R20.111 ISO/IEC 27001 Information Security Management Systems Supplement

1.0 **Scope** - This R20.111 applies to organizations requiring assessment and/or registration of their management system in accordance with ISO/IEC 27001.

The following steps represent additions/clarifications to those defined in SRI Procedures QP 4.0 through QP 8.0 with relevant documents (R20.xx) as indicated. The management system requirements specified in ISO/IEC 27001 and normative documentation are complementary (not alternative) to the technical specified requirements and applicable law and regulatory requirements.

1.1 **Purpose** - The purpose of this document is to outline the process for providing organizations and their suppliers with assessment and registration of their Information Security Management System. It provides requirements for auditing organizations to ISO/IEC 27001 and aligns with current ISO/IEC 17021-1and ISO/IEC 27006guidance.

1.2 **References**

- ISO/IEC 27001 – Information technology – Security techniques- Information security systems – requirements.
- ISO/IEC 27006 Amendment 1- Information technology – Security techniques- Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 17021-1– Conformity assessment – Requirements for bodies providing audit and certification of management systems.

2.0 **Definitions**

2.1 Organization: Company, corporate firm, enterprise, authority or institution, or part or combination thereof, whether incorporated or not, public or private, that has its own functions and administration and is able to ensure that Information Security is exercised.

2.2 Asset: Anything that has value to an organization

2.3 Confidentiality – The property that information is not made available or disclosed to unauthorized individuals, entities or processes.

2.4 Information Security – Preservation of confidentiality, integrity, and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation, and reliability can also be involved.

2.5 Information Security Event - An identified occurrence of a system, service, or network state indicating a possible breach of information security policy or failure of safeguards, or a previous unknown situation that may be security relevant.

2.6 Information Security Incident – a single series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

2.7 Risk Analysis – Systematic use of information to identify sources and to estimate the risk.

2.8 Statement of Applicability – Documented statement describing the control objectives and controls that are relevant and applicable to the organization's ISMS.

2.9 Major (HOLD) Nonconformity - The absence of, or failure to implement and maintain one or more required management system elements, or a situation which would, on the basis of objective evidence, raise significant doubt as to the capability of the ISMS to achieve the security policy and objectives of the organization.

2.10 Minor Nonconformity - A single system failure or lapse in conformance with a procedure, process or element, relating to the applicable standard.

3.0 General

3.1 Information security additional requirements and supplementation are typically shown in ISO/IEC 27001 documents, including baseline management system requirements in ISO/IEC 17021-1. If an organization already has an operative system, (e.g. in relation with ISO 9001 or ISO 14001) it is preferable in most cases to satisfy the requirements of ISO/IEC 27001 within the current established standard.

3.2 All documents and data (in the form of notebooks, approvals, or other company specific information) generated is handled as "sensitive" (or proprietary) among the parties generating, collecting, and/or using the documents and data. Companies using this data shall keep its usage confidential both internally and externally, unless otherwise agreed in writing by the consenting parties.

4.0 Requirements for SRI

4.1 SRI is fully accredited by the ANSI-ASQ National Accreditation Board (ANAB) and Raad voor Accreditatie Accreditation Mark (RvA), in accordance with ISO/IEC 17021-1current version or equivalent for ISO 9001. SRI has completed the application for ISO/IEC 27001 and submitted same for review and consideration/approval and received approval by ANAB. Information Security sector qualification consists of an application review, witness audit, and recommendation for the recognition of SRI's Information Security sector program.

4.2 SRI has prepared an application form for the applicable Information Security Management System (ISMS) registration. This application provided the ANAB with confidence that SRI has developed the necessary documented process to meet ISO/IEC 27001.

4.3 SRI recognizes that ANAB will perform witness audits and oversight of SRI in accordance with their internal procedures and ISO/IEC guidelines, including at a minimum of one office audit per year and one ISO/IEC 27001 based witness audit per year.

