PURPOSE

To describe a procedure for audit planning, conducting the audit, preparation of reports and submitting the reports.

SCOPE

This procedure covers audit planning, execution of audit and reporting for all types of audits as listed below.

- Stage 1 audit
- Stage 2 audit
- Follow up audit
- Surveillance audit
- Recertification audit
- Transfer audit

RESPONSIBILITY

AUDIT TEAM LEADER

Is responsible for the delivery of the above-mentioned audits either working alone or as leader of a team of Auditors. It is the responsibility of the Audit Team Leader to make recommendations to the Certification Manager on the issuance of the certification. It is responsibility of the Audit Team Leader to review report drafts prepared by Audit Team Members.

The audit team 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.

AUDIT TEAM MEMBERS/AUDITORS

Are responsible for execution of audits and preparation of and submitting the audit reports. An Auditor may work unsupervised during an audit. However, the audit report and supporting documentation are required to be reviewed by an Audit Team Leader. It will be the role of the Audit Team Leader to determine the level of autonomy allowed based on the auditor's experience.

AUDIT PROGRAM MANAGER

Is responsible for reviewing applications for certification in order to:

- determine whether Bulletproof has the competence and ability to perform the certification activity,
- determine the audit team competence required,
- select the Audit Team Members,
- develop an Audit Program for the full certification cycle

It is the responsibility of the Audit Program Manager to make a recommendation on whether to accept or decline an application for certification.

It is the responsibility of the Audit Program Manager to review and approve of the Audit Plans prepared by the Audit Team Leader (Initial Certification audits, Recertification Audits and Surveillance audits).

It is the responsibility of the Audit Program Manager to ensure there is no conflict of interest between the Applicant Organization (Customer) and the Audit Team Members (for guidance please see “Impartiality

Policy"). Certification Manager is the chairman of the Certification Committee. The decision to grant/suspend/withdrawn a certification will be the result of evaluations performed by the members of the Certification Committee and will be signed off by the Certification Manager. The decision to accept/decline an application for certification will be the result of evaluations performed by the members of the Certification Committee and will be signed off by the Certification Manager.

CERTIFICATION COMMITTEE

The Certification Committee reviews:

- applications for certification to determine whether to accept or decline applications.
- audit reports from audits to establish that the audit team recommendations for Certification are arrived at through adherence to prescribed procedures and are supported by the evidence gathered during the audit.
- audit team support documentation with respect to recommendations for new or changes to an existing Certification.
- audit team leaders' recommendations for Certification issuance, suspension or withdrawal.

It is the responsibility of the committee to identify the needs for training of personnel where repetitive errors are made, or client appeals are found to be justified.

It is the responsibility of the committee to provide feedback to audit teams where deviations from the prescribed procedures are found.

Audit reports from visits subsequent to the Initial Certification which recommend a change to the Certification status, are also subject to review by the Certification Committee.

CERTIFICATION COORDINATOR

It is the responsibility of the Certification Coordinator to create and process the certificates and to communicate audit results and certification decisions to the client. The Certification Coordinator shall act as the focal point of contact for the client.

DESCRIPTION OF ACTIVITY

INTRODUCTION

The objective is to provide consistent service delivery norms. Audit Team Leaders and auditors are responsible for ensuring the objectives of their assigned audits are fully met. The various activities needed to be carried out are:

- Document review - Stage 1 Audit
- Initial Certification Audit - Stage 2 Audit
- Follow- Up Audit
- Surveillance Audit
- Recertification Audit
- Special Visit

AUDIT VISIT

The purposes of the audit visits are to provide reasonable assurance that the auditee organization's Management System conforms to the requirements of the standard applied, as stated in the Certification Contract, and to verify that the documented system has been implemented. The audit also serves to verify that the Management System is appropriate to auditee organization's activities.

Audit Program Manager is responsible for selection of the audit team. Unless required for technical reasons and logistics, care shall be taken to ensure that same auditor does not visit the client more than four consecutive visits. This shall ensure "no bias" and a fresh look at the system. All auditors / contractors are responsible for identifying any conflict of interest with the specified client and report to Audit Program Manager who shall take necessary decision (which may include replacing the person with some other auditor).

A set of updated documents pertaining to the audit, such as client details, open non conformances, surveillance plan and comments from prior visits as applicable) is provided to every audit team. Activities include the opening meeting with the auditee organization, team briefings, audit interviews, non-conformity issuance, auditee organization briefings, and the closing meeting with the auditee organisation. The Audit Team Leader issues an audit report reflecting the recommendation concerning certification based on the team findings.

If major non-conformities are found, the recommendation will be on hold until suitable corrective action has been taken and evidenced.

