whether or not to grant a change to the scope of the certificate
- If MHM grants a change of scope, the wording of the certificate previously issued shall be reviewed and if necessary, shall require that the old certificate be returned to MHM or destroyed by the client and in that event, a new certificate shall be issued with revised wording reflecting the change of scope.

If revisions to the standards are made by the issuing body. MHM will follow the requirements of the issuing body and the requirements of this manual and describe the service delivery process specific to each Standard that was revised. The Leader of the SPCS Practice will assess changes to the standards and prepare a transition plan. The transition plan will consist of an internal plan to make relevant changes to the BM and training requirements for assessment staff. An external client communication plan will be developed outlining the changes and MHM's process to transitioning the existing certified management system to the revised standard. Engagement Leaders are

required to communicate the transition process to clients through email and or during client meetings.

Short-notice audits

It may be necessary for MHM to conduct audits of certified clients at short notice or unannounced to investigate complaints, or in response to changes, or as follow up on suspended clients. In such cases:

- MHM shall describe and make known in advance to the certified clients the conditions under which such audits will be conducted;
- MHM shall exercise additional care in the assignment of the audit team because of the lack of opportunity for the client to object to audit team members.

Suspending, withdrawing or reducing the scope of certification

MHM will consider suspending or withdrawing certification in the following situations:

- 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
- The certified client has not paid their certification fees
- The occurrence of five or more major nonconformities in a maintenance audit shall be considered as a breakdown of the company's system and the certificate shall be suspended immediately

When a client's certification is suspended, the client's management system certification is considered temporarily invalid. The status of the suspended certification will be recorded in MHMs certification records and will be made publicly available on request.

The Engagement Leader will communicate to the client the actions needed to end suspension and any other actions required.

Failure to resolve the situation within sixty days, will result in either a reduction in the scope of the certification or withdrawal of the certification. Any evaluations, reviews or decisions needed to resolve the suspension or withdrawal will be conducted and reviewed using the same general requirements as certification assessments specified in the BMS.

MHM will reduce the scope of the certification to exclude those activities not meeting the requirements when the client has persistently or seriously failed to meet the certification requirements. A reduction in scope could also be a condition of certificate reinstatement. The reduction of scope will be in line with the requirements of the certification standard.

MHM will advise clients that upon receipt of written notice to withdraw the certification, the client must discontinue its use of all advertising materials that contain any reference to certification status.

The Engagement Leader will follow the following procedures to suspend, withdraw or reduce the scope of a certification:

- Change the status in MHM certification records spreadsheet and make notes in the comment field
- Inform the client in writing of the change, and if certification is suspended or withdrawn, that they must refrain from further promotion of its certification. If the certification is reduced scope, the client must refrain from further promotion of the products, services or locations no longer certified. The notifications shall contain:
    - A clear statement about the invalid status of the certificate (expired, suspended, withdrawn or terminated)
    - The date from which the invalid status of the certificate is official

- The rationale supporting the invalid status of the certificate which shall include, but it is not limited to, the details of the breach of the certification contract and the demonstration of non-conformity with the applicable certification requirements
- The requirement to withdraw all uses of Trademarks
- in the case of an expired, terminated, suspended or withdrawn certification, the requirements to stop making claims and/or using controlled material
- In the case of suspended certificates, the information that the maximum duration of suspension is six months and after this period, the certificate will be withdrawn
- A statement requiring the client to acknowledge receipt of the letter of notification in writing.

- Upon request by any party, state the status of certification

The maximum period of suspension is six months. After this period, the certification shall be withdrawn, unless all major non conformities have been successfully corrected.

Any decision on whether to reduce the scope of the certification to to temporarily or permanently withdraw the certification will be determined during a review process with MHM's E-Team.

MHM will advise its certified clients that it should promptly notify MHM of any intended change to the organization's Management system or other changes that may affect conformity, as specified in the Engagement Letter. MHM may be required to perform a Short-notice assessment of a client (i) to investigate complaints received from interested parties of the certified client (ii) in response to changes in the client's management system or (iii) as a follow up visit to a client whose certification has been suspended.

For integrated audits, if certification to one or more management system standards/specifications is subject to suspension, reduction or withdrawal, the Engagement Leader shall investigate the impact of this on the certification to the other management system.

