R20.109SRSMS ISO 28000:2022 Security and Resilience – Security Management Systems Supplement

1.0 **Scope** - This R20.109 applies to organizations requiring assessment and/or registration of their Security and Resilience security management system in accordance with ISO 28000:2022 and ISO/IEC 28003:2007.

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 28003:2007 and normative documentation are complementary (not alternative) to the technical specified requirements and applicable law and regulatory requirements.

The International Organization for Standardization (ISO) and associated International Accreditation Forum (IAF) Accrediting Bodies have established certain minimum expectations for Certifying Bodies (CB) who wish to accredit their Security and Resilience- Security Management Systems (SRSMS) for auditing against ISO 28001:2007. Fulfillment of these expectations is based upon the successful satisfaction of the requirements of ISO 28003:2007 and relevant applicable supplemental requirements in ISO/IEC 17021, ISO 28000:2022, and ISO 28001:2007.

The interpretations (necessary for provisioning of requirements and achievement of Accrediting Body approval - required to perform accredited audit and third-party registration/certification for ISO 28000:2022 and ISO 28001:2007 certification adjudications) are outlined in the remainder of this document. These requirements have been interpreted by experienced, knowledgeable security and management system professionals with significant Security and Resilience Management experience and analyzed to reflect and interpret requirements in terms of practical audit performance and experience in multiple venues.

It is incumbent upon potential Security and Resilience Security Management System cognizant management and audit personnel to perform comprehensive study and seek training regarding the entire set of ISO 2800X Requirements Specifications, Best Practice Requirements and Guidance, Implementation Guidance, and related supplemental and supplanting documentation relevant to specific industries and business sectors in order to successfully validate and interpret requirements for any particular SRSMS implementation and audit.

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 Security and Resilience Security Management System. It provides requirements for auditing organizations to ISO/IEC 28003:2007 and normative documented information and aligns with current ISO/IEC 17021-1:2015 and ISO/IEC 28003:2007 guidance.

1.2 **References**

A. EA-7/03 – February 2000 – EA Guidelines for Accreditation of Bodies Operating Certification/Registration of Information Security Management Systems.

B. ISO 28003:2007 – Security Management Systems for the Supply Chain – Requirements for bodies providing audit and certification of supply chain security management systems.

C. ISO 28000:2022 – Specification for Security and Resilience Security Management Systems.

D. ISO 28001:2007 – Security management systems for the supply chain- Best practices for implementing supply chain security, assessments, and plans – Requirements and guidance

E. ISO/IEC 17021-1:2015 – Conformity assessment – Requirements for bodies providing audit and certification of management systems.

2.0 **Definitions**

2.1 For the purposes of this document, the terms and definitions given in ISO 22300 and the following apply;

2.1.2 ISO Online browsing platform: available at *https://www.iso.org/obp*

2.1.3 IEC Electropedia: available at *https://www.electropedia.org/*

3.0 **General**

3.1 The second edition of ISO 28000:2022 cancels and replaces the first edition (ISO 28000:2007), which has been technically revised, but maintains all existing requirements to provide continuity for organizations using the previous edition. The main changes between the first edition and the second edition are;

A. Recommendations on principles have been added to clause 4 to give better coordination with ISO 31000

B. Recommendations have been added to clause 8 for better consistency with ISO 22301, facilitating integration including (1) security strategies, procedures, processes, and treatments, and (2) security plans

1) Alignment with Annex SL modifications to management system standards

2) Alignment with the PDCA model

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.

3.3 This document is not intended to add to, minimize, or in any way modify the requirements of the standard(s) identified herein and the requirements for accredited certification to these standard(s). It is meant to be a guidance tool for SRSMS Management and Auditors to set and provide a common understanding on the intent of the standard and accreditation requirements. In addition, it is meant to provide further definition and clarification of text of ISO 28003:2007 for Certifying Bodies seeking accreditation and wishing to perform audits and certification to these series of standards.