During the audit if the Auditor finds a breach of legislation i.e. legal/regulatory/ statutory requirement not having been followed, the auditor will communicate his finding to the Audit Team Leader who in turn will notify the auditee organization's management of the violation. The auditor will further investigate the same and check as to why the auditee organization's management has failed to detect and address the same. If and when after proper investigation, it is clear that the auditee organization's management system has short comings / the infringement of the relevant standard is established, a major/minor non-conformity as appropriate will be raised. **Follow-up visits are made to verify that major non-conformities are effectively remedied before certification is granted**. In case of legal / statutory / regulatory requirements by the auditee organisation, the following policy shall apply:

In the event of the auditee organisation conducting a violation of the legal requirement, the auditee organisation, as a part of the rules and regulations of Bulletproof Certification, will inform Bulletproof on its own pro-actively and voluntarily. This pro-active information communication by the auditee organisation is not to be confined to onsite-audit activity but is applicable to the complete registration period which the auditee organisation is entitled to by way of Bulletproof. In case of violation of legal requirements that is observed during the course of a Registration Audit (Stage 2 Audit) or Surveillance Audit(s), the Bulletproof audit team will notify the auditee organization's management about the observation. Further the audit team will conduct a proper investigation on the issue and check as to why the auditee organization's management system has failed to detect and address the same. Based on the investigation of the audit team, if it is established that the management system has shortcomings / an infringement of the relevant standard is observed, a major or minor non-conformity note will be issued.

The auditee organisation has to ensure and to provide evidence to that effect to Bulletproof that the appropriate authorities have been notified of the violation of legal requirements, as per the prescribed procedure instituted by the relevant authorities.

CYBERSECURE CANADA SPECIFIC DIRECTION FOR AUDIT VISITS

The CyberSecure Canada certifications are performed remotely at this time. There is no requirement for the auditor to perform an on site visit during the audit.

STAGE 1 AUDIT

In this stage the audit team obtains documentation on the MS design covering the documentation required by the relevant standard.

The audit team seeks to obtain a sufficient understanding of the design of the MS in the context of the client's organization, risk assessment and treatment (including the controls determined), information security policy and objectives. The audit team will evaluate client's preparedness for stage 2 and plan accordingly.

The results of stage 1 will be documented in a written report. The audit program manager will review the stage 1 audit report before deciding on proceeding with stage 2 and for selecting the stage 2 audit team members with the necessary competence.

The audit team will make the client aware of further information and records that may be required for detailed examination during stage 2.

Stage 1 audits do not require a formal audit plan. Stage 1 can be carried out onsite if this can help to achieve the audit objectives.

The Stage 1 audit is intended to:

- Assess that the auditee has a documented management system, which is compliant to the relevant standard.
- Obtain necessary information regarding the scope of the management system and other information which might have an impact on the stage 2 audit including:
    - Size and complexity of the organization
    - Location(s)
    - Equipment Used
    - Applicable statutory requirements & licenses
    - Technology expertise necessary
    - Special safety requirements
    - Security clearance requirements
    - Logistics
    - Work hours and schedules
- Establish that the scope of the MS addresses requirements of relevant standard.
- Establish that the proposed scope of certification is appropriate to the auditee organization's business activities (the information security risk assessment and risk treatment covers the organization business activities as defined in the scope of certification and this is reflected in the scope of MS)

- Establish that there is a Statement of Applicability per scope of certification
- Ensure that the system includes an adequate procedure for identification of applicable statutory and regulatory requirements.
- Evaluate the client's location and site-specific conditions and to undertake discussions with the client's personnel to determine the preparedness for the stage 2 audit.
- Review the client's status and understanding regarding requirements of the relevant standard with respect to the identification of key performance or significant aspects such as site activities, processes, objectives
- Ensure that the management system is designed to achieve defined policy, objectives and targets.
- Establish that internal audits are effective and relied upon. Seeking evidence for competence, experience, training & independence of internal auditors; auditing procedure & methodology; reference & standards; resource availability; organization & planning of audits; checks & reports; timelines & effectiveness of corrective action and management of audit follow-up.
- Establish that management reviews are conducted and cover continuing suitability, adequacy, and effectiveness of management system.
- Establish that the management system is designed to realize the concept of continual improvement.
- Confirm the auditee organization's readiness for registration audit.
- Prepare a detailed program including audit trails for the upcoming Stage 2 audit.
- Review the adequacy of audit time for Stage 2 audit. Increase the time duration if required based on the findings of audit; complexity / volume of processes; variation found from the data provided by the client.

When carrying out a review the auditor shall note his/her findings in the Stage 1 audit report and record this against the relevant topic if such fails to satisfy the requirement of the standard.

The documentation must have been issued and would normally have been in place for a minimum of three months.

The documentation to be reviewed shall include at least the following:

- Description of organization and its on-site processes;
- General information concerning the MS and the activities it covers;
- A copy of the required MS documents as specified in the relevant standard;
- Internal audit program with identified non-conformities and records;
- Details of identified non-conformities and corrective action taken in last 12 months.

Additionally, the following associated documentation might be required

- Means and system for realizing continual improvement;
- An overview of applicable regulations and agreements with authorities;
- Records of incidents, breach of regulation and relevant correspondence and MS related communications with action taken;

- Records for management review

Process Steps for Stage 1

The assigned Audit Team Leader is responsible for managing and documenting the results of the documentation review. However, responsibilities for conducting the review may be delegated to other audit team members. The process for the stage 1 audit can be briefly described as follows:

- Audit Program Manager advises the concerned Audit Team of the assignment.
- Audit Team Leader prepares the audit schedule and intimates the client normally a week before the planned audit date. Audit Schedule contains audit team names. Auditors background details are provided to client on request.
- Neither an audit plan nor an opening meeting is required for a Stage 1 Audit. The Audit Team Leader may offer them to the organization.
- Generally, only one person is needed to perform the documentation review, but where a team is used or an auditor under training is present, then a team briefing may be necessary.
- If stage 1 is conducted on site, a tour of the facility should be performed to provide familiarization with the auditee's organization.
- The main objective is to review the auditee organization's readiness with respect to the points listed above. Documents are reviewed only to the level necessary to establish compliance with relevant standard. A record of documents reviewed is made.
- The auditor shall review for any discrepancy in any information provided in MS Application Form and contract review. This shall be reviewed by Audit Team Leader and may result in change in man-days assigned for the contract.
- Auditee organization debrief meeting is held to discuss the audit findings and obtain any further information necessary to program the audit and decide on further action.
- The findings are collated, and an audit report is prepared for handing over at the closing meeting. On the basis of the findings, a recommendation is made to proceed / defer/ cancel the stage 2 audit. The auditor shall explain the reason for considering the documentation or system unsatisfactory. In case of many or larger issues, the stage 1 audit may need to be carried out again. This shall be discussed with the auditee and suitable date decided. This may require working out an amendment to the contract.
- Stage 1 ends with a closing meeting where points agreed with the auditee organization are confirmed. The Certification Scope for audit is confirmed. Audit report is provided to the auditee organization. The client will be informed by the Audit Team Leader that any discrepancies not closed out prior to the audit will result in automatic non-conformity notices being raised. The discrepancies include non-completion of scheduled internal audit programs and management reviews.
- The Stage 2 audit shall be conducted within 3 months of stage 1 audit. Any further delay shall require stage 1 audit to be carried out again.

CYBERSECURE CANADA SPECIFC DIRECTION FOR STAGE 1 AUDITS

For CyberSecure Canada certification audits, the Stage 1 activities will consist a preliminary documentation review in order for the auditor to make an informed decision as to the readiness of the candidate. In the event that the auditor determines, after the review, that insufficient documentation exists to support compliance, a decision to stop the audit will be made and Stage 2 activities will not be performed.

STAGE 2 AUDIT

The objective of the Initial Certification Audit (Stage 2 Audit) is:

- To evaluate the effective implementation of the MS
- To confirm that the auditee organization adheres to its own policies, objectives and procedures.
- To conform that the management system of the auditee organization conforms to all the requirements of the current version of respective standard(s), normative document and achieving the organization's policy & objectives.
- To evaluate compliance to applicable legal and regulatory requirements.
- To establish whether the organization's procedures employed in analysis of significance are sound and properly implemented. Determine if an information security threat to assets, a vulnerability, or an impact is identified as being significant and is managed within the MS.
- To establish that the analysis of security related threats is relevant and adequate for the organization.

The Stage 2 audit will focus on:

- Assess that the auditee organization's information security management system has been implemented and objective evidence is available to demonstrate its effective implementation in line with its policies, objectives and procedures.
- Establish that all requirements of the standard are addressed where they apply to the activities covered by the scope of certification.
- Confirm that information security management system is appropriate to the product, process or service provided by the auditee, with the capability of managing and improving performance.
- Encourage auditee organizations to improve their management system on an on-going basis.

While accomplishing this, the initial certification audit must be conducted to satisfy the needs of the auditee organization and maintain the integrity of the registration process as a whole. The Audit Team Leader is responsible for managing and documenting the results of the initial certification audit. He may delegate specific audit tasks to assigned audit team members.

INITIAL CERTIFICATION STAGE 2 AUDIT

The initial certification audit addresses the implementation of all the elements in the standard and focuses on all that are applicable:

- Top management leadership and commitment to information security policy and information security objectives.

- Documentation requirements listed in the relevant standard.
- Assessment of information security related risks and that the assessments produce consistent, valid and comparable results if repeated;
- Determination of control objectives and controls based on the information security risk assessment and risk treatment processes;
- Information security performance and the effectiveness of the MS, evaluating against the information security objectives;
- Correspondence between the determined controls, the Statement of Applicability and the results of the information security risk assessment and risk treatment process and the information security policy and objectives;
- Implementation of controls, taking into account the external and internal context and related risks, the organization's monitoring, measurement and analysis of information security processes and controls, to determine whether controls are implemented and effective and meet their stated information security objectives;
- Programs, processes, procedures, records, internal audits and reviews of the MS effectiveness to ensure that these are traceable to top management decisions and the information security policy and objectives.
- Inconsistencies between organization's policy, objectives & targets and its procedures to achieve them or the results of their application. Opportunities for improvement may be identified and recorded. Audit findings, however, which are nonconformities, shall not be recorded as opportunities for improvement.
- Auditee's process for achieving continual improvement and its effectiveness.
- Operational control to maintain consistent performance and compliance to procedures
- Performance monitoring, measuring, reporting & reviewing against the legislative requirement, objectives and targets.
- Internal auditing, identification / evaluation of non-conformities and completion of effective corrective actions.
- Management review and management responsibility for information security management system.
- Register of regulatory requirements
- Seeking evidence for competence, experience, training & independence of internal auditors; auditing procedure & methodology; reference & standards; resource availability; organization & planning of audits; checks & reports; timeliness & effectiveness of corrective action and management of audit follow-up.
- Procedures to ensure compliance with legal & other requirements

PROCESS STEPS FOR STAGE 2 AUDIT

- Audit Program Manager select the Audit Team Members and schedules the audit. A set of the

auditee's documents such as policies, procedures is given to the Audit Team Leader. The Audit Team Leader is responsible to prepare the Audit Plan based upon the application. Once the Audit Plan is reviewed and approved by the Audit Program Manager. The Audit Team Leader will discuss it with auditee organization in order to agree on logistics. The Audit Team Leader will inform the client normally a week before the planned audit date and the same is agreed upon prior to the audit. In case of any changes required by the client before the audit, necessary action is taken to adjust the plan accordingly if reasonable. In case of any changes in the audit plan during the audit the same is captured as part of the audit report. Auditor background and possible technical experts/ observers' details are provided to client in advance at least one week before the planned visit.