All final decisions relating to suspending , withdrawing or reducing the scope of a certification will be documented by MHM.

All MHM clients whose systems have been certified, will make available to the Engagement Leader, upon request, records of relevant communications, including complaints and actions taken. This requirement is included in the Engagement Letter signed by the client.

Complaints represent a valuable source of information as to possible system nonconformities. Organizations Certified by MHM are required to maintain processes and procedures for managing relevant communication, including complaints, from external interested parties. Their processes and procedures will include mechanisms for establishing and reporting, where appropriate, on the cause of nonconformity.

During our maintenance assessments, a member of the audit team will review evidence of these system nonconformities if any, and the corrective actions taken. MHM will ascertain if the certified organization has taken appropriate measure to:

- Notify the applicable regulatory agencies, if required by legislation or regulations
- Restore system conformance as quickly as practicable
- Prevent recurrence
- Evaluate and mitigate any adverse system or product impacts
- Ensure satisfactory interaction with other components of the system
- Assess the effectiveness of the corrective action taken

Corrective actions will not be deemed to have been completed unless their effectiveness has been demonstrated, and the necessary changes made to the system procedures, documents and records.

Appeals and Complaints

Definitions

Appeal - An appeal is a request by the client or responsible party for MHM to reconsider its decision relating to a certification.

Complaint - A complaints is the expression of dissatisfaction, other than an appeal, by any person organization to MHM relating to its activities, where a response is expected

Procedure for appeals and complaints

This process applies to all appeals and complaints addressed to MHM whether resulting from a certification or revealed at other times during the engagement. MHM will be responsible for all decisions, at all levels of the appeals and complaints handling process, unless and until the issue is escalated to the relevant accreditation body, the relevant regulator or MHM's legal counsel. MHM will fulfill its duty of reasonable cooperation with all accreditation bodies.

Channels for receiving appeals and complaints include the MHM Appeals and Complaints landing page in our public website, a request directed to MHM's E-Team, as well as general enquiries (under "Contact Us" in the MHM's website). Channels for receiving appeals and complaints are communications to clients in the Planning Memo and Engagement Letter. The complainant or appellant must include a clear description of the complaint or appeal, objective evidence to support each element or aspect of the complaint or appeal and the name and contact information of the submitter.

Persons leading the appeals and complaints handling process will be different from those who carried out the certification.

IDENTIFICATION OF APPEALS AND COMPLAINTS

- Appeals and complaints must be formally addressed to MHM's E-Team in writing and will be handled in accordance with MHM confidentiality policies.
- MHM's E-Team will acknowledge all appeals and complaints in writing within 14 business days of receipt
- MHM's E-Team will appoint an independent senior MHM staff member to investigate appeals or complaints. (The investigator)
- To ensure independence, the MHM E-Team will consult with the Engagement Leader to determine if an existing relationship may compromise the ability of the assigned investigator to maintain impartiality in overseeing the resolution of the appeal or complaint.Any MHM personnel that has consulted for, or been employed by the client within two years shall be used in the appeal/complaint process.
- Appeals or complaints shall initially be investigated to identify whether the issue is due to the certification of MHM. The investigation will consider the effectiveness of the client's management system process. Clients who are the subject of an appeal or complaint will be notified at the time of the appeal or complaint is acknowledged in writing.
- The appeal and complaint handling process shall include tracking and recording appeals and complaints, including actions undertaken to resolve them. This will be done in the Appeals and Complaints register stored in MHM's Google Drive.
- MHM's E-Team will ensure that the necessary information is gathered in order to validate an appeal or complaint. The practice leader, and the investigator, in consultation with the client, will determine whether to make information about the appeal or complaint public, and if so, to what extent

- MHM will ensure submission, investigation decisions on appeals or complaints do not result in any discriminatory actions by MHM against the appellant or complainant.

Investigation process for appeals or complaints

- Upon receipt of an appeal or complaint, the SPCS practice Leader will appoint an independent senior MHM staff member to investigate appeals or complaints. (The investigator)

- The investigator, in consultation with the client or third party, will determine if the parties can ding a mutually-agreed upon solution to the appeal or complaint

- The investigator will consider the results of previous appeals or complaints involving clients or third parties

- The investigator will review and document appeals and complaints brought to MHM and will ensure that where any nonconformity or failure to meet the requirements of MHM's certification is revealed, that the provider of the object of conformity assessment has investigated its own management systems and procedures and taken appropriate corrective action.