4.4 SRI affords ANAB and applicable Authorities the right of review of records and information related to their ISMS sector qualification program, including SRI activities associated with this document.

5.0 Requirements for Certification/Registration Bodies (CRBS)

5.1 SRI is a nationally recognized and qualified to ISO 9001and ISO/IEC 27001. This accreditation is in accordance with ISO/IEC 17021-1for management systems.

5.2 SRI has and/or uses qualified full-time or contract auditors and/or technical experts engaged in certification/registration activities related to ISO/IEC 27001.

A. The essential elements of competence required to perform ISMS certification/ registration are to select, provide and manage those individuals whose collective competence is appropriate to the activities to be audited in consideration of the competency requirements and criteria expanded in ISO/IEC 27006.

5.3 SRI's processes and requirements to obtain ISO/IEC 27001 sector qualification include as a minimum:

A. Evidence that the SRI has an individual with appropriate background and knowledge. (Contract Review will have Oversight by that individual.) Knowledge and competence is gained by attending and passing an ISO/IEC 27001 course. Items listed under "B" below are also added competencies gained by attending the ISO/IEC 27001 course. Appropriate background and experience are a plus.

B. Evidence of SRI's criteria for the training and selection of audit team ensures appropriate levels of:

1) understanding of the ISMS standard or normative document;
2) understanding of information security issues;
3) understanding of risk assessment and risk management ;
4) technical knowledge of the activity to be audited;
5) knowledge of legal and regulatory requirements relevant to the ISMS;
6) management system audit competencies;
7) management system knowledge.

This training is gained by attending and passing an approved ISMS ISO/IEC 27001 course. Records of attendance and passing are maintained in the contractors file for the life of the contractor's contract.

C. Documented auditor training program reviewed and approved by the ANAB prior to or during the qualification process that conforms to ISO/IEC 27001 and records thereof. SRI shall document their auditor training program; it is available for review and approval by ANAB during the initial accreditation process and at subsequent reviews and audits. SRI has purchased an approved training course or will hire a group to supply an approved training course. Content of the training program as defined by ANAB and/or IRCA or other approved training supplier and is:

1) Applicable to the ISO/IEC 27001 standard
2) The scheme as used in the specific sector for Certification/Registration of ISO/IEC 27001.

D. SRI utilizes qualified auditors. Auditors are closely reviewed and competence established which, among other aspects are important in auditing risk analysis, and having the requisite industrial sector qualifications. Qualified auditors will exhibit;

1) A University Degree (extensive experience and supplementary professional education and training can be equivalent);

2) four (4) years full time practical workplace experience in information technology of which at least two years are engaged in a role or function relating to information security;
3) proof of attending and passing an approved five (5) day ISMS training in auditing and audit management;
4) a minimum of four (4) prior assessments (audit experience such as QMS, EMS, ISMS) equal to 20 days or more, including review of documentation and risk analysis, implementation assessment and audit reporting;
5) qualification to ISMS through RABQSA and or IRCA is preferred and the auditor exhibits the following attributes: objective, mature, discerning, analytical, persistent and realistic. Understands complex operations and able to understand the role of individual units in a larger organization;
6) leads shall have acted as an auditor in at least three complete audits, and have demonstrated the capability to communicate effectively, both orally and in writing, have knowledge and attributes to manage the assessment process and have demonstrated to possess adequate knowledge and attributes to manage the assessment process;
7) all relevant experience should be reasonably current;
8) keep up own knowledge and skill in information security and auditing.

E. SRI has specific procedures, tools and techniques in its system for granting, maintaining, extending, reducing suspending and withdrawing certification/registration.

F. A full system witness audit from a recognized AB of an ISMS audit.

G. SRI agrees to periodic surveillance and witness audits by ANAB.

H. No Certificates or approvals to ISO/IEC 27001 shall be issued by SRI unless all major and minor nonconformances are addressed with root cause analysis and corrective action known and effectiveness of implementation verified.