- Where the assignment is complex (multi-site, has specific technological requirements, and/or utilizes a large audit team etc.), a team briefing may be planned before the scheduled audit dates to coordinate details.
- An opening meeting is held to advise the auditee organization of the objectives of registration audit, details of the audit and schedule and obtain for the auditee organization's cooperation.
- Where more than one person has been assigned, daily team meeting may be scheduled after the auditee organization meeting to plan the day's strategy and cover any points not included in the pre-visit team meeting.
- Changes to the auditee organization's documentation since the previous visit is reviewed and outstanding non-conformance(s) followed-up. The auditee organization's management system is assessed according to the schedule and audit trails identified during adequacy audit. Documents reviewed, personnel interviewed, and other pertinent data is recorded by the auditor.
- When audit is for more than a day, daily team debrief meeting is used to discuss findings, followed by auditee organization debrief to present the findings of day.
- On the final day of the audit, the team discusses overall performance during the audit and prepares the audit report. The team decision to approve or defer initial certification is recorded in the report.
- The visit ends with a Closing Meeting where the recorded findings and team recommendations are formally presented to the auditee organization and any follow-up actions agreed upon.
- The report is forwarded for review and processing. The audit-trails are exclusive notes strictly for use of auditors to carry out the audit and the team leader shall ensure that they are never given out to the auditee.
- The Stage 2 audit shall be conducted within 3 months of stage 1 audit. Any further delay shall require stage 1 audit to be carried out again. There is no restriction on minimum time duration; however, the general practice is at least 7 days, depending on the findings of the stage 1 audit and client readiness.
- Evidence requested during audits will be transferred securely to Bulletproof: the use of Information Communication Technology for transmitting and storing information will be mutually agreed between Bulletproof and the customer in accordance with IAF MD4 clauses.

NON-CONFORMITY AND SENTENCING OF MAJOR AND MINOR NON-CONFORMANCES

A non-conformity is defined as failure to fulfil one or more requirements of the management system standard or a situation that arises serious doubts about a client's management system to achieve its intended output. Non-conformities will be classified in two categories – Minor and Major. Auditors are required to refrain from suggesting the cause of nonconformities or their solution.

During an audit a minor non-conformity shall be deemed present when any activity is not undertaken, and which is stipulated in the client's management system as a requirement or which was undertaken and is relevant but is not controlled within the system and is deemed to be of a minor nature. Several non-conformities in any one section, or procedure, shall constitute a major breakdown of the system.

A major non-conformity shall be declared when a system or procedure is not working at all, or where there is complete failure to fulfil one or more requirements of the management system, or where there is significant doubt that the client's system can achieve the intended output, or where a serious cumulative number of minor non-conformities are found overall, or when there is a complete lack of system control. Several non-conformities may be grouped together as one major non-conformity.

If all non-conformities have been rectified within six months of the last day of stage 2, then the award will be recommended. If not, another complete stage 2 is to be carried out at the discretion of the Certification Committee prior to recommending the certification. If on a follow-up audit it is found that the major nonconformity has not been satisfactorily addressed, then another audit is to be performed within two weeks. If this fails, then a full re-audit must take place.

CYBERSECURE CANADA SPECIFIC DIRECTION ON SENTENCING OF MAJOR, MINOR NONCONFORMITIES

For CyberSecure Canada certifications, nonconformities which have been graded as "minor" can have the corrective action reviewed at the annual surveillance audit. For those nonconformities which have been graded as "major", a review of the corrective action taken is required to be performed within ninety (90) calendar days.

FOLLOW UP AUDIT

The purpose of follow-up audits is to conduct the follow-up of non-conformance(s) of an auditee organization's information security management system, identified during a visit, that were determined to require corrective action. Follow-up audit is required where a major non-conformity is raised. Minor non-conformity does not require formal follow-up visit and may be closed off site based on evidence submitted. The time required for follow-up audit shall be determined based on number and nature of major non-conformities issued.

The team leader will plan and determine the type of follow-up that is required and discuss it with the Audit Program Manager who has to approve it. An off-site follow-up may only be conducted when the corrective action can be objectively evaluated on the basis of documented evidence sent to Bulletproof by the auditee organization. If the follow-up audit is not performed within three months of the initial certification audit, a partial re-audit has to be performed (the time required shall be about 50% of that of stage 2 audit). A complete re-audit will be carried out if the follow-up audit is not performed within 6 months.

The non-conformities should be updated to reflect the new status, where the corrective actions are verified. These are reviewed by the Audit Team Leader and then the Certification Committee. Audit Team Leader initiate withdrawal/suspension procedures, if auditee organization fails to effectively respond to a corrective action

request or if the corrective action is not satisfactory. Audit report for Follow-up audit shall be the same as for Certification or Surveillance Audit.