- The actions taken by the organization will be documented by the investigator and communicated to the Engagement Leader who was primarily responsible for the relevant engagement. The Engagement Leader will ensure that the actions for effectiveness are assessed at the next assessment. The report(s) documenting the outcome of the actions taken and results of the assessment will be reviewed and approved by MHM's E-Team.

- The investigator will prepare a written statement outlining the actions taken, the resolution of the appeal or complaint, and the reasons for the decision reached.

- MHM's E-Team will review and approve the resolution before providing it to the client or third party

- MHM's E-Team will clearly indicate to the appellant or complainant the termination of the MHM appeal or complaint process, as appropriate in the circumstances
- MHM shall keep the complainant informed of progress in evaluating the appeal or complaint, and shall have investigated the allegations and specified all its proposed actions within six months of receiving the appeal or complaint
- The SPCPS Practice Leader shall determine, together with the client and the complainant, whether and, if so to what extent, the subject of the appeal or complaints and its resolution shall be made public
- The investigator will document the decision statement in the client's certification file
- The investigator will document correction or corrective actions taken in the client's file and addressed in this BMS, as appropriate

If the MHM E-Team member is not independent from the appellant or complainant (i.e. he was directly involved in the certification process or provided other services to the appellant or complainant) his role described above will be delegated to another MHM E-Team member who is independent.

Internal escalation of appeals or complaints

If the appeal or complaint cannot be resolved by the process described above the investigator or MHM E-Team member will escalate it to an MHM E-Team member who is independent of the certification practice. The MHM E-Team member will review the appeal or complaint and discuss the issues surrounding the problem(s) with the investigator, the MHM E-Team member and the client or third party as appropriate, with the goal of reaching mutually agreeable solution within two months of the receipt by the MHM E-Team member.

The MHM E-Team member will document in a written statement to the client or third party, the actions taken, the resolution of the appeal or complaint, including reasons for

the decision clearly indicating the termination of the MHM appeal or complaint handling process as appropriate, Upon requests regular progress reports will be issued to the client or third party. The E-Team member will also document the decision statement in the client's certification file and any corrections or corrective actions taken.

Appeals or complaints raised to accreditation bodies from MHM

In the event that a mutually agreeable solution to an appeal or complaint against MHM cannot be reached. MHM will advise the client or third party it can appeal the decision to the appropriate accreditation body, and the appeals or complaint findings will be made available by MHM to the accreditation body for resolution.

The SPCS Practice Leader will ensure that the client or third party is advised that the accreditation body review will consist of a determination of whether MHM has operated in conformity with all of the accreditation body requirements, the standard for which MHM has been accredited, the accreditation agreement (Between MHM and the accreditation body) and MHM's internal certification procedures in the processing of the appeal or complaint, and that the accreditation body is the final level of appeal or complaint resolution.

Timing of appeals and complaints

Clients will be given 10 days following the release of MHM's management system assessment report to launch an appeal of complaint against the results of the assessment. Appeals or complaints must be made in writing and will be acknowledged in writing. Verbal appeals or complaints will not be accepted. Any appeals or complaints dated later than 10 days after the release of MHM assessment results will not be accepted, unless required by the terms of its accreditation agreement.

Effectiveness evaluation of Appeals and Complaints process

MHM will review its actions with MHM E-Team stakeholders to determine the effectiveness of the process. The results of this review will be documented and maintained in the BMS continual improvement folder.

Use of the Certification Body's Name and Certification Mark or Logo

An organization must only claim that it is certified with respect to those activities for which it has been granted certification.

The organization must not make any statements regarding its certification that MHM, or the public, may consider misleading or unauthorized. The organization must ensure that the certification mark, or report, or any part thereof, is not sued in a misleading manner.

The organization must discontinue the use of all advertising that contains any reference to its certification in the event of suspension or withdrawal of its certification documents by MHM. In the event of suspension or withdrawal, the organization must immediately return its certificate(s) or certification to MHM. In the event of a scope reduction, the organization must amend all advertising materials.