I. SRI will provide copies when requested of all information pertaining to the audit results, (including notebooks, findings, supporting documents, or other correspondence) with the audited organization for the purpose of the audited organization sharing this information with their customer(s).

J. SRI requires the applicant to prepare a Statement of Applicability describing which parts of the ISMS standard or normative document are relevant and applicable for the organization’s ISMS. The Statement of Applicability shall be part of the working documents provided to the audit team at Stage 1 and will be maintained as required documented information in client files.

K. SRI will ensure that the organization’s information security risk assessment properly reflects its activities and extends to the boundaries of its activities as defined in the ISMS standard or normative document. SRI will confirm that this is reflected in the organization’s Statement of Applicability. Interfaces with services or activities that are not completely within the scope of the ISMS shall be addressed within the ISMS subject to certification/ registration and shall be included in the analysis of the organization's information security risk assessment. An example of such a situation is the sharing of facilities (e.g. computers, telecommunication systems, etc.) with others.

L. SRI does not provide consulting services. Any independent contractor that in the past two years, has provided consulting services to a client, shall have no involvement with the ISO/IEC 27001 registration of that client. Where there may appear to be a conflict of interest, either through consulting or the offering of specific training to a potential client, this shall be disclosed to the ANAB prior to performing the registration process to determine if there is a conflict of interest.

Note: If SRI performs training for an organization for which it will provide registration services, the training must be conducted and managed separately from SRI's registration program. The training must be available to the public and not specific to the attendee base.

5.4 SRI agrees to the "Right of Access" by ANAB and other regulatory or oversight bodies review of all records and information concerning their activities associated with this document and their approval as a certification body under this system. This includes information from audits of clients in accordance with ISO/IEC 27001, current edition.

5.5 SRI agrees to allow ANAB member OEMs to perform surveillance reviews of the SRI's processes and activities associated with this document and their approval as a CRB under this system. This access may include the witnessing of SRI audits at client locations.

6.0 **Requirements for Auditors**

6.1 ISMS auditors shall, as a minimum, continually meet the education, training, work experience and audit experience of ISO 19011 and continually have the following:

A. Auditing Experience - To have participated in at least four audits for a minimum of 20 days, that cover all the elements of the ISO/IEC 27001 standard within the last three years. Auditors shall have the ability to cover all the clauses/elements as determined by the Associate Vice President, Certification. All members of the audit team shall be able to demonstrate appropriate experience and understanding of all of the following:

1) the ISMS standard and applicable Authority normative documented information;
2) the concepts of management systems in general;
3) issues related to various areas of information security, as specified in competency and knowledge requirement cited in ISO/IEC 27006/ Amd. 1;
4) the principles and processes related to risk assessment and risk management;
5) principles relating to information security control selection and implementation and
6) general ISMS auditing principles.

B. The auditor must be trained in ISMS requirements, current edition. This approved training covers all those noted in A. above and as specified in ISO/IEC 27006or current guidance. This training can be performed by SRI or may be obtained independently. SRI's general training program has been reviewed and approved by ANAB. Using the provisional audit activity, auditor has demonstrated competence in auditing as ISMS in accordance with ISO/IEC 27001.

C. The following requirements apply to the audit team as a whole:

1) In each of the following areas at least one audit team member should satisfy the certification/ registration body's criteria for taking responsibility within the team:
   a) managing the team,
   b) knowledge of the legislative and regulatory requirements and of legal compliance in the particular information security field,
   c) identifying information security related threats,
   d) identifying the vulnerabilities of the organization and understanding their impacts, mitigation of risks, and selection of appropriate controls,
   e) knowledge of the current technical state-of-art in the sector,
   f) knowledge of risk assessment related to information security.
2) The audit team should be competent to trace indications of security incidents in the organization's ISMS back to the appropriate elements of the ISMS.
3) An audit team may consist of one person provided that the person meets all the criteria set out in A. above.