SURVEILLANCE AUDIT

The certified management system should continue to meet the requirements of the standard and should be managed effectively by the auditee organization. Surveillance Audits are intended to verify the continued effective maintenance of the auditee organization's Management System, satisfy the needs of the auditee organization and maintain the integrity of the certification process as a whole.

SURVEILLANCE AUDIT IS INTENDED TO:

- Assess that the auditee organization's approved management system has been maintained and continues to be implemented.
- Verify that changes to the management system subsequent to the previous visit are in compliance with respective standard and that objective evidence is available to substantiate implementation.
- Re-confirm that the management system is appropriate to auditee organization's product, process or service provided, with the capability of managing and improving performance.
- Confirm continued compliance with certification requirements
- Promote the effectiveness of information security management system.
- Assess major changes in auditee organization's operations, technology that could affect the certification / registration.

The various mandatory elements to be audited at every surveillance are:

- Changes to documented system
- Areas subject to change
- Legal regulatory compliance
- Document control
- Complaints Handling
- Use of certification marks
- Continuing operational control
- Internal ISMS audit, Management review
- Corrective action
- Use of certificate and logo
- Information Security Risk Assessment Maintenance
- Achievement of organization's policies, objectives and targets.
- Progress of planned activities aimed at continual improvement
- Communication from external parties
- Selected requirements of ISO/IEC 27001
- Other Areas as appropriate

With regards of the client's complaint handling, Bulletproof will check the records of appeals and complaints and, where any nonconformity or failure to meet the requirements of certification is revealed, Bulletproof will verify that the client has investigated its own MS and procedures and taken appropriate corrective action.

In addition, each surveillance audit will include a review of:

- The effectiveness of the MS with regard to achieving its information security objectives;
- The functioning of procedures for the periodic evaluation and review of compliance with relevant information security legislation and regulations;
- Changes to the controls determined, and resulting changes to the SoA;
- Implementation and effectiveness of controls according to the audit program.
- Enquiries from Bulletproof to the certified client on aspects of certification;
- Certified client's statements with respect to its operations (e.g. promotional material, website);
- Requests to the certified client to provide documented information (on paper or electronic media);
- Other means of monitoring the certified client's performance.

PROCESS STEPS FOR SURVEILLANCE AUDIT

The Audit Team Leader is responsible for managing and documenting the results of Surveillance Audit. The Audit Team Leader may delegate specific responsibilities related to audit activities to selected Audit Team Members. The Audit Team Leader is responsible for reviewing audit findings of Audit Team Members. The process steps for the Surveillance Audit are:

- Audit Program Manager select the Audit Team, schedules the audit dates and informs the Audit Team Leader, who is responsible to draft the audit plan and submit it to the Audit Program Manager for review/approval. Once approved, the audit plan is discussed with the auditee organization. Care is taken that the audit is scheduled within 12 months interval – date being last day of Certification Audit.
- Audit Team Leader shall review the functions / processes audited in the earlier surveillances before finalizing the audit plan.
- Where an assignment is particularly complex (i.e. begins at several different locations, it has particular technological requirements, and/or requires a large number of team members, etc.), it may be beneficial to call a team briefing before the scheduled dates to coordinate details.
- An opening meeting is held to advise the auditee organization of the objectives of audit, details of the audit and schedule and obtain auditee organization's cooperation.
- Where more than one person has been assigned, a daily team meeting is scheduled immediately following the auditee organization meeting to plan the day's strategy and cover any points not included in the pre-visit team meeting. Changes to the auditee organization's documentation since the previous visit are reviewed and outstanding non-conformities followed-up. The scope of the certificate will be checked against the scope of activities being carried out by the company. If these are not the same, the auditor will discuss this with the company and inform the Audit Team Leader or appointed person for further consideration.
- Non-conformities are raised after proper investigation against controls found non-compliant. The observations and opportunities for improvements are issued identifying areas of improvement only.
- On the final day of the surveillance audit, the audit team discusses overall auditee organization performance and determines the recommendation (registration to continue or follow-up is required). The team prepares the audit report. The Audit Team Leader decision is recorded on the Audit Report. Areas to be reviewed at the next visit are also detailed.

- The visit ends with a Closing Meeting where the findings and team recommendation are formally presented to the auditee organization and any follow-up actions agreed upon. The Record of Findings is handed to the auditee organization and a copy forwarded to Audit Team Leader for review and processing.
- It is essential to ensure that the full system (as a minimum) is covered over a three-year period by surveillances. At each visit complaints, audits, certification marks, documentation changes, and evidence of improvements will be reviewed.

Any auditee organization has to notify Bulletproof in writing of any major change in the management system and / or the scope of activities. Audit Team Leader shall discuss the changes with the Audit Program Manager, who shall decide if the verification of changes can be assessed during next surveillance audit or if a special visit has to be scheduled. The performance of the special visit shall be similar to normal surveillance and Audit Program Manager shall inform the assigned auditor to audit the required changes in system.

CYBERSECURE CANADA SPECIFC DIRECTION ON SURVEILLANCE AUDITS

For CyberSecure Canada certifications, surveillance audit activities will consist of a review of the candidate'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.