The organization must only use its certification to indicate that the organization's system is in conformance with the applicable standard, and must not use the certification to imply that its products or services have been approved by MHM. The organization must comply with the requirements and restrictions from MHM when making references to its certification in any form of communication media.

Only organizations certified by MHM to a particular standard, have the following rights:

- To indicate to the public in spoken, written or visual communication that they have been certified by MHM to a particular standard. The standard must be specified in the communication. All methods of communications regarding the

certification that are directed toward the public, in whatever form they make take, must be approved by the Engagement Leader, prior to their release

- To utilize the applicable MHM Mark in public communications or certification marks, only with the express written consent of MHM. Prior to use of the applicable logo, the organization must sign the relevant contract agreement with MHM.

If a certification Mark ("Mark") is applied to a product, process or service that has not been authorized to bear it, or is in violation of an agreement with MHM or the Standards body. MHM will investigate the potential misuse of the Mark to the extent required by the relevant standard. There shall be no ambiguity, in the Mark or accompanying text, as to what has been certified and which certification body has granted certification. The Mark shall not be used on a product or in any other way that may be interpreted as denoting product conformity.

MHM will not permit its Marks to be applied by certified clients to laboratory test, calibration or inspection reports or certificates.

If the misuse of the Mark is confirmed, MHM shall take immediate corrective action against the misusers. The type of corrective action will depend on the nature of the misuse, and its subsequent consequences. If the misuser no longer exists, MHM may notify the client and seek legal advice on proceeding.

The initial notification to the misuser will be a written letter that includes:

- The reason for the corrective action
- Any hazardous conditions that may exist
- The actions to be taken by the misuser to resolve the problem
- A statement covering the action to be taken to ensure that the Mark of conformity is not applied to ineligible products

When MHM is satisfied with the corrective action taken by the misuser, another letter shall be sent to the misuser and any other recipients of the first letter. This letter shall state the Mark has been reinstated and suspension of the Mark has been lifted. The letter will summarize the corrective action taken, and describe the new marking required to distinguish the acceptable product from the unacceptable product. Any records of certification will be revised to include any modifications resulting from the corrective action.

MHM may also assess its own procedures to determine (i) whether part of the misuse of the Mark was due to the weakness on part of MHM and (ii) any alterations to our certification and maintenance assessment process are required so that similar misuse will not be repeated.

If a misuser refuses to take suitable corrective action, MHM may take one or more of the following steps:

- MHM may cancel all the certification contracts
- The misuse will be publicized
- Legal advice shall be obtained, and appropriate legal action taken, if necessary

Usage of Marks and logos owned by standards organizations is governed by license agreements between the certified organization and the standards-setting organization. MHM will be responsible for assessing the appropriate usage of marks or logos during the certification assessment process, to the extent specified in the standard.

Restrictions

It is the responsibility of the certified organization to ensure that any material published with the MHM logo attached to it is factual, and that any commentary is not misleading. Certified organizations and applicants are responsible for ensuring that their subsidiaries, affiliates and any agents they utilize are not in contravention of the restrictions.

Public relations and advertising should be closely scrutinized by certified organizations and applicants engaging the services of agents to ensure that it contains nothing objectionable. Certified organizations and their subsidiaries, affiliates and agents should ensure that advertising does not appear in media which might tend to lower public respect for MHM.

The organization must use its certification in such a manner as to not bring MHM into disrepute and certified organizations shall not advertise directly or indirectly, in any manner which makes unfavourable reflections on the competence or integrity of MHM or any employee or subcontractor thereof.

Information requirements

Public information

Refer to this landing page https://mhmcpa.ca/iso-certification-audit with details about the MHM's SPCS Practice, geographical areas in which it operates and information about the audit processes, types of management systems and certifications that are offered and impartiality policy. In addition, there is a public form for obtaining details about granting, refusing, maintaining, renewing, suspending, restoring or withdrawing certification or expanding or reducing the scope of certification as well as the use of the certification body's name and certification mark or logo and processes for handling requests for information, complaints and appeals.

MHM shall provide information upon request about:

- Geographical areas in which it operates
- The status of a given certification
- The name, related normative document, scope and geographical location (City and country) for a specific certified client

Information provided by MHM to any client or in the marketplace, including advertising, shall be accurate and not misleading.