6.2 To maintain ISMS auditor qualification, all auditors must participate in at least four ISMS audits in three calendar years. Additionally, the auditors are required to participate in continuing education. Training should include review of the changes to the industry standards, auditing methods and ISO requirements at a minimum of 15 hours total within every three year period.

7.0 Requirements for Assessment and Reporting

7.1 ISMS Assessment Teams

A. The assessment team leader must be a qualified ISMS lead auditor per applicable Authority guidance and as identified in SRI's accredited system.
B. The team may include other auditors that are approved per SRI.
C. The assessment team shall include an auditor qualified for the supplier's commodity (ies) (IAF Scope Category). The commodity requirement may be met by a technical expert in-lieu of an auditor (per ANAB guidelines) who is additional to the team membership. ISMS credentials are the minimum.
D. Auditor credentials shall be made available to organization's upon request.

7.1.1 SRI shall ensure that all members of the team are aware of the requirements of ISO/IEC 27001 as may affect the scope of their assessment activity. The ISMS Lead Auditor shall provide guidance to the assessment team throughout the assessment on the interpretation of ISMS requirements and, when requested, the significance of any issues identified.

7.1.2 SRI shall review before the assessment what records are considered as confidential or sensitive by the organization such that these records could not be examined by the audit team during the assessment of the organization. The certification/ registration body shall judge whether the records that can be examined warrant an effective assessment. If the certification/ registration body concludes that an effective assessment is not warranted, the certification/ registration body shall inform the organization that the assessment can take place only when appropriate access arrangements have been accepted by the organization with possible use of an independent intermediary, if required.

7.1.3 ANAB or Representatives may accompany the assessment team as observers of the assessment process at any time with due notice. When Customer representatives are

participating in the audit, the Team Leader shall have the option of including (or not) in the assessment report any findings brought forward by these representatives.

7.2 **Duration of Assessment**

7.2.1 An estimation of time that might be required for a certification audit is helpful to plan the audit. However, it is important to note that due to various factors that may affect the necessary time; users, volume of information handled, number of information systems, number of networks, number of platforms, number of critical systems, remote working, number and types of electronic transactions, number and size of any development projects, applicable legislation and any sector specific requirements), it is not possible to give a definitive direction on how necessary time can be estimated. The estimation may need to be adjusted if more detailed information is made available or if factors change. In all cases where adjustments are made to the appropriate starting point, sufficient evidence and records shall be maintained to justify variations.

Guide to determine auditor time for the initial audit: To be used in conjunction with ISO/IEC 27006, Annex B, Table 1, Audit Time Chart and additionally by reference to ISO/IEC 27006, Annex C, Methods for Audit Time Calculations. ISO/IEC 27006 Amd 1 clause B.3.6 and B.6 replace relevant text in 27006 and should be used during the calculation process.

- When the client has an all-inclusive scope, then all personnel at the location(s) to be registered that are under the control of the ISMS management system (i.e. fulfill requirements within 27001 or have Annex A controls applied to their activity) are counted (i.e., the total number of persons doing work under the organization's control for all shifts within the scope of the certification). That includes both employees and contractors at the locations to be registered, and becomes the starting point for the calculation.
- If the organization has a limited scope, then the count is based on the limited scope.

7.2.2 A full assessment of all ISO/IEC 27001 requirements is mandated for any organization transitioning from an already existing ISO 9001 conforming system to ISO/IEC 27001 that was not previously assessed using qualified ISMS auditors and the requirements of this document.

7.3 The audit team shall record all nonconformances identified during an assessment on form R20.35. The team leader shall assign a nonconformance to the categories of "Major" (HOLD) or "Minor". These are defined in section 2.

7.4 Multiple site sampling decisions in the area of ISMS registration are more complex than the same decisions are for non-technical management systems. SRI addresses the full range of issues below in the building of their sampling program and in accord with SRI Multi-Site Sampling documented information.