In order to become accredited to ISO 28003:2007, meet accrediting body scheme requirements, and satisfy certifying body requirements for audit against ISO 28000:2022 and ISO 28001:2007, the certifying organization must provide objective evidence of the implementation of a management system based on relevant policy, procedures, processes, and activities to manage and control business operations, certification and audit activities, and direct and control management, auditor, and external contractor personnel.

4.0 **Requirements for SRI**

4.1 SRI is fully accredited by the ANSI National Accreditation Board (ANAB) and Raad voor Accreditatie Accreditation Mark (RvA), in accordance with ISO/IEC 17021-1:2015 current version or equivalent for ISO 9001:2015. SRI has completed the application for ISO 28000:2022 and submitted same for review and consideration/approval by ANAB. Security and Resilience sector qualification consists of an application review, witness audit, and recommendation for the recognition of SRI's Security and Resilience- Security Management System program.

4.2 SRI has prepared an application form for the applicable Security and Resilience Security Management System (SRSMS) registration. This application provided the ANAB with confidence that SRI has developed the necessary documented process to meet ISO 28000:2022 requirements.

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 28000:2022-based witness audit per year.

4.4 SRI affords ANAB and applicable Authorities the right of review of records and information related to their SRSMS 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 9001:2015 and other management system standards. This accreditation is in accordance with ISO/IEC 17021-1:2015 for 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 28000:2022.

A. The essential elements of competence required to perform SRSMS certification/ registration are to select, provide training, 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 28003:2007.

5.3 SRI's processes and requirements to obtain ISO 28000:2022 sector qualification include as a minimum:

A. Evidence that the SRI has individuals with appropriate background, experience, and knowledge. (Contract Review will have Oversight by that individual.) Knowledge and competence is gained by attending and passing an internal ISO 28000:2022 Transition Auditor course. Items listed under "B" below are also added competencies gained by attending the ISO 28000:2022 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) A basic knowledge of the requirements of ISO 28000:2022 and related standards in the series
2) A basic knowledge of Security and Resilience in SRSMS Management Systems
3) Understanding of the processes, procedures, and plans necessary to design, document, and implement a Security and Resilience Security Management System (SRSMS) conforming to the requirements of ISO 28000:2022

4) Basic knowledge of International and Country-specific Legal and Regulatory requirements for the Security and Resilience in the Security Management Systems
5) Understanding of concepts, tools, and methodologies for assessing and managing Security and Resilience in Security Management Systems
6) Understanding of Security and Resilience in Security Management System audit criteria
7) Understanding of Security Incident Management
8) Understanding of Continuity Management in Security management Systems
9) Understanding of the documented information and evidence necessary to display conformity to ISO 28000:2022

This training is gained by attending and passing an approved ISO 28000:2022 Transition Auditor training course. Records of test completion and satisfactory course completion are maintained in SRI auditor/contractor files.

C. Documented auditor training program reviewed and approved by the ANAB prior to or during the qualification process that conforms to ISO 28000:2022 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 developed a Transition Auditor training course. Content of the training program content, context, and requirements satisfaction constitutes:
1) Applicability to the ISO 28000:2022 standard
2) Generally accepted course content, format, and training objectives
3) The scheme as used in the specific sector for Certification/Registration of ISO 28000:2022.

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 and/or supply chain security;
3) proof of attending and passing a 3-day SRSMS transition auditor course;
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 ISO/IEC 28000:2022 ISMS through Exemplar Global and/or IRCA is preferred, but not required and the auditor exhibits the following attributes: objectivity, maturity, discerning nature, analytical mind, persistence and objective realism;
6) understands complex operations and able to understand the role of individual units in a larger organization;
7) 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;
8) all relevant experience should be reasonably current;
9) 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 SRSMS audit.

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

H. No certificates or approvals to ISO 28000:2022 shall be issued by SRI unless all major and minor nonconformances are addressed with root cause analysis and corrective action evidence and effectiveness of implementation verified.