MAINTAINING OF CERTIFICATES

Certificates will be created and processed by the Certificate Coordinator. Certificates will be maintained provided that the certified client's Management System continue to satisfy the relevant standard: this depends on the positive recommendation from the Audit Team Leader during routine surveillance audits, provided that any non-conformity is resolved and there are no other situations which may lead to withdrawal / suspension of the certification.

In such cases the Audit Team Leader reports to the Certification Committee to initiate a review and decide for suspension, withdrawal or follow up audits.

RECERTIFICATION AUDITS

The purpose of the recertification audit is to confirm the continued and effective management system as a whole is followed and the continued relevance and applicability of the scope of certification, commitment to enhance and maintain overall effectiveness and improvement of the management system and whether the operations of a certified client contribute to the achievement of the client's policy and objective.

Consistent with initial certification audit procedure, the following steps shall be followed when planning the audit:

- The planning and extent of the visit are in accordance with the accreditation board requirements and that determined at the last surveillance visit. The visit is planned based on client's performance during the certification period, previous surveillance audit reports, trends in NC raised, complaints received during the period and corresponding investigation reports etc.
- Recertification audit may include stage 1, if there is considerable internal / external change in ISMS, activities, location and scope of certification or the context in which the management system is operating (e.g. changes to legislation)..

- During recertification audit planning the Audit Program Manager should consider rotation of the audit team members to ensure "no bias" and a fresh look at the system.
- Recertification audits shall include review of effectiveness and improvements of the MS performance
- A recertification audit is a full audit of the auditee organization's information security management system and generally follows the same process as the Stage 2 Audit.
- Recertification audits and review follow the same instructions as those for initial audits. Care should be taken for review of changed scope or activities of the client.
- The time allowed to implement corrective action shall be consistent with the severity of the nonconformity and the associated information security risk.

Decision on renewing the certificate will be made by Certification Committee chaired by the Certification Manager, based upon:

- review of the effectiveness of the certified Management System over the period of certification
- demonstrated commitment to maintain and improve said effectiveness
- review of possible complaints received against the certified client over the certification period
- recommendation made by the Audit Team Lead in the report

In accordance with ISO/IEC 17021–1:2015, the recertification audit, closure of all issues and certification committee decision need to be completed prior to expiry date of the current certificate. The new certificate shall then be considered as continuation of certification (e.g.: 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 recertification decision. The recertification audit should be completed about 2 months before certificate expiry. In case of situations where evidence of corrective actions is not submitted in time to complete the certification decision (e.g.: Bulletproof is unable to verify the implementation of corrective actions for any major nonconformity prior to the expiry date of the certification), then recertification shall not be recommended, and the validity of the certification shall not be extended. The client shall be informed, and the consequences shall be explained.

Where the certification activities cannot be completed before certificate expiry, the client shall be considered as a fresh case and a new Initial Certification audit shall be performed. Also, if the surveillances are not done as per schedule, the client shall be considered as a fresh case.

Following expiration of certification, Bulletproof will restore certification within 6 months provided that the outstanding recertification activities are completed. The effective date on the certificate shall be on or after the recertification decision and the expiry date shall be based on prior certification cycle.

SPECIAL PURPOSE VISITS

Registered information security management system must continue to comply with the current version of specific standard and any changes to the system must also continue to comply. Also, the scope of certification must continue to be appropriate to the auditee organization's objectives and appropriate for the auditee organization's products and services. On the other hand, complaints, appeals, request for change in scope, additional accreditation, audit visits, or surveillance visits may disclose reasons for undertaking an additional visit.

If there are grounds for undertaking a special purpose visit, Audit Program Manager determines what level of review will be required to maintain or extend registration, including but not limited to normal surveillance, unplanned surveillance, partial re-audit, or full re-audit.

Before undertaking any visit, which is not under any contractual agreement, the auditee organization must agree in writing to the new terms.

The scope of the audit shall be pre-determined and shall depend on the reason for the visit. In case of any complaint / appeal / any information resulting in doubt on the effectiveness of system, the audit of concerned and other related activity may be carried out.

Visit / audit report shall be recorded in a report (in the same report template as the initial, surveillance and follow up audits). The report shall also be reviewed for risk to Bulletproof. Certification Committee may also discuss the findings with the audit team.

Extensions to scope change in management systems for clients already registered with Bulletproof

- Bulletproof MS Application Form should be completed by the client and returned to Bulletproof
- Contract Review will always be carried out by the Audit Program Manager whether a full or partial Stage 1 is required.
- An off-site Stage 1 must be completed and sent to the Audit Team Leader or appointed person for review. Under exceptional circumstances an on-site Stage 1 may be required.
- Under no circumstances must the above visit be carried out at the same time as surveillances unless extra time or extra auditor has been allocated. However, Stage 1 shall be completed before the on-site audit.

Audits for the above reasons will be carried out in the same way as the initial audit. An Audit Report must be completed in the normal way and submitted to the Certification Committee for approval.

If successful, a new certificate will be issued by Bulletproof.

Note: After certification, if a client makes major modifications or other changes take place which could significantly affects the basis of its certification, then Bulletproof must be informed. Bulletproof reserves the right to re-assess.