Prior to undertaking its first assessment based on sampling, SRI shall provide to the accreditation body the methodology and procedures which it employs, and provide demonstrable evidence of how these take account of the issues below to manage multiple site ISMS assessment.

SRI's procedures should ensure that the initial contract review identifies, to the greatest extent possible, the difference between sites such that an adequate level of sampling is determined in accordance with the provisions below.

Where an organization has a number of similar sites covered by a single ISMS, a certificate may be issued to the organization to cover all such sites provided that:

A. all sites are operating under the same ISMS, which is centrally administered and audited and subject to central management review;

B. all sites have been audited in accordance with the organization's internal security review procedure(s);

C. a representative number of sites have been sampled by the certification/ registration body, taking into account the requirements below:
   1) the results of internal audits of head office and the sites,
   2) the results of management review,
   3) variations in the size of the sites,
   4) variations in the business purpose of the sites,
   5) complexity of the ISMS,
   6) complexity of the information systems at the different sites,
   7) variations in unique processes and working practices,
   8) variations in activities undertaken,
   9) potential interaction with critical information systems or information systems processing sensitive information,
   10) differing legal requirements;

D. the sample should be partly selective based on the above in point c) and partly non-selective and should result in a range of different sites being selected, without excluding the random element of site selection;

E. every site included in the ISMS which is subject to significant threats to assets, vulnerabilities or impacts should be audited by the certification/ registration body prior to certification/ registration;

F. the surveillance program should be designed in the light of the above requirements and should, within a reasonable time, cover all sites of the organization or within the scope of the ISMS certification/ registration included in the Statement of Applicability;

G. in the case of a nonconformity being observed either at the head office or at a single site, the corrective action procedure should apply to the head office and all sites covered by the certificate/ registration.

The Audit described below should address the organization's head office activities to ensure that a single ISMS applies to all sites and delivers central management at the operational level. The audit shall address all the issues outlined above.

7.5 **Initial Stage 1 Audit**

During the on-site Stage 1 certification audit, the following must be provided to SRI:

A. general information concerning the ISMS and activities it covers,
B. a copy of the ISMS documentation as required in 27001, and mandatory supporting documentation including Risk Assessment and Control Selection documented information.

Objective of the Stage 1 audit is to provide a focus for planning the Stage 2 audit by gaining an understanding of the organization's ISMS policy and objectives and preparedness for the Stage 2 audit. The Stage 1 should not be restricted to a documentation review. The documentation review shall be completed prior to the commencement of the Stage 2 audit.

A. Results of the Stage 1 shall be documented in a written report.
B. SRI will review the report before deciding to proceed to the stage 2 audit and selection of team members with the necessary competence.
C. SRI makes the organization aware of the types of information and records

required for examination at the stage 2 event.

7.6 Stage 2 Audit

An audit plan is drafted based on any corrective action notifications documented at the stage 1 event. Objectives of the Stage 2 audit are:

A. To confirm that the organization adheres to its own policies, objectives and procedures;
B. To confirm that the ISMS conforms to all the requirements of ISO/IEC 27001 and is achieving the organization's policy objectives;
C. Focus on:
    1) Information security risks,
    2) Documentation requirements listed in clause 4.3.1 of ISO/IEC 27001,
    3) Selection of controls and control objectives based on the risk assessment and risk treatment process,
    4) Review the effectiveness of the ISMS, verification of the effectiveness confirmed through test and/or observation of the performance of security controls, and review of the achievement of ISMS objectives,
    5) Internal ISMS Audits and Management Reviews (at least one full cycle of internal audits and management reviews performed),
    6) Management responsibility for the IS policy,
    7) Correspondence between selected and implemented controls, the Statement of Applicability, results of the risk assessment and risk treatment process, ISMS policy and objectives,
    8) Implementation of controls,
    9) Programs, processes, procedures, records, internal audits and reviews of the ISMS effectiveness to ensure traceability to management decisions and the ISMS policy and objectives.