I. SRI will provide copies (when requested) of all information pertaining to the audit results, (including documented information, 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 and make available to the auditor a Statement of Application, Security Policy, Security Objectives, Security Strategies, Security Processes, Security Risk Assessment and Treatment Plans, and Security Declaration describing which parts of the SRSMS standard or normative document are relevant and applicable for the organization's SRSMS. In addition, a Security Plan conformant with the requirements of ISO 28000:2022 must be developed, and must include the following;

1) Purpose, scope, and objectives
2) Roles and responsibilities of implementation team
3) Actions to implement solutions
4) Information needed to activate actions
5) Internal and external dependencies
6) Resource requirements
7) Reporting requirements
8) Process for standing down
9) Recovery from temporary measures to restore organizational security to normal status

K. The SRI Lead Auditor will ensure during the Stage I Readiness assessment that the organization's Security and Resilience Security Management System scope, security declaration, and risk assessment properly reflect its activities and the boundaries of its supply chain applicability as defined in the SRSMS standard, Authorized Economic Operator (AEO) certification(s), and/or normative documentation, and will confirm that this is reflected in the organization's Statement of Application. Interfaces with services or activities that are not completely within the scope of the SRSMS shall be addressed as needed subject to applicable criteria and shall be included in the analysis of the organization's Security Management System risk assessment.

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 28000:2022 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 28000:2022 or current edition.

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

6.0 <u>Requirements for Auditors</u>

6.1 ISMS auditors shall, as a minimum, continually meet the education, training, work experience and audit experience of ISO 19011 and ISO 28003:2007 and satisfy the following criteria:

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 28000:2022 standard within the last three years. Auditors shall have the ability to cover all the clauses/elements as determined by the 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 SRSMS standard and applicable Authority normative documented information;
2) the concepts of management systems in general;
3) issues related to various areas of supply chain security, as specified in competency and knowledge requirements cited in ISO 28003:2022;
4) the principles and processes related to security and resilience in a security management system, including supply chain risk assessment and risk management;
5) principles relating to security management and supply chain security planning, documented information, control selection, and implementation. and
6) general management system and specific security and supply chain security management system auditing principles.

B. The auditor must be trained in SRSMS requirements. This training covers all those noted in A. above and as specified in ISO 28003:2022 or 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.

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 security management system and supply chain security and industry-specific AEO field(s),
   c) identifying security management and supply chain security threats,
   d) identifying the security management and supply chain vulnerabilities of the organization and business partners within the statement of application/SRSMS scope, and understanding the impacts, mitigation of risks, and selection of appropriate controls,

e) knowledge of current criteria, requirements, and technical and administrative guidance and requirements pertaining to applicable security management principles and supply chain sectors and AEO's,

f) knowledge of risk assessment related to security management and supply chain security.

2) The audit team should be competent to trace indications of security incidents in the organization's SRSMS back to the appropriate elements and components of the security management system, including relevant elements of the supply chain.

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 SRSMS auditor qualification, all auditors must participate in at least four SRSMS audits within 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 <u>Requirements for Assessment and Reporting</u>

7.1 <u>SRSMS Assessment Teams</u>

A. The assessment team leader must be a qualified SRSMS 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. SRSMS credentials are the minimum.

D. Auditor credentials shall be made available to organizations upon request.

7.1.1 SRI shall ensure that all members of the team are aware of the requirements of ISO/IEC 28000:2022 as may affect the scope of their assessment activity, consistent as a basis for the Security and Resilience- Security Management System. The SRSMS Lead Auditor shall provide guidance to the assessment team throughout the assessment on the interpretation of SRSMS 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 <u>Duration of Assessment</u>

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, breadth and depth of supply chain, 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.

A. Guide to determine auditor time for the initial audit: To be used in conjunction with ISO/IEC 27006:2015, Annex B, Table 1, Audit Time Chart and additionally by reference to ISO/IEC 27006:2015, Annex C, Methods for Audit Time Calculations.

B. 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 SRSMS security management system must be included. That includes both employees and contractors at the locations to be registered.

C. If the organization has a limited scope, then the count is broken into two categories (count for those 100% in scope, count for those partially in scope). SRI will identify a factor that estimates the percentage of applicable requirements and controls. This factor is known as the partial applicability factor.