A special visit may be carried out on request of the client for additional accreditation. Client may request for additional accreditation any time prior to certification audit or during the three-year period. In case the request is prior to stage 2 audits, the request shall be reviewed by Audit Team Leader and verified if the client's activities are within the Bulletproof scope of accreditation. Stage 2 audit is carried out as described above. If the request is within the three-year period, an additional visit may be required to verify compliance. The visit may be merged with a planned surveillance audit. Additional accreditation shall be affected only after successful completion of the audit. The certificate shall be amended accordingly, however, the expiry date shall be the same. Fees may be charged towards additional accreditation and new certificate issue.

Short Notice audits for clients certified by Bulletproof

These audits are necessary to investigate any complaints, changes in management systems, follow up on suspended clients. Requirements of short notice audits are communicated to the client at time of contract finalization through Client Agreement.

Special care will be taken in assigning the audit team for short notice audits.

TRANSFERS

This applies only to transfers from other accredited certification bodies. Only transfers from companies which have certificates covered by an accreditation of an IAF signatory should be eligible for transfer. Certificates which are not accredited as below shall be treated as new clients.

Pre-transfer Review

- Carry out the normal contract review procedure, Quotation Preparation and Staff Allocation, and possibly visit the client. There is no need for a document review, unless an extension is involved.
- Check that the client's scope on their certificate is as stated on the questionnaire.
- Confirm the client's certificated activities are compatible with that of Bulletproof.
- Try to establish the reason for the client wanting to transfer.
- Check that all of the sites that the client wants transferring are covered by their current registration.
- Check that the certificate is VALID and has not expired and that it is accredited. Certificates that have been suspended or withdrawn or are out of date shall not be considered for transfer. (Note: If the certification body has ceased trading or had its accreditation withdrawn then the transfer can still go ahead on the basis of this review procedure).
- Check the status in their current certificate cycle, i.e., is we to take over the surveillance program or are they due for a re-certification etc. If re-certification is due, we must carry out a full 2 stage audit including planning and site visits. Any extensions to scope will result in visits.
- Request reports / checklists, non-conformances etc. from the previous certification body. The status of any outstanding non-conformance notices must be known. Non-conformities must be closed out by the previous certification body or sent to Bulletproof with evidence of corrective actions taken for Bulletproof. to close out.
- Request verbal confirmation of the effectiveness of the complaint system. Request details of any major problems.
- For ISMS only – request details of any legal engagement with statutory bodies.

If no further outstanding problems from the above review are identified, then a certificate may be issued after authorization by the Certification Committee.

The program of surveillance visits/triennials is to be adopted from the previous certification body if applicable. Appendix Document is signed by the Chairman of the Certification Committee, Chief Executive and Technical Expert (if applicable) to authorize issue of the certificate.

Note: If, as a result of the review, some of the criteria are not met, then a site audit will be required to give confidence to certify by Bulletproof.

CYBERSECURE CANADA DIRECTION ON TRANSFERS

For CyberSecure Canada certifications, Bulletproof will not perform transfers. If an existing certified company approaches Bulletproof to become their certification body during their surveillance audit period, Bulletproof will perform a new initial certification.

AUDIT METHODOLOGY

The audit methodology does not presuppose a particular manner of implementation of an MS or a particular format for documentation and records. The methodology focuses on establishing that a client's MS meets the requirements specified in the relevant standard and the policies and objectives of the client.

Bulletproof shall not certify an MS unless it has been operated through at least one management review and one internal MS audit covering the scope of certification.

The audit team shall audit the MS of the client covered by the defined scope against all applicable certification requirements. The certification body shall confirm, in the scope of the client MS, that clients address the requirements stated in the relevant standard.

Certification bodies shall ensure that the client's information security risk assessment and risk treatment properly reflects its activities and extends to the boundaries of its activities as defined in the scope of certification. Certification bodies shall confirm that this is reflected in the client's scope of their MS and Statement of Applicability. The certification body shall verify that there is at least one Statement of Applicability per scope of certification.

Certification bodies shall ensure that interfaces with services or activities that are not completely within the scope of the MS are addressed within the MS subject to certification and are included in the client's information security risk assessment. An example of such a situation is the sharing of facilities (e.g. IT systems, databases and telecommunication systems or the outsourcing of a business function) with other organizations.

OPENING AND CLOSING MEETINGS

The Opening and closing meeting are a critical part of the audit process. The opening meeting ensures that all parties understand what is going to happen and how best they can cooperate and coordinate their efforts. The closing meeting ensures that all parties understand the relevance of findings, what they need to do and what happens next. The meeting agenda contains a number of essential requirements which must be advised to the auditee organization in addition to other useful items which make for a clearer understanding of what is expected from both parties. It is hence essential that all the agenda items covered in this instruction, as appropriate and applicable to the situation.