D. Require the organization to demonstrate that the analysis of security related threats is relevant and adequate for the organization;
E. 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 ISMS;
F. If documentation is combined with other management systems, the ISMS must be clearly identified along with appropriate interfaces to other systems.

7.7 Audit Team Conclusions and Reporting

7.7.1 SRI shall present the audit report to the client which includes references to clauses/processes listed in the ISO/IEC 27001, current edition, as a minimum, stating its conclusions on conformance and effectiveness of the security system overall to the ISO/IEC 27001 requirements. The assessment shall be documented in an appropriate notebook or an electronic facsimile. The Team leader shall advise whether recorded nonconformance(s) jeopardize an existing certificate. In the event that registration is denied or suspended, an appropriate course of action shall be agreed between the organization and SRI. Where there is a failure to agree on a course of action, the appropriate appeals procedure (QP 8.0) of SRI may be invoked.

7.7.2 The report must provide the following information;

A. An account of the audit and summary of the documentation review;

B. An account of the organization's information security risk analysis including selection and implementation of effective controls;
C. Total time used, time spent on documentation, assessment of risk analysis, on-site audit and audit reporting;
D. Audit enquires that have been followed, rational for their selection, and methodology employed;
E. Audit Corrective Action Notifications responses from the organization must be of sufficient detail to facilitate and support a certification decision and also contain:
    1) Areas covered by the audit, including audit trails and methodology utilized;
    2) Observations made, both positive and negative;
    3) Details of nonconformities identified, supported by objective evidence and a reference to the requirements of the ISMS standard on R20.35;
    4) Comments on conformity with a clear statement on nonconformity, a reference to the Statement of Applicability, and where applicable, a comparison to the results of the previous audit;
    5) The report must consider the adequacy of the internal organization and procedures adopted by the organization to give confidence in the ISMS, including the Operational Requirements established by the organization for personnel under their control;
    6) The report should also cover the degree of reliance placed on internal ISMS audits and management reviews, summary of observations regarding the implementation and effectiveness of the ISMS and a recommendation on whether the organization's ISMS should be certified or not;
    7) A surveillance report will contain information on the clearing of nonconformities previously identified that are indicated in 7.8.E.

7.8 **Surveillance Activities and Renewals**

SRI conducts surveillance audits and re-assessments in accordance with ISO/IEC 17021-1and the requirements of SRI guidance documentation. These organizations may also be subject to witness audits as previously described. The Lead Auditor is responsible for the ISO/IEC 27001 Audit Program (R20.23ISMS). The audit program is established for each certificate cycle, at the start of the cycle.

A. Initial assessments shall cover the entire scope of the ISMS as per the ISO/IEC 27001 standard minus verified exclusions.
B. Surveillance shall be conducted, as a minimum, once per year.
C. During a three-year period, the entire ISMS must be assessed against the ISO/IEC 27001 Standard with important/critical areas covered during surveillance in accordance with IAF Guidance.
D. Surveillance audits normally cover:
    1) System maintenance elements (Internal audits, Management review, Corrective and Preventive action, and Continuous Improvement);
    2) Communications from external bodies and other documents required for certification;
    3) Changes to the documented system;
    4) Areas subject to change;
    5) Selected elements of the ISMS standard;
        a) Operational Requirements are those requirements identified by the organization and placed upon personnel that are "under the control" of the organization. Examples of Operational Requirements include assessment of: any open computers for

access, filing cabinets to check if they were locked, check access doors and camera controls. Review samples of equipment to verify they are of the asset list, interviews with employees regarding the organizations ISO/IEC 27001 policy and their specific responsibilities regarding adherence to identified security controls, etc. Operational Requirement are identified as a specific activity on the audit program and must be included at each stage 1 / stage 2 and or renewal audit. Operational requirements are included as an activity for a least one of the surveillance activities but can be planned at additional surveillance events at the discretion of the Lead Auditor.