1) For a limited scope, two calculation are made. First, those 100% within the limited scope will be applied to the table. Second, the total of all personnel partially within scope + those 100% within scope will be applied to the table. The difference between those two calculations will then be multiplied by the partial applicability factor. The additional time for those partially within scope will be added to the value for those 100% within scope for the total audit time.

2) If those personnel partially within scope fall within more than one partial applicability factor category (i.e., 10 are at 40%, 20 are at 15%), then the following alternative calculation method is used. This method coverts each group into an FTE and then goes to the table a single time based on total FTE count.

For example:

3 @ 100% in scope	3
10 @ 40% in scope	4
20@ 15% in scope	3

Total of 10 FTE applied to table.

7.2.2 A full assessment of all ISO 28000:2022 requirements is mandated for any organization transitioning from an already existing conforming management system that was not previously assessed using qualified 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 SRSMS 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 SRSMS 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 SRSMS, a certificate may be issued to the organization to cover all such sites provided that:

A. all sites are operating under the same SRSMS, 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 SRSMS,
   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 SRSMS 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 SRSMS certification/ registration included in the Statement of Application and Security Plan;

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 SRSMS 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 the SRI auditor, for use during the conduct of the audit:

A. general information concerning the SRSMS and activities it covers,

B. the SRSMS documentation as required, and mandatory supporting documentation including Security Plan, 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 SRSMS 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 SRSMS conforms to all the requirements of ISO 28000:2022 and is achieving the organization's security and resilience management policy and objectives;
C. Focus on:
   1) Security risks,
   2) Documentation requirements listed in clause 7.5 of ISO 28000:2022,
   3) Selection of controls and control objectives based on the risk assessment and risk treatment process,
   4) Review the effectiveness of the SRSMS, verification of the effectiveness confirmed through test and/or observation of the performance of security controls, and review of the achievement of SRSMS objectives,
   5) Internal SRSMS Audits and Management Reviews (at least one full cycle of internal audits and management reviews performed),
   6) Management responsibility for the security policy,
   7) Correspondence between selected and implemented controls, the Statement of Application, results of the risk assessment and risk treatment process, SRSMS security policy, plan, and objectives,
   8) Implementation of controls,
   9) Programs, processes, procedures, records, internal audits and reviews of the SRSMS effectiveness to ensure traceability to management decisions and the SRSMS 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 security threats, vulnerabilities, or impacts are identified as being significant and is managed within the SRSMS;
F. If documentation is combined with other management systems, the SRSMS 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 ISO 28000:2022, stating its conclusions on conformance and effectiveness of the security and resilience management system against overall requirements. The assessment shall be documented. 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 security and resilience 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 SRSMS standard on R20.35;
  4) Comments on conformity with a clear statement on nonconformity, a reference to the Statement of Application, 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 SRSMS, including the Operational Requirements as established in clause 8 of ISO 28000:2022;
  6) The report should also cover the degree of reliance placed on internal SRSMS audits and management reviews, summary of observations regarding the implementation and effectiveness of the SRSMS and a recommendation on whether the organization's security management system 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 17021-1:2015 and 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 28000:2022 Security Management System Audit Program (R20.23SRSMS). 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 SRSMS as per the applicable standards minus verified exclusions.
B. Surveillance shall be conducted, as a minimum, once per year.
C. During a three-year period, the entire SRSMS must be assessed against the applicable standards 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 SRSMS standard;
    a) Operational Requirements are those requirements identified by the organization and placed upon personnel that are “under the control” of the organization. Operational Requirements are identified as a specific activity on the security management system 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 security management system policy, plan, 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 SRSMS and procedures and taken appropriate corrective action.

7.9 <u>Certification/Registration</u>

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 SRSMS 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 28000 Standard.
B. The assessment was performed in accordance with the requirements of ISO/IEC 17021-1 and ISO 28003 (current versions)
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 standards may be issued.

7.8.5 All certificates shall be specific in terms of the scope of the SRSMS 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 rejects the registration process, or disagrees 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 Vice President, Certification, the Vice President, Certification 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 28000:2022. 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 28000:2022 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.