		Opening	Closing
A*	Thank client for selecting Bulletproof. Mutual Introduction of auditors and auditee	●	
B*	Thank auditee for hospitality. Thank guides for their support.		●
C	Circulate attendance sheet	●	●

D*	State and confirm the contracted scope for certification and objectives of audit.	●	●
E*	State that Auditor Team Leader represents audit team. Determine auditee representative and guides	●	
F*	Confirm the audit plan and verify no conflicts with the plan. Reconfirm time and location for closing meeting. Make necessary amendments on request	●	
G*	Explain the terms non-conformance (major & minor) and observation	●	●
H*	Explain the timeframe for the client to present a plan for corrective action for any nonconformities identified during the audit. E.g.: Minor non-conformities must be accompanied by a plan which should be presented by the auditee within 24 hours from the conclusion of the audit: the plan must be validated by the Audit Team Leader. Major non-conformities require formal follow-up visit and may be closed off site based on evidence submitted. Explain that once corrective actions are verified by the audit team (via follow up audit or via corrective action plan) the time frame for reporting is 10 business days including QA.		●
I	Communicate the policy of notification by auditee for legal / statutory violation.	●	●
J*	Request sufficient sets of documentation, suitable room and office support	●	
K*	Explain auditor's responsibility to comply with code of conduct and confidentiality	●	●
L	Explain that audits are sampling exercises and other issues may exist. Refer to the need of ongoing internal audit and ongoing surveillance. Stress that the audit does not guarantee to identify all areas of non-conformance	●	●
M	Request advice on safety requirements and availability of safety equipment.	●	
N*	Explain the findings. Highlight strengths. State non-conformances and observations. Explain the expectation of corrective action for non-conformances, including how lack of corrective action will impact on certification.		●
O*	State conclusion and recommendation of audit team. Explain that the team can only make recommendation. Explain the concept of Certification committee. Explain that appeals process exists and is available on request.		●
P	Obtain auditee organization's signature on the audit report. Request auditee to state the corrective action plan. Explain auditee's responsibility of submission of evidence for non-conformances identified. Request for safekeeping of audit reports		●
Q*	Invite questions	●	●

CYBERSECURE CANADA DIRECTION ON OPENING AND CLOSING MEETINGS

For CyberSecure Canada certifications, sections in the above table marked with an "*" will apply.

MULTI-SITE AUDITS

Multiple site audits under the control of a single MS are carried out in accordance with the following.

All sites will be audited, or the Head Office and a representative number of sites may be sampled by the audit team providing:

- All sites have been audited in accordance with the internal audit procedures
- A central management review has been carried out.

The sampling of the sites must include a representative number. The selection of the sites takes into account:

- The results of central and internal audits
- The results of management review
- Variations in the size of the sites
- Maturity of the system
- Existing knowledge of the organization
- Shift patterns
- Personnel involved
- Repetitiveness of the work
- Complexity of the ISMS
- Complexity of the sites
- Variations in working practices
- Variations in activities undertaken
- The significance of the aspects
- Potential interaction with sensitive environments
- Differing legal requirements
- Communications from interested parties

These requirements will be considered by the Certification Committee before awarding certificates.

Please refer to the "Representative Site Sampling" template for documenting multi-site audits.

SAMPLING PLAN AND AUDITING TIME

As such there is no statistical or mathematical formula to establish the right number of samples to be taken during an audit. Defining the number of samples to be taken to confirm conformity to the requirements of the standard is not efficient and does not ensure conformity. Adequate sampling would refer to a level of sampling taken during on site interviews and record reviews that give sufficient confidence that the auditee's MS is implemented and maintained.

The audit team needs to perform (where applicable):

- Interviews;
- Observation of processes and activities
- Documentation reviews.

The audit team needs to check records and evidence during interviews/ process walk-throughs.

Audit evidence will be collected by the audit team as evidence of conformity. The method used for collating evidence is based on sampling.

The number of samples to be taken depends on the complexity of the processes being audited and the quality of information received from the auditee during the interview. It is also important that the auditor maintains the schedule outlined in the audit plan. At the end of the day the auditor needs to feel comfortable that the samples and the objective evidence seen are representative, in order to draw appropriate conclusions regarding the implementation of MS.

Bulletproof auditors will spend about 60% of the audit time for critical process audits.

Bulletproof shall allow auditors sufficient time to undertake all activities relating to an initial audit, surveillance audit or re-certification audit. The calculation of overall audit time shall include sufficient time for audit reporting.

Please refer to the "Bulletproof Calculating Audit Time SOP".

AUDIT REPORT

The audit report includes the following information or a reference to it:

- 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;
- Deviations from the audit plan (e.g. more or less time spent on certain scheduled activities);
- The MS scope.

The audit report includes sufficient detail to facilitate and support the certification decision. It contains:

- Significant audit trails followed and audit methodologies utilized;
- Observations made, both positive (e.g. noteworthy features) and negative (e.g. potential nonconformities);
- Comments on the conformity of the client's ISMS with the certification requirements with a clear statement of nonconformity, a reference to the version of the Statement of Applicability and, where applicable, any useful comparison with the results of previous certification audits of the client.

Completed questionnaires, checklists, observations, logs, or auditor notes may form an integral part of the audit report. If these methods are used, these documents shall be submitted to the certification body as evidence to support the certification decision. Information about the samples evaluated during the audit shall be included in the audit report, or in other certification documentation.

The report considers the adequacy of the internal organization and procedures adopted by the client to give confidence in the MS.

The report covers:

- A summary of the most important observations, positive as well as negative, regarding the implementation and effectiveness of the MS requirements and IS controls;

- The audit team's recommendation as to whether the client's MS should be certified or not, with information to substantiate this recommendation

Revision History

Version	Change Description	Date
1.0	Initial Release	2021-02-20
1.1	Modified document to reflect all MS audits. Also changed approvers to the new ISF committee as we integrate management of 17021 with the incoming 27001.	2021-12-15
1.2	Added language and process areas which are specific to CyberSecure Canada only	2022-04-25