6) Other selected areas as appropriately prioritized for review;
7) Effectiveness with regard to achieving objectives of the information security policy and security control implementations;
8) Functioning of procedures for the periodic review of compliance with relevant legislation and regulations;
9) Action taken on nonconformities identified during the last audit.

E. SRI will adapt its surveillance program to the information security issues related threats to assets, and vulnerabilities and impacts on the organization.
F. Use of the mark will be audited.
G. SRI will check the records of appeals and complaints and any failure to meet the requirements, and that the organization has investigated its own ISMS and procedures and taken appropriate corrective action.

7.9 **Certification/Registration**

7.8.1 SRI is responsible for ensuring the continued integrity and validity of the certificates it issues and for drawing up and implementing a procedure to enable it to carry out this responsibility.

7.8.2 For the ISMS Sector qualification program, accredited registration documents shall be in the form of a certificate. Letters of conformance and unaccredited assessment statements, if any, shall be clearly distinguishable from accredited certificates.

7.8.3 The certificate(s) shall include the following information at a minimum:

A. The appropriate version of the ISO/IEC 27001 Standard.
B. The assessment was performed in accordance with the requirements of ISO/IEC 17021-1and ISO/IEC 27006
C. Effective date and Expiration dates, with a maximum period of three years.
D. Scope of Registration.

7.8.4 If desired, separate certificates for the applicable ISO/IEC 27001 and ISO 9001 may be issued.

7.8.5 All certificates shall be specific in terms of the scope of the ISMS and the standard(s) being covered.

7.8.6 The certificate(s) shall have marks in accordance with the ANAB requirements. In case of misuse of the marks or logos by SRI, the accreditation may be suspended or withdrawn, or when ANAB detects systemic findings.

7.8.7 If any member of the RRP and/or the Certification Director, reject the registration process, or disagree with the Audit Team, SRI shall attempt to correct or resolve any items or issues that are the basis for disapproval. If an agreement cannot be reached between the two RRP members and the Certification Director, the Certification Director shall in writing submit the RRP conclusions to the President & COO for resolution. The CEO will then choose a third properly qualified individual. The third individual then resolves the issue through majority agreement. (QP-3)

8.0 Authentication and Oversight of Accreditation Bodies, Certification/Registration Bodies, and Auditors

8.1 ANAB shall have primary responsibility to oversee the activities of all recognized organizations under this system.

8.2 Sector qualification of SRI shall be approved by the ANAB and be conducted in accordance with procedures and the requirements of ISO/IEC 27001, current edition. This includes an annual ANAB review to evaluate the effectiveness of the process for recognition of SRI. The review shall be in accordance with ANAB procedures.

8.3 SRI's Audit Management Program has been approved to meet requirements of ISO/IEC 27001 via ANAB oversight. Only individual SRI locations are approved by ANAB. SRI activity can be conducted at any location contingent on local regulations/requirements. All assessments shall be in accordance with the approved office/program management and requirements.

8.4 Oversight performed by other member companies on ANAB or SRI, including witness audit results, shall be used by ANAB and SRI assessment. Any issues resulting from oversight should be relayed to SRI for action and follow-up.

8.5 SRI's internal appeals/complaint process is to be used before other actions are taken. If any client cannot resolve issues with SRI then the matter shall be referred to ANAB. If the problem is related to SRI performance and cannot be resolved to the satisfaction of the organization or the OEM(s) involved, and when all levels of appeal have been exhausted, the matter may be referred to ANAB.

8.6 ANAB may suspend or withdraw the sector qualification of SRI.

8.7 Auditor credentials are valid for three years and may be renewed based on the proof of continuing education and performance of required assessment per paragraph 6.3 above.

9.0 Records of Applicants and clients

9.1 Records are retained for the duration of the current cycle plus one full certification cycle.

Note: In some jurisdictions, the law stipulates that records need to be maintained for a longer time period.